http://www.icact.org/journal.asp

ICACT-TACT JOURNAL

Transactions on Advanced Communications Technology

Volume 10 Issue 1,2,3,4,5,6, 2021, ISSN: 2288-0003

Editor-in-Chief
Prof. Thomas Byeongnam YOON, PhD.

GIRI
Global IT Research Institute

Journal Editorial Board

■ Editor-in-Chief

■ Editors

Dr. Youssef SAID, Tunisie Telecom, Tunisia
Dr. Noor Zaman, King Faisal University, Al Ahsa Hofuf, Saudi Arabia
Dr. Srinivas Mantha, SASTRA University, Thanjavur, India
Dr. Shahriar Mohammadi, KNTU University, Iran
Prof. Beonsku An, Hongik University, korea
Dr. Guanbo Zheng, University of Houston, USA
Prof. Sangho Choe, The Catholic University of Korea, korea
Dr. Gyanendra Prasad Joshi, Yeungnam University, korea
Dr. Tae-Gyu Lee, Korea Institue of Industrial Technology(KITECH), korea
Prof. Ilkyeun Ra, University of Colorado Denver, USA
Dr. Yong Sun, Beijing University of Posts and Telecommunications, China
Dr. Yulei Wu, Chinese Academy of Sciences, China
Mr. Anup Thapa, Chosun University, korea
Dr. Vo Nguyen Quoc Bao, Posts and Telecommunications Institute of Technology, Vietnam
Dr. Harish Kumar, Bhagwant institute of technology, India
Dr. Jin REN, North china university of technology, China
Dr. Joseph Kandath, Electronics & Commn Engg, India
Dr. Mohamed M. A. Moustafa, Arab Information Union (AIU), Egypt
Dr. Mostafa Zaman Chowdhury, Kookmin University, Korea
Prof. Francis C.M. Lau, Hong Kong Polytechnic University, Hong Kong
Prof. Ju Bin Song, Kyung Hee University, korea
Prof. KyungHi Chang, Inha University, Korea
Prof. Sherif Welsen Shaker, Kuang-Chi Institute of Advanced Technology, China
Prof. Seung-Hoon Hwang, Dongguk University, Korea
Prof. Dal-Hwan Yoon, Semyung University, korea
Prof. Chongyang ZHANG, Shanghai Jiao Tong University, China
Dr. H K Lau, The Open University of Hong Kong, Honh Kong
Prof. Ying-Ren Chien, Department of Electrical Engineering, National Ilan University, Taiwan
Prof. Mai Yi-Ting, Hsiuping University of Science and Technology, Taiwan
Dr. Sang-Hwan Ryu, Korea Railroad Research Institute, Korea
Dr. Yung-Chien Shih, MediaTek Inc., Taiwan
Dr. Kuan Hoong Poo, Multimedia University, Malaysia
Dr. Michael Leung, CEng MIET SMIEEE, Hong Kong
Dr. Abu sahman Bin mohd Supa'at, Universiti Teknologi Malaysia, Malaysia
Prof. Amit Kumar Garg, Deenbandhu Chhotu Ram University of Science & Technology, India
Dr. Jens Myrup Pedersen, Aalborg University, Denmark
Dr. Augustine Ikechi Ukaegbu, KAIST, Korea
Dr. Jamshid Sangirov, KAIST, Korea
Prof. Ahmed Dooguy KORA, Ecole Sup. Multinationale des Telecommunications, Senegal
Dr. Se-Jin Oh, Korea Astronomy & Space Science Institute, Korea
Dr. Rajendra Prasad Mahajan, RGPV Bhopal, India
Dr. Woo-Jin Byun, ETRI, Korea
Dr. Mohammed M. Kadhum, School of Computing, Goodwin Hall, Queen's University , Canada
Prof. Seong Gon Choi, Chungbuk National University, Korea
Prof. Yao-Chung Chang, National Taitung University, Taiwan
Dr. Abdallah Handoura, Engineering school of Gabes - Tunisia, Tunisia
Dr. Gopal Chandra Manna, BSNL, India

Dr. Il Kwon Cho, National Information Society Agency, Korea
Prof. Jiann-Liang Chen, National Taiwan University of Science and Technology, Taiwan
Prof. Ruay-Shiung Chang, National Dong Hwa University, Taiwan
Dr. Vasaka Visoottiviseth, Mahidol University, Thailand
Prof. Dae-Ki Kang, Dongseo University, Korea
Dr. Yong-Sik Choi, Research Institute, IDLE co., ltd, Korea
Dr. Xuena Peng, Northeastern University, China
Dr. Ming-Shen Jian, National Formosa University, Taiwan
Dr. Soobin Lee, KAIST Institute for IT Convergence, Korea
Prof. Yongpan Liu, Tsinghua University, China
Prof. Chih-Lin HU, National Central University, Taiwan
Prof. Chen-Shie Ho, Oriental Institute of Technology, Taiwan
Dr. Hyoung-Jun Kim, ETRI, Korea
Prof. Bernard Cousin, IRISA/Universite de Rennes 1, France
Prof. Eun-young Lee, Dongduk Woman s University, Korea
Dr. Porkumaran K, NGP institute of technology India, India
Dr. Feng CHENG, Hasso Plattner Institute at University of Potsdam, Germany
Prof. El-Sayed M. El-Alfy, King Fahd University of Petroleum and Minerals, Saudi Arabia
Prof. Lin You, Hangzhou Dianzi Univ, China
Mr. Nicolai Kuntze, Fraunhofer Institute for Secure Information Technology, Germany
Dr. Min-Hong Yun, ETRI, Korea
Dr. Seong Joon Lee, Korea Electrotechnology Research Institute, korea
Dr. Kwihoon Kim, ETRI, Korea
Dr. Jin Woo HONG, Electronics and Telecommunications Research Inst., Korea
Dr. Heeseok Choi, KISTI(Korea Institute of Science and Technology Information), korea
Dr. Somkiat Kitjongthawonkul, Australian Catholic University, St Patrick's Campus, Australia
Dr. Dae Won Kim, ETRI, Korea
Dr. Ho-Jin CHOI, KAIST(Univ), Korea
Dr. Su-Cheng HAW, Multimedia University, Faculty of Information Technology, Malaysia
Dr. Myoung-Jin Kim, Soongsil University, Korea
Dr. Gyu Myoung Lee, Institut Mines-Telecom, Telecom SudParis, France
Dr. Dongkyun Kim, KISTI(Korea Institute of Science and Technology Information), Korea
Prof. Yoonhee Kim, Sookmyung Women s University, Korea
Prof. Li-Der Chou, National Central University, Taiwan
Prof. Young Woong Ko, Hallym University, Korea
Prof. Dimiter G. Velev, UNWE(University of National and World Economy), Bulgaria
Dr. Tadasuke Minagawa, Meiji University, Japan
Prof. Jun-Kyun Choi, KAIST (Univ.), Korea
Dr. Brownson ObaridoaObele, Hyundai Mobis Multimedia R&D Lab , Korea
Prof. Anisha Lal, VIT university, India
Dr. kyeong kang, University of technology sydney, faculty of engineering and IT , Australia
Prof. Chwen-Yea Lin, Tatung Institute of Commerce and Technology, Taiwan
Dr. Ting Peng, Chang'an University, China
Prof. ChaeSoo Kim, Donga University in Korea, Korea
Prof. kirankumar M. joshi, m.s.uni.of baroda, India
Dr. Chin-Feng Lin, National Taiwan Ocean University, Taiwan
Dr. Chang-shin Chung, TTA(Telecommunications Technology Association), Korea

Editor Guide

■ Introduction for Editor or Reviewer

All the editor group members are to be assigned as a evaluator(editor or reviewer) to submitted journal papers at the discretion of the Editor-in-Chief. It will be informed by eMail with a Member Login ID and Password.

Once logined the Website via the Member Login menu in left as a evaluator, you can find out the paper assigned to you. You can evaluate it there. All the results of the evaluation are supposed to be shown in the Author Homepage in the real time manner. You can also enter the Author Homepage assigned to you by the Paper ID and the author's eMail address shown in your Evaluation Webpage. In the Author Homepage, you can communicate each other efficiently under the peer review policy. Please don't miss it!

All the editor group members are supposed to be candidates of a part of the editorial board, depending on their contribution which comes from history of ICACT TACT as an active evaluator. Because the main contribution comes from sincere paper reviewing role.

■ Role of the Editor

The editor's primary responsibilities are to conduct the peer review process, and check the final camera-ready manuscripts for any technical, grammatical or typographical errors.

As a member of the editorial board of the publication, the editor is responsible for ensuring that the publication maintains the highest quality while adhering to the publication policies and procedures of the ICACT TACT(Transactions on the Advanced Communications Technology).

For each paper that the editor-in-chief gets assigned, the Secretariat of ICACT Journal will send the editor an eMail requesting the review process of the paper.

The editor is responsible to make a decision on an "accept", "reject", or "revision" to the Editor-in-Chief via the Evaluation Webpage that can be shown in the Author Homepage also.

■ Deadlines for Regular Review

Editor-in-Chief will assign a evalaution group(a Editor and 2 reviewers) in a week upon receiving a completed Journal paper submission. Evaluators are given 2 weeks to review the paper. Editors are given a week to submit a recommendation to the Editor-in-Chief via the evaluation Webpage, once all or enough of the reviews have come in. In revision case, authors have a maximum of a month to submit their revised manuscripts. The deadlines for the regular review process are as follows:

Evalution Procedure	Deadline
Selection of Evaluation Group	1 week
Review processing	2 weeks
Editor's recommendation	1 week
Final Decision Noticing	1 week

■ Making Decisions on Manuscript

Editor will make a decision on the disposition of the manuscript, based on remarks of the reviewers. The editor's recommendation must be well justified and explained in detail. In cases where the revision is requested, these should be clearly indicated and explained. The editor must then promptly convey this decision to the author. The author may contact the editor if instructions regarding amendments to the manuscript are unclear. All these actions could be done via the evaluation system in this Website. The guidelines of decisions for publication are as follows:

Decision	Description
Accept	An accept decision means that an editor is accepting the paper with no further modifications. The paper will not be seen again by the editor or by the reviewers.
Reject	The manuscript is not suitable for the ICACT TACT publication.
Revision	The paper is conditionally accepted with some requirements. A revision means that the paper should go back to the original reviewers for a second round of reviews. We strongly discourage editors from making a decision based on their own review of the manuscript if a revision had been previously required.

■ Role of the Reviewer

Reviewer Webpage:

Once logined the Member Login menu in left, you can find out papers assigned to you. You can also login the Author Homepage assigned to you with the paper ID and author's eMail address. In there you can communicate each other via a Communication Channel Box.

Quick Review Required:

You are given 2 weeks for the first round of review and 1 week for the second round of review. You must agree that time is so important for the rapidly changing IT technologies and applications trend. Please respect the deadline. Authors undoubtedly appreciate your quick review.

Anonymity:

Do not identify yourself or your organization within the review text.

Review:

Reviewer will perform the paper review based on the main criteria provided below. Please provide detailed public comments for each criterion, also available to the author.

- How this manuscript advances this field of research and/or contributes something new to the literature?
- Relevance of this manuscript to the readers of TACT?
- Is the manuscript technically sound?
- Is the paper clearly written and well organized?
- Are all figures and tables appropriately provided and are their resolution good quality?
- Does the introduction state the objectives of the manuscript encouraging the reader to read on?
- Are the references relevant and complete?

Supply missing references:

Please supply any information that you think will be useful to the author in revision for enhancing quality of the paperor for convincing him/her of the mistakes.

Review Comments:

If you find any already known results related to the manuscript, please give references to earlier papers which contain these or similar results. If the reasoning is incorrect or ambiguous, please indicate specifically where and why. If you would like to suggest that the paper be rewritten, give specific suggestions regarding which parts of the paper should be deleted, added or modified, and please indicate how.

Journal Procedure

Dear Author,

- **You can see all your paper information & progress.**

- **Step 1. Journal Full Paper Submission**

Using the Submit button, submit your journal paper through ICACT Website, then you will get new paper ID of your journal, and send your journal Paper ID to the Secretariat@icact.org for the review and editorial processing. Once you got your Journal paper ID, never submit again! Journal Paper/CRF Template

- **Step 2. Full Paper Review**

Using the evaluation system in the ICACT Website, the editor, reviewer and author can communicate each other for the good quality publication. It may take about 1 month.

- **Step 3. Acceptance Notification**

It officially informs acceptance, revision, or reject of submitted full paper after the full paper review process.

Status	Action
Acceptance	Go to next Step.
Revision	Re-submit Full Paper within 1 month after Revision Notification.
Reject	Drop everything.

- **Step 4. Payment Registration**

So far it's free of charge in case of the journal promotion paper from the registered ICACT conference paper! But you have to regist it, because you need your Journal Paper Registration ID for submission of the final CRF manuscripts in the next step's process. Once you get your Registration ID, send it to Secretariat@icact.org for further process.

- **Step 5. Camera Ready Form (CRF) Manuscripts Submission**

After you have received the confirmation notice from secretariat of ICACT, and then you are allowed to submit the final CRF manuscripts in PDF file form, the full paper and the Copyright Transfer Agreement. Journal Paper Template, Copyright Form Template, BioAbstract Template,

Journal Submission Guide

All the Out-Standing ICACT conference papers have been invited to this "ICACT Transactions on the Advanced Communications Technology" Journal, and also welcome all the authors whose conference paper has been accepted by the ICACT Technical Program Committee, if you could extend new contents at least 30% more than pure content of your conference paper. Journal paper must be followed to ensure full compliance with the IEEE Journal Template Form attached on this page.

➢ How to submit your Journal paper and check the progress?

Step 1. Submit	Using the Submit button, submit your journal paper through ICACT Website, then you will get new paper ID of your journal, and send your journal Paper ID to the Secretariat@icact.org for the review and editorial processing. Once you got your Journal paper ID, never submit again! Using the Update button, you can change any information of journal paper related or upload new full journal paper.
Step 2. Confirm	Secretariat is supposed to confirm all the necessary conditions of your journal paper to make it ready to review. In case of promotion from the conference paper to Journal paper, send us all the .DOC(or Latex) files of your ICACT conference paper and journal paper to evaluate the difference of the pure contents in between at least 30% more to avoid the self replication violation under scrutiny. The pure content does not include any reference list, acknowledgement, Appendix and author biography information.
Step 3. Review	Upon completing the confirmation, it gets started the review process thru the Editor & Reviewer Guideline. Whenever you visit the Author Homepage, you can check the progress status of your paper there from start to end like this, " Confirm OK! -> Gets started the review process -> ...", in the Review Status column. Please don't miss it!

Volume. 10 Issue. 1

Volume. 10 Issue. 2

Volume. 10 Issue. 3

Volume. 10 Issue. 4

Volume. 10 Issue. 5

Volume. 10 Issue. 6

Early Detection of LDDoS Attacks in IoT Utilizing Locality Sensitive Incremental TSVM Method

Xiaochun Yin*, Zengguang Liu**, Deyong Liu***, Zhenge Liu****

*Blockchain Laboratory of Agricultural Vegetables, Weifang University of Science & Technology, Shouguang, Weifang, Shandong, China

**College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao, Shandong, China

***Shandong Software Engineering Technology Center, Weifang University of Science & Technology, Shouguang, Weifang, Shandong, China

****School of Software & Microelectronics, Peking University, Beijing, China

xiaochunyin@wfust.edu.cn, st.lzg@163.com, gm@univalsoft.com, 1931087307@qq.com

***Abstract*—The Mirai botnet and its variants has made Internet of Things (IoT) devices a powerful amplifying platform for Low-rate Distributed Denial-of-Service (LDDoS) attacks. In this paper, we firstly propose a new low-rate variant, which is a sophisticated crossfire low-rate DDoS attack mechanism. At the same time, we investigate and develop a novel semi-supervised Locality Sensitive Incremental Transductive Support Vector Machine (LS-ITSVM) method. The proposed method maximizes the margins of different network flows by incorporating local frequency-domain features from the autocorrelation sequence of network flow into the regularization time-domain framework of TSVM. And it saves training and detecting time by incremental training support vectors and new added samples. In experiments, we verify the proposed crossfire LDDoS is more concealed and harmful firstly. Then, the result in public dataset proves the proposed method can distinguish abnormal network flows with higher detection accuracy, faster training and response time, and prevent abnormal network flow groups with less impaction. At last, the results in private testbed prove LS-ITSVM is still available to new LDDoS variants.**

***Keyword*—LDDoS, Internet of Things, Locality Sensitive Incremental TSVM, Frequency-Domain Features, Semi-Supervised Clustering**

I. INTRODUCTION

DISTRIBUTED Denial-of-Service (DDoS) attacks, characterized by brute-force, sustained high rate or specifically designed to explore the protocol limitations or software vulnerabilities in services, are well-known. The difficulty of traditional internet DDoS is how to control as many as desktop computers, which has strong password, updated anti-virus software regularly, and unexpected off-line. With the emergence of IoT, things change. IoT devices have weak security configurations, lacked computational capabilities to run anti-virus, and constantly connected to Internet. As a result, it becomes soon a powerful amplifying platform for DDoS attacks. The recent prominent examples are Mirai botnet. According to the French webhost and cloud service provider OVH, a DDoS attack using Mirai malware hit them with 1.1 Tbps at peak by about 145K hacked cameras in September 2016 [1]. Moreover, hackers announced they could rent a Mirai botnet of 400K Bots only two months later [2]. Thus, researches tried to understand Mirai botnet operation and communication model [3], and proposed many feasible methods.

In order to dodge existing detection proposals, Mirai's variants with low-rate attack mechanisms start to obfuscate their DDoS activity and are becoming a serious threat to Internet. As we know, a successful DDoS attack needs to tune a tuple (T, R, L) of TCP at least. T is an integer multiple coincides with minRTO value of TCP; R is the peak rate and L is the burst length. In order to cause TCP packet loss and begin slow-start, R should be large enough and L should be longer than RTT value. As Fig. 1 shown, we simulated a LDDoS attacks of 4 Mirai Bots with the R of 50Kb/sec. For the purpose of drawing them clearly in Fig. 1, we start to attack one by one with a delay of 10ms. Obviously, we can see that the LDDoS attack stream hides itself among normal traffic by making its peak rate even lower than the normal

Manuscript received Dec. 14, 2020. This research was supported by Scientific Talent Fund Project of Weifang University of Science & Technology of China (Grant number: KJRC2021002) and was also supported by the Scientific Fund Project of Facility Horticulture Laboratory of Universities in Shandong of China (Grant number: 2018YY016) and Key Research and Development Program of Shandong, (Grant number: 2019GNC106034). , and a follow-up of the invited journal to the accepted & presented paper entitled " Early Detection of LDDoS Attacks in IoT Utilizing Locality Sensitive Incremental TSVM Method" of the 22th International Conference on Advanced Communication Technology (ICACT2020).

Xiaochun Yin is with the blockchain laboratory of agricultural vegetables, Weifang university of science & technology, China. (e-mail: xiaochunyin@wfust.edu.cn).

Zengguang Liu is with college of computer science and engineering, Shandong university of science and technology, China. (Corresponding author, phone: 18853688750; e-mail: st.lzg@163.com).

Deyong Liu is with Shandong software engineering technology center, Weifang university of science & technology, China. (e-mail: gm@univalsoft.com).

Zhenge Liu is with school of software & microelectronics, Peking university, China. (e-mail: 1931087307@qq.com).

traffic rate. All in all, compared with traditional DDoS attacks, LDDoS ones have three mainly characteristics: hard to detect, because it has same flow classified features with normal flow; low-cost and multi-targets, because the attacks can be finished in a few nodes with small flow data, they can be orchestrated to attack multiple targets simultaneously; long term attacked-target insensitive attacks, because attacked-target has self-adapt mechanism to adjust network flow. Thus, the aim of this paper is to have a method with high detection accuracy, fast response time to detect LDDoS attacks.

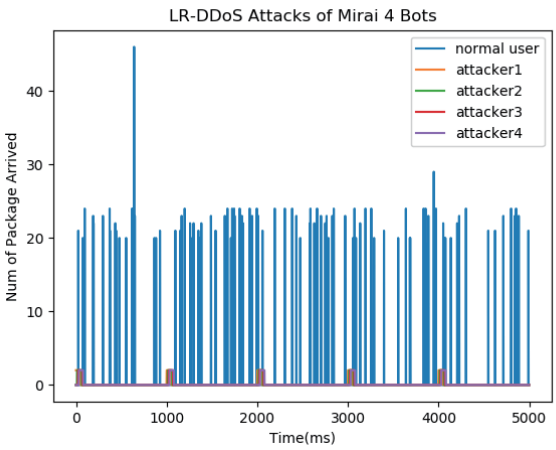


Fig. 1. LDDoS Attacks of Mirai 4 Bots

This paper is organized as follows: we firstly review the related state-of-the-art work in section II. Next, we work out a Mirai's variant: crossfire LDDoS by adding sophisticated low-rate TCP attack mechanisms and multiplexing algorithm to IoT DDoS in section III. And then, a novel semi-supervised Locality Sensitive Incremental Transductive Support Vector Machine (LS-ITSVM) method is proposed and described to address the new crossfire LDDoS in section IV. Next, simulation results are presented to show the effectiveness of defending against LDDoS attacks in Section V. Finally, Section VI concludes the paper with suggestive future enhancements.

II. RELATED WORK

After Mirai botnet, IoT botnets had received spread attention. Including traditional detection methods, researchers began to protect IoT with the skill of machine learning (ML) and Artificial Intelligence (AI) [4-7]. When LDDoS attacks came into the world, above methods were not applied to these new type attacks. As a result, researchers had to focus on new attacks, and a few defensive solutions had been existed in the literature. G. Kaur et al. [8] worked out a variant of the Shiryaev-Roberts's procedure to detect and deter these stealthy low-rate DoS attacks dynamically, using Checkpoint Anomaly Detection techniques. Z. Wu et al. [9] studied complex multifractal structure for developing concise mathematical models, and proposed an algorithm of multifractal detrended fluctuation analysis (MF-DFA), which is used to explore the change in terms of multifractal characteristics over a small scale of network traffic due to LDDoS attacks. ML and AI also were applied in LDDoS. Z. G. Liu et al. [10] proposed a new method to take frequency-domain characteristics from the autocorrelation sequence of network flow as clustering feature to group end-user flow data by BIRTH algorithm, and re-merge these clustering results into new groups by overcoming the deficiency of BIRTH algorithm. M. Yue et al. [11] investigated a new identification approach based on wavelet transform and combined neural network to classify normal network traffic and LDDoS attack traffic. Z. J. Wu et al. [12] used the propagation back (BP) model of neural network to establish the nonlinear model of network traffic, and proposed a method of LDDoS attacks detection based on particle filter according to the mechanism of LDDoS attack. In this method, the difference between the estimated value of the particle filter and the one step prediction is used as the detection basis, and a detection threshold is designed to determine the initiation and termination of the LDDoS attacks for the purpose of detecting LDDoS attacks. P. Nagar et al. [13] provided a comparative study between the ANN and the optimizer-based ANN technology. They concluded that the convolution neural network with SVM show effective analysis providing accurate forms of IDS, thereby improving its detection based on individual class along with maintaining its results fundamentally. X. Peng et al. [14] optimized a Mahalanobis distance by perturbing continuous features and discrete features of DDoS samples respectively, and proposed an improved boundary-based method to craft adversarial DDoS samples. M. Begli et al. [15] designed an intrusion detection system (IDS) using SVM algorithm, and proved its efficiency. P. Rivas et al. [16] implemented and trained a non-probabilistic binary linear attack pattern classifier, and trained a support vector machine and a convolutional neural network using a supervised learning model with labelled data sets. Experimental results suggested that the models can detect DDoS attacks with high accuracy rates. T. A. Tuan et al. [17] performed an experimental analysis of the machine learning methods (including Support Vector Machine, Decision Tree, Naive Bayes, and ANN) for Botnet DDoS attack detection. The evaluation is done on the UNBS-NB 15 and KDD CUP-99 which are well-known publicity datasets for Botnet DDoS attack detection. Results showed SVM has higher accuracy. Although these methods have high accuracy, they need more training and detecting time when new samples were labelled.

Based on above insights and the truth of massive untagged packages in IoT, we will propose and develop a novel semi-supervised LS-ITSVM method for higher detecting accuracy and fast training and response time. Additionally, we try to present a sophisticated IoT-Bots Multiplexing Method for crossfire LDDoS Attack, which is more powerful and stealthy.

III. CROSSFIRE LDDOS ATTACKS MODEL

In IoT era, there are huge number of Mirai bots. But lots of bots' attack capability are wasted, because there are many unused gaps between bursts, which can be well-organized to have another attack. Thus, hackers could be exactly leveraged on their large number of Mirai bots and divide them into several subsets to low individual traffic rates for hiding their attack behaviors further. At the same time, the bots' capability can be used fully to fire orchestrated crossfire attack [18, 19].

Crossfire attack [18] is a powerful attack that degrades and often cuts off network connections to a variety of selected server targets by flooding only a few network links. In its attack-flow assignment step, each bot can try its best to send attack flow without worrying about being discovered. Because there is an assumption that the middle routers only have failure

detection mechanism, instead of attack detection mechanism. However, it is not true in network world, especially in IoT world. For example, some attackers set the goal of bots multiplexing to form desired waves with fewest bots [20]. But these kind of attacking flow were detected easily by statistical approach in middle router's idle CPU circle. More researchers are hiring Software-Defined Networking (SDN) to control switches and routers placed at the network edges, which helps prevent LDDoS in time. If we use random ultra-low peak rate, existing detecting methods are hard to find these flows out. Thus, the question is how to work out an attacking plan based on a simple multiplexing method for the attackers. Fortunately, we can have lots of hacked bots in IoT, that is, we have chance to patch the gap on the bursts and make an efficient bot multiplexing scheme. Therefore, we use dynamic random fewest bots to fire attacks alternately. According to this idea, we propose the bots multiplexing low-rate algorithm as following algorithm 1. In this algorithm, one key point is to split bots' capability into random small ones, which can utilize much less bandwidth and resources. This will be harder to detect.

ALGORITHM 1: BOTS MULTIPLEXING ALGORITHM

Input: DelayMatrix = mat(NBOTS, NTARGETS); CapMatrix = mat(NBOTS, 1); TargetIPMatrix = mat(NTARGETS, 1);
Output: AttackPlan, which includes TargetBots, BeginTime and TargetIP.
Notes: NBOTS is the number of bots, while NTARGETS is the number of targets; MAXALLOWCAP is the max allowed capability of ultra-low-rate attack.

Procedure:

```
Initialize DelayMatrix based on detected delay time from bots to targets;
Initialized CapMatrix based on bots' max bandwidth;
for cap in range(CapMatrix):
    if cap >= MAXALLOWCAP:
        split into multiple parts, and insert them into CapMatrix random;
Set attacking count, attacking time(L) and peakrate(R);
for i in range(attacking count):
    for j in range(NTARGETS):
        random  k in range(NBOTS):
            if bots has been used in current attacking:
                continue;
            end if
            if bots ever used to attack this target:
                continue;
            end if
            if attacking peak rate has been met:
                break;
            end if
            if DelayMatrix[TargetBots[j][-1]][j]-DelayMatrix[k][j]>=L:
                update TargetBots by targetBots[j].append(k);
                update corresponding DelayMatrix line by
DelayMatrix[k][eachTarget] = DelayMatrix[k][eachTarget] + L;
            end if
        end random
    end for
    refresh TargetBots matrix when time up or most bots has been used;
end for
generate AttackPlan based on TargetBots, DelayMatrix and TargetIPMatrix;
```

IV. LOCALITY SENSITIVE ITSVM METHOD

In LDDoS attacks scenarios, attack flows almost have same classified features with normal flows, and they can fire long term attacked-target insensitive attacks. As a result, the traffic volume analysis method cannot detect such a stealthy attack any more. Recently, some researchers begin to introduce the semi-supervised TSVM methods [21-25]. The pros are that these methods can take use of the underlying geometric structure of unlabelled samples to train the classifier, while the cons are that they are not suitable for incremental learning and their training speed is too slow to meet IoT's requirement. In order to address above issues, we propose a novel locality sensitive incremental TSVM method in this paper. "Locality sensitiveness" helps to quickly locate which cluster the unlabelled data belongs to and speed up training. "Incremental TSVM" can help to do incremental learning by support vectors and prior classified unlabelled data.

A. Locality Sensitive Features Extraction

ALGORITHM 2: LOCALITY SENSITIVE FEATURES EXTRACTION ALGORITHM

Input: NetworkDataSet = mat(labeled dump network items); EntropyThresh;
Output: priComps = array(features). HashTable = array(hashBuckets)

Procedure:

```
Initialized FeatureList based on NetworkDataSet;
Set well-tuned EntropyThresh;
Calculate frequency-domain features based on time-domain features (PSD) based on DFT/FFT, and add it into FeatureList;
for features in FeatureList:
    Calculate its entropy based on (3);
end for
Extract features in ascending order by probability value based on EntropyThresh;
for vector in NetworkDataSet:
    Cast vector with extracted features by Hamming min-Distance algorithm, and generate h(vector);
end for
Generate hash buckets with same hash values;
Generate HashTable based on buckets.
```

The idea of locality sensitive is for solving the approximate in high dimensional spaces. It can help to map similar items to the same buckets with high probability. With it, the problem of "searching the similar samples in a huge data set" is turned to "searching them in a small bucket". Thus, the searching can speed up. In order to use locality sensitive, we need to satisfy the following conditions for any $x_1, x_2 \in M$:

- if $d(x_1, x_2) \le d_1$, then $h(x_1) = h(x_2)$ with probability at least P_1;
- if $d(x_1, x_2) \ge d_2$, then $h(x_1) = h(x_2)$ with probability at most P_2;

Here, M is data set space; d is a distant function in M; x_1, x_2 is vectors in M; d_1 and d_2 is the threshold of distance; h is a function used to map elements from M to a bucket $s \in S$.

As to x_1, x_2, we should choose them from training dataset well. In our case, if we review the Fig. 1 carefully, we find that there are always periodic low-rate rectangle shape waves. Generally, what exactly happens is that more power of the autocorrelation function is distributed in the lower frequency band if there is shrew stream contained in the traffic. Discrete Fourier Transform (DFT) and Fast Fourier Transformation (FFT) is exactly the mathematics method to convert a finite sequence of equally-spaced samples of a function into a same-length sequence of equally-spaced samples of the discrete-time Fourier transform. Thus, we add frequency-domain representations of time-domain features Power Spectrum Density (PSD) converted by DFT/FFT as new features.

After that, features subset is chosen by enhanced information entropy. Information entropy is the average rate at which information is produced by a stochastic source of data. The measure of information entropy associated with

each possible data value is the negative logarithm of the probability mass function for the value:

$$S = -\sum_i P_i \log P_i \quad (1)$$

When the data source produces a low-probability value, the event carries more "information" than when the source data produces a high-probability value. In order to use entropy in feature extraction, conditional probability is introduced into entropy definition. Now entropy is calculated based on event probability. Every feature value is treated as event. Thus, event entropy means the distribution of value. The re-definition of (1) is as following:

$$S(i,l) = \int P(x|\omega_i) \log P(x|\omega_i)\, dx \quad (2)$$

Here, $S(i,l)$ is the entropy of i^{th} feature value in single classification of l. Thus, the expectation of all classification would be $S(i)$, it is a reference point of different features. The formula can be defined as

$$S(i) = E\big(S(i,l)\big) = \sum_i S(i,l) P(\omega_i) \quad (3)$$

As to h, which aims to maximize the probability of a "collision" for similar items, there are several open-sourced and validated methods [26-28]. We can use any one of them directly. Here, we use minimal distance algorithm family in Hamming space [26]. Since it has a huge improvement compared to other algorithms.

B. *Incremental TSVM Algorithm*

TSVM extend SVMs in that they could treat partially labelled data in semi-supervised learning by following the principles of transduction. The key idea of TSVM is that it begins with a labelling of the test/predict data based on the classification of an inductive SVM. Then it improves the solution by switching the labels of test/predict examples so that the objective function decreases. In other words, TSVM can be treated as seeking an optimal solution in given labelled dataset: $\{(x_i, y_i)\}, i = 1, 2, \dots, n;\ x_i \in R_m;\ y_i \in \{+1, -1\}$; and unlabelled dataset: $x_1^*, x_2^*, \dots, x_k^*$, and it can be described as following:

$$\begin{aligned} &min\ V(y_1^*, \dots, y_k^*, \omega, b, \varepsilon_1, \dots, \varepsilon_i, \varepsilon_1^*, \dots, \varepsilon_k^*) \\ &= \tfrac{1}{2}||\omega||^2 + C\sum_{i=1}^{n}\varepsilon_i + C^*\sum_{j=1}^{k}\varepsilon_j^* \\ &\mathbf{s.t.} \\ &\forall_{i=1}^{n}: y_i[\omega \cdot x_i + b] \geq 1 - \varepsilon_i \quad (4) \\ &\forall_{j=1}^{k}: y_i[\omega \cdot x_j^* + b] \geq 1 - \varepsilon_j^* \\ &\forall_{i=1}^{n}: \varepsilon_i \geq 0 \\ &\forall_{j=1}^{k}: \varepsilon_j^* \geq 0 \end{aligned}$$

In (4), parameter C is the impact factors of hyperplane of labeled samples, while C^* is the impact factors of unlabeled samples; ξ_i and ξ_i^* are slack variables; $< \omega, b >$ is the hyperplane. For obtaining the optimal solution of (4), the first step is to set well-tuned C and C^* by historical experiment, and to learn the initialized SVM classifier based on labeled samples through induction method. The second step is to use this SVM classifier to classify all unlabeled samples, and mark only pairwise labels of positive and negative samples in support vectors nearby. The last step is to re-train SVM based on new chosen samples and labeled samples. Training procedure is repeated between step 2 and 3, until all unlabeled samples have their own classification. From above procedure, there are two disadvantages of transduction method. The one is that TSVM builds no predictive model. And the other one is if a previously unknown point is added to the set, the entire transductive algorithm would need to be repeated with all of the points in order to predict a label.

In real IoT environment, we need not only train a predictive model on limited labeled samples, but also adjust the model by new coming packages in real-time. Obviously, TSVM can be computationally expensive in this kind of case. Further, this might cause the predictions of some of the old points to change, which is unexpected in early warning system and is treated as false positive. After an in-depth study of TSVM, we find that "not all samples" play the same important role during learning the optimal solution of (4). These samples that meets the support vector conditions contribute a lot to find out optimal hyperplanes and decision functions. In general, the x_i whose lagrange multiplier's value a_i is between 0 and C ($0 < a_i < C$) is defined as normal vector, while the $\mathbf{x_i}$ whose lagrange multiplier's value a_i equals C ($a_i = C$) is defined as support vector. The later represents classified features of most samples, and can be learned to get the final classification. In other words, the set of support vectors can fully describe the features of the whole training set, learning in the set of support vectors is equivalent to learning in whole training set. Obviously, the scale of support vectors set is far smaller than training set. In every iterable training, only the support vectors are mentained and combined with the new added samples for new classifier. With this, TSVM has the capacity of incremental learning. The incremental TSVM algorithm can be described as following algorithm 3.

ALGORITHM 3: INCREMENTAL TSVM ALGORITHM

Input: NetworkDataSet = mat(labeled dump network items);
NewNetworkDataSet=mat(unlabeled network items);
Output: ITSVMClassifiers, LabledNewNetworkDataSet;
Notes: NetworkDataSet ∩ NewAddedNetworkDataSet=∅

Procedure:
1: Initialized NetworkDataSet;
2: Use TSVM algorithm to train NetworkDataSet, and get the base ITSVMClassifier, and SupportVecSet;
3: **while** (NewNetworkDataSet != NULL):
4: get k samples from NewNetworkDataSet; // k can be any pre-set value.
5: Generate new training set combined SupportVecSet and k, marked as NewTrainingSet;
6: Use TSVM algorithm to train NewTrainingSet to get NewITSVMClassifier, and NewSupportVecSet;
7: **end while**

ALGORITHM 4: INTEGRATED ALGORITHM OF LOCALITY SENSITIVE AND ITSVM

Input: $\mathbf{\Omega_o}, \mathbf{\Omega_k}$;
Output: classifier $f(x)$, predictedResults

Procedure:
1: create HashTable $\mathbf{H_o}$ and $\mathbf{\Omega_{o\ sv}}$ for $\mathbf{\Omega_o}$ per Algorithm 1 & 2;
2: **while** ($\mathbf{\Omega_i}$!= NULL && i<=k):
3: calculate hash vectors $\mathbf{h}(\mathbf{\Omega_i})$;
4: **for** each hash vectors $\mathbf{h}(\mathbf{\Omega_i})$:
5: **if** (vector exists in HashTable $\mathbf{H_{i-1}}$):
6: pre-mark the vector per the correlated label of HashTable $\mathbf{H_{i-1}}$;
7: pick up this vector into $\mathbf{\Omega_{i\ lsh}}$;
8: **end if**
9: **end for**
10: merge $\mathbf{\Omega_{i-1\ sv}}$ into $\mathbf{\Omega_{i\ lsh}}$ for $\mathbf{new\Omega_{i\ lsh}}$;
11: **do**
11: train classifier $f(x)$ based on $\mathbf{\Omega_o}$, $\mathbf{new\Omega_{i\ lsh}}$ per Algorithm 3;
12: classify $\mathbf{\Omega_{i\ lsh}}$ based on $f(x)$;
13: **if** (pre-marked values != predicted values)
14: unmark these values, and treat them as unlabeled samples;
15: **end if**
16: **while** (unlabeled samples != NULL)
17: report predictedResults for $\mathbf{\Omega_i}$;
18: generate new support vector set $\mathbf{\Omega_{i\ sv}}$;
19: create new HashTable $\mathbf{H_i}$;
20: **end while**

From algorithm 3, the biggest distinguished difference between incremental TSVM and SVM is that the learning samples of incremental SVM consist of only the support vectors of the learned samples and the new learning samples, while the SVM consists of all the learned samples and the new learning samples. Incremental TSVM discards some samples without losing classification accuracy. At the same time, its training time is speeded up.

C. *Integrated with Locality Sensitive and ITSVM*

Now that we have worked out locality sensitive features extraction method for locating and pre-labelling examples, at the same time, we have incremental TSVM for quickly incremental learning. Thus, we further integrate them together for semi-supervised learning quickly more and trying to improve classification accuracy by a small margin.

Assumed that there is a small labeled dataset Ω_o, the new sequenced added unlabeled dataset $\Omega_k(k = 1, \ldots, n)$. The support vector set correlated Ω_k is $\Omega_{k\ sv}$. The hash table of Ω_k is $\mathbf{H}_k$. $\mathbf{h}(\Omega_k)$ is used to represent hashed values vector. Samples set filtered by locality sensitive hash function is $\Omega_{k\ lsh}$. $f(x)$ is the classifier of ITSVM. With these, integrated algorithm of locality sensitive and ITSVM is detailed described as algorithm 4.

V. EXPERIMENTS AND RESULTS

A. *Crossfire LDDOS Attacks Experiments*

A.1 Experiment Environment

In order to verify that crossfire LDDoS attack has more concealment on the premise of maintaining the same attack effect. A crossfire LDDoS attack test platform is designed and implemented as shown in Fig. 2.

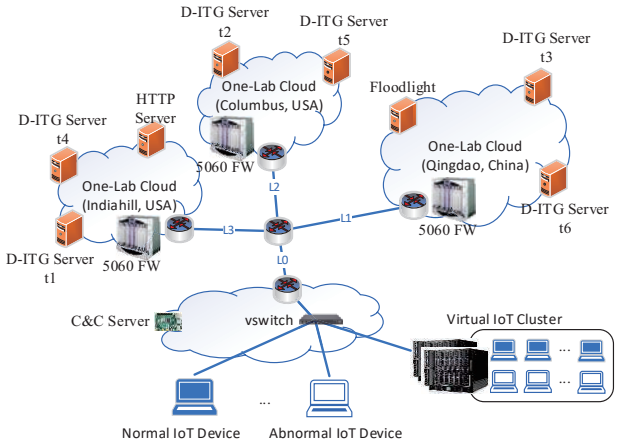


Fig. 2. LDDoS Attack Test Bed

In the IoT part of the test platform, Lenovo ThinkPad T470 laptop is used to simulate IoT device, run D-ITG tool to generate normal traffic and LDDoS attack traffic, and run slowhttptest tool to launch HTTP LDDoS attack. In order to simulate massive IoT devices, 10 HP C7000 servers are used to simulate 4,000 IoT devices through virtualization technology at max. Nokia one-lab cloud is used to deploy D-ITG server, HTTP server and Nokia 5060 FW, respectively. The link bandwidth between different nodes is as following. the link bandwidth in cloud is 10,000 Mbps, the link bandwidth of L0 and L1 is 50Mbps, the link bandwidth of L2 and L3 is 10Mbps, and the local bandwidth is 100Mbps.

A.2 The Experiment of Attack Concealment

We assume that we have 10 bots (says b_0-b_9) for 3 targets (says t_1-t_3). These bots belong to heterogeneous bots group, which includes 4 random size sub groups: 1Mbps, 2Mbps, 3Mbps and 4Mbps. As a result, the capability matrix of bots is as Fig. 3. The targets is D-ITGs who locate in Indiahill, Columbus and Qingdao.

C&C server expects to use enough distributed bots to generate 7Mbps peak rate with 500ms of burst length. Per algorithm 1, we random choose the first bot (says b_0), and recalculate its delay times to other targets as shown in Fig. 4-Delay Matrix-b_0. And then, the sequenced bots (b_2) is chosen based on its CapMatrix and its interval, since b_1 cannot meet "concurrent attack time" with b_0. The part of final attacking plan are shown in Fig. 4-Attacking Plan. We can see that attack targets of bots are totally different in the given time (or in the given the utilization rate of bots). Take b_0 and b_3 as an example, b_0 begins to attack t_1 in "relative time" 0ms, and then to attack t_2 in 500ms. while b_3 begins to attack t_2 in "relative time" 5ms, and then to attack t_1 in 507ms. Obviously, this algorithm can enhance attack ability effectively.

	b0	b1	b2	b3	b4	b5	b6	b7	b8	b9
R	1M	4M	4M	2M	1M	3M	2M	3M	3M	4M

Fig. 3. The Capability Matrix (CapMatrix) of Bots

Delay Matrix:

Original Matrix			
	t1	t2	t3
b0	72	78	6
b1	86	70	44
b2	30	80	0
…			
b9	47	24	20

Matrix after two bots chosen			
	t1	t2	t3
b0	572	578	506
b1	86	70	44
b2	572	622	542
…			
b9	47	24	20

Attacking Plan:

epochs	bots	Begin Time	Target IP
1	b0	0	t1
2	b0	500	t2
……			
1	b3	5	t2
2	b3	507	t1
1	b4	52	t1
2	b4	578	t2
2	b5	513	t2

Fig. 4. The Case of Crossfire LDDoS Algorithm of Bots

It can be seen from the attacking plan that bots attack multiple targets in turn. Taking b_0 as an example, b_0 attacked the target t_1 in a time of 0ms, and then attack the target t_2 in 500ms. Here, we draw the attacking plans of 1000 epochs (including the enlarged view of the attacking plans of the first 10 epochs) into a 3D graph as shown in Fig. 5. From the perspective of the attacker, each bot b_i constantly attack two or more targets. This shows that bots' attack capability has been fully utilized. From the perspective of the attacked target, each target t_i is attacked by a very wide range of b_i. The bots do not repeatedly attack the same target for a long time. This shows that the attack is more concealed. With the increase of attack epochs, as shown in the 3D graph of 1000 epochs of attacking plan in Fig. 5, all bots' attack capabilities are fully invoked to attack the targets as concealed as possible.

If the number of bots is enough, the attack behaviour will be more concealed. Here, we increase the number of controlled bots to 4,000, and draw the 3D attacking plan from

the perspective of the attack target. The experimental results are shown in Fig. 6. It is clear that there is no duplicate b_i appeared from any t_i's view.

In conclusion, the proposed attack algorithm has good concealment, and can make full use of the ability of bots to launch low-rate attacks that are more difficult to detect.

A.3 The Experiment of Attack Performance

This section designs crossfire attack experiments to verify the attack performance of the algorithm through the indices of throughput.

In the experiment, we start 10Mbps aggregation traffic to D-ITG t_2, and start 20Mbps aggregation traffic to D-ITG t_3, which lead to L_0 blocked. We also initiate normal access of 5Mbps to D-ITG t_1. The sampling period is set to 100ms, and the sampling length is set to 120s. The throughput of L_0 and t_1 is shown in Fig. 7. Per L_0, the throughput reaches the peak bandwidth of the link, which shows that the proposed attack algorithm can generate effective attacks and block the link. But per t_1, It is seen that the normal access traffic has been at a low level, indicating that the proposed algorithm successfully downgrades the normal access. Therefore, the experiment proves that the proposed crossfire LDDoS attack algorithm has more low-rate attack ability.

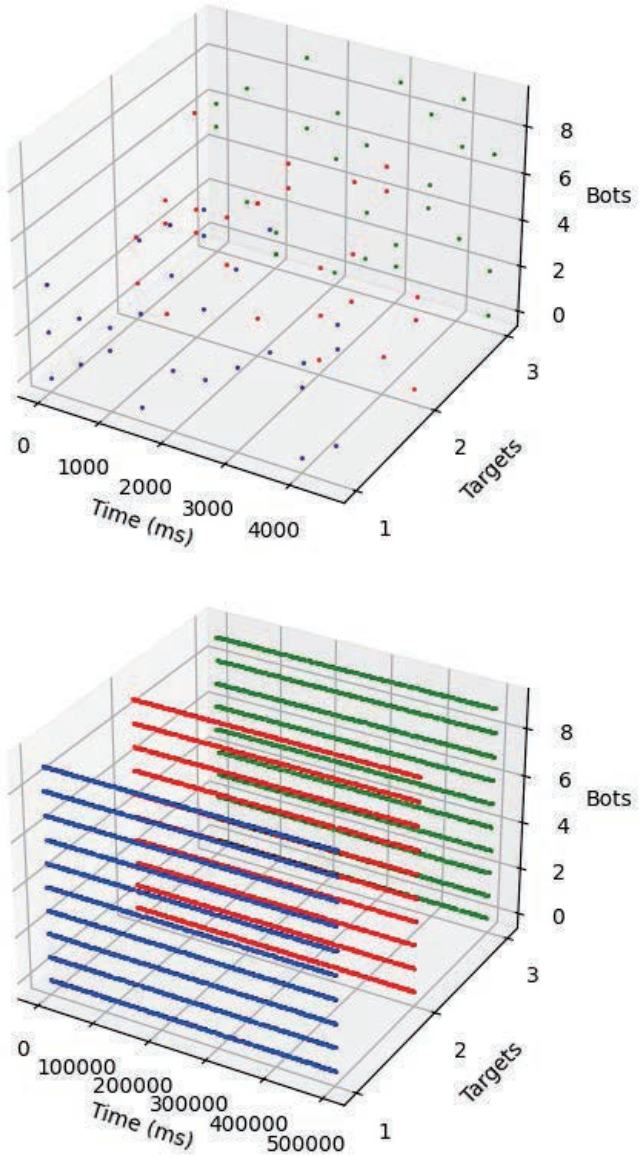


Fig. 5. The 3D Graph of Attacking Plan with 10 Bots

B. LS-ITSVM Defense Algorithm Experiments in Public Dataset

The proposed LS-ITSVM method should be a general and universal method, which has high detection accuracy and fast training and response time. In order to verify these, we carried out the following experiments, and made the comparison with Label propagation algorithm (LPA), and ISVM.

In the experiment, we apply our algorithm in KDD CUP 1999 dataset, which can prove the algorithm is general and universal method, and it has a good performance than others.

B.1 Experiment Environment and Dataset Description

The experiment is conducted on a laptop with Intel(R) Core (TM) i5-7200U CPU. GPU is not used here. The library Keras with TensorFlow as the backend is imported into the proposed model implementation.

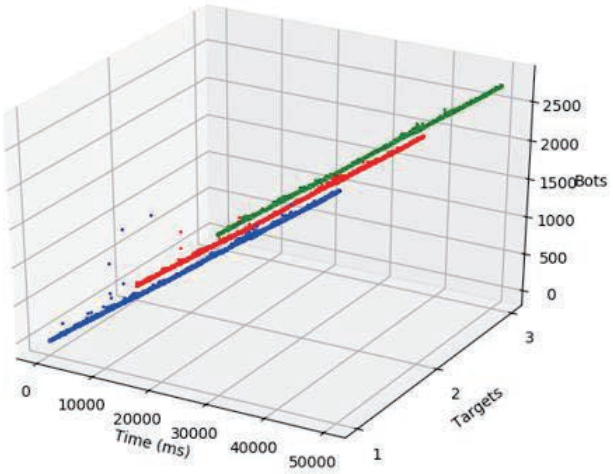


Fig. 6. The 3D Graph of Attacking Plan with 4,000 Bots

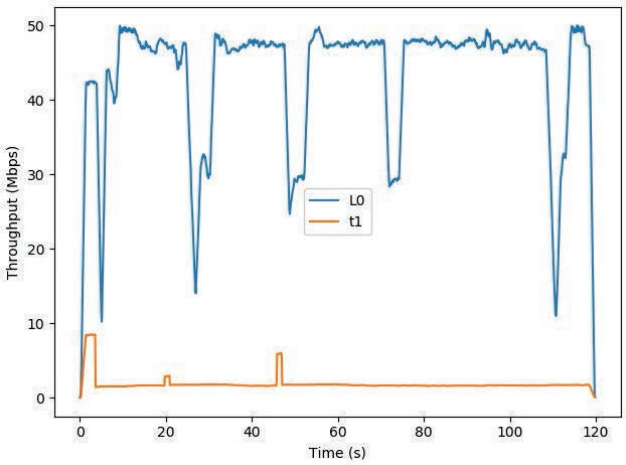


Fig. 7. The Throughput of Services and Links under Crossfire Attacks

KDD CUP-99 dataset was provided by Lincoln Labs, who set up an environment to acquire nine weeks of raw TCP dump data for a local-area network simulating a typical U.S. Air Force LAN. They operated the LAN as if it were a true Air Force environment, but peppered it with multiple attacks. The raw training data was about four gigabytes of compressed binary TCP dump data. Each connection is labeled as either normal, or as an attack, with exactly one specific attack type. In order to verify the above algorithm quickly, we use kddcup.data_10_percent as data source. We randomly choose 50,000 data items as test set. We split the to-be-trained data set into labeled and unlabeled parts by 20%:80%.

B.2 Features extraction

Each of those samples in "KDD CUP-99 10% dataset" has 41 features. 38 features of them are character and number related features. Thus, we pre-process them by reflecting and normalization. E.g. there are 3 choices in protocol_type: tcp, udp, icmp, which are reflected into 0, 1, 2. And then, we generate PSD by FFT and add them as new dimensions. E.g. in Fig. 8, the normalized cumulative amplitude spectrum (NCAS) value of dst_bytes are shown. What exactly happens is that more power of the autocorrelation function of dst_bytes is distributed in the lower frequency band when there is LDDoS contained in the traffic. After above operations, dimensions of features are bumped to 110.

In order to avoid the influence of the dimension of feature attribute on the experiment, it is necessary to unify the dimension of the experimental data. Thus, we use (5) to normalize the feature attributes to [0, 1]. In (5), x is the feature vectors. MIN is the minimal value of x, while MAX is its maximal value.

$$x = \frac{x - MIN}{MAX - MIN} \quad (5)$$

After above necessary dimensionality expand and normalize. The entropies of them are calculated for feature extraction. We well tune the threshold to 50, whose entropy values are bigger than 0.1, and chose them as training features.

B.3 Evaluation Indicators Analysis

In order to explain that the proposed method is better than others, we compare two indicators: detection accuracy score, training and response CPU time.

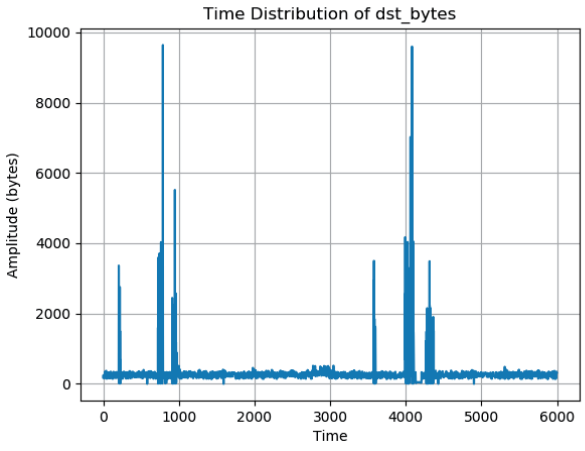


Fig. 8. The Time and Frequency Distribution of dst_bytes

Detection accuracy refers to how closely a prediction comes to measuring a "true value", since prediction are always subject to error. Here, we use the ratio between predicted value and the corresponding true value detailed as following, where $\mathbf{1}(x)$ is the indicator function.

$$\mathbf{accuracy}(\mathbf{y}, \hat{\mathbf{y}}) = \frac{1}{n}\sum_{i=0}^{n-1} \mathbf{1}(\hat{y}_i = y_i) \quad (6)$$

As Fig. 9 shown, the proposed locality sensitive ITSVM almost has the same accuracy with ISVM, even if we bump the semi-supervised increase set size to 100k. but locality sensitive ITSVM method has far better detection accuracy than LPA method. The accuracy of LPA is stick to 80% or so. And even worst, LPA is a huge memory-consumed method. It reports memory is not enough when it calculates label. Thus, there is not statistical data when size is bigger than 15k.

The training and detecting CPU time is the other critical parameter to evaluate the performance of locality sensitive ITSVM method. We define it as the time when method trains with semi-supervised incremental data and detects whether malicious flows exist or not. As Fig. 10 shown, the CPU time of ISVM is increased continually with the growth of increase set size, and bumps to almost 100s from 60s. Same to accuracy, LPA method is stopped when size is bigger than 15k. Compared with them, our proposed method training and detecting time is stable in 50s.

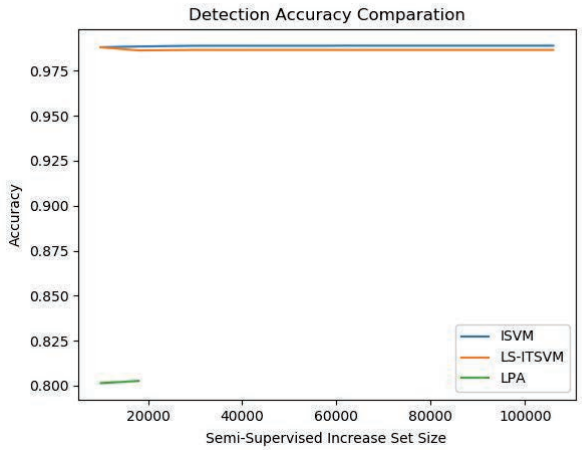


Fig. 9. The Detection Accuracy Comparation with KDD-CUP Dataset

Thus, take both detection accuracy score and CPU time into account, locality sensitive ITSVM, which has better performance, can detect DDoS with higher accuracy and shorter CPU time.

Fig. 10. The Training and Detecting Time Comparation with KDD-CUP Dataset

C. LS-ITSVM Defence Algorithm Experiments in Simulated IoT Dataset

C.1 Dataset Description

We hacked randomly 1k endpoints/users as bots, and start to attack our cloud data center by algorithm 1 with the peak rate of 50Kb/sec and the attacking period of 500ms. This can lead to network traffic jam of whole cloud data center. We collect all raw TCP dump data with same dimensions and with extra source and destination IP. Thus, our detection target becomes to not only detect abnormal flows, but also detect which bots fire the attacks.

C.2 Features extration

We do the same things with "KDD CUP-99 10% dataset", and find out the top 50 features with sorted entropy values. Especially, we reserve IP addresses as features for the purpose of detecting bots.

C.3 Evaluation indicators Analysis

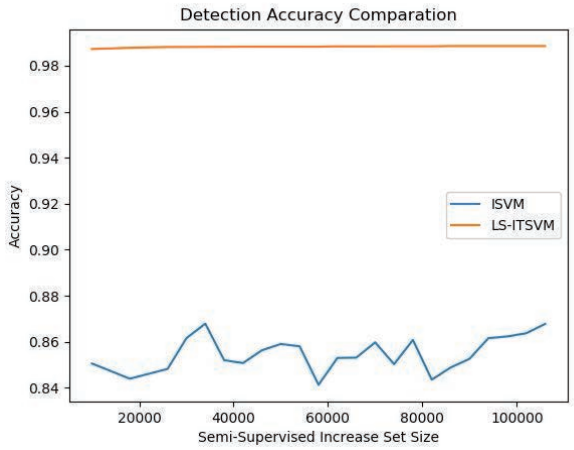


Fig. 11. The Detection Accuracy Comparation with IoT Dataset

Fig. 12. The. Training and Detecting Time Comparation with IoT Dataset

If we remove IP addresses temporarily, the comparations are almost the same with the experiment result of "KDD CUP-99 10% dataset". That is, both LS-ITSVM and ISVM have higher detection accuracy when we do FFT transform. whereas when we merge IP info into features, the accuracy of ISVM is down to 86% or so as Fig 11 shown. Notes: we don't compare with LPA, since it has been approved that it has worst performance in above experiment.

In CPU time facet, they have the same trend. With the growth of the size of data set, ISVM CPU time is increased continually, while the CPU time of LS-ITSVM keeps stable from time to time as Fig. 12 shown.

VI. CONCLUSION

In the paper, we firstly enhance IoT DDoS attack mechanism as a kind of new Mirai botnet variants: crossfire LDDoS attacks. And then, we develop a novel semi-supervised locality sensitive incremental TSVM method for resolve Mirai botnet and this new variant. At last, the results in KDD CUP-99 prove LS-ITSVM has better performance, and the indicators in simulated IoT lab prove LS-ITSVM is still available to new LDDoS variants. Per above experiments, we can conclude that the proposed method can differ bots from normal users. As known, LDDoS is a complex large-scale network attack behavior. The KDD CUP-99 is a good dataset, but it is too old. In order to improve the fidelity and ensure the scale of LDDoS attack and defense technology emulation, we will use Long Short-Term Memory Networks (LSTM) to extract time-domain characteristics of LDDoS as the specific generating conditions of GAN, and establish a Condition Generative Adversarial Networks (CGAN) model to generate mimicking behaviors of bots in the near future. Meanwhile, we will also spend more time in SDN and work out a method to prevent these bots into the data center.

ACKNOWLEDGWMENT

This research was supported by Scientific Talent Fund Project of Weifang University of Science & Technology of China (Grant number: KJRC2021002) and was also supported by the Scientific Fund Project of Facility Horticulture Laboratory of Universities in Shandong of China (Grant number: 2018YY016) and Key Research and Development Program of Shandong, (Grant number: 2019GNC106034).

REFERENCES

[1] D. Goodin, "Record-Breaking DDoS Reportedly Delivered by > 145K Hacked Cameras", *Ars Technica*, Sept. 2016.

[2] C. Cimpanu, "You Can Now Rent a Mirai Botnet of 400,000 Bots", *BleepingComputer.com*, Nov. 2016.

[3] C. Kolias, G. Kambourakis, *et al.*, "DDoS in the IoT: Mirai and Other Botnets", Computer, vol. 50, no. 7, pp. 80-84, Jul. 2017.

[4] A. Mehmood, M. Mukherjee, et al., "NBC-MAIDS: Naïve Bayesian Classification Technique in Multi-agent System-enriched IDS for securing IoT against DDoS attacks", J Supercomput, May. 2018, DOI. 10.1007/s11227-018-2413-7

[5] E. Hodo, X. Bellekens, et al., "Threat Analysis of IoT Networks Using Artificial Neural Network Intrusion Detection System", presented at 2016 Int. Symp. on Net., Comp. & Comm., Yasmine Hammamet, Tunisia, May 11-13. 2016.

[6] C. Zhang, R. Green, et al., "Communication Security in Internet of Thing: Preventive Measure and Avoid DDoS Attack over IoT Network", presented at the 18th Symp. on Comm. & Net., Alexandria, Virginia, Apr. 12-15, 2015.

[7] J. W. Su, V. D. Vasconcellos, et al., "Lightweight Classification of IoT Malware Based on Image Recognition", presented at 2018 IEEE 42nd Annu. Comp. Soft. & App. Conf., Tokyo, Japan, Jul. 2018.

[8] G. Kaur, P. Agrawal, "Detection of LDoS Attacks Using Variant of CUSUM and Shiryaev-Roberts's Algorithm", presented at the 4th Int. Conf. on Para., Dist. & Grid Comp., Waknaghat, India, Dec. 22-24, 2016.

[9] Z. Wu, L. Zhang, et al., "Low-rate DoS Attacks Detection based on Network Multifractal", IEEE Trans. Depend. Sec. Comput., vol. 13, no. 5, pp. 559-567, Sept. 2016.

[10] Z. G. Liu, X. C. Yin, et al., "A New Network Flow Grouping Method for Preventing Periodic Shrew DDoS Attacks in Cloud Computing", presented at the 18th Int. Conf. on Advanced Comm. Tech., Pyeongchang, Korea, Jan. 31-Feb. 3, 2016.

[11] M. Yue, L. Liu, et al., “Identifying LDoS Attack Traffic based on Wavelet Energy Spectrum and Combined Neural Network”, Int J Commun Syst., Sept. 2017.
[12] Z. J. Wu, J. Jiang, et al., “A Particle Filter-Based Approach for Effectively Detecting Low-rate Denial of Service Attacks”, presented at the Int. Conf. on Cyber-Enabled Dist. Comp. & Know. Disc., Chengdu, China, Oct. 13-15, 2016.
[13] P. Nagar, H. K. Menaria, M. Tiwari, "Novel Approach of Intrusion Detection Classification Deeplearning Using SVM", presented at the 1st Int. Conf. on Sust. Tech. for Comp. Intel., Jaipur, India, Mar. 20-30, 2019.
[14] X. Peng, W. Q. Huang, Z. X. Shi, "Adversarial Attack Against DoS Intrusion Detection: An Improved Boundary-Based Method", presented at 2019 IEEE 31st Int. Conf. on Tools with Art. Intel., Portland, USA, Nov. 4-6, 2019
[15] M. Begli, F. Derakhshan, H. Karimipour, "A Layered Intrusion Detection System for Critical Infrastructure Using Machine Learning", presented at 2019 IEEE 7th Int. Conf. on SEGE, Oshawa, Canada, Aug. 12-14 2019.
[16] P. Rivas, C. DeCusatis, M. Oakley, A. Antaki, N. Blaskey, S. LaFalce, S. Stone, "Machine Learning for DDoS Attack Classification Using Hive Plots", presented at 2019 IEEE 10th Annual UEMCON, New York City, USA, Oct. 10-12, 2019
[17] T. A. Tuan, H. V. Long, L. H. Son, R. Kumar, I. Priyadarshini, N. T. K. Son, "Performance Evaluation of Botnet DDoS Attack Detection Using Machine Learning", Evolutionary Intelligence, pp. 1-12, Nov. 2019.
[18] M. S. Kang, S. B. Lee, V. D. Gligor, “The Crossfire Attack”, presented at 2013 IEEE Sym. on Secu. and Pri., Berkeley, USA, May. 19-22, 2013.
[19] H. S. Li, J. H. Zhu, “The New Threat to Internet: DNP Attack with the Attacking Flows Strategizing Technology”, Int. J. Commun. Syst., vol. 28, no. 6, pp.1126C1139, 2014.
[20] H. S. Li, J. H. Zhu, “LAAEM: A Method to Enhance LDoS Attack”, IEEE Comm. Letters, vol. 20, no. 4, pp. 708-711, Apr. 2016.
[21] Y. Yang, Z. Z. Li, et al., “An Adaptive Semi-supervised Clustering Approach via Multiple Density-based Information”, Neuro Computing, vol. 257, pp. 193-205, Sept. 2017.
[22] X. Z. Gao, Q. S. Sun, et al., “Multiple Instance Learning via Semi-supervised Laplacian TSVM”, Neural Proc. Letters, vol. 46, no. 2, pp. 219-232, Aug. 2017.
[23] H. L. Du, Y. Zhang, “Transductive Support Vector Machine Algorithm Based on Cluster and Cooperative Labeling”, HeNan Sci., vol. 35, no. 1, Jan. 2017.
[24] N. Piroonsup, S.Sinthupinyo, “Analysis of Training Data Using Clustering to Improve Semi-supervised Self-training”, Knowledge-Based Systems, vol. 143, pp. 65-80, Mar. 2018.
[25] K. J. Zhang, M. Xian, “Research on Hybird Intrusion Detection Model Based on DBN and TSVM”, Comp. App. and Software, vol. 35, no. 5, May. 2018.
[26] A. Andoni, P. Indyk, et al., “Beyond Locality-Sensitive Hashing”, presented at 25th Ann. ACM-SIAM symp. On dis. Alg., New York, 2014.
[27] G. Aluç, M. T. Özsu, et al., “Building self-clustering RDF databases using Tunable-LSH”, The VLDB Journal, https://doi.org/10.1007/s00778-018-0530-9, Dec. 2018.
[28] F. Wu, X. Y. Jing, Q. H. Huang, “Uncorrelated Locality-Sensitive Multi-view Discriminant Analysis”, Natl. Acad. Sci. Lett. (2020), doi. 10.1007/s40009-019-00864-4, Jan. 2020.

Xiaochun Yin (M’12) was born in Shouguang, China in 1980. She received the B.S. degree in Education and Technology from Qufu Normal University in 2004, and received the M.S. degree in Education and Technology from Nanjing Normal University in 2007, and received the Ph.D. from Dongseo University in 2015.

From 2007 to now, she is an associate professor in Weifang University of Science &Technology. Her research interests include network security, IoT security, blockchain and AI areas.

Professor Yin was a recipient of the Science Research Innovation Award of Weifang University of Science & Technology in 2017 and 2018.

Zengguang Liu was born in Shouguang, China in 1982. He received the B.S. and M.S. degrees in computer science from the University of Shanghai for Science and Technology in 2005 and 2008 respectively. He is currently pursuing the Ph.D. degree in computer science at the University of Shandong for Science and Technology.

From 2008 to 2016, he was a Senior Architecture Engineer in Core Network Department of Alcatel-Lucent. He had been a Principal AI Engineer of Hewlett Packard Enterprise since 2016. His research interests include big data, AI and network security areas.

He was a recipient of the Innovation Award of Shandong for Excellence in 2011.

Deyong Liu received the B.S. degree in computer science and technology from Shandong Normal University in 1996 and the M.S. degree in computer technology from Ocean University of China in 2010.

He is currently a Professor with the Weifang University of Science & Technology. He is focusing on Cloud Computing, IoT, and Smart city big data research. At present, he is the tutor of Shandong Normal University, the tutor of the Torch High-tech Industry Development Center of the Ministry of Science and Technology, the director of Shandong Software Industry Association.

Zhenge Liu received the B.S. degree in QingDao University in 2020, majoring in accounting. He is now studying in Peking University for software engineering.

He is now engaged in research cloud computing, IoT, and machine learning algorithm for paired financial trading.

Fixed–Point Arithmetic for Implementing Massive MIMO Systems

Mi Tian, Mihai Sima, and Michael McGuire
Department of Electrical and Computer Engineering, University of Victoria
P.O. Box 1700 Stn CSC, Victoria, B.C. V8W 2Y2, Canada
tianmi66@uvic.ca, msima@ece.uvic.ca, mmcguire@uvic.ca

***Abstract*—Massive MIMO base stations are expensive to build due to the requirement for a large number of RF transceivers and high-resolution analog-to-digital converters. A way to reduce the implementation cost is to build the base stations with inexpensive hardware, resulting in the received signals to be coarsely quantized. First, the required signal power needed to achieve different receiver Bit-Error Rate (BER) levels is determined, as well as the extra signal power needed due to the quantization for given BER levels. To implement the data detection and decoding process in real time, fixed-point arithmetic with reduced precision is used. This article also reports the minimum wordlength needed to maintain the BER at acceptable levels. Specifically, the eigenvalue decomposition, which is the most computationally demanding portion of the receiver algorithm, can be calculated with wordlengths of 7 and 10 bits for eigenvectors and eigenvalues, respectively.**

***Index Terms*—Massive MIMO, fixed-point arithmetic**

I. Introduction

The number of Receive Antennas (Receivers), R, deployed in a Massive Multiple-Input Multiple-Output (MMIMO) base station is much larger than the number of Transmit Antennas (Transmitters), T, where only one transmit antenna per mobile user is considered in this article. Since large-scale computation is needed for data detection and decoding based on measurements from high-resolution Analog-to-Digital Converters (ADC) connected to highly-linear RF front-end amplifiers for each antenna, the cost of a MMIMO base station is very high. A way to reduce the cost of the implementation is to build the base stations with inexpensive low-end hardware [1], such as simple RF receivers feeding the received signals to coarse (1-, 2-, or 3-bit) ADCs [2], [3].

The conceptual equations of the detection process are given below, where $\boldsymbol{X}$ is the $T\times1$ transmitted complex signal vector, $\boldsymbol{Y}$ is the $R\times1$ received complex signal vector, $\boldsymbol{H}$ is the $R\times T$ channel transfer matrix, where each entry is modeled as an independent identically distributed as complex circulary symmetric Gaussian random value, $\boldsymbol{N}$ is an $R\times1$ complex noise vector, and $\boldsymbol{N}'$ is a $T\times1$ complex noise vector.

$$\boldsymbol{Y}=\boldsymbol{H}\cdot\boldsymbol{X}+\boldsymbol{N} \;\Rightarrow\; \boldsymbol{H}^{\mathrm{H}}\cdot\boldsymbol{Y}=\underbrace{(\boldsymbol{H}^{\mathrm{H}}\cdot\boldsymbol{H})}_{\boldsymbol{\Theta}}\cdot\boldsymbol{X}+\underbrace{\boldsymbol{H}^{\mathrm{H}}\cdot\boldsymbol{N}}_{\boldsymbol{N}'} \quad (1)$$

The multiplication of both sides by $\boldsymbol{H}^{\mathrm{H}}$ converts the $R\times T$ system to a $T\times T$ system, which is less expensive to solve. It is known that the Minimum Mean Square Error (MMSE) estimate of $\boldsymbol{X}$ from the reduced-order system has the same mean squared error as the solution of the original system [18]. The estimation of $\boldsymbol{X}$ through the solution of this linear system is the most computationally demanding portion of the receiver algorithm for reasonably high values of T. In this process, two major operations need to be performed: (i) calculation of the Hermitian matrix $\boldsymbol{\Theta}=\boldsymbol{H}^{\mathrm{H}}\cdot\boldsymbol{H}$, and (ii) EigenValue Decomposition (EVD) [4] of matrix $\boldsymbol{\Theta}=\boldsymbol{Q}\cdot\boldsymbol{\Lambda}\cdot\boldsymbol{Q}^{\mathrm{H}}$ followed by solving the linear system by matrix multiplications.

The challenge is to perform these linear-algebra operations in real time on inexpensive hardware, such as reasonably sized Field-Programmable Gate Arrays (FPGA). To achieve such performance, only fixed-point arithmetic [5], [6] will be used. The channel matrix, $\boldsymbol{H}$, and the received signal vector, $\boldsymbol{Y}$, will be coarsely quantized with $B=1$, $B=2$, or $B=3$ bits. This article expands our previous work [31] and reports the FPGA fixed-point arithmetic implementation details together with the minimum wordlength needed in the data detection and decoding process to maintain the BER at acceptable levels. Our contributions are as follows.

1) Strategy to efficiently load the estimated channel matrix, $\boldsymbol{H}$, into FPGA and efficiently calculate the matrix $\boldsymbol{\Theta}$.
2) FPGA implementation of the squared Euclidean norm and the square root operations with reduced precision used in converting $\boldsymbol{\Theta}$ first into a Hessenberg form and then into a diagonal form.
3) Assessment of the minimum wordlength needed to complete the eigenvalue decomposition of matrix $\boldsymbol{\Theta}$ through the Francis-Kublanovskaya algorithm.
4) Assessment of the BER and the extra signal power which is needed to compensate for the information loss due to quantization for different coarse quantization levels.

The article is organized as follows. Background information is presented in Section II. Coarse quantization in Massive

Manuscript received January 23, 2021. This work was supported in part by the University of Victoria, British Columbia, Canada, under a PhD fellowship, and a follow-up of the invited journal to the accepted and presented paper entitled "Massive MIMO in Fixed-Point Arithmetic" of the 23rd International Conference on Advanced Communication Technology (ICACT2021).

Mi Tian is a postdoctoral fellow in the Department of Electrical and Computer Engineering at University of Victoria, British Columbia, Canada (e-mail: tianmi66@uvic.ca).

Mihai Sima is an associate professor in the Department of Electrical and Computer Engineering at University of Victoria, British Columbia, Canada (corresponding author, phone: +1-250-721-8680, e-mail: msima@ece.uvic.ca).

Michael McGuire is an associate professor in the Department of Electrical and Computer Engineering at University of Victoria, British Columbia, Canada (e-mail: mmcguire@uvic.ca).

MIMO uplink communications is analyzed in Section III. The detection process implemented in fixed-point arithmetic is presented in Section IV. Section V concludes the article.

II. Background

This section provides the fundamentals of MMIMO iterative channel estimation and simulation software for coarsely quantized MMIMO communications used in our previous work. It also outlines the basic FPGA architectural features.

A. Iterative Channel Estimation for MMIMO

In MMIMO a large number of sufficiently-spaced receive antennas results in a large probability of a high-capacity communications channel from each mobile user's transmitter to the base station [7]. This allows MMIMO systems to communicate over random multipath propagation channels with transmission power nearly as low as ideal Additive White Gaussian Noise (AWGN) channels. To take advantage of this situation, the receiver requires accurate estimates of radio Channel State Information (CSI), which in turn leads to the requirement for a large number of pilot symbols to be used when standard channel estimation techniques are employed [8].

Recently we have shown that the channel state information can be accurately estimated from coarsely quantized measurements using an iterative procedure, where data symbols detected and decoded in previous iterations are used as additional (virtual) pilot symbols [9]. For the first iteration, only the pilot symbols are used to estimate the channel, since no prior knowledge of the transmitted data is available. For the second and following iterations, channel estimation is enhanced by using the estimated data symbols from the previous iterations as virtual pilot symbols, to get a lower error estimate of the channel parameters. Our simulation results indicate that an accurate estimation is achieved in three iterations or less.

B. Simulation Software for Coarsely Quantized MMIMO

In our previous work [9] the linear system shown in Equation (1) was solved in 64-bit floating-point arithmetic [10] using the standard MATLAB® linear solution mechanism, where $\widetilde{\boldsymbol{X}} = \boldsymbol{H}^{+} \cdot \boldsymbol{Y}$, where $\boldsymbol{H}^{+}$ is the pseudo-inverse, is coded as $\widetilde{\boldsymbol{X}} = \boldsymbol{H} \backslash \boldsymbol{Y}$, as shown in Equations (2) and (3). While these standard solution computations give accurate results, direct implementation of these solutions for use in MMIMO receivers would require computational hardware with prohibitive cost in base stations. The backslash operator method was also applied for estimating the channel matrix, $\boldsymbol{H}$.

$$\boldsymbol{Y} = \boldsymbol{H} \cdot \boldsymbol{X} + \boldsymbol{N} \quad \Rightarrow \quad \widetilde{\boldsymbol{X}} = \boldsymbol{H} \setminus \boldsymbol{Y} \tag{2}$$

$$\boldsymbol{H}^{\mathrm{H}} \cdot \boldsymbol{Y} = \boldsymbol{\Theta} \cdot \boldsymbol{X} + \boldsymbol{N}' \;\Rightarrow\; \widetilde{\boldsymbol{X}} = \boldsymbol{\Theta} \setminus (\boldsymbol{H}^{\mathrm{H}} \cdot \boldsymbol{Y}) \tag{3}$$

To reduce the latency of estimating $\boldsymbol{X}$, we have recently proposed to solve the linear system in fixed-point arithmetic with reduced precision [31] through an eigenvalue decomposition of the Hermitian matrix $\boldsymbol{\Theta}$, as shown in Equation (4). It should be observed that the eigenvalue decomposition is intrinsically stable, since unitary matrix $\boldsymbol{Q}$ is a rotation matrix, which means that all its elements range from -1.0 to $+1.0$.

$$\boldsymbol{\Theta} = \boldsymbol{Q} \cdot \boldsymbol{\Lambda} \cdot \boldsymbol{Q}^{\mathrm{H}} \;\Rightarrow\; \widetilde{\boldsymbol{X}} = \boldsymbol{Q} \cdot \boldsymbol{\Lambda}^{-1} \cdot \boldsymbol{Q}^{\mathrm{H}} \cdot \boldsymbol{H}^{\mathrm{H}} \cdot \boldsymbol{Y} \tag{4}$$

C. Coarse Quantization

When signal x is in the range of the quantization range i, $q^i_{min} \leq x < q^i_{max}$, its reported quantized value is $q(x) = q_i$. The values of q_i for all the intervals i, which minimize the mean square error, $E[|q(x) - x|^2]$, where $E[\cdot]$ is the expectation operator, are easily shown to be the mean value of the signal in each interval $q_i = E\left[x | q^i_{min} \leq x < q^i_{max}\right]$ [11].

An independent Additive White Gaussian Noise (AWGN) channel with mean $\mu = 0$ and standard deviation, $\sigma = 1$, is assumed for each receive antenna in this article. Table I presents the probabilities, quantization thresholds, and the corresponding bin-average values for $B = 1$-bit, $B = 2$-bit, and $B = 3$-bit quantization processes for a Gaussian random variable with zero mean and unity standard deviation.

TABLE I
PROBABILITIES, QUANTIZATION THRESHOLDS, AND THE CORRESPONDING BIN-AVERAGE VALUES.

B	Probabilities	Quantization thresholds	Bin-average values
1	50%	0	±0.797884561
2	25%	0 ±0.674489572	±0.324662678 ±1.271106444
3	12.5%	0 ±0.318634923 ±0.674489572 ±1.150349346	±0.157972012 ±0.491353344 ±0.895384581 ±1.646828306

In fixed-point representation, it is beneficial to scale up the smallest magnitude of the bin-average values, since this will simplify the implementation and slightly increase the precision. For example, in a $B = 2$ quantization process, 0.324662678 is promoted to 1.000000000, and 1.271106444 is promoted to $1.271106444/0.324662678 = 3.915160350$. The other quantization processes will follow a similar pattern. The updated values are presented in Table II.

TABLE II
QUANTIZATION THRESHOLDS, SCALE FACTORS, AND THE CORRESPONDING BIN-AVERAGE VALUES.

B	Quantization thresholds	Scale factor	Bin-average values
1	0	0.797884561	±1.000000000
2	0 ±0.674489572	0.324662678	±1.000000000 ±3.915160350
3	0 ±0.318634923 ±0.674489572 ±1.150349346	0.157972012	±1.000000000 ±3.110382264 ±5.667995047 ±10.424810617

It is apparent that the measurements of the channel output can take only a small number of different values (for example, ± 1.0000 and ± 3.9152 in a process with $B = 2$ quantization bits). The estimated channel coefficients, the entries of $\boldsymbol{H}$, are also coarsely quantized to reduce the computation cost in the receiver. Since the quantized values have equal probability, the entropy of the quantized signal is maximized, which in turn maximizes the upper bound of the mutual information between the received signal and the transmitted signal when their joint distribution is not known [12].

D. FPGA Architecture

Modern FPGA architectures consist of five types of modules: I/O Blocks (IOB), Configurable Logic Blocks (CLB), Digital Signal Processing (DSP) slices, Block Random Access Memories (BRAM), and a configurable Interconnection Network. The CLBs belonging to the fine-grained fabric are organized as a 2D array, where each CLB includes a configurable Look-Up Table (LUT) to implement bit-level logic functions, dedicated carry logic to support arithmetic operations such as binary and ternary adders [27], dedicated multiplexors, and Flip-Flops (FF). Software support for the fine-grained fabric includes macros and primitives, such as *CARRY4* which concatenates four LUTs to build a 4-bit binary / ternary adder or subtractor, *MUXF7* and *MUXF8* which instantiate 2-to-1 multiplexors, *BRLSHFT4* and *BRLSHFT8* which instantiate 4-bit and 8-bit barrel shifters, etc. The DSP slices belong to the coarse-grained fabric and support the implementation of large units such as 25×18 two's-complement multipliers, 48-bit acumulators, dual 24-bit or quad 12-bit adders, subtractors, and accumulators. The configurable interconnection network connects these the modules together to complete the implementation of digital circuits.

Modern FPGAs also integrate Block Random Access Memories (BRAM) on chip. The BRAM in the Virtex-7 family [29] can operate as either *one* $36\,\mathrm{Kb}$ dual-port RAM, which can be configured as $32\mathrm{K} \times 1$, $16\mathrm{K} \times 2$, $8\mathrm{K} \times 4$, $4\mathrm{K} \times 9$, $2\mathrm{K} \times 18$, $1\mathrm{K} \times 36$, or 512×72, or *two independent* $18\,\mathrm{Kb}$ dual-port RAMs, where each RAM can be configured as $16\mathrm{K}\times1$, $8\mathrm{K}\times2$, $4\mathrm{K} \times 4$, $2\mathrm{K} \times 9$, $1\mathrm{K} \times 18$, or 512×36. These BRAMs can be used as large storage area or as large LUTs with multiple outputs to implement logic functions.

III. Massive MIMO Uplink Communications with Coarse Quantization

In this article, we consider the receivers in the base stations of massive MIMO communications systems. The number of transmitters (or users) is denoted as T, each of which has one antenna. The base station is equipped with R antennas. The transmit and receiver antennas are spaced so that the channel propagation gains from each pair of transmit and receive antennas are independent. A spacing greater than one half of a wavelength between antennas can accomplish this independence. For a communication frequency of $1\,\mathrm{GHz}$, which corresponds to a wavelength of $\lambda = 30\,\mathrm{cm}$, an array of 256 antennas can be organized as a square with the side length equal to $\sqrt{256} \times \frac{30}{2} = 240\,\mathrm{cm} = 2.4\,\mathrm{m}$. Such an array can be mounted, for example, on the roof of a city building.

If the measured signal on the receiver antennas for sample time n is held in a length R vector denoted as $\mathbf{y}\,[n]$, with the full received signal being denoted as

$$\mathbf{y}\,[n] = \sum_{l=0}^{L-1} \mathbf{h}\,[l]\,\mathbf{x}\,[n-l] + \mathbf{v}\,[n]\,, \tag{5}$$

where $\mathbf{h}\,[l]$ is the R-by-T matrix holding channel gains from the transmitters to receivers with the entry in column t on row r specifying the propagation gain from transmitter t to receive antenna r for the delay of l sample periods, then $\mathbf{x}\,[n]$ is a length T vector specifying the transmitted signals at sample time n, $\mathbf{v}\,[n]$ is a length R vector giving the measurement noise at sample n, and L is the length of the channel impulse responses in sample periods. The problem of the receiver is to estimate the vectors $\mathbf{x}\,[n]$ from the received signals $\mathbf{y}\,[n]$. A method of accomplishing this in modern wireless systems, such as advanced Wireless Local Area Networks (WLANs) or 5G advanced radio networks, is the use of Frequency Domain Equalization (FDE) [17]. For FDE, the received signals for all receiver antennas are first split into blocks of N samples. The key to OFDM is to compute the Discrete Fourier Transform (DFT) of the received signal $\mathbf{y}\,[n]$ as

$$\mathbf{Y}\,[k] = \sum_{n=0}^{N-1} \mathbf{y}\,[n] \exp\left(-\mathrm{j}\,\frac{2\pi k n}{N}\right) \text{ for } k = 0 \ldots N-1 \tag{6}$$

where N is the length of the DFT where a value of $N = 256$ is often used. If a cyclic prefix of CP $> L$ samples from the end of each block of N samples is copied and prepended to the start by the transmitter, as is performed in the OFDM signalling method used in most modern wireless standards, then a convolution in time is converted into a multiplication in the DFT domain. Thus, the relation from (5) becomes:

$$\mathbf{Y}\,[k] = \mathbf{H}\,[k]\,\mathbf{X}\,[k] + \mathbf{V}\,[k] \text{ for } k = 0, \ldots, N-1 \tag{7}$$

where $\mathbf{H}\,[k]$, $\mathbf{X}\,[k]$, and $\mathbf{V}\,[k]$ are the DFTs of time-domain signals $\mathbf{h}\,[l]$, $\mathbf{x}\,[n]$, and $\mathbf{v}\,[n]$, respectively (Equation 1 is one out of N instances of Equation 7 for an unspecified frequency index k). It is apparent that the MIMO signalling over multipath radio channels becomes a simple matrix-vector multiplication in the frequency domain. The advantage of MIMO-OFDM signalling with FDE is that the equalization of the multiple antenna, multipath radio propagation channel can be reduced to linear algebra [18] where the methods described above can be applied.

For MIMO systems, each antenna $r = 1, \ldots, R$ requires a radio receiver. In Massive MIMO (MMIMO) systems, where R is very large, this can lead to a prohibitive cost. If high resolution Analog-to-Digital Converters (ADCs) and highly-linear RF amplifiers are used, they can make up a large proportion of this cost. However, we can show that only inexpensive devices are needed for many MMIMO systems. This article considers an implementation of MMIMO in terms of Bit-Error Rate (BER) using both demodulation linked with an error correction code as opposed to [1]–[3] which only present capacity calculations. Here we present a demonstration of a MMIMO system performance showing that highly quantized measurements with lower precision calculations can give acceptable BER performance.

For the sake of presentation, the numbers of transmit and receive antennas will be powers of 2. A MMIMO system in a Standard Configuration (SC), as we propose to name it, has $T = 16$, $R = 128$. Other configurations can be of practical interest, for example Extended Users (EU) with $T = 32$, $R = 128$, Extended Base Station (EBS) with $T = 16$, $R = 256$, Extended Configuration (EC) with $T = 32$, $R = 256$, and Maximum Configuration (MC) with $T = 64$, $R = 256$, but they will not be considered in this article.

The number of taps L required to model the radio channel for acceptable receiver performance is determined by the difference in propagation distance between the shortest radio signal path and the longest radio signal path with significant received power. This distance is directly related to the so-called delay spread of the radio propagation channel after division by the radio signal propagation speed. The tolerated propagation distance difference is given by $L \times T_s \times c$ where T_s is the sampling time and the c is radio signal propagation speed which is approximately 3×10^8 m/s. For the radio systems of greatest interest, such as 5G cellular and advanced wireless local area networks, $L = 9$ and $T_s \approx 10^{-7}$ seconds [19]. This indicates that the system described in this article tolerates a difference of propagation distance up to $9 \times 10^{-7} \times 3 \times 10^8 = 270$ meters, which is sufficient for most urban microcells or indoor networking applications.

An MMIMO system in Standard Configuration was simulated using 4-QPSK modulation having a standard rate $1/2$ convolutional error corrrection code with a constraint length of 7. We have assumed that the receiver has access to ideal channel state information, since it has been shown that with pilot-signals and iterative receiver algorithms, the channel estimation error can be made smaller than the measurement noise [9]. In practice, several methods exist for MIMO channel estimation [20]. The radio channel from each transmitter to receive antenna has a random propagation path with a length of $L = 9$ sample periods. In the Standard Configuration of $R = 128$ and $T = 16$ for a total received energy over all receivers per data bit over measurement noise density at each receiver, E_b/N_0, of 5.15 dB an acceptable Bit Error Rate (BER) after coding of about 10^{-6} is achieved using a simulated ideal ADC with zero quantization error [9]. This provides an ideal system figure of merit to compare our systems with quantized measurements with. Given that $R/T = 8$, the signal-to-noise ratio (SNR) on each receive antenna is equal to $5.15 \text{ dB} - 10 \log 8 = 5.15 \text{ dB} - 9 \text{ dB} = -3.85 \text{ dB}$. This indicates that the noise power is significantly greater than the information signal power on each individual antenna, so that if a high resolution ADC is employed most of its output bits are nearly independent of the information signal. This provides the motivation for the use of coarse quantization, as for high-resolution quantizers the bits of lower significance are mostly independent of the data signal.

The system simulations are run with lower resolution ADCs to see the effects on the BER. For 4-bit quantization ($B = 4$) at 5 dB of E_b/N_0, the BER is increased to 1.2×10^{-6} with an additional 0.05 dB of power being required to match the BER performance of 10^{-6} for ideal non-quantized measurements. For 3-bit quantization ($B = 3$), the BER is increased to 2.2×10^{-6} with an additional 0.22 dB of power required to match the BER performance of ideal non-quantized measurements. For 2-bit quantization ($B = 2$), the BER is increased to about 2×10^{-5} with an additional 0.85 dB of power required to match the performance of ideal non-quantized measurements. Finally, for 1-bit quantization ($B = 1$), the BER is increased to 4×10^{-3} with an additional 3 dB of power required to match the performance of ideal non-quantized measurements. It is apparent that there is not much gain in the BER to operate above a 4-bit quantization. The additional 3 dB of power needed by a 1-bit quantization can be compensated out by doubling the number of receive antennas (which is mechanically feasible). A good trade-off is the 2-bit quantization ($B = 2$), which is used in this article as a case study to discuss the implementation of the data detection and decoding process.

IV. Detection in Fixed-Point Arithmetic

In this section the major operations of the receiver algorithm implemented in fixed-point arithmetic (calculating the Hermitian matrix $\boldsymbol{\Theta}$, its Hessenberg decomposition, and the eigenvalue decomposition through a numerically stable algorithm) are discussed, and numerical results for Standard Configuration ($T = 16$, $R = 128$) are presented.

A. Calculating $\boldsymbol{\Theta} = \boldsymbol{H}^{\mathrm{H}} \cdot \boldsymbol{H}$ in Fixed-Point Arithmetic

The computational pattern for calculating the matrix $\boldsymbol{\Theta} = \boldsymbol{H}^{\mathrm{H}} \cdot \boldsymbol{H}$ is sum-of-products, and the computation budget consists of T^2 inner products of R-element complex vectors. The inner product of two R-element complex-valued column vectors $\boldsymbol{X}$ and $\boldsymbol{Y}$

$$\begin{aligned} \boldsymbol{X} &= [\, x'_1 + \mathrm{j}\, x''_1 \;\; , \;\; \ldots \;\; , \;\; x'_R + \mathrm{j}\, x''_R \,]^{\mathrm{T}} \\ \boldsymbol{Y} &= [\, y'_1 + \mathrm{j}\, y''_1 \;\; , \;\; \ldots \;\; , \;\; y'_R + \mathrm{j}\, y''_R \,]^{\mathrm{T}} \end{aligned} \tag{8}$$

is given by

$$\begin{aligned} \boldsymbol{X}^{\mathrm{H}} \cdot \boldsymbol{Y} = [\, (x'_1\, y'_1 + x''_1\, y''_1) \; + \; \ldots \; + \; (x'_R\, y'_R + x''_R\, y''_R) \,] \\ - \mathrm{j}\, [\, (x''_1\, y'_1 - x'_1\, y''_1) \; + \; \ldots \; + \; (x''_R\, y'_R - x'_R\, y''_R) \,] \end{aligned} \tag{9}$$

In coarse quantization with $B = 2$-bit precision, only the values ± 1.0000 and ± 3.9152 can occur, as shown in Subsection II-C. Their encoding can be, for example, **10**, **11**, **00**, and **01**. It is apparent that these codes do not represent numerical values; they are merely labels. As a result, arithmetic cannot be directly implemented, and parallel counters [21]–[26] cannot be directly used to perform the multioperand additions required for the calculation of inner products. This problem is addressed below. In any case, the FPGA I/O data transfer time is significantly reduced due to this encoding style.

To calculate $\boldsymbol{X}^{\mathrm{H}} \cdot \boldsymbol{Y}$, the products of two B-bit quantized values (such as $x'_1\, y'_1$) are first calculated. The number of product values is also small, reaching 6 for $B = 2$ (± 1.0000, ± 3.9152, and ± 15.3288, which can be encoded with 3 bits). Each product is a 4-bit logic function (2 bits for each of the multiplicands and multipliers). Its three bits can be calculated in parallel with three LUTs (one LUT per bit). It should be observed that these products are also labels corresponding to values, not the standard numerical values.

Collapsing these products is performed in two stages. In the first stage, BRAMs, which are each configured as a $4\text{K} \times 9$ memory element, are used as look-up tables. Four 3-bit products are concatenated to form a 12-bit address into a BRAM, which in turn returns their sum. The maximum 4-product sum is 4×15.3288, which is a 7-bit quantity (sign bit included), if only the whole part is retained. However, since a BRAM provides a 9-bit output, two additional bits of precision

are available at no additional cost, making the sum a 9-bit quantity (sign bit included).

The advantage of using BRAMs is that the collapsing of four products into one larger sum is performed simultaneously with their conversion from labels to numerical values. In Equation (9) it is apparent that $2R = 256$ 3-bit products per real component (and $2R = 256$ 3-bit products per imaginary component) need to be collapsed. This means that $2 \times \frac{2R}{4} = 128$ BRAM accesses per complex-valued inner product are needed. In the second stage, the remaining $\frac{2R}{4} = 64$ sums in each of the real and imaginary components will be added together by a tree of ternary ripple-carry adders [27]. The final sum is a $9 + \log_2 64 = 15$-bit quantity (2 fractional bits and 1 sign bit are assigned to the value) in the extreme case that all values have maximum magnitude and add up constructively. This translates into a tree of $22+8+3+1 = 34$ ternary adders with the wordlength of 15 bits for each real and imaginary component, which requires an estimate of $2 \times 15 \times 34 = 1020$ LUTs. As a result, the latency of an inner product is the sum of a LUT delay (for calculating the initial 3-bit products), a BRAM delay (for calculating the sum of four products), and the delays of four 15-bit ripple-carry adders (for collapsing the remaining sums). The two fractional bits of the final sum are removed through right shift and rounding; thus, the final sum is a 13-bit integer. Since $\boldsymbol{\Theta}$ is Hermitian, its diagonal components are real, so the diagonal imaginary components do not need to be calculated. In addition, the entries above the main diagonal are the complex conjugates of the entries below the main diagonal, which means that the number of operations can be further reduced.

Due to their length and random nature, data signals of different users are likely to have very low correlation with each other. For this reason, $\boldsymbol{\Theta}$ is diagonal dominant. A sample of the reduced-wordlength matrix $\boldsymbol{\Theta}$ in a MMIMO with $R = 128$ and $T = 16$ is shown below. It is observed that its diagonal elements are real-valued and positive; in comparison, the real and imaginary components of off-diagonal elements are significantly smaller in magnitude. Statistics collected over one million samples of matrix $\boldsymbol{\Theta}$ indicate that the largest off-diagonal magnitude has an average of 49 and a standard deviation of 6. This means that most off-diagonal values can be represented with 7 bits (sign bit included). The overflowing off-diagonal values will be saturated to ± 63.

$$\boldsymbol{\Theta} = \begin{pmatrix} 289 & 5+\mathrm{j}\ 4 & -11-\mathrm{j}\ 2 & 7+\mathrm{j}\ 6 & \cdots \\ 5-\mathrm{j}\ 4 & 244 & 3+\mathrm{j}\ 1 & 6-\mathrm{j}\ 8 & \cdots \\ -11+\mathrm{j}\ 2 & 3-\mathrm{j}\ 1 & 211 & -9-\mathrm{j}\,13 & \cdots \\ 7-\mathrm{j}\ 6 & 6+\mathrm{j}\ 8 & -9+\mathrm{j}\,13 & 208 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \tag{10}$$

It is apparent that a wordlength of 9 bits provides sufficient precision to store each element of the matrix $\boldsymbol{\Theta}$. For higher quantization levels a longer wordlength may be required. However, if needed, a reduction of the wordlength could be performed in such cases by right shifting followed by truncation or rounding.

The channel matrix, $\boldsymbol{H}$, has $R \times T$ complex-valued elements. This translates into a storage requirement of $2 \times R \times T \times B$ bits. In standard configuration with $B = 16$-bit precision, a number of $2 \times 128 \times 16 \times 16 = 65536$ bits will have to be downloaded and stored into FPGA. Given that the XC7VX1140T, which is the largest FPGA in the top of the line family of Virtex-7, has *only* 1100 I/O pins, all those bits cannot be downloaded in parallel. The benefits of the coarse quantization are apparent, as both the channel state transfer time and storage capacity requirement are highly reduced.

A channel matrix $\boldsymbol{H}$ in the standard configuration has $R \times T = 128 \times 16 = 2048$ complex-valued elements. Even with coarse quantization, the number of FPGA I/O pins is too small to accomodate the transfer of all these elements in parallel. A single column, which includes $R = 128$ complex-valued elements (or $2\,R = 256$ real-valued elements), would require $2 \times 256 = 512$ I/O pins with a coarse quantization with $B = 2$ bits. Since the XC7VX1140T FPGA, which is the top of the line in the Virtex-7 family, has 1100 I/O pins, it is difficult to download the entire matrix $\boldsymbol{H}$ in parallel, since not many pins would remain available for other tasks. As a result, multiplexing is needed. It is mentioned that Serializer / Deserializer (SERDES) techniques [28] are intentionally not used in order to keep the digital hardware of each receive antenna as simple and inexpensive as possible.

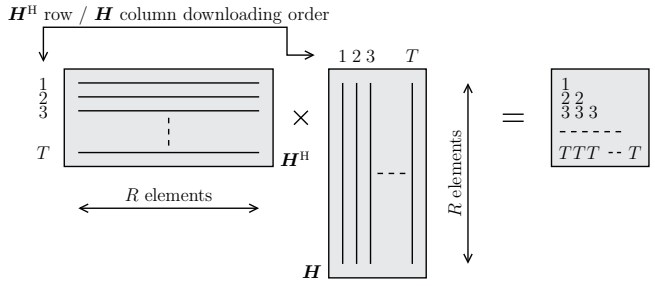


Fig. 1. Calculating $\boldsymbol{\Theta} = \boldsymbol{H}^{\mathrm{H}} \cdot \boldsymbol{H}$.

Figure 1 shows the strategy of calculating $\boldsymbol{\Theta} = \boldsymbol{H}^{\mathrm{H}} \cdot \boldsymbol{H}$. The elements of each column of $\boldsymbol{H}$ are loaded into the FPGA in parallel through separate I/O pins, and the columns are loaded sequentially. Column 1 of $\boldsymbol{H}$ (Row 1 of $\boldsymbol{H}^{\mathrm{H}}$) is first downloaded, allowing the inner product producing the top-left element, which is labeled 1, to be calculated. Column 2 of $\boldsymbol{H}$ (Row 2 of $\boldsymbol{H}^{\mathrm{H}}$) is downloaded next, allowing the inner products producing elements labeled 2 to be calculated. After the last column of $\boldsymbol{H}$ (last row of $\boldsymbol{H}^{\mathrm{H}}$) is downloaded, the inner products producing elements labeled T in the output matrix can be calculated. It is observed that each of the elements in a row of $\boldsymbol{\Theta}$ can be calculated in parallel. The ability of exploiting this data-level parallelism depends on the FPGA logic capacity.

The BRAM is a true dual-port memory, which means that only $\frac{128}{2} = 64$ BRAM units are needed for each inner product. This means that $T \cdot 64 = 16 \cdot 64 = 1024$ BRAMs are needed for calculation of the entire matrix $\boldsymbol{\Theta}$. This hardware cost is significant. The number of BRAMs can be reduced by calculating the first eight columns of $\boldsymbol{\Theta}$ in a first phase, and the last eight columns of $\boldsymbol{\Theta}$ in a second phase. This technique will reduce the number of BRAM units to $\frac{1024}{2} = 512$, but will

require iterating through the last eight columns of $\boldsymbol{H}$ again. The matrix's upper triangular portion is the complex conjugate of the lower triangular portion, and thus computing its values does not require additional operations.

Each inner product is implemented with a pipeline of three stages: (i) LUT plus BRAM, (ii) two 15-bit ripple-carry adders, and (iii) two 15-bit ripple-carry adders. There are $T = 16$ rows, out of which 8 will be accessed twice, as mentioned in the previous paragraph. This means that $16 + 8 + (3 - 1) = 26$ pipeline stages are needed to complete the calculation of $\boldsymbol{\Theta}$. Additional stages will be needed by housekeeping routines. The source code was implemented in VHDL and Xilinx Design Constraints (XDC) were carefully specified. Simulations carried out with Vivado [30] indicate that matrix $\boldsymbol{\Theta}$ can be calculated with a clock frequency of at least 100 MHz and with a latency of 50 cycles. The hardware utilization is 512 BRAMs, 23190 LUTs, and 8464 flip-flops.

B. Hessenberg Decomposition of $\boldsymbol{\Theta}$ in Fixed-Point Arithmetic

It is well known that a Hessenberg form is preserved during a similarity transformation [4]. For this reason, a conversion from a Hermitian form, $\boldsymbol{\Theta}$, to a Hessenberg form, $\boldsymbol{A}_{\text{hess}} = \boldsymbol{Q}_{\text{hess}} \cdot \boldsymbol{\Theta} \cdot \boldsymbol{Q}_{\text{hess}}^{\text{H}}$, is beneficial to be performed prior to applying the Francis-Kublanovskaya recursion, since this will significantly reduce the operation count [4]. It is observed that the reduced off-diagonal wordlength is highly beneficial for the fixed-point arithmetic since only off-diagonal elements are rotated in the Hessenberg conversion. For example, the first-column vector $\boldsymbol{v}$ (diagonal element is excluded), where $\boldsymbol{v}^T = [5 - \text{j}\,4\,,\ -11 + \text{j}\,2\,,\ 7 - \text{j}\,6\,,\ \dots]$, is converted into a vector $\boldsymbol{w}$, where $\boldsymbol{w}^T = [59 - \text{j}\,62\,,\ 0\,,\ 0\,,\ \dots]$. This vector still has a small magnitude compared to diagonal elements, which means that the Hessenberg form is also diagonal dominant. Moreover, since the off-diagonal elements of a Hessenberg form decrease in magnitude over Francis-Kublanovskaya iterations [13]–[15], there is no danger of overflow in any of those elements. According to our simulations, a wordlength of 8 bits can represent with sufficient precision the unitary matrices, $\boldsymbol{Q}_{\text{hess}}$, leading to Hessenberg and diagonal forms.

Calculating the Hessenberg / triagonal form of the Hermitian matrix $\boldsymbol{\Theta}$ is performed with Householder reflectors. A Householder reflector of a complex-valued column vector $\boldsymbol{z} = [z_1, z_2, \dots]^{\text{T}}$, where $z_i \in \mathbb{C}, \forall i$, is expressed in terms of a Hermitian unitary matrix, $\boldsymbol{F}$, which is constructed as:

$$\boldsymbol{F} \;=\; \boldsymbol{I} - 2\,\frac{\boldsymbol{v} \cdot \boldsymbol{v}^{\text{H}}}{\boldsymbol{v}^{\text{H}} \cdot \boldsymbol{v}}\ , \tag{11}$$

where:

$$\begin{aligned} \boldsymbol{v} \;&=\; \text{sgn}(z_1)\,\|z\|\ \boldsymbol{e}_1 - \boldsymbol{z} \\ \boldsymbol{e}_1 \;&=\; [1, 0, \dots]^{\text{T}} \\ \text{sgn}(z_1) \;&=\; \frac{z_1}{|z_1|} \quad \text{(complex signum)} \end{aligned} \tag{12}$$

A Householder reflector forces all vector elements with the exception of the first one to zero, as shown below.

$$\boldsymbol{F} \cdot \boldsymbol{z} \;=\; \text{sgn}(z_1)\,\|z\|\ \boldsymbol{e}_1 \tag{13}$$

In the above equations it is apparent that a Householder reflector relies on the squared Euclidean norm and the square root operation. Since these two operations are on the critical path of the computation, it is critical to minimize their latencies. This will be addressed in the next two subsections.

C. Squared Euclidean Norm

To simplify the presentation, the Squared Euclidean Norm of a K-element complex-valued vector $\boldsymbol{X}$ with elements $X_{\text{re},k} + \text{j}\,X_{\text{im},k}$ is written as the Squared Euclidean Norm of a $2K$-element real-valued vector with elements X_i:

$$\|\boldsymbol{X}\|^2 \;=\; \sum_{k=1}^{K} X_{\text{re},k}^2 + X_{\text{im},k}^2 \;=\; \sum_{i=1}^{2K} X_i^2 \tag{14}$$

The two's complement representation of each element X_i is given by:

$$\begin{aligned} X_i \;&=\; \overline{s_i\ x_{i,N-1}\ \dots\ x_{i,1}\ x_{i,0}} \;= \\ &=\; -2^{N\,r}\,s_i + 2^{(N-1)\,r}\,x_{i,N-1} \cdots + 2^r\,x_{i,1} + x_{i,0} \end{aligned} \tag{15}$$

where $x_{i,N-1}\,,\ \dots\ ,\ x_{i,1}\,,\ x_{i,0}$ are digits in a numeral system of radix r and s_i is the sign bit. In coarsely quantized MMIMO systems, the precision of the off-diagonal elements of matrix $\boldsymbol{\Theta}$ is on the order of a few bits. It is apparent that a two's complement representation with $r = 3$ (octal digits) and a precision of $N = 2$ digits plus a sign bit (which corresponds to a 7 bit two's complement integer) is sufficient to encode those off-diagonal elements shown in Equation 10. Therefore, the square of an element X_i is given by:

$$\begin{aligned} X_i^2 \;&=\; (-2^{2\cdot 3}\,s_i + 2^3\,x_{i,1} + x_{i,0})^2 \;=\; 2^{12}\,s_i + 2^6\,x_{i,1}^2 \\ &\quad + x_{i,0}^2 - 2^{10}\,s_i\,x_{i,1} - 2^7\,s_i\,x_{i,0} + 2^4\,x_{i,1}\,x_{i,0} \end{aligned} \tag{16}$$

where, obviously, $s_i^2 = s_i$. The last product, $x_{i,1}\,x_{i,0}$, can be decomposed in a similar fashion. Assume that $b_{i,02}$, $b_{i,01}$, and $b_{i,00}$ are the three bits of the octal digit $x_{i,0}$:

$$x_{i,0} \;=\; \overline{b_{i,02}\,b_{i,01}\,b_{i,00}} \tag{17}$$

Then, one can write:

$$x_{i,1}\,x_{i,0} \;=\; 2^2\,b_{i,02}\,x_{i,1} + 2\,b_{i,01}\,x_{i,1} + b_{i,00}\,x_{i,1} \tag{18}$$

It is observed that the negative terms in Equation (16) and all the terms in Equation (18) are products of an octal digit ($x_{i,1}$ and $x_{i,0}$) by a binary digit (s_i, $b_{i,02}$, $b_{i,01}$, and $b_{i,00}$). The importance of this representation will become apparent below. The sum of squares in Equation (14) can be written as

$$\begin{aligned} \sum_{i=1}^{2K} X_i^2 \;&=\; 2^{12}\,\underbrace{\sum_{i=1}^{2K} s_i}_{\Sigma_1} + 2^6\,\underbrace{\sum_{i=1}^{2K} x_{i,1}^2}_{\Sigma_2} + \underbrace{\sum_{i=1}^{2K} x_{i,0}^2}_{\Sigma_3} \\ &\quad - 2^{10}\,\underbrace{\sum_{i=1}^{2K} s_i\,x_{i,1}}_{\Sigma_4} - 2^7\,\underbrace{\sum_{i=1}^{2K} s_i\,x_{i,0}}_{\Sigma_5} + 2^6\,\underbrace{\sum_{i=1}^{2K} b_{i,02}\,x_{i,1}}_{\Sigma_6} \\ &\quad + 2^5\,\underbrace{\sum_{i=1}^{2K} b_{i,01}\,x_{i,1}}_{\Sigma_7} + 2^4\,\underbrace{\sum_{i=1}^{2K} b_{i,00}\,x_{i,1}}_{\Sigma_8} \end{aligned} \tag{19}$$

In a Householder reflector for matrix $\mathbf{\Theta}$, $K \leq T-1$. In MMIMO standard configuration $T = 16$; therefore, $K \leq 15$. The sum Σ_1 (which is a 5-bit quantity) is calculated with a parallel counter in two stages. First, sums of six s_i bits are calculated with three 6-input LUTs per sum, since each such a sum is a 3-bit quantity; thus, no carry propagation occurs and the hardware requirement is $3 \times \lceil \frac{2K}{6} \rceil = 15$ LUTs. In the second stage the $\lceil \frac{2K}{6} \rceil = 5$ resulting 3-bit sums can be collapsed with two ternary ripple-carry adders [27] requiring 4 and 5 LUTs, respectively. According to our VHDL code synthesized and simulated with Vivado [30], ternary adders are instantiated out of behavioral code only if the bitwidth ≥ 7. For bitwidth ≤ 6, ternary adders are instantiated by coding with Xilinx primitives.

Sums Σ_2 and Σ_3 (11-bit quantities) have the same computational pattern. Σ_2, for example, can be expanded as

$$\Sigma_2 = \sum_{j=1}^{K} \underbrace{x_{(2j-1),1}^2 + x_{(2j),1}^2}_{\Sigma'_{2,j}} \tag{20}$$

Since $x_{(2j-1),1}$ and $x_{(2j),1}$ are octal digits, each sum $\Sigma'_{2,j}$ (a 7-bit quantity) is a 6-input logic function and can be implemented with seven 6-input LUTs (no carry propagation occurs). $7 \times K = 105$ LUTs are needed in this stage. In the second stage $K = 15$ 7-bit arguments are to be collapsed. This is achieved by a tree of $5+1+1 = 7$ ternary ripple-carry adders, which require up to $7 \times 11 = 77$ LUTs.

The sums Σ_4, Σ_5, Σ_6, Σ_7, and Σ_8 are 8-bit quantities and have the same computational pattern, which is sum of products of an octal digit by a binary digit. Σ_4, for example, can be expanded as

$$\Sigma_4 = \sum_{j=1}^{\lceil \frac{2K}{3} \rceil} \underbrace{s_{3j-2}\, x_{(3j-2),1} + s_{3j-1}\, x_{(3j-1),1} + s_{3j}\, x_{(3j),1}}_{\Sigma'_{4,j}} \tag{21}$$

It is apparent that each sum $\Sigma'_{4,j}$ is a 5-bit value, and can be regarded as having three octal arguments ($x_{(3j-2),1}$, $x_{(3j-1),1}$, $x_{(3j),1}$) and three mask bits (s_{3j-2}, s_{3j-1}, s_{3j}). It can be implemented with a 4-bit ternary ripple-carry adder, that is, with a *CARRY4* primitive and four 6-input LUTs in which the mask bits will drive three out of those six inputs. $4 \times \lceil \frac{2K}{3} \rceil = 40$ LUTs are needed in this stage. In the second stage $\lceil \frac{2K}{3} \rceil = 10$ four-bit arguments are to be collapsed. This is achieved by a tree of $3+1+1 = 5$ ternary ripple-carry adders, which requires up to $5 \times 8 = 40$ LUTs.

In the final stage, sums Σ_1, Σ_2, Σ_3, Σ_4, Σ_5, Σ_6, Σ_7, and Σ_8 are collapsed to give the squared Euclidean norm, $\|\boldsymbol{X}\|^2$ (a 16-bit quantity). This is achieved by a tree of $3+1 = 4$ ternary ripple-carry adders, which requires up to $4 \times 16 = 64$ LUTs. Long carry propagation over 12 bits, as it is apparent in Equation (19), occurs only in this final stage.

The source code was implemented in VHDL and Xilinx Design Constraints (XDC) were carefully specified. Simulations carried out with Vivado [30] indicate that the squared Euclidean norm can be calculated with a clock frequency of 100 MHz and with a latency of 5 cycles with timing slack to spare. The hardware utilization includes 1160 LUTs and 235 flip-flops. This is a good result compared to the behavioral solution in implementing Equation (14) by collapsing $2K = 30$ squared 6-bit operands, whose latency would be approximately 50% larger that the proposed solution and would require over 2000 LUTs.

D. Square Root Operation

A number of $T-2 = 14$ Householder reflectors need to be calculated for each matrix $\mathbf{\Theta}$. Since the square root operation is on the critical path of the Householder reflector, it is imperative to reduce its latency. Thus, recursive bit-level solutions, such as the Convergence Computing Method [32], would be too slow for a MMIMO application. A parallel implementation in fixed-point / integer arithmetic is sought.

Statistics collected over one million samples of matrix $\mathbf{\Theta}$ and the resulting Hessenberg form indicate that the sum-of-squares of lower off-diagonal elements in a column can be represented with a bitwidth of 16 bits or less. In integer arithmetic, when only the integer bits are retained, the square root of 16-bit argument has a wordlength of 8 bits. In the most general case, the square root of an integer X has a integer part, $\lfloor Y \rfloor$, and a fractional part, $\{Y\}$:

$$\sqrt{X} = Y = \lfloor Y \rfloor + \{Y\}\,, \quad \text{where } \{Y\} \in [0,1) \tag{22}$$

In order to keep the truncation error in the range $(-0.5, 0.5)$, the square root implemented in integer arithmetic is approximated as:

$$\sqrt{X} \approx \begin{cases} \lfloor Y \rfloor & \text{if } \{Y\} < 0.5 \\ \lfloor Y \rfloor + 1 & \text{if } \{Y\} > 0.5 \end{cases} \tag{23}$$

It is apparent that the fractional part, $\{Y\}$, can never be equal to 0.5, since in that case the argument X, which is an integer, would have a fractional part $\{X\} = 0.25$:

$$\begin{aligned} \sqrt{X} = Y = \lfloor Y \rfloor + 0.5 \quad &\Rightarrow \\ \Rightarrow \quad X = (\lfloor Y \rfloor + 0.5)^2 = \lfloor Y \rfloor^2 + \lfloor Y \rfloor + \underbrace{0.25}_{\{X\}} \end{aligned} \tag{24}$$

This fractional part is small. Therefore, with a very good approximation:

$$\sqrt{\lfloor Y \rfloor^2 + \lfloor Y \rfloor} \approx \lfloor Y \rfloor + 0.5 \tag{25}$$

As a result, Equation (23) can be replaced by Equation (26), which in turn can be more easily converted into LUT configuration information. For example, consider the threshold in the square root domain $Y = 251.5 \Rightarrow \lfloor Y \rfloor = 251$. This translates into a threshold in the argument domain of $\lfloor Y \rfloor^2 + \lfloor Y \rfloor = 63252$. Then, the argument values $X \geq 63252$ will map into $\sqrt{X} = 252$, and the argument values $X < 63252$ will map into $\sqrt{X} = 251$. In a second example, the threshold in the square root domain $Y = 131.5 \Rightarrow \lfloor Y \rfloor = 131$ translates into a threshold in the argument domain of $\lfloor Y \rfloor^2 + \lfloor Y \rfloor = 17292$. Then, the argument values $X \geq 17292$ will map into $\sqrt{X} = 132$, and the argument values $X < 17292$

will map into $\sqrt{X} = 131$. All the other thresholds will follow a similar pattern.

$$\sqrt{X} \approx \begin{cases} \lfloor Y \rfloor & \text{if } X < \lfloor Y \rfloor^2 + \lfloor Y \rfloor \\ \lfloor Y \rfloor + 1 & \text{if } X \geq \lfloor Y \rfloor^2 + \lfloor Y \rfloor \end{cases} \quad (26)$$

In a brute force implementation, the integer part of the square root is retrieved from a large lookup table built with BRAM units. Since the argument and square root are 16-bit and 8-bit integers, respectively, the LUT size needs to be 2^{16} bytes or 64 KB. Such a large LUT is implemented with sixteen 32K $\times$ 1 BRAMs (two BRAMs per output bit). The square root latency is one BRAM delay, thus it is very short, but the hardware cost is large. A technique to reduce the LUT size is presented next.

It is observed that $\lfloor Y \rfloor^2 + \lfloor Y \rfloor$ is an even number. This means that only 15 bits are in fact needed to form the LUT address, and the square root approximation can be written as:

$$\sqrt{X} \approx \begin{cases} \lfloor Y \rfloor & \text{if } (X >> 1) < [(\lfloor Y \rfloor^2 + \lfloor Y \rfloor) >> 1] \\ \lfloor Y \rfloor + 1 & \text{if } (X >> 1) \geq [(\lfloor Y \rfloor^2 + \lfloor Y \rfloor) >> 1] \end{cases} \quad (27)$$

Consider the same example of the threshold in the square root domain $Y = 251.5 \;\Rightarrow\; \lfloor Y \rfloor = 251$. By removing the least significant bit, argument values $(X >> 1) \geq (63252 >> 1) = 31626$ will map into $\sqrt{X} = 252$, and argument values $(X >> 1) < 31626$ will map into $\sqrt{X} = 251$. This strategy reduces the number of BRAMs from sixteen to eight, thus halving the cost of the implementation.

In the described implementation, it is apparent that the maximum rounding error is slightly above 0.5, since that small fraction of 0.25 in Equation (24) is lost in approximating $X \approx \lfloor Y \rfloor^2 + \lfloor Y \rfloor$. In order to limit the maximum rounding error to exactly 0.5, the approximation in Equation (26) needs to be rewritten as:

$$\sqrt{X} \approx \begin{cases} \lfloor Y \rfloor & \text{if } X \leq \lfloor Y \rfloor^2 + \lfloor Y \rfloor \\ \lfloor Y \rfloor + 1 & \text{if } X > \lfloor Y \rfloor^2 + \lfloor Y \rfloor \end{cases} \quad (28)$$

Considering the same numerical example, that means that the argument values $X > 63252$ will have to map into $\sqrt{X} = 252$, and the argument values $X \leq 63252$ will have to map into $\sqrt{X} = 251$. In this case, the right shift operation needs to be accompanied with rounding, such that $63253 >> 1 = 31627$. The implementation is shown in Figure 2. The latency of this implementation is given by the delay of a 15-bit adder and a BRAM delay, which is a very low. The hardware cost is eight BRAMs plus a 15-bit adder.

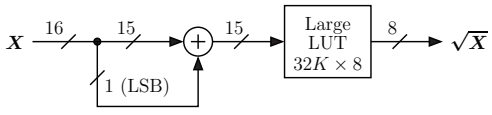


Fig. 2. Square root implemented with a large LUT.

The squared Euclidean norm and the square root, which are on the critical path of the Householder reflector implementation, as it is apparent in Equations (11) and (12), are implemented with LUTs and BRAMs. The application of a Householder reflector, $\boldsymbol{F}_i \cdot \boldsymbol{\Theta}$, where $i = 1, 2, \ldots T-2$, and the accumulation of the successive Householder reflectors into a global unitary matrix, $\boldsymbol{Q}_{\text{hess}}$, is implemented with DSP slices.

E. Francis-Kublanovskaya Algorithm in Fixed-Point Arithmetic

The eigenvalue decomposition of matrix $\boldsymbol{\Theta}$ is performed in two steps: (i) initial transformation of $\boldsymbol{\Theta}$ into a Hessenberg matrix $\boldsymbol{A}_{\text{hess}}$, and (ii) diagonalization of $\boldsymbol{A}_{\text{hess}}$ through the Francis-Kublanovskaya (FK) recursion [13]–[15], in which each iteration consists of a QR decomposition followed by a reverse product. The QR decomposition is performed through rotating the 2-element vertical vector in each column such that the off-diagonal element in that column is forced to zero. This rotation can also be implemented with a Householder reflector.

Since the FK algorithm can diagonalize the matrix $\boldsymbol{\Theta}$ directly, although with a much larger number of operations, the matrices $\boldsymbol{\Theta}$ and $\boldsymbol{A}_{\text{hess}}$ are used interchangeably to simplify the remaining part of the presentation. At iteration k, the matrix $\boldsymbol{\Theta}^{(k)}$ (where $\boldsymbol{\Theta}^{(0)} = \boldsymbol{\Theta}$) is decomposed into the product of a unitary matrix $\boldsymbol{Q}^{(k)}$ and an upper triangular matrix $\boldsymbol{R}^{(k)}$. By multiplying $\boldsymbol{R}^{(k)}$ by $\boldsymbol{Q}^{(k)}$, a similarity transformation of $\boldsymbol{\Theta}^{(k)}$ is obtained, as shown in Equation 29.

$$\boldsymbol{\Theta}^{(k+1)} = \boldsymbol{R}^{(k)} \cdot \boldsymbol{Q}^{(k)} = \boldsymbol{Q}^{(k)\,\mathrm{H}} \cdot \boldsymbol{\Theta}^{(k)} \cdot \boldsymbol{Q}^{(k)} \quad (29)$$

If $k \to \infty$, then the matrix $\boldsymbol{\Theta}^{(k)}$ tends to a diagonal matrix, $\boldsymbol{\Lambda}$, whose elements are the eigenvalues of the initial $\boldsymbol{\Theta}$:

$$\boldsymbol{\Theta} = \underbrace{\boldsymbol{Q}^{(n)\,\mathrm{H}} \cdot \ldots \cdot \boldsymbol{Q}^{(k)\,\mathrm{H}} \cdot \ldots \cdot \boldsymbol{Q}^{(0)\,\mathrm{H}}}_{\boldsymbol{Q}^{\mathrm{H}}} \cdot \boldsymbol{\Lambda} \cdot \underbrace{\boldsymbol{Q}^{(0)} \cdot \ldots \cdot \boldsymbol{Q}^{(k)} \cdot \ldots \cdot \boldsymbol{Q}^{(n)}}_{\boldsymbol{Q}} \quad (30)$$

The off-diagonal elements of matrix $\boldsymbol{\Theta}$ (or the Hessenberg form $\boldsymbol{A}_{\text{hess}}$) decrease in magnitude over FK iterations. As a result, there is no danger of overflow in any of those elements, and the wordlength needed to represent diagonal elements would suffice for representing the off-diagonal elements, too.

The unitary matrix $\boldsymbol{Q}$ of the eigenvalue decomposition of the Hermitian matrix $\boldsymbol{\Theta}$, and all unitary matrices $\boldsymbol{Q}^{(k)}$ of the QR decompositions, are essentially rotation matrices. As a result, all their elements range between -1.0 and $+1.0$ (thus, there is no danger of encountering an overflow). In our fixed-point arithmetic implementation, a scale factor equal to 2^{qwl-1} is embedded into the matrix $\boldsymbol{Q}$, so that its wordlength is $(qwl - 1)$ magnitude bits + 1 sign bit $= qwl$ bits. The matrices $\boldsymbol{\Theta}$ and $\boldsymbol{\Lambda}$ are already in fixed-point representation, their wordlengths being equal, $\theta wl = \lambda wl$. As a result, the eigenvalue decomposition can be written as:

$$\boldsymbol{\Theta} = \boldsymbol{Q} \cdot \boldsymbol{\Lambda} \cdot \boldsymbol{Q}^{\mathrm{H}} \;\Rightarrow\; \boldsymbol{\Theta} = \frac{2^{qwl-1}\boldsymbol{Q}}{2^{qwl-1}} \cdot \boldsymbol{\Lambda} \cdot \frac{2^{qwl-1}\boldsymbol{Q}^{\mathrm{H}}}{2^{qwl-1}} \;\Rightarrow$$
$$\Rightarrow \quad 2^{2\cdot(qwl-1)}\,\boldsymbol{\Theta} = \underbrace{\left(2^{qwl-1}\boldsymbol{Q}\right)}_{\underline{\boldsymbol{Q}}} \cdot \boldsymbol{\Lambda} \cdot \underbrace{\left(2^{qwl-1}\boldsymbol{Q}^{\mathrm{H}}\right)}_{\underline{\boldsymbol{Q}}^{\mathrm{H}}} \quad (31)$$

where $\underline{\boldsymbol{Q}}$ and $\underline{\boldsymbol{Q}}^{\mathrm{H}}$ is the unitary matrix and its Hermitian transpose in fixed-point representation (that is, with the scale factor

embedded). Similarly, $\underline{\boldsymbol{\Theta}}^{(k)}$ is the fixed-point representation of $\boldsymbol{\Theta}^{(k)}$, and an FK iteration in the fixed-point domain can be written as:

$$\left.\begin{aligned} \boldsymbol{\Theta}^{(k)} &= \boldsymbol{Q}^{(k)} \cdot \boldsymbol{R}^{(k)} \;\Rightarrow\; \underline{\boldsymbol{\Theta}}^{(k)} = \underline{\boldsymbol{Q}}^{(k)} \cdot \boldsymbol{R}^{(k)} \\ \underline{\boldsymbol{\Theta}}^{(k+1)} &= \boldsymbol{R}^{(k)} \cdot \underline{\boldsymbol{Q}}^{(k)} \end{aligned}\right\} \Rightarrow$$
$$\Rightarrow \quad \boldsymbol{\Theta}^{(k+1)} = \underline{\boldsymbol{\Theta}}^{(k+1)} >> (qwl - 1) \quad (32)$$

It is mentioned that the last right shift operation may be performed with or without rounding.

The convergence of the Francis-Kublanovskaya algorithm can be significantly improved by introducing shifts in the diagonal values of matrices $\boldsymbol{\Theta}^{(k)}$ [4]. There are three common shifts used in FK algorithms: (i) the Rayleigh quotient shift, which is equal to the last diagonal element; (ii) the Wilkinson shift, which is equal to the eigenvalue of the lower rightmost 2-by-2 sub-matrix of $\boldsymbol{\Theta}^{(k)}$; and (iii) the Francis double shift, which applies a complex conjugate pair of shifts. In our simulations, the Rayleigh quotient shift has been used due to its implementation simplicity.

A challenge of designing a MMIMO base station is to minimize the wordlengths θwl and qwl, while the bit-error rate is maintained at acceptable levels. As mentioned in previous paragraphs, our simulation software using floating-point arithmetic used in prior work [9] has been converted to use fixed-point arithmetic. To estimate the transmitted vector $\boldsymbol{X}$, the linear system shown in Equation (1) is solved through an eigenvalue decomposition rather than the MATLAB® backslash operator. The wordlength of matrix $\boldsymbol{Q}$ was set to $qwl = 6$ and $qwl = 7$ bits, and the wordlength of matrix $\boldsymbol{\Theta}$ was set to $\theta wl = 9$, $\theta wl = 10$, and $\theta wl = 11$. The number of quantization bits were set to $B = 1$, $B = 2$, and then $B = 3$. Extensive simulation runs were attempted, and BER performance figures were recorded.

In the system we have evaluated, each user independently transmits a single-carrier signal with a modulation of order 4 QPSK using 256-symbol blocks with a cyclic prefix of 16 samples. An error correction code consisting of a rate $\frac{1}{2}$ convolutional code applied over 32 single-carrier blocks is used. The simulated random multipath fading channel had a maximum delay of 9 symbol periods. The channel state is assumed to be stable over each set of 32 single-carrier blocks, where for each set the user transmits 2 pilots per block with content known a priori at the receiver which is used for initial channel estimation. A joint channel estimation/data detection/data decoding algorithm as described in [9] is used to provide the final result.

The BER figures versus the wordlength for implementing the eigenvalue decomposition in fixed-point arithmetic with reduced precision are presented in Table III. For reference, the BER figures corresponding to a double-precision floating-point implementation are also provided. It is apparent that for a coarse quantization with $B = 1$ bit, neither the floating-point nor the fixed-point implementations achieve a satisfactory BER in a small number of iterations. For a coarse quantization with $B = 2$ or $B = 3$, three to four iterations are sufficient to achieve a good BER. It is observed that an additional iteration is generally needed in fixed-point implementation over the floating-point implementation to match their BERs; for example, BER$(B = 2, qwl = 6, \theta wl = 9, i = 3) = 0.0259$ (fixed-point), whereas BER$(B = 2, qwl = 64, \theta wl = 64, i = 2) = 0.0236$ (floating-point).

TABLE III
BER VERSUS WORDLENGTH FOR $R = 128$, $T = 16$, $E_b/N_0 = 5\,\text{dB}$ (ONLY THE FIRST THREE ITERATIONS ARE SHOWN).

B	Wordlength		Iteration		
	qwl	θwl	$i = 1$	$i = 2$	$i = 3$
1	Double-Precision Floating-Point Arithmetic				
	64	64	0.4581	0.3235	0.2116
	Fixed-Point Arithmetic				
	6	9	0.4717	0.3990	0.2670
	6	10	0.4713	0.3443	0.2503
	6	11	0.4706	0.3461	0.2482
	7	9	0.4705	0.3930	0.2666
	7	10	0.4741	0.3442	0.2516
	7	11	0.4723	0.3520	0.2539
2	Double-Precision Floating-Point Arithmetic				
	64	64	0.2854	0.0236	0.0078
	Fixed-Point Arithmetic				
	6	9	0.3284	0.0823	0.0259
	6	10	0.3225	0.0395	0.0112
	6	11	0.3203	0.0311	0.0125
	7	9	0.3277	0.0794	0.0303
	7	10	0.3245	0.0399	0.0107
	7	11	0.3206	0.0315	0.0106
3	Double-Precision Floating-Point Arithmetic				
	64	64	0.1849	0.0396	0.0066
	Fixed-Point Arithmetic				
	6	9	0.2380	0.0379	0.0091
	6	10	0.2265	0.0389	0.0089
	6	11	0.2226	0.0453	0.0104
	7	9	0.2342	0.0354	0.0083
	7	10	0.2255	0.0371	0.0090
	7	11	0.2201	0.0436	0.0119

It is apparent that for a quantization with $B = 2$ bits, the matrix $\boldsymbol{Q}$'s wordlength, qwl, has little impact on BER. As an example, BER$(B = 2, qwl = 6, \theta wl = 9, i = 2) = 0.0823$, and BER$(B = 2, qwl = 7, \theta wl = 9, i = 2) = 0.0794$. On the other hand, the matrix $\boldsymbol{\Theta}$'s wordlength, θwl, has a much stronger impact on BER. For example, BER$(B = 2, qwl = 6, \theta wl = 10, i = 2) = 0.0395$, which a significant decrease from 0.0823. It should be observed that the BER does not improve significantly for $\theta wl \geq 11$. A MMIMO system with $B = 3$ is robust enough to operate with $\theta wl = 9$, but the cost of the implementation will be higher due to the increased complexity of the implementation in fixed-point arithmetic.

Based on these considerations, it is apparent that a good trade-off in implementing a MMIMO base station is a coarse quantization with $B = 2$ bits, a $\boldsymbol{Q}$'s wordlength $qwl = 7$ bits, and a $\boldsymbol{\Theta}$'s wordlength $\theta wl = 10$ bits. With such a reduced qwl, vector rotations can be implemented in inexpensive hardware, such as an array of reasonably sized FPGAs. A reduced θwl allows the extensive use of FPGA Digital-Signal Processing slices to perform the reverse products in the FK recursion, as well as complete the calculation of the solution of the linear system shown in Equation (1) through matrix multiplication, as outlined in Equation (4). Previous works are in line with these claims [16].

V. Conclusions

For 2-bit quantization ($B = 2$), an additional 0.85 dB of signal power is required to match the performance of ideal non-quantized measurements. The eigenvalue decomposition, the most computationally demanding portion of a MMIMO receiver algorithm, can be implemented in fixed-point arithmetic with wordlengths of 7 and 10 bits for eigenvectors and eigenvalues, respectively, at the expense of a small degradation of the Bit-Error Rate achieved in a double-precision floating-point implementation. An inexpensive set of reasonably sized FPGAs further reduce the cost of implementing massive MIMO base stations, which is a key impediment to their widespread deployment. In future work, the wordlength of the fixed-point implementation will be assessed in the presence of signal contamination from adjacent networks.

References

[1] C. Mollén, "High-End Performance with Low-End Hardware. Analysis of Massive MIMO Base Station Transceivers," Ph.D. dissertation, Linköping University, Linköping, Sweden, 2018.

[2] C. Mollén, J. Choi, E. G. Larsson, and J. Robert W. Heath, "Uplink Performance of Wideband Massive MIMO with One-Bit ADCs," *IEEE Transactions on Wireless Communications*, vol. 16, no. 1, pp. 87–100, January 2017.

[3] ——, "Achievable Uplink Rates for Massive MIMO with Coarse Quantization," in *Proceedings of the 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2017)*. New Orleans, Louisiana: IEEE, March 2017, pp. 6488–6492.

[4] G. H. Golub and C. F. van Loan, *Matrix Computations*, 3rd ed. The Johns Hopkins University Press, 1996.

[5] B. Parhami, *Computer Arithmetic: Algorithms and Hardware Designs*. Oxford University Press, 2000.

[6] M. Ercegovac and T. Lang, *Digital Arithmetic*, Morgan Kaufmann, 2003.

[7] A. Chockalingam and B. S. Rajan, *Large MIMO Systems*. Cambridge University Press, 2014.

[8] M. K. Ozdemir and H. Arslan, "Channel Estimation for Wireless OFDM systems," *IEEE Communications Surveys and Tutorials*, vol. 9, no. 2, pp. 18–48, July 2007.

[9] Z. Zhang, M. McGuire, and M. Sima, "Iterative Channel Estimation for Large Scale MIMO with Highly Quantized Measurements in 5G," in *The 28th European Signal Processing Conference (EUSIPCO 2020)*. Amsterdam, The Netherlands: European Association for Signal Processing (EURASIP), January 2021, pp. 1643–1647.

[10] *IEEE Standard for Floating-Point Arithmetic. IEEE STD 754-2019*, IEEE Computer Society, July 2019.

[11] J. M. Mendel, *Lessons in Estimation Theory for Signal Processing, Communications, and Control*, 2nd ed. Prentice-Hall, 1995.

[12] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley-Interscience, 2006.

[13] J. Francis, "The QR transformation – Part 1," *The Computer Journal*, vol. 4, no. 3, pp. 265–272, October 1961.

[14] ——, "The QR transformation – Part 2," *The Computer Journal*, vol. 4, no. 4, pp. 332–345, January 1962.

[15] V. N. Kublanovskaya, "On some algorithms for the solution of the complete eigenvalue problem," *USSR Comput. Math. and Math. Physics*, no. 3, pp. 637–657, March 1961.

[16] G. Xu, Y. Li, J. Yuan, R. Monroe, S. Rajagopal, S. Ramakrishna, Y. H. Nam, J.-Y. Seol, J. Kim, M. M. U. Gul, A. Aziz, and J. Zhang, "Full Dimension MIMO (FD-MIMO): Demonstrating Commercial Feasibility," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 8, pp. 1876–1886, August 2017.

[17] A. Molisch, *Wireless Communications*, 2nd ed. West Sussex, United Kingdom: John Wiley & Sons, 2011.

[18] A. Chockalingam and B. Sundar Rajan, *Large MIMO Systems*. Cambridge, United Kingdom: Cambridge University Press, 2014.

[19] A. Zaidi, F. Athley, J. Medbo, U. Gustavsson, G. Durisi, and X. Chen, *5G Physical Layer: Principles, Models and Technology Components*. Academic Press, 2018.

[20] M. Ozdemir and H. Arslan, "Channel estimation for wireless OFDM systems," *IEEE Communications Surveys Tutorials*, vol. 9, no. 2, pp. 18–48, 2007.

[21] J. Robert F. Jones and J. Earl E. Swartzlander, "Parallel Counter Implementation," *Journal of VLSI Signal Processing Systems for Signal, Image and Video Technology*, vol. 7, no. 3, pp. 223–232, October 1994.

[22] H. Parandeh-Afshar, P. Brisk, and P. Ienne, "Efficient Synthesis of Compressor Trees on FPGAs," in *Proceedings of the 13th Asia and South Pacific Design Automation Conference (ASP-DAC 2008)*, Seoul, Korea, March 2008, pp. 138–143.

[23] ——, "Exploiting Fast Carry-Chains of FPGAs for Designing Compressor Trees," in *Proceedings of the 19th International Conference on Field Programmable Logic and Applications (FPL'09)*, Prague, Czech Republic, August-September 2009, pp. 242–249.

[24] T. Matsunaga, S. Kimura, and Y. Matsunaga, "Multi-Operand Adder Synthesis on FPGAs using Generalized Parallel Counters," in *Proceedings of the 15th Asia and South Pacific Design Automation Conference (ASP-DAC 2010)*, Taiwan, January 2010, pp. 337–342.

[25] H. Parandeh-Afshar, A. Neogy, P. Brisk, and P. Ienne, "Compressor Tree Synthesis on Commercial High-Performance FPGAs," *ACM Transactions on Reconfigurable Technology and Systems*, vol. 4, no. 4, pp. 39:1–39:19, December 2011.

[26] B. Khurshid and R. N. Mir, "High Efficiency Generalized Parallel Counters for Look-Up Table Based FPGAs," *International Journal of Reconfigurable Computing*, vol. 2015, September 2015.

[27] J. M. Simkins and B. D. Philofsky, "Structures and Methods for Implementing Ternary Adders / Subtractors in Programmable Logic Devices," U.S. Patent 7,274,211 B1, September 2007.

[28] Xilinx, Inc., "All Programmable 7 Series – Product Selection Guide," User Guide XMP101, v1.7, February 2018.

[29] Xilinx, Inc., "7 Series FPGAs Memory Resources: User Guide," User Guide UG473, v1.13, February 2019.

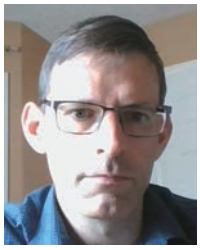
[30] Xilinx, Inc., "Vivado Design Suite – HLx Editions," ver. 2018.3, 2018.

[31] M. Tian, M. Sima, and M. Michael McGuire, "Massive MIMO in Fixed–Point Arithmetic," in *Proceedings of the 23rd International Conference on Advanced Communications Technology (ICACT 2021)*, PyeongChang, Korea, February 2021, pp. 91–95.

[32] Chen TC (1972) Automatic Computation of Exponentials, Logarithms, Ratios, and Square Roots. IBM Journal of Research and Development 16(4):380–388

Mi Tian was born in the People's Republic of China in 1988 and received her B.S. degree in optical communications engineering from Jilin University, Changchun, Jilin, China, in 2010, her M.S. degree in analogue and digital integrated circuit design from Imperial College London, U.K., in 2011, and her Ph.D. degree from the University of Victoria, British Columbia, Canada, in 2021. She is currently a postdoctoral fellow in the Department of Electrical and Computer Engineering at the same institution. Her research interests include wireless communication systems, hardware implementation on FPGAs of massive MIMO communication systems.

Mihai Sima (S'00–M'04) was born in Romania in 1964 and received his B.Eng. degree in electronics engineering from Polytechnic Institute of Bucharest, Romania in 1989, and his Ph.D. degree in computer engineering from Delft University of Technology, The Netherlands, in 2004. Since 2003, he has been a faculty member in the Department of Electrical and Computer Engineering at the University of Victoria, British Columbia, Canada. His research interests include computer architecture and engineering, reconfigurable computing, embedded systems, circuit design, and hardware security.



Michael McGuire (S'95–M'97) was born in Canada in 1970 and received his B.Eng. in computer engineering from the University of Victoria, British Columbia, Canada, in 1995, his M.A.Sc. in electrical engineering from the same institution in 1997, and his Ph.D. from the University of Toronto in 2003. Since 2003, he has been a faculty member in the Department of Electrical and Computer Engineering at the University of Victoria. Dr. McGuire's research area is in the application of signal processing to communications, developing new techniques for Faster-than-Nyquist signaling, iterative channel estimation/data detection, and wireless radio localization suitable for advanced wireless systems.

Automatic Vocabulary Grouping and Deep Combination for News Credibility and Reliability Evaluation Corresponding to Specific Language

Ming-Shen Jian*, Rong-Bin Deng**, Chen-Wei Fang***, Hua-Yu Wu****, Wen-Hsiang Hsieh*****

Cloud Computing and Intelligent System Lab., Dept. of CSIE, National Formosa University

Yunlin County, Taiwan 632

jianms@nfu.edu.tw, 40743162@gm.nfu.edu.tw, 40743206@gm.nfu.edu.tw, 40743212@gm.nfu.edu.tw, 40743160@gm.nfu.edu.tw

***Abstract*—Considering the spread of the intentional false news, to be aware of the new news is important. In this research, the Automatic Deep Vocabulary Grouping and Combination for News Credibility and Reliability Evaluation is proposed which includes Key Vocabularies Merging Method and False News Warning Method. By merging different algorithms, the proposed system could cluster and group the fake news according to the found features of various fake news content. The proposed system could find and verify the features of the specific intentional false news according to the proposed deep combination evaluation function. After suitable verification and recursive checking, the minimum groups for clustering the fake news could be given. Based on the collected features of the various intentional false news, the new coming news can be classified as the false news due to the feature matching percentage. According to the verification, all the collected and proved fake news could be found and clustered into the corresponding fake news groups.**

***Keyword*—False News, Cluster, Web Crawler, Cloud Computing**

Manuscript received August 23, 2021 ", and a follow-up of the invited journal to the accepted & presented paper entitled " Automatic Vocabulary Grouping and Deep Combination for News Credibility and Reliability Evaluation Corresponding to Specific Language " of the 21th International Conference on Advanced Communication Technology (ICACT2021)." This work is Final File 20210125_finalpaper.pdf and was supported in part by the Cloud Computing and Intelligent System Lab., Dept. of CSIE, National Formosa University.

Ming-Shen Jian is with the Cloud Computing and Intelligent System Lab., Dept. of CSIE, National Formosa University, Taiwan (corresponding author to provide phone: 886-922-916612; fax: 886-563-60306; e-mail: jianms@nfu.edu.tw).

Rong-Bin Deng is with the Cloud Computing and Intelligent System Lab., Dept. of CSIE, National Formosa University, Taiwan

Chen-Wei Fang is with the Cloud Computing and Intelligent System Lab., Dept. of CSIE, National Formosa University, Taiwan

Hua-Yu Wu is with the Cloud Computing and Intelligent System Lab., Dept. of CSIE, National Formosa University, Taiwan

Wen-Hsiang Hsieh is with the Cloud Computing and Intelligent System Lab., Dept. of CSIE, National Formosa University, Taiwan

I. INTRODUCTION

DUE to the online community or social media, various information can be exchanged quickly. Without verification, all the information broadcasted between people may be under misrepresentation [1]. Considering the anonymous using or none-recognition social media user, false news or fictitious information could be made for specific purpose. The false news could spread faster than the true story or clarification news. Although most news can be searched and verified through the search engine such as Google [2], Yahoo [3], etc., to find the correct information from various sources and various news is still difficult.

There were different methods proposed to detect the false news based on the supervision [4]. To find and detect the false new, the content of the news could be the important factor [5]. In addition, to take the background or profiles of the user into consider could be also the solution for false news finding [6]. Based on the crowd-sourcing approach, the false news could be verified according to the public annotations or replies. However, when the false news are intentionally given or spread, public news readers may not differentiate true or false news [7]. Furthermore, if the false news is written maliciously, it's more difficult to classify the news due to some organizations or groups would intentionally spread the false news.

In addition, some languages would make the verification of news more difficult. For example, the possible combination of Chinese vocabularies would make the meanings completely different [11]. Currently, by using the specific keywords, the search engines would find the possible information for verification according to the statics of keywords. Hence, considering the probability of the keywords included in the found information or web pages, different keywords could be combined as the new potential vocabularies [8-10]. In other words, by adaptively combining the key words, the features of the news can be described and defined.

Considering the rapidly changing of the online news and information spread through the online media or social community, the feature keywords or vocabularies are changed quickly. Furthermore, the content of false news

could be various and huge. To continuously collect the data from social media is needed. In addition, to manage big data from the online media is also required. Corresponding to the big data management, the Hadoop/MapReduce[10,15,19,20] and Spark were proposed [25]. All the vocabularies are treated as the key. Then, the total among of the keys (vocabularies) appeared in the article or web page can be evaluated and counted as the value. Hence, each online article or news can be represented as (key, value) corresponding to all the vocabularies appeared.

According to the proposed research, by adaptively combining the found vocabularies, the feature of the similar online information can be found [10]. However, different false news would be various in different content. Some false news may appear only few hours, some may cause several days spreading with huge data. Therefore, to collect the huge data online for feature of the intentionally spread false news is an important issue.

In this research, the first step is to collect the proved false news from the third party impartial agency. To collect the verified data or information, the automatic data collection based on the online crawler is needed. Corresponding to the vocabulary combination procedure, the suitable length of keywords for the same false news could be found. In other words, the suitable features of the same feature can be found. By comparing different types of false news and the evaluation based on the dynamic multiple dimension K-mean algorithm, the features or groups which intentionally spread the false news could be found.

This paper is presented as follows. Section 2 gives the related works. Then, the proposed procedure for news credibility and reliability prediction is given in section 3. Section 4 provides the conclusion.

II. Related Works

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

These days, dur to the online media including video streaming, social media, or online forum, people could receive various information more quickly. However, some intentional false news would cause damage from the health to the vote. Some research were proposed to differentiate the true and false news. In addition, corresponding to the various languages, the complete vocabulary in the sentence or article should be taken into consideration [10]. There were procedures proposed based on the language corpus [9,11,12]. According to the vocabularies stored in the corpus, the various vocabularies could be identified and recorded as the text-pattern. However, the information or new vocabulary comes every day. To automatically collect the information online is important.

Hence, in this research, the web crawler [13,14,20] is used to collect the online information included in the web pages. Based on the web crawler, the application could continuously collect the data from the Internet. From different search engines or web pages, the information or potential news can be gathered.

After obtaining the data from the Internet by crawler, the data or vocabularies should be evaluated. Since the total amount of the collected data could be huge, to parallel process the big data based on the distributed system is needed. Hadoop/MapReduc was the data analysis application proposed by Apache or Google [10,15,19,20]. Since the data size from the Internet could be huge, the Hadoop Distributed File System or Google File System was proposed for dividing the huge data into blocks and distributed storing [16-19]. All the corresponding information about data storage can be managed based on the HBase, the database based on the cloud environment. The HBase is the noSQL type database. Hence, the length of each data can be various instead of the traditional fixed data length in database. In other words, although the size of information or data from different network sources could be different, the HBase on cloud could still provide the storage space and record it with better performance.

Suppose that to analyze the complete collected data is called Job. Then, the data will be divided into several partitions for parallel processing, called Tasks. Each job could be divided into multiple tasks. These tasks are mapped to multiple computing nodes or virtual machines [26]. After the computing and evaluation, each report of the task from the computing node could be sent back and summarized. Based on the Hadoop/MapReduce, each found vocabulary from the collected information or data will be represented as 'key'. The total amount of occurrences corresponding to this 'key' vocabulary can be counted and represented as the 'value'. In other words, the report related to the data after analysis could be represented as the set: {key, value}. Finally, according to the reduce procedure, the value with the same key will be added up. At last, only one report corresponding to each information collected from Internet could be given.

Since the content of the co0llected information from the Internet could be various, the data size after analysis would be different and huge. In addition, to execute the Hadoop/MapReduce program also requires huge computing resource. Hence, considering the computing ability, the cloud computing environment is needed. Via network connection and virtualization technology, the virtualized computing resource such as CPU, memory, and storage space, could be merged into the computing resource pool. When a user needs the computing resource, the computing resource in the resource pool can be integrated as the virtual machine for the user. If no more using the virtual machine, the computing resource can be returned to the resource pool for further using. Therefore, the computing resource for services such as IaaS, PaaS, and SaaS, can be rapidly used [27]. In other words, if the configuration and environment of the virtual machine is on demand defined, the user could obtain the cloud services such as SaaS more directly and quickly. Therefore, the cloud computing could be the solution to repeatedly and continuously analyze the information gathered from the Internet.

After analysis related to the collected information, the feature of the content should be found. In addition, there are various news, information, and data from Internet. The features between different information or data could be different. Therefore, to group the similar information or data from these collected data is important. Then, the possible features of this grouped data such as the false news makers or spreaders could be found. To find the possible relationship

between different data, the clustering algorithms based on K-means were proposed. According to the group analysis with vector quantization, different groups with different features could be found and divided by the following equation:

$$J = \sum_{i=1}^{k} \sum_{x_j \in S_t} (x_j - \mu_i)^2 \quad (1)$$

Suppose that there are total k randomly selected group centres from μ_1 to μ_k . The all found features x are measured the distance between x and group centres. Finally, all the x which is included in the group S_i with the shortest distance between x and μ_i are called members of group i. In other words, when the minimized J is found, all the x could be individually classified to its nearest group with the centre μ.

III. Proposed System

In this research, to continuously collect the proved news, especially proved false news, is very important for training the proposed system. Therefore, some specific online websites or news proof data sources are on demand recorded in the proposed web crawler procedure which is based on the HTTP protocol [20,21]. By using the selenium [22], Google search Engine [2], or Taiwan FactCheck Center [28], the corresponding news (proved false news) could be collected. Then, the false news spread through the websites, social media, forum, etc., could be further collected. In other words, the false spreading paths, media, content, etc., can be searched and found.

The false news studied in this research is spreading in Chinese language. Due to the characteristics of the Chinese, the vocabularies in the content should be divided according to the ambiguity resolution rules such as Maximum Matching [23] (mmsegj). Each chunk which includes the neighbour vocabularies would follow the rules: largest average and smallest variance of word length, largest degree of the summation related to morphemic freedom corresponding to the one-character word, and maximum matching [24]. Therefore, each independent data or information from web page or social media could be divided into multiple key vocabularies.

However, to find the key vocabularies, the huge data from the Internet should be managed. Hence, in this research, the Hadoop/MapReduce procedure is implemented based on the cloud environment. By looped mmsegj and Hadoop/MapReduce procedures, the largest average length of key vocabularies could be found. However, considering the intentionally spread false news today, new vocabularies, names, or new homophonic or metaphor vocabularies would appear. Therefore, in this research, the Key Vocabularies Merging method is proposed. By sorting, grouping and combining different found vocabularies according to the on demand defined limitations and considerations, the key vocabularies could be deeply searched through the verification via search engines. The flowchart can be shown as follows.

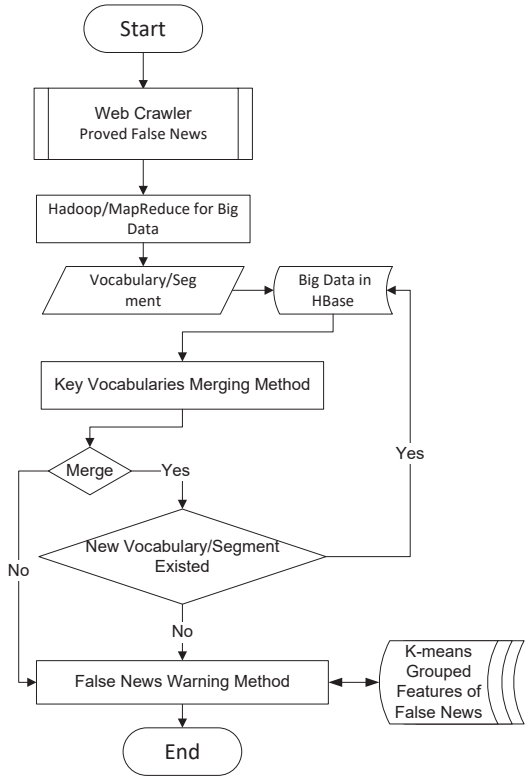


Fig. 1. The flowchart of the proved false news system training.

In this research, the proved false news in Chinese language could be collected from Taiwan FactCheck Center [28]. Since the news was already proved as the false news, the corresponding data or information could be the training data of the proposed system. According to the mmsegj and Hadoop/MapReduce procedures, the largest average length of vocabularies or frequently appeared specific vocabularies could be found and sorted. Then, the clustered and found vocabularies should be proved and verified as the features of the specific false news. In this research, the similar content of the proved false news from different news sources could be collected and analysed together. Therefore, these similar intentionally spread false news could be used to train the proposed system and cluster the possible features of the collected false news. To find the available and possible features of the similar false news, the Key Vocabularies Merging Method is proposed.

A. Key Vocabularies Merging Method

In this research, the Key Vocabularies Merging Method is proposed for extending the found key vocabularies. Based on the mmsegj algorithm for Chinese vocabulary recognition, the basic segments or simple vocabularies can be found. Considering the intentionally spread false news, the feature vocabularies may be combined from various found vocabularies. For example, the vocabulary could be combined from the name, location, food, even foreign language. Hence, in this research, the Key Vocabularies Merging Method is proposed for further extended key vocabulary searching.

After analysing the similar proved false news, the initial key vocabularies which represented and sorted according to value of the set, {key, value}, can be obtained. Then, suppose that there are total v found initial vocabularies or segments according to the mmsegj algorithm. The occurrences of the i^{th}

vocabulary which represented as v_i can be shown as $O_c(v_i)$ = value. Hence, the Key Vocabularies Merging could evaluate and decide to merge two vocabularies by following the decision function based on difference percentage shown as follows:

$$\text{Merge} = \begin{cases} \text{true} & \frac{|O_c(v_i) - O_c(v_j)|}{O_c(v_i)} \leq \alpha \\ \text{false} & \text{otherwise} \end{cases} \quad (2)$$

where $i \neq j$ and α is the on demand given value. If the result of the merge evaluation is true, the i^{th} vocabulary and the j^{th} vocabulary will be merged as the new vocabulary.

If there are new vocabulary or segment merged according to the proposed decision function, these new merged vocabulary or segment should be verified by the following two checking steps. First step, these new vocabulary will be tested through the search engines online including different language vocabulary checking. If the new merged vocabulary is existed in the general articles, then this new merged vocabulary should occur frequently. Second step, the new merged vocabulary should also occur in the all original proved similar false news. In other words, the occurrence of the new merged vocabulary should be satisfied the function shown as follows:

$$O_c(v_i) \geq O_c(\text{new merged vocabulary}) \geq O_c(v_j) \quad (3)$$

where the $O_c(v_i) \geq O_c(v_j)$. If these two steps can be satisfied, this new merged vocabulary or segment can be recorded. To find the longest feature vocabulary or segment, the found merged vocabulary and segment will be checked according to the proposed Key Vocabularies Merging Method again. When no new merged vocabulary can satisfy the two checking steps, the Key Vocabularies Merging Method stops.

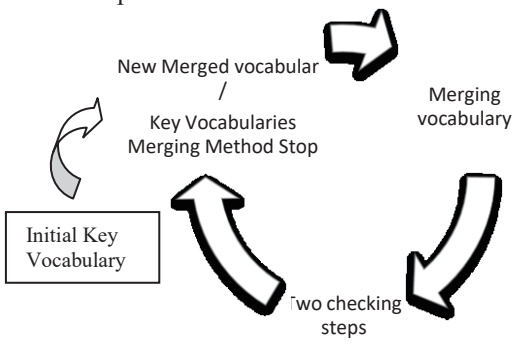


Fig. 2. The cycle of the proposed Key Vocabularies Merging Method.

Therefore, based on the proposed Key Vocabularies Merging Method, the key vocabulary can be extended. Suppose that the false news intentionally broadcasted would be written corresponding to the specific person, specific fake news or sentences, specific organizations, etc. Then, the probabilities of individual word or vocabularies should be very closer to another frequently appearing word or vocabulary. For example, the personal name "韓國瑜" in Chinese could be divided as two vocabularies: "韓國" and "瑜". The first vocabulary is the proper nouns. However, initially the complete personal name is not defined as the proper nouns in the database. Therefore, after several cycles of the proposed Key Vocabularies Merging Method, these two independent vocabularies, "韓國" and "瑜", could be found that the probability of appearance corresponding to these two vocabularies are almost the same since originally it is a personal name. According to Key Vocabularies Merging Method, the key vocabulary "韓國" can be extended with another key vocabulary "瑜" as "韓國瑜". Especially, according to two checking steps of Key Vocabularies Merging Method, the new found key vocabulary can be proved as the new merged and useful key vocabulary as the feature of the false news. In addition, the new merged key vocabulary can be recorded into the Chinese proper nouns database.

Since it is difficult to find the new potential vocabularies excluding in the database, in this research, additional method: jieba algorithm, is used for extending the vocabularies. Jieba algorithm is used to find the possible and potential vocabulary segmentation of Chinese language [29].

Jieba algorithm is the method to find the vocabulary segmentation in Chinese [29]. In this research, to find the possible segment of Chinese words, two possible methods are used: 1) Rule Segmentation and 2) Statistical Segmentation.

Based on jieba algorithm, a vocabulary dictionary tree would be used for words comparing and matching by rule segmentation. In other words, if the segments are already recorded in the dictionary, the results of matching could identify the found segments. Considering the vocabularies used in the social community media, new created words are frequently appeared. It means that only matching the vocabulary tree by rule segmentation is not enough. Therefore, the Statistical Segmentation is also included for the new vocabularies or segments finding. By counting the appearance frequency of the potential new vocabularies, the potential new created vocabularies could be found due to the frequent using in the text content from various sources. In other words, with the statistical results, the high frequently appeared words could be identified and recognized as the new vocabulary. The new created new vocabulary will be recorded into the database for matching by Rule Segmentation in the future. Hence, the new created vocabularies used in the fake news or social media could be found and extended more automatically. In this research, the MapReduce for evaluating the various key segments is used. Since the fake news spread today would include the personal names or some homophonic vocabularies created by social media, the found potential new vocabularies would be various with huge amount. Therefore, to evaluate and obtain the statistical results of different text content from various sources would request huge computing resource. In this research, by following the MapReduce procedure, the statistical results could be obtained through counting the {Key, Value} format which Key is the potential vocabulary and the Value indicate the appearance times.

In addition to the Statistical Segmentation, the directed acyclic graph is used to structure the possible vocabularies according to the word graph scanning based on the prefix dictionary. The maximum probability of the dynamic programming path could be found. By using the Hidden Markov Models (HMM), the words excluded in the dictionary database could be learned and found. Hence, even the new words or vocabularies are created according to the pronounce or other non-traditional grammar method, the statistical results of the similar content from various news sources could still be used to identify and recognize the new

feature vocabularies.

After recursively processing the proposed Key Vocabularies Merging Method and the jieba algorithm with Hidden Markov Models (HMM), the hidden vocabularies and txt segmentations could be found and identified. The possible feature key vocabularies could be merged and extended by different segments.

B. Clustering Method

After finding the vocabularies and counting the appearance of each vocabulary, the features of the specific fake news should be found and defined. Since the similar fake news would have similar key vocabularies, these vocabularies could be used to cluster or group the fake news. In this research, term frequency-inverse document frequency (TF-IDF) method is used. Term frequency-inverse document frequency is a statistical method for information exploration and text mining through the weighting techniques [30,31]. Each found vocabulary will be evaluated for its importance of the text content or corpus. Suppose that the term frequency (TF) of the key vocabulary is high if this specific vocabulary is important in the fake news. In other words, if the words are not important in these fake news, the appearance frequency of the words is decrease in inverse proportion called inverse document frequency (IDF).

Due to the term frequency-inverse document frequency method, the important vocabularies could be filtered with less common words. In other words, after filtering multiple similar fake news, the specific key vocabularies could be possibly found since these specific key vocabularies would be important in the same or similar fake news. In other words, the similar fake news would include the similar specific key vocabularies. In this research, these similar or the same specific key vocabularies are called features of the specific fake news. Suppose that the features of different fake news related to various topics would be also different. Then, after term frequency-inverse document frequency method, the fake news with the similar key vocabularies or features should be grouped or clustered as the same topic or purpose of the fake news. In this research, the Scikit-learn [32,33] is used for enhance the accuracy of classification and clustering. Scikit-learn is the machine learning method which uses Numpy to efficiently perform the linear algebra and array operations. Scikit-learn provides various classification, regression and clustering algorithms, such as support vector machine, gradient boosting, term frequency-inverse document frequency, k-means clustering, DBSCAN, etc. In this research, the value k for the k-means clustering in eq. (1) should be assigned and given. To find the suitable value k, the Elbow Method [34] is used. Based on Elbow Method, the elbow point is used to find the minimized value of k which to be used for k-means algorithm. Hence, by recursively executing the Scikit-learn method and Elbow Method, the fake news which were already verified could be clustered and grouped automatically with less manual operation according to the found k. In other words, the when the value k is defined, the total numbers or the fake news groups or clusters is also defined. In addition, when the numbers or the fake news groups is defined, the key vocabularies related to each groups could be called as the features of the specific fake news group. In other words, after Scikit-learn method and Elbow Method, the groups and the corresponding features are defined and found.

C. False News Warning Method

After Key Vocabularies Merging Method, the features of the proved similar false news can be found. By analysing various types of the proved false news, different features related to these various false news could be obtained. Therefore, based on the K-means algorithm, the intentional false news even the news sources can be grouped. After K-means grouping, the possible types of false news and possible spreading news sources could be found.

Therefore, based on the classification of the various intentional false news groups, the features of each group could be collected. In other words, these features could be used to represent or indicate the similar false news. Finally, through comparing and matching the features, the new news can be analysed and predicted.

Suppose that there are total f_g features of the g^{th} false news group. In addition, by K-means algorithm, the new news would be classified and grouped to the g^{th} false news group. Then, comparing the found features of the new coming news, there would be f_n features of the new news that included or the same in the g^{th} false news group. Therefore, in this research, the new news could be evaluated as the possible intentional false news by following function:

$$\text{False News Warning} = \begin{cases} \text{true} & \frac{f_n}{f_g} \times 100\% \geq \beta \\ \text{false} & \text{otherwise} \end{cases} \quad (4)$$

where the β is the on demand given value for the intentional false news warning.

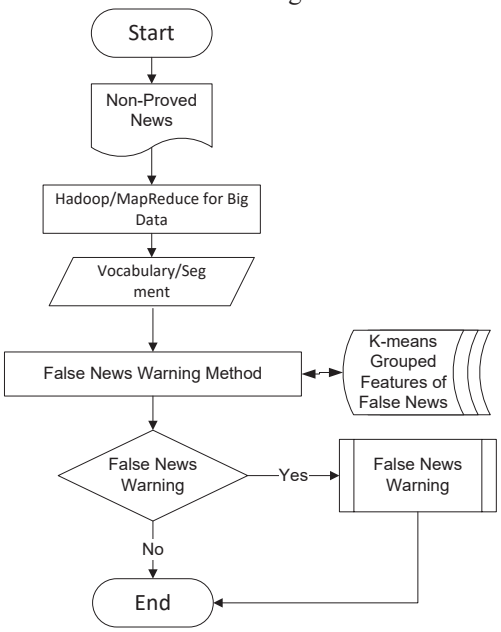


Fig. 3. The flowchart of the false news warning.

IV. Verification and Results

Following is the implementation example. Based on mmsegj algorithm for Chinese vocabulary recognition, the Chinese vocabularies presented in the website or web page could be separated and recognized as Figure 4. According to the {key, value} structure, the initially found key vocabularies and the corresponding appearance probability are checked. Some proper nouns are already recognized.

However, many key vocabularies are recognized as the single Chinese word. Based on the proposed Key Vocabularies Merging Method, the two vocabularies could be merged according to equation 1. In figure 4, for example, the appearance probabilities of "西" and "坑" are almost the same. According to equation 1, these two vocabularies could be merged as "西坑" or "坑西". However, after next cycle of the Key Vocabularies Merging Method, due to that the "西坑" is the independent proper nouns, and "坑西" is not the independent proper nouns, the appearance probability differences between "西坑" and "坑西" will be very huge. In other words, only the "西坑" can be reserved and survived for the further feature searching.

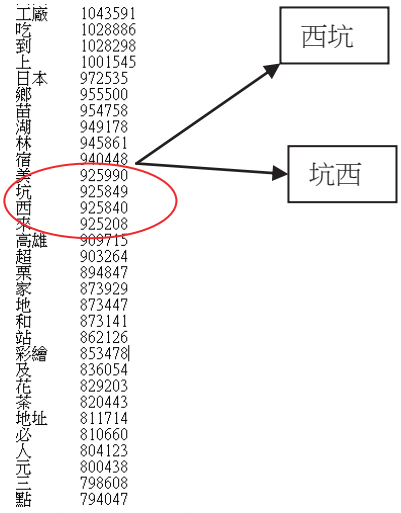


Fig. 4. The example of the implemented Key Vocabularies Merging Method.

In this research, to cluster and group the fake news which are collected by the web crawler, the scikit-learn for and the jieba algorithm are connected by the python program. The collected fake news and the related features are stored in the noSQL database on cloud. To provide the visual presentation and interface, the python matplotlib is also used. In the beginning, the specific topics of news from the Taiwan Fact Check Center are all already proved and recognized as the fake news. According to this recognized topic, the normal search engines such as Google or Yahoo are used to collect the similar news. Based on the proposed Key Vocabularies Merging Method, jieba algorithm, and term frequency-inverse document frequency (TF-IDF) method, the total found feature vocabularies or segmentations are various and huge. To cluster and group the collected fake news which are corresponding to the fake news proved by Taiwan Fact Check Center, the K-means algorithm integrated with the Elbow methods is recursively executed. According to Elbow Method, elbow point could be found around 4 with less differences of summation of squared distance when the value k is increased. The result is shown as Figure 5.

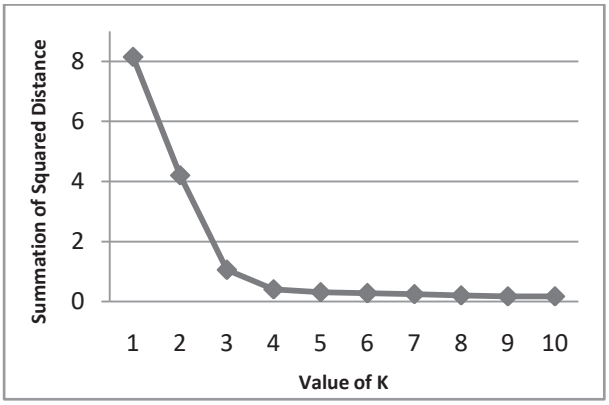


Fig. 5. The found value K based on Elbow Method according to the corresponding squared distance.

In the beginning of the verification, there are four different topics of fake news from the Taiwan Fact Check Center are collected. Since according to the proposed methods the final groups could be clustered into correct 4 groups, the related news from the search engine could be also recognized and clustered. In this research, there are total 34 fake news from various sources corresponding to the four main fake news topics are collected as the data for verifying the classification. There are 9 fake news are proved similar or the same as fake news group 1; 10 fake news are proved similar or the same as fake news group 2; 9 fake news are proved similar or the same as fake news group 3; and 6 fake news are proved similar or the same as fake news group 4. To verify the proposed system, these all 34 fake news are initially given without grouping and definitions. The proposed system receives these fake news without understanding the numbers of topics and the numbers of fake news in each fake news groups.

After the recursively processing the proposed Key Vocabularies Merging Method, jieba algorithm, and term frequency-inverse document frequency (TF-IDF) method with Elbow Method, the related fake news could be clustered into the same group by evaluation the square distance between each fake news and the group center. In addition, due to the Elbow Method, the minimum numbers of the groups could be also decided according to the obtained square distance. Finally, the related fake news could be correctly clustered into the corresponding groups. Figure 6 presents the average distance between each fake news group and the different group centers. The average distance of the 9 fake news which clustered into the fake news group 1 is only about 0.1 square distance from the cluster center 1 but more than 0.4 square distance to any other cluster centers. The average distance of the 10 fake news which clustered into the fake news group 2 is only about 0.1 square distance from the cluster center 2 but more than 0.6 square distance to any other cluster centers. The average distance of the 9 fake news which clustered into the fake news group 3 is only about 0.13 square distance from the cluster center 3 but more than 0.58 square distance to any other cluster centers. The average distance of the 6 fake news which clustered into the fake news group 4 is only about 0.05 square distance from the cluster center 4 but more than 0.47 square distance to any other cluster centers. In other words, the proposed algorithm and processes could really recognize and cluster the fake news correctly.

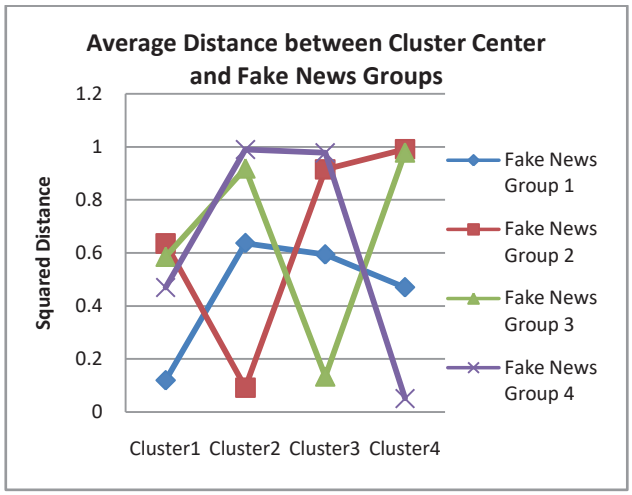


Fig. 6. The average square distance between the fake news and the cluster center.

Therefore, according to the proposed Key Vocabularies Merging Method, jieba algorithm, term frequency-inverse document frequency (TF-IDF) method with Elbow Method, the trained fake news data could be correctly recognized. Considering the purposes of the malicious organizations or users, the fake news would be frequently announced or created related to some specific person or topics. In other words, the rapidly announced fake news from the same organizations or groups could be recognized and found.

V. Discussion

Although according to the proposed system the proved fake news could be recognized and clustered, to predict the new coming news is still difficult. First, the proposed system can recognized and cluster the existed and proved fake news. Based on the collected huge amount of the proved fake news, the recognition and clustering could be correct. However, the accuracy of the prediction should depend on huge data found from the Internet. It means that the prediction is difficult when there is only a few data collected from the Internet. In addition, since the new coming news is not identified and verified, the proposed system could only differentiate this news according to the related information collected and announced in the past. In other words, if the most of the news disseminated by the social media or organization is true news, then according to the proposed system the new coming news would be easily recognized as true news. In opposition, if most of the news disseminated by the social media or organization is fake news, the new coming news would be identified and clustered as fake news even it is really true. The found features would result in the bias when cluster and recognize the news from specific media or group. In other words, the history of the media or organization itself would affect the prediction result. The media or group with more proved fake news in the past would be easily recognized and clustered as the fake news in the future.

Second, due to the verification and the proof of each news, some information or messages hidden in the news would need time for searching and finding. Some inside information could be only be proved and recognized after long time. Therefore, to prove the news true or fake itself is an difficult issue. In addition, only more information found then the current news could be identified as the true or fake news in the future. Therefore, to directly verify and recognize a news is true or fake is not easy especially when the related information is not enough. Finally, the credibility of the media or organization still plays the main and important role.

However, due to some political purposes, the fake news would be created and broadcasted by specific malicious media organization and groups. These malicious parties would actively spread the fake news. According to the proposed system, these groups, individual person, even media organization could be found and evaluated. In the future, some more tags could be found and defined for these malicious fake news spreaders. In other words, the credibility of these malicious fake news spreaders could be evaluated and given the warning according to the new spreading history.

VI. Conclusion

In this research, the proposed Key Vocabularies Merging Method could find the features of the specific intentional false news. Based on the term frequency-inverse document frequency (TF-IDF) method with Elbow Method, the proved false news or fake news could be correctly clustered into the corresponding groups. In addition, the numbers of the groups related to the false news could be automatically increased. In other words, according to the analysis of the historic proved news, the repeatedly found news could be recognized and verified.

Based on the proposed False News Warning Method, different intentional false news could be grouped. According to the comparing with the various groups of the intentional false news, the false news warning could be given corresponding to the new news.

Acknowledgment

Thanks for the support of Cloud Computing and Intelligent System Lad. (CCIS Lab.) of National Formosa University.

References

[1] Soroush Vosoughi, Deb Roy, Sinan Aral, " The spread of true and false news online," *Science*, Vol. 359, Issue 6380, pp. 1146-1151, 2018. DOI: 10.1126/science.aap9559

[2] http://www.google.com

[3] http://tw.yahoo.com

[4] S. Yang, K. Shu, S. Wang, R. Gu, F. Wu, and H. Liu. "Unsupervised fake news detection on social media: A generative approach." *Proc. of 33rd AAAI Conference on Artificial Intelligence*, 2019. DOI: https://doi.org/10.1609/aaai.v33i01.33015644

[5] W. Y Wang, " liar, liar pants on fire": A new benchmark dataset for fake news detection. *arXiv* preprint arXiv:1705.00648. 2017.

[6] C. Castillo, M. Mendoza, B. Poblete, "Information credibility on twitter." *In Proc. of the 20th international conference on World wide web*, 675–684. ACM, 2011.

[7] C. F. Bond Jr, B. M. DePaulo, "Accuracy of deception judgments." *Personality and social psychology Review* 10(3) pp.214–234, 2006.

[8] J. Kim, B. Tabibian, A. Oh, B.S cholkopf, M. Gomez Rodriguez, "Leveraging the crowd to detect and reduce the spread of fake news and misinformation." *In Proc. of the 11th ACM International Conference on Web Search and Data Mining*, pp.324–332. ACM 2018.

[9] K.J. Chen & Ming-Hong Bai, "Unknown Word Detection for Chinese by a Corpus-based Learning Method," *International Journal of Computational linguistics and Chinese Language Processing*, 1998, Vol.3, No.1, pages 27-44

[10] Ming-Shen Jian, Wei-Cheng Hong, Sheng-Che Tsai, Yu-Wei Chen, Chih-Ling Fan "Based on Automatic Correlation Keyword Grouping and Combination Based Deep Information Search Corresponding to Specific Language Big Data -- Case of Leisure Recreation " *ICACT*, pp.372-377, Feb. 2020.

[11] Wei-Yun Ma & K.J. Chen, "A bottom-up Merging Algorithm for Chinese Unknown Word Extraction," *Proc. of ACL workshop on Chinese Language Processing*, pages 31-38, 2003.

[12] http://120.108.221.55/profchwu/ml/%E6%95%99%E6%9D%90/%E6%96%87%E4%BB%B6%E5%88%86%E9%A1%9E/%E4%B8%AD%E7%A0%94%E9%99%A2%E8%A9%9E%E6%80%A7%E5%AE%9A%E7%BE%A9.pdf

[13] Chandni Saini, Vinay Arora, "Information retrieval in web crawling: A survey," *International Conference on Advances in Computing, Communications and Informatics* (ICACCI), 2016.

[14] M. S. Jian, et al, "Cloud Based Agriculture Safety Inspection with Multiple Standard Sources," *Proc. of IEEE ICACT*, pp. 201-206, Feb. 2018.

[15] Yu-Chen Wang, "The Structure of the Big Data Based on the Hadoop Platform", *thesis*, National Chi Nan University, Taiwan, 2015.

[16] Zhi-Kai Liao, "Fault-Tolerant Management Framework for Hadoop Distributed File System", *thesis*, Tamkang University, Xinbei, Taiwan, 2013.

[17] Jia-Chun Lin, "Study of Job Execution Performance, Reliability, Energy Consumption, and Fault Tolerance in the MapReduce Framework", *thesis*, National Chiao Tung University, Hsinchu, Taiwan, 2015.

[18] Man-Ning Wu, "Data Analysis Results Storge Design in HBase, Chung Yuan Christian University", *thesis*, Taoyuan, Taiwan, 2015.

[19] Hadoop – Introduction, Available online : https://www.tutorialspoint.com/hadoop/hadoop_introduction.htm

[20] Ming-Shen Jian, Yi-Chi Fang , Yu-Kai Wang, Chih Cheng, " Big Data Analysis in Hotel Customer Response and Evaluation based on Cloud," *Proc. of IEEE ICACT*, pp.791-795, Feb. 2017.

[21] Fredrik Erlandsson, Roozbeh Nia, Martin Boldt, Henric Johnson, S. Felix Wu, " Crawling Online Social Networks," *Proc. of 2015 2nd ENIC*, pp.9-16, Sept. 2015

[22] https://www.seleniumhq.org/

[23] Chih-Hao Tsai, "MMSEG: A Word Identification System for Mandarin Chinese Text Based on Two Variants of the Maximum Matching Algorithm," http://technology.chtsai.org/mmseg/

[24] https://www.itread01.com/articles/1476609057.html

[25] https://spark.apache.org/

[26] Ming-Shen Jian, Ming-Sian You, "Cloud Based Hybrid Evolution Algorithm for NP-Complete Pattern in Nurse Scheduling Problem," *International Journal of Innovation, Management and Technology*, Vol. 7, No. 5, pp.234-237, 2016

[27] Ming-Shen Jian, "*Intelligent System Based on Cloud and IOT*," Mar. 2019, EHGBooks Publishing, (ISBN: 978-1-62503-503-5)

[28] https://tfc-taiwan.org.tw/articles/report

[29] Zhang, X.; Wu, P.; Cai, J.; Wang, K. A Contrastive Study of Chinese Text Segmentation Tools in Marketing Notification Texts. *Journal of Physics: Conference Series.* Vol. 1302, No.2, 2010. doi: 10.1088/1742-6596/1302/2/022010

[30] Hakim, A. A.; Erwin, A.; Eng, K. I.; Galinium, M.; Muliady, W. Automated document classification for news article in Bahasa Indonesia based on term frequency inverse document frequency (TF-IDF) approach. *2014 6th International Conference on Information Technology and Electrical Engineering (ICITEE)*. pp.1-4, 2014. doi: 10.1109/ICITEED.2014.7007894.

[31] Havrlant, L.; Kreinovich, V. A Simple Probabilistic Explanation of Term Frequency-Inverse Document Frequency (tf-idf) Heuristic (and Variations Motivated by This Explanation). *International Journal of General Systems*. Vol. 46, No.1, pp.27-36, 2017. doi: 10.1080/03081079.2017.1291635

[32] Hishamuddin, M. N. F.; Hassan, M. F.; Tran, D. C.; Mokhtar, A. A. Improving Classification Accuracy of Scikit-learn Classifiers with Discrete Fuzzy Interval Values. *2020 International Conference on Computational Intelligence (ICCI)*, pp.163-166, 2020. doi: 10.1109/ICCI51257.2020.9247696.

[33] Brites, D. and Wei, M. PhishFry - A Proactive Approach to Classify Phishing Sites Using SCIKIT Learn. *2019 IEEE Globecom Workshops (GC Wkshps)*, pp.1-6, 2019. doi: 10.1109/GCWkshps45667.2019.9024428.

[34] Syakur, M. A.; Khotimah, B. K.; Rochman, E. M. S.; Satoto, B. D. Integration K-Means Clustering Method and Elbow Method For Identification of The Best Customer Profile Cluster. 2018 *IOP Conf. Ser.: Mater. Sci. Eng.* 336, 2017.

Ming-Shen Jian was born in Kaohsiung City, Taiwan in 1978. He received the B.S. from the National Chiao Tung University, HsinChu, and Ph.D degrees in Computer Science and Engineering from the National Sun Yat-sen University, Kaohsiung, Taiwan in 2007.
From 2018, he was an Associate Professor and director with the National Formosa University Cloud Computing and Intelligent System Laboratory. Currently he is also an IEEE Senior Member. Since 2009, he has been an Assistant Professor with the Computer Science and Information Engineering Department, National Formosa University. He is the author of four books, more than 50 articles, and at least 15 invention patents. His research interests include IOT development and application, Big Data, Optimal Solution, Intelligent System, and Cloud Computing. He was a Secretary of the Taiwan Association of Cloud Computing. Dr. Jian was a recipient of the IEEE sponsored international conference Paper Award in 2016, 2017, and 2018.

Rong-Bin Deng was born in 2000, Taiwan. Currently he is an B.S. degree student of Dept. Computer Science and Information Engineering at National Formosa University. His current research interests are in the area related to Web Service, and Cloud Computing. He joins the Cloud Computing and Intelligent System Lad. (CCIS Lab.) from 2019.

Chen-Wei Fang was born in 1999, Taiwan. Currently he is an B.S. degree student of Dept. Computer Science and Information Engineering at National Formosa University. His current research interests are in the area related to IoT, and Cloud Computing. He joins the Cloud Computing and Intelligent System Lad. (CCIS Lab.) from 2019.

Hua-Yu Wu was born in 1999, Taiwan. Currently he is an B.S. degree student of Dept. Computer Science and Information Engineering at National Formosa University. His current research interests are in the area related to Big Data, and Cloud Computing. He joins the Cloud Computing and Intelligent System Lad. (CCIS Lab.) from 2019.

Wen-Hsiang Hsieh was born in 2000, Taiwan. Currently he is an B.S. degree student of Dept. Computer Science and Information Engineering at National Formosa University. His current research interests are in the area related to Web Service, and Cloud Computing. He joins the Cloud Computing and Intelligent System Lad. (CCIS Lab.) from 2019.

A Novel Fully Distributed EPON-Based 5G RAN Architecture Modeling with Handover Analysis

Syed R. Zaidi*, Ajaz Sana*, and Shahab Hussain**
*Dept. of Engineering, Physics & Technology, Bronx Community College of the City University of New York, USA
** Mobile Networks Department, Nokia Corporation, 1 Robbins Rd., Westford, MA 01886, USA
syed.zaidi@bcc.cuny.edu, ajaz.sana@bcc.cuny.edu , shahab.hussain@nokia.com

***Abstract*— Traditional mobile backhaul Radio Access Network (RAN) employ centralized data and control plane scheme. In this work, we propose a novel Passive Optical Network (PON) based next-generation mobile backhaul RAN architecture in a distributed scheme that enables the redistribution of some of the intelligence currently centralized in the Mobile Packet Core (MPC) platform out into the access nodes of the RAN. Specifically, this work proposes a fully distributed ring-based EPON architecture that enables the support of a converged PON-5G option 3X access networking transport infrastructure to seamlessly backhaul both mobile and wireline multimedia traffic and services. Performance analysis show that the proposed distributed architecture show better results in throughput, latency and handover analysis.**

Keywords- 5G, EPON, LTE, Option 3x, PON, TDM

I. INTRODUCTION

THE only viable solution to support extraordinary growth of mobile backhaul to provision the emerging 5G traffic that includes 5G and cellular Long-Term Evolution (LTE), requires rapid migration from today's legacy circuit-switched T1/E1 wireline and microwave backhaul technologies to a new fiber-supported, all-packet-based mobile backhaul infrastructure [1-4]. Mobile backhaul sometimes referred to, as the Radio Access Network (RAN), is used to backhaul traffic from individual base stations (BSs) to the Core Network (CN). In contrast with the typically centralized 2G/3G RAN infrastructure, the 5G architecture specifically 5G option 3x has fundamentally different RAN design requirements.

Manuscript received Jan 20, 2021. This work is a follow-up of the invited journal to the accepted paper entitled "An efficient & Cost-Effective EPON-Based Next Generation 5G Mobile Backhaul RAN Architecture" of the 23rd International Conference on Advanced Communication Technology (ICACT2021).

Syed Rashid Zaidi, he is an assistant professor at the Bronx Community College of the City University of New York, USA. (corresponding author, phone:+1-718-289-5100; fax:+1-718-289-6403; e-mail:syed.zaidi@ bcc.cuny.edu).

Ajaz Sana, he is assistant professor at the Bronx Community College of the City University of New York, USA. (e-mail: ajaz.sana@ bcc.cuny.edu).

Shahab Hussain, he is a senior professional at the Nokia Corporation, USA. (e-mail: shahab.hussain@ nokia.com).

Hence, a cost-effective fiber supported all-packet-based mobile backhaul RAN architecture that is compatible with these inherently distributed and packet-oriented NG RAN architectures, is needed to efficiently scale current mobile backhaul networks. However, deploying a new fiber-based mobile backhaul infrastructure is a costly proposition mainly due to the significant cost associated with digging the trenches in which the fiber is to be laid.

The 5G System can use non-standalone solution with dual connectivity to 4G. That approach is called Option 3. As shown in Fig. 1. 5G can be deployed as a standalone solution without LTE.

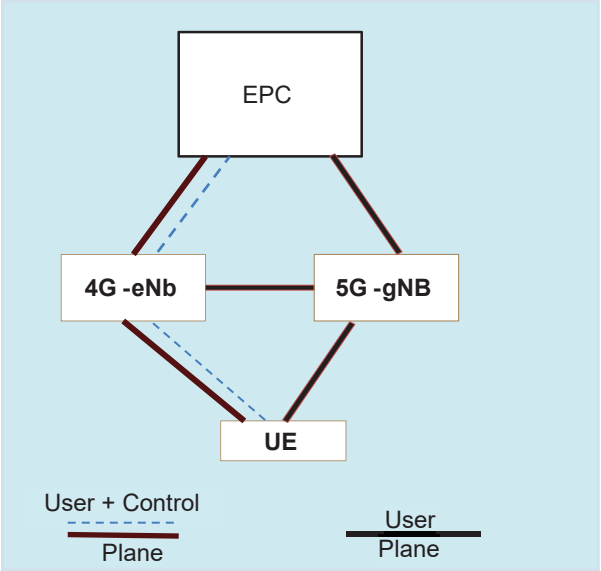


Fig. 1. 5G Option 3x

This approach is called Option 2 in 3GPP. The very first 5G networks must use Option 3 because it is available in 3GPP 6 months before Option 2. Dual connectivity has also other benefits. It allows to combine 4G and 5G data rates together and it allows to reuse existing Evolved Packet Core (EPC). Option 3 is a dual connectivity deployment with E-UTRA as the anchor Radio Access Technology (RAT) and

NR as the secondary RAT in a non-standalone configuration based on the existing EPC. Both 5G base stations (gNodeB) and 4G base stations (eNodeB) are connected to the EPC. The control plane goes via LTE. In Option 3X the gNB is deployed to support the user traffic and the control traffic goes through the 4G eNB. The option 3X seems preferred by majority operators for enhanced mobile broadband.

This underlying potential prompted many carriers around the world to consider the use of the fiber-based Passive Optical Network (PON) access infrastructure as an all-packet-based converged fixed-mobile optical access networking transport architecture to backhaul both mobile and typical wireline traffic backhaul RAN architecture. A PON connects a group of Optical Network Units (ONUs) located at the subscriber premises to an Optical Line Terminal (OLT) located at the service provider's facility. While the economies for commercially deploying TDM-PON in the access arena as a near-term converged fixed-mobile optical networking transport infrastructure are quite convincing, however, several technical issues must be addressed first before mainstream TDM-based PONs could be used as viable optical access networking technology that enables the support of a truly unified PON-5G access networking architecture or just a 5G mobile.

The most notable issue is, TDM-PON is a centralized access architecture– relying on a component at the distant OLT to arbitrate upstream traffic, while 5G is a distributed architecture where, in particular, the 5G 3x option with gNB is anchored on 4G eNB requires a new distributed RAN architecture and further create a requirement to fully meshing the BSs (the X2 interface for 5G-LTE BS-BS handoffs requires a more meshed architecture) [1-3, 9]. The major weakness is that mainstream PONs are typically deployed as tree topologies and the tree-based topology can neither support the distributed access architecture nor intercommunication among the access nodes (ONUs) attached to the PON. The key challenge in devising a truly unified PON-5G access architecture is how to reconcile the traditionally centralized PON's architecture and NCM operations with the typically distributed 5G's architecture and NCM operations. Though numerous hybrid Fiber-Wireless network architectures have been expected to utilize the fiber-based PON access infrastructure to backhaul mobile traffic [5-8], most of these architectures, however, have utilized the typically centralized tree-based PON topology, which can only support a centralized RAN architecture. Since both wireless and wireline segments of these hybrid architectures are assumed to be centralized, the key design requirements and challenges associated with overlaying a fully distributed mobile RAN segment (e.g., 5G/LTE) over a typically centralized PON-based wireline segment, still remain unresolved. The purpose of this paper is to propose a novel, simple, and cost effective PON-based 5G mobile backhaul RAN architecture that enables redistribution of some of the intelligence (e. g., bandwidth/QoS provisioning) currently centralized in the Mobile Packet Core (MPC) platform out into the access nodes of the RAN [9-11]. Specifically, this project devises a fully distributed ring-based EPON architecture that enables the support of a converged PON-5G LTE access networking transport infrastructure to seamlessly backhaul both mobile and wireline multimedia traffic and services. We quantify the merits of utilizing a distributed EPON-based 5G option 3x RAN architecture and those of traditional mobile 5G backhaul infrastructure. The salient feature of the proposed architecture is that it supports a fully distributed control plane that enables intercommunication among the access nodes (ONUs/BSs) as well as signaling, scheduling algorithms, and handoff procedures that operate in a distributed manner. We outline some of the key technical requirements associated with devising a truly unified fixed-mobile 5G LTE access transport architecture that is built on top of a typically centralized PON infrastructure.

The proposed architecture supports several key networking features that significantly improves the performance of both the RAN and MPC in terms of handoff capability, overall network throughput and latency, and QoS support. Though we have chosen Ethernet-based PON and5G as representative techniques for fixed PON and 5G mobile access technologies, the proposed architecture and related operation principles are also applicable to other PON and 5G access networks such as GPON and 5G/LTE.

The rest of the paper is organized as follows: Section II gives an overview of the standalone ring-based EPON architecture and Section III discusses how to evolve the ring-based architecture to an all-packet-based converged fixed-mobile optical access networking transport infrastructure. Section IV presents some of the key salient features enabled by the proposed architecture. Section V reports simulation results and Section VI offers some concluding remarks.

II. Overview of the Standalone Ring-Based EPON Architecture

Fig. 2. illustrates the proposed standalone ring-based PON architecture [12]. An OLT is connected to N ONUs via a 20 km trunk feeder fiber, a passive 3-port optical circulator, and a short distribution fiber ring.

The ONUs are joined with point-to-point links in a closed loop around the access ring. The links are unidirectional. Both downstream (DS) and upstream (US) signals (combined signal)

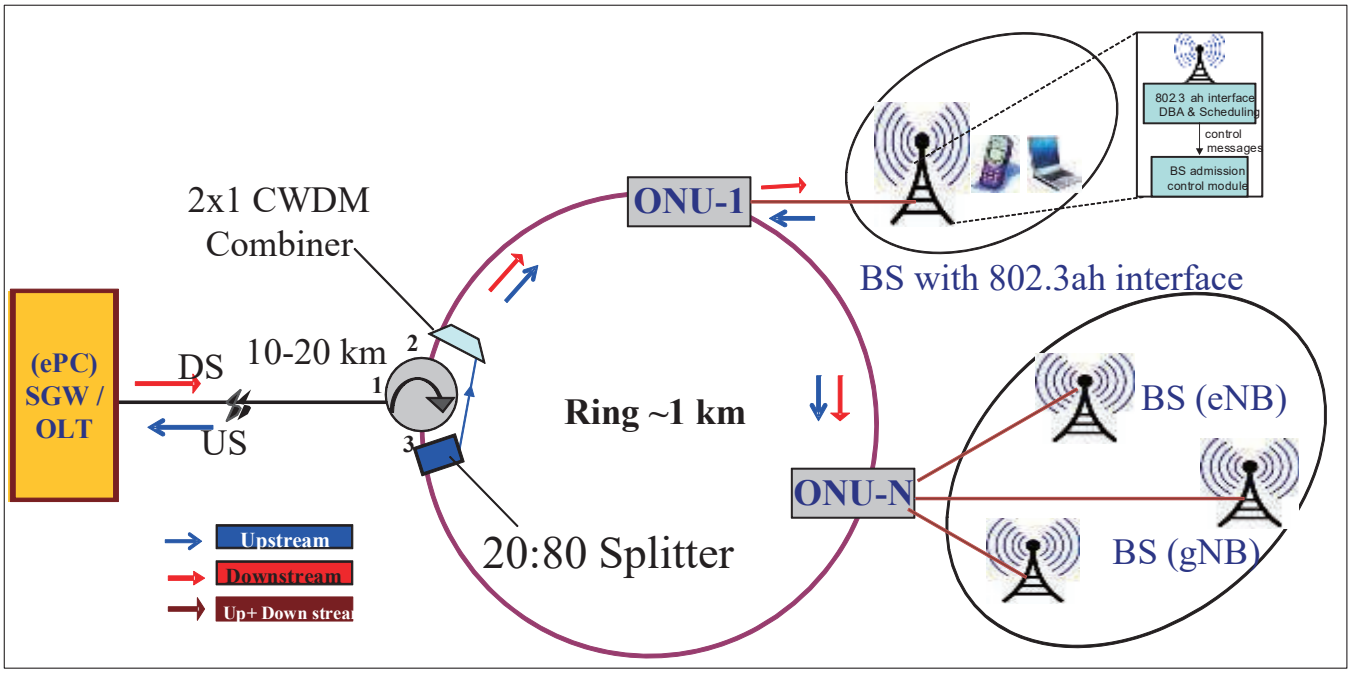


Fig. 2. Standalone Ring-based Architecture

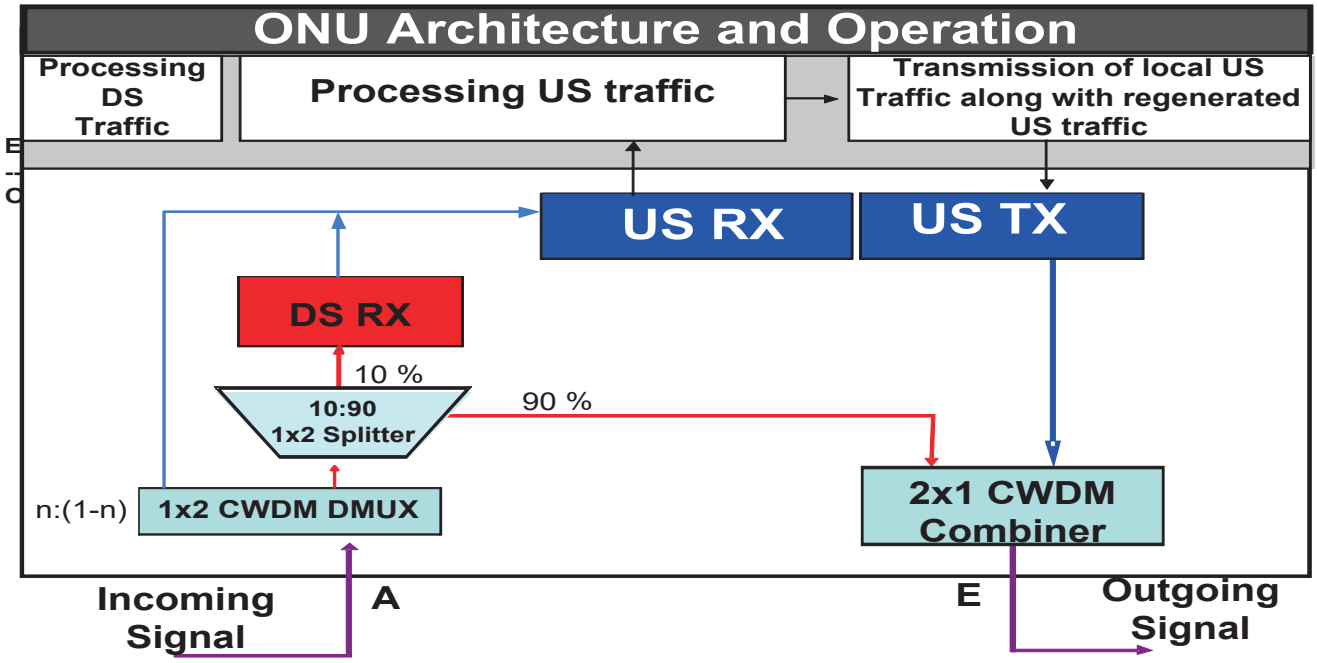


Fig. 3. ONU Architecture

are transmitted in one direction only. The US signal is transmitted sequentially bit by bit around the ring from one node to the next where it is terminated, processed, regenerated, and retransmitted at each node (ONU). Since US transmission is based on a TDMA scheme, inter-ONU traffic (LAN data and control messages) is transmitted along with upstream traffic destined to the OLT (MAN/WAN data) within the same pre-assigned time slot. Thus, in addition to the conventional transceiver maintained at each ONU (a λ_{up} US transmitter (Tx) and a λ_d DS receiver), this approach requires an extra receiver (Rx) tuned at λ_{up} to process the received US/LAN signal.

DS signal is coupled with the ring at port 2 of the optical circulator. After recombining it with the re-circulated US signal via the 2x1 CWDM combiner placed on the ring directly after the optical circulator, the combined signal then circulates around the ring (ONU_1 through ONU_N) in a Drop-and-Go fashion,

where the DS signal is finally terminated at the last ONU. The US signal emerging from the last ONU is split into two replicas via the 20:80 1x2 passive splitter (Fig. 2) placed on the ring directly after the last ONU. The first replica (80 %) is directed towards the OLT via circulator ports 1 and 3, where it is then received and processed by the US Rx (housed at the OLT), which accepts only MAN/WAN traffic, discards LAN traffic, and process the control messages, while the second replica (20 %) is allowed to recirculate around the ring having been recombining with the DS signal via the 2x1 CWDM combiner. The detailed ONU architecture is shown in Fig. 3. Each ONU attaches to the ring via the input port of a 1x2 CWDM DMUX housed at each ONU (incoming signal at point A in Fig. 3.) and can transmit data onto the ring through the output port of a 2x1 CWDM combiner (outgoing signal at point E in Fig. 3.). At each ONU, the incoming combined signal is first separated into its two constituent: DS and US signals via the 1x2 CWDM DMUX housed at the ONU. As can be seen from Fig. 3., the separated US signal is then received and processed via the US Rx housed at the ONU, where it is regenerated and retransmitted along with the ONU's own local control and data traffic.

As can also be seen from Fig. 3, the separated DS signal is coupled with the input port of the (10: 90) 1x2 passive splitter, which splits the DS signal into a small (10%) "Drop-signal-portion" and a large (90%) "Express-signal-portion". The small portion (Drop-Signal) is then received and processed by the DS Rx housed at the ONU. The remaining large portion emerging from the 90% output splitter's port (Express-Signal) is further transmitted through the ring to the next ONU, where it is, once again, partially split and detected at the corresponding DS Rx and partially transmitted towards the rest of the ring. Note that the Express-Signal recombines again with the retransmitted US signal (all previous ONU's regenerated US signals plus its own US signal) via the 2x1 CWDM combiner to form the outgoing combined signal (incoming signal for next ONU) that circulates around the ring.

III. Proposed EPON-Based Converged Fixed-Mobile Optical Access Networking Architecture

The standalone ring-based EPON architecture can be evolved around an all-packet-based converged fixed-mobile optical access networking transport infrastructure (or just 5G 3x mobile backhaul RAN) by simply interconnecting (overlying) the ONUs with the 5G and 4G's BSs and the OLT with serving access gateway (SGW). Under this simple overlay (independent) model, the PON and 5G/4G systems are operated independently where the RAN system is assumed to have its own NCM operations, independent of those for the PON. The BS is assumed to be collocated with an ONU or treated as a generic user attached to it. The ONU and BS can be interconnected as long as they support a common standard interface. Thus, the OLT, SGW, ONUs, and 5G/4G BSs, are all assumed to support a common standard interface (e.g., 802.3ah Ethernet interface). Each ONU is assumed to have two different Ethernet port ranges; the first port range will support wired users, while the second port range will support mobile users. The port ranges will be used by the ONUs to identify and differentiate between mobile users versus fixed users.

A. Fully Distributed Control Plane

This work uses the control and management messages defined by the IEEE 802.3ah multi-point control protocol (MPCP) standard [13] that facilitate the exchange of control and management information between the ONUs/BSs and OLT. The protocol relies on two Ethernet control messages, GATE (from OLT to ONUs/BSs) and REPORT (from ONUs/BSs to OLT and between ONUs/BSs) messages in its regular operation. Direct communication among ONUs/BSs is achieved via the US wavelength channel {control messages along with both LAN and US data share the same US channel bandwidth (in-band signaling)}, which is terminated, processed, regenerated, and retransmitted at each ONU. Since control messages are processed and retransmitted at each node, the ONUs can directly communicate their US/LAN queue status and exchange signaling and control information with one another in a fully distributed fashion. Likewise, BSs can also directly communicate the status of their queues and radio resources and exchange signaling and control messages with one another. The control plane utilized among the ONUs/BSs can thus support a distributed PON-4G RAN architecture, where each access node (ONU/BS) deployed around the ring has now truly physical connectivity and is, thus, capable of directly communicating with all other access nodes, in conformity with 4G standards.

Each access node maintains a database about the states of its queue and the state of every other ONU/BS's queue on the ring. This information is updated each cycle whenever the ONU receives new REPORT messages from all other ONUs. During each cycle, the access nodes sequentially transmit their REPORT messages along with both US and LAN data in ascending order within their granted timeslots around the ring from one node to the next, where each REPORT message is finally removed by the source ONU after making one trip around the ring. The REPORT message typically contains the desired size of the next timeslot based on the current ONU's buffer occupancy. Note that the REPORT message contains the aggregate bandwidth of both fixed and mobile data buffered at each ONU's/BS's queue (requested size of next timeslot).

An identical dynamic bandwidth allocation (DBA) module, which resides at each access node (ONU/BS), uses the REPORT messages during each cycle to calculate a new US timeslot assignment for each ONU. ONUs sequentially and independently run instances of the same DBA algorithm outputting identical bandwidth allocation results each cycle. The execution of the algorithm at each ONU starts immediately following the collection of all REPORT messages. Thus, all ONUs must execute the DBA algorithm prior to the expiration of the current cycle so that bandwidth allocations scheduled for the next cycle are guaranteed to be ready by the end of the current cycle. Once the algorithm is executed, the ONUs

sequentially and orderly transmit their data without any collisions, eliminating the OLT's centralized task of processing requests and generating grants for bandwidth allocations.

B. Dynamic Bandwidth Allocation and QoS Support & Mapping

Based on bandwidth demands, ONUs can be classified into two groups, namely: (i) lightly loaded ONUs that have bandwidth demands less than B_{MAX} (ii) heavily loaded ONUs that have bandwidth demands more than B_{MAX}. B_{MAX} is defined as follows in equation (1)

$$B_{max} = \frac{1}{N}[R_{EPON}(T_{MAX} - (N*T_G)] \quad (1)$$

Where, T_G is guard band interval, N is number of ONU's, T_{MAX} is EPON maximum cycle period and R_{EPON} is EPON data rate. Bandwidth demand here is the aggregate of wired and wireless demand. During each cycle, the DBA module keeps track of the unclaimed bandwidth from the set of lightly loaded ONUs. It then redistributes this excess bandwidth to other heavily loaded ONUs based on their requested bandwidth. During each cycle, the DBA module keeps track of the unclaimed bandwidth from the set of lightly loaded ONUs. It then redistributes this excess bandwidth to other heavily loaded ONUs based on their requested bandwidth i.e. two ONUs requesting bandwidths B1 and B2 more than B_{MAX} will be assigned excess bandwidths proportional to B1 and B2. During each cycle, the lightly loaded ONUs with $R_i < B_{MAX}$ will contribute a total remainder cycle bandwidth:

The heavily loaded ONUs with $R_i > B_{MAX}$ will require a total over the limit cycle bandwidth as shown in equation (2):

$$B_{Cycle\_Overlimit} = \sum_i^H (R_i - B_{MAX}) \quad (2)$$

The total remainder cycle bandwidth can be fairly distributed amongst the heavily loaded ONUs to expand their maximum transmission window as follows in equation (3)

$$\Delta B_i^{extra} = B_{Cycle\_Remainder} \left[\frac{R_i - B_{MAX}}{B_{Cycle\_OverLimit}}\right] \quad (3)$$

The granted bandwidth, B_{GH}, for a heavily loaded ONU_i is given by equation (4):

$$B_{GH} = \Delta B_i^{extra} + B_{MAX} \quad (4)$$

If R_i is the requested bandwidth of ONUi, $B_{Granted}$ is the bandwidth granted using the proposed limited service-based distributed DBA scheme, then $B_{Granted}$ can be expressed as equation (5):

$$B_{Granted} = \begin{cases} R_i & If\ R_i \le B_{MAX} \\ R_i & If\ R_i > B_{MAX}\ \&\ B_{Cycle\_Remainder} \ge B_{Cycle\_OverLimit} \\ B_{GH} & If\ R_i > B_{MAX}\ \&\ B_{Cycle\_Remainder} < B_{Cycle\_OverLimit} \end{cases} \quad (5)$$

We call this process as Inter-ONU scheduling.

After each ONU is given fair share of its bandwidth then it runs Intra-ONU scheduling module to distribute its total granted bandwidth to wired and wireless users. Intra-ONU scheduling algorithm is given as follows in (6) and (7);

$$B_{5G\_granted} = \begin{cases} R_{5G} & if\ R_{5G} \ge 0.4B_{granted} \\ 0.4B_{granted} + \{0.6B_{granted} - R_{wired}\}\ if\ R_{5G} > 0.4B_{granted}\ \&R_{wired} < 0.6B_{granted} \end{cases} \quad (6)$$

$$B_{wired\_granted} = \begin{cases} R_{wired} & if\ R_{wired} \ge 0.6B_{granted} \\ 0.6B_{granted} + \{0.4B_{granted} - R_{5G}\}\ if\ R_{wired} > 0.6B_{granted}\ \&\ R_{5G} < 0.4B_{granted} \end{cases} \quad (7)$$

Where R_{5G} is the bandwidth demand from 5G users and R_{wired} is the bandwidth demand from the wired users. Moreover $B_{5G\_granted}$ and $B_{wired\_granted}$ is the bandwidth granted to 5G and wired users respectively. Since, typically the wired data rate is more than wireless, it is given more share.

Typical 5G/4G MAC is centralized and connection-oriented. A connection identifier (CID) identifies each 5G/4G connection. The main mechanism for providing a connection-based QoS is to classify and associate packets traversing the MAC interface to IP Service Flows (SFs), where each existing SF is identified by a 32-bit SF identifier (SFID) and is characterized by a set of QoS parameters. A CID is then mapped into an SFID provided that the SF has already been admitted (active SF). Once the UE's CIDs are terminated at the BS, they are mapped into the appropriate mobility tunnels based on their CIDs. The BS's packet classifier then maps their constituent IP SFs into their appropriate priority queues based on CIDs attached to the IP packets. To allow for traffic separation in the PON-based transport network (IP cloud connecting the BSs to the OLT/SGW), the BS maps each CID into a corresponding DiffServ Code Point (DSCP) in order to translate CID to transport-based QoS (DSCP). Using this mapping function, packets on a given CID associated with specific QoS parameters are marked with a specific DSCP for forwarding in the transport network. The MPC performs the mapping for DL packets

On the other hand, EPON technology does not allow this type of CID-based connection. Rather, it supports only enhanced QoS through prioritization where packets are classified, stored in different priority queues and, then, scheduled for service according to their priorities. In a typical centralized EPON, QoS support is implemented via two independent scheduling mechanisms [10]: 1) inter-ONU scheduling: an aggregate bandwidth is allocated to each ONU by the OLT. 2) intra-ONU scheduling: each ONU makes a local decision to allocate the granted bandwidth and schedules packets transmission for up to eight different priority queues in the ONU. In the case of the proposed architecture, however, instances of the same DBA algorithm are executed simultaneously at each ONU. Thus, both scheduling mechanisms (inter and intra-ONU scheduling) are performed at each ONU-BS in a fully distributed approach, leading to the notion of integrating both scheduling mechanisms

at the ONU. This enables the proposed distributed architecture to provide better QoS support and guarantees.

For simplicity, we assume that each ONU maintains three separate priority queues that share the same buffering space. We consider three priority classes P0, P1, and P2, with P0 having the highest priority and P2 having the lowest. These classes are used for delivering voice (CBR), video stream (variable-bit-rate or VBR), and best-effort (BE) data, respectively, as they allow easy mapping of DiffServ's Expedited Forwarding (EF), Assured Forwarding (AF), and BE classes into 802.1D classes. Since both EPON and 5G/LTE classify data traffic in a differentiated services mode, an effective mapping mechanism is required between EPON priority queues and CID-based 5G/LTE IP flows. Specifically, the mapping has to identify which 5G/LTE IP flow should be stored in which EPON priority queue for equivalent QoS. EPON has up to eight different priority queues in each ONU, while 5G/LTE supports Guaranteed Bit Rate (GBR) & Non-GBR classes of service. QoS in 4G is based on bearers and in 5G is based on flow. In this work we assume that 5G/LTE GBR queues are mapped into EPON P0 queue and Non-GBR queues into P1 and P2 based on QoS parameters setting.

IV. Key Salient Networking Features Enabled By the Distributed EPON-Based RAN Architecture

The distributed ring-based architecture along with the supporting control plane enables the proposed EPON-based RAN architecture to support several key salient networking features that significantly enhance the performance of both the RAN and MPC in terms of handoff capability, overall network throughput and latency, and QoS support. These include:

A. Significance of Local Mobile LAN Traffic:

Local mobile LAN traffic is defined here as bidirectional multimedia traffic exchange (including VOIP, video, and data sessions) between two mobile users served by two different BSs that are either collocated or attached with/to two different ONUs on the same ring (same PON domain). In the proposed EPON-based RAN architecture, this traffic is directly routed on the ring from the source BS directly to the destination BS and vice-versa as local LAN traffic, without the direct participation of either the OLT or the MPC (e. g., SGW). This is significant as the volume of VOIP calls and/or multimedia data exchange between all local mobile users that are served by the many different BSs attached to the same ring, is substantial. In a typical 5G/LTE RAN, however, this traffic represents bidirectional US/DS data exchange between the two mobile users, which must be routed first from the source BS to the MPC (US traffic) and then from the MPC to the destination BS (DS traffic), and vice-versa.

Thus, a substantial volume of local mobile traffic and associated signaling overhead, as well as the lengthy and complex processing of this traffic (e. g., sessions (LTE bearers/mobility tunnels) switch/set-up, retain, and tear-down and associated signaling commands from the BSs to the MPC and vice-versa), have been offloaded from the overburdened MPC to the access nodes (ONUS/BSs) of the RAN. This has a significant impact on the performance of the MPC. First, it frees up a sizable fraction of the badly needed network resources as well as processing on the centralized serving nodes (e. g. SGW) in the MPC to handle Internet-bound traffic more efficiently. Second, it frees up capacity and sessions on the typically congested mobile backhaul from the BSs to the MPC and vice-versa.

B. Enhanced Handoff Capabilities

In 5G and LTE standards, hard handoff (HHO) is mandatory. The HHO is a break-before-make procedure, in which LTE user equipment (UE) breaks its connections with the serving BS (SBS) before setting up new connections with the target BS (TBS) and this is when traffic interruption and packet loss take place. By exploiting both the distributed nature of the ring-based RAN architecture and the supporting control plane, the proposed architecture enables the support of seamless and speedy inter-BS Hos in which, as the simulation results will show, packet loss is almost totally avoided and VoIP and other real-time IP applications can be adequately supported during HO. This is accomplished as follows:

1) When a UE enters a domain served by the PON-RAN, it needs to register itself to the domain OLT's access router and updates the new location in its home subscriber server (HSS). As long as the UE is roaming within the same PON-RAN domain, it does not need to reregister again.

2) The physical connectivity of both the SBS and TBS attached to the ring allows direct data exchange and intercommunications among them during HO (compare the simplicity and reduced latency and signaling overhead of this direct approach versus that of the typical 4G indirect bidirectional lengthy intercommunications and logical connectivity among the SBS and TBS via the MPC). Thus, once the TBS accepts the HO command, the SBS may immediately start to forward the buffered data (which have not yet been successfully sent to the UE), to the TBS directly on the ring as local LAN traffic. This is significant for creating the typical 4G logical connectivity among the SBS and TBS, which requires the lengthy process of signaling to the EPC to coordinate the mobility-tunnel set up/switch from the SBS to TBS (and vice-versa) via the MPC, is totally avoided as well as the direct participation of the SGW/OLT.

3) For the HO to complete, the TBS signals the OLT/SGW to inform it that the HO is complete and to update its records with the new TBS, i.e., to add TBS (and corresponding target ONU (TONU) that is collocated or attached with/to the TBS) to the forwarding list for the UE. Then, under the typical 4G/5G RAN scenario, to resume normal operation and forward DS traffic to the TBS (or UE), the typical lengthy process of setting up a mobility tunnel form the MPC to the TBS is essential. Under the proposed PON-based RAN architecture, however, the scheduler at the OLT just simply redirects the UE's DS traffic from the DS queue that was serving the SONU/SBS before the HO (the OLT houses N dedicated DS queues, each serving one of the N

ONUs-BSs attached to the ring) to the new DS queue that is now serving the TONU/TBS. The HO can happen from 4G to 5G and vice versa. This proposed setup supports and enhances performance. To further reduce the signaling latency and packet loss during the HO, the OLT may concurrently broadcast DS traffic destined to the UE to both the SBS and TBS.

Overall, the proposed EPON-based RAN architecture introduces several significant advantages over typical 5G/LTE RAN and the advantages include: 1) a significant reduction in the signaling overhead and handoff latency; 2) offloading a sizable fraction of the local mobile sessions switch/set-up and tear-down and associated lengthy and complex signaling processing from the overloaded MPC to the RAN's access nodes; 3) re-registration procedures to the HSS when the UE moves from a BS to another is avoided as long as the UE roams within the coverage area served by the BSs attached to the ring; 4) during inter-BSs HOs, no path switch/setup command is needed since the path (mobility tunnels) from MPC to the UE remains unchanged.

V. Performance Evaluation

In this section, we first compare the performance of the proposed EPON-based mobile 5G RAN with that of the typically centralized 5G RAN. Two simulation programs were developed using MATLAB, one for the typical 5G RAN and the other one for the EPON-based RAN. The performance metrics used here are network utilization, average throughput, and End-to-End (ETE) delay. We consider the practical case of non-uniform traffic load in which, during a given period, some BSs might be lightly loaded/idle, while other BSs might be heavily loaded. At a given total network load, different BSs have different average traffic loads. Under this non-uniform traffic load scenario, the significance of utilizing PON-based RAN architecture is established.

The following are the system parameters used for simulating the EPON-based RAN architecture: (1) a PON with 16 ONUs, each serving a varying number of BSs (a minimum of one BS to a maximum of 10 BSs), depending on the varying traffic load.; (2) aggregate access link data rate from the UEs to a given ONU is 100 Mb/s; (3) the RAN DS line rate (from the OLT/SGW(ePC) to the ONUs/BSs) is assumed to be same as the US line rate (from the ONUS/BSs to the OLT/SGW) and is equal to 1 Gb/s; (4) the average distance between the OLT/SGW(ePC) and ONS/BSs is 20 km; (5) the buffer size in each ONU/BS is 1 Mbyte; (6) the maximum EPON cycle time is 2 ms for US transmission, while a standard fixed periodic cycle of 10 ms is assumed for 5G US transmission (from the UEs to the BS); (7) the IEEE 802.3ah MPCP REPORT/GATE message is 64 bytes; (8) we assume that all network traffic is just mobile traffic initiated by 5G UEs, i.e., traditional EPON's fixed wired end-user's traffic is assumed to be zero; (9) the total mobile traffic is divided equally among US mobile traffic and local mobile LAN; (10) the mobile traffic model used here is as described above in Section III B, we assume that 5G/LTE GBR queues are mapped into EPON P0 queue and Non-GBR queues into P1 and P2 based on QoS parameters setting.; (12) the DBA scheme reported in [12] is used here to provision EPON US traffic, whereas the proportional fairness algorithm is used to provision 5G US traffic.

To have a fair comparison, all EPON-based RAN parameters listed above are also used for simulating the typical 5G except for the following: each and every dedicated link data rate of the typical 5G RAN in either US (16 dedicated point-to-point links between the ONUs/BSs and the OLT/SGW) or DS (16 dedicated point-to-point links between the OLT/SGW and the ONUs/BSs) direction is set to 62.5Mbps. Thus, the aggregated link data rate in either direction is: 62.5Mbps * 16 = 1 Gbps, which is equal to that of the EPON-based RAN.

Table I shows the possible scenarios of four unevenly loaded Base Stations i.e., ligtly loaded, moderately loaded, heavy loaded and super heavily loaded BS's. Similarly Fig.s 4 and 5 show the uplink utilization versus time at a given single network load of 0.83 and versus the total network load for unevenly and evenly BSs respectively. This is for both the typical 5G and EPON ring-based RAN architectures.

Although traditional 5G shows on average similar performance in evenly loaded BSs as in Fig. 5. nonetheless Fig. 4 demonstrates that EPON ring-based RAN has a much higher level of usefulness as well as stability with less variation with time compared to typical 5G. This enhances the network's stability and predictability. Fig. 6 shows that the average uplink throughput EPON-based RAN architecture is much higher than the typical 5G RAN architecture at a higher total network load.

Table I:
Unevenly Loaded Base Stations Scenarios

Heavily Loaded BSs		Lightly Loaded BSs		Total Network Load
BSs	BS Load	BSs	BS Load	
1	0.8488	15	0.1051	0.24
3	0.8488	13	0.1051	0.39
5	0.8488	11	0.1051	0.54
Super Heavily Loaded BSs		**Moderately Loaded BSs**		**Total Network Load**
BSs	BS Load	BSs	BS Load	
1	1.85	15	0.3262	0.68
2	1.85	14	0.3262	0.83
3	1.85	13	0.3262	0.98
4	1.85	12	0.3262	1.13
5	1.85	11	0.3262	1.28

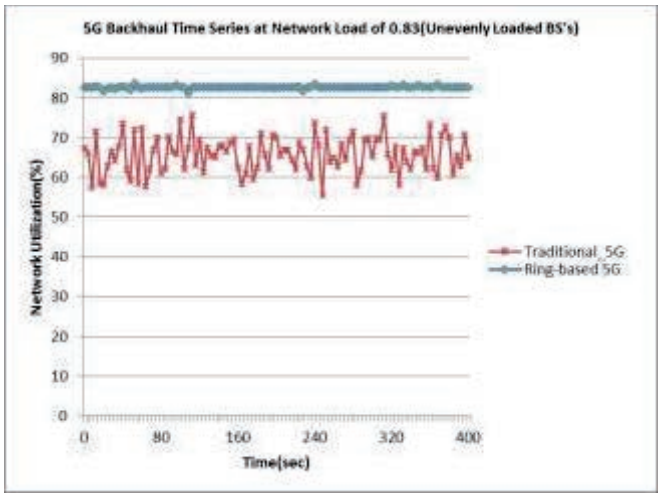


Fig. 4. Uplink Utilization Time Series at Network Load = 0.83

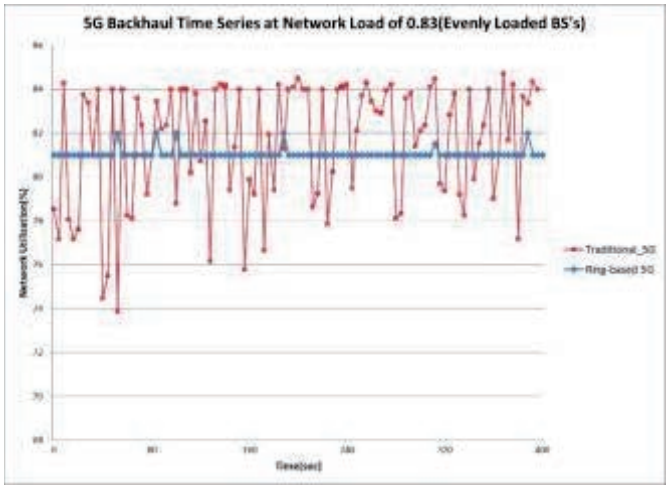


Fig. 5. Uplink Utilization Time Series of Evenly loaded BSs at Network Load = 0.83

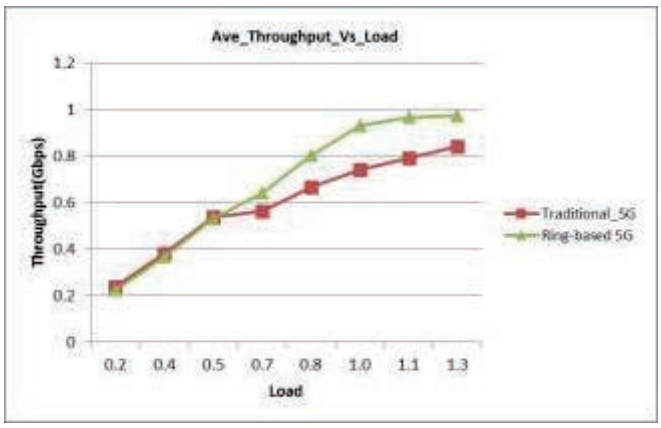


Fig. 6. Uplink Ave Throughput

Fig. 7. shows the ETE network delay for both Guaranteed Bit Rate (GBR) and Non-Guaranteed Bit Rate (N-GBR) traffic for both the typical 5G and Ring-based RAN architectures.

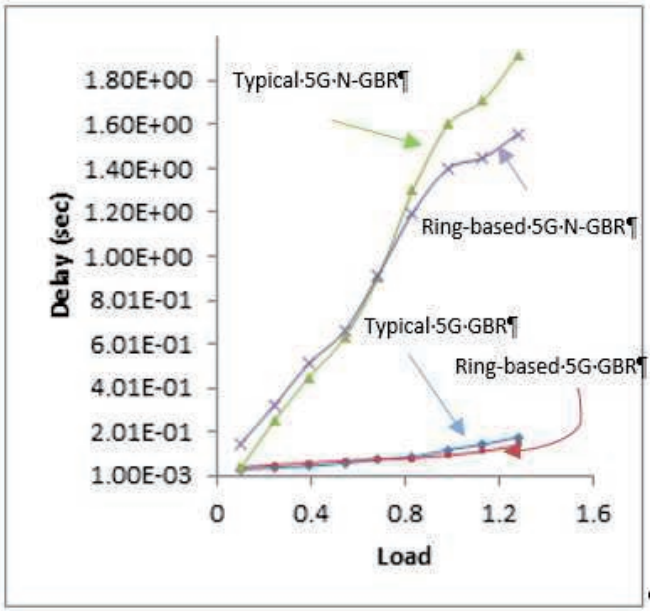


Fig. 7. Average network ETE delay for GBR and Non-GBR traffic

It can be observed from the Fig. 7. that at a lower load, the typical 5G has a lower delay than the Ring-based RAN. This is expected as typical 5G traffic utilizes dedicated point-to-point links and the queuing delay are still almost zero. However at higher traffic load, as expected, the Ring-based 5G RAN exhibits much lower delay.

A. Handover scenario

One significant benefit of using EPON ring-based 5G network would be less handover delay and packet drop. To validate this, we use a scenario where UE node moves from its Home Agent BS 4 to Foreign Agent BS 5. Uni-directional best effort application traffic is conFig.d between UE and the server at the rate of 64 Kbps. UE from BS 4 has trajectory that starts moving around 110 seconds. Its movement converges to BS 5 between 115 to 120 seconds. Same scenario is set up for both traditional 5G backhaul and 5G BS's connected to ring network. Parameters collected for comparison are the traffic received/dropped and handover delay vs. time. Handover delay is computed from the time the User Equipment sends a Handoff REQ message starting the handoff process until initial ranging with the Fig. 8. shows the throughput versus time for a UE during HO when moving away from the SBS attached to ONU_1 and approaching the TBS attached to a neighboring ONU_2 for both the typical 5G and EPON ring-based RAN architectures.

A unidirectional BE application traffic is conFig.d between UE and the server at the rate of 64 Kbps. The UE has trajectory that starts moving around 110 seconds and converges to the TBS between 115 to 120 seconds. Same scenario is set up for both traditional 5G and EPON-based RAN. Parameters collected for comparison are the traffic received/dropped and HO latency. HO latency is computed from the time the UE sends a HO request message to initiate the HO process until initial ranging with the TBS is successfully completed. As

expected, EPON-based RAN show lower HO latency (15 ms versus 20 ms) as shown in Fig. 9. and almost no packets drop as compared to typical 5G.new Serving BS successfully completed.

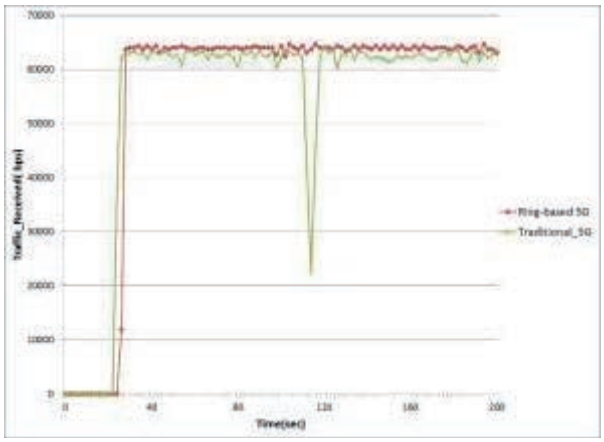


Fig. 8. Traffic Throughput during UE handoff

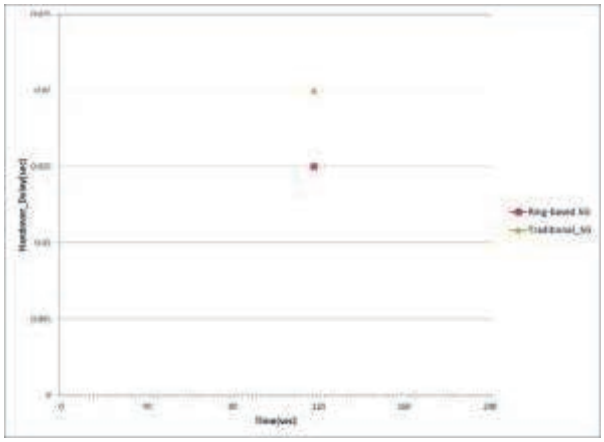


Fig. 9. UE Handover Delay

VI. CONCLUSION AND FUTURE WORK

This study presents a simple and cost effective PON-based 5G mobile backhaul RAN architecture supporting several key salient networking features that collectively contribute towards significant enhancement of the performance of both the RAN and MPC in terms of handoff capability, overall network throughput and latency, and QoS support. We quantify and compare between the merits of utilizing a distributed EPON-based 5G/4G RAN architecture and that of traditional LTE backhaul infrastructure. Some of the key technical requirements associated with devising a truly unified fixed-mobile 5G/ LTE access transport architecture that is built on top of a typically centralized PON infrastructure are also outlined in the work. For future work we will like to test the performance of the network with higher data rates, perform packet loss and power budget analysis for increased number of ONUs connected in the ring.

REFERENCES

[1] UMTS Evolution, from 3GPP Release 7 to Release 8, HSPA and SAE/LTE, June 2008 UPDATE, www.3gamericans.org.

[2] 3GPP TS 23.401 “GPRS Enhancements for E-UTRAN access”, October 2007.

[3] H. Ekstrom, “QoS control in the 3GPP Evolved Packet system,” *IEEE Communication Magazine*, 47(2):76-83, 2009.

[4] IEEE 802.6e-2005, “Air interface for fixed and mobile broadband wireless access systems,”

[5] S. Sarkar, S. Dixit, and B. Mukherjee, “Hybrid Wireless-Optical Broadband-Access Network (WOBAN): A Review of Relevant Challenges,” *IEEE/OSA Journal of Lightwave Technology*, 25(11):3329-3340, 2007.

[6] Kun Yang, et al., “Convergence of Ethernet PON and IEEE 802.16 Broadband Access Networks and its QoS-aware Dynamic Bandwidth Allocation Scheme,” *IEEE J. Selected Areas in Comm.*, 27(2):101-116, 2009

[7] G. Shen, R. S. Tucker, and C-J. Chae, “Fixed Mobile Convergence Architectures for Broadband Access: Integration of EPON and WiMAX”, *IEEE Com. Mag.*, 45(8):44-50, 2007.

[8] N. Ghazisaidi, M. Maier, and C. M. Assi, “Fiber-Wireless (FiWi) Access Networks: A Survey,” *IEEE Communications Magazine*, 47(2):160-167, Feb. 2009

[9] 5G PPP Architecture Group, “View on 5G Architecture: https://5g-ppp.eu/wp-content/uploads/2019/07/5G-PPP-5G-Architecture-White-Paper_v3.0_PublicConsultation.pdf, June 2019.

[10] 3GPP Study on scenarios and requirements for next generation access technologies, Technical report, TR 38.913 (Release 14), October 2016.

[11] Gupta, A. et al., “A survey of 5G networks: Architecture and emerging technologies” IEEE Access, vol 3, 1206– 1232, 2015

[12] A. Delowar, et al., “Ring-Based Local Access PON Architecture for Supporting Private Networking Capability,” *OSA Journal of Optical Networking*, 5(1):26-39, 2006.

[13] IEEE 802.3 Ethernet in the First Mile Study Group, http://www.ieee802.org/3/ efm/ public/ index.html

Syed Rashid Zaidi received the M.S., M.Phil. and Ph.D. degrees in Electrical Engineering from City University of New York, NY, USA. He is currently Assistant Professor & Program Director of Cybersecurity & Networking Technology and Electronic Engineering Technology in The Department of Engineering, Physics & Technology of the Bronx Community College of The City University of New York. His research areas are Fiber Optics Communications, LTE, WiMAX, 5G, and next generation wireless networks and cybersecurity. He has numerous peer-reviewed publications, invited talks, conference presentations and received numerous awards, a recent one is a prestigious grant award from the U.S. Department of Education to update the Cybersecurity program and build the latest industrial-standard lab.

Ajaz Sana received the M.S., M.Phil. and Ph.D. degrees in Electrical Engineering from City University of, New York, NY, USA. He is currently an Assistant Professor in The Department of Engineering, Physics & Technology of Bronx Community College of The City University of New York. His research areas are Free Space Optics, WiMAX, and next generation wireless networks. He has many peer-reviewed research publications.

Shahab Hussain received his M.S., M.Phil., and Ph.D. degrees in Electrical Engineering from The City University of New York, USA. He is working as Senior Professional in the Mobile Networks Division of Nokia. His research areas are LTE, PON, and next generation (5G) wireless networks. Dr. Hussain has over 20 years of experience in Research & Development and Wireless Services Delivery with a specialty in Testing, Architecture Design, Integration, Performance of Wireless Networks, Business Development, and Operations Support Competency. Dr. Hussain is also serving as an Adjunct Professor of Engineering in the Department of STEM of North Shore Community College in Massachusetts.

A Method for Controlling Scan Rate Based on Estimated Retransmission Rate of Background Traffic

Kenta SUZUKI*, Takuya KURIHARA*, Kazuto YANO*, Yoshinori SUZUKI*
Advanced Telecommunications Research Institute International (ATR), Kyoto, Japan.
*Email: {kenta-suzuki, tkurihara, kzyano, yoshinori.suzuki}@atr.jp

***Abstract*—For efficient network scan to narrow-band wireless networks, this paper proposes a method for controlling a scan rate based on the estimated retransmission rate of background traffic from a scan response delay obtained at a scan rate. This proposed method is aiming to select the highest scan rate that can keep the estimated retransmission rate of the background traffic below a predetermined retransmission threshold. First, through computer simulations considering a Wi-SUN sensor network with two different network situations and multiple scan rates, we derive a regression function between the mean of scan response delay and COR (Channel Occupation Rate) of the background traffic, and that between the COR and the retransmission rate of the background traffic, for each the network situation and the scan rate using the least-squares method. Then, we propose a method for estimating the retransmission rate of the background traffic at a different scan rate using three kinds of estimators; network situation estimator, COR estimator, and retransmission rate estimator. After that, we propose a control scheme of scan rate based on the estimated retransmission rate of the background traffic. We evaluate the estimation accuracy of the retransmission rate of the background traffic using the proposed estimation method. We confirm that the proposed estimation method can estimate the retransmission rate of the target network with the average error lower than 0.058 regardless of the situation of the target network and the scan rate. Moreover, we evaluate the performance of scan rate control using proposed method. We confirm that proposed method can scan faster by 0.18 pps and decrease the retransmission rate of the background traffic by 0.015 compared with a fixed scan rate.**

***Index Terms*—Network scan, Wi-SUN, Scan rate control, QoS estimation, Network simulation**

Manuscript received on Jan. 25, 2021. This work is a result of the project entitled "Research and Development of Technologies of Efficient Network Scanning for Wide-Area IoT Wireless Networks," which is supported by the Ministry of Internal Affairs and Communications as part of the research program "R&D for Expansion of Radio Wave Resources (JPJ000254)." This paper is a follow-up of the invited journal to the presented paper entitled "A Study on Estimation of Retransmission Rate of Background Traffic for Various Scan Rates with Scan Response Delay" of the 23th International Conference on Advanced Communication Technology (ICACT2021).

Kenta Suzuki is with the Wave Engineering Laboratories, Advanced Telecommunications Research Institute International, Japan. (corresponding author, email: kenta-suzuki@atr.jp)

Takuya Kurihara is with the Wave Engineering Laboratories, Advanced Telecommunications Research Institute International, Japan. (email: tkurihara@atr.jp)

Kazuto Yano is with the Wave Engineering Laboratories, Advanced Telecommunications Research Institute International, Japan. (email: kzyano@atr.jp)

Yoshinori Suzuki is with the Wave Engineering Laboratories, Advanced Telecommunications Research Institute International, Japan. (email: yoshinori.suzuki@atr.jp)

I. Introduction

RECENTLY, the number of IoT (Internet of Things) wireless devices has been increasing dramatically, and vulnerable IoT devices for cyber-attacks are also increasing rapidly. Attacked IoT devices can be used as a stepping stone by attackers and are used as perpetrators of DDoS attacks. Such devices transmit a large number of packets of unauthorized traffic to disturb traffic which is originally transmitted in their network; hereafter, we call this original traffic as background traffic. In order to find such vulnerable IoT devices, network scan toward a wide area of the Internet is useful.

In existing applications of network scan for a wide area of the Internet [1], a scanner makes the network scan at a high rate to finish the scan quickly. However, when making a scan toward wireless networks with a small network capacity like LPWA (Low Power, Wide Area) networks such as Wi-SUN [2] and LoRa [3], these networks are easily congested. Consequently, QoS (Quality-of-Service) such as transmission delay will be degraded due to collide and retransmit packets [4].

In order to keep the QoS degradation of the background traffic at an allowable level, it is necessary to select the highest scan rate that can keep a balance between the processing time of the network scan and the QoS degradation of the background traffic. Examples of QoS are throughput and delay of background traffic observed in application layer. In this paper, we focus on the retransmission rate of the background traffic in MAC (Medium Access Control) layer which causes these QoS degradations. For realizing this control, the scanner needs to know the retransmission rate of the background traffic in the target network.

However, the scanner cannot directly know the QoS in the target network if it scans from the outside of the target network. The retransmission rate of the background traffic depends on the situation of the target network. For example, the retransmission rate of the background traffic increases as the mean of the scan response delay or scan rate increases [5]. This is because that collision is occurred by congestion of the target network and retransmission is triggered by the collision. Therefore, the scanner needs to estimate the retransmission rate of the background traffic which is different for each target

network by using information which can be observed at the scanner such as scan response delay.

As related works for estimating the situation of network, a method for estimating the number of users in IEEE 802.11 network based on collision probability obtained through an analysis of state transition of CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is proposed by [6]. Moreover, a method for estimating the number of users using a PDF (Probability Density Function) of transmission deferring time in the backoff algorithm of IEEE 802.11 and collision probability obtained through simulations is proposed by [7]. These methods aim to grasp the network situation using the collision information which is obtained from the target network directly.

As other related work, estimating the available bandwidth in IEEE 802.11-based multi-hop wireless networks using the number of retransmission is proposed by [8]. By this method, the number of retransmissions is directly obtained from the target networks. Although there are various related works as mentioned above, it is difficult to apply these methods to estimate the retransmission rate of background traffic at the scanner. Therefore, a method for estimating the retransmission rate of background traffic at the scanner existing out of the target network is required.

In order to estimate the retransmission rate of the background traffic via Internet, we have proposed a method for estimating the retransmission rate of the background traffic from the scan response delay [9]. The proposed method consists of two kinds of estimators. The first one estimates the situation of the target network from the distribution of the scan response delay. The second one estimates the retransmission rate of the background traffic in the target network from the mean of scan response delay and the regression function between the mean of scan response delay and the retransmission rate of the background traffic corresponding to the estimated network situation. The regression function is empirically obtained for several network situations through simulations assuming a Wi-SUN PAN (Personal Area Network).

For realizing the control of the scan rate, we need to determine the proper scan rate from the current scan rate and obtained scan response delay. Therefore, we also proposed a method for estimating the retransmission rate of the background traffic at a different scan rate using three kinds of estimators; network situation estimator, COR (Channel Occupation Rate) estimator, and retransmission rate estimator [10].

This paper shows a method for controlling the scan rate based on the retransmission rate of the background traffic estimated from the scan response delay using the estimators proposed in [10]. First, the followings are confirmed through empirical analysis using network simulation assuming various situations with different number of terminals or the transmission interval of the background traffic.

1) The relationship between the scan response delay and the transmission interval of the background traffic can be expressed by a regression function.
2) The relationship between the transmission interval of the background traffic and the retransmission rate of the background traffic can also be expressed by a regression function.
3) The shape of the regression function is different depending on the situation of the target network and the scan rate.

Next, based on the above empirical analysis, we propose a method for estimating the retransmission rate of the background traffic for various scan rates different from the current scan rate and the scan response delay. The proposed estimation method consists of three kinds of estimators. The first one estimates the situation of the target network from the distribution of the scan response delay. The second one estimates the COR of the background traffic from the mean of the scan response delay, the scan rate at which the scan response delay is obtained, and the estimated situation of the target network. Here, the COR of the background traffic is used instead of the transmission interval of the background traffic. The third one estimates the retransmission rate of the background traffic at the target scan rate from the estimated COR of the background traffic and the estimated situation of the target network.

Finally, we propose a control scheme of the scan rate based on the estimated retransmission rate of the background traffic. The proposed method selects the highest scan rate that can keep the estimated retransmission rate of the background traffic below a predetermined retransmission threshold. The performance of the proposed method is also evaluated through computer simulations.

II. Situation of target network

In general, a situation of a network varies by time of day such as morning, work time, or midnight. In addition, how the network situation varies depends on the application run in the network or network topology. Therefore, it is necessary to analyze the statistical characteristics of the retransmission of the background traffic in various situations of target networks.

In the empirical analysis, we consider a sensor network that consists of Wi-SUN devices. Examples of the factor of determining the network situation are the number of terminals, the transmission interval, frame length, and communication direction. In this paper, we focus on the number of terminals and the transmission interval because these factors affect the congestion situation of the background traffic significantly.

As shown in Fig. 1, we vary the situation of the target network by changing the transmission interval of the background traffic (Case 1), or the number of terminals which transmit the background traffic (Case 2). The background traffic is transmitted from terminals to their application server. We assume that the interval of situation change is much longer than the transmission interval of the background traffic.

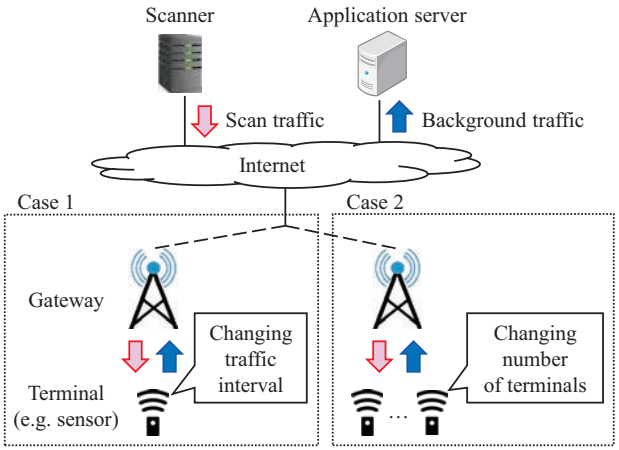


Fig. 1: Example of situations of target network (without scan traffic).

III. Empirical Analysis of Relationship between the Scan Response Delay and Retransmission Rate of Background Traffic

We conduct empirical analysis of the relationship between the scan response delay and the retransmission rate of the background traffic through computer simulations, assuming the system model described in the previous section. We try to express the relationship by a polynomial regression function given by Eq. (1).

$$p(x) = \sum_{k=0}^{n} a_k \cdot x^k \tag{1}$$

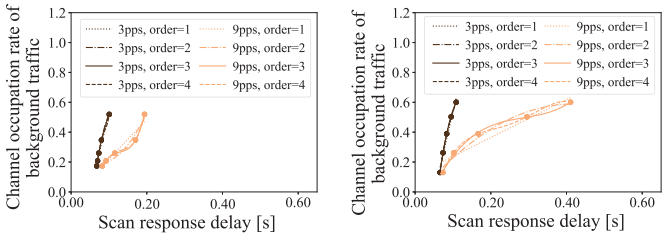
where n is the regression order of the least-squares method, and a_k is the coefficient for the k-th regression order that minimizes the squared error.

In order to determine the coefficients in Eq. (1), we first evaluate the scan response delay, the transmission interval of the background traffic, and the retransmission rate of the background traffic for various scan rates and network situations. Here, we assume that the packet length of the background traffic is fixed, and thus we use the COR of the background traffic instead of its transmission interval. We simulate two different network situations by ns-3 [11]. Table I shows the baseline parameters for the entire simulation in this paper. As a network topology, there are at least two terminals (for the background traffic source(s) and for the scan traffic) that are connected to the same Wi-SUN gateway. The Wi-SUN gateway is connected to the scanner by wired LAN. The scan rate changes in a range of 1–10 pps (packet per second).

In the network situation corresponding to Case 1 in Fig. 1, we assume that there is one terminal that transmits the background traffic, and its transmission interval is changed from 60 to 180 ms with a 30 ms step. In the network situation corresponding to Case 2 in Fig. 1, we assume that there are several terminals for transmitting the background traffic with a fixed transmission interval of 180 ms, and the number of terminals is changed from one to five.

TABLE I
Baseline parameters for entire simulation.

Common	Overall	Simulation time	100 sec
		Number of trials	100
	Wi-SUN system	Bandwidth	200 kHz
		Phy communication rate	50 kbps
		Symbol duration	50 kbps
		CCA duration	0.16 us
		Turnaround time	1 ms
		Unit of backoff period	1.16 ms
		Minimum backoff exponent	3
		Maximum backoff exponent	5
	Scan traffic	Number of terminals	1
		Scan rate	1–10 pps
		Frame length	12.8 ms
	Background traffic	Communication direction	UL
		Frame length	27.84 ms
Case 1	Background traffic (Situation index 1)	Number of terminals	1
		Transmission interval	60–180 ms
		Configuration index 1	180 ms
		Configuration index 2	150 ms
		Configuration index 3	120 ms
		Configuration index 4	90 ms
		Configuration index 5	60 ms
Case 2	Background traffic (Situation index 2)	Number of terminals	1–5
		Configuration index 1	1
		Configuration index 2	2
		Configuration index 3	3
		Configuration index 4	4
		Configuration index 5	5
		Transmission interval	180 ms



(a) Case 1 (b) Case 2

Fig. 2: Regression function of scan response delay vs. COR of background traffic [10].

A. Relationship between scan response delay and COR of background traffic

In order to determine the regression order of the regression function, we draw regression curves for different regression orders from 5 points of the average scan response delay and the average COR of the background traffic with different networks situations, i.e. the values of the transmission interval in Case 1 or the number of terminals in Case 2.

Figure 2 shows the regression functions derived for different regression order n. When both the network situation and traffic configuration are same, the COR of the background traffic is also same regardless of the scan rate. The mean of the scan response delay of the higher scan rate (9 pps) is higher than

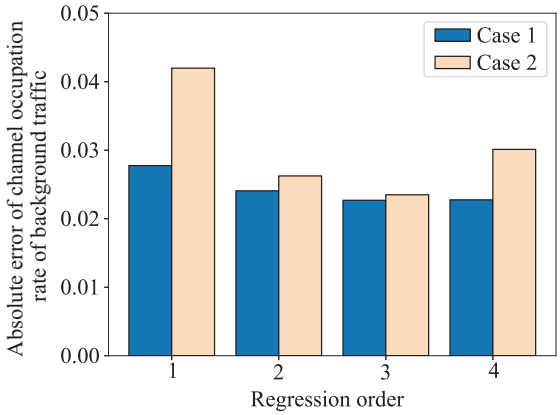


Fig. 3: Fitting accuracy of each regression order [10].

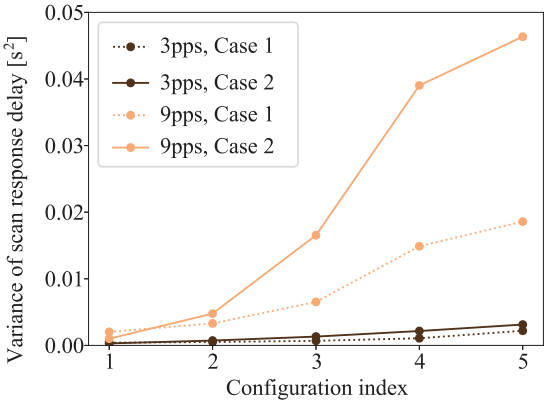
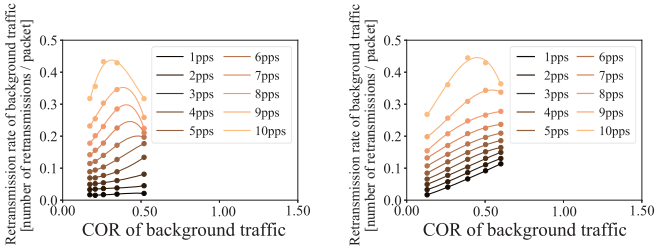
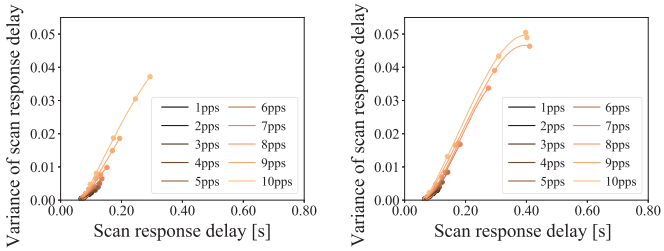


Fig. 5: Variance of scan response delay [9].



(a) Case 1 (b) Case 2

Fig. 4: Regression function of COR of background traffic vs. retransmission rate of background traffic [10].



(a) Case 1 (b) Case 2

Fig. 6: Regression function of scan response delay vs. its variance [9].

that of the lower scan rate (3 pps). We can also find that the shapes of curves are different between two network situations.

Figure 3 shows the fitting accuracy of the regression function for different regression orders and network situations. The fitting accuracy is calculated as the absolute error between the fitting data and the actual simulation result. Since regression order 3 shows the best performance, we use it for the subsequent evaluation.

B. Relationship in background traffic between COR and retransmission rate

Figure 4 shows the regression functions for the COR of the background traffic and the retransmission rate of the background traffic. We draw a regression curve from 5 ($average\ COR\ of\ background\ traffic$, $average\ retransmission\ rate\ of\ background\ traffic$) points in the same way as in Section III-A for each network situation. Since the shapes of curves are different between two network situations, we use these regression functions for the estimation of the situation of the target network.

C. Distribution of scan response delay

This section summarizes the previous research [9] for estimating the network situation in the target network confirmed the relationship between the scan response delay and its variance through empirical analysis of the distribution of the scan response delay.

Figure 5 shows the variance of the scan response delay versus the situation of the target network at scan rates of 3 pps and 9 pps. The variance of the scan response delay becomes larger as the amount of the background traffic or the scan rate increases. Therefore, the relationship between the scan response delay and its variance can also be derived with a regression function.

Figure 6 shows the regression functions for the mean of scan response and its variance. We draw a regression curve from 5 ($average\ scan\ response\ delay$, $variance\ of\ scan\ response\ delay$) points for each network situation in the same way as in Section III-A. Since the shapes of curves are different between two network situations, the network situation can be distinguished by the relationship between the mean of scan response and its variance. Therefore, in order to estimate the situation of the target network, we use the regression functions for the mean of scan response and its variance.

IV. Estimation of Retransmission Rate of Background Traffic

Based on the empirical analysis described in Section III, we propose a method for estimating the retransmission rate of the background traffic at the target scan rate from a scan response delay obtained at a different scan rate. Figure 7 shows the block diagram of the proposed method that employs three kinds of estimators $\mathbb{E}$. The first estimator E^S estimates

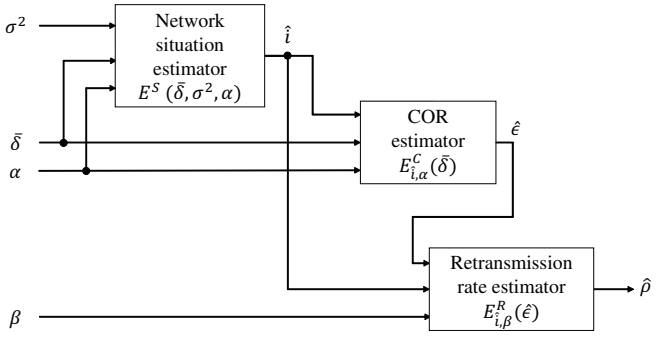


Fig. 7: Block diagram of proposed method.

the situation $\hat{i}$ of the target network; hereafter, we call this estimator as network situation estimator. The second estimator E^C estimates the COR of the background traffic in the target network; hereafter, we call this estimator as COR estimator. The third estimator E^R estimates the retransmission rate of the background traffic in the target network; hereafter, we call this estimator as retransmission rate estimator. Each estimator of $\mathbb{E}$ is trained for each cases $\mathbb{I}$ i.e. Case 1 or Case 2 mentioned in previous section. Therefore, the function E of the proposed estimation and its output $\hat{\rho}$ are described as following equation.

$$\hat{\rho} = E(\bar{\delta}, \sigma^2, \alpha, \beta) = E^R_{\hat{i},\beta}(E^C_{\hat{i},\alpha}(\bar{\delta})) \tag{2}$$

$$\hat{i} = E^S(\bar{\delta}, \sigma^2, \alpha) \tag{3}$$

where $\bar{\delta}$ is the mean of the scan response delay observed at the scanner, σ^2 is the variance of the scan response delay, α is the scan rate when the scan response delay is observed, β is the target scan rate for estimating retransmission rate of the background traffic, and $\hat{\rho}$ is the estimated retransmission rate of the background traffic at β.

In network situation estimator E^S, the network situation index $\hat{i}$ is estimated by finding the situation that gives the minimum distance of the variance of the scan response delay between the observed and estimated values. The observed variance is calculated from the scan response delay observed at the scanner. For each situation of the target network, the estimated variance is calculated from the mean of the scan response delay by using the regression functions for the mean of the scan response delay and its variance.

The index $\hat{i}$ of the situation of the target network is estimated from the following equation.

$$\hat{i} = E^S(\bar{\delta}, \sigma^2, \alpha) = \arg\min_i |\sigma^2 - V_{i,\alpha}(\bar{\delta})| \tag{4}$$

where $V_{i,\alpha}$ is the regression function for the mean of the scan response delay and its variance shown in Fig. 6.

COR estimator E^C estimates the COR $\hat{\epsilon}$ of the background traffic from the mean $\bar{\delta}$ of the scan response delay by using the regression function for the mean of the scan response delay and the COR of the background traffic, for the situation index i and the scan rate α.

The COR $\hat{\epsilon}$ of the background traffic is estimated from the following equation.

$$\hat{\epsilon} = E^C_{\hat{i},\alpha}(\bar{\delta}) = \sum_{l=0}^{3} a^C_{l,\hat{i},\alpha} \cdot \bar{\delta}^l \tag{5}$$

where $a^C_{l,\hat{i},\alpha}$ is the coefficient for the l-th regression order that minimizes the squared error for the estimated situation index $\hat{i}$

Retransmission rate estimator E^R estimates the retransmission rate $\hat{\rho}$ from the COR $\hat{\epsilon}$ of the background traffic by using the regression function for the COR and the retransmission rate of the background traffic, for the situation index i and the scan rate β.

The retransmission rate $\hat{\rho}$ is estimated from the following equation.

$$\hat{\rho} = E^R_{\hat{i},\beta}(\hat{\epsilon}) = \sum_{l=0}^{3} a^R_{l,\hat{i},\beta} \cdot \hat{\epsilon}^l \tag{6}$$

where $a^R_{l,\hat{i},\beta}$ is the coefficient for the l-th regression order that minimizes the squared error for the estimated situation index $\hat{i}$.

V. Control of Scan Rate Based on Estimated Retransmission Rate of Background Traffic

We propose a method for controlling the scan rate based on the estimated retransmission rate of the background traffic by using the proposed estimation method described in Section IV. Figure 8 and Table II show a processing image and notations of the proposed method, respectively. First, the proposed method requires following information; the observed scan response delay ($\mathbb{D}$), the scan rate ($\alpha \in \mathbb{B}$) for observing the scan response delay, the candidate scan rates for estimation target ($\mathbb{B}$), and the retransmission rate threshold (θ). Second, the estimated retransmission rate ($\hat{\rho}_k$) of the background traffic for each candidate scan rate ($B_k \in \mathbb{B}$) is estimated by using the proposed estimators ($\mathbb{E}$) which are trained with cases (the set of the indexes is defined by $\mathbb{I}$). Finally, the highest scan rate ($\alpha' \in \mathbb{B}$) that satisfied the condition $\hat{\rho}_k \leq \theta$ is calcurated.

TABLE II
Notations.

i	Case index of network situation.
j	Configuration index of network situation.
θ	Retransmission rate threshold.
$\mathbb{I}$	Trained cases for proposed estimators.
$\mathbb{E}$	Proposed estimators trained with $\mathbb{I}$.
$\mathbb{B}$	Candidate scan rates for estimation target.
k	Scan rate index of $\mathbb{B}$.
$\alpha\ (\in \mathbb{B})$	Scan rate when observed scan response delay.
$\alpha'\ (\in \mathbb{B})$	Scan rate controlled by proposed method.
$\mathbb{D}$	Samples of scan response delay when using α.
ρ_k	Retransmission rate at B_k.
$\hat{\cdot}$	A value estimated by using proposed method.

Figure 9 shows the scanning flow of the proposed method. First, the scanner is initialized by setting θ, α, $\mathbb{E}$, and $\mathbb{B}$. After that, the scanner makes a scan using α in phase $2n$ of the n-th trial. Here, n is a natural number. During phase $2n$, the scan

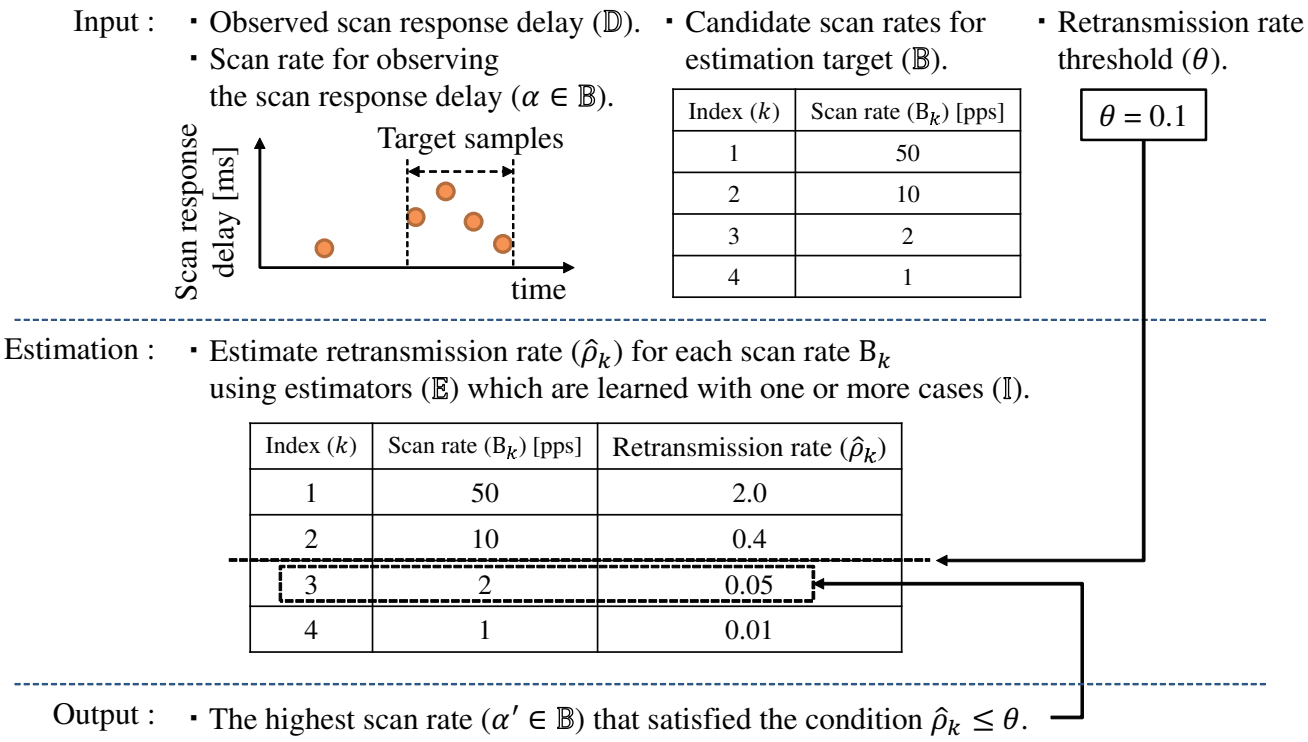


Fig. 8: Processing image of proposed method.

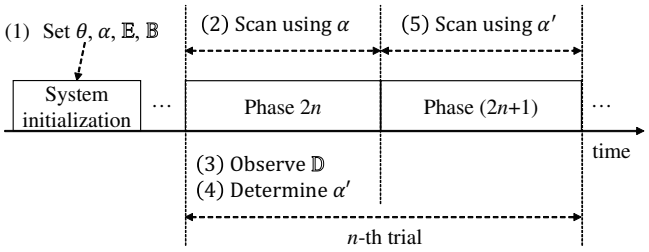


Fig. 9: Scanning flow of proposed method.

response delay $\mathbb{D}$ are observed at the scanner. At the end of phase $2n$, the scanner determines α' by using the proposed algorithm shown in Fig. 10. Finally, the scanner makes a scan using α' during phase $(2n+1)$. In this paper, we assume that the situation of the target network is stable from phase $2n$ to phase $(2n+1)$. Moreover, we assume that the scanner can get one or more samples of the scan response delay in each phase.

Figure 10 shows the proposed algorithm for controlling the scan rate based on the estimated retransmission rate of the background traffic. First, the average $\bar{\delta}$ and the variance σ^2 of the scan response delay are calculated from the observed scan response delay $\mathbb{D}$. After that, the retransmission rate $\hat{\rho}_k$ of the background traffic for each candidate scan rates is estimated by using the proposed estimators in Fig. 7. While estimating the retransmission rate of the background traffic, β is added into the set of the candidate scan rates $\mathbb{B}'$ when satisfied the condition $\hat{\rho}_k \leq \theta$. Finally, the controlled scan rate α' is calculated by getting the maximum scan rate in $\mathbb{B}'$ if $\mathbb{B}'$ is not empty. Otherwise, the minimum scan rate in $\mathbb{B}$ is set to α'.

VI. Performance Evaluation of Proposed Method

In this section, we evaluate the proposed method by the following steps. First, we evaluate the estimation accuracy of the retransmission rate of the proposed estimators. Next, we evaluate the performance of the scan rate control of the proposed algorithm. Finally, through analysis of these evaluation results, we confirm that proposed method can scan faster and improve the retransmission rate of the background traffic compared with a fixed scan rate.

A. Estimation accuracy of the retransmission rate

We evaluate the estimation accuracy of the retransmission rate of the proposed method. We calculate the estimation error γ between an actual value γ_A and the estimated one γ_E by the following equation.

$$\gamma = |\gamma_E - \gamma_A|. \tag{7}$$

Figure 11 shows the true positive rate (TPR) of the situation estimation as the performance of network situation estimator, which had evaluated in previous research [9]. The TPR of Case 1 is 55% on average, and the TPR of Case 2 is 67% on average. Therefore, network situation estimator sometimes selects the wrong situation.

Figure 12 shows the average estimation error of the COR of the background traffic for different training cases. When

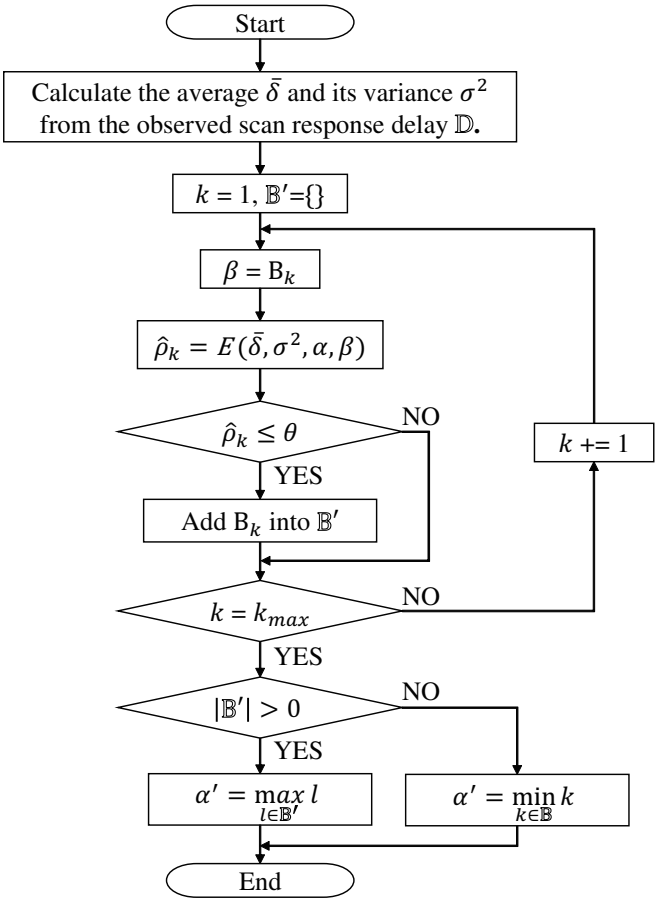
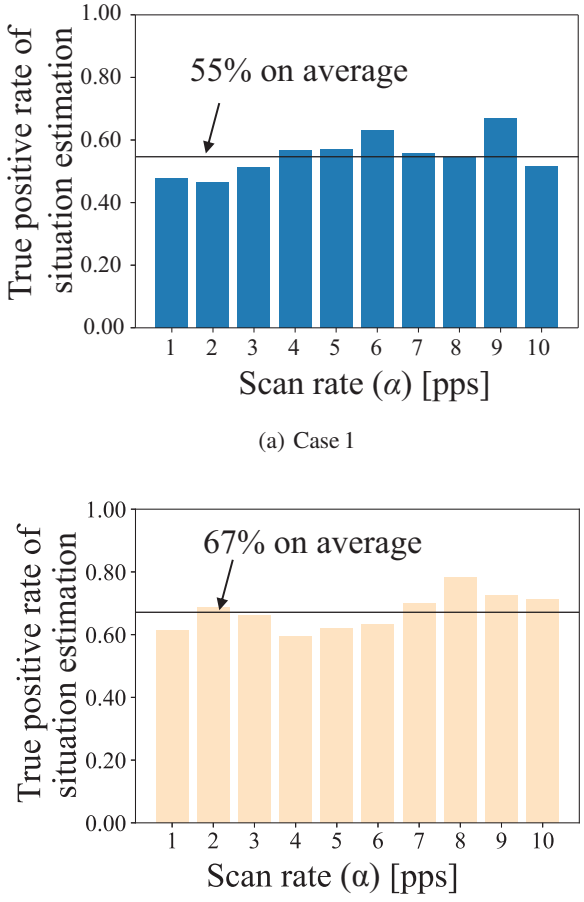


Fig. 10: Proposed algorithm.



(a) Case 1

(b) Case 2

Fig. 11: True positive rate of situation estimation of target network [9].

estimating the retransmission rate in Case 1, the estimator trained both for Cases 1 and 2 can decrease the estimation error by 0.003 from that of the estimator trained only for Case 2 (i.e., the mismatched training case). On the other hand, when estimating the retransmission rate in Case 2, the estimator trained for both Cases 1 and 2 can decrease the estimation error by 0.015 from that of the estimator trained only for Case 1 (i.e., the mismatched training case).

Figure 13 shows the average estimation error of the retransmission rate of the background traffic for different training cases. When estimating the retransmission rate in Case 1, the estimator trained both for Cases 1 and 2 can decrease the estimation error by 0.004 from that of the estimator trained only for Case 2 (i.e., the mismatched training case). On the other hand, when estimating the retransmission rate in Case 2, the estimator trained for both Cases 1 and 2 can decrease the estimation error by 0.009 from that of the estimator trained only for Case 1 (i.e., the mismatched training case).

From Figs. 12 and 13, we can find that COR estimator and retransmission rate estimator trained both for Cases 1 and 2 can improve the estimation accuracy compared with the mismatched training case. On the other hand, compared with the estimator trained for the actual situation of the target network (i.e., the matched training case), the estimator trained for both Cases 1 and 2 degrades the estimation accuracy because of the imperfect estimation of the situation at network situation estimator. However, the estimation error of the COR and that of the retransmission rate are not significant compared with the matched training case. Therefore, training for both cases can be a fail-safe approach.

Figure 14 shows the average estimation error of the retransmission rate of the background traffic for each the current scan rate α and the candidate scan rate β when the estimators are trained for both Cases 1 and 2. This result shows that the average error is lower than 0.058 regardless of the scan rates α and β.

B. Performance of controlling scan rate

We evaluate the performance of the scan rate control. Table III shows the parameter set for the performance evaluation. In this simulation, the proposed method scans according to the scanning flow explained in the previous section V. Here, the candidate scan rates $\mathbb{B}$ are set 1–10 pps. We also evaluate the performance when a fixed scan rate is used as in existing scan applications for comparison. In the case, a fixed scan rate α

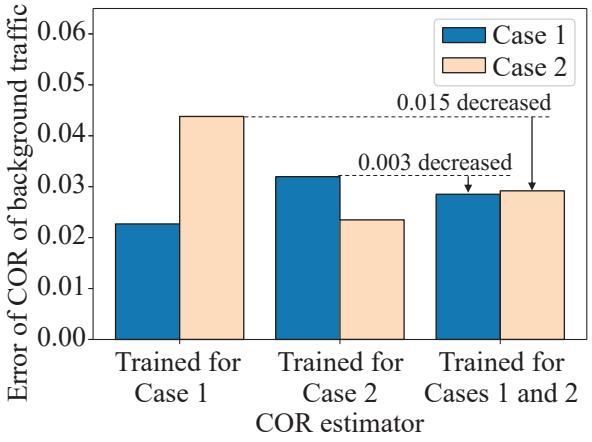


Fig. 12: Average estimation error of COR of background traffic for different estimators [10].

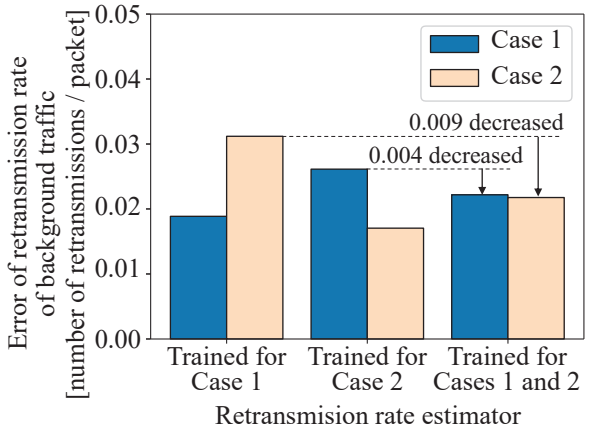


Fig. 13: Average estimation error of retransmission rate of background traffic for different estimators [10].

is used from phase $2n$ to phase $(2n+1)$ of the scanning flow. During scanning, we assume that the situation of the target network is stable in each phase. In addition, the samples of the scan response delay observed at the scanner is not empty. We ran simulation with 10,000 different seeds.

Figure 15 shows the average retransmission rate of the background traffic for all situations when $\mathbb{I} = \{1, 2\}$. This

TABLE III
Parameter set for performance evaluation.

Parameter	Value
Case index of network situation (i)	[1-2]
Configuration index of network situation (j)	[1-5]
Trained case for proposed estimators ($\mathbb{I}$)	[1, 2, {1, 2}]
Retransmission rate threshold (θ)	[0.05, 0.1, 0.15]
Scan rate when observed scan response delay (α)	[1-10]
Number of observed scan response delay (N)	[1-100]

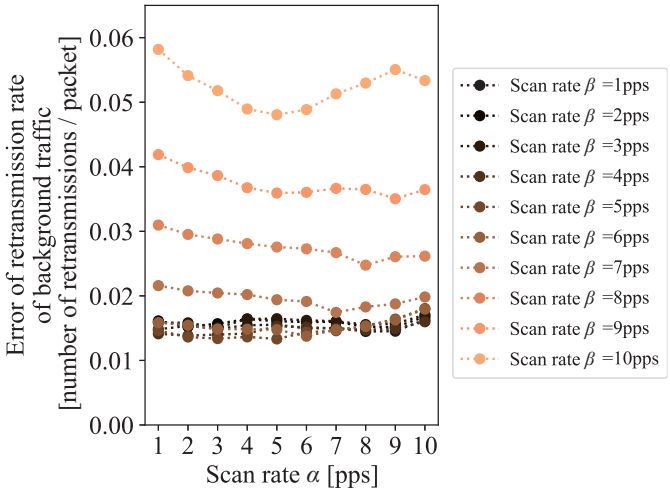


Fig. 14: Average estimation error of retransmission rate of background traffic for different scan rates (α, β) [10].

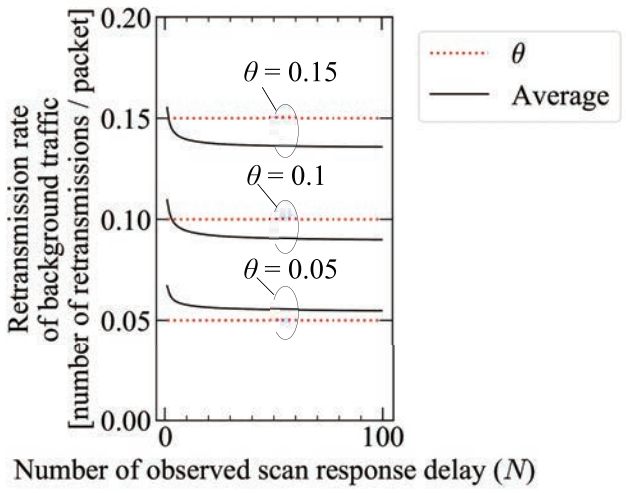
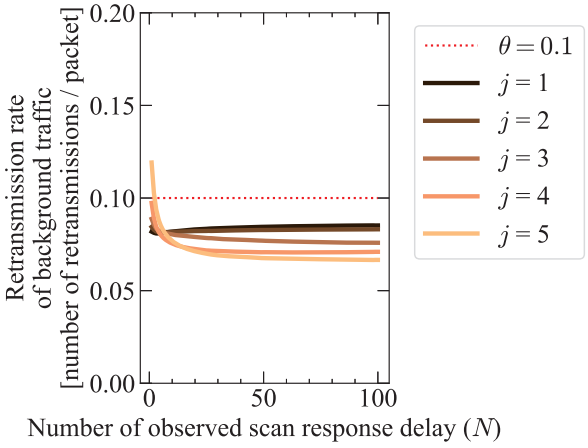


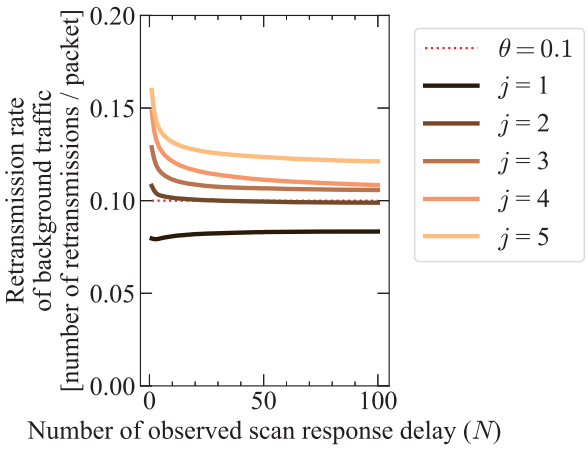
Fig. 15: Average retransmission rate of background traffic for all situations when $\mathbb{I} = \{1, 2\}$.

result shows that proposed method can converge the average retransmission rate of the background traffic with the increase of the number of the observed scan response delay (N). When θ = 0.1 and 0.15, the average retransmission rate of the background traffic can achieve less than θ if at most 10 samples of the observed scan response delay are obtained. However, when θ = 0.05, the average retransmission rate of the background traffic dose not achieve θ regardless of N. This result implies that there is the lower bound of the achievable retransmission rate because the accidental retransmission of the background traffic can occur as long as scanning.

Figure 16 shows the average retransmission rate of the background traffic for defferent situation (i, j) of the target network when $\theta = 0.1$ and $\mathbb{I} = \{1, 2\}$. When $i = 1$ (case 1), θ is satisfied regardless of j with the increase of N. On the



(a) Case 1 ($i = 1$)



(b) Case 2 ($i = 2$)

Fig. 16: Average retransmission rate of background traffic for different situation of target network when $\theta = 0.1$ and $\mathbb{I} = \{1, 2\}$.

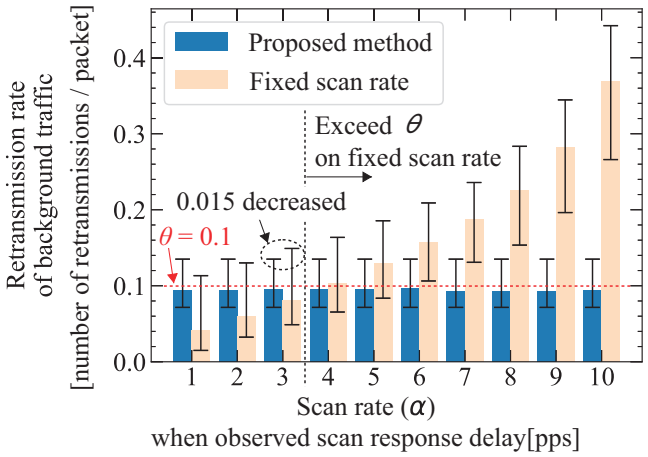


Fig. 17: Average retransmission rate of background traffic for different current scan rates (α) when $\theta = 0.1, N = 10$, and $\mathbb{I} = \{1, 2\}$.

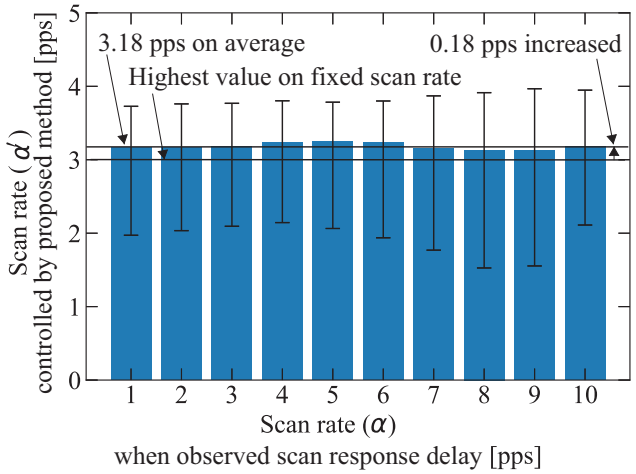


Fig. 18: Average scan rate (β) for different current scan rates (α) when $\theta = 0.1, N = 10$, and $\mathbb{I} = \{1, 2\}$.

other hand, when $i = 2$ (case 2), θ is not satisfied in most case of j even if the N increases. Here, the higher value of j represents the higher congesting level. And also, each j of case 2 is congested compared with the same j of case 1 . Therefore, these results imply that the lower bound of the achievable retransmission rate of case 2 is higher than that of case 1 because the collision of the background traffic is easily occurred in case 2 in which there are more terminals than case 1.

Figures 17 and 18 show the average retransmission rate of the background traffic and controlled scan rate α' for different current scan rates α when $\theta = 0.1, N = 10$, and $\mathbb{I} = \{1, 2\}$. Here, each error bar in each graph shows the range of the average value for all situations of the target network. This result shows that the proposed method can keep the retransmission rate of the background traffic below θ regardless of the current scan rate α. As seen in the result of a fixed scan rate, $\alpha = 3$ pps is the highest scan rate which satisfies θ on average. Compared with this result, the proposed method can decrease the upper range of the retransmission rate of the background traffic by 0.015. Moreover, the proposed method increases the scan rate by 0.18 pps compared with the highest scan rate of the fixed scan rate. Therefore, the proposed method can scan faster and improve the retransmission rate of the background traffic compared with the fixed scan rate.

Figures 19 and 20 show the average of the retransmission rate of the background traffic and the average of the controlled scan rate α' for all situations of the target network. The proposed estimators are trained for different cases $\mathbb{I}$, respectively. Figure 19 shows that the estimator trained for case 2 only and cases 1 and 2 can keep the average retransmission

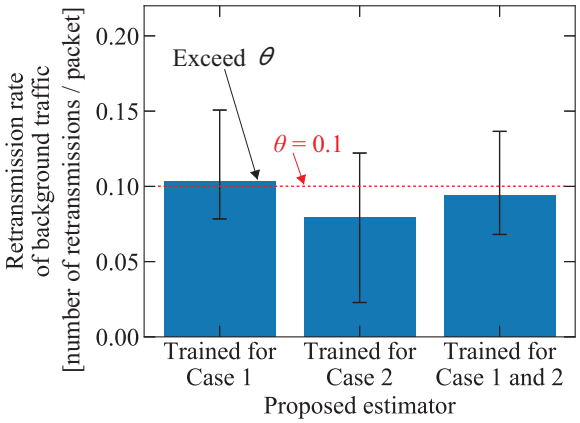


Fig. 19: Average retransmission rate of background traffic for different training cases (𝕀) when $\theta = 0.1$ and $N = 10$.

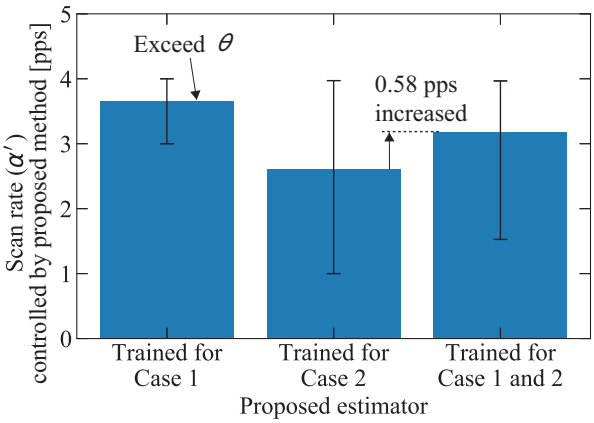


Fig. 20: Average scan rate (α') for different training cases (𝕀) when $\theta = 0.1$ and $N = 10$.

rate of the background traffic below θ. Moreover, Fig. 20 shows the estimator trained for cases 1 and 2 can scan faster by 0.58 pps compared with the estimator trained for case 2 only on average. Therefore, the proposed estimator trained for multiple cases can more effectively control the scan rate than the estimator trained for a single case.

VII. Conclusion

This paper proposed a method for controlling the scan rate based on the retransmission rate of the background traffic from a scan response delay obtained at a scan rate.

First, through computer simulations considering a Wi-SUN sensor network with two different network situations and multiple scan rates, we derived a regression function using the least-squares method for the mean of the scan response delay and the COR of the background traffic, and that for the COR of the background traffic and the retransmission rate of the background traffic.

Then, we proposed the method for estimating the retransmission rate of the background traffic for various scan rates different from the current scan rate and the scan response delay. First, network situation estimator estimates the situation of the target network from observed value and estimated value regarding the variance of scan response delay. Second, COR estimator estimates the COR of the background traffic from the mean of scan response delay, the estimated situation of the target network, and the scan rate which is used for observing the scan response delay. Third, retransmission rate estimator estimates the retransmission rate of the background traffic from the COR of the background traffic at the estimated situation of the target network, and a scan rate of estimation target.

After that, we proposed the method for controlling the scan rate based on the estimated retransmission rate of the background traffic. First, the scanner is initialized by setting retransmission rate threshold, scan rate for observing the scan response delay, the proposed estimators trained for one or more cases of the situation of the target network, and candidate scan rates. Second, the scanner scans by using the current scan rate and observes the scan response delays during scanning. Finally, the scanner selects the highest scan rate that can keep the estimated retransmission rate of the background traffic below the retransmission threshold.

We evaluated the estimation accuracy of the retransmission rate of the background traffic by using the proposed estimation method. We confirmed that the proposed estimation method can estimate the retransmission rate of the background traffic with the average error lower than 0.058 regardless of the situation of the target network and the scan rate. Moreover, we evaluated the performance of scan rate control by using the proposed method. We confirmed that the proposed method can scan faster by 0.18 pps and decrease the retransmission rate of the background traffic by 0.015 compared with the case using a fixed scan rate.

Acknowledgment

This work is a result of the project entitled “Research and Development of Technologies of Efficient Network Scanning for Wide-Area IoT Wireless Networks,” which is supported by the Ministry of Internal Affairs and Communications as part of the research program “R&D for Expansion of Radio Wave Resources (JPJ000254).”

References

[1] “The ZMap Project”, https://zmap.io/ (Retrieved on Aug. 30, 2021)
[2] “Wi-SUN Alliance”, https://wi-sun.org/ (Retrieved on Aug. 30, 2021)
[3] “LoRa Alliance”, https://lora-alliance.org/ (Retrieved on Aug. 30, 2021)
[4] K. Suzuki, T. Kurihara, K. Yano, and Y. Suzuki, “Impact of Congestion Level on Success Probability of Network Scan for IoT Wireless Equipment,” *IEICE Society Conf. 2019*, B-6-7, September 2019. (in Japanese)
[5] K. Suzuki, T. Kurihara, K. Yano, and Y. Suzuki, “Impact of Network Scanning on Communication Performance of Wi-SUN,” *IEICE Society Conf. 2020*, B-6-21, September 2020. (in Japanese)
[6] Giuseppe Bianchi and Ilenia Tinnirello, “Kalman Filter Estimation of the Number of Competing Terminals in an IEEE 802.11 network,” *Proc. IEEE INFOCOM 2003*, March-April 2003. DOI:10.1109/INFCOM.2003.1208922

[7] N. Matsumoto, I. Oka, and S. Ata, "Estimation of The Number of Users by Backoff and Collision Information on WLAN," *IEICE technical report*, IT2018-12, pp. 1–4, July 2018. (in Japanese)
[8] N. V. Nguyen, I. Guerin-Lassous, V. Moraru, and C. Sarr, "Retransmission-based available bandwidth estimation in IEEE 802.11-based multihop wireless networks," *Proc. ACM MSWiM 2011*, Oct.-Nov. 2011. DOI: 10.1145/2068897.2068961
[9] K. Suzuki, T. Kurihara, K. Yano, and Y. Suzuki, "A study on Estimation of Retransmission Rate of Background Traffic with Scan Response Delay of Network Scan," *IEICE technical report*, NS2020-79, pp. 20–25, November 2020.
[10] K. Suzuki, T. Kurihara, K. Yano, and Y. Suzuki, "A Study on Estimation of Retransmission Rate of Background Traffic for Various Scan Rates with Scan Response Delay," *Proc. ICACT 2021*, pp. 160–165, Feb. 2021, doi: 10.23919/ICACT51234.2021.9370480
[11] "ns-3 Network Simulator", https://www.nsnam.org/ (Retrieved on Aug. 30, 2021)

Kenta Suzuki was born in Japan, 1988. He received his B.S. degree in Computer Science from Hirosaki university, Japan in 2011, and received his M.S. degree in Computer Science from Tohoku university, Sendai, in 2013.In 2013, he joined Mobile Techno Corp., where he was engaged in development on broadcast radio system for disaster prevention and system level simulator for network simulation. Since April 2019, he has been assigned to Advanced Telecommunications Research Institute International (ATR) as a researcher, and he is engaged in research and development on network scan systems. He is a member of the IEICE.

Takuya Kurihara was born in Japan, 1988. He received his B.E., M.E., and Ph. D. degrees in electrical engineering from Nippon Institute of Technology, Saitama, Japan, in 2011, 2013, and 2017, respectively. In 2018, he joined Advanced Telecommunications Research Institute International (ATR), Kyoto, Japan, where he is currently a researcher of Wave Engineering Laboratories. His research interests include nonlinear systems, signal processing, and optimization. He received the 2013 Presentation Award in Nonlinear Problems from IEICE Technical Committee on Nonlinear Problems and the IEICE Young Researcher's Award in 2014. He is a member of IEICE.

Kazuto Yano was born in Japan, 1977. He received the B.E. degree in electrical and electronic engineering, and the M.S. and Ph.D. degrees in communications and computer engineering from Kyoto University in 2000, 2002, and 2005, respectively. He was a research fellow at the Japan Society for the Promotion of Science (JSPS) from 2004 to 2006. In 2006, he joined the Advanced Telecommunications Research Institute International (ATR). Currently, he is the Head of Dept. Wireless Communication Systems at Wave Engineering Laboratories, ATR. His research interests include spacetime signal processing for interference suppression, MIMO transmission, and PHY/MAC cross-layer design of wireless communication systems for ISM bands. He is a member of IEEE and a senior member of IEICE.

Yoshinori Suzuki was born in Japan, 1970. He received the B.E., M.E. and Ph.D. degrees from Tohoku University, Sendai, in 1993, 1995 and 2005 respectively. He joined NTT Wireless Systems Laboratories in 1995. Since then, he engaged in researching microwave signal processing techniques for satellite onboard applications and onboard multiple beam antenna feed techniques. He worked as a parttime lecturer at Niigata University in 2012 and 2014. From 2013 to 2014, he was in charge of sales engineering of satellite communication services in NTT Software Corporation (currently NTT Techno Cross Corporation). Since then, he was a research engineer in NTT Access Network Service Systems Laboratories working on future mobile satellite communication systems. From June 2018, he has been engaged in the research of innovative radio communication systems at ATR Wave Engineering Laboratories, Kyoto, Japan. He received the Younger Engineer Award from the IEICE Japan in 2003. He is a senior member of IEICE.

Ransomware Detection Using Open-source Tools

Sun-Jin Lee, Hye-Yeon Shim, Yu-Rim Lee, Tae-Rim Park, Il-Gu Lee

Department of Future Convergence Technology Engineering, Sungshin Women's University, South Korea

{220214013, 220214012, 220214014, 220214011, iglee}@sungshin.ac.kr

***Abstract*—The recent development of new and variant malicious codes, and the increase in cyberattacks in the form of intelligent Advanced Persistent Threat (APT), has led to rapidly increasing levels of damage. In particular, in the case of ransomware, the damage per attack is large, because ransomware uses a network propagation method, by which each attack can infect multiple victims. As ransomware as a service (RaaS) has increased recently, even people without the capacity to develop malicious code have become able to attack via ransomware. In this study, we built and experimented with a framework that detects ransomware in network and system environments using open-source tools. This study showed through analysis and experiments that open-source tools can quickly identify and respond immediately to APT attacks.**

***Keywords*—Open-source, Endpoint Detection and Response (EDR), Google Rapid Response, Open-source HIDS SECurity (OSSEC), osquery, Ransomware Detection**

I. INTRODUCTION

Due to the prolonged COVID-19 pandemic, remote work has become commonplace, and the number of industries using the Internet of Things (IoT) has increased, expanding the attackable area. Among the potential modes of attack, ransomware is widely used in crimes, because it can attack multiple people simultaneously through networks. Ransomware—a portmanteau of Ransom and Software—penetrates the system to be attacked, encrypts data, and then demands money from the victims in return for decryption. Attack types include penetrating the system to encrypt data, stealing confidential information, and blocking critical systems [1]. Starting with the infection of > 230,000 computers across 150 countries through encryption by "WannaCry" in 2017, ransomware has increased its attack success rate by utilizing new and modified malware and obfuscation techniques. Even attackers who cannot develop their own malware have recently used ransomware as their main means of attack, by licensing malware from hackers and sharing the profits obtained [2, 3]. According to Statista, the number of ransomware outbreaks worldwide in 2020 was around 340 million, up 61.8% from 2019 [4]. According to the Cyber Attack Trends 2021 Mid-year Report released by Checkpoint, the number of ransomware attacks in the first half of 2021 increased by about 93% over six months, and ransomware damage is rising rapidly [5]. Therefore, research into systems which can respond efficiently to cyberattacks is needed to respond to and minimize the damage caused by ransomware. The use of digital forensics technology is important to quickly detect and efficiently respond to intelligent and advanced cyberattacks. Among the digital forensic technologies, research into Endpoint Detection and Response (EDR), an approach which involves the analysis of a client's system event log to identify attacker intentions and respond immediately to attacks is underway [6]. An EDR tool connects a server to a client, allowing them to rapidly obtain client information from the server, and then analyze and respond to this information. This study used open-source EDR tools to analyze in real-time whether a client connected to an EDR server was infected with ransomware, and to check whether an attack could be detected based on this information. The experiments used File Finder [7], one of the flows of Google Rapid Response (GRR), an open-source EDR tool, Query's file-related query statement [8], and Open-source HIDS Security (OSSEC)'s integrity monitoring function [9] to analyze whether clients were infected with RAASNet [10], an open-source ransomware.

The contributions of this study are as follows.

- We propose a framework for detecting attacks using open-source tools in network and system environments.
- We confirmed that the proposed ransomware countermeasure method was feasible in a real system environment, by examining the characteristics of each open-source tool, selecting the tool's core function, and experimenting.

The rest of this paper is structured as follows: Section II introduces related research. Section III describes our experiments with ransomware detection in three open-source tools, and analyzes the results. Section IV describes a ransomware detection methodology for each open-source tool, and Section V provides the conclusions.

Manuscript received January 19, 2021. This work was partly supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1F1A1061107) and Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (P0008703, The Competency Development Program for Industry Specialist), and a follow-up of the invited journal to the accepted & presented paper entitled "Study on Systematic Ransomware Detection Techniques" of the 23th International Conference on Advanced Communication Technology (ICACT2021).

Sun-Jin Lee is with the Department of Future Convergence Technology Engineering, Sungshin Women's University, South Korea (e-mail: 220214013@sungshin.ac.kr)

Hye-Yeon Shim is with the Department of Future Convergence Technology Engineering, Sungshin Women's University, South Korea (e-mail: 220214012@sungshin.ac.kr)

Yu-Rim Lee is with the Department of Future Convergence Technology Engineering, Sungshin Women's University, South Korea (e-mail: 220214014@sungshin.ac.kr)

Tae-Rim Park is with the Department of Future Convergence Technology Engineering, Sungshin Women's University, South Korea (e-mail: 220214011@sungshin.ac.kr)

Il-Gu Lee is with the Department of Future Convergence Technology Engineering, Sungshin Women's University, South Korea (Corresponding Author phone: +82-2-920-7145; e-mail: iglee@sungshin.ac.kr)

II. Related Work

As the number of APT attacks such as ransomware increase exponentially, technologies to prevent and defend against such attacks are being actively studied.

A. Cyber Attack Detection

One study detected attacks using the characteristics of ransomware communication by analyzing the HTTP message sequence and content size of ransomware products [11]. In that paper, network communication results such as HTTP traffic attributes were observed using the representative ransomware families "CryptoWall" and "Locky," and a detection approach based on Proof of Concept Software Defined Network (SDN) was used. The system achieved a 97% detection rate, showing the feasibility of the approach. However, this approach had a limitation, in that the HTTP response size of the command and control server, which is mainly used for attacks, was not considered. This study differed from ours, in that it detected attacks based on network attribute information.

There have also been studies into systems that defend against attacks by analyzing the characteristics of the ransomware. Representative studies include the detection of Android malware by benchmarking the detection engines of Dr-Droid and Virustotal, open-source malware detection tools [12]. In this study, for malware based on adware, ransomware, scareware, and Short Message Service (SMS), Dr-Droid detected attacks with an accuracy of 79.06% and Virustotal's detection engine detected attacks with an accuracy of 98.7%. The work reported in this paper was similar to this study in that ransomware was detected, but it did not cover artifact information such as files or the time infected with each ransomware.

In some studies, attacks were detected by identifying suspicious behavior in event logs. A representative study related to a score-based anomaly detection technique at endpoints using the Local Outlier Factor (LOF) and Autoencoder [13]. This study used unsupervised learning to detect abnormal behavior as suspicious attacks after learning normal behavior. Suspicious behavior was identified by applying the allowed list operation policy, which resulted in 107 previously undetected suspected processes in LOF, 44 in AutoEncoder-based system behavior, and 24 in network behavior. However, it is difficult to filter all files using this study's proposed operational policy, and there was a limitation in that some false detection occurred because unsupervised learning was used.

B. Attack Detection Using Open-source EDR Tools

Recently, studies have used open-source EDR tools to detect malicious code. A representative study detected exploits using GRR [14]. In this paper, we studied a monitoring system which aimed to track attack threats, and demonstrated that two types of exposures could be detected. In controlled experiments, attacks due to vulnerabilities in FTP servers and Adobe Reader could be detected using GRR, and abnormal behavior of memory and networks was detected using Hunts among the GRR functions. This work demonstrated that cyberattacks are detectable by GRR tools, but there was a limitation, in that it could not determine how to detect cyberattacks using EDR tools other than GRR.

Another study was tested using osquery, flet, and elastic stack solutions, to demonstrate the effectiveness of open-source EDR systems in real-world environments [15]. In this study, various types of trojan attacks such as "Applejeus: Lazarus" and "jRAT/Adwind" were detected using open-source EDR, demonstrating their applicability in real-world environments. However, there was a limitation, in that it was not possible to confirm whether this approach was effective in all environments, because experiments were not conducted with attacks other than trojan horses.

A previous study evaluated the detectability of attacks using several types of open-source EDR tools [16]. In this study, we analyzed the EDR tools osquery, GRR, and Mozilla InvestiGator (MIG), which can detect attacks using real-time forensic functions. The three real-time forensic tools can collect information by processing vast amounts of data in real-time over a network, without turning off the power to a computer suspected of damage. In this study, three tools were evaluated for process creation, persistence, and network connection. It was possible to monitor the internal operations of the operating system using osquery, find attacked files using GRR and MIG, and detect attacks by searching for strings expected to be malware samples in the actual file content. The authors confirmed that MIG is useful, in that it can handle embedded systems, but was not sufficient to check the Windows registry. The use of osquery demonstrated that a system can be automatically monitored based on a variety of attributes and artifacts, along with the real-time investigation capabilities provided by GRR and MIG. By evaluating the possibility of detecting attacks at the level of process generation, persistence, and network connection among open-source EDR tools, this study attempted to demonstrate the value of the use of EDR tools for ransomware detection in network and system environments.

III. Open-source-based Ransomware Detection

A. Ransomware Detection Frameworks

In this study we used open-source EDR tools to detect when a device was infected by RAASNet, an open-source ransomware. At this time, the payload of ransomware generated by RAASNet is an "override and name" method. This is an attack that copies an existing file, changes the file extension to the .DEMON format, and then removes the existing file to prevent viewing or modifying the encrypted file. The following is a ransomware detection method for each of the representative open-source tools, GRR, osquery, and OSSEC.

1) Google Rapid Response

GRR is a framework for responding to infringement accidents, focusing on remote live forensics developed by Google.

A GRR server communicates with pre-registered clients using messages. A client communicates with a server using the HTTP protocol, and sends a batch of responses via periodic HTTP POST requests. The client generates a message queue based on the client's name, and then processes the responses in the queue. The client may only receive a request corresponding to its own queue, but may transmit a response to all worker queues. Communication between the server and client is encrypted using an RSA public key, signed using the sender's private key [17].

Table I summarizes the core functions provided by GRR.

TABLE I
KEY FEATURES OF GRR

Feature	Description
Cross-platform	Support for cross-platform Linux, OS X and Windows
Memory Analysis	Real-time remote memory analysis using YARA library
Can schedule action queries	Recurring tasks can be scheduled
Registry search function	Search and download capabilities for files and Windows registry
Large-scale host monitoring	Large-scale monitoring using the Hunt function

GRR can run on Linux, OS X (macOS), and Windows environments and enables real-time remote memory analysis using YARA, a tool designed to help malware researchers identify and classify malware samples. It is possible to automate the process using the reservation function for repeatedly performed Flow or Hunt. The user can also search for or download files and the Windows registry. Hundreds of digital forensic artifacts can be collected, and OS-level and native file systems are accessible using SleuthKit (TSK) [18].

In this study, queries about before and after the infection of the victim device systems were performed using File Finder, which can obtain information about files in specific memory spaces during the flow of the GRR server. Using this approach, changes in the file system were checked before and after their infection with ransomware.

2) osquery

osquery is a SQL-based operating system instrumentation, monitoring, and analysis framework developed by Facebook. It has a built-in SQL language and hundreds of tables, so it is effective at responding to incidents. There are two types of osquery: osqueryi and osqueryd. osqueryi is an interactive query console/shell that allows users to explore the state of the operating system through the shell without the need to communicate with a daemon or run as administrator. osqueryd is a host monitoring daemon that can schedule queries and record state changes in an operating system. The daemon aggregates query results over time and analyzes changes in the query's state. The OS event API can be used to log file or directory changes and hardware and network events [19].

Table II summarizes the core functions provided by osquery.

TABLE II
KEY FEATURES OF OSQUERY

Feature	Description
Cross platform	Can be built and used on a variety of OSs
Interactive Query Console	An interactive query console, osqueryi, provides a SQL interface for testing new queries and navigating the operating system.
Can schedule action queries	A high-performance host monitoring daemon osqueryd allows users to schedule queries that run across their infrastructure
Large-scale host monitoring	osqueryd's logging is tech stack-agnostic thanks to its powerful plugin architecture. It can be integrated into the existing internal log aggregation pipeline.

osquery can run in the Windows, OS X, Linux, and FreeBSD environments, and manages the operating system as an interactive query console and relational database. Large-scale environmental monitoring is possible using various plug-in functions.

In this study, all files in the victim's infected memory space were queried using the file query statement of osqueryi. As with GRR, queries were performed before and after ransomware infection to investigate changes in the file system before and after infection.

3) Open-source HIDS SECurity (OSSEC)

OSSEC is an open-source host-based intrusion detection system that allows administrators to monitor information on agents, syslogs, databases, and agentless devices. OSSEC's agent uses UDP communication, collects information, and forwards information to administrators for analysis. At this time, some information is collected in real time and some is collected periodically [20]. In the absence of an agent, it is possible to monitor firewalls, routers, and Unix systems for agentless devices.

Table III summarizes the core functions provided by OSSEC.

TABLE III
KEY FEATURES OF OSSEC

Feature	Description
Cross platform	Can be built and used on a variety of OSes
File Integrity Check	Detect system changes in real-time to files and Windows registry settings, maintain and manage forensic copies of data
Log monitoring	Monitoring and analysis of multiple log data in real time
Rootkit detection	Process and file-level analysis to detect malicious applications and rootkits
Active response	Real-time response to attacks and changes to systems through firewall policies, integration with third parties such as Content Delivery Networks (CDNs) and support portals, and multiple mechanisms

OSSEC provides comprehensive host-based intrusion across multiple platforms, including Linux, Solaris, Advanced Interactive eXecutive (AIX), Hewlett Packard Unix (HP-UX), Berkeley Software Distribution (BSD), Windows, Mac, and VMware Elastic Sky X (ESX). OSSEC enables real-time change history management of files and Windows registry settings, and specializes in analyzing logs in real time. Various policies can be used to respond to attacks or changes, and users can set alert rules according to their security requirements, enabling the performance of customized actions when an alert occurs.

In these experiments, changes to the ransomware-infected files were detected using the integrity check, which is a function of OSSEC; it sets the space to be checked for integrity in an OSSEC configuration, and detects encryption and file extension changes that exist in the memory space.

B. Experimental Environment

The environment was configured by dividing the server and the client to be attacked. An open-source EDR (GRR, osquery, and OSSEC) system was built on the server, and each client version of the open-source EDR was installed on the client before the files were attacked.

Table IV summarizes the components and versions of the environment used in the experiment.

TABLE IV
COMPONENTS AND VERSIONS USED TO BUILD THE EXPERIMENTAL ENVIRONMENT

Component	Version
CPU	Intel® Core™ i7 Processor 10700K @ 3.80 GHz
RAM	32.0 GB
Server, Client (agent) OS	Ubuntu 18.04.4 LTS
RAASNet	https://github.com/leonv024/RAASNet
GRR	3.4.0-1
osquery	3.1.0
OSSEC	4.3.0

The CPU was Intel's i7 10th generation, and Ubuntu 18.04.4 LTS version was used for the OS in each server and client. The software used was GRR 3.4.0-1, osquery 3.1.0, and OSSEC version 4.3.0.

C. Experimental Process

1) Google Rapid Response

For the experiments, each victim was registered in the GRR Server in advance so that it could be managed as a single agent. Figure 1 shows the attack detection process using GRR.

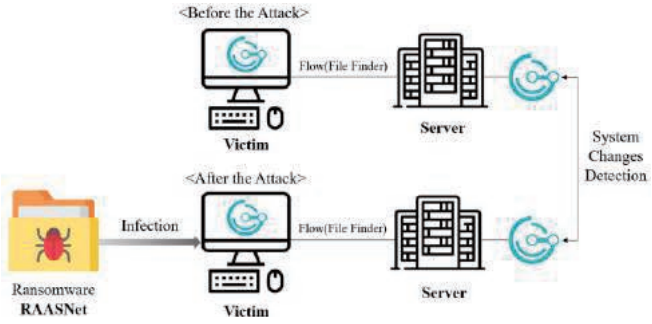


Fig. 1. Configuration of the Google Rapid Response (GRR) experiment environment.

Typical tasks provided by GRR include Flow and Hunt. Flow is a logical collection unit that achieves a given goal in the server and client, and Hunt is a Flow experimental mechanism optimized for a large number of systems. Hunt is used to search for and monitor specific data in a large-scale system, and Flow is used for general experiments. In this experiment, attacks were detected using File Finder during Flow. The attacker attacked a specific folder in the file system of the victim PC registered as a GRR client, and the GRR Server sent a query to the infected system to compare the query results before and after the attack.

2) osquery

The experiments were carried out by installing osquery on a victim system. Figure 2 shows the attack detection process using osquery.

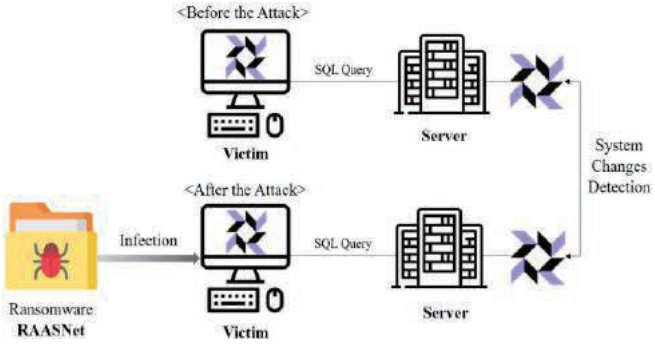


Fig. 2. Configuration of the osquery experiment environment.

In osquery, SQL queries can be written to check and compare data from the operating system. Using a SQL table, it is possible to detect running processes, changes in the hash value of a file, changes in network connections, and other information. osqueryi, an interactive query console, enables incident response, system operation problem diagnosis, and the identification of the causes of performance problems.

In the experiments, we queried osqueryi for file properties in the victim's target folder, and compared the SQL table values before and after infection with RAASNet. We used 'Select * from file WHERE path like "/home/osquery1/target/%"', compared the results using a query, and analyzed the results to check whether the files were infected with ransomware.

3) Open-source HIDS SECurity (OSSSEC)

For the experiments, the victim was registered as an agent in the OSSEC server and system changes were monitored based on the registered ID. Figure 3 shows the attack detection process using OSSEC.

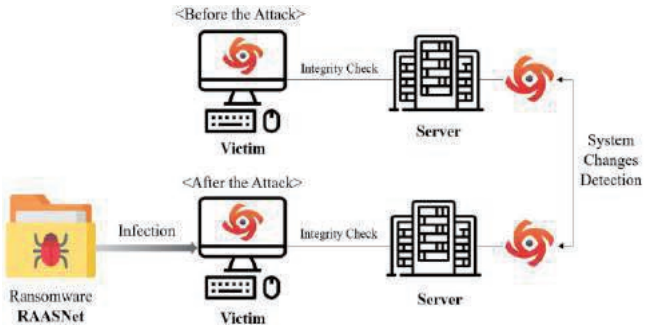


Fig. 3. Configuration of the Open-source HIDS SECurity (OSSEC) experiment environment.

OSSEC allows users to customize alert rules to meet their security requirements by modifying configuration options. In this experiment, OSSEC's integrity check function was used to detect RAASNet ransomware. The rules for the integrity check were set in the OSSEC configuration, and the monitoring results were checked and compared before and after the attack to determine the ransomware infection status.

D. Experimental Results

To confirm the detection of ransomware, detection was carried out separately before and after RAASNet was executed. For the experiments, 10 MS Office Presentation files, 10 MS Office Word files, and 10 MS Office Excel files were created in a target folder.

1) Google Rapid Response

Figures 4 and 5 show the flow results for one file in the target folder before and after executing RAASNet using GRR File Finder. Checking the experimental result revealed that the atime, mtime, and ctime of the target files in target_folder had changed.

Atime is an abbreviation of last access time, meaning the previous time the file was accessed. The atime value changes when a file is opened or read by a command such as cat or vi. mtime is an abbreviation of last modification time, which means the last time the file was modified. The mtime value is updated when the file contents are added or the file size changes. Ctime is an abbreviation of inode change time, and indicates the last change time of a file. When changing the permission of a file using chmod or changing the owner of a file via chown, the ctime also changes while the permission information is updated in the inode, and ctime is affected when creating or deleting hard links. Unlike atime and mtime, ctime has the characteristic that it cannot be changed with the touch command. When changing data contents, both mtime and ctime are changed.

When the victim's file was encrypted using RAASNet, atime, mtime, and ctime all changed.

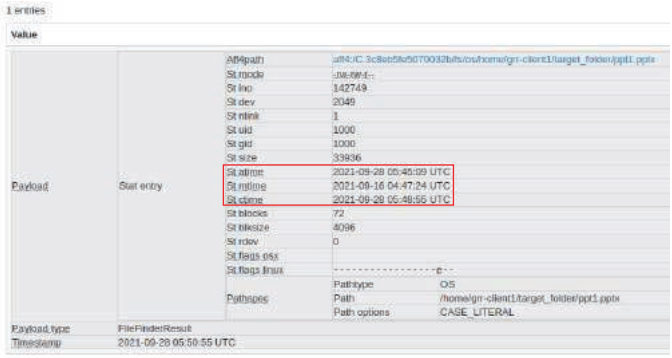


Fig. 4. Results of Google Rapid Response File Finder Flow before running RAASNet.

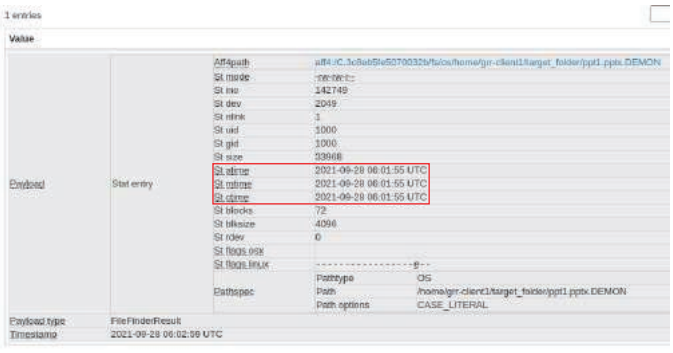


Fig. 5. Results of Google Rapid Response File Finder Flow after running RAASNet.

2) osquery

Figures 6 and 7 show the query results before and after executing RAASNet using osqueryi, and an analysis of whether the files in the target folder are infected. After executing RAASNet, we used select * from the file with a path like "/home/osquery1/target/%". When the query was executed, it was confirmed that the name and file size of the ppt1.pptx file, one of the target files, and the atime, mtime, and ctime properties of the file, were changed. As the ransomware RAASNet was executed by targeting the victim's folder, the files in the osquery1 directory were encrypted and detailed properties of the file system changed.

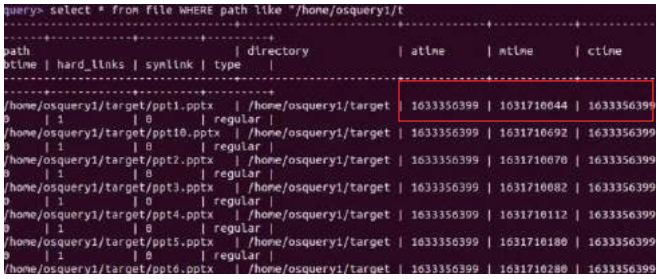


Fig. 6. Results of osqueryi before RAASNet execution.

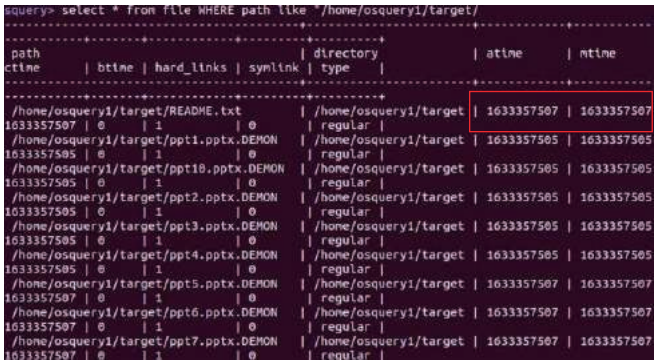


Fig. 7. Results of osqueryi after RAASNet execution.

3) Open-source HIDS SECurity (OSSEC)

OSSEC provides real-time monitoring capabilities. In these experiments, modifying the ossec.conf file changed the detection time in real time, and the detection range was changed to the target folder range. Using a dump of the database and integrity checking on the administrator screen, the status of files in the target folder could be checked, as shown in Figure 8. After RAASNet was infected and the monitoring results were observed through database dumping, it was confirmed that a file was created, as shown in Figure 9, and that the file name and file hash value were changed.

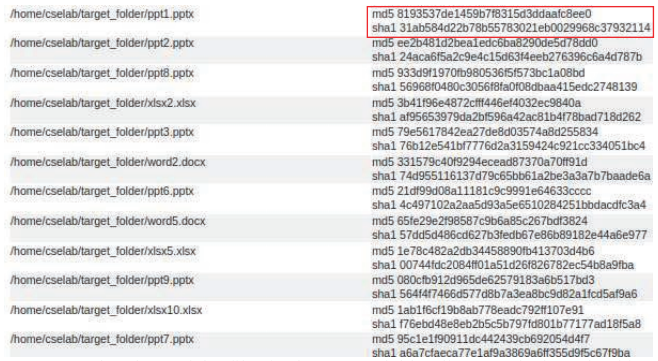


Fig. 8. Hash values of the files in the target_folder directory before checking RAASNet execution using Open-source HIDS SECurity (OSSEC)

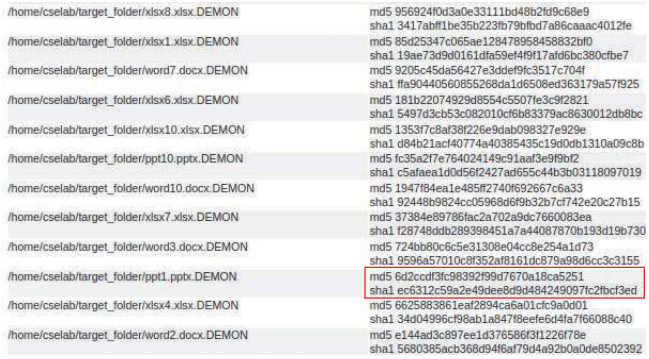


Fig. 9. Hash values of the files in target_folder directory after checking RAASNet execution using Open-source HIDS SECurity (OSSEC).

IV. Analysis of Experimental Results

In this study, we confirmed the ability of open-source EDR to detect when the target PC was infected with ransomware. For GRR, Flow's File Finder was used. Attacks could be detected by the changes to the target file name and the file's atime, mtime, and ctime properties. In the case of osquery, the file system of the target PC could be checked using the query statement provided by itself, and at tacks could be detected by changes to the target file name and the atime, mtime, and ctime file properties. In the case of OSSEC, the integrity check function was used among the constant monitoring functions provided, and attacks could be detected by changing the file name and hash value. Table V shows the functions, methods, and results of ransomware attack detection by the open-source tools used in this study.

By utilizing the key features of each open-source EDR tool, it was possible to quickly detect various cyberattacks, including ransomware. As shown in Table V, GRR can check condition changes such as the name of the attack target file and the atime, mtime, and ctime properties using the file finder among the filesystems in the flow it provides. In the case of osquery, it was possible to recognize changes in atime, mtime, and ctime in the file system by querying a database that is updated in real-time for information about the target file. OSSEC uses its own real-time integrity monitoring function to check changes in the attack target file by changing the hash value, such as md5 or sha1, of each attack target file. All three open-source tools detect attacks by changing the environment of the ransomware-infected system, and when a file's hash value and file attribute values change suddenly, it is judged as abnormal behavior and can prompt a real-time response.

V. Conclusions

As cyberattacks increase and spread, it is essential to quickly detect and take action when attacks occur, to minimize damage to the system. Therefore, it is necessary to introduce tools and information collection systems that can detect attacks in real-time.

In this study we analyzed the unique characteristics and functions of each EDR tool. The target PC's file system was attacked using RAASNet, an open-source ransomware. The possibility of attack detection in open-source EDR was confirmed using GRR, osquery, and OSSEC.

The results of these experiments show that GRR detects attacks through a file finder that can check for file changes during flow, osquery detects attacks through a query statement that detects system changes, and OSSEC detects attacks through a constant monitoring system.

This paper demonstrates the potential of detecting attacks and warning users in the form of logs or alerts. In a follow-up study, we plan to check the detection efficiency of each open-source EDR tool in a large-scale environment, and determine the scope of the response.

Table V
Analysis of Ransomware Detection Methods Using Open-source Tools

Open-source software	Detection Function	Detection Section	Detection Method	Detection Result
GRR	File System Changes	File Finder	Select * from file where path like "/target directory/%";	Filename, Atime, Mtime, Ctime
osquery		SQL Query		
OSSEC		Integrity Check	Database Dumping	Hash(md5, sha1)

REFERENCES

1. S. Aurangzeb, M. Aleem, M. Iqbal, and A. Islam, "Ransomware: A Survey and Trends," *Journal of Information Assurance and Security*, Vol. 6, No. 12, pp. 48–58, 2017.
2. O. Aslan and R. Samet, "A Comprehensive Review on Malware Detection Approaches," *IEEE Access*, vol. 8, pp. 6249–6271, 2020.
3. P. H. Meland, Y. F. F. Bayoumy, and G. Sindre, "The Ransomware-as-a-Service economy within the darknet," *Computers & Security*, vol. 92, 2020.
4. "Annual number of ransomware attacks worldwide from 2016 to 2020" Statista. [Online]. Available: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/. [Accessed: 12-Nov-2021].
5. "Cyber Attack Trends – 2021 Mid Year Report" Check Point Research. [Online]. Available: https://research.checkpoint.com/2021/check-point-softwares-mid-year-attack-trends-report-reveals-a-29-increase-in-cyberattacks-against-organizations-globally/. [Accessed: 12-Nov-2021].
6. W. U. Hassan, A. Bates, and D. Marino, "Tactical Provenance Analysis for Endpoint Detection and Response Systems," *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 1172–1189, 2020.
7. "GRR Flows," GRR Flows - GRR documentation. [Online]. Available: https://grr-doc.readthedocs.io/en/v3.2.1/investigating-with-grr/flows/what-are-flows.html. [Accessed: 10-Nov-2021].
8. "Anomaly detection with osquery," osquery. [Online]. Available: https://osquery.readthedocs.io/en/stable/deployment/anomaly-detection/. [Accessed: 10-Nov-2021].
9. "Syscheck," OSSEC. [Online]. Available: https://www.ossec.net/docs/docs/manual/syscheck/index.html. [Accessed: 10-Nov-2021].
10. leonv024, "leonv024/RAASNet," GitHub. [Online]. Available: https://github.com/leonv024/RAASNet. [Accessed: 10-Nov-2021].
11. K. Cabaj, M. Gregorczyk, and W. Mazurczyk, "Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics," *Computers & Electrical Engineering*, vol. 66, pp. 353–368, 2018.
12. Samara, M., & El-Alfy, E.-S. M., "Benchmarking Open-Source Android Malware Detection Tools," *2019 2nd IEEE Middle East and North Africa COMMunications Conference (MENACOMM)*. 2019. doi:10.1109/menacomm46666.2019.8988
13. Kim, Sujeong & Hwang, Chanwoong & Lee, Taejin, "Anomaly Based Unknown Intrusion Detection in Endpoint Environments," *Electronics*. 9. 1022. 2020. 10.3390/electronics9061022.
14. H. Rasheed, A. Hadi, and M. Khader, "Threat Hunting Using GRR Rapid Response," *2017 International Conference on New Trends in Computing Sciences (ICTCS)*, pp. 155–160, 2017.
15. Christopher Hurless, "Exploring Osquery, Fleet, and Elastic Stack as an Open-source solution to Endpoint Detection and Response," *SANS Institute Reading Room site*, 2019. Available: https://www.sans.org/reading-room/whitepapers/detection/paper/39165. [Accessed: 11-Nov-2021].
16. Kieseberg, Peter & Neuner, Sebastian & Schrittwieser, Sebastian & Schmiedecker, Martin & Weippl, Edgar. (2018). Real-Time Forensics Through Endpoint Visibility. 10.1007/978-3-319-73697-6_2.
17. M.I. Cohen, D. Bilby, G. Caronni, "Distributed forensics and incident response in the enterprise," *Digital Investigation*, Volume 8, Supplement, Pages S101-S110, ISSN 1742-2876, 2011. https://doi.org/10.1016/j.diin.2011.05.01
18. "What is GRR?" GRR. [Online]. Available: https://grr-doc.readthedocs.io/en/latest/what-is-grr.html [Accessed: 7-Dec-2021]
19. "Welcome to osquery" osquery. [Online]. Available: https://osquery.readthedocs.io/en/stable/. [Accessed: 11-Nov-2021].
20. "OSSEC Architecture" OSSEC. [Online]. Available: https://www.ossec.net/docs/docs/manual/ossec-architecture.html. [Accessed: 11-Nov-2021].

Sun-Jin Lee was born in Korea in 2000. She is a student of the Integrated B.S./M.S. course in the Department of Convergence Security Engineering in Sungshin Women's University, Seoul, Korea. Her current research interests are in the area of deep learning, Internet of Things, malware detection, voice security, image security, and video security.

Hye-Yeon Shim was born in Korea in 2000. She is a student of the Integrated B.S./M.S. course in the Department of Convergence Security Engineering in Sungshin Women's University, Seoul, Korea. Her current research interests are in the area of artificial intelligence, deep learning, malware detection, and programming.

Yu-Rim Lee was born in Korea in 1999. She is a student of the Integrated B.S./M.S. course in the Department of Convergence Security Engineering in Sungshin Women's University, Seoul, Korea. Her current research interests are in the area of artificial intelligence, threat defense, malware detection, and Internet of Things.

Tae-Rim Park was born in Korea in 1999. She is a student of the Integrated B.S./M.S. course in the Department of Convergence Security Engineering in Sungshin Women's University, Seoul, Korea. Her current interests are in the areas of artificial intelligence, network security, malware detection, cloud computing, and Internet of Things.

Il-Gu Lee was born in Korea in 1978. He received his PhD degree in the Graduate School of Information Security in Computer Science & Engineering Department from KAIST at 2016. He is a professor at the Department of Convergence Security Engineering, Sungshin Women's University, Seoul, Korea. His current research interests are in the area of wireless/mobile networks with an emphasis on information security, networks, and wireless systems.

Dimension Dependent Effective Index Analysis for a Nano-scale Silicon Waveguide in Transverse Mode

A. T. C. Chen*, R. Petra*, K. S. K. Yeo* and M. Rakib Uddin**

* *Electrical and Electronic Engineering Programme Area, Faculty of Engineering, Universiti Teknologi Brunei (UTB), Gadong, Brunei Darussalam*

** *The State University of New York Research Foundation, State University of New York Polytechnic Institute, Fuller Road, Albany, New York 12203*

angie_teo236@hotmail.com, rafidah.petra@utb.edu.bn, kenneth.yeo@utb.edu.bn, mmrakib@yahoo.com

***Abstract*—In this paper, we propose and demonstrate the effect of effective index on silicon waveguide dimensions by using MODE solution. The objective of this paper is to study the effect of effective index which is influenced by waveguide width variations and waveguide height variations. The effect of effective index variations is presented by fixing the core height at 200nm and varying the core width from 300nm to 600nm and by fixing the core width at 500nm and varying core height from 150nm to 300nm for Transverse Electric (TE) and Transverse Magnetic (TM) MODE. With the simulation results, the thickness of the core width and core height are used for the determination of fundamental or higher order mode design. It is seen that higher effective index can be achieved as the core width and core height increases. The determination of fundamental or higher order mode design can be achieved by analyzing the graphs of effective indices for TE0, TM0, TE1 and TM1 modes at varied core height and width. Based on the analysis, it is concluded that fundamental order can only be achieved when the silicon core width is kept at a value of approximately 500nm and core height is kept at a value of less than 250nm. At a higher order mode, excess noise and losses can be introduced.**

Keyword— Core Height, Core Width, Effective Index, Rib Waveguide and Silicon

Manuscript received on Jan. 10, 2021. This work is supported by UTB Scholarship Award and is a follow-up of the invited journal to the accepted & presented paper entitled "Transverse Electric (TE) and Transverse Magnetic (TM) Modes Dependent Effective Index Analysis for a Nano-scale Silicon Waveguide" of the 23rd International Conference on Advanced Communication Technology (ICACT2021).

Angie Teo Chen Chen is a Ph.D. student in the Department of Electrical and Electronic Engineering at University of Teknologi Brunei (UTB). (Corresponding author, phone: +673 8666643, fax: +673 2461035/6, email: angie_teo236@hotmail.com).

PG DR Rafidah Pg Hj Petra is currently a professor in the Department of Electrical and Electronic Engineering, Faculty of Engineering, at University of Teknologi Brunei (UTB), Brunei Darussalam. (Phone: +673 8757108, fax: +673 2461035/6, email: rafidah.petra@utb.edu.bn).

DR.Kenneth Siok Kiam Yeo is currently a professor in the Department of Electrical and Electronic Engineering, Faculty of Engineering, at University of Teknologi Brunei (UTB), Brunei Darussalam. (Phone: +673 8963788, fax: +673 2461035/6, email: kenneth.yeo@utb.edu.bn).

DR. M. Rakib Uddin is currently a Research Engineer at the State University of New York Polytechnic institute, Albany, New York, USA. (Phone: +1 (404) 903-3312, fax: +673 2461035/6, email: mmrakib@yahoo.com).

I. Introduction

In recent past, silicon photonics has been one of the most fascinating topics in the communication sector where tremendous impacts have been realized by utilizing Silicon-On-Insulator (SOI) platform with very thin top layer of silicon [1-3].

Silicon waveguides based on Silicon-on-Insulator (SOI) platform have become the famous research field in the interest of their high capability in optoelectronic circuits. SOI technology is a good choice for optical waveguiding owing to its very high index contrast between silicon and silicon dioxide [4-6]. With high index contrast, the fabrication of dimensions of a few μm × μm ultracompact silicon photonic devices and circuits can be achieved [7-9]. The most standard design of single mode SOI nanowire is that it has a cross section of approximately 500nm x 220nm [1]. It is well-known that effective index is one of the most significant characteristics in silicon waveguides especially in designing of optical system as it determines the propagation constant of optical field although, more essentially, in high-speed communication in which dispersion might be a limiting factor [4]. Usually, TE-polarization mode is used in this design as it has a stronger confinement of light compared to TM-polarization mode. Therefore, small bending radii can be achieved which lead to the fabrication of ultra-compact devices. Optical waveguide such as SOI based platform waveguide is acknowledged as the most extensive bridging element in optical integrated devices [10 and 11]. Therefore, a low loss optical waveguide is important in the design and fabrication of reliable and effective optical communication system. Low loss optical waveguides can be attained by applying or varying various parameters.

II. Theory for Rib Waveguide

To the greatest extent, Silicon waveguides based on SOI platform can be easily built from SOI wafers as shown in Figure 1 by employing Complementary Metal-Oxide Semiconductor (CMOS) processes [12].

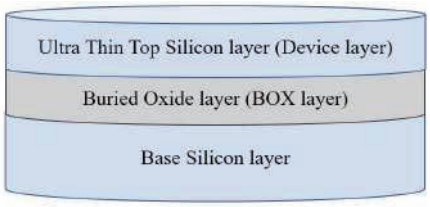


Fig. 1. SOI wafers.

A standardized SOI wafers are made up of a layer of buried oxide (BOX) centrally located to an ultra-thin top silicon layer and base silicon layer. The techniques used to design Silicon-based type waveguides are optical lithography and etching process [12]. In an SOI based-type waveguide, guiding of light will occurs in the core of silicon in which it is separated from the silicon substrate by a layer of silicon oxide that acts as lower cladding [13]. An example of the commonly used waveguide is the rib waveguide in which the geometry of the waveguide is shown in Figure 2.

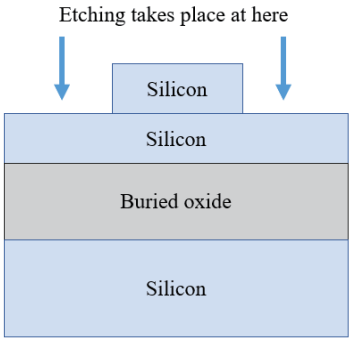


Fig. 2. The geometry of rib-type based waveguide on SOI platform.

III. PROPOSED DESIGN OF RIB TYPE WAVEGUIDE

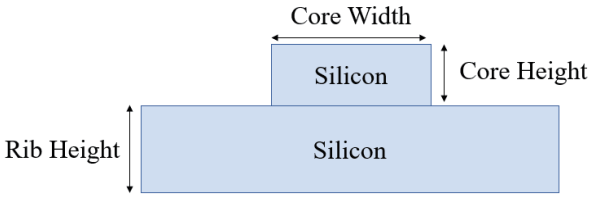


Fig. 3. Cross section of core section of the rib waveguide.

A cross section diagram of core part of the rib waveguide is shown in Figure 3. This paper is divided into two sections. In the first section, the core of the rib waveguide is designed to be in a fixed height of 200nm, a fixed rib height of 50nm and varied core width from 300nm to 600nm at the steps of 100nm. Next, the core of the rib waveguide is designed at a fixed core width of 500nm, a fixed rib height of 50nm and varied core height from 150nm to 300nm at the steps of 50nm.

IV. SIMULATION AND RESULTS ON VARIED WIDTH

In this work, the cross-section rib-type based waveguide is simulated by using MODE solution to generate the waveguide characteristics such as effective index for different polarization mode. The mode profile of core waveguide for the first section are shown in Figure 4 to Figure 7, respectively in which the height of the core is at a fixed value of 200nm with varied width from 300nm to 600nm.

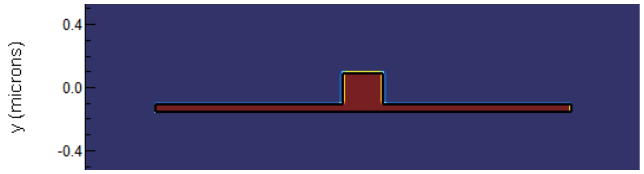


Fig. 4. Mode profile at core height of 200nm and core width of 300nm.

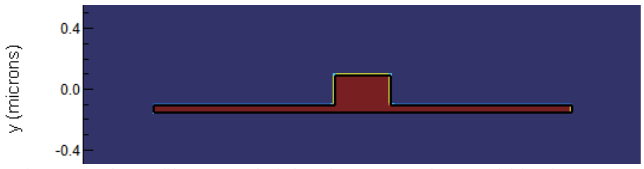


Fig. 5. Mode profile at core height of 200nm and core width of 400nm.

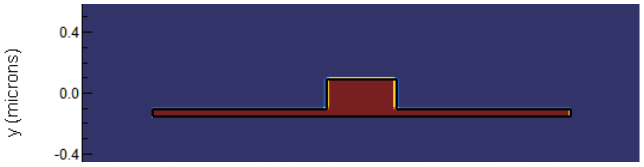


Fig. 6. Mode profile at core height of 200nm and core width of 500nm.

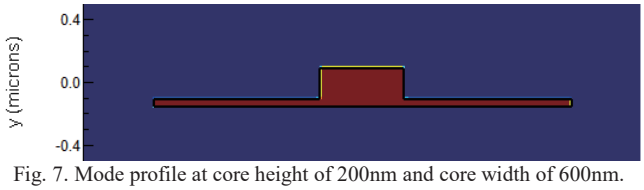


Fig. 7. Mode profile at core height of 200nm and core width of 600nm.

Figures 8 to 11 show the graphs of effective index at a fixed height of 200nm with varied width from 300nm to 600nm. The characteristic performance in terms of effective index have been noticed at core width of 300nm, 400nm, 500nm and 600nm. From the results, it is clearly shown that as the wavelength increases, effective index also increases for the 4 modes. It is also noticed that core waveguide width variations will have impacts on effective index. Thus, based on the results, it is deduced that effective index increases gradually as we increased the width of the core.

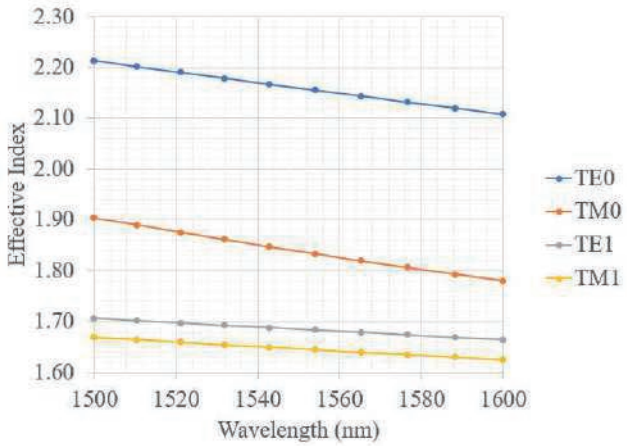


Fig. 8. Graphs of Effective index at height of 200nm with width of 300nm for 4 modes.

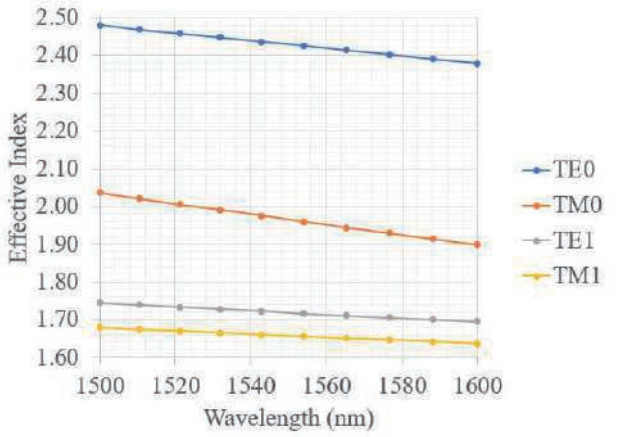


Fig. 9. Graphs of Effective index at height of 200nm with width of 400nm for 4 modes.

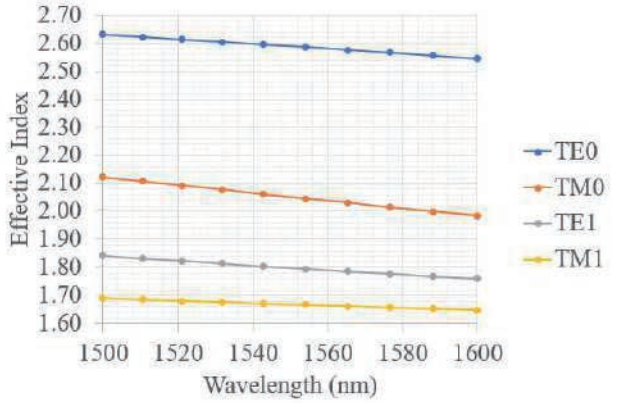


Fig. 10. Graphs of Effective index at height of 200nm with width of 500nm for 4 modes.

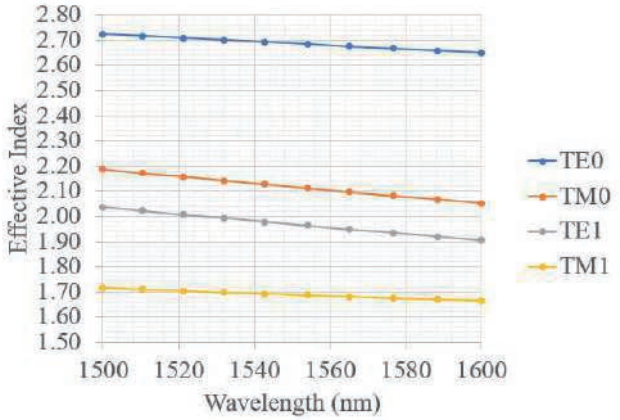


Fig. 11. Graphs of Effective index at height of 200nm with width of 600nm for 4 modes.

Based on the graphs of the effective index for dimension variables, the value of the effective index at λ = 1550nm for core height of 200 nm are deduced, tabulated, and shown in Table I. Accordance with the results, graphs of effective indices for 4 modes with respect to the varied core width to core height of 200nm are shown in Figure 12.

TABLE I
EFFECTIVE INDEX AT WAVELENGTH OF 1550NM FOR CORE HEIGHT OF 200NM WITH VARIED CORE WIDTH

Width of the Core (nm)	Effective index at λ = 1550nm for TE and TM Mode			
	TE0	TM0	TE1	TM1
300	2.16	1.83	1.68	1.64
400	2.42	1.96	1.72	1.66
500	2.58	2.05	1.80	1.67
600	2.68	2.11	1.96	1.69

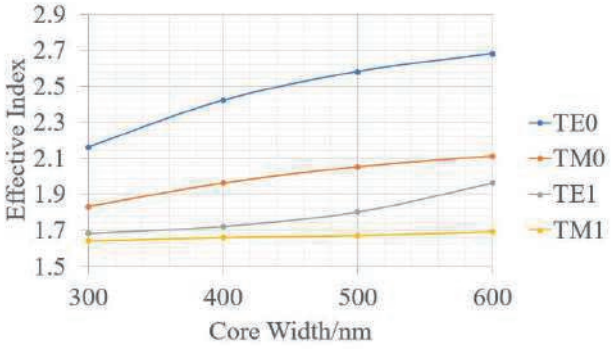


Fig. 12. Effective indices for TE0, TM0, TE1 and TM1 modes at core height of 200nm with width variation.

Based on the results shown in Figure 12, it is observed that as the silicon core width is made thicker, the effective index will increase. But if the silicon core width is made thinner, it is seen that effective index will eventually become smaller. Whereas for core height variations, it is noticed that thicker height will lead to higher effective index. As seen from the graph, it can be deduced that a width of 500nm is recommended when designing the waveguide. This is because when the width of the core is more than 450nm, it is observed that the effective index for higher order (TE1) mode gradually increases. Thus, the waveguide is said to be multimode and supports not only the fundamental mode but also higher order modes. At higher order mode, more noise and losses will be obtained. Thus, it is recommended that the silicon core width is set to be around 500nm to achieve a fundamental mode design which include TE0 and TM0 modes only.

In addition to that, the percentage change in effective index of each width with respect to 500nm for the TE0 mode is calculated and recorded in Table II as referred to Table I.

TABLE II
PERCENTAGE CHANGE IN EFFECTIVE INDEX OF EACH WIDTH WITH RESPECT TO 500NM FOR TE0 MODE

Width of Core (nm)	Percentage Change (%)
300	-16.3
400	- 6.20
500	0
600	+3.88

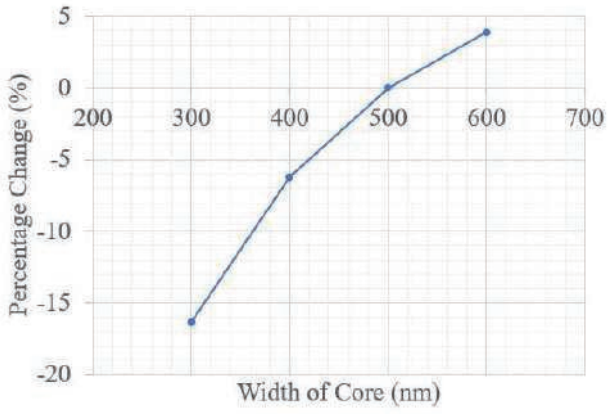


Fig. 13. Percentage Change in effective index of each width with respect to 500nm for TE0 mode.

In terms of effective index, higher effective index will lead to highest confinement of light and thus it is deduced that effective index is at the highest at core width of 600nm. In accordance with the analysis using the width of ± 100nm and -200nm from 500nm, it can be deduced that it is better for the design to have a core height of between 400nm to 500nm rather than more than 500nm as the balanced of high effective index and single order mode are maintained.

V. SIMULATION AND RESULTS ON VARIED HEIGHT

The mode profile of core waveguide for the next section are shown in Figure 14 to Figure 17, respectively in which the core width is fixed at 500nm with variation of height from 150nm to 300nm.

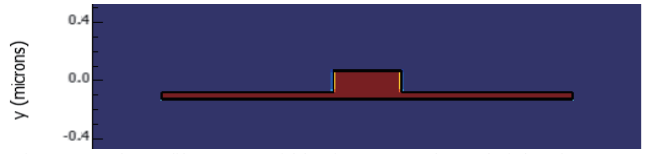


Fig. 14. Mode profile at core width of 500nm and core height of 150nm.

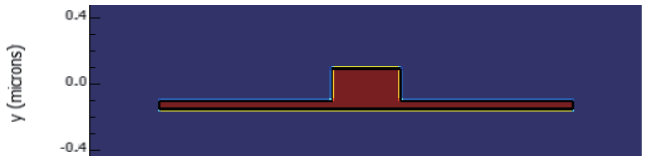


Fig. 15. Mode profile at core width of 500nm and core height of 200nm.

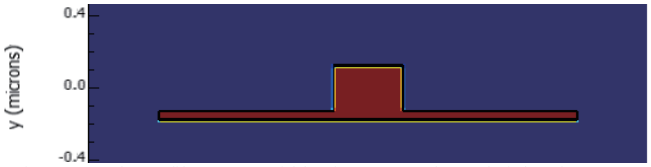


Fig. 16. Mode profile at core width of 500nm and core height of 250nm.

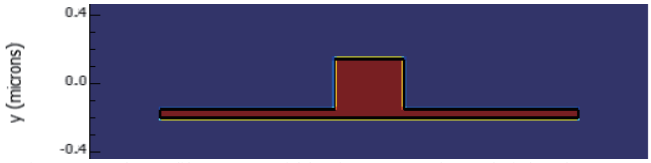


Fig. 17. Mode profile at core width of 500nm and core height of 300nm.

From there on, with fixed core width of 500nm, the core height of the waveguide is varied and the performances of various angle on fundamental and higher order mode effective index are observed and analyzed. The characteristic performance in terms of effective index has been noticed at core height of 150nm, 200nm, 250nm and 300nm. Based on the results, it is noticeable that effective index increases as wavelength increases. Furthermore, it is deduced that effective index increases with increased height.

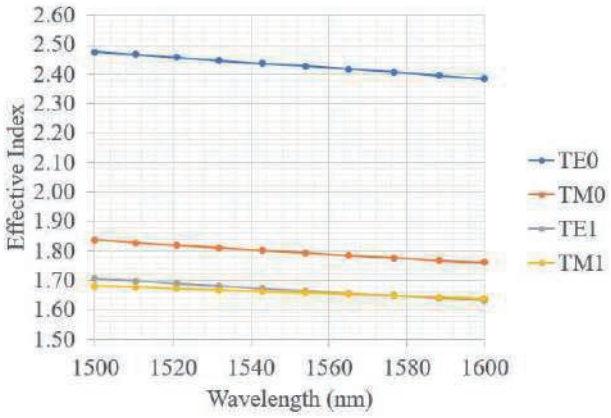


Fig. 18. Graphs of Effective index at width of 500nm with height of 150nm for 4 modes.

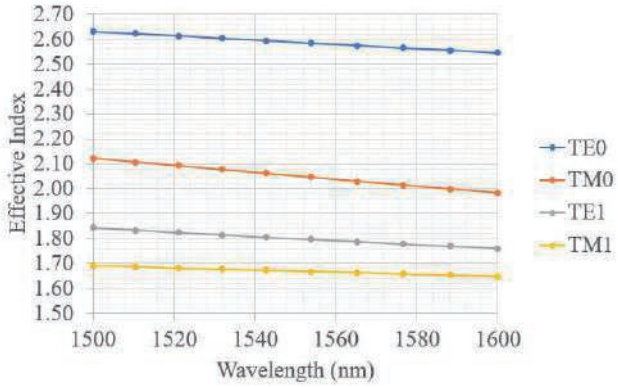


Fig. 19. Graphs of Effective index at width of 500nm with height of 200nm for 4 modes.

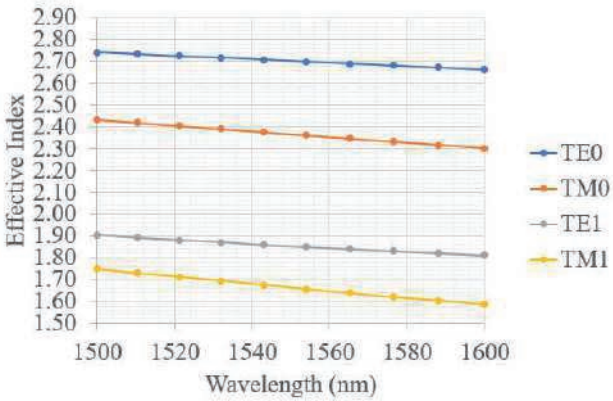


Fig. 20. Graphs of Effective index at width of 500nm with height of 250nm for 4 modes.

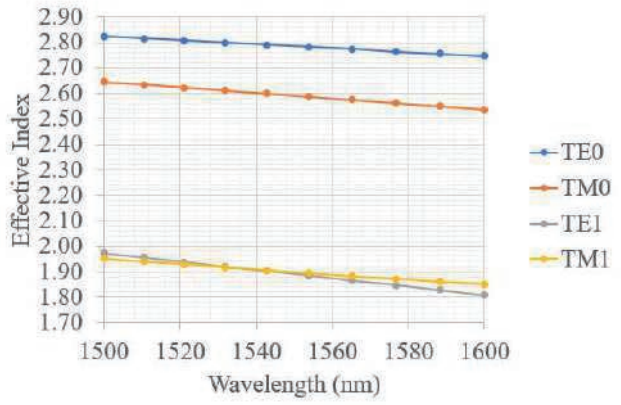


Fig. 21. Graphs of Effective index at width of 500nm with height of 300nm for 4 modes.

Based on the outcome results, summary of effective indices for TE0, TM0, TE1 and TM1 modes at fixed core width of 500nm over a range of core height dimensions is shown in Figure 22. Comparisons showing how polarization modes affect effective index as we varied core height from 150nm to 300nm are summarized, tabulate and shown in Table III.

TABLE III
EFFECTIVE INDEX AT WAVELENGTH OF 1550NM FOR CORE WIDTH OF 500NM WITH VARIED CORE HEIGHT

Height of the Core (nm)	Effective index at λ = 1550nm for TE and TM Mode			
	TE0	TM0	TE1	TM1
150	2.43	1.79	1.66	1.66
200	2.58	2.05	1.8	1.67
250	2.7	2.36	1.85	1.66
300	2.78	2.59	1.88	1.89

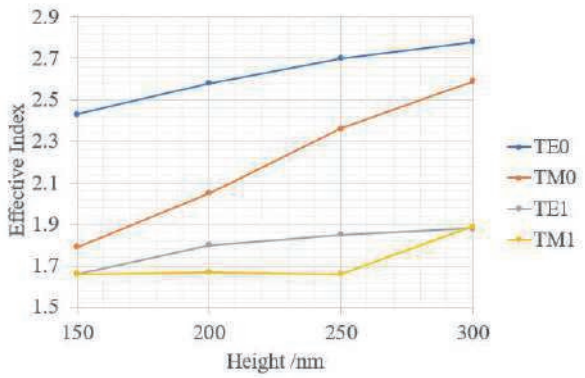


Fig. 22. Effective indices for TE0, TM0, TE1 and TM1 modes at core width of 500nm with height variation.

Based on the results shown in Figure 22, it is observed that effective index is inversely proportional to wavelength. Hence, as wavelength increases, effective index will decrease for all of the modes. In addition to that, with regards to core height, it is deduced that effective index increases with increased height.

From the simulation results shown, it is observed that as we increase the core height of the waveguide, the waveguide is said to be in higher order mode instead of fundamental mode only. It is also noticed that the effective index at fundamental mode is higher as compared to higher-order mode. Thus, it is deduced that the core height is recommended to be lesser than 250nm when designing waveguide as multi-order mode will come in if the core width is higher than 250nm. Higher-order mode will tend to introduce some excess loss and crosstalk, therefore only fundamental mode is preferred. In consequence, the dimension of the waveguide needs to be carefully designed to prevent the excitation of higher order mode.

Moreover, the percentage change in effective index of each height with respect to 250nm for the TE0 mode is calculated and recorded in Table IV as referred to Table III.

TABLE IV
PERCENTAGE CHANGE IN EFFECTIVE INDEX OF EACH HEIGHT WITH RESPECT TO 250NM FOR TE MODE

Height of Core (nm)	Percentage Change (%)
150	-10.0
200	-4.44
250	0
300	+2.96

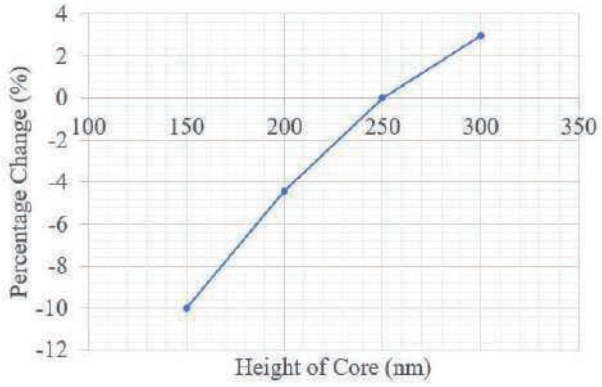


Fig. 23. Percentage Change in effective index of each height with respect to 250nm for TE0 mode.

In terms of effective index, higher effective index will lead to highest confinement of light and thus it is deduced that effective index is the highest at core height of 300nm. Based on the analysis using the height of ± 50nm and -100nm from 250nm, it can be deduced that it is better for the design to have core height between 200nm to 250nm rather than more than 250nm as the balanced of high effective index and single order mode are maintained.

VI. CONCLUSION

The simulation and analysis of the performance of polarization modes for a nano-scale silicon rib waveguide with respect to the dimensions of the waveguide have been presented. The performances of the polarization modes (fundamental mode and higher order mode) are observed and analyzed by using effective index. The study and analysis of polarization modes is to avoid the excitation of higher order modes that can cause excess loss and crosstalk. From the results, it is worth noting that as core width and core height increases, effective index also increases. Thus, it is said that core width and core height is directly proportional to the effective index. From this analysis, it is concluded that silicon core width is recommended to be set at around 500nm and core height is recommended to be set at around 250nm in order to achieve a good compromise between effective index and polarizations. This is because as the core width and core

height are more than 500mm and 250nm, respectively, it is seen that higher order mode started to come in and caused additional losses and crosstalk. As a conclusion, the study of waveguide dimensions and polarization mode is important in the realization of novel and optical devices with optimized performance.

ACKNOWLEDGMENT

We would like to thank Universiti Teknologi Brunei (UTB) for financial support to carry on this research.

REFERENCES

[1] Dai, D., & Zhang, M. "Mode hybridization and conversion in silicon-on-insulator nanowires with angled sidewalls." *Optics Express*, 2015, 23(25), 32452.

[2] Ting Hu, Bowei Dong, Xianshu Luo, Tsung-Yang Liow, Junfeng Song, Chengkuo Lee, and Guo-Qiang Lo, "Silicon photonic platforms for mid-infrared applications," *Photonics Research*. 2017, pp. 417-430.

[3] Prabhu, A. M., Tsay, A., Zhanghua Han, & Vien Van. "Extreme Miniaturization of Silicon Add–Drop Microring Filters for VLSI Photonics Applications." *IEEE Photonics Journal*, 2010, 2(3), pp. 436–444.

[4] Y. Dattner and O. Yadid-Pecht, "Analysis of the Effective Refractive Index of Silicon Waveguides Through the Constructive and Destructive Interference in a Mach–Zehnder Interferometer," in *IEEE Photonics Journal*, Dec 2011 vol. 3, no. 6, pp. 1123-1132.

[5] Troia, B., De Leonardis, F., Lanzafame, M., Muciaccia, T., Grasso, G., Giannoccaro, G., … Passaro, V. M. N. "Design and Optimization of Polarization Splitting and Rotating Devices in Silicon-on-Insulator Technology". *Advances in OptoElectronics*, 2014, pp. 1–16.

[6] Dwivedi, S., Ruocco, A., Vanslembrouck, M., Spuesens, T., Bienstman, P., Dumon, P., … Bogaerts, W. "Experimental Extraction of Effective Refractive Index and Thermo-Optic Coefficients of Silicon-on-Insulator Waveguides Using Interferometers." *Journal of Lightwave Technology*, 2015, 33(21), pp. 4471–4477.

[7] W. Bogaerts, P. Dumon, D. Van Thourhout et al., "Compact wavelength-selective functions in silicon-on-insulator photonic wires," *IEEE Journal on Selected Topics in Quantum Electronics*, 2016, vol. 12, no. 6, pp. 1394–1401.

[8] Ding, Y., Liu, L., Peucheret, C., & Ou, H. "Fabrication tolerant polarization splitter and rotator based on a tapered directional coupler." *Optics Express*, 2012, 20(18), pp. 20021.

[9] Dwivedi, S., Van Vaerenbergh, T., Ruocco, A., Spuesens, T., Bienstman, P., Dumon, P., & Bogaerts, W. "Measurements of Effective Refractive Index of SOI Waveguides using Interferometers." *Advanced Photonics* ,2015.

[10] Ibrahim, M. H. "Rib sidewall scattering loss estimation for trapezoidal optical waveguide." I*nstitutul National de Cercetare-Dezvoltare pentru Optoelectronica* , 2019, pp. 917-920.

[11] Sun, L., Y. Zhang, Y. He, H. Wang and Yikai Su. "Subwavelength structured silicon waveguides and photonic devices." *Nanophotonics 9* ,2020, pp. 1321 - 1340.

[12] Steglich, P. "Silicon-on-Insulator Slot Waveguides: Theory and Applications in Electro-Optics and Optical Sensing." *Emerging Waveguide Technology*, 2018.

[13] Ye, W. N., Xu, D.-X., Janz, S., Cheben, P., Picard, M.-J., Lamontagne, B., & Tarr, N. G. "Birefringence control using stress engineering in silicon-on-insulator (SOI) waveguides." *Journal of Lightwave Technology*, 2015, 23(3), pp. 1308–1318.

A.T.C.Chen (M'21). Angie Teo Chen Chen was born in Brunei Darussalam on June 23, 1995. She received her BEng in electrical and electronic engineering from Universiti Teknologi Brunei, Brunei Darussalam in 2014. She is currently having her PhD degree in electrical and electronic engineering in Universiti Teknologi Brunei, Brunei Darussalam and started since 2019.

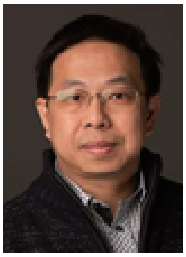
She has three papers in international conference proceedings. She had presented her first paper in Brunei Darussalam for Brunei International Conference on Engineering and Technology (BICET) in 2018. In 2019, she had presented her second paper in Kuala Lumpur for 4th IEEE International Circuit and System Symposium (ICSyS). Her third paper is presented in South Korea for 22nd International Conference of Advanced Communications Technology in 2020. Her research focuses mainly on various nano-scale waveguide structure to see the device performance characteristics by applying her waveguide design variations and characterize the device performance.

Ms. Chen is a member of IEEE. Ms. Chen got her BSc degree with first class honors and received Excellent Student Award from the Ministry of education, Brunei Darussalam. Ms. Chen received UTB Scholarship Award for her programme, PhD in electrical and electronic engineering.

Rafidah Petra received the B.Eng. degree Electrical & Electronic Engineering from Glasgow University, UK, under twinning programme with University Brunei Darussalam (UBD), in 2004. She received her master's degree in Nanoelectronics & Nanotechnology, from the University of Southampton, UK, where she further her studies and obtained her PhD in Electronics and Electrical Engineering from the same University. Her major is in silicon nano-photonics technology for telecommunications where she specializes on the design, fabrication and characterization of nanoscale waveguide devices. Her expertise is in thin-film fabrication for devices at nanometer scale, for the application of solar cells and sensors for environmental sensing.

She is currently an Assistant Professor at Universiti Teknologi Brunei (UTB), Bandar Seri Begawan, Brunei Darussalam. She has been working as an educator since she graduated from her bachelor's degree, back in 2004 and progressively becomes an active academia, where she has been involved both in teaching and research.

She is a member of the IET and an active member for Centre for Innovative Engineering. She currently holds the position as deputy director for Corporate Communications Office, UTB.



Kenneth S. K. Yeo received the B.Eng. degree (with honours) in electronic and communication engineering and the Ph.D. degree from Birmingham University, Edgbaston, Birmingham, U.K., in 1996 and 2000, respectively. In 2009, he received the PG Cert in learning and teaching in higher education from University of East London, London, UK. He doctoral research concerned high-temperature superconducting microwave devices.

He is currently a Senior Assistant Professor at Universiti Teknologi Brunei (UTB), Bandar Seri Begawan, Brunei Darussalam. Prior to joining UTB, he was a Senior Lecture at University of East London, London, UK for nearly 10 years. He worked as a Principal RF Engineer at CryoSystems Ltd., Luton, U.K. between 2004 and 2006. He has spent more than 6 years at the University of Birmingham, as Research Fellow. From 2013 to 2017, he also served as External Link Tutor at Canterbury Christ Church University, Canterbury, Kent, U.K while working at University of East London. In Mar 2016 and May 2017, he was also a Visiting Professor at Hangzhou Dianzi University, Hangzhou, China.

Dr. Yeo is a qualify Chartered Engineer with Engineering Council, UK and a member of IET. He is also a Fellow of HEA, UK.

Dr M. Rakib Uddin was born in Bangladesh on February 18, 1978. He received his PhD degree in communication engineering from KAIST, Daejeon, Korea in 2010. He received his MSc in Electrical and Electronic Engineering from Bangladesh University of Engineering and Technology, Dhaka, Bangladesh in 2005 and BSc in Electrical and Electronic Engineering from Chittagong University of Engineering and Technology, Chittagong, Bangladesh in 2002. He is currently a Research Engineer at the State University of New York Polytechnic institute, Albany, New York, USA.

He worked as ASSOCIATE PROFESSOR with Electrical and Electronic Engineering Programme Area, University Teknologi Brunei (UTB), Bandar Seri Begawan, Brunei Darussalam from December 2014 to December 2020. He worked for Samsung Electronics/Samsung Advanced Institute of Technology, Hwaseong/Geheung, Korea as research staff Member/Senior Engineer from 2011 to 2014. He worked as post-doctoral fellowship with

KAIST from 2010 to 2011. He has more than 60 articles in international journals and conference proceedings along with seven international patents.

Dr Rakib Uddin is a Senior member of IEEE, USA and Member of IET, UK. He got Korean government IITA full scholarship for his PhD programme from 2006 to 2010 at KAIST. He also got Korean Government Brain Korea 21 (BK21) fellowship for his post-doctoral research with KAIST, Korea. Dr Rakib Uddin received University Teaching as well as Research Excellence Awards in 2017 and 2019 at UTB, Brunei Darussalam

An Efficient hole Recovery Method in Wireless Sensor Networks

Mary Wu

Dept. Of Computer Culture, Yongnam Theological University and Seminary, Korea

mary-wu@hanmail.net

***Abstract*— In a wireless sensor network, since sensor nodes are separated from the sensor network area due to environmental obstacles or are randomly placed in the area of interest, there are cases where there are no sensor nodes in some areas. In addition, a hole may occur in the sensor coverage area due to the sensor node running out of energy or physical destruction of the sensor node. A coverage hole in a sensor network may adversely affect the performance of a sensor network, such as reducing the reliability of data sensed by the sensor network and worsening the data transmission load due to a change in the sensor network topology or disconnection of the data link. The coverage hole can be recovered by discovering the coverage hole that has occurred and additionally placing new sensor nodes in the detected coverage hole. This can be solved by finding the coverage hole that has occurred, and recovering the coverage hole by additionally placing new sensor nodes in the detected coverage hole at appropriate locations. Existing studies on coverage hole recovery suggest a very complex method for discovering a coverage hole by identifying a coverage hole boundary node and recovering a coverage hole through the two-step process of finding a hole and recovering a coverage hole. This study does not separate the process of discovering and recovering a coverage hole in a sensor network, but determines whether a sensor node is a hole boundary node or a hole interior node by checking the connection line structure of its one-hop neighbor node. The hole boundary nodes determine the location of the mobile node to be added by a simple calculation, and perform coverage hole recovery. The proposed method is expected to have better efficiency in terms of complexity and message transmission compared to previous methods.**

***Keyword*— Sensor network, Coverage hole, Boundary node, Connection line, Isosceles triangle**

I. INTRODUCTION

A sensor network is used to monitor and control the area in the military and civilian fields for various purposes by placing sensor nodes in a specific area. Sensor nodes are arbitrarily placed for special purposes, detect the environment and collect data, and the collected data is wirelessly transmitted to the sink node and then provided to the user by the application application[1-6].

When sensor nodes are arranged remotely or randomly in an area of interest, separation of the sensor network area occurs due to environmental obstacles or there are cases in which sensors do not exist in some areas. In addition, since sensor nodes are difficult to use by exchanging or recharging batteries, when the energy of some nodes is exhausted, it becomes impossible to collect environmental data in some network areas, which lowers the reliability of sensing data in that area. If the sensing data around the coverage hole has certain characteristics, it is possible to compensate to some extent the problem of reducing the reliability of sensor data in the corresponding area by estimating the value of the sensed data in the coverage hole with the sensing data around the coverage hole. However, the number and size of coverage holes in a sensor network gradually increases over time, which reduces transmission efficiency due to changes in network topology and disconnection of data links, and adversely affects the performance of the entire sensor network[7-18].

The discovery and recovery of coverage holes is an important factor for efficient sensor networking, such as ensuring data reliability and minimal delay in sensor networks. The sensor network coverage hole may be detected by discovering boundary nodes constituting the coverage hole, and existing sensor nodes may move to the coverage hole, or a new mobile node may be additionally deployed to recover the coverage hole. Since a mobile sensor node requires a higher cost than a fixed sensor node, when a coverage hole is restored by adding a mobile node, it is required to achieve the maximum coverage effect with a minimum number of mobile nodes for cost-effective coverage recovery. That is, when determining the location of a mobile node to be newly added, it is required to select an optimal location that maximizes the sensing area of the entire sensor network and minimizes overlap of the sensing area. The level of coverage required by a particular application depends on its characteristics. For example, a military surveillance application requiring a high level of security may require a high level of coverage, while other types of applications may not require a high level of coverage. A ratio of the number of mobile nodes to the number of fixed nodes may be determined according to the coverage request level of the application.

There are many studies that find coverage holes. It is determined whether the sensor node is a boundary node by connecting the sensor nodes in a Delaunay triangle or Voronoi polygon structure or by applying geometric features between neighbors. When a sensor node is identified as a

Manuscript received January 10, 2021. This work was adopted as a follow-up of the invited journal to the accepted & presented paper entitled "An Efficient hole Recovery Method in Wireless Sensor Networks" at the 22nd International Conference on Advanced Communication Technology (ICACT2020).

Mary Wu is a professor in the Dept. Of Computer Culture, Yongnam Theological University and Seminary, 26, Bonghoe 1-gil, Jillyang-eup, Gyeongsan-si, Gyeongsangbuk-do, Republic of Korea. (corresponding author to provide phone: +82-10-5648-8876; fax: +82-53-852-9815; e-mail: mary-wu@hanmail.net).

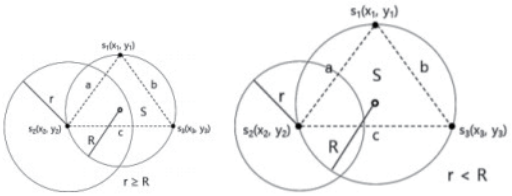
boundary node, a coverage hole is found in the sensor network by verifying the geometrical features of polygons with neighboring boundary nodes[7-10]. In these methods, sensor nodes perform complex calculations based on location information between neighbors in order to construct a polygon, and a coverage hole boundary node performs complex calculations and procedures to determine whether a coverage hole is the same as a neighboring hole boundary node. In these methods, after performing the coverage hole discovery procedure, a procedure for coverage recovery is additionally performed.

This study does not separate the process of discovering and recovering a coverage hole in a sensor network, but recovers a coverage hole by determining whether the sensor node itself is a node inside the sensor network or a node at the edge of the coverage hole. The hole boundary node uses the distance from the neighboring boundary node as the base, and calculates the vertex of an isosceles triangle using the double sensing radius as the hypotenuse, and provides it as the location of the mobile node to be added.

The sensor node examines whether the connection line of its one-hop neighbor node has a closed or open line structure to determine whether it is a hole boundary node. If the connection line of the one-hop neighbor node has an open line structure, the sensor node determines itself as a coverage hole boundary node. Compared to previous methods, the proposed method discovers a coverage boundary node and recovers a coverage hole in a very simple and intuitive way.
The structure of this paper is as follows. Section 2 introduces related research, and section 3 describes the proposed coverage hole discovery and recovery technique. Section 4 shows the superiority of the proposed technique through performance evaluation with existing techniques, and finally, section 5 presents the research results of this paper.

II. Related Research

Li [7] proposed a method for discovering coverage hole boundary nodes by configuring sensor nodes in a Delaunay triangle in a sensor network. A sensor node recognizes its own position and the position of a one-hop neighbor node, and constructs a Delaunay triangle with neighboring nodes based on the distance and angle between the neighbors. This process is performed by all sensor nodes in the entire sensor network. To construct the Delaunay triangle, the sensor node constructs a triangle in which the largest interior angle among the circular neighboring nodes is the smallest. When a sensor node has a radius of the circumcircle of its own Delaunay triangle that is greater than a sensing radius of the sensor node, a sensor node constituting the Delaunay triangle is regarded as a Hall boundary node. In fig. 1, s_1, s_2, and s_3 are one-hop neighbor sensor nodes, and a, b, and c are the distances between sensor nodes. S is the area of the Delaunay triangle, R is the radius of the Delaunay triangle circumscribed circle, and r is the sensing radius of the sensor node. Since the area of the circumcircle of the Delaunay triangle is expressed as abc/4R, the sensor node can determine whether it is an inner node or a boundary node constituting a coverage hole in the corresponding Delaunay triangle.



(a) r is greater than R (b) r is less than R

Fig. 1. Relationship between the circumcircle radius R of the Delaunay triangle and the sensing radius r

In order to discover the coverage hole to which the coverage hole boundary node belongs, it checks whether it has a special geometric characteristic with the neighboring hole boundary node and proceeds with the process of identifying the coverage hole.

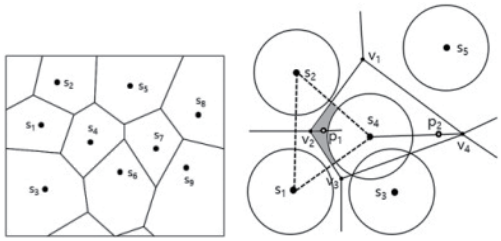
Ma[8] proposed a method for sensor nodes to discover a coverage hole based on information about their two-hop nodes. A sensor node divides its two-hop neighbor nodes into an upper node group and a lower node group based on the y-axis, aligns the nodes in each group based on the x-axis value, and forms a triangle for itself and the other two neighboring nodes. When the radius of the circumscribed circle of the triangle is greater than the sensing radius and the center of the circumscribed circle is not included in the sensing region of the neighboring node, the corresponding node is determined as a coverage hole boundary node. In fig. 2, the upper node group of sensor node s1 includes sensor nodes s_2, s_3, and s_4, and the lower group includes sensor nodes s_5, s_6, s_7, and s_8. Since the radius R of the circumscribed circle of $\Delta s_1s_2s_3$ is greater than the sensing radius r, and the center of the circumscribed circle is not included in the sensing radius of any neighbor of the sensor node s_1, the node s1 is determined as a coverage hole boundary node.

Fig. 2. Relationship between the radius R of the triangular circumscribed circle of the neighboring sensor nodes and the sensing radius r

In the study of Ghosh and Wand[9,10], the sensor nodes in the entire sensor network were configured in a Voronoi polygonal structure. When the center point of a Voronoi polygon is connected to the center point of a neighboring Voronoi polygon, it appears as a Delaunay triangle. In the study of Ghosh[9], when the size of the region not included in the sensing region in the region of the intersection of the region constituting the Delaunay triangle and its own Voronoi region is larger than a certain threshold ($\rho\pi r^2$, r is the sensing radius), it is determined that a coverage hole has occurred. In fig. 3(b), the gray area shows the coverage hole generation area for the Delaunay triangle area formed by the sensor node s_4 with the neighboring nodes s1 and s_2. When node s_4 determines that a coverage hole has occurred in the region of intersection of $\Delta s_1s_2s_4$ and Voronoi polygon, it is determined as the location of the mobile node to add the point

of min(2r, d(v_2, s_4) on the bisector of ∠$v_1v_2v_3$.

In the study of Wand[10], if the distance between the sensor node and the furthest Voronoi vertex is greater than the sensing radius, it is considered that there is a coverage hole. In this case, the point of max($\sqrt{3}$ r, d(s_4,v_4)) on the straight line between the Voronoi vertex of the furthest distance and the sensor node is determined as the location of the mobile node to be added.



(a) Voronoi polygonal structure (b) Location of the mobile node to add

Fig. 3. Constructing a sensor network with Voronoi polygons

Existing studies require complex rules and calculations based on geometrical locations for sensor nodes to discover coverage holes. In order to implement this in an actual situation, a complicated procedure is required, and after a coverage hole is discovered, a procedure for recovering the coverage hole is additionally required. This study discovers a coverage hole in a sensor network in a very simple and intuitive way, and proposes a coverage hole recovery method that does not separate the coverage hole discovery process and the recovery process.

III. Discovery and Recovery of Coverage Holes

This study proposes a technique for discovering and recovering coverage holes based on the connectivity structure of one-hop neighbor nodes. The proposed method assumes that sensor nodes are arranged at arbitrary locations, and that each sensor node recognizes its own location and location information of a one-hop neighbor node that exists within a transmission radius. If r_s is greater than or equal to $\frac{r_c}{\sqrt{3}}$, it is assumed that $r_s > \frac{r_c}{\sqrt{3}}$ is based on the feature that there is no sensing gap between one-hop neighboring nodes(r_s : sensing radius, r_c : transmission radius).

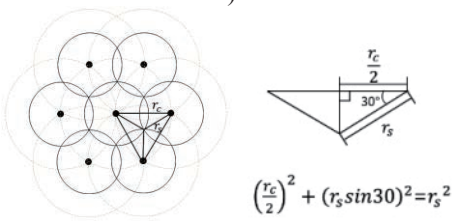


Fig. 4. Model of sensing radius and transmission radius

A. Coverage hole discovery

A sensor node determines whether or not it is a boundary node of a coverage hole by determining the connectivity structure of its one-hop neighbor node. If the connectivity of the one-hop neighbor node is determined to be a closed shape structure, the node is not a boundary node of a coverage hole, and if it is determined as a closed shape structure, the node is determined as a hole boundary node. The coverage hole discovery process has two processes: a process in which a sensor node creates a one-hop neighbor node connection line, and a process in which the connection line determines whether the connection line has a closed shape structure.

① One-hop neighbor connectivity

The sensor node broadcasts a 'Hello' message including its ID, and the node that receives the 'Hello' message records the neighbor list in the 'one-hop neighbor list'. The sensor node broadcasts a 'one hop neighbor' message, including a 'one hop neighbor list'. Each sensor node has a 'one-hop neighbor list' for its one-hop neighbor node. In fig. 5, after the sensor node sends a 'Hello' message, node 29 has a 'one-hop neighbor list' <28, 30, 39, 40>, and node 30 has a 'one-hop neighbor list' <27, 28, 29, 31, 38, 39>. After the sensor node broadcasts the 'one-hope neighbor' message, node 29 has a 'one-hop neighbor list' of nodes 28, 30, 39, and 40, and node 30 has a 'one-hop neighbor list' of nodes 27, 28, 29, 31, 38, and 39. This is shown in table 1.

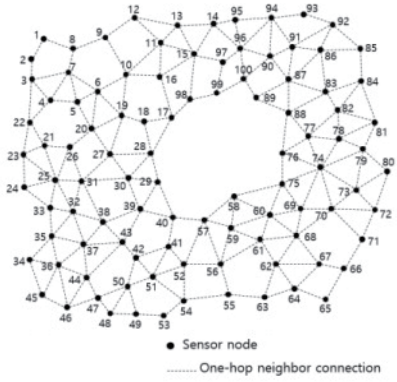


Fig.5. Constructing a sensor network with Voronoi polygons

TABLE I
Units for Magnetic Properties

One-hope neighbors of node 29	List of one-hope neighbors of node 29	One-hope neighbors of node 30	List of one-hope neighbors of node 30
28	{17, 18, 27, 29, 30}	27	{19, 20, 28, 30, 31}
30	{27, 28, 29, 31, 38, 39}	28	{17, 18, 27, 29, 30}
39	{29, 30, 38, 40, 43}	29	{28, 30, 39, 40}
40	{29, 39, 41, 57}	31	{25, 26, 27, 30, 32, 38}
		38	{31, 32, 37, 39, 43}
		39	{29, 30, 38, 40, 43}

The sensor node creates a neighbor node connection line based on the 'one-hop neighbor list' of the one-hop neighbor node. To determine the starting node of the neighbor node connection line, one of its neighbor nodes with the smallest number of one-hop neighbor nodes is selected. The node 29 designates the node 40 having the smallest number of one-hop neighbor nodes among its neighbors as the starting node of the neighbor node connection line. Node 30 designates node 29 with the smallest number of one-hop neighbor nodes among its neighbors as the start node of the neighbor node connection line.

After checking whether a one-hop neighbor of the reference node exists in the 'one-hop neighbor list' of the starting node of the connection line, if it exists, the node is designated as the next connection node. In the 'one-hop neighbor list' of node 40, since node 39 is a one-hop neighbor of reference node 29, node 39 is designated as the next connection node, and the connection line of node 29 is connected to <40-39>. In the 'one-hop neighbor list' of node 29, since node 28 and node 39 are one-hop neighbors of the

reference node 29, any node 28 among the two nodes is designated as the next connection node, and the connection line of node 30 is connected to <29-28>.

If there is an additional one-hop neighbor of the reference node in the one-hop neighbor list, the node is connected in the opposite direction of the connection line. For the connection line of node 30, in the 'one-hop neighbor list' of node 29, the node 39 that is a one-hop neighbor relationship with the reference node exists in addition to node 28, so the connection line of node 30 appears as <39-29-28>.

Designate the first node of the connecting line as the 'first node' and the last node as the 'end node'. In the 'one-hop neighbor list' of the 'end node', a node with a one-hop neighbor relationship with the reference node is found and connected to the connecting line repeatedly. Through this process, the one-hop neighbor node connection line of node 29 is <40-39-30-28>, and the one-hop neighbor node connection line of node 30 is shown as <39-29-28-27-31>.

When the connection line includes all the neighboring nodes of the reference node, the connection line creation process is terminated. If not, the connection process is repeated for the 'first node' of the connection line, and this process is repeated until all one-hop neighboring nodes of the reference node are included.

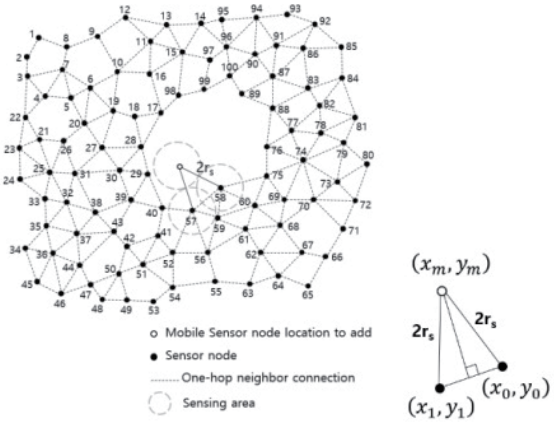
Since the one-hop neighbor connection line of node 30 does not include all the neighbors of node 30, it is checked whether a one-hop neighbor node of the reference node exists in the one-hop neighbor list of node 39 and the 'first node' of the connection line. Since node 38 exists, when connected to the connecting line, the connecting line of node 30 appears as <38-39-29-28-27-31>.

② One-hop neighbor connectivity

The sensor node determines whether the structure of the one-hop neighbor node connection line is a closed figure or not. When the structure of the connection line is a closed diagram, the sensor node is determined as an internal node. When the structure of the connection line is not a closed diagram, the sensor node is determined as a boundary node of the coverage hole. When the 'first node' and 'end node' of a one-hop neighbor node connection line have a one-hop neighbor relationship, the neighbor node connection line has a closed shape structure. The one-hop neighbor node connection line of node 29 is <40-39-30-28>, and the 'first node' 40 and 'end node' 28 are not one-hop neighboring nodes, so the connection line does not have a closed shape structure. As a result, node 29 is determined as a coverage hole boundary node. The connecting line of node 30 is <38-39-29-28-27-31>, and since 'first node' 38 and 'end node' 31 have a one-hop neighbor relationship, the connecting line has a closed shape structure. As a result, node 30 is determined to be an internal node, not a boundary node.

B. Coverage hole recovery

If the sensor node itself is determined to be a boundary node, it proceeds with the process of recovering the coverage hole. A boundary node sends a 'boundary node notification' message including its ID and location information. A boundary node that receives a 'boundary node notification' message from a one-hop neighbor calculates the location of a mobile node to be added based on its own location and the location of the neighboring edge node. The position of the mobile node to be added is calculated as the vertex of an isosceles triangle with the two boundary nodes as the base and the double sensing radius (r_s) as the hypotenuse. The vertices of an isosceles triangle are calculated by the two equations (1) and (2).



(a) Sensor network model (b) Isosceles triangle

Fig. 6. Sensor network and mobile node locations to be added

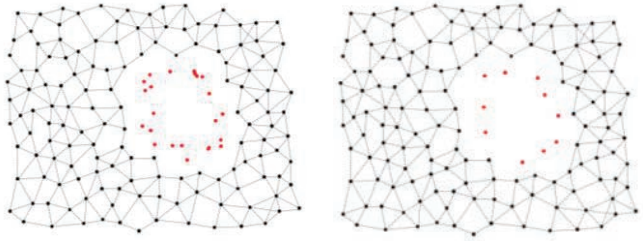
$$\frac{y_1 - y_0}{x_1 - x_0} \times \frac{y_m - \frac{(y_1 + y_0)}{2}}{x_m - \frac{(x_1 + x_0)}{2}} = -1 \quad (1)$$

$$(2R_s)^2 = \left(\frac{(x_1+x_0)}{2} - x_0\right)^2 + \left(\frac{(y_1+y_0)}{2} - y_0\right)^2 + \left(\frac{(x_1+x_0)}{2} - x_m\right)^2 + \left(\frac{(y_1+y_0)}{2} - y_m\right)^2 \quad (2)$$

The border node sends a 'coverage recovery request' message including the location of the mobile node to be added. Upon receiving the 'coverage recovery request' message, the mobile node moves to the nearest target location and transmits a 'coverage recovery response' message including the moved location.

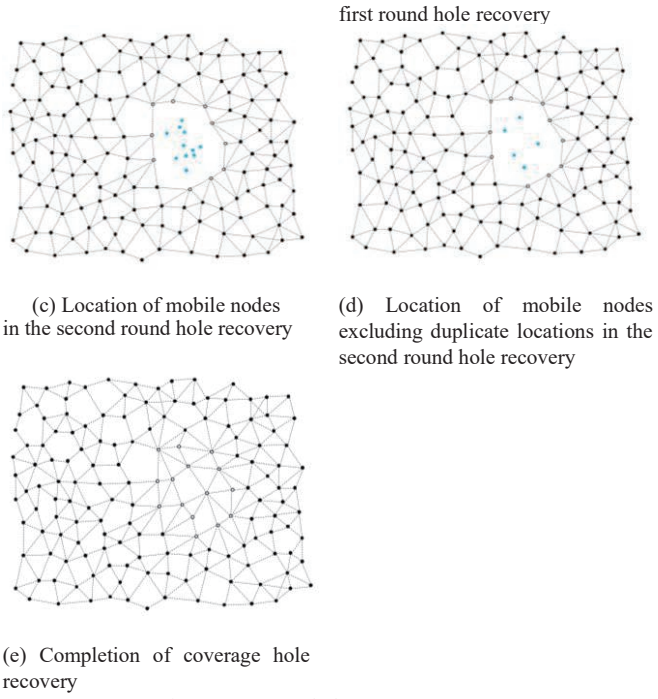
In order to avoid redundant deployment of mobile nodes, the mobile node that receives the 'coverage recovery response' message from a distance closer than the sensing radius gives up its role in the sensor network and waits for the next round of recovery process.

The coverage discovery and recovery process is repeated over several rounds until no coverage boundary nodes are found. Fig. 7 shows the coverage hole recovery process in a 150 sensor nodes topology. Through the second round coverage hole recovery process, the coverage hole recovery process is completed. Fig. 7(a) shows that 23 mobile nodes locations are determined in the first round coverage hole recovery. Fig. 7(b) shows 10 mobile nodes excluding overlapping locations. Fig. 7(c) shows that 11 mobile nodes positions are determined in the second round coverage hole recovery. Fig. 7(d) shows 5 mobile nodes elected by excluding overlapping positions.



(a) Location of mobile nodes in the first round hole recovery

(b) Location of mobile nodes excluding duplicate locations in the



(c) Location of mobile nodes in the second round hole recovery

(d) Location of mobile nodes excluding duplicate locations in the second round hole recovery

(e) Completion of coverage hole recovery

Fig. 7. Coverage hole recovery process

IV. Experiments

An experiment was conducted to verify the effectiveness of the proposed coverage hole recovery technique. The experimental comparison object used the bidding protocol and the sensing intersection-based hole recovery technique. Using C language, a transmission range of 20m, a sensing range of 15m ($>20\sqrt{3}$), and 150 nodes were placed in an arbitrary location in an area of 100m x 100m, and a control message of 512kbit and a data message of 2048kbit were used.

Fig. 8 shows the results of comparing the bidding protocol, the sensing intersection-based method, and the proposed method as an experiment on the amount of computation according to rounds. Compared to the bidding protocol applying the geometric rule of Bornois polygons, the proposed method shows about 33% of the results, and about 58% of the results compared to the sensing intersection-based hole recovery technique. As the round progresses, the amount of computation tends to decrease, and this is seen as a result of the decrease in the coverage area to be restored as the round progresses, and the reduction in the number of coverage hole boundary nodes.

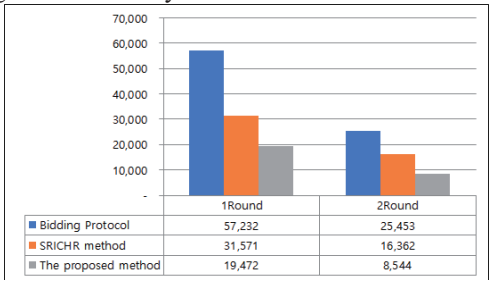


Fig. 8. Computational amount of coverage hole recovery

Fig. 9 shows the results of the bidding protocol, the sensing intersection-based method, and the proposed method as an experiment on the amount of message transmission according to the coverage recovery rate. The proposed method shows a result of about 62% of message transmission compared to the bidding protocol, and about 81% of the result compared with the sensing intersection-based hole recovery technique.

It is analyzed that as the coverage recovery rate increases, the amount of messages transmitted increases as the number of rounds increases to reach the coverage recovery rate.

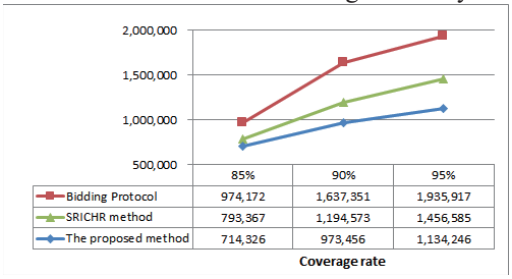


Fig. 9. Transmission amount of coverage hole recovery message

Figure 10 shows the experimental results of the coverage recovery rate for the number of mobile nodes in the proposed method. The larger the number of mobile nodes, the greater the coverage recovery rate. 8 (about 5%), 15 (10%), and 23 (about 15%) mobile nodes were applied. A lot of recovery is made in the first round, and as the rounds increase, a small increase in coverage recovery is shown. In the third round, all cases show a coverage recovery rate of 90% or more. For the 15% with the largest number of mobile nodes, 100% coverage is achieved in the third round. Since a mobile node is more expensive than a general sensor node, it is considered as an important factor for effective coverage recovery to determine the appropriate number of mobile nodes in consideration of the coverage recovery rate required by the sensor application.

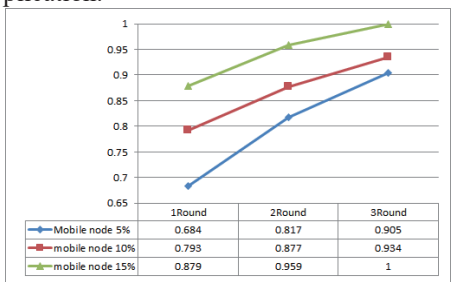


Fig. 10. Coverage hole recovery rate according to the number of mobile nodes

V. Conclusions

This study is a method of recovering a coverage hole in a sensor network. A sensor node determines whether it is a coverage hole boundary node or not based on the connection structure of one-hop neighboring sensors, and if it is determined as a boundary node, a method of recovering a coverage hole suggested. In order to recover the coverage hole, the boundary node determines the location of the vertex of an isosceles triangle with the distance from the neighboring boundary node as the base and the double sensing radius as the hypotenuse as the location of the mobile node to be added. The proposed coverage hole recovery technique recovers the coverage hole using a very simple procedure and formula compared to the existing method. In a randomized sensor network, coverage hole recovery is a very important factor for sensor application data reliability and

efficient networking, and the proposed method shows better performance in terms of complexity and message transmission compared to previous studies in experiments.

REFERENCES

[1] Xiaoqing Yu,Pute Wu, Wenting Han, Zenglin Zhang, A survey on wireless sensor network infrastructure for agriculture, *Computer Standards & Interfaces*, Vol. 35, Issue 1, pp. 59–64, Jan. 2013.

[2] Mary Wu, Hyunjin Park, ChongGun Kim, Multihop Routing based on the Topology Matrix in Cluster Sensor Networks, *Journal of The Institute of Signal Processing and Systems,* Vol. 14, No. 1, pp. 45-50, Jan. 2013.

[3] Zhao Han, Jie Wu, Jie Zhang, Liefeng Liu, Kaiyun Tian, A general self-organized tree-based energy-balance routing protocol for wireless sensor network, *IEEE Transactions on Nuclear Science*, Vol. 61, Issue 2, pp. 732-740, Apr. 2014.

[4] Mary Wu, Balanced Cluster-based Multi-hop Routing in Sensor Networks, *Journal of Korea Multimedia Society*, Vol. 19, No. 5, pp. 910-917, May. 2016.

[5] Mary Wu, An Efficient Routing Protocol for Mobile Sinks in Sensor Networks, *Journal of Korea Multimedia Society*, Vol. 20, No. 4, pp. 640-648, Apr. 2017.

[6] Mary Wu, Strong Connection Clustering Scheme for Shortest Distance Multi-hop Transmission in Mobile Sensor Networks, *Journal of Korea Multimedia Society*, Vol. 21, No. 6, pp. 667-677, Jun. 2018.

[7] Wei Li, Wei Zhang, Coverage hole and boundary nodes detection in wireless sensor networks, *Journal of Network and Computer Applications*, Vol. 48, pp. 35-43, Feb. 2015.

[8] Hwa-Chun Ma, Prasan Kumar Sahoo, Wen-Wen Chen, Computational Geometry based distributed coverage hole detection protocol for the wireless sensor networks, *Journal of Network and Computer Applications*, Vol. 34, Issue 5, pp. 1743-1756, Sep. 2011.

[9] Amitabha Ghosh, Estimating Coverage Holes and Enhancing Coverage in Mixed Sensor Networks, *Proceedings of the 29th Annual IEEE International Conference on Local Computer Network*, Nov. 2004.

[10] Guiling Wang, Guohong Cao, T. LaPorta, A bidding protocol for deploying mobile sensors, *Proceedings of the 11th IEEE International Conference on Network Protocols*, Nov. 2003.

[11] Wei Li, Yuwei Wu, Tree-based coverage hole detection and healing method in wireless sensor networks, *Computer Networks*, Vol. 103, pp. 33-43, Jul. 2016.

[12] Rachid Beghdad, Amar Lamraoui, Boundary and holes recognition in wireless sensor networks, *Journal of Innovation in Digital Ecosystems*, Vol. 3, Issue 1, pp. 1-14, Jun. 2016.

[13] Anju Sangwan, Rishi Pal Singh, Coverage Hole Detection and Healing to Enhance Coverage and Connectivity in 3D Spaces for WSNs: A Mathematical Analysis, *Wireless Personal Communications*, Vol. 96, Issue 2, pp. 2863-2876, Sep. 2017.

[14] Shuangjiao Zhai, Zhanyong Tang, Dajin Wang, Zhanglei Li, Xiaojiang Chen, Dingyi Fang, Feng Chen, Coverage Hole Detection and Recovery in Wireless Sensor Networks Based on RSSI-Based Localization, *IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, 21-24 Jul. 2017.

[15] Tarachand AmgothEmail author, Prasanta K. Jana, Coverage hole detection and restoration algorithm for wireless sensor networks, *Peer-to-Peer Networking and Applications*, Vol. 10, Issue 1, pp. 66-78, Jan. 2017.

[16] Ahmed M. Khedr, Walid Osamy, Ahmed Salim, Distributed coverage hole detection and recovery scheme for heterogeneous wireless sensor networks, *Computer Communications*, Vol. 124, pp. 61-75, Jun. 2018.

[17] Mary Wu, Adjacent Matrix-based Hole Coverage Discovery Technique for Sensor Networks, *Journal of The Korea Society of Computer and Information*, Vol. 24, No. 4, pp. 169-176, Apr. 2019.

Mary Wu was born in Korea in 1973 and received a BS in Mathematics from Yeungnam University in 1996, a MS in Computer Science in 2001, and a Ph.D in Computer Science in 2005. She has been a computer professor at Youngnam Theological University and Seminary since 2013. Her research interests include sensor network, social network analysis, bigdata, IoT, metaverse education and so on, .

End-to-End Routing Algorithm Based on Max-Flow Min-Cut in SDN Controllers

Nada Alzaben*, Daniel W. Engels**

** Dept. of Computer Science, College of Computer Science and Information, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia*

***AT&T Center for Virtualization, Southern Methodist University, Dallas, USA*

nialzaben@pnu.edu.sa, Daniel.w.engels@gmail.com

***Abstract*— In this paper, we present seven novel Max-Flow Min-Cut (MFMC) based algorithms that solve the flow routing problem in the Software Defined Network Controller. Our algorithms identify potential traffic bottlenecks using the MFMC cut, and they avoid the bottlenecks during flow route construction through their choice of the cut edge added to the route. Our algorithms utilize either a random edge selection, a shortest path edge selection, or an edge capacity-based selection from the set of cut edges. Our simulation results show improvement in the network performance when using MFMC and shortest path edge selection compared to simple shortest path first algorithms, such that the mean wait time is reduced by 15.1%, the mean slowdown is reduced by 5.1%, reducing the maximum completion time by 9.6%, and increasing the mean throughput by 18.3%. Therefore, by explicitly considering congestion in routing decisions, better network performance is achieved.**

***Keyword*— Heuristic algorithm, Peer-to-peer computing, Routing, Software defined networking.**

I. INTRODUCTION

ROUTING in computer networks is a fundamental process for finding a communication path that connects two end points in the network for data transfer. The routing process is recognized as an essential factor in solving the network performance problem. In traditional networks the two main functionality of routing is coupled in the router, however, in the new network layer paradigm, the Software Defined Networking (SDN), the network functionality is decoupled in two separate planes of operation: the control plane and data plane [1]-[4].

Benefiting from the SDN global view, the control plane runs the routing algorithms to find path for each flow in the network. Once the path is defined for the flow, the forwarding plane uses that path to deliver the data from one end to another through network switches [5].

With the increase use of Virtual Private Networks (VPNs), secured communications with Transport Layer Security (TLS), along with the high demand of sending video files, which consume the network bandwidth and dominate the network traffic, have highlighted the importance of flow routing problem. In this type of traffic, they demand that all packets follow the same path from source to destination. Using Software Defined Networks (SDNs) enables end-to-end routing of flows through its global view which result in optimizing a given objective function such as maximizing the mean throughput [6]-[9].

The end-to-end flow routing problem is defined as follows. Given a network graph G(V,E), such that each edge $e \in E$ is with a capacity c, where $c \in Z^+$, meaning only c flows may be sent at a time on that edge. Having a set of flows F where each flow $\mathbf{f_i} \in F$ has a given number of packets and a release time Rt, non-preemptively route all flows in F on G to optimize the objective function.

The Shortest Path First algorithms (*SPF*) are most commonly used in end-to-end flow routing [10][11], however, due to their lack of explicitly considering congestion when routing causes network performance degradation in a high load traffic. Therefore, we present our Max-Flow Min-Cut based algorithm which is capable of explicitly considering congestion in routing decisions. The *SPF* algorithms are based on either statically or dynamically calculate the path with shortest distance or minimum number of hops. The static shortest path is a topological shortest path that ignores path capacity availability. Moreover, the dynamic shortest path is more logical in considering the edge capacity availability at the time of flow released before assigning a flow on it [12].

In a network with high traffic flow demand which place these flows over edges with limited capacity, such that the flow demand exceeds the edge capacity, consequently causes congestion in the network, i.e., bottleneck arise. In the Static Shortest Path (SSP) algorithm, the flows between any two ends will always take the short path regardless of available capacity, while for the Dynamic Shortest Path (*DSP*) algorithm, the algorithm finds the shortest available path

A manuscript received Jan. 26, 2021. A follow-up on the invited journal to the accepted and presented paper entitled " End-to-End Routing in SDN Controllers Using Max-Flow Min-Cut Route Selection Algorithm" of the 23rd International Conference on Advanced Communication Technology (ICACT2021).

Nada Alzaben is a PhD student in Southern Methodist University and a lecturer in the Department of Computer Science at Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. (corresponding author, phone:001-214-768-3050, e-mail: nialzaben@pnu.edu.sa).

Daniel W. Engels, is with AT&T Center for Virtualization, Southern Methodist University, Dallas, TX 75205 USA (e-mail: Daniel.w.engels@gmail.com).

which considers congestion implicitly during the flow release time. However, flows placed on these kinds of paths in a high traffic flow causes bottleneck problem which means that these flows are most likely going to be sharing same segments of the path in the network. This indicates the need for a routing algorithm that considers congestion explicitly to minimize this problem.

The Max-Flow Min-Cut (*MFMC*) algorithm, with a polynomial time complexity, is capable of identifying the minimum set of edges in the network; such that by their removal the source node is disconnected from the destination [13]-[15]. We present a suite of algorithms (*MC*) that utilize the *MFMC* algorithm in partitioning the network into two sub-networks, where the first one has the source whereas the other has the destination, by explicitly identifying the bottleneck edges that is represented by the minimum number of edges which hold the maximum possible flow across the cut. The *MC* algorithms runs the *MFMC* algorithm recursively and chooses one edge from the cut set to be part of the path in each run which consequently construct a path that connects the source node to the destination. By repeating the process of slicing the network using *MFMC* algorithm, we are explicitly identifying the bottleneck edges in the network through path construction process.

We evaluate all of our variant *MC* algorithms in our simulation by comparing the result of our measured objective functions to the results obtained by variant shortest path algorithms. These simulations evaluate our algorithms under different flow size distributions and under high load networks. The Shortest Path algorithms we evaluated are: shortest path with minimum hops, shortest path with minimum distance, and the shortest path based on the least congested links. In our evaluations, we adopted two types of each *SP* algorithm, either a static algorithm or dynamic which consider edge availability when routing. The *SP* variant algorithms are: Dynamic Shortest Path with Minimum Hop (*DSP-mh*) and Static Shortest Path with Minimum Hop (*SSP-mh*), Dynamic Shortest Path with Minimum Distance *DSP-md* and Static Shortest Path with Minimum Distance *SSP-md*, and the invert version of that which is the Shortest Path based on the least congested links, *DSP-inv* and *SSP-inv*.

The end-to-end routing problem is simulated as a non-preemptive routing with no clairvoyant, where the flow size is only known once released. Moreover, different variations of the problem were as simulated based on network topology (Barabasi Albert, Mesh), release time (identical/arbitrary), flow size distribution (Pareto/Gaussian). Our results showed improvement in minimizing the mean wait time by 15.1%, the mean slowdown by 5.1%, the maximum completion time (makespan) by 9.6%, and maximizing the mean throughput by 18.3%. These results highlight the need to consider other algorithms other than *SP*.

Our Max-Flow Min-Cut based algorithm (*MFMC*) proved to improve our evaluated objective functions in the evaluated networks. Therefore, we conclude that by explicitly considering network congestion in routing decisions yield better performance.

The remainder of this paper is organized as follows. We cover the relevant related work in Section Ⅱ. The Max-Flow Min-Cut routing algorithm is presented in Section Ⅲ. In Section Ⅳ we introduce the simulation environment. In Section Ⅴ we present the simulation results and analysis of our algorithm. We draw a summary and conclusions in Section Ⅵ.

II. RELATED WORK

End-to-end routing algorithms in the traditional network routers base picking the next hop on their routing tables. Different algorithms for end-to-end routing were designed based on various criteria such as: bandwidth capacity and delay propagation [16][17], minimize end-to-end delay [18][19], minimize energy consumption [20]-[22], and minimize congestion [23]. All of which work on improving the network performance through end-to-end routing algorithms.

One of the oldest routing algorithms is the Shortest Path algorithm *SP* which was designed by Richard Bellman and Lester Ford as the Bellman-Ford algorithm in 1958 [24] and Edsger W. Dijkstra as the Dijkstra algorithm in 1956 [25]. Many network routing algorithms have been developed based on finding the shortest path as part of their algorithm, such as the Widest Shortest Path (*WSP*) [26] which finds all short paths and picks the path with the widest bandwidth. Moreover, the Shortest-Widest Path [27] is the opposite of the (*WSP*), where all edges less than the required bandwidth capacity are removed then the shortest path is selected using Dijkstra's algorithm.

There are two variations of any shortest path algorithm based on considering the network link state or not which is referred to as the static shortest path or the dynamic shortest path algorithms. The Static Shortest Path (SSP) calculates the path using the topological state of the network which ignores the links availability; however, the Dynamic Shortest Path algorithms consider the link state in their calculations. According to Chang H. S. et al. [28], the static algorithm minimizes the overhead of requesting updated link states, however, the dynamic approaches are far superior than static approaches.

In an arbitrary network, routing a set of arbitrary flows over it demands applying routing algorithms which are capable of achieving the goal of utilizing the network bandwidth. Routing algorithms usually are either based on using static link cost or dynamic link cost. For the static link state algorithms, for instance the Minimum Hop Routing Algorithm (*MHR)* [29][30] and Static Shortest Path Algorithm (*SSP*) [31], are finding short paths as on the minimum number of hops to reach the destination or as the shortest distance, however, they do not consider bottleneck congestion in their calculations.

In Software Defined Networks, these types of algorithms are preferable in case minimizing the update messages overhead of the link states between the controller and the network switches is under concern. However, these algorithms congest the network by neglecting the fact of link availability while routing through sending flows with same source and destination over the same path. Akin and Korkmaz [32] listed some of the dynamic shortest path algorithms which are based on considering link bandwidth availability, dynamic link cost algorithms, such as Dynamic Shortest Path (*DSP*). Even though the dynamic link cost algorithms would cause overhead communications by

sending link state update messages with the network switches in the SDN network, with known flows these algorithms utilize network bandwidth and balance load. In the online flow setting where the future flows are not known, their performance is not guaranteed. Our work is an extension of the line of research in the end-to-end routing problem with known flows in SDN controlled networks where we compare our proposed algorithm with the *DSP* and *MHR* algorithms.

In a huge network such as the World Wide Web, flows tend to be heavier tailed with an approximately (α=1) [33]. Self-similarity traffic tends to be heavy tailed distribution file size, proved by Park K. et al. [34]. Consequently, that self-similarity effects the network performance. The Pareto flow size distribution is a one common heavy tailed distribution and for that we adopt it when we generate our flows in the simulation to evaluate our novel *MFMC* algorithm.

The network layer fragments large data files before transmitting them to fit the packet frame which does not exceed the Maximum Transfer Unit (MTU). The larger data size the more packet frames created to transfer that data. Previous studies shown that the packet size effect the network performance, where the size of a packet can degrade the throughput once it exceeds its dedicated packet size [35]. Since the space allocation for that packet to be transferred may be doubled in size which waste an unused space allocation. For instance, for a packet frame size of 10 and a flow size of 12 the MTU will cause the flow to be fragmented in two frames where the second one has 8 unused spaces, which doesn't utilize network resources. According to Lin et al. [36] sending large files over the network while maintaining high quality of service, one must select an intelligent routing and scheduling algorithms for fast transfer and better network utilization.

The shortest path algorithm has been widely adopted with both traditional networks and SDN controlled networks. Since it is widely applied in many routing algorithms, we choose to compare our algorithm performance to it.

III. MAX-FLOW MIN-CUT ROUTING ALGORITHM

In the 1950s, Ford Fulkerson and Elias-Feinstein-Shannon [37] developed the Max Flow Min Cut (*MFMC*) theory. Researchers since then have worked on a lot of algebraic topology versions made of MFMC [38][39]. The *MFMC* algorithm runs in polynomial time with a complexity measured by the number of edges E multiplied by the maximum number of flows f^*, represented by ($O(E f^*)$). To find the min cut edges in a graph of 50 nodes, assume each node sends out 10 flows, it is expected to consume 122 ms on a Microchip PIC at 5MIPS, while in a graph of 1000 nodes it is expected to consume 49.95 ms on Intel Core i7 with 100,000 MIPS [40].

Routing flows in a network is performed in two folds: choosing which flow to route from the flow set and then find a path to route that flow over it. Picking a flow from the flow set in our simulation is based on picking the shortest flow first to process and in case more than one flow have the same flow size then we pick one of them randomly. Considering consistency in our algorithm's evaluation, we use the same flow pick order across the evaluated algorithms. After picking a flow, the next process step is defining the path for that flow where we use our novel Max-Flow Min-Cut (*MFMC*) algorithm [41][42].

A general description of our *MFMC* algorithm is defined in Algorithm 1. Our algorithm is based on a recursive process of slicing the network graph by removing the edges in the cut set. The edges in the cut set represent the minimum number of edges which with their removal the graph gets disconnected. By picking one edge from the cut set in each loop we construct the path. We base our edge selection on one of these categories: random selection, shortest path selection, and capacity-based selection.

In an arbitrary network, to find a path that connects between two nodes ***(s, d)***, we use our Max-Flow Min-Cut routing algorithm as defined in Algorithm 1. Given {**G**} as an undirected graph and a flow $\mathbf{f_i}$ to be routed over **G**, furthermore, knowing that the set **Cut** holds the minimum number of edges with the maximum flow obtained by following the min cut algorithm, the list **path** holds the selected edges from each cut set which defines the flow path from the source node **s** to the destination node **d** for the flow $\mathbf{f_i}$.

Algorithm 1 General Min-Cut Routing Algorithm

find a path in *G* from source *s* to destination *d*.
Input: undirected graph *G* and a flow $f_i=(s,d)$
Output: a path in *G* for f_i that connects *s* to *d*.
function: FIND PATH IN GRAPH (G,f,path)
  if *{Connectivity(f_s,f_d)} =False* **then**
    return *path = Null*
  else
    Cut= get minimum edge cut between (s,d)
    Partition G into G` and G`` by removing edges in cut from G.
    pick edge e=(e_1,e_2) from cut.
    append e to path list
    if *(f_s,f_d) ==e* **then**
      return *path*
    else
      set new $f_s = e_2$ and new $f_d = e_1$
      set f`=(f_s ,new f_d) and f``=(new f_s ,f_d)
    if *G` >1* **then**
      FIND PATH IN GRAPH (G`,f`,path)
    if *G`` >1* **then**
      FIND PATH IN GRAPH (G``,f``,path)

In our recursive process of cutting the network edges, during each step we result in having a set of edges each one could be a possible edge within the path. Our suit of algorithms *MFMC* have variant variations based on the edge selection criteria used for each algorithm. In this paper we present seven different variations as stated in Table Ⅰ.

In our variant variations of *MFMC*, we are constructing different paths based on the edge selection criteria adopted by the algorithm. In random based selection algorithms, *MC1* and *MC2*, the edge selection criteria from the cut set are based on randomness. However, algorithm *MC1* does not consider cycles within the process and remove cycles after constructing the path, while *MC2* removes any edge that may cause cycles from the candidate edges in the cut set.

In shortest path selection algorithm, the *MC3,* the edge that

is selected from the cut set is the edge that leads to an available shortest path. The difference between a path constructed by this algorithm and a DSP-md is that MC3 explicitly consider capacity availability when routing which reduce network congestion caused by high traffic demand.

Table I
Edge selection criteria

Algorithm	Edge selection criteria
MC1	the edge is selected randomly and then once path is constructed any cycles in the path will be removed.
MC2	any edge in the cut edge list causing a cycle will be removed then the edge is selected randomly.
MC3	the edge selection is based on being part of possible available shortest path based on minimum hop.
MC4	the edge with minimum available capacity will be selected
MC5	the edge with maximum available capacity will be selected
MC6	the edge with minimum capacity will be selected
MC7	the edge with maximum capacity will be selected

The third category in our edge selection-based criteria is capacity-based selection. We have four variant algorithms based on this category: MC4, MC5, MC6, and MC7. When considering edge capacity, we have another two classification which consider static edge capacity or dynamic edge capacity. In the static edge capacity, we select the edge with minimum capacity with MC6 algorithm and we select the edge with maximum capacity with MC7. However, in the dynamic edge capacity, we consider the available remaining edge capacity of an edge in the cut set. Furthermore, choosing the edge with minimum remaining capacity is *MC4 algorithm and choosing* the edge with maximum remaining capacity is *MC5*. The *MC6* and *MC7* algorithms consider the edge capacity, regardless of available amount of capacity at the time of the cut, where *MC6* select the edge with the minimum capacity in the cut set while *MC7* selects the one with maximum capacity. When an algorithm considers the edge capacity, it is actually considering the most congested or the least congested. When routing using *MC4* the flows tend to use the remaining capacity available of an edge to send the flow over it while in *MC5* the flow tends to load balance by sending the flows over the least congested paths.

IV. SIMULATION ENVIRONMENT

In our simulation, the network is modeled as an undirected graph G(V,E), where the set of nodes V are connected by edges from the edge list E. Each edge $e_i(v_{i-1}, v_i) \in E$ is characterized by two nodes v_{i-1} and v_i and hold a capacity $(C(e)>0)$. The flows are in our model are defined by the set flows (F), where each $f_i \in F$ is characterized by a source node indicated as (s) and the destination node by (d). The flow path which connects (s) to (d) is defined by the set P, where $(P=\{e_{(s,v1)},e_{(v1,v2)},...,e_{(vi,d)}\})$. The path P bandwidth is indicated by (b(P)) which defines the minimum edge capacity in the path P.

Two network topologies are simulated to evaluate the proposed algorithms, the Max-Flow Min-Cut suit of algorithms *MFMC*, the Mesh network and the Barabasi Albert network. The Mesh network, modeled as graph **G**, is the network where in general each node v_i is connected to at least one node in G. The full connected mesh network is the mesh network where each node v_i is connected with every other node in V and it has an edge degree of N-1, otherwise we call it partial connected mesh network. We simulate a partial connected mesh network which gives a distinctive result in calculating an objective function such as maximizing the mean throughput compared to the full connected mesh, therefore, we choose the partial connected mesh network with an edge degree of $N/2$.

The second network topology we simulate is the Barabasi Albert (BA) network which is based on generating networks with power law degree distribution. The power law degree distribution starts with a minimum two nodes n_1 and n_2 then it starts to expand by adding one node at a time with a degree of K, where $K<|n|$. Every new node has the choice to be connected with another with higher degree in the network which highlight node popularity or most visited [40].

The *MFMC* algorithms are evaluated over these two-network topology, the partial connected Mesh and the Barabasi Albert network. Our simulator is developed in Python language and to generate our network graphs, we have used the NetworkX library[1] to develop graph nodes and edges and used its built-in functions to maintain the graphs. The network size ranges from 10 to 50 nodes and the edges capacity are generated randomly, where each edge capacity C is bound by $(1 \le C(e) \le 10)$. The flows are generated randomly by randomly selecting a source node s and a destination node d in a uniform distribution.

The problem, as defined earlier, with having a network graph G and a set of flows F we need to non-preemptively route those flows over G such that we optimize a set of defined objective functions. These objective functions are defined in Equations (1) to (5). The source node is represented as s and the destination as d. The time is t, which is measured in unit time, therefore, flow release time is denoted by *Rt,* flow completed or finished time by *Ft* and the maximum completion time by *max(Ft*). The minimum travel time between s and d is denoted by *Tt,* as defined in Equation (1), and the flow size and path length are denoted by *l(fi)* and *l(pi)*, respectively. Our simulated objective functions represent an optimization factor which calculates network performance such as: the mean wait time representing average delay rate *WT,* the mean throughput *TH,* the mean slowdown *SD,* the mean makespan *MS,* and the maximum completion time *(max(MS))*.

$$Tt_i = l(f_i) + l(p_i) - 1 \quad (1)$$
$$WT_i = Ft_i - Rt_i - Tt_i \quad (2)$$
$$MS_i = Ft_i - Rt_i \quad (3)$$
$$TH_i = l(f_i)/(Ft_i - Rt_i) \quad (4)$$
$$SD_i = (Ft_i - Rt_i)/Tt_i \quad (5)$$

In our simulation each node in the graph could be either a source node, a destination node or a router. Flows are generated randomly by randomly picking a source node and a destination node and define its release time either randomly or all flows release times are set to zero. The size of each flow is defined by either a Gaussian distribution or Pareto

[1] https://networkx.github.io

distribution. The parameters for the Gaussian distribution are set as (μ=5) and (∂=1) and for the Pareto distribution, to represent very long flows as large files in the network, is set as (α=1).

The algorithms, the *MFMC* suit of algorithms and the Shortest Path *SP* algorithms, are evaluated under different set of problem scenarios. Under different network topology, the flows could be generated with all release times set to zero (Rt=0) to evaluate the algorithms under a huge burst of flows in the network, otherwise, flows are released in arbitrary times set by a uniform distribution where (Rt≥0). In both scenarios the flow size is set by either a Gaussian flow size distribution or a Pareto flow size distribution.

In simulating a non-preemptive scheduling problem with a non-clairvoyant constrain, we simulate an uninterruptible flow packets sequence where the flows are not known before they are released. In the non-clairvoyant we hold no knowledge of the future network flows in advance, therefore, the flows are visible to the scheduler once they are released.

V. RESULTS AND ANALYSIS

Our Max-Flow Min-Cut based routing algorithm *MFMC* is evaluated within different problem variations based on the network and flow characteristics. *MFMC* is evaluated against different Shortest Path algorithms which consider short in number of hops or short in distance. These shortest path algorithms are noted as: (SSP-md/DSP-md), which calculates the Static/Dynamic Shortest Path based on minimum distance, (SSP-mh/DSP-mh), which calculates the Static/Dynamic Shortest Path based on minimum hops, and (SSP-inv/DSP-inv) which chooses the most congested path in the network by applying Dijkstra's algorithm over the inverted edge weights. With this kind of evaluation in variant problem formulation, it gives clear evaluation of our algorithm performance.

The performance of the algorithms was measured by the results of the underlying objective functions. We have evaluated four objective functions: We evaluated four objective functions: minimizing the Mean Wait Time, minimizing the Mean Slowdown, minimizing the maximum completion time (makespan) and maximizing the Mean Throughput.

The performance of the dynamic routing algorithms performs better than the static algorithms because they take the network link states in consideration when finding the path. We have evaluated the performance of the three shortest path algorithms for both static state and dynamic. For example, in a Barabasi Albert network, as in Fig 1, we show the results of running the dynamic shortest path algorithms next to the static once in minimizing the mean wait time.

In the results and analysis of our *MFMC* algorithms, we omit the static version of the shortest path algorithms for simplicity. Furthermore, we compared our *MFMC* suit of algorithms to each other where we have found that *MC3* performed better than the rest of *MFMC* algorithms. As an illustration we show in Fig 2, the mean wait time is minimized by *MC3* on average more than the rest of *MFMC* algorithms by 28.2%, minimize the mean slowdown by 7.24%, minimizing the maximum completion time by 18.5% and maximizing the mean Throughput by 5.93%. The *MC6* and *MC7* algorithms in a sense are the static version of *MC4* and *MC5* since they consider the minimum/maximum edge capacity instead of the minimum/maximum available edge capacity, therefore, for the rest of the analysis section we omit it from our figures for better visibility. Detailed analysis of these algorithms is stated in Table Ⅱ, where denote the mean wait time by (MWT), the mean slowdown by (MSD), the mean throughput by (MTH), and the maximum completion time by (Makespan).

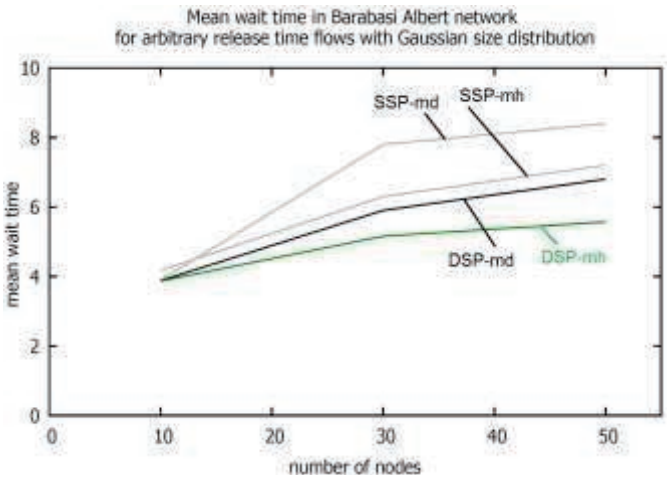


Fig. 1. Comparing the performance of Static Shortest Path (SSP) algorithms with the Dynamic Shortest Path (DSP) algorithms in minimizing the mean wait time

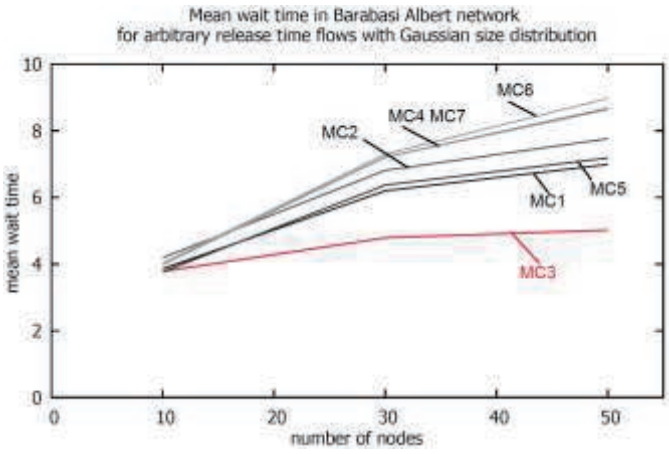


Fig. 2. Comparing the performance of our MFMC suit of algorithms in minimizing the mean wait time

maximizing the mean Throughput by 5.93%. The *MC6* and *MC7* algorithms in a sense are the static version of *MC4* and *MC5* since they consider the minimum/maximum edge capacity instead of the minimum/maximum available edge capacity, therefore, for the rest of the analysis section we omit it from our figures for better visibility. Detailed analysis of these algorithms is stated in Table Ⅱ, where denote the mean wait time by (MWT), the mean slowdown by (MSD), the mean throughput by (MTH), and the maximum completion time by (Makespan).

In minimizing the mean wait time regardless of network topology we have found that our *MC3* algorithm minimized the mean wait time more than the *DSP-md*, *DSP-mh*, *DSP-inv* on average by 18.4%, 11.7% and 15.3%, respectively.

However, the remaining of the *MFMC* algorithms on

Table II
Comparing Max-Flow Min-Cut Algorithm to the Path Finding Algorithms

Objective Function	Network Type	Flow Size Distribut-ion	Percent difference with DSP-md							Percent difference with DSP-mh				
			MC1 &2	MC3	MC4	MC5	MC6	MC7	MC1&2	MC3	MC4	MC5	MC6	MC7
Minimize MWT	BA	Gaussian	12.6%	-14.5%	25.2%	8.9%	27.7%	24.8%	22.6%	-7.0%	36.3 %	18.6 %	38.9 %	35.8 %
		Pareto	-5.6%	-23.6%	7.5%	-3.1%	2.6%	10.6%	10.7%	-10.4%	26.1 %	13.7 %	20.4 %	29.7 %
	Mesh	Gaussian	37.5%	-16.1%	36.9%	20.5%	28.5%	20.7%	26.0%	-8.4%	49.5 %	31.4 %	40.2 %	31.7 %
		Pareto	-10.2%	-25.1%	4.9%	-4.7%	3.8%	-4.2%	7.0%	-10.7%	25.1 %	13.6 %	23.7 %	14.2 %
Minimize MSD	BA	Gaussian	1.8%	-4.8%	6.6%	0.7%	6.7%	5.6%	4.5%	-2.3%	9.4%	3.4%	9.6%	8.4%
		Pareto	-4.1%	-7.3%	-3.8%	-4.9%	-3.3%	-2.5%	2.5%	-0.8%	2.9%	1.8%	3.5%	4.3%
	Mesh	Gaussian	4.7%	-5.9%	8.3%	3.1%	5.9%	2.9%	9.1%	-2.0%	12.9%	7.5%	10.4 %	7.2%
		Pareto	-2.9%	-7.4%	1.1%	-3.2%	2.4%	-2.8%	3.8%	-0.9%	8.1%	3.5%	9.5%	3.9%
Maximize MTH	BA	Gaussian	-5.2%	6.8%	-3.7%	7.3%	-1.9%	-1.8%	-8.9%	2.6%	-7.5%	3.1%	-5.8%	-5.6%
		Pareto	1.3%	15.6%	4.8%	9.4%	7.8%	8.5%	-3.4%	4.5%	-5.3%	-1.1%	-2.6%	-2.0%
	Mesh	Gaussian	-4.9%	7.8%	-1.1%	7.1%	2.5%	3.3%	-5.0%	7.7%	-1.3%	6.7%	2.3%	3.2%
		Pareto	-4.2%	10.4%	-1.3%	11.6%	1.8%	3.6%	-9.6%	4.2%	-7.0%	5.3%	-4.0%	-2.3%
Minimize makespan	BA	Gaussian	7.1%	-7.7%	11.1%	6.6%	14.4%	12.9%	11.8%	-3.7%	16.0%	11.3 %	19.1 %	17.8 %
		Pareto	3.1%	-5.3%	16.2%	3.11%	27.5%	11.1%	11.7%	2.5%	27.4%	11.7 %	31.1 %	20.3 %
	Mesh	Gaussian	29.3%	-10.9%	11.8%	-0.7%	16.4%	7.3%	36.7%	-1.0%	24.2%	10.4 %	29.2 %	19.2 %
		Pareto	21.8%	-10.6%	8.2%	-9.9%	10.3%	-2.7%	28.8%	-5.5%	14.3%	-4.8%	16.5 %	2.9%

average have increased the mean wait time compared with all *DSP* algorithms by 16.4%. In addition, comparing the

performance of the algorithms with different flow size distributions we have found that the mean wait time is minimized with flows with Pareto size distribution more than with flows of Gaussian size distribution by 20.6% and 16.1%, respectively.

We illustration our results in the objective function minimizing the mean wait time with the example: having a Barabasi Albert network with arbitrary release time flows with Pareto flow size as in Fig 3. The Red line represent our *MC3* algorithm and the gray lines represent the other variation of *MFMC* and we compare them to the dynamic algorithms, *DSP-md, DSP-mh, DSP-inv*.

The analysis result in minimizing the mean slowdown we also found that *MC3* algorithm minimized this objective function more than the *DSP-md, DSP-mh, DSP-inv* on average by 6.4%, 1.5% and 7.2%, respectively. Moreover, the mean slowdown is again minimized by Pareto flow size distribution more than Gaussian flow size distribution by 8.4%, respectively. However, the remaining *MFMC* algorithms have increased the mean slowdown over all *DSP* on average by 5% as illustrated in Fig 4.

With the aim to maximize the mean throughput, regardless of network topology, our analysis shows that our *MC3* algorithm has maximized the mean throughput more than all DSP on average by 18.3%. Moreover, comparing the results of this objective function between flows with Pareto size distribution and flows with Gaussian size distribution they both performed the same by 18.6% and 17.2%, respectively. However, *MC1, MC2* and *MC4* have not increased the mean throughput over the *DSP*, it has minimized it by 2.7%. As for *MC5, MC6* and *MC7*, they maximized the mean throughput more than all *DSP* on average by 2.4%.

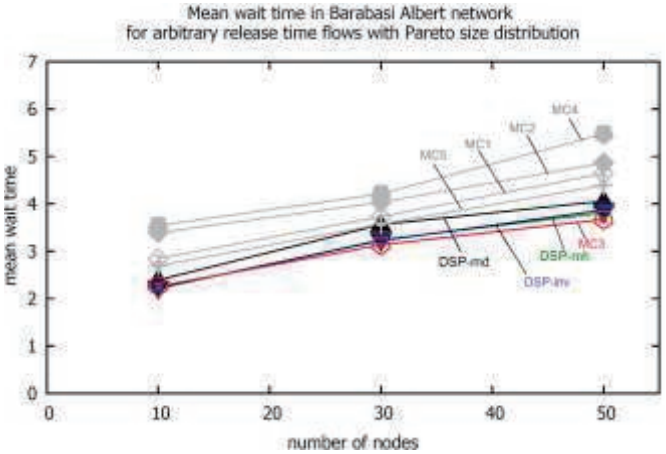


Fig. 3. Mean wait time in Barabasi Albert network with arbitrary release time flows and Pareto size distribution

We illustration our results in the objective function maximizing the mean throughput with the example: having a Barabasi Albert network with arbitrary release time flows with Pareto flow size as in Fig 5. The Red line represent our *MC3* algorithm and the gray lines represent the other variation of *MFMC* and we compare them to the dynamic algorithms, *DSP-md, DSP-mh,* and *DSP-inv*.

In minimizing the maximum completion time (makespan), regardless of network topology, we also found that our *MC3* algorithm minimizes the maximum completion time more than all *DSP* on average by 9.6%. Moreover, this objective

function is minimized with flows of Pareto size distribution more than with flows of Gaussian size distribution by 18.2% and 7.5%, respectively. However, the remaining *MFMC* algorithms have increased the makespan over the *DSP* on average by 5.7%.

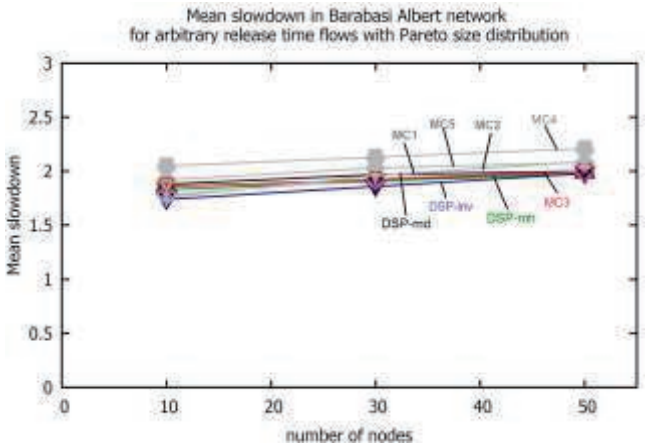


Fig. 4. Mean Slowdown in Barabasi Albert network with arbitrary release time flows and Pareto size distribution

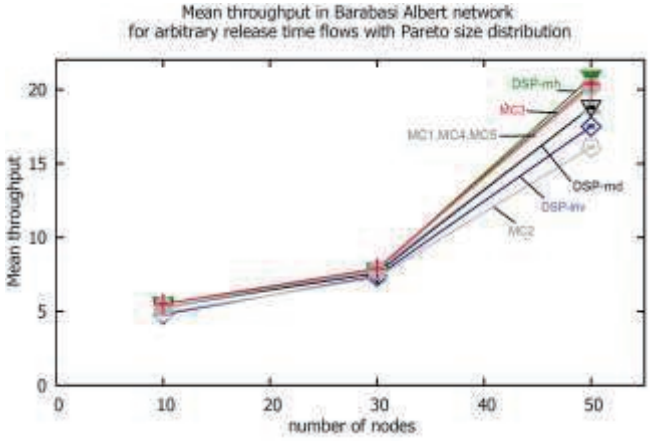


Fig. 5. Mean Throughput in Barabasi Albert network with arbitrary release time flows and Pareto size distribution

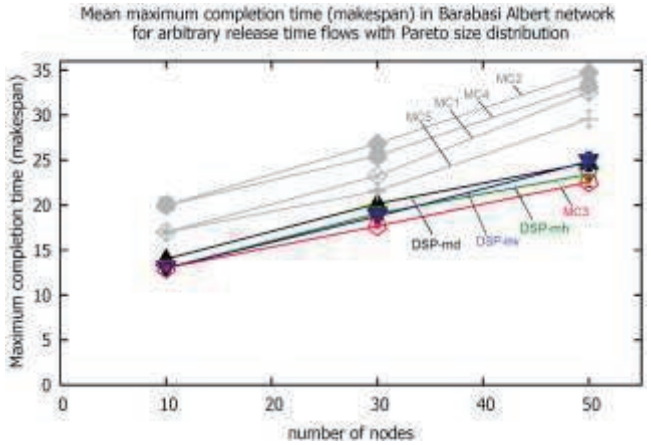


Fig. 6. Mean Maximum Completion Time in Barabasi Albert network with arbitrary release time flows and Pareto size distribution

In Fig 6, we illustrate the results of minimizing the maximum completion time in a Barabasi Albert network with flows released in arbitrary times with Pareto flow size distribution. Again, the red line represents our *MC3* algorithm while the gray lines represent the remaining *MFMC* algorithms and we compare them to the dynamic shortest path algorithms as well.

In our various simulations we have found that constraint on flows release time, wither arbitrary or identical, had no impact on the evaluation on our objective functions. Moreover, selecting the edge from the cut set in our *MFMC* algorithms based on being part of a minimum hop path optimized the network performance in minimizing the mean wait time, minimizing the mean slowdown, minimizing the maximum completion time and maximizing the mean throughput.

VI. Conclusion

In summary, we present seven Max-Flow Min-Cut (MFMC) based algorithms that solve the flow routing problem in the Software Defined Network Controller. The performance of end-to-end routing in the Software Define Network controllers can be maximized with the use of a routing algorithm that is fast and near optimal. These algorithms identify potential traffic congestion using several MFMC cut through their choice of edges in constructing the route to send flows over them. The route construction mechanism is based on one of three categories: random selection, capacity-based selection, and shortest path selection. In random selection, the path is constructed by randomly picking edges from the cut set which our results didn't show improvements in the network objective functions. However, with capacity-based selection the flows tend either to route through the most congested paths with minimum capacity or they tend to balance network load by routing through maximum edge capacity. In the third category, we considered shortest path-based algorithm where we have found that MC3 algorithm optimized the network performance, such that the mean wait time is reduced by 15.1%, the mean slowdown is reduced by 5.1%, reducing the maximum completion time by 9.6%, and increasing the mean throughput by 18.3%. By comparing shortest path based selection to the capacity based selection, we found that MC3 performed better which indicates that topology based decision is more important than capacity based in choosing an edge from the cut set.

The evaluation results of our simulation showed that our novel Max-Flow Min-Cut (*MFMC*) algorithm with an edge selection based on shortest path which picks the edge in the cut set with minimum hops provides superior performance contrast to the Shortest Path *SP* algorithm variants. Using *SP* algorithms for network routing often degrade the network performance due to the bottlenecks it causes by sending most flows over the most congested links which minimizes the throughput and increase the slowdown. These simulations show that by explicitly identifying bottlenecks in a routing algorithm through the least available flows in the cut edges along with picking the edge that is part of potential shortest path yield better network performance. Our *MFMC* is capable to finding the path which result in significant improvement over the commonly used shortest path algorithms. We have demonstrated with our *MFMC* algorithms that choosing the edges that leads to shortest path, such as in *MC3*, yields better performance across a broad range network types and flow size distributions compared to a balanced or longer path approach.

REFERENCES

[1] Sugam Agarwal, Murali Kodialam, and TV Lakshman. Traffic engineering in software defined networks. In 2013 *Proceedings IEEE INFOCOM*, pages 2211–2219. IEEE, 2013

[2] C. J. Bernardos, A. de la Oliva, P. Serrano, A. Banchs, L. M. Contreras, H. Jin, and J. C. Zúniga. An architecture for software defined wireless networking. *IEEE Wireless Communications*, 21(3):52–61, June 2014

[3] Nick Feamster, Jennifer Rexford, and Ellen Zegura. The Road to SDN: An Intellectual History of Programmable Networks. *SIGCOMMComput*. Commun. Rev., 44(2):87–98, Apr 2014.

[4] N. McKeown. *How SDN will shape networking*, Oct 2011.

[5] Matthew Caesar, Donald Caldwell, Nick Feamster, Jennifer Rexford, Aman Shaikh, and Jacobus van der Merwe. Design and implementation of a routing control platform. In *Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation*-Volume 2, pages 15–28. USENIX Association, 2005

[6] H. Kim and N. Feamster. Improving network management with software defined networking. *IEEE Communications Magazine*, 51(2):114–119, February 2013

[7] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig. Software Defined Networking: A Comprehensive Survey. *Proceedings of the IEEE*, 103(1):14–76, Jan 2015.

[8] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. Openflow: Enabling innovation in campus networks. *SIGCOMMComput*. Commun. Rev., 38(2):69–74, March 2008.

[9] A. Detti, C. Pisa, S. Salsano, and N. Blefari Melazzi. Wireless Mesh Software Defined Networks (wmSDN). In 2013 *IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 89–95, Oct 2013.

[10] Q. Chen, K. Zheng, F. Ouyang, X. Gan, Y. Xu, and X. Tian. A shortest path routing algorithm based on virtual coordinate in NELs. In 2016 *8th International Conference on Wireless Communications Signal Processing (WCSP)*, pages 1–5, Oct 2016.

[11] A. Nanda and A. K. Rath. Cost effective mod leach-a x2217; search algorithm for shortest path routing in wireless sensor networks. In 2016 *Sixth International Symposium on Embedded Computing and System Design (ISED)*, pages 147–151, Dec 2016.

[12] Dexiang Xie, Haibo Zhu, Lin Yan, Si Yuan, and Junqiao Zhang. An improved Dijkstra algorithm in GIS application. *In World Automation Congress* 2012, pages 167–169, June 2012.

[13] L. R. Ford and D. R. Fulkerson. Network flow and systems of representatives. *Canadian Journal of Mathematics*, 10:78–84, 1958

[14] Lester Randolph Ford and Delbert R Fulkerson. Maximal flow through a network. *Canadian journal of Mathematics*, 8:399–404, 1956.

[15] Lester R Ford Jr. *Network flow theory*. Technical report, Rand CorpSanta Monica Ca, 1956.

[16] P. Huang, C. Wang, and L. Xiao. Improving end-to-end routing perfor-mance of greedy forwarding in sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 23(3):556–563, March 2012.

[17] Nageswara S. V. Rao, Sridhar Radhakrishnan, and Bang-Young Choel. Netlets: Measurement-based routing for end-to-end performance over the internet. In *Pascal Lorenz*, editor, Networking ICN 2001, pages184–193, Berlin, Heidelberg, 2001. Springer

[18] L. Wang and H. Liang. Research and Improvement of the Wireless Sensor Network Routing Algorithm GPSR. In 2012 *International Conference on Computing, Measurement, Control and Sensor Network*, pages 83–86, July 2012.

[19] Y.-F. Wen and Y.-S. Lin. Fair bandwidth allocation and end-to-end delay routing algorithms for wireless mesh networks. *IEICE Transactions on Communications*, E90-B(5):1042–1051, 2007

[20] T. N. Nagabhushan, S. P. S. Prakash, and K. Krinkin. Power-saving routing algorithms in wireless mesh networks: A survey. In 2012 11th *Conference of Open Innovations Association (FRUCT)*, pages 107–115, April 2012

[21] Rajan Sharma. ANN Based Framework for Energy Efficient Routing In Multi-Hop WSNs. *International Journal of Advanced Research in Computer Science*, 8(5), 05 2017

[22] Hua R. Wu and Li Zhu. A wireless sensor network routing algorithm based on Zigbee. *Applied Mechanics and Materials*, 513-517:1845–1849, 2014.

[23] Abdeljalil Rachadi, Mohamed Jedra, and Noureddine Zahid. Self-avoiding paths routing algorithm in scale-free networks. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 23(1), 2013.

[24] Richard Bellman. On a routing problem. *Quarterly of Applied Mathematics*, 16(1):87–90, 1958

[25] Donald B Johnson. A note on Dijkstra's shortest path algorithm. *Journal of the ACM (JACM)*, 20(3):385–388, 1973.

[26] Jang-Ping Sheu, Quan-Xiang Zeng, R. Jagadeesha, and Yeh-Cheng Chang. Efficient unicast routing algorithms in software-defined net-working. In 2016 *European Conference on Networks and Communications (EuCNC)*, pages 377–381, June 2016.

[27] Man-Ching Yuen, Weijia Jia, and Chi-Chung Cheung. Simple math-ematical modeling of efficient path selection for qos routing in load balancing. In 2004 *IEEE International Conference on Multimedia and Expo (ICME) (IEEE Cat. No. 04TH8763)*, volume 1, pages 217–220. IEEE, 2004.

[28] Hong Seong Chang, Byoung Wan Kim, Chang Gun Lee, Sang Lyul Min, Yanghee Choi, Hyun Suk Yang, Doug Nyun Kim, and Chong Sang Kim. Performance comparison of static routing and dynamic routing in low-earth orbit satellite networks. In *Proceedings of Vehicular Technology Conference - VTC*, volume 2, pages 1240–1243 vol.2, 1996.

[29] Robert W Floyd. Algorithm 97: shortest path. *Communications of the ACM*, 5(6):345, 1962.

[30] J. J Garcia-Luna-Aceves. A minimum-hop routing algorithm based on distributed information. *Computer Networks and ISDN Systems*,16 (5):367 – 382, 1989..

[31] R. A. Guerin, A. Orda, and D. Williams. Qos routing mechanisms and ospf extensions. In *GLOBECOM 97. IEEE Global Telecommunications Conference*. Conference Record, volume 3, pages 1903–1908 vol.3, Nov1997

[32] E. Akin and T. Korkmaz. Comparison of Routing Algorithms with Static and Dynamic Link Cost in Software Defined Networking (SDN). *IEEE Access*, 7:148629–148644, 2019.

[33] Martin F. Arlitt and Carey L. Williamson. Web server work load characterization: The search for invariants. In *Proceedings of the 1996 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems*, SIGMETRICS '96, page 126–137, New York, NY, USA, 1996. Association for Computing Machinery.

[34] Kihong Park, Gitae Kim, and M. Crovella. On the relationship between file sizes, transport protocols, and self-similar network traffic. In *Proceedings of 1996 International Conference on Network Protocols (ICNP-96)*, pages 171–180, 1996.

[35] A. U. Shah, D. H Bhatt, P. R. Agarwal, and P. R. Agarwal. Effect of packet-size over network performance. *International Journal of Electronics and Computer Science Engineering*, 1:762–766, 2012.

[36] Chuan Lin, Yuanguo Bi, Hai Zhao, Zeshen Wang, and Jinfa Wang. Scheduling algorithms for time-constrained big-file transfers in the internet of vehicles. *Journal of Communications and Information Networks*, 2(2):126–135, Jun 2017.

[37] R. Ghrist and S. Krishnan. A topological max-flow-min-cut theorem. In2013 *IEEE Global Conference on Signal and Information Processing*, pages 815–818, Dec 2013.

[38] Ravindra K Ahuja, Thomas L Magnanti, and James B Orlin. *Networkflows: Theory, applications and algorithms*. Prentice-Hall, Englewood Cliffs, New Jersey, USA Arrow, KJ (1963). Social Choice and Individual Values, Wiley, New York. Gibbard, A. (1973). "Manipulation of Voting Schemes: A general result", Econometrica, 41:587–602, 1993.

[39] Honghua Hannah Yang and D. F. Wong. *Efficient Network Flow Based Min-Cut Balanced Partitioning*, pages 521–534. Springer US, Boston, MA, 2003.

[40] S. Tie-li, D. Jing-wei, and D. Kai-ying. Scale-free network model with evolving local-world. In 2008 *Fourth International Conference on Natural Computation*, volume 1, pages 237–240, Oct 2008

[41] Nada Alzaben and Daniel W. Engels. End-to-end routing in SDN controllers using max-flow min-cut route selection algorithm. In 2021 *23rd International Conference on Advanced Communication Technology (ICACT)*, pages 461–467. IEEE, 2021

[42] Nada Alzaben and Daniel W. Engels. End-to-end routing approach for SDN based wireless ad hoc network. In 2021 *IEEE Symposium on wireless technology and applications (ISWTA)*, 2021, pp. 16-21.

Nada Alzaben. This author became a Member (M'18) of IEEE in 2018. Saudi citizen born in Riyadh, Saudi Arabia. Received her B.S. (2001) and M.S. (2012) in computer science and information from King Saud Univ. in Riyadh, Saudi Arabia.

She is currently working on her Ph.D. in computer science at Southern Methodist Univ., Dallas, TX, USA. Her research interests include network communications, routing and scheduling, network performance analysis. She is a Lecturer in computer science and information college at Princess Nourah Bint Abdulrahman Univ.,

Riyadh, Saudi Arabia. Previously she worked as a senior programmer at King Saud Univ. She has 5 research publications in the field of computer networks and AI.

Dr. Daniel W. Engels received his Ph.D. from the Massachusetts Institute of Technology. Born in the US.

Dr. Engels is currently Head of AI, Cyber security Science and Analytics, at HSBC. Previously, Dr. Engels was a professor at Southern Methodist University (SMU) where he was one of the creators of, and the first Director of, the Master of Science in Data Science (MSDS) program where he grew the program from 0 students to more than 300 students in its first two years of operation In addition to his data science expertise, Dr. Engels is an expert in security and in RFID and IoT technologies, systems, and applications. He was one of the founders of the IEEE International Conference on RFID, and he was the Chair of the IEEE Technical Committee on RFID in 2011 and in 2012. Dr. Engels is the former Director of Research of the Auto-ID Labs at MIT, where he led the development of several RFID protocols including the original "Gen2" protocol, and he is an original member of the research team that founded the Auto-ID Center at MIT and created the EPC System.

He has over 100 peer reviewed publications and 8 issued U.S. patents in data science, RFID, RFID applications, Internet of Things, security, embedded computing, and computer-aided design. Dr. Engels received the 2014 AIM Ted Williams Award in recognition of his contributions to the AIDC industry. Dr. Engels is a member of AIDC 100 and is a Senior Member of IEEE.

Volume 10 Issue 1,2,3,4,5,6, 2021, ISSN: 2288-0003

ICACT-TACT JOURNAL

GIRI
Global IT Research Institute

1713 Obelisk, 216 Seohyunno, Bundang-gu, Sungnam Kyunggi-do, Republic of Korea 13591
Business Licence Number : 220-82-07506, Contact: tact@icact.org Tel: +82-70-4146-4991