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

ICACT-TACT JOURNAL

Transactions on Advanced Communications Technology

Volume 5 Issue 1, Jan. 2016, 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. 5 Issue. 1

Load Adaptive and Fault Tolerant Distributed Stream Processing System for Explosive Stream Data

Myungcheol Lee*, Miyoung Lee*, Sung Jin Hur*, Ikkyun Kim**

*Big Data SW Research Department, ETRI(Electronics and Telecommunications Research Institute), 218 Gajeong-ro, Yuseong-gu, Daejeon, 305-700, Republic of Korea

** Cyber Security System Research Department, ETRI(Electronics and Telecommunications Research Institute), 218 Gajeong-ro, Yuseong-gu, Daejeon, 305-700, Republic of Korea

{mclee, mylee, sjheo, ikkim21}@etri.re.kr

***Abstract*—As smart devices such as sensors, smartphones, and CCTVs are becoming extensively utilized recently, stream data from those smart devices are consistently generated explosively. There are also increasing cases that we notice security attacks after already important assets are damaged by cyber-targeted attacks such as APT attacks due to the lack of real-time security log processing capability. Accordingly, the demand to process and analyse the exploding stream data in real-time and in advance is consistently increasing in many application domains. However, existing distributed stream processing systems like Storm and S4 are not well adaptive when there are drastic increase of input stream data. In this paper, we propose a distributed stream processing system which supports several load adaptation techniques utilizable for various circumstances of explosive data stream, and also supports fault tolerance mechanisms to fail over in several failure situations.**

***Keyword*—Big Data, Distributed Stream Processing, Load Adaptation, Data Explosion, Load Shedding, Task Scheduling, Fault Tolerance**

I. INTRODUCTION

As smart devices such as sensors, smartphones, and CCTVs are becoming extensively utilized recently, stream data from those smart devices are consistently generated explosively and the need to process and analyse the exploding data stream in real-time is increasing [1]-[2].

There are also increasing cases such as eBay hacking(2008), Stuxnet(2010), Nonghyup(2011), and recent 3.20 Cyber Incident (2013.03.20) that we notice security attacks after already important assets are damaged by cyber targeted attacks like APT (Advanced Persistent Threat) attacks. These APT attacks are designed to steal industrial secrets or military secrets from major government agencies or enterprises and customer information, and paralyse the industrial control system and consequently cause tremendous physical damages, or wage an act of war [3].

According to Verizon data breach report [4] published in 2010, even though there were attack and breach logs left for 86% of breach cases, attacked organization's attack detection mechanism was not able to alert security warnings before the actual damage, due to the lack of real-time processing capability.

For providing real-time data processing and analysis to handle these explosive large-volume of stream data and predict future, or detect attack and damages, researches on real-time distributed stream processing systems such as Apache Storm [5] and Yahoo S4 [6] are actively being studied.

Existing distributed stream processing systems support fundamental real-time stream processing functionalities [7], but are not dynamically scalable enough because they are not adaptive when there are drastic increase of input stream data.

In this paper, we propose a distributed stream processing system which supports several load adaptation techniques utilizable for various circumstances of explosive data stream, and also supports fault tolerance mechanisms to fail over in several failure situations.

The remainder of this paper is organized as follows: Section 2 describes the system architecture and programming model of our proposed distributed stream processing system. Section 3 describes several load adaptation techniques for the various circumstances of explosive stream data, which were applied to our proposed distributed stream processing system. Section 4 describes several fault tolerance mechanisms applied to the proposed system. Finally, Section 5 presents the conclusion and future works.

II. DISTRIBUTED STREAM PROCESSING SYSTEM

A. System Architecture

Our proposed techniques were implemented in a

Manuscript received April 29, 2015. This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP). (B0101-15-1293, Cyber-targeted attack recognition and trace-back technology based on the long-term historic analysis of multi-source data)

Myungcheol Lee is with the Electronics and Telecommunications Research Institute, Daejeon, 305-700, Korea (corresponding author to provide phone: +82-42-860-1691; fax: +82-42-860-6699; e-mail: mclee@etri.re.kr).

Miyoung Lee is with the Electronics and Telecommunications Research Institute, Daejeon, 305-700, Korea (e-mail: mylee@etri.re.kr).

Sung Jin Hur is with the Electronics and Telecommunications Research Institute, Daejeon, 305-700, Korea (e-mail: sjheo@etri.re.kr).

Ikkyun Kim is with the Electronics and Telecommunications Research Institute, Daejeon, 305-700, Korea (e-mail: ikkim21@etri.re.kr).

distributed stream processing system depicted in Fig. 1, which consists of a service manager, several service manager candidates, several task execution managers, several task executors, a cluster coordinator, and a metadata storage.

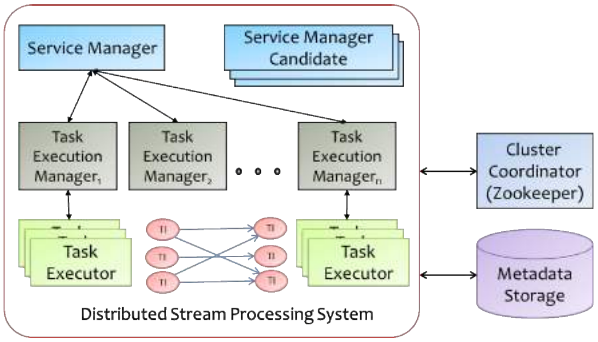


Fig. 1. Distributed Stream Processing System Architecture

Service manager manages entire cluster and schedules task instances of user-defined distributed stream processing service to distributed nodes for parallel execution. Task execution managers manage task executors on each node, and the task executors run each assigned task instances as separate threads in the same process space within the task executor. Task instances are cloned from user-defined task and they run on distributed nodes in parallel by sharing and partitioning the same input data stream.

Cluster coordinator is used for master election in case of master node's failure, and for shared storage and coordination of communication between several cluster components. Metadata storage is for the management of all the data related to the cluster, service, user, and QoS (Quality of Service) preferences.

B. Programming Model

The distributed stream processing system supports DAG(Directed Acyclic Graph) based distributed stream processing programming model to users as in Fig. 2, and the programming model contains input sources, task processing logics and output sources. LamaTask is a DAG node for representing task processing logic, and LamaInput and LamaOutput are DAG nodes for representing communication with external input and output sources.

Users write their distributed stream processing service according to the programming model, and the tasks containing processing logic belonging to the service are dispatched to distributed nodes and run continuously in parallel as task instances. The data communicated by each task instances are represented in key/value-based record stream.

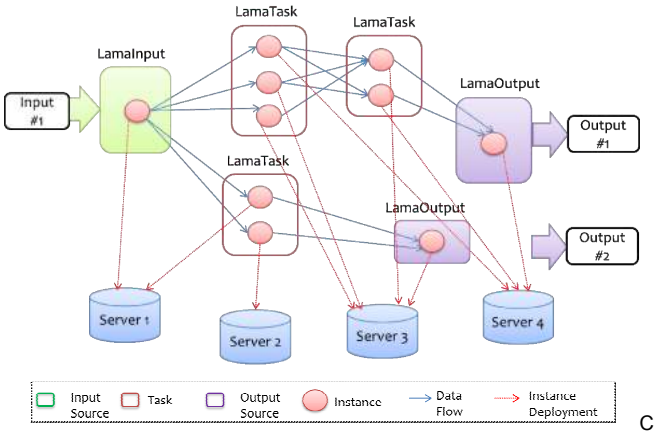


Fig. 2. Distributed Parallel Stream Processing Model

Common stream data model are defined as LamaRecord so that users can process various structured and unstructured stream data generated from diverse application environments. LamaRecord consists of key and value pair, where key is represented as String, and value is represented as POJO (Plain Old Java Object) which can be any primitive Java type or user-defined object type. Programming model components like input sources, tasks, output sources exchange data each other as a stream of LamaRecords as in Fig. 3.

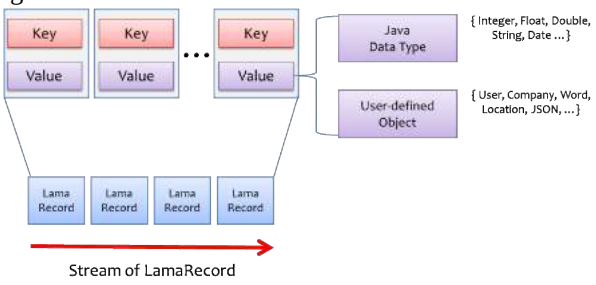


Fig. 3. Stream Data Model

We provide an abstract class called ILamaTask for users to implement their processing logic as task in Java language, and users define tasks by extending ILamaTask abstract class and implementing the processing logic inside the ILamaTask's execute() method just as defining the MergeTask class in Fig. 4.

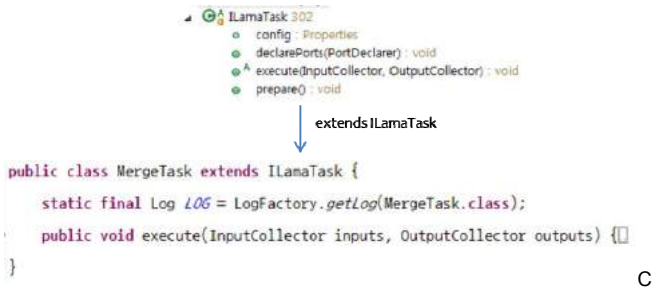


Fig. 4. Implementation of User-defined Task

ILamaTask abstract class has other several methods supporting the implementation of user-defined tasks.

- void prepare(ServiceConf config) : define what needs to be prepared before initially running execute() method

- void execute(InputCollector inputs, OutputCollector outputs) : user processing logic is implemented inside execute() method
- void declarePorts(PortDeclarer declarer) : define input port number, output port number, whether to synchronize all the input ports, etc.

C

```
// from any channel
List<LamaRecord> records = inputs.get();
for (LamaRecord record : records) {
   String key = record.getKey();
   Object value = record.getValue();
   // Process key/values here
   // …

   // Generate new key/values here
   String newKey  = …;
   Object newValue = …;
   // new LamaRecord is created inside emit()
   outputs.emit(newKey, newValue);
}
```

C

Fig. 5. Reading and Writing Key/Value Pairs

Fig. 5 depicts how users read and write the stream data inside execute() method. Users access input data by calling InputCollector.get(), LamaRecord.getKey(), and LamaRecord.getValue(), and send the processing results to next tasks by calling OutputCollector.emit().

Port is used for data transmission between input sources, task, and output sources as in Fig. 6. There is a channel for data communication established between preceding port (output port of any input source or task) and following port (input port of any output source or task), and the channels can communicate only one kind of data, or with the same schema (key, value).

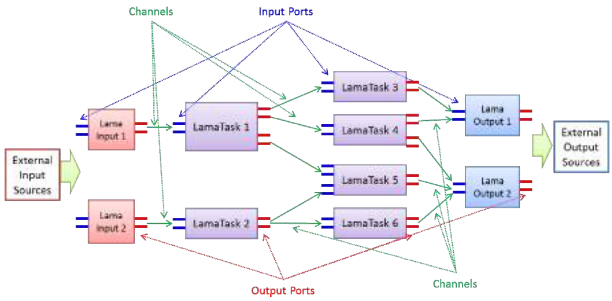


Fig. 6. Port-based Inter-Task Communication

Input source and output source are allowed to have exactly one input port and one output port, and tasks can have several input and output ports by user's definition, but the default number is one. For example, LamaTask 5 in Fig. 6 has 2 input ports and 1 output port, and input port 0 has 1 input channel from LamaTask 1's second output port and input port 1 has 1 input channel from LamaTask 2's first output port, and output port 0 has 1 output channel to LamaOutput 2's input port 0.

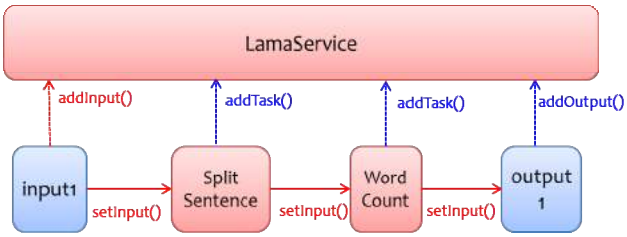


Fig. 7. Defining Distributed Stream Processing Service

Basic procedure for defining distributed stream processing service begins with creating LamaService object, and then create InputSource object and then register the created input source to the service object by calling LamaService.addInput() as in Fig. 7. All the subsequent tasks and output sources are registered to the service by calling previous tasks' LamaTask.setInput() method.

We support multiple input and output ports for tasks and multiple channels between ports, and users also define the specifics of input and output ports when they define tasks.

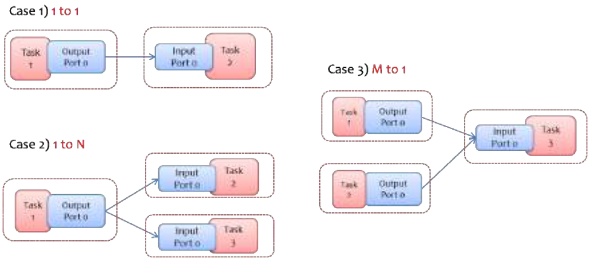


Fig. 8. Relationship between I/O Ports

Relationship between input and output ports are classified as in Fig. 8. 1 to 1 is for exchanging data directly between 1 input port and 1 output port, and 1 to N is used for broadcasting data from 1 input port to several output ports, and M to 1 is used for collecting output data generated from several tasks into a task and perform reduction operation.

Users can choose whether they would access synchronously or asynchronously data from multiple input ports as depicted in Fig. 9. In the synchronous mode, whenever data are ingested at *all* the input ports, user-defined ILamaTask.execute() method is called. Inside the execute() method, users can access data from each port by calling InputCollector.get(port) method with port index argument. In asynchronous mode, whenever data are ingested at *any* one of the input ports, user-defined ILamaTask.execute() method is called, and users can access the ingested data by calling InputCollector.get() method without port index argument.

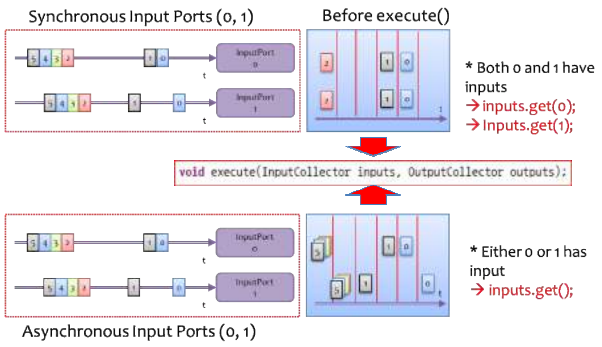


Fig. 9. Synchronous and Asynchronous Data Access from Multiple Input Ports

The synchronized access mode between multiple input ports is predefined using PortDeclarer.syncInputPorts(boolean flag) method and the PortDeclarer is set to the task by overriding ILamaTask.declarePorts(PortDeclarer declarer) when extending ILamaTask.

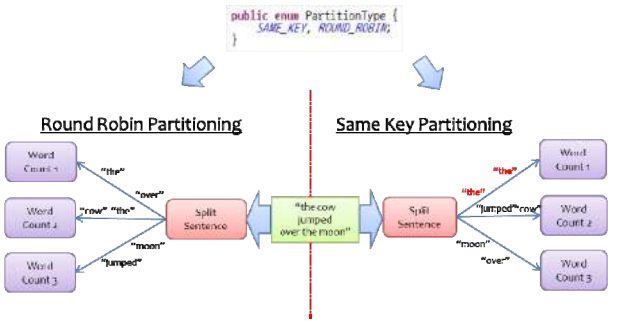


Fig. 10. Data Partitioning Scheme

Our proposed distributed stream processing system supports 2 kinds of partitioning scheme, which are used for partitioning data from several instances of previous task to several instances of next task. ROUND_ROBIN scheme is used for load balanced partitioning and SAME_KEY is used for sending the data with the same key to the same target instance, and which is useful for receiving the same classes of data, as in counting words shown in Fig. 10.

C. *Dynamically Optimized Communication Channel*

The distributed stream processing system supports optimized communication channels between task instances based on their execution location. If the two task instances, which communicate data each other, run on the same node, they run as separate threads in the same task executor process, and they exchange data using a common queue as the non-serialized data object itself. There are no serialization and deserialization overhead required for communicating the data in this case. On the other hand, if the two task instances, which communicate data each other, run on the different nodes, they run as separate threads in the different task executor processes on different nodes, and they exchange data using TCP-based sockets, and the data need to be serialized to array of bytes using Kryo [8] or Java's serialization mechanism [9] and after the transmission, the data need to be deserialized back to Java objects to be accessed by the consuming task instances.

In our experimental observation, in the extremely optimized distributed stream processing system execution, most of the overhead was generated by the object serialization and deserialization for TCP-based communication between nodes. Based on this observation, our proposed system tries to schedule task instances, which communicate data each other, on the same node as possible.

D. *Stream Data Window*

Our proposed system provides stream data windowing function so that users can process unbounded structured and unstructured stream data by limiting them as a sequence of bounded data batches. Time-based and count-based window types are supported, and both of the windows are defined by the window size and how much to slide the window as time elapses or as data are ingested. In a time-based window, window size and sliding size is defined in the millisecond unit, and in a count-based window, window size and sliding size is defined as the number of records.

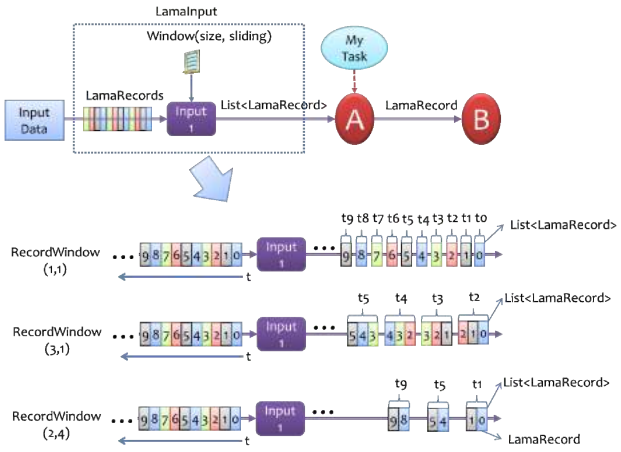


Fig. 11. Stream Data Window

Window is defined at the input source by calling e.g. LamaInput.setWindow(window_type, window_size, sliding_size) method and the input source slices the input data as defined by the window definition. Examples of more detailed window operations are depicted in Fig. 11.

III. Load Adaptation Techniques

All the load adaptation techniques applied to the proposed distributed stream processing system are summarized in Table I, and the detailed explanation for each technique follows in the next subsections.

TABLE I
Load Adaptation Techniques for Distributed Stream Processing Systems

Purpose	Technique
Inter-node Load Balance	– Load-aware Instance Dispatch
Inter-task Load Balance	– Load-aware CPU Scheduling
Increasing Processing Capability	– Task Split and Merge – Task Migration – Adding More Nodes
Load Shedding	– Input Data Shedding

A. *Load-aware Instance Dispatch*

In a distributed stream processing system, user-defined tasks are split into several task instances for exploiting data parallelism and dispatched by global scheduler to different nodes for parallel execution. If we dispatch task instances on the node with the least load, we can shorten the processing time and the latency when users access the outputs.

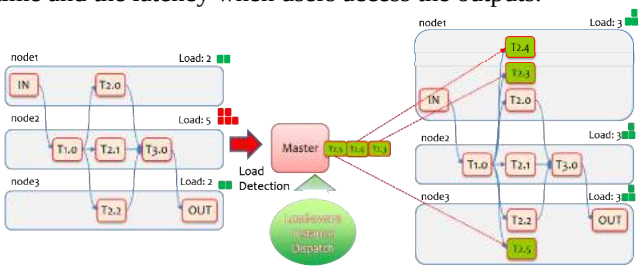


Fig. 12. Load-aware Instance Dispatch

Our global scheduler gathers load status information from

each worker nodes and mark their status as “NORMAL” or “OVERLOADED”, and dispatch task instances to “NORMAL” nodes preferentially, for example node2 in Fig. 12 is the most loaded node, therefore the global scheduler dispatches T2.3 and T2.4 to node1, and T2.5 to node3, and no task instances to node2.

B. *Load-aware CPU Scheduling*

Task instances dispatched to each nodes are executed by task executors running on each nodes, and they run as separate threads inside the task executor processes and have their own input queue for receiving data from previous tasks or input sources.

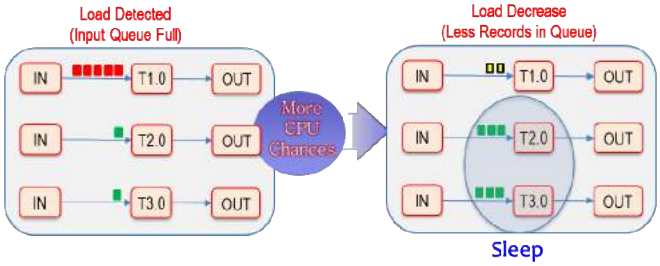


Fig. 13. Load-aware CPU Scheduling

Our local scheduler monitors each input queue’s load, or whether there are any waiting records. If there are any waiting records in the queue, it means that the task instance bound to the input queue is not processing fast enough for the input data rate. Local scheduler marks each instance as “NORMAL”, “YELLOW”, and “RED” according to the number of waiting records in their input queue, and try to make more CPU times assigned to the more loaded task instance by having the less loaded task instances to sleep for a while as in Fig. 13.

C. *Task Split and Merge*

If all the task instances, which belong to the same task, are overloaded in all the nodes, and there are still available resource in the cluster, global scheduler increases the data parallelism of the task by adding more task instances to the task. The added task instances can share the input data load and lower the burden of existing task instances as in Fig. 14.

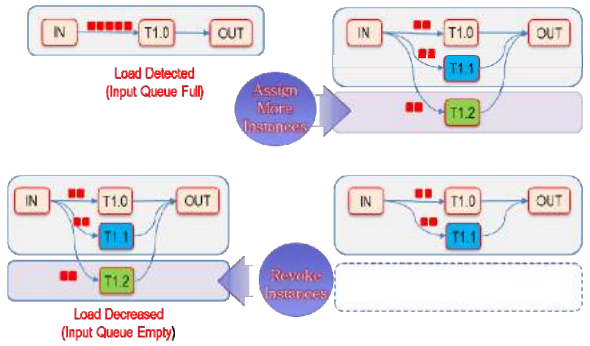


Fig. 14. Task Split and Merge

This task split technique can be applied to only the tasks that their data partitioning is ROUND_ROBIN, and the task instances before and after the newly added task instances are notified of the new task instances and their communication channels are re-established to exchange data with the new task instances.

D. *Task Migration*

If a node is fully utilized and the task instances running on the node cannot be split into more instances, then the global scheduler migrates the less loaded task instances to another idle nodes as in Fig. 15 so that they are not affected by other heavy task instances. The migrated task instances need to store their current input queue data and memory status into the persistent storage for the continuation of execution after the migration.

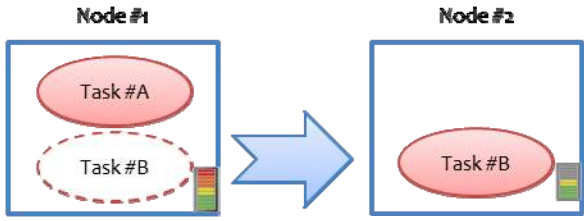


Fig. 15. Task Migration

E. *Adding More Nodes*

If load of all the nodes are close to their limit, system manager can add more nodes to the cluster so that entire cluster can handle more explosive data stream and have more distributed stream processing capability.

Global scheduler recognizes immediately the dynamically added nodes by system manager. By system manager’s option, the global scheduler performs immediate rebalancing among entire nodes or let the newly added nodes be utilized for later dispatch only.

When rebalancing is performed, service manager detects the most loaded node and migrates the task instances running on the node to the newly added node, and the inputs and outputs of the migrated task instances are all re-established according to the new service topology.

If service load becomes lower as time elapses, some of the nodes will become idle, and the idle nodes might be excluded from the cluster and returned back to free pool by system manager’s preference.

F. *Load Shedding*

In case there are no more resources available, global scheduler decides to drop data at the input source layer as in Fig. 16. Users can specify their satisfaction for service execution as QoS (Quality of Service) in our system, where four QoS items such as acceptable shedding rate, acceptable latency, whether to do recovery, and finally whether to preserve order between data are supported. Only the services for which user has specified shedding rate as more than 0 are chosen for load shedding.

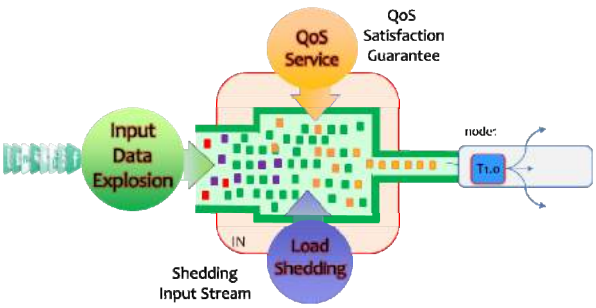


Fig. 16. Load Shedding

IV. Fault Tolerance

Our proposed distributed stream processing system

supports 3 kinds of fault tolerance techniques (master failover, node failover, and instance failover) so that users' distributed stream processing service can seamlessly run even in the various failure situations.

A. Master Failover

In the normal cluster startup, service manager writes its address to ZooKeeper's master address node in ephemeral mode to notify service manager candidates and task execution managers that it is now the master. All the other components hold watcher on the ZooKeeper's master address node. If service manager dies, the address in the master address node disappears with the node itself because the node was ephemerally written. And the deletion of the master address node is notified to all the components which have left watchers for the node.

All the service manager candidates tries to write their address to the master address node, and one of them wins the race and becomes the new master, and the election of new service manager is notified to all the other components, and they try to communicate with the new service manager and report their status to the new service manager.

Eventually the new service manager gets to know the cluster status and the execution status of all the distributed stream processing service and task instances seamlessly.

B. Node Failover

If a node is in trouble, it is detected by the global scheduler, and all the task instances running on the failed node become the target of the new scheduling. The task instances are dispatched by the global scheduler to other normal nodes and the communication channels between the task instances and preceding/following task instances are reestablished using the instance channel information stored in ZooKeeper.

As a first step, the new task instances try to connect to their output targets using targets' channel information acquired from ZooKeeper, and they create new TCP ports for their input ports and store the new channel information to ZooKeeper, and in turn their preceding tasks need to update their output channels to the new task instances by getting channel information from ZooKeeper. Thus, only the instance channel information about receivers are stored in the ZooKeeper node in the name of "receiver_instance_id@input_port" with the value of "receiver_host_name:tcp_port".

All the task instances acquire the receivers' channel information from ZooKeeper and compare if both of the senders and receivers run on the same node by comparing the "receiver_host_name" with the host name of their own execution node. If they run on the same node, the sender establishes common queue based communication channel with the receiver. Otherwise, the sender establishes TCP socket channel to the receiver with the acquired "receiver_host_name:tcp_port" information.

Newly established instance channel information are again stored in ZooKeeper also for later failover activities.

C. Instance Failover

If a task instance fails suddenly, it is detected by global scheduler. And the global scheduler dispatches the failed task instance to another normal node, and the communication channels between new task instance and preceding/following tasks are reestablished as explained in the previous section. If the task instance continues to fail several times and the failure count reaches the predefined threshold, the task instance is marked as failure and excluded from rescheduling since then.

V. Conclusion

In this paper, we proposed a new distributed stream processing system which supports several load adaptation techniques to process explosive stream data in distributed stream processing environments and several fault tolerance techniques for resilient distributed stream processing in the various failure situations.

Our proposed system provides stream data model, and stream data programming model, multiport-based communication mechanism, several data partitioning schemes, and dynamic optimized communication channels between tasks. Our proposed load adaptation techniques are designed considering various conditions of nodes and tasks, and classified as inter-node load balancing, inter-task load balancing, increasing processing capability, and finally load shedding for the last way to avoid entire system halt due to the data explosion. Our proposed fault tolerance techniques are designed considering various failure situations like master, node, and instance failure.

We just implemented the load adaptation techniques and the fault tolerance techniques in the distributed stream processing system and are going to experiment the usefulness of them thoroughly in a real-world environment as future works. We hope our proposed techniques are useful as a hint for flexibly handling problems in many data processing domains experiencing input data explosion or fluctuation, and seamlessly providing distributed stream processing service in various failure situations.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government(MSIP). (B0101-15-1293, Cyber-targeted attack recognition and trace-back technology based on the long-term historic analysis of multi-source data)

References

[1] Mark A. Beyer, Anne Lapkin, Nocholas Gall, Donald Feinberg, Valentin T. Sribar, "Big Data Is Only the Beginning of Extreme Information Management," *Gartner*, 2011.

[2] John F. Gantz, "The Diverse and Exploding Digital Universe," *IDC*, 2008.

[3] Colin Tankard, "Advanced Persistent threats and how to monitor and deter them," *Network Security*, vol. 2011, no. 8, pp. 16-19, 2011.

[4] Verizon Inc., "2010 Data Breach Investigation Report," 2010, *http://www.verizonenterprise.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf*

[5] Storm Project, Available at https://github.com/nathanmarz/storm/wiki/ (referenced at Sep. 1, 2014)

[6] Leonard Neumeyer, Bruce Robbins, Anish Nair, Anans Kesari, "S4: Distributed Stream Computing Platform," *Proc. of ICDMW 2010*, pp.170-177, Sydney, 2010

[7] Miyoung Lee, Wan Choi, "Trends of Big Data Processing Technology for Big Data Analytics," *Korea Information Processing Society Review*, vol.19, no.2, pp.20-28, 2012 (in Korean)

[8] Kryo Project, Available at http://code.google.com/p/kryo/ (referenced at Sep. 1, 2014)

[9] Java Object Serialization Spec, Available at http://docs.oracle.com/javase/8/docs/platform/serialization/spec/serial-arch.html (reference at Sep. 1, 2014)

Myungcheol Lee (M'2015) received his Bachelor's Degree in Computer Engineering and his Master's Degree in Computer Engineering from Chungnam National University, Daejeon, Korea in 1999 and 2001, respectively. He became a Member (M) of IEEE in 2015. He is now a senior researcher at ETRI since 2001. His research interest includes Big Data processing and analytics, database, cloud computing, and distributed computing.

C

Miyoung Lee received her Bachelor's Degree in Food and Nutrition, and Master's Degree in Computer Science and Statistics from Seoul National University, Seoul, Korea in 1981 and 1983, respectively. She received her Doctor's Degree in Computer Engineering from Chungnam National University, Daejeon, Korea in 2005. She is now a principal researcher at ETRI since 1988. Her research interest includes big data management and processing, database, and distributed computing.

Sung Jin Hur received his Bachelor's Degree in Electronics, Master's Degree and Doctor's Degree in Computer Engineering from Kyungpook National University, Daegu, Korea in 1990, 1992 and 1999, respectively. He was a professor at Changsin University from 1999 to 2001, and is now a principal researcher at ETRI since 2001, and is leading Data Management Research Section. His research interest includes database, stream data processing, cloud computing

C

Ikkyun Kim received his Bachelor's Degree, Master's Degree and Doctor's Degree in Computer Engineering from Kyungpook National University, Daegu, Korea in 1994, 1996, and 2009, respectively. He was a visiting researcher at Purdue University from 2004 to 2005. He is now a principal researcher at ETRI since 1996, and is leading Network Security Research Section. His research interest includes network security, computer network, cloud security, big data analytics.

A Triple Hill Cipher Algorithm Proposed to Increase the Security of Encrypted Binary Dataand its Implementation Using FPGA

Ashraf A.M. Khalaf, Mona S. Abd El-karim,Hesham F. A. Hamed
Department of Electronics & Communications Engineering, Faculty of Engineering, Minia University, Minia, Egypt
ashkhalaf@yahoo.com,engmona1889@gmail.com,hfah66@yahoo.com

***Abstract*—Encrypted binary data security is an important task in the field of data communication systems since many decades. In this paper,we study the security problem and present a proposed triple hill cipher algorithm and its implementation on FPGA to encrypt any binary data such as images , audio , video … etc. The proposed algorithm uses three stages of a modified hill cipher to make the algorithm more robust and gives high level security of the data,each stage is considered a block cipher with a block length of 128 bits and key length of 256 bits. The message to be encrypted is processed by this block cipher in three stages. The keys are taken from random number generator. The proposed algorithm is promising to give better security.**

***Keyword*—hill cipher , 256 bit key ,cryptography, VHDL, FPGA.**

I. INTRODUCTION

Nowadayssecurity becomes an important feature with the growth of electronic communication systems. Cryptography is one of the methods used to protect data from unauthorized access and being stolen [1]. Cryptography is the science and study of secret writing. A cipher is a secret method of writing , whereby plaintext is transformed into cipher text .The process of transforming plaintext into cipher text is called encryption. The reverse process of transforming cipher text into plaintext is called decryption. Both encryption and decryption are controlled by a cryptographic key or keys [2][3].

There are two types of cryptosystem, which are symmetric cryptosystem and asymmetric cryptosystem. In Symmetric cryptosystem, the sender and recipient share the same key. It means the same key is used for encryption and decryption. In Asymmetric cryptosystem, different keys are used. A public key is used by sender to encrypt the message while the recipient used a private key to decrypt it [1][2].

In this paper we focus on hill cipher which is a type of symmetric cryptosystem.

The hill cipher was first described in 1929 by its inventor, the mathematician Lester S. Hill, in the journal of the american mathematical monthly (Eisenberg, 1998).[1][3][4]

The hill cipher is a classical symmetric cipher based on matrix transformation. It has several advantages including its resistance to frequency analysis and simplicity due to the fact that it uses matrix multiplication and inversion for encryption and decryption. However, it succumbs to the known plaintext attack [5] and as such there have been efforts to strengthen the cipher through the use of various techniques which have improved the security of the cipher quite significantly [6],[7],[8].

In this paper, we present a proposed *triple hill cipher algorithm* which consists of three stages of hill cipher ,each stage is considered a block cipher with a block length of 128 bits and key length of 256 bits. The message to be encrypted is processed by this block cipher in three stages to increase the security. The keys are taken from random number generator. Each stage consists of eight rounds with different eight keys , in each round three operations are implemented ; key and plaintext matrix multiplication , stir operation and XOR operation . this will be discussed in details in section III .we expect to achieve an algorithm more robust to cryptanalysis as we will use three layers of security.

The reason for using three stages is that, we used the concept of the common triple DES algorithm which is standardized by ANS X9.52 and is used to enhance the DES algorithm [12].

II. THE BASIC CONCEPT OF THE CLASSICAL HILL CIPHER

Hill Cipher was the first polygraphic cipher in which the key (K), plain text (P), and cipher text (C) are represented in the form of matrices. The basic method of encryption and decryption is represented by the following equations[9][10].

Manuscript received July 9 , 2015. This work was self-supported, and a follow-up of the invited journal to the accepted conference paper of the 17th International Conference on Advanced Communication Technology, and without Grants (Self -support).
Ashraf M. Khalaf is with the Faculty of Engineering, Department of Electrical Engineering. (Corresponding author, Phone: +20 86 2355261; fax: +20 86 2346674; e-mail: ashkhalaf@yahoo.com).
Mona S. Abd El-karim, is with the Faculty of Engineering, Departement of Electrical Engineering. (Phone: +201116123919; e-mail: engmona1889@gmail.com).
Hesham F. A. Hamedis with the Faculty of Engineering, Department of Electrical Engineering. (E-mail:hfah66@yahoo.com).

$$C = (K\,P) \bmod (26) \quad (1)$$

$$P = (K^{-1}\,C) \bmod (26) \quad (2)$$

where K^{-1} is the inverse of key matrix

Here modulo 26 arithmetic is used as the study was performed on the English alphabet, where each letter (Alphabet) is allotted a number generally starting from 0 in a continuous sequence one after the other as shown in Fig. 1 [3].

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Fig. 1 Alphabet Numbering

As shown in figure 1, Alphabets are numbered as A equals 0, B equals 1,... , and Z equals 25, but this is not a fixed requirement of the cipher. The encryption of plain text takes n successive plain text letters and substitutes them for n cipher text letters. In case n = 3, the encryption can be expressed in terms of the matrix multiplication as follows[3]

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{21} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \bmod(26) \quad (3)$$

III. THE PROPOSED TRIPLE HILL CIPHER ALGORITHM

As shown in Fig. 2 the proposed Triple Hill Cipher algorithm consists of three stages ,where plaintext is encrypted three times using three different 256 bits keys.

Keying options :

- Option 1: k_1 ,k_2 and k_3 are different (not equal).
- Option 2: k_1 ,k_2 are different and k_3 equal to k_1, this option is considered double encryption ,but it is stronger than simply hill cipher encrypting twice, e.g with k_1 and k_2 because it protects against meet in the middle attack[13],
- Option 3: k_1 ,k_2 and k_3 are the same, this option is considered the least secure one.

In our proposed algorithm we used the first option 1, the key of the first stage is taken from random number generator ,then 1st key is rotated one time to get the 2nd key and two times to get the 3rd key or we can take the three keys from different generators.

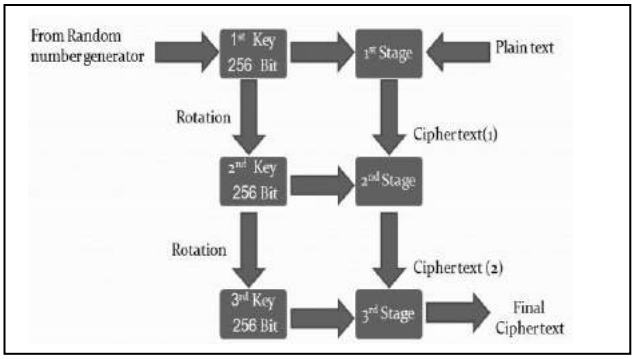


Fig. 2 The Proposed Triple Hill Cipher Algorithm

Random number generators (RNGs)

Is a computational or physical devices designed to generate a random sequence of numbers or symbols. There are two types of these generators:

- True Random Number Generators (TRNGs) which divided into two categories physical and nonphysical TRNGs[14]. Physical TRNGs use nondeterministic effects of electronic circuits such as shot noise from zener diode, inherent semiconductors thermal noise, and free running oscillators. They produce a truly random numbers. Their outputs depend only on physical or nonphysical process not on any initial value.
- Pseudo Random Number Generators (PRNGs) is considered an algorithm to generate a sequence of numbers that appear random. The sequence is not truly random in which it is completely determined by an initial value called a seed. There are several techniques used to perform PRNGs such as Linear Feedback Shift register, Linear Congruential Generator and Blum BlumShub[15].

In this paper we will use PRNG with the Linear Feedback Shift register (LFSR).

Linear Feedback Shift Register (LFSR)

A LFSR is made of sequential shift-register with combinational feedback logic connected to it which can generate a sequence of binary values in a pseudo-random manner.

Feedbacks around an LFSR's shift register are connected to the certain points (taps) of LFSR construction and constitute either XORing or XNORing these taps to provide taps back into the register.

The selection of taps determines how many values can be generated in a given sequence before the sequence is repeated. A certain tap arrangements lead to amaximal length sequences of $(2^n - 1)$. These settings are calculated for different lengths of LFSRs and are represented in[16].

In our algorithm, we need a 256 bit LFSR to get pseudo random keys to enhance the security of the proposed algorithm. Our cipher is symmetric (sender and receiver share the same key) so when we use random keys at transmitter we need to synchronize these keys with the receiver's keys, we can do that by using the same seed at transmitter and receiver.Here we will explain four-bit LFSR as example:

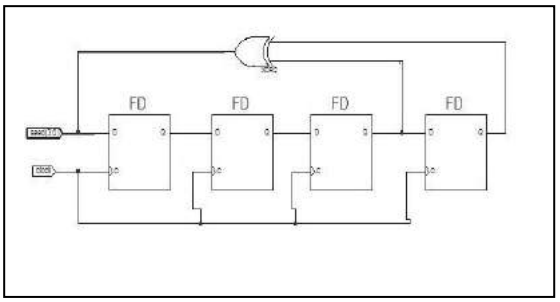


Fig. 3 Four-bit LFSR

As shown in Fig. 3, four-bit LFSR consists of four D-flip flops and xor gate in its shift path. The feedback taps are selected from taps 3 and 4. When LFSR seed is loaded to the four flip flops ,LFSR generates random numbers startingfrom an initial value selected by the user.

A. Steps of the proposed algorithm

Each stage in this algorithm includes eight rounds and sub keys generation module as shown in Fig. 4.

For the first stage ; plaintext is divided into blocks of lengths 128 bits ,each block is represented in 4 by 4 byte matrix .

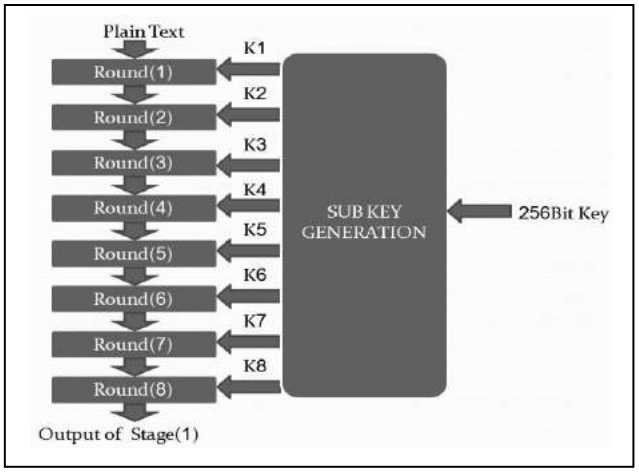


Fig. 4 Single Stage Diagram

Sub keys generation:

128 bits sub keys are generated from the 256 bits key as follow :

The 1st sub key k_2 is obtained by taking the bits from 255 to 224 , from 191 to 160 ,from 127 to 96 and from 63 to 31.

$$k_1 = \text{key}(255 \text{ downto } 224)\&key(191 \text{ downto } 160)\& \text{key}(127 \text{ downto } 96)\&key(63 \text{ downto } 32) \quad (4)$$

The 2nd sub key k_2 is obtained by taking the bits from 223 to 192 , from 159 to 128 ,from 95 to 64 and from 31 to 0 .

$$k_2 = \text{key}(223 \text{ downto } 192)\&key(159 \text{ downto } 128)\& \text{key}(95 \text{ downto } 64)\&key(31 \text{ downto } 0) \quad (5)$$

The 3rd sub key k_3 is obtained by taking the bits from 255 to 160 and from 31 to 0.

$$k_3 = \text{key}(255 \text{ downto } 160)\&key(31 \text{ downto } 0) \quad (6)$$

The 4th sub key k_4 is obtained by taking the bits from 127 to 32 and from 159 to 128.

$$k_4 = \text{key}(127 \text{ downto } 32)\&key(159 \text{ downto } 128) \quad (7)$$

The 5th sub key k_5 is obtained by taking the bits from 223 to 96.

$$k_5 = \text{key}(223 \text{ downto } 96) \quad (8)$$

The 6th sub key k_6 is obtained by taking the bits from 95 to 0 and from 255 to 224.

$$k_6 = \text{key}(95 \text{ downto } 0)\&key(255 \text{ downto } 224) \quad (9)$$

The 7th sub key k_7 is obtained by taking the bits from 31 to 0 and from 255 to 160.

$$k_7 = \text{key}(31 \text{ downto } 0)\&key(255 \text{ downto } 160) \quad (10)$$

The 8th sub key k_8 is obtained by taking the bits from 159 to 32.

$$k_8 = \text{key}(159 \text{ downto } 32) \quad (11)$$

Each of k_1 ,k_2 , k_3 ,k_4 ,k_5 ,k_6 ,k_7 and $k_8$is then represented in 4 by 4 byte matrices .

B. Operations in each round

Each round includes three operations as shown in Fig. 5.

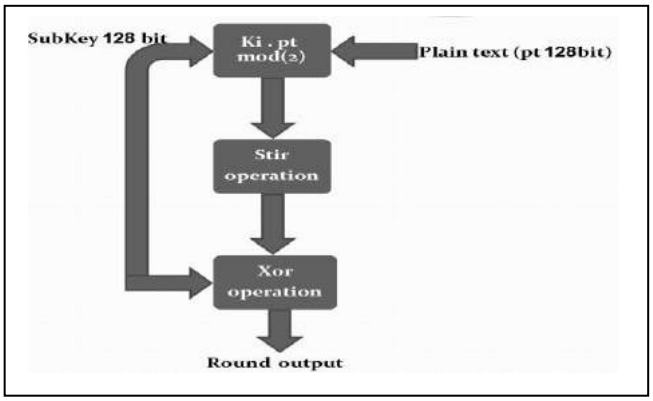


Fig. 5 Single Round Diagram

Operation 1 represents matrix multiplication of plaintext (pt) and sub keys (k_i), where k_i represents k_1 ,k_2 , k_3 ,k_4 ,k_5 ,k_6 ,k_7 and k_8.Here we encrypt any binary data ,so we use modulo 2 field , when values in the matrices are multiplied, bitwise AND is used and when values are added bitwise XOR is used[10][11].

At decryption process the same operation is performed but instead we use the inverse matrices of the sub keys.

Operation 2 represents the Stir operation

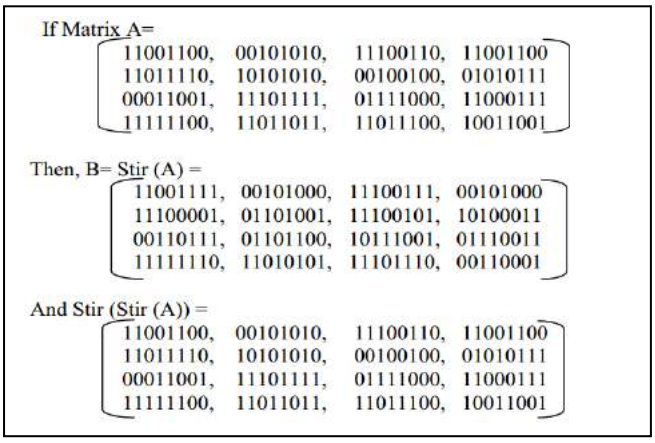


Fig. 6 Stir operation

As shown in Fig. 6, the stir operation is defined by the following steps:

- The 1st and 2nd bits from each byte in a row of A are combined to form the first byte of B in that row.
- The 3rd and 4th bits from each byte in a row of A are combined to form next byte of B in that row.
- The 5th and 6th bits from each byte in a row of A are combined to form next byte of B in that row.

- The 7th and 8th bits from each byte in a row of A are combined to form the last byte of B in that row.
- This stir operation is reversible, i.e. Stir(Stir(A))=A[9].

Operation 3 represents XOR operation
We perform XOR between sub keys k_i and the output of stir operation .it is performed as bit by bit XOR ,as example if we have $M = 11110000$ and $L = 00110011$ then $XOR(M, L) = 11000011$
XOR operation is reversible if $N = XOR(M, L)$
then$L = XOR(N, M)$ and $M = XOR(N, L)$.

The three operations of the round are repeated eight times with different sub keys for k_i=1:8 to perform one stage of the Triple Hill Cipher , so to perform the triple hill cipher we repeat the stage three times ,so we can achieve an algorithm more robust to cryptanalysis.

Summary of The Proposed Triple Hill Cipher Algorithm

i. Encryption process

1. Read the message (plaintext) as a binary and divide it into blocks of lengths 128 bits ,then is represented in 4 by 4 byte matrices
2. 128 bits sub keys matrices (k_i =1:8) are generated from 256 bits key
3. Find inverse of the sub keys matrices
4. If the matrices are noninvertiblechange the key and go to step 2
5.

$for\ m = 1:3$
{
$for\ i = 1:8$
{
$p_{m1} = (k_i . pt)\ mod(2)$
$p_{m2} = stir(p_{m1})$
$p_{m3} = XOR(k_i, p_{m2})$
$pt = p_{m3}$
}
}
$c = pt$

Where pt is the plain text ,c is the cipher text ,m is the number of stages and i is the number of rounds.

i. Decryption process

1. Prepare the inverse of the sub keys matrices k_i^{-1}.
2.

$for\ m = 1:3$
{
$for\ i = 1:8$
{
$c_{m1} = XOR(k_i, c)$
$c_{m2} = stir(c_{m1})$
$c_{m3} = (k_i^{-1} . c_{m2})\ mod(2)$
$c = c_{m3}$
}
}
$pt = c$

IV. SIMULATION AND IMPLEMENTATION RESULTS

A. Simulation results

The proposed algorithm is coded using VHDL language and simulation results taken from Modelsim6.0C as sown in the following figures:

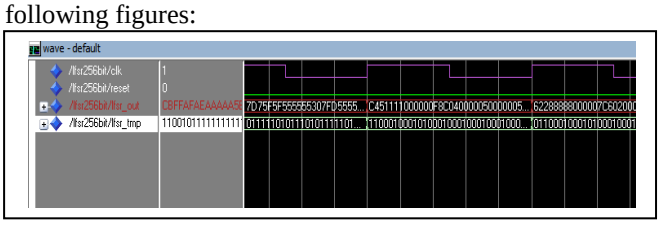


Fig. 7 Timing Simulation of The 256 bit LFSR

Fig. 7 shows timing simulation of the 256 bit LFSR which works as a pseudo random number generator ,as shown in figure in each clock cycle different bits are generated.

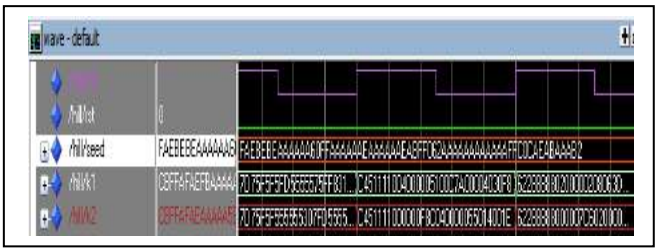


Fig. 8 Timing Simulation of the sub keys generation

Fig. 8 shows Timing simulation of sub keys generation process from the 256 bit key , as shown in figure in each clock cycle k_1 ,k_2 , k_3 ,k_4 ,k_5 ,k_6 ,k_7 and k_8 are generated with different values depending on the value of the 256 bit key used.

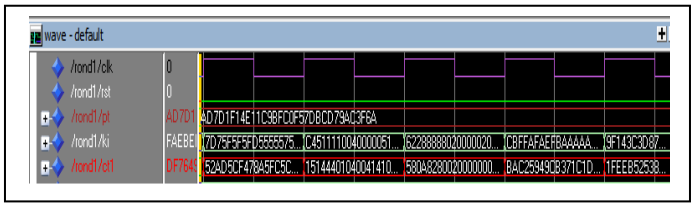


Fig.9 Timing simulation of one round

Fig. 9 shows timing simulation of one round ,wherept is the plain text , $k_i$is the 128 bit sub key and ct is the cipher text from one round ,as shown we have ct with different values and this process is repeated eight times in each stage.

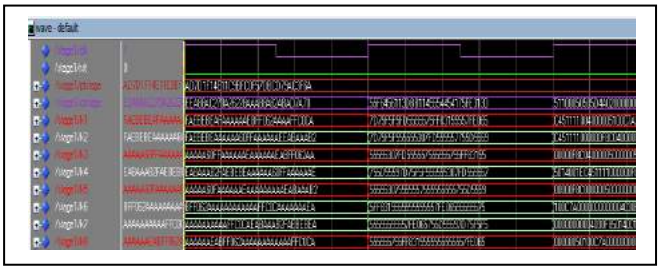


Fig.10 Timing Simulation of one stage

Fig. 10 shows the timing simulation of one stage from the encryption process, where ptstage is the plain text and ctstage is the cipher text from one stage, also we note the contents of the cipher text changes in each clock cycle and this process is repeated three times.

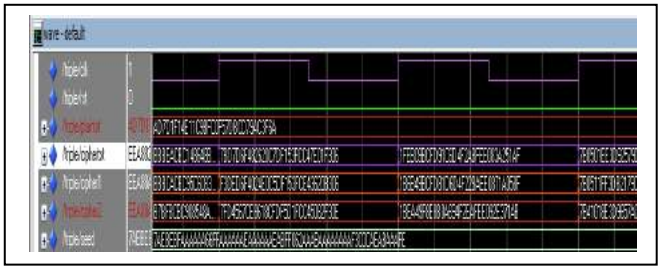


Fig. 11 Timing Simulation of the overall Proposed Triple Hill Cipher

Fig. 11 shows the timing simulation of the overall proposed algorithm, where plaintext is the input message needed to be encrypted, seed is the initial value of the pseudo random number generator to get the random 256 bit keys, cipher1 is the cipher text from the first stage,cipher2 is the cipher text from the second stage and ciphertext is the final cipher text which is the output of the third stage

Because of using random number generator to get keys we get cipher text with different values in each clock cycle which enhance encryption process and make the attacker's task more difficult.

We used this data during the simulation process,here data is arranged as vectors of bits.
256 bits first key:
1111101011101011111010111110101010101010101010101010
1010011000001111111110101010101010101010101010101110
1010101010101010101010101011101010101111111111110000
0110001010101010101010101010101010101010101010101010
1010101011111111110000001100101011101010101110101010
1010101010110010

Plaintext:
1111111111010101010101010101010101010101010101010101
0100000000001111111111010101010110101010100011000
1100110101010101010101010101010101

The outputs of the three stages is
Cipher text1:
1110111010101000100010001100001001010100101000100
0110001011101000101010101010100010001000100000010
1010111110101101111100101011000 0
Cipher text 2:
0101010011110010010001000110000100000000111011111
0011000101010100010101000101000001000100010000001
0111010011111010001100010101000 0
Cipher text 3 which also is the Final Cipher text of the proposed algorithm :
0010101001111011001010000011001010000011010001111
1001101011101010001010100010101000010100000100010
1001000001111111001100100011000 0
As shown from the simulation results,plain text is encrypted three times ,which proves that our proposed algorithm increases the difficulty in cryptanalysis .

B. Implementation results

FPGA implementation of the proposed algorithm was accomplished on Space-Grade Virtex-4QV XQR4VSX55-10CF1140 using Xilinx ISE Design Suite 13.2 as synthesis tool.The top level RTL schematic of the proposed algorithm as shown in figures is given to establish the fact that the HDL codes are synthesizable.

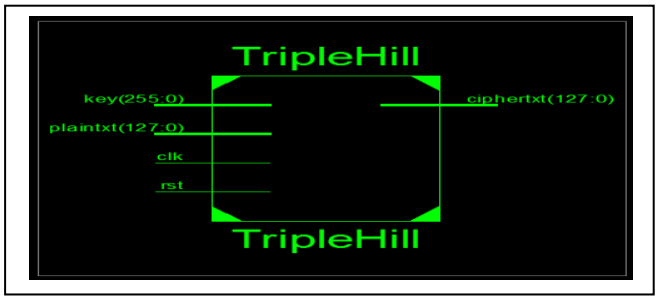


Fig. 12. Top Level RTL schematic of the proposed algorithm

Fig. 12 represents the complete hardware implementation of the proposed algorithm, as shown the data (plaintxt) is 128 bit which is ciphered using a 256 bit key. The rst bit is used to reset the module and clk bit is used to clock the design. The output is the 128 bit cipher text.

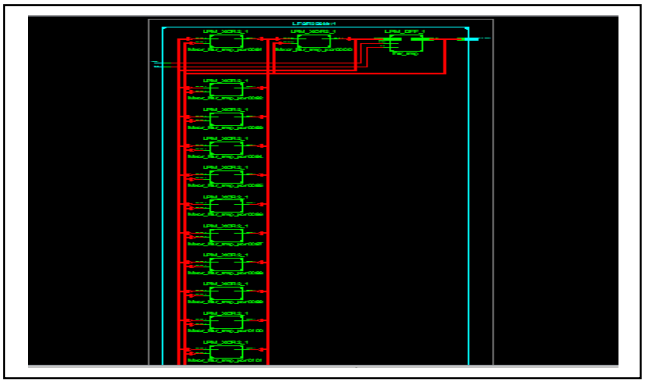


Fig. 13 Top Level RTL schematic of the 256 bit LFSR

Fig. 13 shows the components (actually it is a part of the components because we can't attach all components in the figure) of the 256 bit LFSR which acts as random number generator to give us the random 256 bit keys.

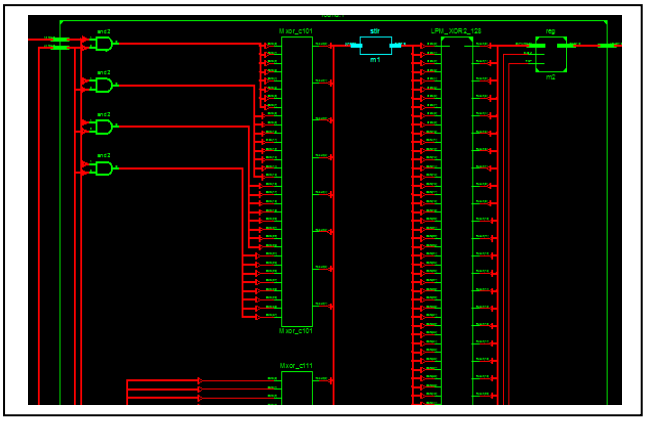


Fig. 14 Top Level RTL schematic of one Round

Fig. 14 shows the components of one round which consists of three operations; matrix multiplication which is the first part in the figure from the left, stir operation the second part and the xor operation the third part (also it is a part of the components because we can't attach all components in the figure).

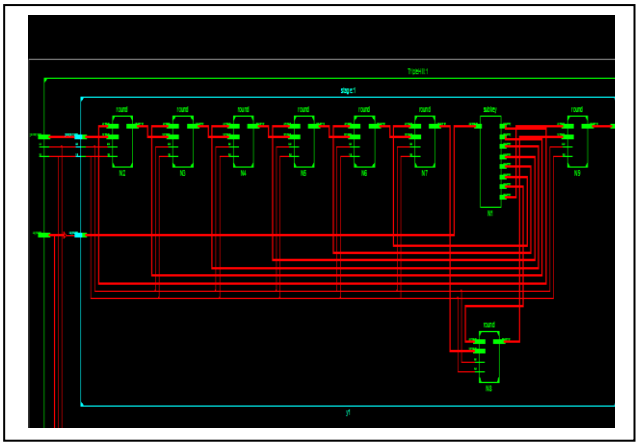


Fig. 15 Top Level RTL schematic of one Stage

Fig. 15 shows the components of one stage which consists of eight rounds and sub keys generation module which is the second part in the figure from the right.

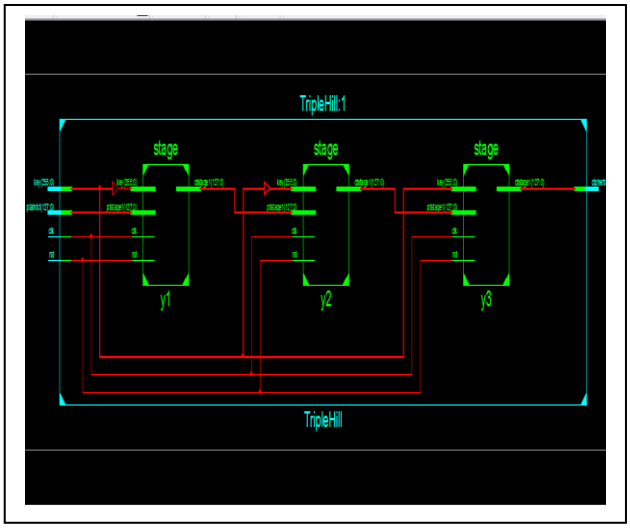


Fig. 16 Top Level RTL schematic of The overall triple Hill cipher

Fig. 16 shows the complete hardware of the proposed algorithm.

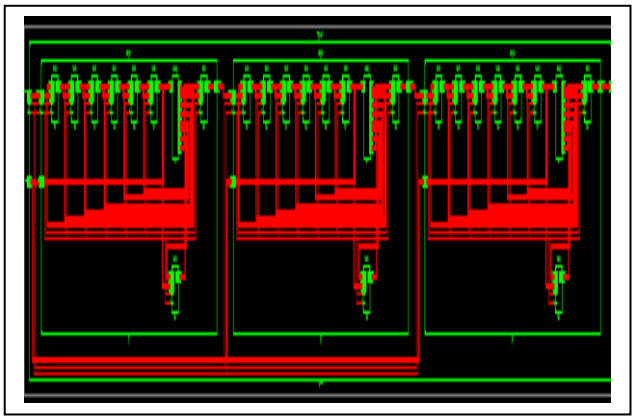


Fig. 17 Top Level RTL schematic of The overall triple Hill cipher cont.

Fig. 17 also shows the complete hardware of the proposed algorithm but with more details.

Design summary for the proposed algorithm is specified in Table I to set up details .

TABLE I
Design summary of the proposed algorithm

Logic Utilization	*Used*	*Available*	*Utilization*
Number of Slice Flip Flop	*3,072*	*49,152*	*6%*
Number of 4input LUTs	*9,222*	*49,152*	*18%*
Number of occupied slices	*4,636*	*24,576*	*18%*
Number of bonded IOBs	*514*	*640*	*80%*
Number of BUFG/BUFGCTRLs	*1*	*32*	*3%*
Average Fanout of Non-clock Nets	*3,77*		

Design summary in Table Igives the number of slice flip flops, number of 4 input LUT (Look Up Tables), number of BUFG/BUFGCTRLS, number of bonded IOBs and average fanout of non-clock network that used from the FPGA kit to implement the hardware of our design.

Power analysis of the proposed algorithm design

The total power dissipation is the sum of two types of power ;

- Quiescent (static) power is defined as the product of the power supply voltage and static current, which itself has two dual components: leakage currentand through current. Leakage currents are parasitic effects and are small in magnitude Through currents occur in normal operation and are due to transistors being continuously operated in their saturation region.
- Dynamic power which is frequency dependent and it has two components: the “capacitive” load power and the cell power. The latter is consumed internally bythe cell primitives. This component accounts for the power that is required to mainly charge and discharge the internal cell capacitance. “Capacitive” load power represents the currents required to charge the external loads driven by each cell. The overall dynamic power for an entire chip is given by [17]

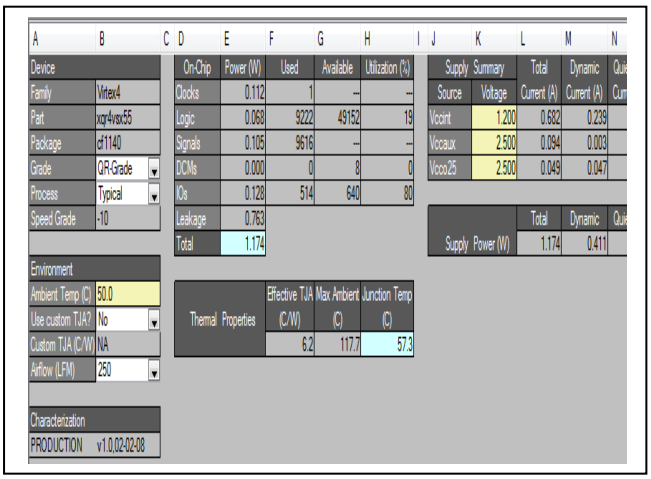


Fig. 18 Power analysis summary of the design with Clock frequency 25 MHZ

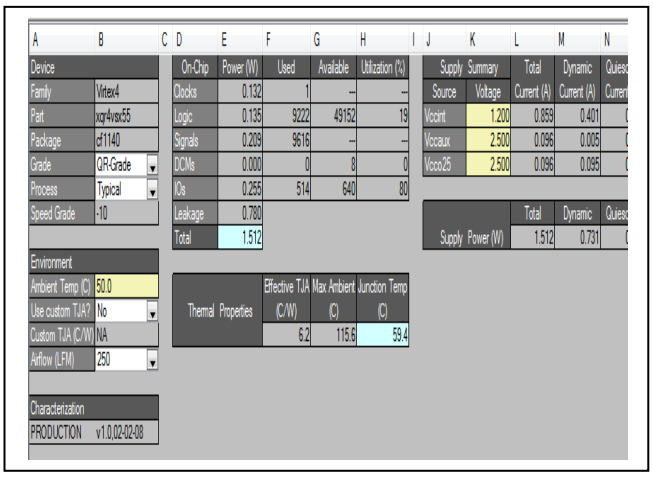


Fig.19 Power analysis summary of the design with Clock frequency 50 MHZ

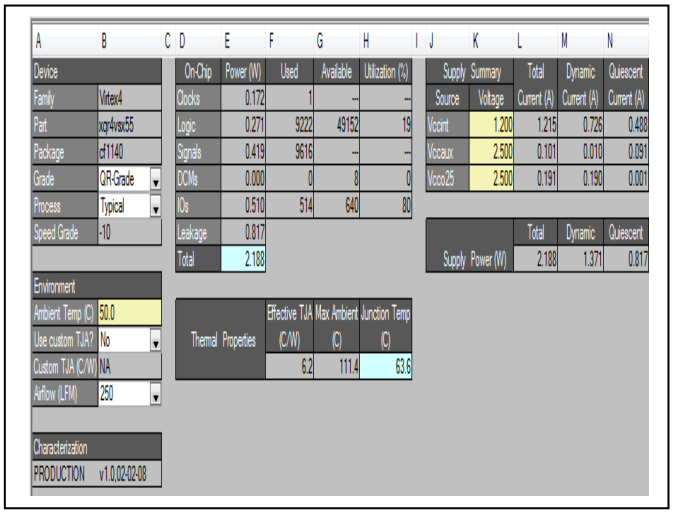


Fig. 20 Power analysis summary of the design with Clock frequency 100MHZ

Figs 18, 19 and 20 specifies the power analysis summary of the design at frequencies 25, 50 and 100 MHZ. As shown in figure the quiescent power is approximately constant at different frequencies, but the dynamic power changes with the frequency it increases as the frequency increases.

It is clear from these figures that the dynamic power increases as the frequency increases, so we need to know the maximum allowed frequency of this design. Here is the timing summary of that design, that from it we can know the maximum frequency:

- Minimum input arrival time before clock: 4.263ns
- Maximum output required time after clock: 4.677ns
- Minimum period: 1.894ns (Maximum Frequency: 528.067MHz)

Power analysis summary of the design at the maximum allowed clock frequency will be shown in Fig. 21

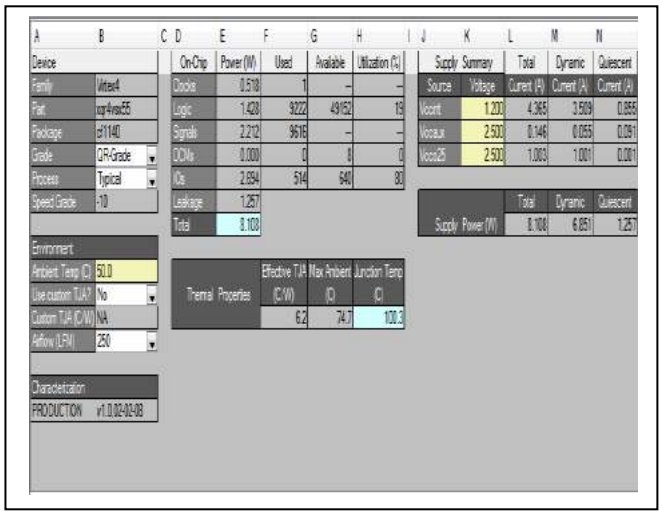


Fig. 21 Power analysis summary of the design with Clock frequency 528.067 MHZ

V. CONCLUSION

In the cryptanalysis of the classical hill cipher ,the known plaintext attack is performed using the method $k = p^{-1} c$ where p is an invertible matrix , so if an attacker has m distinct plaintext and cipher text ,can retrieve the key using the previous method .In the proposed triple Hill Cipher algorithm the known plain text attack becomes more difficult as the plain text is encrypted in eight rounds with eight different keys three times ,we can say that , we used 24 different keys which makes the task of the known plain text attack more difficult, there is no doubt that increasing the number of stages for example four stages instead of three increases the level of security but the overall performance of the algorithm become more slower. Also using LFSR as a random number generator to get random keys enhances the security of the proposed algorithm as the keys change more times.

REFERENCES

[1]A.F.A. Abidin, O.Y. Chuan and M.R.K. Ariffin''A Novel Enhancement Technique of the Hill Cipher for Effective Cryptographic Purposes" *Journal of Computer Science* 7 (5): 785-789, 2011.

[2] William Stallings ,''*Cryptography and Network Security Principles and Practices*", Fourth Edition, Prentice Hall, November 16, 2005.

[3] Jasdeep Singh Bhalla,'' A Database Encryption Technique to Enhance Security Using Hill Cipher Algorithm", *International Journal of Engineering and Advanced Technology* (IJEAT), Vol. 2, No. 4, April 2013.

[4] M. Nordin A. Rahman, A. F. A. Abidin, MohdKamirYusof, N. S. M. Usop,'' Cryptography: A New Approach of Classical Hill Cipher", *International Journal of Security and Its Applications*,Vol. 7, No. 2, March, 2013.

[5]D.R. Stinson, "*Cryptography Theory and Practice*",Third Edition, Chapman and Hall/CRC, Pp.13-37, 2006.

[6] V. U. K. Sastry, D. S. R. Murthy, S. DurgaBhavani, "A Block Cipher Involving a Key Applied on Both the Sides of the Plain Text," *International Journal of Computer and Network Security* (IJCNS), Vol. 1, No. 1, Pp. 27 -30, Oct. 2009.

[7] V. U. K. Sastry, V. Janaki, "A Modified Hill Cipher with Multiple Keys", *International Journal of Computational Science*, Vol. 2, No. 6, 815-826, Dec. 2008.

[8] Bhibhudendra Acharya, GirijaSankarRath, and Sarat Kumar Patra, "Novel Modified Hill Cipher Algorithm,",*Proceedings of ICTAETS*, Pp. 126-130, 2008.

[9]GandharbaSwain,andSaroj Kumar Lenka,''A Technique for Secret Communication Using a New Block Cipher with Dynamic Steganography'', *International Journal of Security and Its Applications*,Vol. 6, No. 2, April, 2012.

[10] Ahmed Desoky, AnjuPanickerMadhusoodhanan,''*Bitwise Hill Crypto System*'',
DOI: 10.1109/ISSPIT.2011.6151539
[11] Ali Muhammad Ali Rushdi and Fares Ahmad Muhammad Ghaleb,''On Self-Inverse Binary Matrices Over the Binary Galois Field'',*Journal of Mathematics and Statistics* 9 (3): 238-248, 2013.
[12] D. Coppersmith, D. B. Johnson and S. M. Matyas, ''A proposed mode for triple-DES encryption",*IBM J. RES, DEVELOP*. VOL. 40 NO, 2 MARCH 1996.
[13] Ralph C. MerkleElxsi, ''On the Security of Multiple Encryption",*Technical Note Programming Techniques and Data Structures D. Mcllroy Editor, Int. Martin E. Hellman Stanford University, Pp. 465-467,* Volume 24 the ACM Number 7, July,*1981*.
[14]C¸ .K. Koc¸ (ed.) " *Cryptographic Engineering",* DOI 10.1007/978-0-387-71817-0 3, c Springer Science+Business Media, LLC 2009
[15] Jay Kumar, Sudhanshu Shukla, Dhiraj Prakash, Pratyush Mishra and Sudhir Kumar,'' Random Number Generator Using Various Techniques through VHDL'',*International Journal of Computer Applications in Engineering Sciences* ,VOL I, ISSUE II, JUNE 2011 , ISSN: 2231-4946.
[16] Douglas, J.S., 1997, "*HDL Chip Design*" 3rd, Doone Publications, Madison, AL, USA, ISBN 0-9651934-3-8, , pp. 179-187.
[17] HichemBelhadj, BehroozZahiri, Albert Tai and Actel Corporation,''Power-sensitive designtechniques on FPGA devices'', *International IC – Taipei Conference Proceedings*.http://www.eetasia.com.sci-hub.org/ARTICLES/2001JUL/2001JUL03_PL_POW_TAC.PDF.

Ashraf A. M. Khalaf (M'98) received his B.Sc. and M.sc. degrees in electrical engineering from Minia university, Egypt, in 1989 and 1994 respectively. He received his Ph.D in electrical engineering from Graduate School of Natural Science and Technology, Kanazawa university, Japan, in Marsh, 2000. He is currently works as an associate professor at electronics and communications engineering Department, Minia University, Egypt.. His research interest includes digital signal processing and its applications in communications, neural networks, and optical communications.

Mona S. Abd El-karimwas Born : 1-8-1989, she worka as a teaching assistant and is currently a master course student for M.Sc. degree in Electrical Engineering (Communication and Electronics), Faculty of Engineering, Minia University, El-Minia, Egypt.

Hesham F.A. Hamed received the B.Sc. degree in Electrical Engineering, the M.Sc. and Ph.D. degrees in Electronics and Communications Engineering from EL-Minia University, ELMinia, Egypt, in 1989, 1993, and 1997 respectively. He currently is Professor and a Dean of the faculty of Engineering EL-Minia University. From 1989 to 1993 he worked as a Teacher Assistant in the Electrical Engineering Department, ELMinia University. From 1993 to 1995, he was a visiting scholar at Cairo University, Cairo, Egypt. From 1995to 1997, he was a visiting scholar at Texas A&M University, College Station, Texas (with the group of VLSI). From 1997 to 2003, he was anAssistant Professor in the Electrical Engineering Department, EL-Minia University. From 2003 to 2005, he was Associate Professor in the sameUniversity. From 2005 to 2007, he was a Visiting Researcher at Ohio University, Athens, Ohio. He has published more than 65 papers and onebook chapter. His research interests include analog and mixed-mode circuit design, low voltage low power analog circuits, current mode circuits,nano- scale analog and digital integrated circuits design, and FPGA.

Fast Intra-Beam Switching Scheme using Common Contention Channels in Millimeter-wave based Cellular Systems

Nak Woon Sung*, Yong Seouk Choi*

**Communications Internet Research Laboratory, ETRI,*
218 Gajeong-ro, Yuseong-gu, Daejeon, 305-700, Korea

nwsung@etri.re.kr, choiys@etri.re.kr

***Abstract*—Millimeter wave (mmWave) cellular system has recently been introduced as an attractive approach for 5G mobile broadband communications. In the mmWave beamforming cellular systems, the user equipment (UE) can experience frequent service disruptions due to frequent switching among a plurality of beams if the UE follows the network controlled LTE handover procedures. In this paper, we shows how the mmWave beamforming cellular system can operate and which kind of new handovers UEs can experience. And we propose UE controlled beam switching mechanism based on contention based uplink channels. In this mechanism, UEs switch the serving beam to the target beam without random access delay using the pre-acquired contention based channels.**

***Keyword*—Beam switching, millimeter wave communication, millimeter wave cellular systems**

I. INTRODUCTION

Recently, as the growing number of smart phones and tablet PCs drives the increase of applications requiring much more traffic, the mobile data usage and traffic is more accelerated. According to [1], the high-definition video, sophisticated augmented reality and new types of games will be becoming major applications in the next decade which require 1000x bandwidth. However it is very difficult to satisfy the demand for bandwidth hunger applications with spectral efficiency enhancement because it has reached near practical Shannon limits. In addition, acquiring more spectrum below 6GHz cannot provide the capacities required because there isn't enough spectrum there. To meet 1000x requirements, approaches different from the existing methods have to be considered [2].

An attractive approach is to use millimeter wave (mmWave) spectrum for 5G mobile communication systems [3]. mmWave has experienced higher propagation losses such as path losses or return losses than bands below 6GHz. This characteristic reduces both of cell coverage and interference. However minimized interference enables dense deployments of small cells. Therefore, the total capacity can be scaled with the number of base stations (BSs).

Path losses at mmWave bands, meanwhile, can be overcome in use of massive MIMO (Multiple-input and multiple-output) technology in which antenna arrays consist of many active antenna elements. Nevertheless, the propagation losses have a negative effect on service coverage of the mmWave wireless communication systems. In this case, beamforming technology can be utilized to increase service coverage, expand cell capacity and minimize interference [4], [5]. Beamforming is an advanced technology in which a transmitting side transmits a plurality of beams in different directions and a receiving side receives a plurality of beams in different directions.

In the mmWave cellular systems using beamforming technology, a BS can forms a plurality of beams towards the desired users (UE). In this beamforming architecture, a new type of handover - beam switching within the same BS or among different BSs - can occur.

While multiple narrow beams increase network capacity, they also cause frequent beam switching even if the UE moves around within the same BS. If the UE follows the conventional network controlled/UE assisted handover procedures in Long Term Evolution (LTE) defined by the Third Generation Partnership Program (3GPP) [6], the UE experiences frequent service disruptions. In this paper, we propose simple UE controlled beam switching mechanism using contention based uplink channels.

The rest of this paper is organized as follows. Section II describes the architecture of the proposed mmWave beamforming cellular systems. Section III discusses the contention based intra beam switching mechanisms. Finally, we conclude our work in Section IV.

Manuscript received July 6, 2015. This research was funded by 'The Cross-Ministry Giga KOREA Project ' [GK15N0100, 5G mobile communication system development based on mmWave] of the Ministry of Science, ICT and Future Planning, Korea.

Nak Woon Sung is with the Electronics and Telecommunications Research Institute, 218 Gajeong-ro, Yuseong-gu, Daejeon, 305-700, Korea (corresponding author phone: +82-42-860-4890; fax: +82-42-861-1966; e-mail: nwsung@ etri.re.kr).

Yong Seouk Choi is with the Electronics and Telecommunications Research Institute, Daejeon, 305-700, Korea (e-mail: choiys@ etri.re.kr).

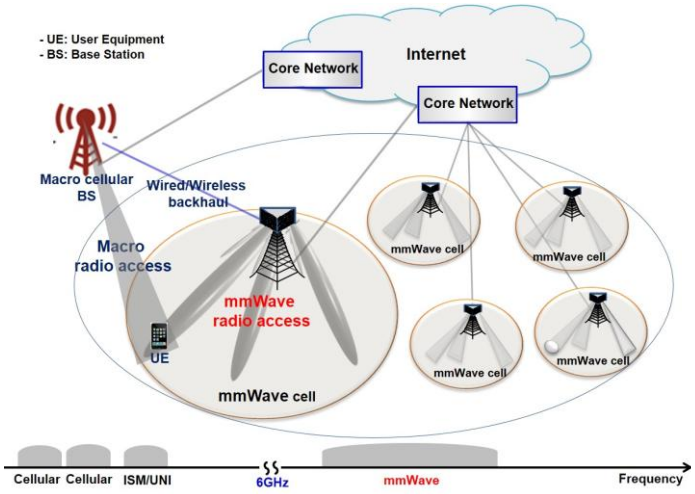


Fig. 1. mmWave based beamforming cellular systems.

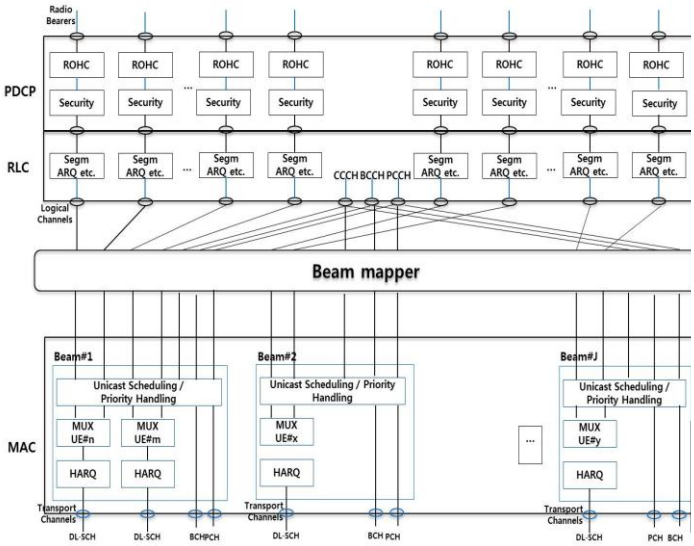


Fig. 2. The protocol architecture of mmWave based beamforming BS system.

II. MMWAVE BEAMFORMIG CELLULAR SYSTEMS

A. *mmWave beamforming cellular system architecture*

To meet the 1000-fold bandwidth requirements, the mmWave cellular system is one of the promising solutions [2]. First, the wide bandwidths for carrying bandwidth hunger applications are available at mmWave spectrum above 6GHz. Second, a number of picocell BSs with a plurality of directional beams can be densely deployed in the small areas due to the minimized mutual interference at the high frequency spectrum. Therefore, total capacity increases proportionally with the number of the BSs. Consequently, more available bandwidth at mmWave and capacity scalability deliver per-user data rate for supporting high speed data and high definition video transmission. The Giga Korea Project is a representative example to develop the mmWave based mobile communications systems to deliver Gbps broadband connection by 2020.

Fig. 1 depicts our proposed mmWave beamforming cellular systems which provide a kind of outdoor picocells and can be installed on existing street poles like lamp posts. In this architecture mmWave cells are overlayed in macro cellular networks or run as a stand-alone. We consider both of dual connectivity and stand-alone operation possible for future 5G networks. Thus, the UE supports different operation modes like 4G and 5G radio access and different coverage layers such as macro cells or mmWave picocells. In addition, a single common 5G core network is designed to support 4G and WiFi access in use of the network virtualization based on the distributed architecture approaches. These proposed unified systems enables a various types of connectivity, services, and use cases integrated.

In addition to achieving high per-user data rates, low latency is another key target for the proposed systems since latency minimization provides new business opportunities to the industry and performance improvement which the advanced networks require for fast coordination and transmission among different network entities [7]. Latency is determined by one round trip transmission to deliver the control signaling or data transmission. And low latency is achieved by the shorter transmission time interval (TTI) length. With the short TTI length data blocks has to be transmitted for a short time but in wide frequency range.

The TTI length of 200us is set for the proposed system. In case of LTE the total user plane (U-plane) delay is 4.8ms under the assumption of 10% Hybrid Automatic Repeat-reQuest (HARQ) Block Error Rate (BLER) [8]. Using the same LTE latency calculation model, the U-plane one-way access latency for the proposed system is given as 2.46ms. This one-way access latency is calculated as $T_{USER-PLANE} = 2.1 + P * 3.6$ where p is the error probability of the first HARQ retransmission and UE Processing Time of 1ms and eNB Processing Time of 1.1ms are considered. The minimum U-plane latency is expected to be 2.1ms when p equals zero. However, the U-plane latency of 2.46ms is more realistic when considering radio frame alignment.

B. *Beamforming base station architecture*

An mmWave BS is designed to consist of three sectors which form forty eight narrow beams. Each beam uses the same 1 GHz bandwidth in 28GHz band and support theoretical speeds up to about 3.3Gbps. In our systems, the uplink transmission timing of all the beams within a BS is also assumed to be synchronized as the cell coverage is relatively small due to properties of the ultra-high frequency. And each beam works like a kind of the small cell BS which has its own physical channels, transport channels, and logical channels.

While each beam within the same BS shares the same cell identity (Cell ID) which is unique within the network, it has the different beam identity (Beam ID) which is unique within only the BS. There is only the single radio resource control (RRC) [9] entity in a BS and therefore the same RRC signaling messages can be delivered to UEs through broadcast channels or shared channels per beam within the same BS. For example, although UEs associates with different beams, each UE receives the same Master Information Block (MIB) broadcast on Physical Broadcast CHannel (PBCH) per beam and the same System Information Blocks (SIBs) sent on the Physical Downlink Shared Channel (PDSCH) through the same RRC messages.

We show the proposed beamforming mmWave cellular system architecture in Fig. 2. The logical channels from radio link control (RLC) entity are mapped to the most proper beam including beam-specific medium access control (MAC) entities through the beam mapper which is newly introduced in the proposed mmWave beamformig cellular systems. Beam mapping has considerable effect on network throughput and depends on beam switching policy; network controlled UE assisted beam switching or UE-controlled beam switching.

- In case of network controlled UE assisted beam switching, beam switching is decided and initiated by the BS based on the measurement feedback information which the network asks the UE to measure the signal of the surrounding beams and report.
- In case of UE-controlled beam switching, the UE estimates the signal quality from each beam from the serving BS and the neighboring BSs and performs an appropriate beam switching procedures for selecting its target beam.

In our paper, we are just concerned about the UE-controlled beam switching which promises greatly increased scalability for the mmWave cellular systems.

Within each single beam, the unicast scheduler in MAC entity is responsible for scheduling the beam's radio resources utilized in the uplink and downlink whilst satisfying the required quality of service (QoS) for all active radio bearers within the beam.

III. Contention Based Beam Switching Mechanism

A. *Introduction of beam switching*

In our proposed mmWave beamforming cellular systems, the initial camp on procedure is similar with the existing LTE camp on procedure except that the UE searches for both of suitable beams and cells and camps on the selected beam instead of the cell. The reason is that each beam acts like the single small cell BS in which its own physical channels are defined as shown in Fig. 2. The UE then performs the attach procedure in order to register in the tracking area of the selected cell. However, the location registration process takes place on cell level, not on beam level. The UE now continuously monitors and searches for the best beam/cell on which to camp.

In LTE, there are three kinds of handovers relying on whether the evolved packet core (EPC) entities that a UE is connected to are switched after the handover or not: intra-LTE, inter-LTE, and inter-RAT.

- Intra-LTE: An intra-LTE handover will occur within current LTE nodes either via the X2 or via the S1 (intra-MME and intra-SGW)
- Inter-LTE: Inter-LTE handover will take place toward the other LTE nodes that belong to the different pooling area (inter-MME and inter-SGW)
- Inter-RAT: Handover between different radio technology networks, for example E-UTRAN and GERAN/UIRAN

As mentioned in Section II, new types of handovers are required in mmWave beamforming cellular systems because a UE has the connection with a BS through the channels in the beams, not the channels in the cell. In other words, each cell consists of the multiple beams and there are separate physical channels per beam which transport control messages and user beam (serving beam) to the other beam (target beam) within the same serving BS or the BS different from the serving BS shown in Fig. 3. Two types of beam switching can occur:

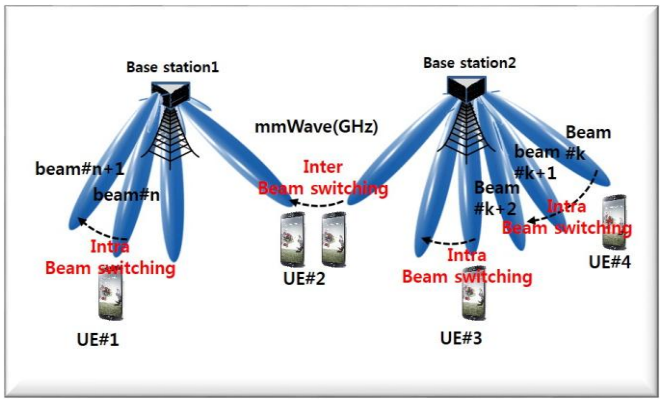


Fig. 3. The types of beam switching in beamforming cellular systems

- Intra beam switching: When a beam switching happens, the target beam is selected among the beams transmitted by the same BS which the serving beam belongs to.
- Inter beam switching: When a beam switching happens, the target beam is selected among the beams transmitted by the target BS different from the serving BS which the serving beam belongs to.

For instance, in Fig. 3, UE#1 and UE#3/UE#4 change the serving beams within Base station 1 and Base station 2, respectively. This is the example of intra beam switching. In contrast, UE#2 moves toward the target beam which belongs to the neighboring BS. In this case, inter beam switching is required. The inter beam switching is very similar with a kind of general LTE handover procedure above mentioned. In this paper, we are concerned about intra beam switching instances.

B. *Problems in intra-beam switching*

Our proposed mmWave beamforming cellular approach provides network throughput advantages up to over 100Gbps and the solution to the wireless spectrum shortage. However, this approach also has a few technical limitations to be overcome. Newly introduced interference is proportional to the number of the overlapped beams which share and reuse the same frequency band within a serving BS and neighboring BSs. Another problem is more frequent switching between beams because the cell coverage of mmWave beamforming cellular systems is relatively small due to the properties of high frequency band and beam area per beam is a little narrow in comparison with the LTE cell. When a UE moves around, the UE may experience more frequent switching between neighboring beams although the UE stays in the same BS.

In LTE handover, MME always instructs the UE to change the cell, i.e. network controlled handover. Therefore, the

existing LTE handover procedure aims to get minimum latency in case of cell changes [10]. While this type of handover has the advantage of better traffic load balancing [11], it is not suitable for a rapidly changing environment and high user density areas due to the associated signaling delay [12]. In the proposed mmWave beamforming cellular systems, users experience rapidly changing beam environment because of multiple narrow beams and the limited propagation distances of mmWave beams. This environment at mmWave frequencies makes UE controlled handover schemes more attractive. This type of handover has the advantage of a short reaction time and is suitable for small cell systems [13].

Another beam switching problem is related to the handover procedures. In LTE handover a UE sends a measurement report according to the measurement configuration specified by RRC protocol entity in the serving BS. And the serving BS decides handover initiation depending on this measurement report. In accordance with handover decision algorithm, handover preparation and handover execution phases are performed. After the UE sends a handover completion message to the BS, the handover procedure is migrated into handover completion phase. In response to this completion message, the target BS notifies the serving BS to release all the resources utilized by the UE and the target MME to switch the path of the packet to the target BS. This mobility management is conducted in RRC entity in Layer 3.

Intra beam switching procedure has characteristics different from above the LTE handover procedure because any switching of the current LTE nodes is not required, i.e. the UE keeps the connection with the same serving BS. Therefore, handover preparation phase is not required and handover completion phase can be simplified to notify the serving BS the completion of intra beam switching. Only the beam switching decision and execution processes need to be carried out in handover decision and execution phase as in LTE handover procedure. In particular, the handover execution phase needs to be swiftly completed within the domain of single BS. Thus, efficient fast intra beam switching schemes are required.

C. Contention based beam switching scheme

During the handover execution phase, the UE is asked to connect to the selected target networks. In this phase, the LTE UE generally performs random access procedures for uplink transmission timing synchronization and UL allocation for the handover completion message [14]. This means that the increasing distance between the UE and the BS requires consideration of propagation delay. However, the problem is that it takes about 10 Transmission Time Interval (TTI) to complete these procedures as shown in [15], [16]. In the result, these procedures cause considerable service disruptions in the rapidly changing beam environments.

In the proposed mmWave beamforming cellular systems, the beam coverage is relatively small, i.e. under about 500 m and each BS can synchronize the UE uplink transmission timing between its own beams. Thus, intra beam switching can be done without UL timing alignment procedures. To enable the efficient and low latency beam switching, the UE

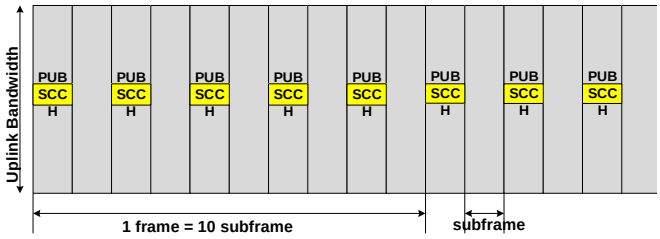


Fig. 4. Common contention based channels among all uplink beams, i.e. named Physical Uplink Beam Switching Control Channels (PUBSCCH).

sends Beam Switching Request MAC message in use of contention based access schemes.

In [17], the authors show that in LTE networks, unlimited use of contention based access is clearly useless since the collision probability over contention based channels increases rapidly. But limiting contention based transmissions on certain frames, for example voice frames, improve the satisfaction rate and the network throughput. In addition, in [18] authors proposed contention based uplink transmission in order to allow uplink synchronized UE to transmit uplink data without sending Scheduling Request message in advance. Thus, considering the relatively rich wireless resources at the high frequency bands and the smaller number of users per beam in mmWave cellular systems, contention based access schemes can be utilized for intra beam switching. As shown in Fig. 6, the limited number of uplink Resource Blocks (RBs) are dynamically scheduled on a per some subframe basis for beam switching. And the use of these RBs is constrained only for sending the uplink beam switching control element which is under a few bytes.

In our contention based beam switching scheme, some specific radio regions are defined as common contention based channels among all uplink beams, i.e. named Physical Uplink Beam Switching Control Channels (PUBSCCH), as shown in Fig. 4. This means that intra beam switching, i.e. contention based transmissions, does not interfere with other uplink transmissions for user data, i.e. contention free (CF) transmission. And the configuration for these common channels are broadcast by using system information block 2 (SIB 2) which is shared among the beams within single BS. In addition, a group of contention based radio network temporary identifiers (CB-RNTIs) is also defined in order to identify the UE within the single BS domain and a CB-RNTI is added into Beam Switching Request MAC PDU transmitted over contention based channels. Therefore, a UE can send the Beam Switching Request MAC CE through the serving beam without acquisition of PDCCH as in [17] since the UE can already know the CB grants by using the SIB 2 pre-acquired over the previous or current serving beam.

D. Fast intra-beam switching scheme

In this paper, we propose UE controlled contention based beam switching schemes done in MAC entity in Layer 2 as shown in Fig. 5. In our scheme, a UE measures RSRP (Reference Signal Received Power) parameter on beam-specific reference signal for each beam after the measurement configuration is provided to the UE in RRC-CONNECTED mode by the BS.

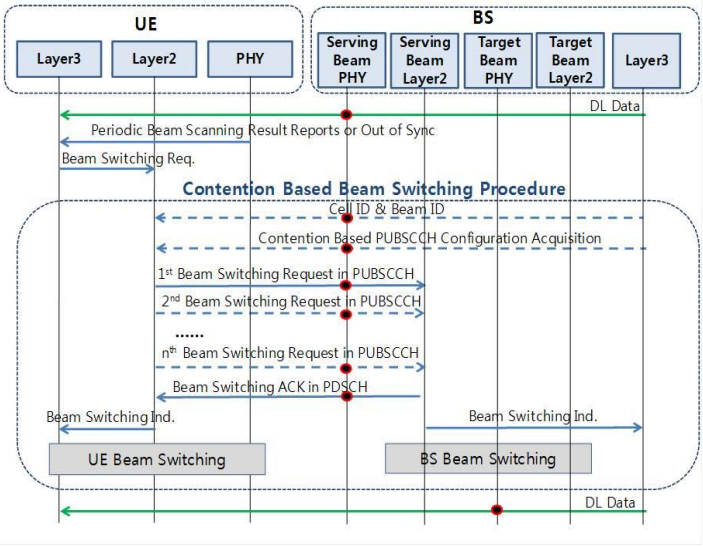


Fig. 5. The fast intra-beam switching: Communication success procedures.

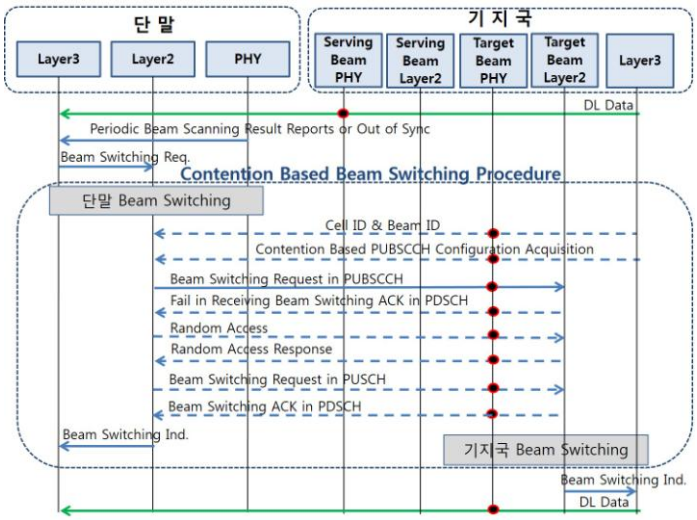


Fig. 6. The fast intra-beam switching: Communication failure procedures.

And the measurement results are managed by the RRC entity in the UE instead of the serving BS. Considering the rank of RSRP from the entire candidate beams along with serving beam, beam switching decision is made by the UE if the RSRP of any candidate beams within the serving cell meets the pre-defined threshold.

In the following handover execution phase, connection needs to be re-routed from the serving beam to the selected target beam by sending Beam Switching Request message to the serving BS. Using the contention based uplink channels as described in Section II-C, the UE transmits this control message through PUBSCCH without monitoring PDCCH. This is possible since the UE already acquires UL grants through the PUBSCCH configuration in the SIB. Then the UE starts the Beam Switching timer. This timer is stopped only when the Beam Switching ACK MAC CE is received through PDSCH. Whenever this timer reaches its time-out values, the UE retransmits the Beam Switching Request message. Due to a collision in PUBSCCH, the UE may fail in successfully receiving the Beam Switching ACK MAC CE within the specified time interval. The collided UE starts above the process again based on the uniform backoff algorithm in LTE [19]. However, the backoff indicator parameters which define the upper limit for a random backoff period is controlled by the UE, not by the BS.

After receiving Beam Switching Request MAC CE, the MAC entity on the BS site corresponding to the serving beam notifies the beam mapper and the RRC entity about the beam switching request. The beam mapper commands the UE to switch the serving beam to the target beam by sending Beam Switching ACK MAC CE through PDSCH in the serving beam using the same CB-RNTI in Beam Switching Request MAC CE. After the MAC entity in the UE sends Beam Switching Indication message to the RRC entity for beam switching completion, the UE and the beam mapper changes the serving beam to the target beam in the following subframe. Then, the UE can receive the packets through the target beam using the same C-RNTI used in the serving beam.

If the UE fails in intra-beam switching despite of a number of random backoffs, the UE transmits the scheduling request (SR) message through random access as shown in Fig. 6. The random access is necessary for applying for uplink resource grants for sending the Beam Switching Request message. It will take 2.8ms to complete this procedures in the best. Although this channel access latency is faster than that of LTE random access which provides about 14ms, it has significant impact on capacity decrease in rapidly changing beam environments.

IV. Conclusions

In the mmWave beamforming cellular systems, a plurality of beams causes frequent beam switching even if the UE moves around within the same base station. If the UE follows the network controlled LTE handover procedures, the UE experiences frequent service disruptions. In this paper, we shows how the mmWave beamforming cellular system can operate and which kind of new handovers UEs can experience. And we propose UE controlled beam switching mechanism based on contention based uplink channels. In this mechanism, UEs switch the serving beam to the target beam without random access delay using the pre-acquired contention based channels.

Acknowledgment

This research was funded by 'The Cross-Ministry Giga KOREA Project' [GK15N0100, 5G mobile communication system development based on mmWave] of the Ministry of Science, ICT and Future Planning, Korea.

References

[1] Nokia Solutions and Networks White Paper – 'Enhance mobile networks to deliver 1000 times more capacity by 2020' http://networks.nokia.com/sites/default/files/document/technology_vision_2020_1000x_capacity_white_paper_0.pdf.

[2] Y. Zhu, Z. Zhang, Z. Marzi, C. Nelson et al., "Demystifying 60GHz Outdoor Picocells," in Proc. ACM MobiCom, 2014.

[3] T. Rappaport et al., "Millimeter Wave Mobile Communications for 5G Cellular: It Will Work!," IEEE Access, vol. 1, 2013, pp. 335–49.

[4] W. Roh, J.-Y. Seol, J. Park, B. Lee, J. Lee, Y. Kim, J. Cho, K. Cheun, and F. Aryanfar, "Millimeter-wave beamforming as an enabling technology for 5G cellular communications: theoretical feasibility and prototype results," Communications Magazine, IEEE, vol. 52, no. 2, pp. 106- 113, 2014.

[5] Meejoung Kim, Yongsun Kim, and Wooyong Lee, "Resource Allocation Scheme for Millimeter Wave-Based WPANs Using Directional Antennas," ETRI Journal vol. 36, no. 3, pp. 385-395, June 2014.

[6] 3GPP TS36.300, "E-UTRA and E-UTRAN; Overall description; Stage 2 (Release 11)," v.11.1.4, Dec. 2012.

[7] Nokia Solutions and Networks White Paper – 'Technology Vision 2020: Reducing network latency to milliseconds' http://networks.nokia.com/sites/default/files/document/technology_vision_2020_reduce_latency_white_paper_1.pdf.

[8] 3GPP TR 36.912, "Feasibility Study for Further Advancements of E-UTRA (LTEAdvanced)"

[9] 3GPP TS36.331, "E-UTRA Radio Resource Control (RRC); Protocol specification (Release 11)", v11.2.0, Dec. 2012.

[10] Y. S. Hussein, B. M. Ali, M. F. A. Rasid and A. Sali, "Reduction of Outage Probability due to Handover by Mitigating Inter-cell Interference in Long-Term Evolution Networks," ETRI Journal, vol. 36, no. 4, p. 554, 2014

[11] SNK Marwat, S. Meyer, T. Weerawardane, and C. Goerg, "Congestion Aware Handover in LTE System for Load Balancing in Transport Network," ETRI Journal, July 2014 (Early Access). http://dx.doi.org/10.4218/etrij.14.0113.1034

[12] J. Li, X. Wu, and R. Laroia, *OFDMA Mobile Broadband Communications:A Systems Approach*. Cambridge U.K.: Cambridge Univ Press, 2013.

[13] N. D. Tripathi, J. H. Reed, and H. F. VanLandingham, "Handoff in Cellular Systems," IEEE Pers. Commun., Dec. 1998, pp. 26–37.

[14] M. Amirijoo, F. Gunnarsson, F. Andren, "3GPP LTE Random Access Channel," IEEE Transactions on Vehicular Technology, vol. 63, no. 6, pp. 2784–2793, 2014.

[15] D. Singhal, M. Kunapareddy, and V. Chetlapalli, "LTE-Advanced: Latency Analysis for IMT-A Evaluation," Tech Mahindra, Tech. Rep., 2010.

[16] Singhal, D., Kunapareddy, M., Chetlapalli, V., James, V.B., Akhtar, N., "LTE-Advanced: Handover interruption time analysis for IMT-A Evaluation," Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on, vol., no., pp.81-85, 21-22 July 2011

[17] L.K.S. Sunna, "Contention-based Uplink Transmission in Unscheduled Access", M.SC. Thesis, Dept. Computer Science and Elec. Eng., Lulea University of Technology, Jan. 2010.

[18] 3GPP "Contention based uplink transmissions", R2-093812, June, 2009

[19] J.-B. Seo and V. C. M. Leung, "Design and analysis of backoff algorithms for random access channels in UMTS-LTE and IEEE 802.16 systems," IEEE Transactions on Vehicular Technology, vol. 60, no. 8, pp. 3975–3989, 2011.

Nak Woon Sung received the Ph.D Degree in Computer Science from KAIST, Korea, in 2013. He received his B.S. and M.S. degree in Computer Engineering from Pusan National University, Korea in 1997 and 1999. During 1999-2000, he was a member of researchers at ADD (Agency for Defense Development). Since 2000, he has been currently the principal researcher at ETRI (Electronics and Telecommunications Research Institute) in Korea. His research interests include the medium access control (MAC) of wireless communication including the broadband wireless access (BWA) and millimeter wave communication systems.

Yong Seouk Choi received his Ph.D degree from in the Information and Communication System from Chungbuk National University, Korea in 2007. He received his bachelor's degree and M.S. degree in Electrical Engineering from Hongik University, Korea, in 1990 and 1992. During 1992-1998, he was a member of researchers at Hanhwa Information and Communication Research Lab. Since 1992, he has been the principal researcher at ETRI (Electronics and Telecommunications Research Institute) in Korea. His research interests are the wireless access technology and millimeter wave communications system.

Improving Beam Distribution Evenness in 3-Dimensional Beamforming with Carrier Aggregation

Jun-woo Kim, Gosan Noh, Jang-won Moon, Youn-ok Park, Ilgyu Kim

Communications & Internet Research Laboratory, *ETRI (Electronics and Telecommunications Research Institute), Daejeon 34129, Korea*

jwkim74@etri.re.kr, gsnoh@etri.re.kr, jwmoon@etri.re.kr, parkyo@etri.re.kr, igkim@etri.re.kr

***Abstract*— The 3-dimensional beamforming is a highly attractive issue in 5G telecommunication. Equipped with 2-dimensional antenna arrays, it allows vertical sectorization within a cell as well as horizontal one, by making a beamforming zone for the corresponding sector. However, there is considerable inequality among the areas of beamforming zone. Since the farther from the base station, the bigger the beamforming zone area is, the farther beamforming zone area is likely support more users than nearer beamforming zone.**

In this paper, we propose to utilize carrier aggregation (CA) from additional base stations for relieving the uneven beamforming zone area problem and prove this method is more efficient in improving cell throughput especially in mmWave environment. Even if the additional base station is more simple type which offers only a few beamformings, it can effectively improve the equality of UE's radio resource occupation.

***Keyword*—3-Dimensional Beamforming, Carrier Aggregation, 5G Telecommunication**

I. INTRODUCTION

THE 3-DIMENSIONAL beamforming allows both horizontal and vertical beam pattern adaption in order to enhance system performance over the conventional beamforming techniques [1][2]. Lots of recent researches in 5G communication also consider adopting 3-dimensional beamforming for mmWave systems [4][5].

Manuscript received October 9, 2015. This work is a follow up of the invited journal of the accepted conference paper for the 17th International Conference on Advanced Communication Technology. This research was supported by 'The Cross-Ministry Giga KOREA Project' of The Ministry of Science, ICT and Future Planning, Korea. [GK15N0100, 5G mobile communication system development based on mmWave]

Jun-woo Kim is with the Communications & Internet Research Laboratory, Electronics and Telecommunications Research Institute (ETRI), Daejeon 305-700, Korea (Corresponding Author phone: +82-42-860-6682; fax: +82-42-861-1966; e-mail: jwkim74@etri.re.kr).

Gosan Noh is with Electronics and Telecommunications Research Institute (ETRI), Korea (e-mail: gsnoh@etri.re.kr).

Jang-won Moon is with Electronics and Telecommunications Research Institute (ETRI), Korea (e-mail: jwmoon@etri.re.kr).

Youn-ok Park is with Electronics and Telecommunications Research Institute (ETRI), Korea (e-mail: parkyo@etri.re.kr).

Ilgyu Kim is with Electronics and Telecommunications Research Institute (ETRI), Korea (e-mail: igkim@etri.re.kr).

In 3-dimensioanl beamforming, each beam is formed and controlled by antenna arrays. Then each cell can be split into multitude of beamforming zone as shown in Fig. 1.

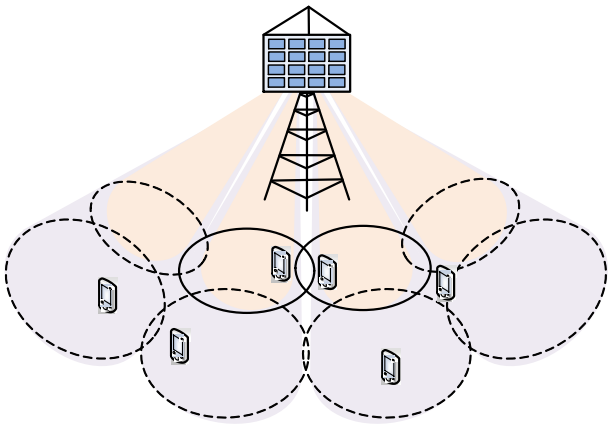


Fig. 1. Multiple beamforming zones using 3-dimensioanl beamforming.

One of the expected problems of 3-dimensional beamforming is its inequality of each beamforming zone area [3][4]. Since the farther from the base station, the bigger the beamforming zone area is, the farther beamforming zone area is likely support more users than nearer beamforming zone. Even though the considered cell sizes are small due to the propagation limitation of mmWave, most part of the cell area was covered by only a small portion of 3-dimensional beamformings [4]. Generating sharper beamforming for farther area may be a solution [10]. But even if downlink beamforming inequality problem is solved by this method, since UE cannot make as sharp uplink beamforming as that of downlink, the uplink beamforming still remains as a problem to solve [12].

This inequality of beamforming zone area causes inequality of users each beamforming supports, i.e. uneven average radio resource occupation of each user equipment (UE) since many UEs in wide area are likely supported from a small number of beamformings in far region from the BS.

Prior researches considered relay systems to be adopted in this situation. Relays are helpful in filling coverage holes but they also can interfere neighbor beamforming zone area [4]. In this paper, we will show this inequality of radio resource

occupation can be alleviated by installing other BSs for carrier aggregation (CA) [6] at adequate places.

The additional BS for CA can be the same type of the main BS or simpler type with a few steering beamforming. While the high-capacity BS for carrier aggregation can greatly improve the unequal radio resource occupation problem, the simpler BS with steering beamforming can moderately improve this problem with less expensive installations.

The CA technology is frequently adopted to multiply the cell capacity. But this paper shows it can be used to alleviate resource occupation inequality also.

II. The Inequality of 3-Dimensioanl Beamforming Zone

A. The downward tilt angle and the beamforming zone area

The area of beamforming zone can be varied due to the height, downward tilt angle, vertical and horizontal beamforming angles of base station (BS) antenna. This relation is shown in Fig.2 and equation (1). The beam radius R can be calculated from the BS antenna height H, downward tilt angle ω, and vertical beamforming angle θ. The horizontal beamforming angle is assumed to be the same with the vertical beamforming angle.

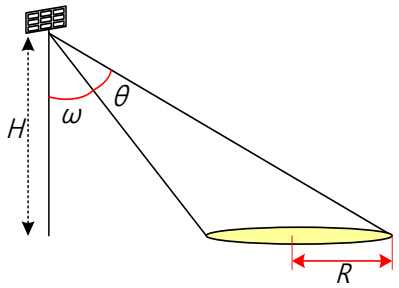


Fig. 2. The relation between 3-dimensioanl beamforming zone and downward tilt angle.

$$R = \frac{H \times [\tan(\theta + \varpi) - \tan(\varpi)]}{2} \qquad (1)$$

Since the area of beamforming zone is dictated by the beamforming radius R, it also increases rapidly depending on the downward tilt angle especially when the downward tilt angle is greater than π/4. Fig.3 shows the increase of beamforming zone diameter as per downward tilt angle. The BS antenna height H is assumed to be 50 m and beamforming angle θ is 30°.

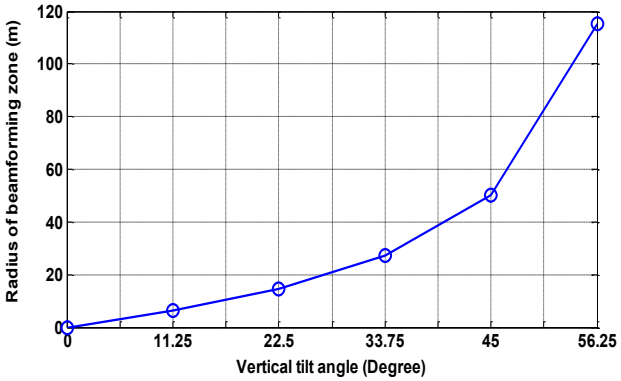


Fig. 3. The beamforming zone diameter as per downward tilt angle.

B. Our exemplary system

If the BS antenna configuration is as shown in Table I, the expected beamforming zone of that cell in flat terrain is as depicted in Fig. 4 and Table II. The vertical beamforming is composed of 3 layers whose vertical beamforming angles are all the same and downward tile angles are different from those of others.

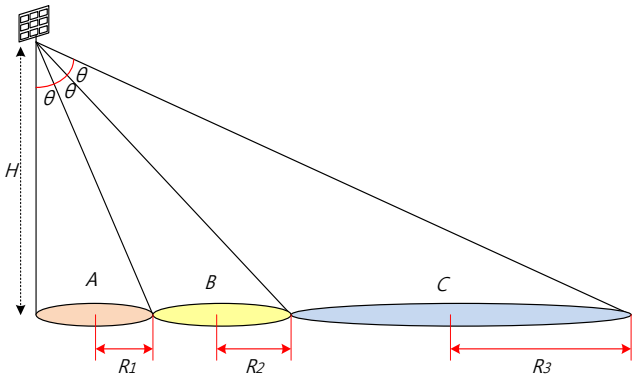
TABLE I
BS Configuration Parameters.

Symbol	Parameter	Value
H	BS antenna height	50m
θ	Vertical beamforming angle	π/8
ω	Downward tilt angle	0, π/8, 2π/8
φ	Horizontal beamforming angle	π/8
L	Number of vertical layers	3
R_1	Beam radius (1st vertical layer)	10.36 m
R_2	Beam radius (2nd vertical layer)	14.64 m
R_3	Beam radius (3rd vertical layer)	35.36 m

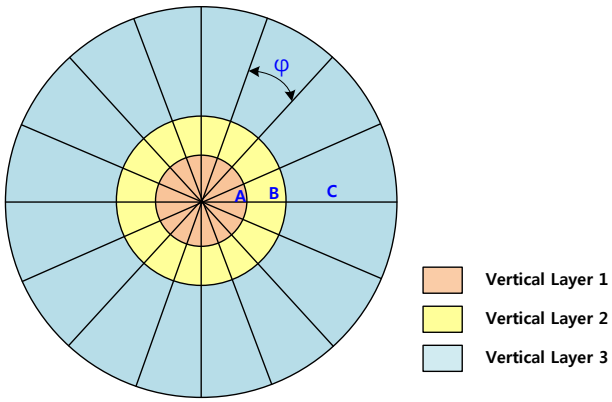
Fig. 4 clearly shows that the relation between the distances from BS and the area of beamforming zone. The calculated area of each beamforming zone A, B and C under the parameter of Table I also certifies it as is shown in Table II.

The (a) of Fig.4 shows the lateral view of 3-dimensional beamforming and the (b) is the ground plan of it.

In real cell deployment, each cell radius is much greater, every beamforming angle is varied or steerable, and each beamforming zone shapes oval and surrounded by interference zone [4]. However we apply simpler model of beamforming zone as shown in Fig. 4 for convenient verification of proposed method.



(a) Vertical view of beamforming layers



(b) Horizontal view of beamforming layers

Fig. 4. The deviation of beamforming zone area with the distance.

While the transmission data rate of each beamforming does not vary widely, its coverage is quite different according to the vertical layer it belongs to. Table II shows the beamforming zone of belonged to 3rd vertical layer is as wide as 28-fold of that belonged to 1st vertical layer.

TABLE II
BEAMFORMING ZONE AREAS OF DIFFERENT VERTICAL LAYERS.

Vertical Layer	1st Layer (A)	2nd Layer (B)	3rd Layer (C)
Single beamforming zone area (m^2)	1347.5	6506. 5	37,922.4
Total beamforming zone area (%)	2.94	14.21	82.84

These unequal areas between beamforming zones cause uneven service quality per equal area in the same cell. If users are evenly distributed in that cell, 82.84% of users are supported by beamformings of 3rd vertical layer while only 2.94% of users receive service of 1st vertical layer beamforming.

Fig. 5 shows the uniformly distributed 1,000 user's occupation of radio resources under this circumstance. All users in each beamforming are supposed to share the equal portions of radio resources.

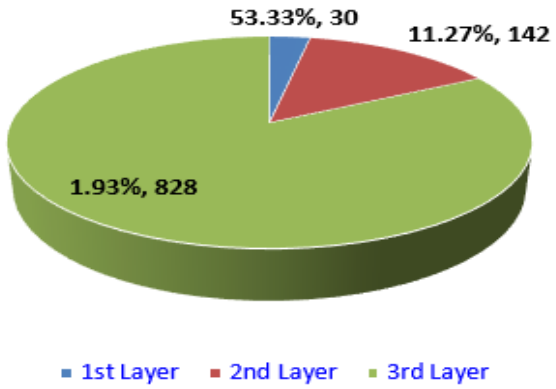


Fig. 5. Occupied Radio Resource per UE (%), Number of UEs.

Fig. 5 depicts occupied radio resource by each UE according to its belonged beamforming layer. Since each layer is assumed to be composed of 16 beamformings as shown in Fig. 4, among 1,000 thousand of uniformly distributed UEs, only 30 UEs are supported by 1st vertical layer and they can occupy about 53.33% radio resource of each beamforming, and 142 UEs are supported by 16 2nd layer beamformings while most UEs - 828 UEs- are belonged to 3rd vertical layer. Since 828 UEs have to share the resources of 16 beamformings in 3rd layer beamforming zone, each UE can occupy only 1.93% of radio resources of each beamforming in average.

In this system, even if the serving BS offers CA with 2 more frequency band, the benefit of CA converges to only 17.16 percent of UEs in the cell and overall resource occupation of UE does not varied.

III. USING CA FOR RELIEVING BEAMFORMING ZONE DEVIATION

A. A CA-BS of the same BS type with the main BS

Many remedies can alleviate this resource occupation inequality. They are the sharper beamforming [10], heterogeneous networking (HetNet) [7][11], relaying [4][5], etc. CA can be one of those solutions also.

Generally, CA is used to improve data rates for UEs and many scenarios are proposed of its deployment [6]. If CA is offered by the same BS with the main serving BS, the benefit is concentrated only a few UEs which are adjacently placed to BS in 3-dimensional beamforming system.

However, if extra CA base station (CA-BS) is located adequately apart, it can reduce the inequality of user service quality because its highly concentrated service zone is not overlapped with that of main BS.

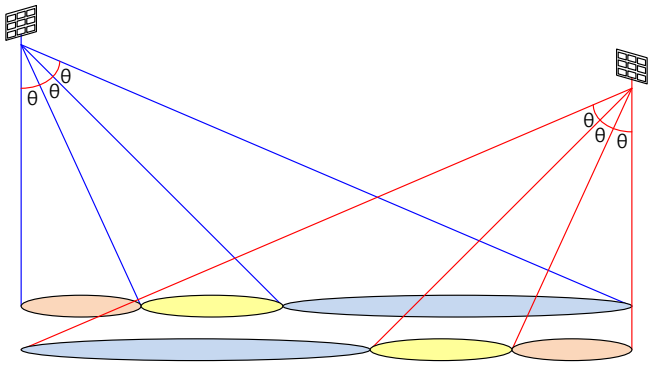


Fig. 6. The effect of CA for relieving beamforming zone area deviation.

Fig. 6 is the lateral view of the proposed CA-BS disposition. It shows that adequately located another CA-BS can offer effectively dense beamformings in large part of thin 3rd layer beamforming zone area by means of carrier aggregation.

Fig. 7 depicts ground plan of an exemplary CA-applied cells. Each CA-BS is supposed to be the same type with the main service BS but they use different component carrier band. This figure shows a large part of cell edge region can be supported by CA -BS.

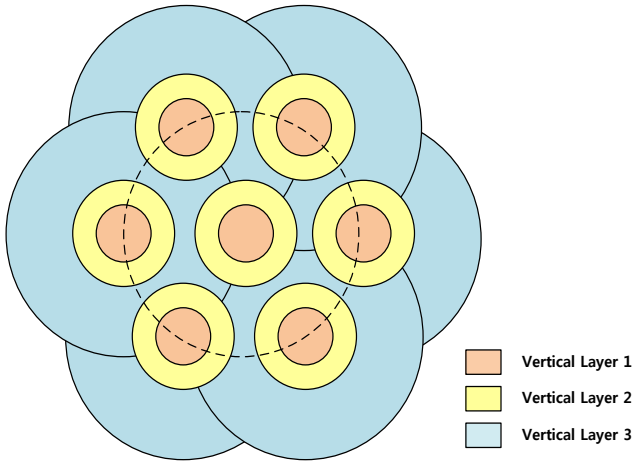


Fig. 7. Beamforming layer of CA-applied cell.

Fig. 7 depicts the situation of CA with 3 different component carrier (CC) frequency bands are used. Each CA-BS is supporting two adjacent neighbor cells also and its 3rd vertical layer beams can be adjustable to avoid inflicting interference to particular UEs.

With the cooperation of CA-BS, more than half of the UEs of our exemplary system can be supported by either 1st or 2nd vertical layer signals as shown in Table III.

TABLE III
BEAMFORMING ZONE AREAS UNDER CA CIRCUMSTANCES

CA type	1st Layer + 3rd Layer	2nd Layer + 3rd Layer	3rd Layer + 3rd Layer
Total beamforming zone area (%)	8.82	42.64	48.55

Fig. 8 depicts the calculated number of UEs and their radio resource occupation in each beamforming. Among uniformly distributed 1,000 UEs, now 486 UEs are supported by solely 3rd vertical layer, and they can occupy 9.88% of beamforming's radio resource.

88 UEs are supported by the 1st layer and as many as 426 UEs are supported by the 2nd layer beamformings. This means more than half of UEs in the cell can occupy more than moderate part of radio resources.

The resource occupation of UEs in the 1st layer and the 2nd layer does not much increase as the addition of component carriers. This means that our proposed method is for improving frequency resource sharing equality rather than enhancing data rate for small number of users through carrier aggregation.

Although the exact radio resource occupation percentage can be varied with different resource assignment strategy or CA-BS parameters, this picture shows that each UE can occupy at least about 10 % of radio resource of each beamforming, and can enjoy better degree of freedom in resource assignment.

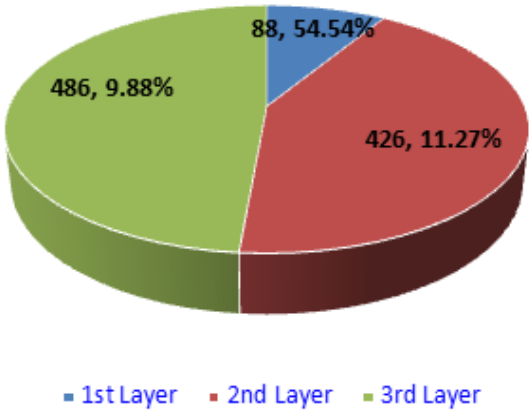


Fig. 8. Occupied Radio Resource per UE (%), Number of UEs with CA.

B. A CA-BS of the different BS type with the main BS

The CA-BS can be more simplified form compared to main BS. While main BS have to cover all its service zone with densely packed beamforming zones not to miss any unsupported UE, CA-BS can offer a few steering beams to support a small most-needed area [13]. It can dynamically change its beamforming's tilt angle and beamforming angle vertically and horizontally which dictates the location and sharpness of beamforming.

Fig. 9 shows this kind of CA-BS can support the required area flexibly. Since in most cases UEs are not evenly distributed but tend to be concentrated in relatively small area [9], so a small number of steering beams from CA-BS can be effective in supporting this hot-zone.

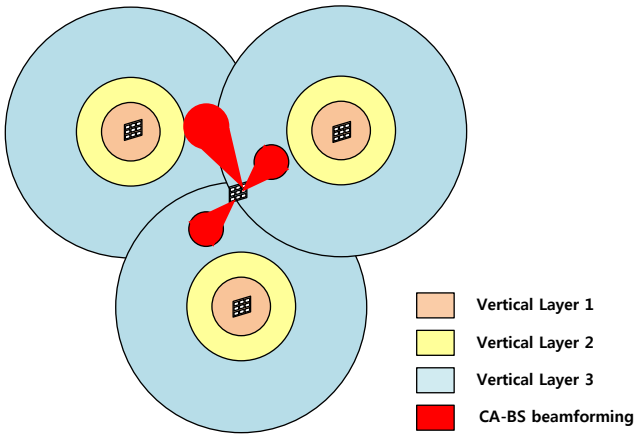


Fig. 9. The CA-BS with Dynamic steering beamforming.

When the CA-BS offers dynamically steering beamformings as shown in Fig. 9, the resultant improvement is shown in Fig.10. The capacity of CA-BS is assumed to be the same with the vertical layer 2. Although in this case, CA beamforming can afford only a small number of UEs compared to the case of Fig. 7, this kind of CA-BS can cover wide range of area with its steering beamformings.

This kind of CA-BS has relatively small capacity and it offer only one component carrier of frequency resource. However it is also helpful in supporting moderate data rate to many disadvantageous UEs.

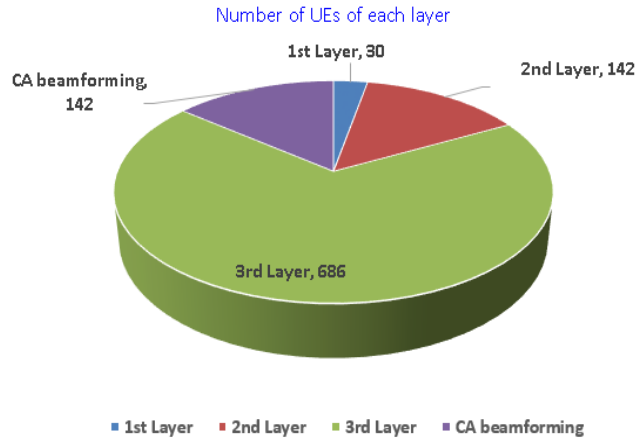


Fig. 10.Number of UEs in each beamforming layer with dynamic steering beamforming.

This displacement of extra CA-BSs is more desirable in mmWave system. Since the propagation limitation of mmWave is sterner compared to other commercial band signal [8], its cell size is relatively small and the extra CA-BSs' signal can easily cover the wide range of each cell, while any possibility can be evaded by beam steering.

Generally CA signals are transmitted from the same serving BS to enhance user data rate. However in the aspect of beamforming zone area inequality in 3-dimensional beamforming, we can see that offering CA by separated BS is desirable.

The separated CA-BSs are also important in the case of propagation deterioration such as rainfall attenuation, since mmWave is especially vulnerable to the effect of rainfall [14], separated CA-BSs can fill the coverage gap between the diameter-reduced cells in the rainy condition.

IV. Conclusions

In this paper, we showed the reason and the seriousness of the inequality of 3-dimensional beamforming zone area and its solution from adopting additional CA base station. Since the area of each beamforming becomes wider according to the distance from the base station, a large part of cell cannot help being supported from only a small number of beamformings.

Our research is about effectively alleviating this inequality to share cell capacity more evenly. Whether the CA base station's beamforming is the fixed beamforming or steering beamforming, if it is adequately placed, the radio resource occupation equality is greatly improved. Usually the CA is used to multiply the capacity of cell, but our research shows it can be used to alleviate resource occupation inequality also.

Various terrain, UE distribution, and service environment influence the most efficient cell disposition, and our research shows cooperation with remote CA base station is also vital in user service quality in 3-dimensioanl beamforming environment.

References

[1] J. Koppenborg, H. Halbauer, S. Saur, C. Hoek, "3D beamforming trials with an active antenna array," *Smart Antennas (WSA), 2012 International ITG Workshop on*, 7-8 March 2012, pp. 110-114

[2] B. Ku, D. Ahn, S. Lee, A. Shishlov, A. Reutov, S. Ganin, A. Shubov, "Radiation Pattern of Multibeam Array Antenna with Digital Beamforming for Stratospheric Communication System: Statistical Simulation," *ETRI Journal*, vol. 24, no. 3, Jun. 2002, pp. 197-204.

[3] J. Jung, "Method and apparatus for jointly transmitting/receiving a signal in a mobile communication system," K.R. Patent 10-2013-0127192, Nov. 22, 2013.

[4] J. Bae, Y. Choi, J. Kim, M. Chung, "Architecture and Performance Evaluation of MmWave Based 5G Mobile Communication System," *ICTC 2014*, 22-24. Oct. 2014, pp.847-851

[5] J. Bae, H. Park, S. Lee, Y. Choi, Jun Suk Kim, Min Young Chung, "System Coverage of MmWave Based 5G Mobile Communication System," *APCC 2014*, October 1-3, 2014, pp.1-4

[6] Z. Shen, A. Papasakellariou, J. Montojo, D. Gerstenberger, F. Xu, Overview of 3GPP LTE-advanced carrier aggregation for 4G wireless communications. *IEEE Communications Magazine*, 50(2), 2012, pp. 122-130.

[7] J. Wang, J. Liu, D. Wang, J. Pang, G. Shen, "Optimized Fairness Cell Selection for 3GPP LTE-A Macro-Pico HetNets," *Vehicular Technology Conference (VTC Fall)*, 5-8 Sept. 2011, pp.1-5

[8] M. Kim, S. Hong, Y. Kim, J. Kim, "Analysis of Resource Assignment for Directional Multihop Communications in mm-Wave WPANs," *ETRI Journal* vol.35, no.1, pp. 120-130, Feb. 2014.

[9] K. Son, S. Chong, "Dynamic Association for Load Balancing and Interference Avoidance in Multi-Cell Networks," *Wireless Communications, IEEE Trans.*, Volume 8, July 2009, pp. 3566-3576

[10] W. Roh, et al. "Millimeter-wave beamforming as an enabling technology for 5G cellular communications: theoretical feasibility and prototype results," *IEEE Communications Magazine*, 52(1), 2014, pp.106-113

[11] J. Kim, Y. Han, S. Lee, "An Efficient Downlink Coordinated Beamforming for Heterogeneous Networks," *The 78th Vehicular Technology Conference (VTC Fall)*, Sept. 2013

[12] B. K. Chalise, A. Czylwik, "Robust uplink beamforming based upon minimum outage probability criterion," *Global Telecommunications Conference (GLOBECOM),* Nov. 2004, Vol.6, pp.3974-3978

[13] S. Ha, Y. Jung, Y. Kim, C. Jung, "Reconfigurable Beam-Steering Antenna Using Dipole and Loop Combined Structure for Wearable Applications," *ETRI journal*, vol. 34, no. 1, Feb. 2012, pp. 1-8.

[14] C.Enjamio, E. Vilar, F. Perez-Fontan, "Rain Scatter Interference in mm-Wave Broadband Fixed Wireless Access Networks Caused by a 2-D Dynamic Rain Environment," *IEEE transactions on wireless communications*, Vol. 6, July 2007, pp.2497-2507

Jun-woo Kim received the B.S. degree in electronics engineering from Kyongpook National University, Daegu, Korea, in 1996, the MS from KAIST, Daejeon, Korea in 1998, and the Ph.D degree from Chungnam National University, Daejeon, Korea in 2013.
From January 1998 to September 2001, he was a researcher of Dacom Corporation. Since October 2001, He has been working in ETRI, Daejeon, Korea, where he currently works in a Giga wireless transmission research section as a senior engineer. His current research interests are VSLI, on-chip communication architecture, and various modem design.

Gosan Noh received the B.S. and Ph.D degrees in Electrical and Electronic Engineering from Yonsei University, Seoul, Korea, in 2007 and 2012, respectively.
From March 2012 to February 2013, he was a Postdoctoral Researcher at the School of Electrical and Electronic Engineering, Yonsei University, Seoul, Korea. Since March 2013, he has been with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea, where he is a Senior Researcher. His research interests include millimeter wave transmission and polarization diversity/multiplexing techniques.

Jang-won Moon received the BS degree in electronics engineering from Shibaura Institute of Technology, Tokyo, Japan, in 2007, the MS degree in wireless communication engineering from Waseda University, Tokyo, Japan in 2009. Since 2010, He has been working in ETRI, Daejeon, Korea, where he currently works in a Giga wireless transmission research section as a senior engineer. His current research interests are VSLI, on-chip communication architecture, and various modem design.

Youn-Ok Park received the B.S. degree in Electronic Engineering from Hanyang University, Seoul, Korea, in 1986, M.S. and Ph.D degrees in Information and Communication Engineering from Chungnam National University, Daejeon, Korea in 1997 and 2011 respectively.
From December 1985 to January 1987, he was a researcher of Samsung Electronics. Since February 1987, He has been with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea, where he is a Principal Member of Technical Staff of Giga wireless Transmission Research Laboratory Section.

Il-gyu Kim received the B.S. and M.S. degrees in electronics engineering from the Seoul City University, Seoul, Korea, in 1993 and 1995, respectively. In 1995, he joined the Network Implementation Section of Shinsegi Telecomm, Inc. (STI), Seoul, where he was involved in the implementation of CDMA cellular systems. Since 2000, He has been working in ETRI, Daejeon, Korea, where he currently works in a Giga wireless transmission research section as a Section Leader.

Differentiated Assignment of Extrinsic Information in Iterated Decoding of Fixed Weight Codewords

Wonsun Bong*, Yong Cheol Kim*
*Dept. of Electrical and Computer Eng., University of Seoul, Korea
gaam@uos.ac.kr, yckim@uos.ac.kr

***Abstract*—Constant amplitude multi-code (CAMC) CDMA has the same structure as a recursively generated single parity check product code. A top-level codeword of CAMC is recursively constructed from lower-level codewords. In the iterative decoding of CAMC, log likelihood ratio (LLR), *a priori* information and *extrinsic* information (EI) of a codeword is a weighted sum of LLR values of associated codewords from which it is despread or into which it is spread. In this paper, we show that differentiated assignment of EI in the computation of LLR can improve the performance of bit error correction. The weights of CAMC codewords are fixed at two fixed values. We let EI converge fast to saturation value when a codeword has the correct weight. The proposed method achieved performance improvement of $0.1 \sim 0.3$ dB in E_b/N_0 over the regular iterated decoding of CAMC. When compared with despreading ON/OFF control, a gain of about 0.1 dB is achieved, which is meaningful near the Shannon capacity limit.**

***Keywords*—Constant Amplitude Multi Code, Code Weight, Extrinsic Information, Iterated Decoding, Single Parity Check Product Code**

I. Introduction

PRODUCT codes were first introduced by Elias in 1954 [1]. The concept of product codes is that powerful long block codes can be constructed by concatenating two or more shorter constituent codes. Single parity check product code (SPCPC) is a product code in a simple structure, where a parity bit is appended to a sequence of information bits [2].

A codeword of 3-D (dimensional) SPCPC is shown in Fig. 1, which is composed of the data block, the parity checks along all three directions and parity on parity check bits. Multi-dimensional SPCPC are constructed in a similar way. In the encoder, a parity bit is appended to each of $(n-1)$-bit-long sequences along all the dimensions of a Q-D hypercube consisting of $(n-1)^Q$ information bits. The encoded output of n^Q bits is a Q-D product code with a code rate of $(1-1/n)^Q$.

Manuscript received date is November 9, 2015. This research was supported by Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology (grant number NRF-2013R1A1A2012745). This paper is a follow-up of the invited journal to the accepted conference paper of the 16th International Conference on Advanced Communication Technology.

Wonsun Bong is with the department of Electrical and Computer Engineering, University of Seoul, Seoul 02504, Korea (email: gaam@uos.ac.kr). Yong Cheol Kim is with the department of Electrical and Computer Engineering, University of Seoul, Seoul 02504, Korea (corresponding author; +82-2-6490-2331; e-mail: yckim@uos.ac.kr).

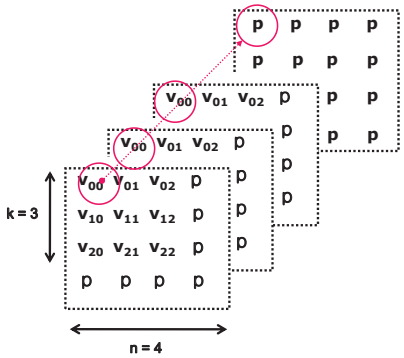


Fig. 1: 3-D SPCPC: Parities are in all three directions.

Kim presented a recursive SPCPC, where a codeword is recursively constructed by pseudo-Hadamard spreading of three lower-dimensional codewords concatenated with their parity bits [3]. Recursive SPCPC was originally developed as a constant amplitude multi-code (CAMC) CDMA.

Multi-code CDMA is a technique of providing versatile data rates by assigning multiple channels to a single user [4] [5] [6]. Multi-code signal has a large amplitude variation since it is a sum of random binary signals from several channels. Large variation signal requires a highly linear power amplifier, which consumes a large power. CAMC was developed to perfectly remove the amplitude fluctuation of multi-code signal.

The encoder of CAMC accommodates $M(=3^Q)$ information bits, $\mathbf{b}^{\mathrm{M}} = [b_0, b_1, ..., b_{M-1}]$, and generates a $N(=4^Q)$-bit-long string, $\mathbf{v}^{\mathrm{N}} = [v_0, v_1, ..., v_{N-1}]$, of constant amplitude by pseudo-Hadamard spreading in a recursive manner. The code rate of CAMC is $R = (3/4)^Q$, which is equivalent to that of SPCPC with $n = 4$. Throughout this paper, recursive SPCPC with $n = 4$ is interchangeably referred to as CAMC.

Previous works show that CAMC outperforms conventional SPCPC. CAMC has some advantageous features as follows [7] [8]. First, CAMC benefits from the despreading process which is performed after the iterative decoding. Second, CAMC does not have any low weight codewords which usually degrade the performance at low SNR. The weights of codewords are evenly distributed at two fixed values. Third, the property of fixed weight can guide the computation of extrinsic information (EI) which is the key element in the iterative decoding.

Analysis on the first and the second features were reported in [8] [9]. In this paper, we focus on the third feature. We show that, with differentiated assignment of EI based on the integrity of code weights, we get performance improvement of 0.1∼0.3 dB when compared to previous works.

This paper is organized as follows: In Section II, encoding and decoding of CAMC are briefly presented. In Section III, iterated decoding of conventional SPCPC is described. In Section IV, iterative decoding and despreading of CAMC are presented. In Section V, ON/OFF control of despreading after iterative decoding is presented. In Section VI, the proposed differentiated assignment of EI, based on the fixed weight property of CAMC, is presented. In Section VII, computer simulation results on performance improvement are presented. Finally, a conclusion is drawn in Section VIII.

II. Constant Amplitude Multi Code

In this Section, the generation of CAMC signal vectors is briefly described [3]. Throughout this paper, the polarity of a bit is bipolar, either (+1) or (-1). An encoded CAMC vector at J-level has a length of $L(=4^J)$ bits. Then, for every three J-level vectors, a bit-by-bit J-level parity vector is generated. Spreading the concatenation of three J-level vectors and their parity vector generates a $(J+1)$-level vector with a length of $4L$ bits. Inversely, despreading a J-level vector results in three $(J-1)$-level signal vectors and their bit-by-bit parity vector, each with a length of $L/4$ bits.

In the following notations, a superscript represents the size of the vector, except when the subscript is of the form $i/4$. Integer subscripts of $\{0,1,2,3\}$, if any, stand for the distinct number of vectors. Either $\mathbf{v}_i^{\mathrm{L}}$ or $\mathbf{v}^{\mathrm{L}}$ is a L-bit-long CAMC vector, There is no meaningful difference between them. Subscripts of $\{0/4, 1/4, 2/4, 3/4\}$ represent the index of the four quadrants of a regular CAMC vector. For example, $\mathbf{v}_{i/4}^{\mathrm{L}},\ i \in \{0,1,2,3\}$, is not a regular CAMC vector by itself, but just a quadrant of a regular L-bit-long CAMC vector, $\mathbf{v}^{\mathrm{L}}$, as shown in (1). The vertical bar represents concatenation.

$$\mathbf{v}^{\mathrm{L}} = [\mathbf{v}_{0/4}^{\mathrm{L}} \mid \mathbf{v}_{1/4}^{\mathrm{L}} \mid \mathbf{v}_{2/4}^{\mathrm{L}} \mid \mathbf{v}_{3/4}^{\mathrm{L}}] \tag{1}$$

Fig. 2 and Fig. 3 show the generation of parity bits in a CAMC vector [3]. An input of M information bits is divided into $M/3$ strings of three bits each. Each 3-bit-long string is encoded at the basic-level encoder $\mathbf{Q^4}$. For input $[b_0, b_1, b_2]$, a parity bit $p_3 = -b_0 \cdot b_1 \cdot b_2$ is appended to them. Then, four bits of unit amplitude, $\mathbf{v}_0^4 = [v_0, v_1, v_2, v_3]$ are generated from spreading by 4×4 Hadamard matrix.

$$\mathbf{v}_0^4 = \frac{1}{2} \cdot [b_0 \quad b_1 \quad b_2 \quad p_3] \cdot \mathbf{H}^4 \tag{2}$$

$$\mathbf{H}^4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \tag{3}$$

In a similar way, $[b_3, b_4, b_5]$ and $[b_6, b_7, b_8]$ are encoded into $\mathbf{v}_1^4$ and $\mathbf{v}_2^4$ of constant amplitude. A 4-bit-long parity $\mathbf{p}^4$ is

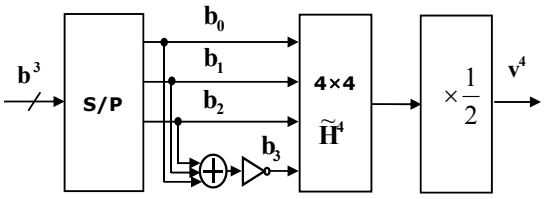


Fig. 2: Generation of 4-bit CAMC vector

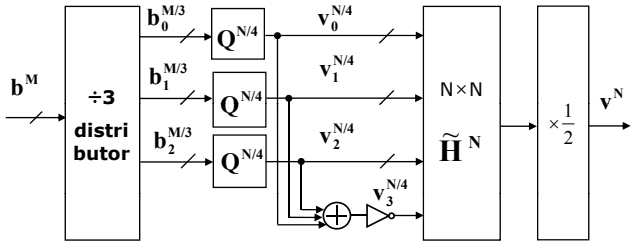


Fig. 3: Generation of N-bit CAMC vector

generated from bit-by-bit product (denoted as $.*$) of $\mathbf{v_0^4}$, $\mathbf{v_1^4}$ and $\mathbf{v_2^4}$.

$$\mathbf{p}^4 = -\mathbf{v_0^4}. * \mathbf{v_1^4}. * \mathbf{v_2^4} \tag{4}$$

For the spreading of concatenation of three CAMC vectors and one parity vector, we use a pseudo-Hadamard matrix, $\tilde{\mathbf{H}}^{\mathrm{N}}$. This is in the form of Hadamard matrix with "1" element in (3) replaced by an identity matrix $\mathbf{I}^{\mathrm{N}/4}$ of size $N/4 \times N/4$. As a special case, $\tilde{\mathbf{H}}^4$ is identical to $\mathbf{H}^4$.

$$\tilde{\mathbf{H}}^{\mathrm{N}} = \begin{bmatrix} \mathbf{I}^{\mathrm{N}/4} & \mathbf{I}^{\mathrm{N}/4} & \mathbf{I}^{\mathrm{N}/4} & \mathbf{I}^{\mathrm{N}/4} \\ \mathbf{I}^{\mathrm{N}/4} & -\mathbf{I}^{\mathrm{N}/4} & \mathbf{I}^{\mathrm{N}/4} & -\mathbf{I}^{\mathrm{N}/4} \\ \mathbf{I}^{\mathrm{N}/4} & \mathbf{I}^{\mathrm{N}/4} & -\mathbf{I}^{\mathrm{N}/4} & -\mathbf{I}^{\mathrm{N}/4} \\ \mathbf{I}^{\mathrm{N}/4} & -\mathbf{I}^{\mathrm{N}/4} & -\mathbf{I}^{\mathrm{N}/4} & \mathbf{I}^{\mathrm{N}/4} \end{bmatrix} \tag{5}$$

Both $\tilde{\mathbf{H}}^{\mathrm{N}}$ and $\mathbf{H}^{\mathrm{N}}$ are orthogonal, subject to a scaling factor.

$$\tilde{\mathbf{H}}^{\mathrm{N}} \cdot (\tilde{\mathbf{H}}^{\mathrm{N}})^t = \tilde{\mathbf{H}}^{\mathrm{N}} \cdot \tilde{\mathbf{H}}^{\mathrm{N}} = 4 \cdot \mathbf{I}^{\mathrm{N}} \tag{6}$$

$$\mathbf{H}^{\mathrm{N}} \cdot (\mathbf{H}^{\mathrm{N}})^t = \mathbf{H}^{\mathrm{N}} \cdot \mathbf{H}^{\mathrm{N}} = N \cdot \mathbf{I}^{\mathrm{N}} \tag{7}$$

The 16-bit-long concatenation of $\mathbf{v_0^4}$, $\mathbf{v_1^4}$, $\mathbf{v_2^4}$ and $\mathbf{p}^4$ is spread into $\mathbf{v}^{16}$ of unit amplitude.

$$\mathbf{v}^{16} = \frac{1}{2} \cdot [\mathbf{v}_0^4 \mid \mathbf{v}_1^4 \mid \mathbf{v}_2^4 \mid \mathbf{p}^4] \cdot \tilde{\mathbf{H}}^{16} \tag{8}$$

Continuing this way, the output of three $\mathbf{Q}^{\mathrm{N}/4}$ encoders ($3N/4$ bits, in all) and their bit-by-bit parity vector ($N/4$ bits) are generated.

$$\mathbf{p}^{\mathrm{N}/4} = -\mathbf{v}_0^{\mathrm{N}/4}. * \mathbf{v}_1^{\mathrm{N}/4}. * \mathbf{v}_2^{\mathrm{N}/4} \tag{9}$$

Finally, thee N-bit-long concatenation of $\mathbf{v_0}^{\mathrm{N}/4}$, $\mathbf{v_1}^{\mathrm{N}/4}$, $\mathbf{v_2}^{\mathrm{N}/4}$ and $\mathbf{p}^{\mathrm{N}/4}$ is spread by $\tilde{\mathbf{H}}^{\mathrm{N}}$, into $\mathbf{v}^{\mathrm{N}} = [v_0, v_1, ..., v_{N-1}]$ of unit amplitude.

$$\mathbf{v}^{\mathrm{N}} = \frac{1}{2} \cdot [\mathbf{v}_0^{\mathrm{N}/4} \mid \mathbf{v}_1^{\mathrm{N}/4} \mid \mathbf{v}_2^{\mathrm{N}/4} \mid \mathbf{p}^{\mathrm{N}/4}] \cdot \tilde{\mathbf{H}}^{\mathrm{N}} \tag{10}$$

While a top-level codeword $\mathbf{v}^{\mathrm{N}}$ is encoded from recursive spreading by pseudo-Hadamard $\tilde{\mathbf{H}}^{\mathrm{N}}$, decoding of $\mathbf{v}^{\mathrm{N}}$ is obtained from one-time despreading by a regular $\mathbf{H}^{\mathrm{N}}$.

$$\begin{aligned} & \mathbf{v}^{\mathrm{N}} \cdot \mathbf{H}^{\mathrm{N}} \qquad (11) \\ &= 2[\mathbf{v}_0^{\mathrm{N}/4}\mathbf{H}^{\mathrm{N}/4} \mid \mathbf{v}_1^{\mathrm{N}/4}\mathbf{H}^{\mathrm{N}/4} \mid \mathbf{v}_2^{\mathrm{N}/4}\mathbf{H}^{\mathrm{N}/4} \mid \mathbf{v}_3^{\mathrm{N}/4}\mathbf{H}^{\mathrm{N}/4}] \\ &= 2^{(\log_4 N-1)}[\mathbf{v}_0^4\mathbf{H}^4 \mid \mathbf{v}_1^4\mathbf{H}^4 \mid \mathbf{v}_2^4\mathbf{H}^4 \mid \mathbf{v}_3^4\mathbf{H}^4 \mid \ldots] \\ &= 2^{\log_4 N}[d_0, d_1, d_2, d_3, d_4, \ldots] \end{aligned}$$

The values of correlation vector, $\mathbf{D}$, of noise-free $\mathbf{v}^{\mathrm{N}}$ are $d_i = \pm 1$. But, $\mathbf{D}$ obtained from a noisy received signal at the receiver takes on non-binary values. In this case, we hard-limit $\mathbf{D}$ into binary values. The correlation vector $[d_0, d_1, d_2, ...]$ is in the form of a hypercube consisting of information bits and parity bits, just like a conventional SPCPC as shown in Fig. 1. The information bits are extracted from the corresponding positions. Bits $\{d_3, d_7, d_{11}, d_{12}, d_{13}, d_{14}, d_{15}, d_{19}, ...\}$ are in the positions which correspond to the parity positions in the hypercube. Removing such bits, we get the information-only bits $[b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7, ...]$.

III. Iterative Decoding of a Product Code

The decoding process of a product code is similar to solving a crossword puzzle. In the product array, one symbol is associated with two values through *diversity* effect: One is the very value of the received symbol itself and the other is the *extrinsic* value which can be inferred from the other symbols. When bit errors through a channel , these two values may be different. This discrepancy can be relaxed in the iterative decoding process where the range of the possible values of a target symbol is adjusted through exchange of EI among neighboring symbols.

Being a product code, SPCPC has powerful error correcting capability, SPCPC has the same basic features of turbo codes: interleaving, iteration and soft-output decoding [10]. Hagenauer developed a soft input, soft output-based decoding algorithm for a multi-dimensional product code [11].

Rankin [2] extended the works of [11] and proposed an iterative decoding algorithm for SPCPC. It is an iterative algorithm which refines the log likelihood ratio (LLR) for each bit by iteratively exchanging information in a relaxational scheme.

In SPCPC, a parity bit is appended along all the dimensions of a Q-D interleaved hypercube. The LLR, $L_q(X_k)$, for the k-th bit in the q-th dimension is iteratively refined by exchanging the extrinsic information between dimensions.

LLR consists of three terms: the channel reliability which is proportional to the signal strength, the *a priori* information (API, $A_q(X_k)$) and the extrinsic information (EI, $E_q(X_k)$). $\mathbf{X} = [X_0, X_1, ..., X_{N-1}]$ is the input vector and $\mathbf{Y} = [Y_0, Y_1, ..., Y_{N-1}]$ is the received signal vector through a binary-input AWGN channel.

$$L_q(X_k) = \log \frac{\Pr(X_k = +1 \mid \mathbf{Y})}{\Pr(X_k = -1 \mid \mathbf{Y})} = \frac{2}{\sigma^2} Y_k + E_q(X_k) + A_q(X_k) \tag{12}$$

$$E_q(X_k) = 2 \tanh^{-1} \left[\prod_{j=0, j \neq k}^{N-1} \tanh\left(\frac{A_q(X_j) + \frac{2}{\sigma^2} Y_j}{2} \right) \right] \tag{13}$$

$$A_q(X_k) = \sum_{i=1, i \neq q}^{Q} E_i(X_k) \tag{14}$$

IV. Decoding of CAMC

CAMC is generated by direct sequence spreading of lower dimensional codewords concatenated with their bit-by-bit parity vector. The internal structure of CAMC has both aspects of a product code and a spread spectrum signal.

The decoding process of CAMC consists of two stages: the iterative decoding for SPCPC and the despreading for spread spectrum signal. First, the noisy received bits, ***Y***, are iteratively decoded into ***X***, which consists of information bits and parity bits, as encoded in the recursive encoder. ***X*** is despread into ***D***, which consists only of information bits. Fig. 4 illustrates the flow of data, the recursive spreading, transmission through a noisy channel, iterated decoding and despreading.

Since CAMC belongs to SPCPC, a similar decoding algorithm could be used for CAMC. The decoding algorithm for conventional SPCPC described in Section III, however, cannot be directly applied to CAMC. Unlike SPCPC, there are no *raw* parity bits in a CAMC vector since parity bits are mixed with information bits through the spreading process.

Kim developed a decoding algorithm which separates parity bits and then iteratively refines the LLR of the bits [7]. Parity bits required for the iterative decoding are recursively extracted by decomposing higher level CAMC vectors into lower level vectors. One J-level vector, $\mathbf{v}^{\mathrm{L}}$, is despread by $\tilde{\mathbf{H}}^{\mathrm{L}}$ into four $(J-1)$-level vectors, $(\mathbf{v}_0^{\mathrm{L}/4}, \mathbf{v}_1^{\mathrm{L}/4}, \mathbf{v}_2^{\mathrm{L}/4}, \mathbf{p}^{\mathrm{L}/4})$.

$$\begin{aligned} & \frac{1}{2} \cdot \mathbf{v}^{\mathrm{L}} \cdot \tilde{\mathbf{H}}^{\mathrm{L}} \qquad (15) \\ &= \frac{1}{4} \cdot [\mathbf{v}_0^{\mathrm{L}/4} \mid \mathbf{v}_1^{\mathrm{L}/4} \mid \mathbf{v}_2^{\mathrm{L}/4} \mid \mathbf{p}^{\mathrm{L}/4}] \cdot \tilde{\mathbf{H}}^{\mathrm{L}} \cdot \tilde{\mathbf{H}}^{\mathrm{L}} \\ &= [\mathbf{v}_0^{\mathrm{L}/4} \mid \mathbf{v}_1^{\mathrm{L}/4} \mid \mathbf{v}_2^{\mathrm{L}/4} \mid \mathbf{p}^{\mathrm{L}/4}] \end{aligned}$$

The fourth vector, $\mathbf{p}^{\mathrm{L}/4}$, is the bit-by-bit parity vector of the three preceding CAMC vectors. Each of the three vectors, $\{\mathbf{v}_0^{\mathrm{L}/4}, \mathbf{v}_1^{\mathrm{L}/4}, \mathbf{v}_2^{\mathrm{L}/4}\}$, can be despread into four $(J-2)$-level CAMC vectors, $[\mathbf{v}_0^{\mathrm{L}/16} \mid \mathbf{v}_1^{\mathrm{L}/16} \mid \mathbf{v}_2^{\mathrm{L}/16} \mid \mathbf{p}^{\mathrm{L}/16}]$.

The parity relation among four J-level vectors holds only in the context of the J-th dimension. Likewise, EI and API associated with J-level CAMC vectors are valid only in the J-th dimension. For other dimensions, we need to spread or despread CAMC vectors as needed. Hence, when EI is exchanged between dimensions, it needs to be spread or

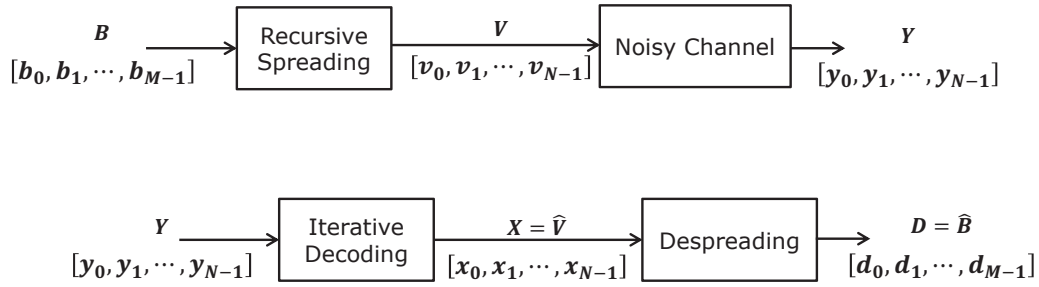


Fig. 4: Received bits ($\boldsymbol{Y}$) are iteratively decoded ($\boldsymbol{X}$) and then despread into information bits ($\boldsymbol{D}$).

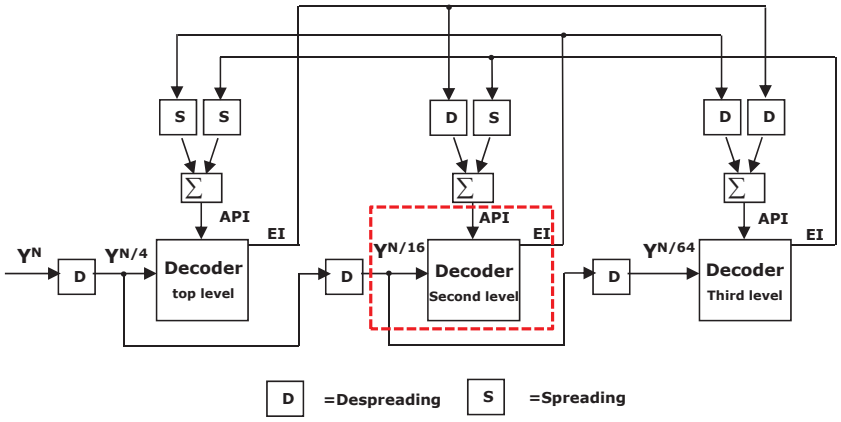


Fig. 5: EI is despread/spread between dimensions.

despread to fit into the structure of three CAMC vectors plus one parity vector in the corresponding dimensions.

Fig. 5 illustrates the block diagram for the decoding of CAMC for $N = 64$. The blocks S(.) and D(.) stand for the spreading process and the despreading process, respectively. Expressions for LLR ($L_q(X_k^q)$), EI ($E_q(X_k^q)$) and API ($A_q(X_k^q)$) for CAMC are shown in (16) through (18).

X_k^q is the k-th bit of the vector reconfigured into the q-th dimension. $[X_0^q, X_1^q, \ldots, X_{L-1}^q]$ and $[Y_0^q, Y_1^q, \ldots, Y_{L-1}^q]$, $(L = 4^q)$, stand for an input vector and the received vector reconfigured into the q-th dimension.

$$L_q(X_k^q) = \frac{2}{\sigma^2} Y_k^q + E_q(X_k^q) + A_q(X_k^q) \tag{16}$$

$$E_q(X_k^q) = 2\tanh^{-1}\left[\prod_{j=0, j\neq k}^{N-1} \tanh\left(\frac{A_q(X_j^q) + \frac{2}{\sigma^2} Y_j^q}{2}\right)\right] \tag{17}$$

$$A_q(X_k^q) = \sum_{i=1}^{q-1} S(E_i(X_k^q)) + \sum_{i=q+1}^{Q} D(E_i(X_k^q)) \tag{18}$$

The final estimate of X_k^Q, is obtained from hard-limiting of the top-level LLR. In the case of conventional SPCPC, the decoding process would end here. Unlike SPCPC, the decoding process of CAMC passes through one more stage, as shown in Fig. 4. In CAMC, the decoded output is obtained from despreading of iteratively decoded signal. The LLR values of the iteratively decoded bits are multiplied by $\mathbf{H}^{\mathrm{N}}$ and then the information bits are extracted from the despread hypercube.

Though the structure of CAMC is similar to conventional SPCPC, some distinct features of CAMC provides advantage over SPCPC. The first advantage is the processing gain which comes from the spread spectrum property of CAMC. While, in conventional SPCPC, correction of bit errors is performed only in the iterative decoding stage, additional correction of bit errors is also achieved in the despreading of the iteratively decoded bits in CAMC.

Another advantageous feature is the fixed weight of CAMC, as will be described in Section VI. In error correcting codes, the minimum distance of the code has been regarded as an important factor for BER performances. Battail [13] suggested that, in SPCPC, the weight distribution is more important than the minimum distance.

Later, Biglieri [14] showed that iterated product codes have Gaussian weight distribution even when they are relatively

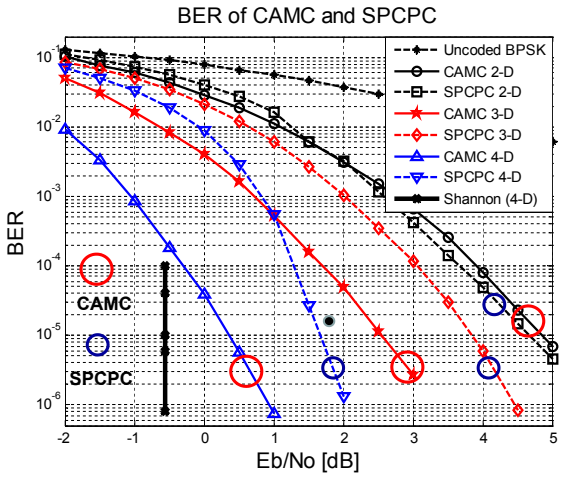


Fig. 6: CAMC, SPCPC and Shannon limit

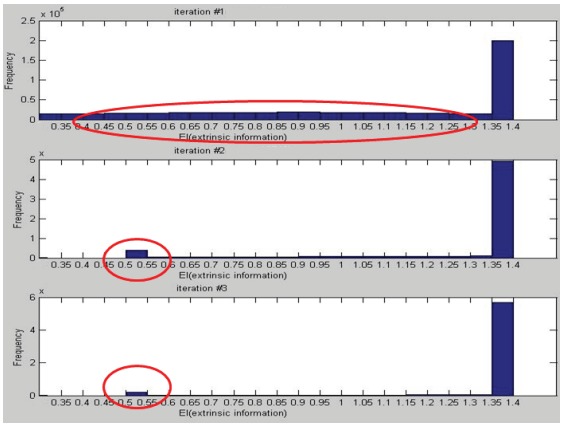


Fig. 7: Over iterations, |EI| converges to $|E_{max}|$

short codes. The random-like criterion for designing a product code (or a turbo code) was supported by several other works [15]. A product code with Gaussian weight usually has good performance. Some of the codewords, however, at the tail of the Gaussian distribution have small weights and can affect the performance adversely.

While conventional SPCPC usually has Gaussian weight distribution, the codeword weights of CAMC are very close to the $N/2$. Hence, CAMC does not have any low weight codewords which usually degrade the performance at low SNR.

As a comparison of (12),(13),(14) with(16),(17),(18) shows, iterative decoding of CAMC is more expensive than the iterative decoding of conventional product codes since the computation is crossing over the whole dimensionality of CAMC. This computational cost, however, helps to achieves a performance improvement in error correction.

In Fig. 6 is shown the performance of CAMC compared with that of corresponding SPCPC with $n = 4$ [7]. BPSK modulated signal is transmitted through a binary-input AWGN channel. The code rates are $R_2 = 9/16$ (2-D), $R_3 = 27/64$ (3-D) and $R_4 = 81/256$ (4-D), respectively. For BER of 10^{-5}, CAMC outperforms SPCPC by 1.3∼1.4 dB. The Shannon capacity limit of the binary-input AWGN channel for code rate $81/256$ is -0.55 dB. Hence, 4-D CAMC is only 0.95 dB away from Shannon limit [12].

V. On/Off Controlled Despreading of CAMC

EI is a rough estimate of the reliability for the received signal. We examined how the distribution of EI changes over the iterative steps [8]. Fig. 7 shows the histogram of |EI| during the process of the iterated decoding. At the initial stage, a large part of the EI values are randomly distributed in the range between $-E_{max}$ and $+E_{max}$. Gradually, EI converges either to $+E_{max}$ for a positive bit or to $-E_{max}$ for a negative bit. $\pm|E_{max}|$ is the saturation value of EI which is set to prevent EI from diverging.

The convergence of EI is highly correlated with the process of error correction. Fast convergence to $\pm|E_{max}|$ implies that errors continue to be corrected. On the contrary, slow convergence or no convergence imply that soft decision values are close to zero and the polarity of EI randomly toggles. Practically, no errors are being corrected when EI does not converge.

We can use EI as a performance predictor of despreading control, where the information bits are finally obtained from despreading of iteratively decoded signal. In the despreading process of the previous work [7], the LLR values of *all* the iteratively decoded bits are multiplied by $\mathbf{H}^{\mathrm{N}}$.

We modified this scheme such that such that only those bits with EI converged to $\pm|E_{max}|$ keep their LLR values. The other bits with $|\mathrm{EI}| < |E_{max}|$ are assigned LLR values of zero [8]. The basic idea is that we perform despreading only when it is likely to help to reduce the bit errors. This algorithm has been tested and it brings a performance gain of about 0.2 dB for 4-D CAMC [16].

VI. Differentiated Assignment of EI by Weight

An interesting feature of CAMC is that, unlike conventional SPCPC, the weights of CAMC are evenly distributed at two fixed values [9].

$$w(\mathbf{v}^{\mathrm{N}}) = (N \pm \sqrt{N})/2 \tag{19}$$

This is true of codewords at any level. When a N-bit-long codeword is despread into sub-level codewords of L-bit-long, they also have weights of $(L \pm \sqrt{L})/2$. Weights for code length of $N = 4 \sim 64$ are shown in Table I.

TABLE I
Weights of CAMC for $N = 4 \sim 64$

Code Length (N)	4	16	64
Dimension	1	2	3
Weights	1,3	6,10	28,36

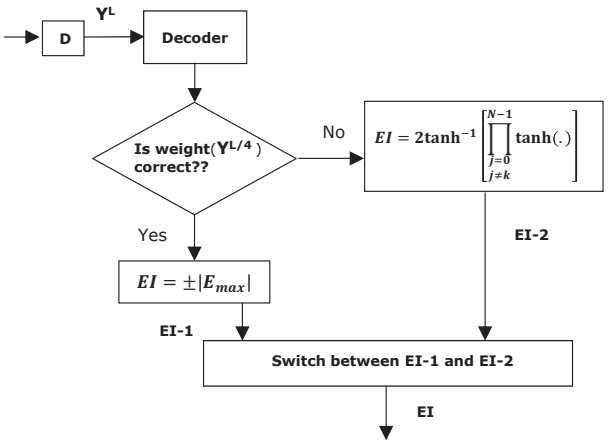


Fig. 8: EI converges fast to $\pm|E_{max}|$ if weight is correct.

The property that CAMC has fixed weight can be used to detect erroneous received vectors. When the weight of $\mathbf{y}^{\mathrm{L}}$ is not equal to $(L \pm \sqrt{L})/2$, then at least one bit of $\mathbf{y}^{\mathrm{L}}$ is erroneous. The uncertainty range of the bit error is the entire length of the received vector. This range can be reduced to $1/4$ by despreading $\mathbf{y}^{\mathrm{L}}$ into four quarter-sized vectors and examining the weight of each of them. This is the motivation of differentiated assignment of EI to codewords in accordance with their weight integrity.

A. Reduction of Uncertainty Range by Despreading

The received signal $\mathbf{y^L}$ is a sum of a CAMC vector and a noise vector.

$$\begin{aligned} \mathbf{y}^{\mathrm{L}} &= \mathbf{v}^{\mathrm{L}} + \mathbf{n}^{\mathrm{L}} \\ v_i &\in \{+1, -1\} \\ y_i &\begin{cases} \text{no error} & -1 \le n_i \le +1 \\ \text{error} & \text{if } v_i = -1 \text{ AND } n_i \ge +1 \\ \text{error} & \text{if } v_i = +1 \text{ AND } n_i \le -1 \end{cases} \end{aligned} \tag{20}$$

Despreading $\mathbf{y}^{\mathrm{L}}$ by $\tilde{\mathbf{H}}^{\mathrm{N}}$ generates three CAMC vectors and a parity vector. Using (6) and (10), we get:

$$\begin{aligned} & \frac{1}{2} \cdot \mathbf{y}^{\mathrm{L}} \cdot \tilde{\mathbf{H}}^{\mathrm{L}} \\ &= \frac{1}{2} \cdot [\mathbf{v}^{\mathrm{L}}_{0/4} + \mathbf{n}^{\mathrm{L}}_{0/4} \mid \mathbf{v}^{\mathrm{L}}_{1/4} + \mathbf{n}^{\mathrm{L}}_{1/4} \mid \ldots] \cdot \tilde{\mathbf{H}}^{\mathrm{L}} \\ &= \quad [\mathbf{y}^{\mathrm{L}/4}_0 \mid \mathbf{y}^{\mathrm{L}/4}_1 \mid \mathbf{y}^{\mathrm{L}/4}_2 \mid \mathbf{y}^{\mathrm{L}/4}_3] \end{aligned} \tag{21}$$

Then, it follows that each of the four despread vectors, $\{\mathbf{y}^{\mathrm{L}/4}_0, \mathbf{y}^{\mathrm{L}/4}_1, \mathbf{y}^{\mathrm{L}/4}_2, \mathbf{y}^{\mathrm{L}/4}_3\}$ is a sum of a regular CAMC vector (or a parity vector) and noise vectors.

$$\mathbf{n}^{\mathrm{L}} = [\mathbf{n}^{\mathrm{L}}_{0/4} \mid \mathbf{n}^{\mathrm{L}}_{1/4} \mid \mathbf{n}^{\mathrm{L}}_{2/4} \mid \mathbf{n}^{\mathrm{L}}_{3/4}] \tag{22}$$

$$\begin{aligned} \mathbf{y}^{\mathrm{L}/4}_0 &= \mathbf{v}^{\mathrm{L}/4}_0 + \frac{1}{2}\left\{\mathbf{n}^{\mathrm{L}}_{0/4} + \mathbf{n}^{\mathrm{L}}_{1/4} + \mathbf{n}^{\mathrm{L}}_{2/4} + \mathbf{n}^{\mathrm{L}}_{3/4}\right\} \\ \mathbf{y}^{\mathrm{L}/4}_1 &= \mathbf{v}^{\mathrm{L}/4}_1 + \frac{1}{2}\left\{\mathbf{n}^{\mathrm{L}}_{0/4} - \mathbf{n}^{\mathrm{L}}_{1/4} + \mathbf{n}^{\mathrm{L}}_{2/4} - \mathbf{n}^{\mathrm{L}}_{3/4}\right\} \\ \mathbf{y}^{\mathrm{L}/4}_2 &= \mathbf{v}^{\mathrm{L}/4}_2 + \frac{1}{2}\left\{\mathbf{n}^{\mathrm{L}}_{0/4} + \mathbf{n}^{\mathrm{L}}_{1/4} - \mathbf{n}^{\mathrm{L}}_{2/4} - \mathbf{n}^{\mathrm{L}}_{3/4}\right\} \\ \mathbf{y}^{\mathrm{L}/4}_3 &= \mathbf{p}^{\mathrm{L}/4} + \frac{1}{2}\left\{\mathbf{n}^{\mathrm{L}}_{0/4} - \mathbf{n}^{\mathrm{L}}_{1/4} - \mathbf{n}^{\mathrm{L}}_{2/4} + \mathbf{n}^{\mathrm{L}}_{3/4}\right\} \end{aligned} \tag{23}$$

The added noise is one half of the sum of four quadrants of the noise vector. If we assume that $\mathbf{n}^{\mathrm{L}}$ is an AWGN random process, then the noise component in $\mathbf{y}^{\mathrm{L}/4}_i$ is also an AWGN random process and the noise variance in each bit of $\mathbf{y}^{\mathrm{L}/4}_i$ is the same as that of each bit of $\mathbf{y}^{\mathrm{L}}$.

With equal noise power, the expected number of bit errors is also the same in $\mathbf{y}^{\mathrm{L}}$ and in $[\mathbf{y}^{\mathrm{L}/4}_0 \mid \mathbf{y}^{\mathrm{L}/4}_1 \mid \mathbf{y}^{\mathrm{L}/4}_2 \mid \mathbf{y}^{\mathrm{L}/4}_3]$. For example, if $\mathbf{y}^{\mathrm{L}}$ has a single bit error, then it is highly likely that only one of $\mathbf{y}^{\mathrm{L}/4}_i,\ i \in \{0, 1, 2, 3\}$, is in error and the other three are free from errors. In that case, we can easily find which one of the four is in error by examining the weight of each of $\mathbf{y}^{\mathrm{L}/4}_i$. As a result, the uncertainty range of the position of bit error is reduced to $1/4$ of the initial range.

B. Assignment of EI Based on Weight Integrity

The fixed value of code weight can guide the iterative decoding. In a product code, the magnitude LLR of a bit is a rough estimate of the reliability of the bit, that is, how well the parity relation is consistent with other bits. The magnitude of LLR for noisy bits is usually low.

In the iterative decoding of CAMC, the LLR of a codeword is a weighted sum of LLR values of associated codewords from which it is despread or into which it is spread. If any of the codewords have a wrong weight, then they are definitely in error. The iterative decoding can be improved by differentiated handling of EI of codewords in accordance with their weight integrity. We can give larger confidence to those codewords with correct weights.

We propose to let EI quickly converge to $\pm E_{max}$ if the weight is correct. When the weight of the codeword has the correct weight, EI for the bits in the codeword takes on the saturation value. We set EI $= +|E_{max}|$ or EI $= -|E_{max}|$ if the sum in (17) is positive or negative, respectively. For the other bits in codewords with wrong weights, the computation of EI follows the normal computation in (17).

Fig. 8 is the modified block for EI computation which replaces the dotted block in Fig. 5. The modified version of EI computation in (17) is shown in (24).

$$E_q(X_k^q) = \begin{cases} 2\tanh^{-1}\left[\prod_{j=0,j\neq k}^{N-1}\tanh\left(\frac{A_q(X_j^q)+\frac{2}{\sigma^2}Y_j^q}{2}\right)\right] \\ \qquad \text{bits in wrong codeword} \\ \pm E_{max} \\ \qquad \text{bits in correct codeword} \end{cases} \tag{24}$$

VII. Results of Differentiated EI

The performance of the differentiated EI assignment is tested in a computer simulation. Comparison with two previous results are presented. Both results are for BPSK modulations of 2-D, 3-D and 4-D of CAMC in binary-input AWGN channel. First, a comparison with plain iterated decoding of CAMC [7] is shown in Fig. 9. A gain of 0.1∼0.3 dB in E_b/N_0 is achieved.

Second, a comparison with despreading On/Off control in Section V is shown in Fig. 10. We get a gain of about 0.1 dB. Though the amount of gain appears small, this gain is meaningful near the Shannon capacity limit, which is achieved by CAMC. We can observe that most of the improvement are obtained in channels of high SNR. For low SNR channel, little improvement is obtained. A logical analysis is as follows:

There are two possibilities of a codeword having the correct weight. One is that an erroneous codeword with even number of bit errors with opposite polarity canceling each other happens to have a correct weight. When the channel SNR is low, this probability is not negligible. Favored assignment of EI to these *unqualified* codewords does not help. It may even slow down the convergence of EI.

The other possibility is that the codeword is indeed error-free. This probability gets larger as SNR is higher. Preferred assignment of EI at high SNR helps.

VIII. Conclusions

The codewords of CAMC have fixed weight of $(N \pm \sqrt{N})/2$. This feature provides outperformance of CAMC over conventional SPCPC. The uncertainty range of the position of bit errors can be reduced to $1/4$ by examining the weights of despread quarter-sized vectors. We showed that differentiated computation of EI depending on the integrity of a code weight helps to improve the performance.

In the proposed scheme, a codeword with a correct weight is given a larger confidence. EI values for their bits quickly converge to $\pm E_{max}$. Performance improvement of $0.1 \sim 0.3$ dB in E_b/N_0 are obtained, when compared with plain iterated decoding. A gain of about 0.1 dB is when compared with despreading control of CAMC where the improvement is mostly found in high SNR channel. Near the Shannon capacity limit, which is achieved by CAMC, even slight values of gains are meaningful.

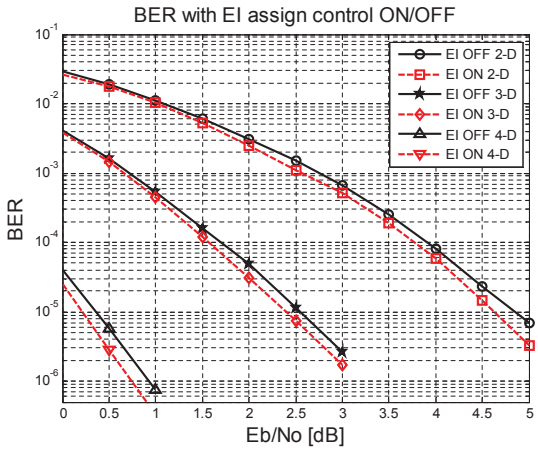


Fig. 9: Differentiated EI vs. plain decoding

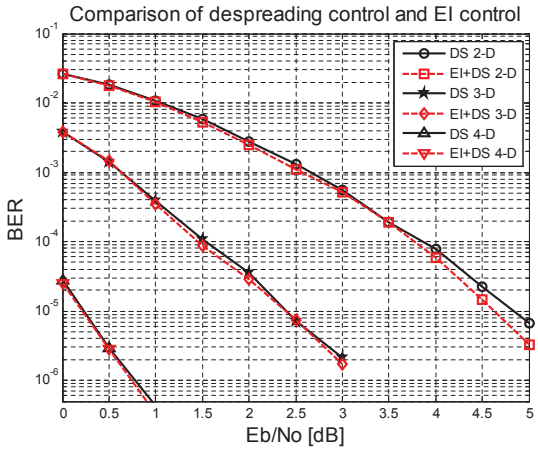


Fig. 10: Differentiated EI vs. despreading control

References

[1] P. Elias, "Error free coding", *IRE Trans. on Inform. Theory*, vol. IT-4, pp. 29-37, Sep. 1954

[2] D. Rankin and T. Gulliver, "Single parity check product codes," *IEEE Trans. on Comm.*, Vol.49, No.8, pp.1354-1362, Aug. 2001

[3] Y. Kim, "Recursive generation of constant amplitude multi-code S-CDMA signal," *IET Electronics Letters*, Vol. 39, No.25, pp.1782-1783, Dec. 2003

[4] I. Chih-Lin and R. Gitlin, "Multi-code CDMA wireless personal communications networks," in *IEEE Proceedings of ICC 1995*, pp.1060-1064, June, 1995

[5] T. Wada *et al.*, "A constant amplitude coding for orthogonal multi-code CDMA systems," *IEICE Trans. on Fund.*, vol. E80-A, pp. 2477-2484, Dec. 1997

[6] A. Shiozaki, M. Kishimoto and G. Maruoka, "Close-to-capacity performance of extended single parity check product codes," *IET Electronics Letters* Vol. 47 No. 1, Jan. 2011

[7] Y. Kim, "Constant amplitude multi-code CDMA with built-in single parity check product code," *IEEE Communications Letters*, Vol. 10, No.1, pp.4-6, Jan. 2006

[8] K. Lee, I. Park, B. Kim and Y. Kim, "Processing Gain in a Recursive Single Parity Check Product Code with Non-Gaussian Weight Distribution," *Proceedings of IEEE VTC 2009-Spring*, Barcelona, Spain, Apr. 2009

[9] I. Park, T. Kim and Y. Kim, "A Recursive Single Parity Check Product Code with Non-Gaussian Fixed Weight Distribution," *Proceedings of IEEE ATNAC 2008*, Adelaide, Australia, Dec. 2008

[10] G. Battail, "A conceptual framework for understanding turbo codes," *IEEE J. Selected Areas in Comm*., Vol.16, No.2, pp.245-254, Feb. 1998

[11] J. Hagenauer, E. Offer and L. Papke, "Iterative decoding of binary block and convolutional codes," *IEEE Trans. on Inform. Theory*, Vol.42, pp. 429-445, Mar. 1974

[12] S. Benedetto and E. Biglieri, *Principles of digital communications with wireless applications*, Kluwer Academic, Chap.10, 1999

[13] G. Caire, G. Taricco and G. Battail, "A Weight distribution and performance of the iterated product of single-parity-check codes," *Proceddings of IEEE Globecom 1994*, pp.206-211, Dec. 1994

[14] E. Biglieri and V. Volski, "Approximately Gaussian weight distribution of the iterated product of single-parity-check codes," *IEE Electronincs Letters*, vol.30, No.12, pp.923-924, June, 1994

[15] D. Yue and E. Yang, "Aymptotically Gaussian weight distribution and performance of multicomponent turbo block codes and product codes," *IEEE Trans. on Comm*, vol.52, No.5, pp.728-736, May, 2004

[16] S. Chon and Y. Kim, "Contribution of Processing Gain in Turbo Decoding of a Recursive Single Parity Check Product Code," *Information Journal* vol.13 no. 2, pp. 329-338, March, 2010, International Information Institute, Japan

[17] S. Lin and D. Costello, *Error control coding*, 2nd ed. Pearson Prentice Hall, 2004

Wonsun Bong received the B.S. in electrical engineering from Cheongju University, Korea, in 2009 and the M.S. degree in the electrical and computer engineering from the University of Seoul, Korea, in 2011. He is currently working toward the Ph.D. degree at the department of electrical and computer engineering in the University of Seoul, Korea.

His research interests are wireless communications, signal processing with an application to security surveillance systems from image sand videos.

Yong Cheol Kim (M'93) received the B.S. degree in electronics engineering from Seoul National University, Korea, in 1981 and the M.S. degree in electrical engineering from KAIST, Korea, in 1983 and the Ph.D. degree in electrical engineering from University of Southern California, Los Angeles, in 1993.

From 1993 to 1996, he was a team leader in Military Digital Communications Sector in LIG Nex1, Korea. In 1996, he joined the faculty at the Department of Electrical Engineering, University of Seoul, Korea. He is currently a Professor at the Department of Electrical and Computer Engineering. His research interests include mobile communications, image processing and computer vision.

Professor Kim is a member of Association for Computing Machinery, Institute of Electronics Engineers of Korea and The Korean Institute of Communications and Information Sciences.

Volume 5 Issue 1, Jan. 2016, ISSN: 2288-0003

ICACT-TACT JOURNAL

Global IT Research Institute

1713 Obelisk, 216 Seohyunno, Bundang-gu, Sungnam Kyunggi-do, Republic of Korea 13591

Business Licence Number : 220-82-07506, Contact: secretariat@icact.org Tel: +82-70-4146-4991