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

ICACT-TACT JOURNAL

Transactions on Advanced Communications Technology

Volume 2 Issue 3, May 2013, 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 2, Issue 3

Performance Investigation of Reduced Complexity Bit-Flipping using Variable Thresholds and Noise Perturbation

Julian Webber, Toshihiko Nishimura, Takeo Ohgane, Yasutaka Ogawa
Graduate School of Information Science and Technology, Hokkaido University, Sapporo 060-0814, Japan
jwebber@ieee.org, {nishim,ohgane,ogawa}@icl.hokudai.ac.jp

***Abstract*—The near Shannon capacity approaching low-density parity-check (LDPC) linear block codes are now in widespread use in modern systems including the long term evolution advanced (LTE-A) cellular, 802.11n Wi-Fi and DVB-S2 satellite communications standards. The decoders based on the iterative belief propagation algorithm provide near optimum performance but also have very high computational complexity. Therefore significant research has recently focused on reduced complexity architectures based on the group of so-called bit-flipping algorithms. In the basic bit-flipping algorithm the number of failed parity checks for each bit is computed and the bit with the maximum failed parity checks is inverted. Inverting bits above a certain threshold removes the complexity involved with a maximum-search and, adaptive thresholds on each bit can further reduce the computation overhead. The criterion for the threshold update affects the error and convergence performances. Here, we describe a low-complexity architecture that has two (or more) decoder branches each with a different threshold scaling factor and select the threshold and bits at each iteration from the branch with the lowest syndrome sum. We then investigate the effect of adding a random Uniform or Gaussian noise perturbation to the threshold in order to reduce the average iteration count further in order to provide the opportunity to escape from stuck decoding states.**

***Index Terms*—bit-flip algorithm, gradient-descent, reduced-complexity, noise perturbation, LDPC decoding.**

I. Introduction

Gallager first proposed LDPC codes in his 1963 PhD thesis [1]. However until their rediscovery in the mid-1990s [2] and coinciding with the availability of powerful low-cost digital signal processors, their use was largely forgotten. Near-optimum decoding performance can be achieved with the soft-decision belief propagation algorithm (BPA) that computes the marginal probabilities at the nodes on factor graphs [3]. The highest performance is achieved with long-length cycle-free codes and when the soft data at the decoder input is independent. However, the BPA also features a very high decoding complexity. At the other end of the complexity spectrum reside the bit-flipping algorithms (BFA) which are aimed at low-power portable applications. The average number of iterations in the BFA is higher than that of the BPA, but at each iteration a considerably smaller number of computations are required which can be computed in parallel, and the overall complexity is much less onerous.

In previous work we investigated the performance of a low complexity dual-scaling factor bit-flipping decoder with adaptive thresholds [4]. The addition of adding a simple noise perturbation to escape a stuck decoding state was proposed and initially investigated. In this paper we have extended the research to examine in more detail the effects of the noise perturbation on both the BER and iteration count. In particular, we investigate increasing the perturbation multiplication coefficient as well as the iteration delay size before which the perturbation is applied.

The paper is organized as follows: The belief propagation and bit-flipping algorithms are discussed in Section II. The adaptive bit-flipping technique together along with single and multiple-branch scaling factor decoders are introduced in Section III. The addition of a noise perturbation to escape a stuck-state is proposed and the effect of a noise coefficient multiplier and a sliding window counter concept are analysed in Section IV. Bit error and iteration count performance results are discussed in Section V and a conclusion is finally drawn in Section VI.

II. Decoding algorithms

The received sample vector is $\mathbf{y} = (y_1, y_2, ..., y_N)$ and the hard decoded bits are given by $\mathbf{x} \in \{+1, -1\}$. A sparse parity check matrix $\mathbf{H}$ is of size $M \times N$, where the number of check nodes is M and the number of bits is N [5]. The non-zero elements in column j are written as $M(j)$ and the non-zero elements in row i of $\mathbf{H}$ are $N(i)$. The syndrome associated with the m-th check node is denoted as s_m or equivalently the bipolar syndrome is written as $\prod_{j \in N(i)} x_j$. It is often instructive to graphically represent the parity check matrix by a bipartite Tanner graph [6] with N variable nodes (number of bits in the codeword) and M check nodes (number of parity bits) (Fig. 1).

Manuscript received June 27, 2012. The work was supported by the GCOE program 2009-2012, Hokkaido University, Japan.

J. Webber was with the Graduate School of Information Science and Technology, Hokkaido University, Kita-ku, Sapporo 060-0814, Japan. He is now with Wave Engineering Laboratory, Advanced Telecommunications Research Institute International (ATR), Kyoto, 619-0288, Japan. (Tel: +81-774951313; email: jwebber@ieee.org).

T. Nishimura is with the Graduate School of Information Science and Technology, Hokkaido University, Kita-ku, Sapporo, 060-0814, Japan. (Tel: +81-117067396; email: nishim@ist.hokudai.ac.jp).

T. Ohgane is with the Graduate School of Information Science and Technology, Hokkaido University, Kita-ku, Sapporo, 060-0814, Japan. (email: ohgane@ist.hokudai.ac.jp).

Y. Ogawa is with the Graduate School of Information Science and Technology, Hokkaido University, Kita-ku, Sapporo, 060-0814, Japan. (email: ogawa@ist.hokudai.ac.jp).

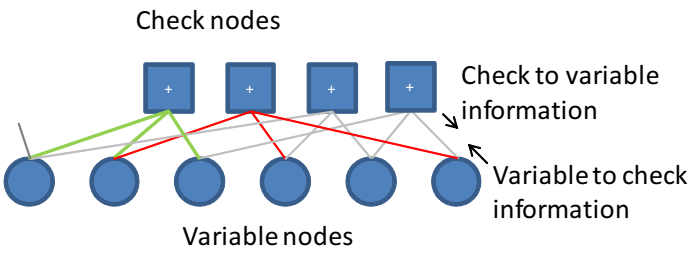


Fig. 1. LDPC decoding using Tanner graph representation.

A. Belief Propagation

The belief propagation algorithm is based on the concept of exchanging probabilities via 'messages' between check nodes and variable nodes which generally become more accurate with each iteration. The message passed from the check node to the variable node is the probability that the variable node has a certain value given all the messages passed to that check node in the preceding iteration from message nodes except the variable node itself. At the same time, the message passed from a variable node to a check node is the probabilty that it has a certain value given its observed value, and all values passed to it in the previous iteration from check nodes connected to it other than the check node itself [7]. Usually the probabilities are represented by log-likelihood ratios. The algorithm provides optimum performance but at the cost of very high computational complexity.

B. Bit-flipping algorithms

The sign of a single bit n with a maximum inversion function, E_n is inverted at each iteration in the basic BFA. A weighted BF (WBF) algorithm was proposed by Kou et al. [8] that incorporates a term related to the energy of the least reliable bit involved in each check. This however necessitates a search over the complete slot-length which contributes to an increased complexity and delay. The WBF is expressed as

$$E_n = \sum_{i \in M(n)} \{\min_{j \in N(i)} |y_j|\} \prod_{j \in N(i)} x_j, \tag{1}$$

where y_m^{min} is the least reliable message node associated with the m-th check.

Given that two message bits have contributed to a failed parity check, it is the message with the highest energy $|y_j|$ that is deemed most likely to be correct. In the reliability ratio algorithm [9] a normalization factor $R_{ij} = \beta \frac{|y_j|}{|y_i^{max}|}$ is calculated where $|y_i^{max}|$ is the highest soft magnitude of all message nodes associated with the m-th check (Eq. 2). The normalization improves the performance with respect to the WBF algorithm but the division operation in the initialization stage contributes to an increased complexity. An implementation-efficient reliability ratio WBF (IRRWBF) algorithm was subsequently proposed which lowered the complexity particularly when the iteration count was low and the code length was high [10].

$$E_n = \sum_{i \in M(n)} \prod_{j \in N(i)} / R_{ij}. \tag{2}$$

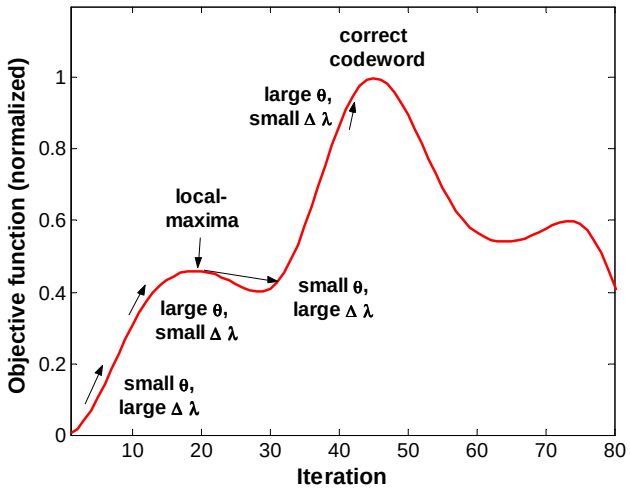


Fig. 2. Concept of the stuck decoding states. The step-size is reduced on reaching a local-maxima and increased on escaping it. Eventually the correct codeword is found.

where, $R_{ij} = \beta \frac{|y_j|}{|y_i^{max}|}$. In addition to the syndrome sum the gradient descent bit flipping (GDBF) algorithm [11] includes a correlation term between the initial received soft and hard decision which should be large and positive for a correctly estimated bit [11].

$$\Delta_n^{GD}(\mathbf{x}) = \sum_{i \in M(n)} \prod_{j \in N(i)} x_j + x_n y_n. \tag{3}$$

A bit is inverted if $\Delta_n^{GD}(\mathbf{x})$ is less than a global threshold. An objective function indicates the state of the algorithm at each iteration and is defined as

$$f^{GD}(\mathbf{x}) = \sum_{i \in M(n)} \prod_{j \in N(i)} x_j + \sum_{n=1}^{N} x_n y_n. \tag{4}$$

By monitoring the objective function it was proposed to switch from a large step-size (multiple bit-flips) to a small step-size if a stuck decoding state was detected. On such occasions a single small-descent of the objective function using a lower set threshold with a random component was shown experimentally to improve the performance. On escaping a local-maxima the step-size can then increase and eventually the correct codeword is found (Fig. 2).

III. Adaptive Flipping Thresholds

Recently adaptive thresholds for codes with a large number of checks per bit were investigated by Cho [12]. The benefit gained from inverting erroneous bits minus the loss from inverting correct bits was defined as the 'flipping-gain'. A known monotonically increasing number of errors was injected into a packet, and the threshold range p that produced a flipping-gain greater than one was calculated. It was observed that there was indeed an optimal threshold that resulted in a minimum number of iterations. It was conjectured that a similar analysis could be applied to parity check codes containing a smaller number of checks per bit, (e.g. as M=3), using non-integer

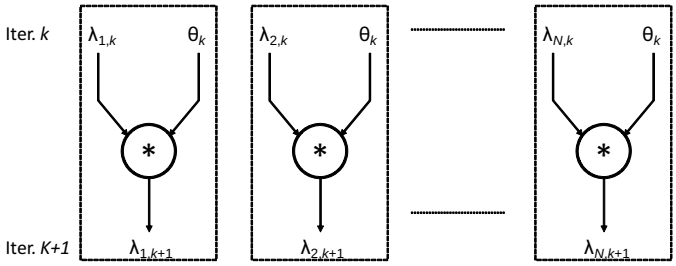


Fig. 3. The updated threshold $\lambda_{n,k+1}$ for bit n at iteration $k+1$ is computed by summing one or more shifted versions of the previous threshold $\lambda_{n,k}$.

thresholds (e.g. 1.33) and using a probabilistic strategy (e.g. thresholds 1.0, 1.0, 2.0).

In [13], an adaptive threshold λ_n was set on each bit. The sign of a bit was inverted if its inversion function was below the particular threshold (5), and otherwise it's threshold was lowered.

$$E_n(k) \leq \lambda_n(k). \tag{5}$$

The threshold update rule is written as (6)

$$\lambda_n(k+1) = \theta\ \lambda_n(k), \tag{6}$$

where k is the iteration number and θ is a threshold scaling value. With this technique the algorithm moves naturally from many to few bit-flips as the threshold is successively lowered. The computational complexity is lowered as each bit-processing operation (i.e. scaling / inversion) is computed independently of other bits. Furthermore, the physical hardware multiplier can be replaced a simple shift if the scale factor is chosen to be proportional to a power of two (Fig. 3).

A. Threshold scaling factor

The scaling factor θ in this paper is expressed as the sum of two fractional parts as :

$$\theta = 2^{-d_X} + 2^{-d_Y}, \tag{7}$$

where d_X and d_Y are integers. The range of values for θ that were investigated in this work along with the required shifts are listed in TABLE I. To generate the threshold update $\lambda_n(k+1) = 0.625\lambda_n(k)$ for example, the current threshold $\lambda_n(k)$ is shifted once 1 place (i.e. 0.5), once 3 places (i.e. 0.125), and the two partial products are summed. A small value of θ (e.g. 0.5) clearly equates to a large step-size and a large value of θ (e.g. 0.969) corresponds to a small step-size. By applying more shift addition operations any arbitrary scaling factor can be created, though for simplicity two additions were demonstrated in this work.

B. Single scaling-factor

In this paper two progressive edge growth (PEG) regular LDPC codes are investigated with their properties listed in Table II. PEG codes are created with the aim to maximize the girth (i.e. length of the shortest cycle) and therefore generally provide good performance [14]. The inversion function E_n recorded from a random trial at iteration 60 is plotted in Fig. 4. The bits whose inversion function E_n are above the threshold

TABLE I
THRESHOLD SCALING VALUES, θ AND PARTIAL COMPONENTS.

θ (decimal)	d_X	d_Y	θ_A	θ_B
0.5	1	0	1/2	0
0.625	1	3	1/2	+1/8
0.75	1	2	1/2	+1/4
0.875	0	3	1	-1/8
0.9375	0	4	1	-1/16
0.969	0	5	1	-1/32

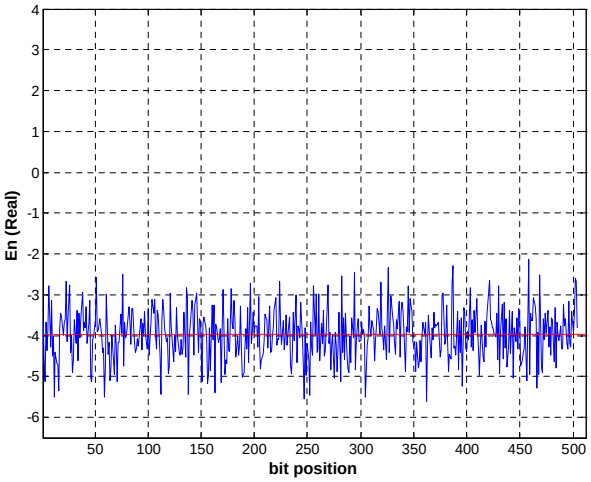


Fig. 4. Snapshot of the inversion function E_n of each bit at iteration 60 (θ=0.97). The mean value is indicated by the red horizontal line.

are flipped at each iteration. On flipping the value of the bits' inversion function will change and become more negative as its' probability of being correct increases.

C. Multiple scaling-factors / branches

In this work a novel dual-scaling switching algorithm (DSA) is proposed that jointly uses a fine and a coarse step-size decoder. The estimated hard bits from the decode-branch that have the minimum syndrome sum are passed to both decoder branches for the start of the next iteration (Fig. 5). The optional noise perturbation block is discussed further in the next section. The algorithm is sumarized as

---

STAGE 1- Initialize the inversion thresholds λ_n=λ_0, $\forall\ n$. Set State=1.
STAGE 2- Compute the inversion function E_n, for $m = 1, 2, ..., M$.

TABLE II
LDPC CODE PROPERTIES.

Code	Name [15]	Rows	Cols.	Col. deg.
1	PEGReg504x1008	504	1008	3
2	PEGReg252x504	252	504	3

STAGE 3- If $E_n(\theta_2) \geq \lambda_n$, Flip bit n.
Else λ_n=$\theta_2\lambda_{n-1}$. Optionally add noise perturbation to λ_n.
STAGE 4- If state=1, Repeat STAGE 3 for θ=θ_1.
STAGE 5- If $\Sigma s_m(\theta_1) \geq \Sigma s_m(\theta_2)$, Set state=2; λ_n=$\lambda_n(\theta_2)$,
$\forall$ n and **x**=**x**(θ_2); Deactivate branch no.1 to reduce energy consumption. Else λ_n=$\lambda_n(\theta_1)$, $\forall$ n and **x**=**x**(θ_1).
STAGE 6- Terminate if $\Sigma s_m = 0$ or maximum iterations reached.
Else Goto STAGE 2.

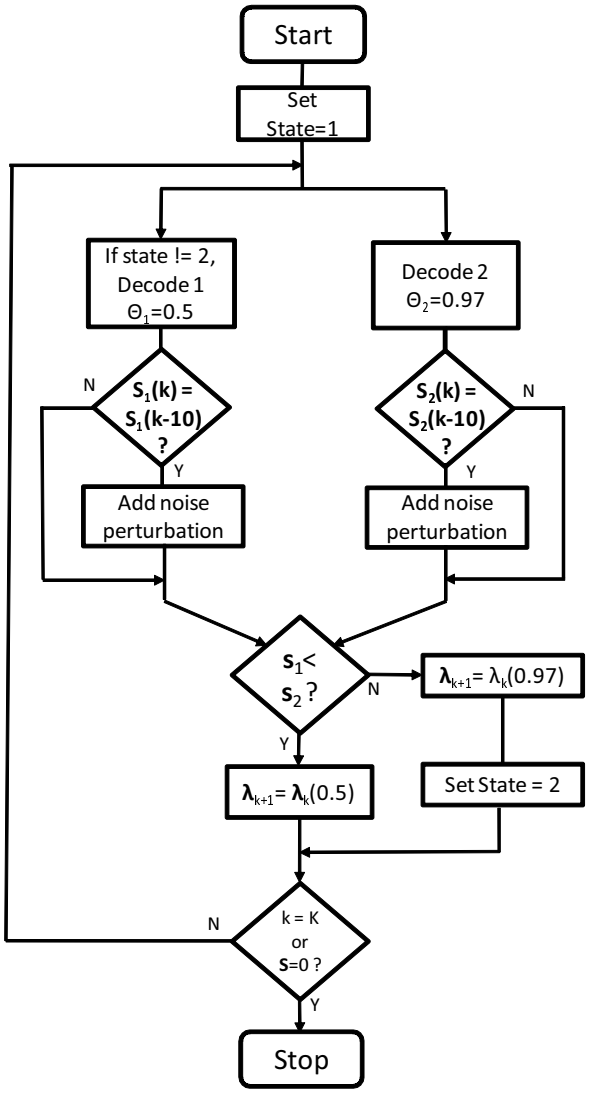


Fig. 5. Proposed dual scaling threshold algorithm flow chart showing optional noise perturbation unit.

The number of failed parity checks versus iteration number for the DSA is shown in Fig. 6. The solid line (marked '.') plots the syndrome sum when θ_1=0.5 and the solid line (marked '+') when θ_2=0.969. The number of failed checks decreased to zero by iteration 98 using the small step-size. However, by switching at iteration 11 from θ_1=0.5 to θ_2=0.969 when the syndrome sum was lower on that branch, the number of failed checks was rapidly reduced to zero by the 18th iteration.

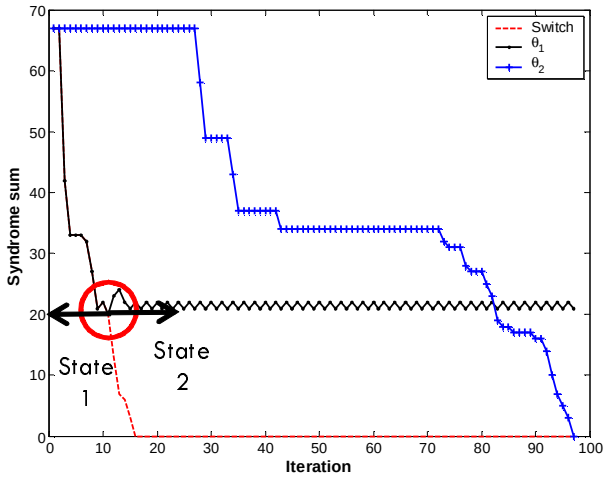


Fig. 6. Graph showing the syndrome sum versus iteration count. Single scaling factor θ_1=0.5 and θ_2=0.97. 'Switch' indicates the dual branch decoder.

Although the overall complexity is increased relative to a single branch decoder, this can be limited by deactivating the θ_1 branch once the θ_2 branch produces less errors. The optimum scaling factor is a function of the modulation, SNR, and particular code characteristic which makes calculating an optimum value very complex and an off-line statistical approach was made in [13] through experiment trials.

A further benefit of the dual-scaling detector proposed here is that both a real-time or off-line threshold calculation are avoided. A three-branch (three-scaling factors) detector was also evaluated but achieved only a small reduction in the iteration count with respect to the dual-scaling decoder and hence, due to the additional complexity, was not considered further in this work.

To reduced complexity an early-stopping algorithm was investigated in which processing was stopped if $f(k)$=$f(k-10)$ or $f(k)$=$f(k-11)$. It was necessary to apply the two conditions in case $f(k)$ oscillates between two values such as seen by the black zig-zag line in Fig. 6.

IV. Noise Perturbation

The local minima are a feature of the gradient descent algorithm where trapped search points occur but the estimated sequence does not correspond to the transmitted code-word. In such a situation we investigate the technique of inserting a small random perturbation to the threshold of each bit whenever the syndrome sum does not change over a sliding window of the previous W iterations. When this condition is satisfied a new random noise sample z_n is added to the current value of λ_n as shown by

$$\lambda_{n+1} = \lambda_n + Kz_n, \tag{8}$$

where z_n is a random Uniform or Gaussian sample for bit n and K is a noise perturbation coefficient typically between 1.2 and 2.4 for Uniform noise and 0.7 to 1.3 for Gaussian noise.

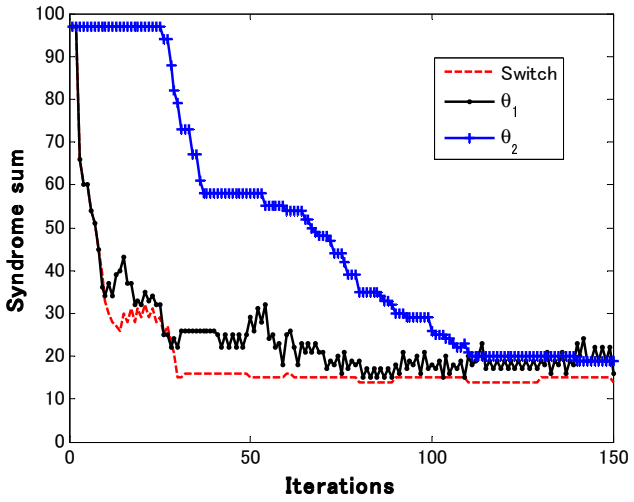


Fig. 7. Graph showing the syndrome sum against iteration with noise perturbation at iterations: 50, 60, ... 150.

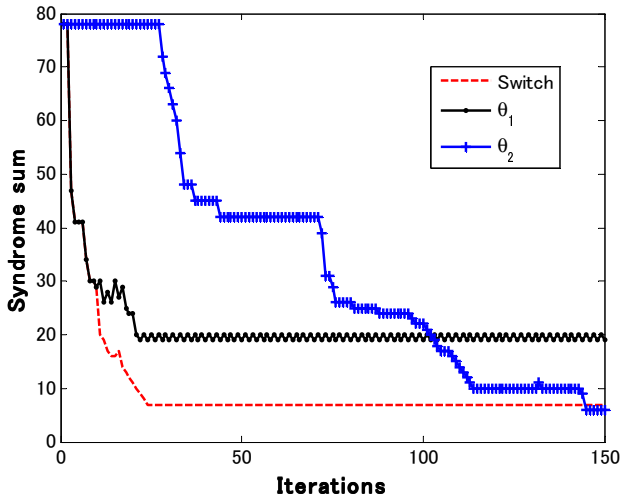


Fig. 8. Syndrome sum for another trial without added random perturbation.

A. Temporal study

We first investigate through experiment the instantaneous effect on the syndrome sum of adding a noise perturbation. In Fig. 7 Uniform noise was injected at iteration 50 and subsequently at intervals of 10 iterations thereafter. We observe a small but noticeable lowering in the number of syndrome errors at iterations 50, 80 and 110. Due to the random nature of the noise perturbation, there can be occasions when there is no improvement such as at iteration 100 for example.

In the absence of a random perturbation, the syndrome sum recorded during another random decoding trial, is plotted in Fig. 8. Next, using the same received signal sequence **y** for fairness, the syndrome sum is computed in a trial with perturbation permitted (Fig. 9). The benefit of the the random perturbation can clearly be seen where a stuck decoding state was successfully exited and the syndrome sum reduced to zero by iteration 66. On adding the perturbation, the particular bits whose current inversion function is nearest to the threshold are most likely to be inverted and the noise coefficient K controls the number of additional bits that have the potential to be inverted. Note that a program 'break' was used within the iteration loop and in parallel the three independent decoders were ran generating the red, blue, black curves. Once the syndrome sum was zero on the red dual-threshold detector, the loop was exited and so the trajectories for the blue and black curves are not plotted beyond iteration 66, even though they would continue in normal operation.

In the following two subsections we study in more detail the effects of the noise coefficient multiplier K and the sliding window counter size W. In particular, we aim to find optimum values through experimentation across a range of practical signal to noise ratios.

B. Noise coefficient

A very low noise coefficient K would result in applying no perturbation and too high a value would cause the flipping threshold to be adjusted too quickly with a similar effect to that of a large step-size θ. Thus an optimum coefficient range would be expected and an experiment was set-up to find the range. The number of iterations versus the noise coefficient were recorded across the SNR range from 2-4 dB. It is shown in Fig.10 that in the transition region the optimum value is about 1.6 for both Code 1 (top) and Code 2 (bottom).

A comparison between Gaussian and Uniform noise perturbations is shown in Fig.11. It was found that in terms of the number of iterations, the same performance can be achieved when K was set to 1.0 when applying a Gaussian source and 1.5 for Uniform sources. This result was valid for both LDPC codes Code 1 and Code 2.

C. Sliding window counter size

The noise perturbation is only required when a stuck decoding state is reached. This can be detected when there is

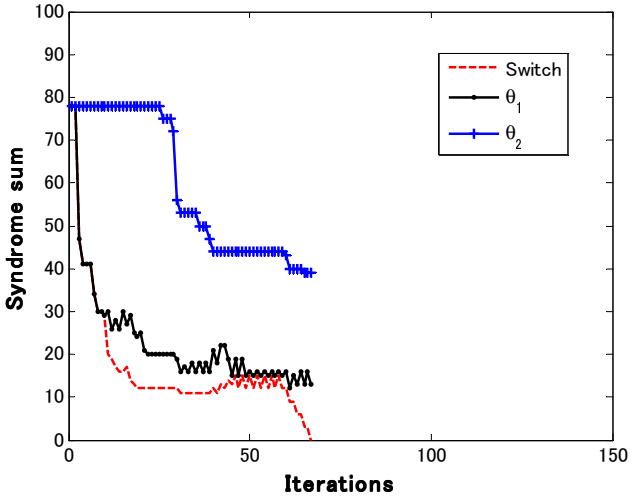


Fig. 9. Plot showing syndrome sum with added perturbation. This trial used the exact same received soft data, **y** as in Fig. 8 for fairness.

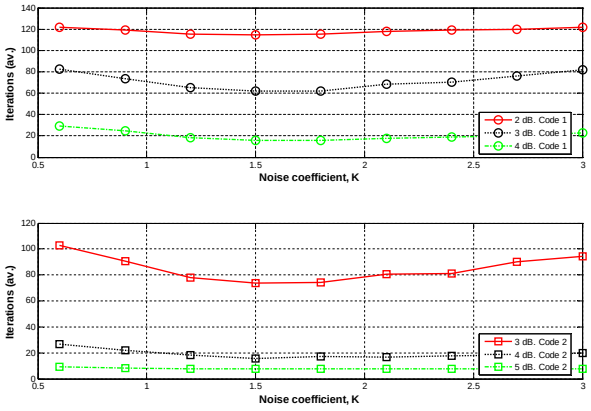


Fig. 10. Effect of the noise coefficient K on iteration count for Code 1 (top) and Code 2 (bottom).

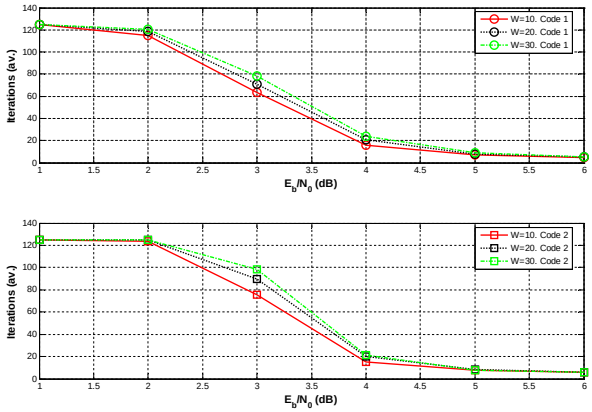


Fig. 12. Effect of sliding window size W on iteration count for Code 1 (top) and Code 2 (bottom).

no improvement in the syndrome sum despite the threshold being lowered over a number of iterations. In such a situation a counter is incremented at each iteration and otherwise reset to zero if the threshold was successfully lowered. If the counter reaches a set number, referred to as the sliding window counter size W then a noise perturbation is added.

If a perturbation is added too soon the benefit of a small step-size is not realized as there is little opportunity to slowly lower the threshold. On the other hand, if the perturbation is added too late then the algorithm takes an unnecessary long time and wasteful iterations are required increasing the power consumption. It was therefore thought that an optimum range for the sliding window counter would exist.

In this experiment the counter is varied between 10 and 30 iterations and the maximum number of iterations was set at 125. The resulting number of iterations until convergence (or algorithm termination) is shown in Fig.12 for Code 1 (top) and for Code 2 (bottom). The effect of the sliding window length W on the average number of iterations as the SNR increases is shown in Fig.13 Code 1 (top) and Code 2 (bottom).

The effect of the noise coefficient K on the average number of iterations for various SNR is shown for Code 1 in Fig.14 for (top) Gaussian and (bottom) Uniform perturbation noise sources. The optimum value is observed when the BER gradient is at its largest value. For the case of Code 1 we can clearly see a minimum number of iterations exist at between 2 and 4 dB SNR for both Gaussian and Uniform noise sources. In low SNR or as the algorithm approaches convergence there is clearly no benefit in adding the perturbation. Further work could investigate the optimum value for each threshold factors.

V. Error Performances

The error performances of the various bit flipping algorithms were evaluated in an AWGN channel through simulation. The maximum number of iterations was set at 150 with BPSK modulation. In the BER evaluation the sliding window counter size, W was set at 10 iterations. Although the IRRWBF algorithm performed the best it also has the highest complexity. The BER depends on the particular value of θ when the

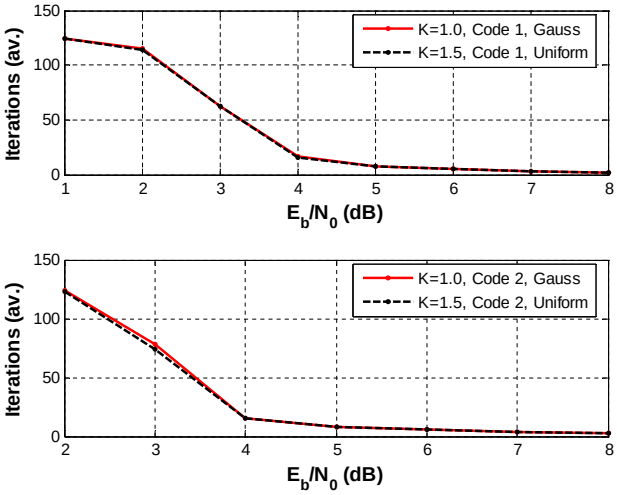


Fig. 11. Comparison of Gaussian and Uniform noise perturbations for (top) Code 1 and (bottom) Code 2.

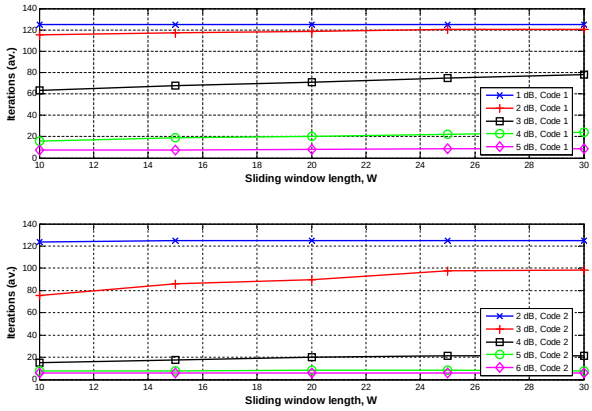


Fig. 13. Effect of sliding window length on average number of iterations (top) Code 1 and (bottom) Code 2.

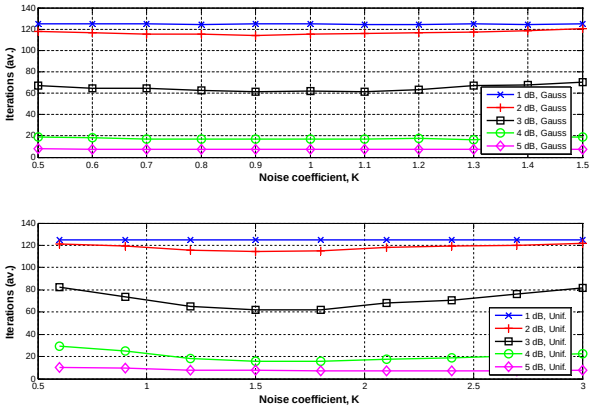


Fig. 14. Effect of Noise coefficient K on average number of iterations for various SNR (top) Gaussian and (bottom) Uniform noise using Code 1.

number of iterations is limited as shown in Fig. 15. When θ=0.5, more bits are inverted on average per iteration and the overall performance is worse than when θ=0.97. The proposed DSA with θ=0.625/0.97 performed as well as well as the one with a single θ=0.97 but its advantage is the reduced iteration count as seen in Fig. 16 where the average number required is lowered by 41% from 66 to 39 at 4 dB SNR. The number of iterations of the 'Dual early-stop' algorithm was similarly reduced to 17 at an E_b/N_0 of 4 dB.

The performance of the random perturbation decoders are denoted by '+ perturb.'. At the BER of 10^{-3}, an improvement of 0.5 dB was obtained for the dual scaling decoder with perturbation (Fig. 17). As the fine step-size decoder slowly converges to the desired solution there is only a small improvement in BER. However, at 3 dB E_b/N_0 the number of iterations was reduced on average by (16.4, 9.2, 2.0) for the (dual-scale, θ=0.63 and θ=0.97) decoders respectively (Fig.18). The corresponding savings were (11.0, 10.1, 2.6) iterations at4 dB E_b/N_0.

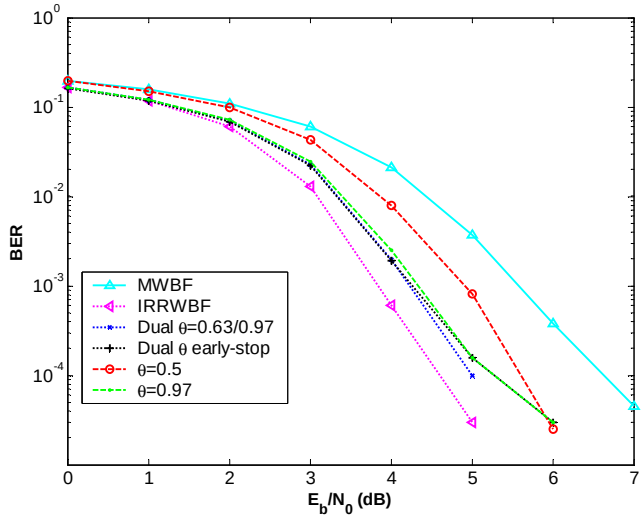


Fig. 15. BER versus E_b/N_0 (dB) with LDPC Code 1 in AWGN.

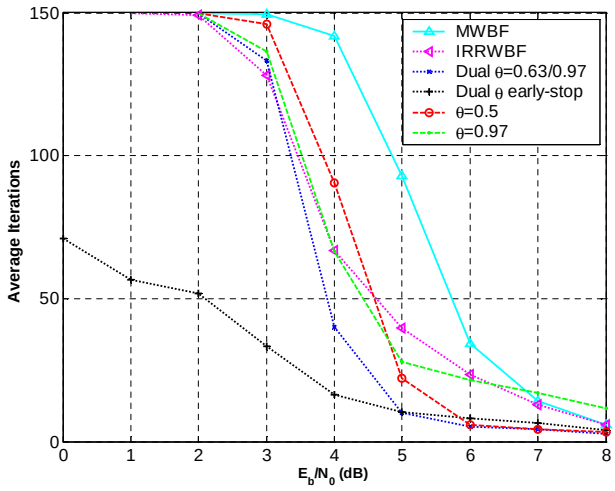


Fig. 16. Average number of iteration versus E_b/N_0 (dB) for Code 1.

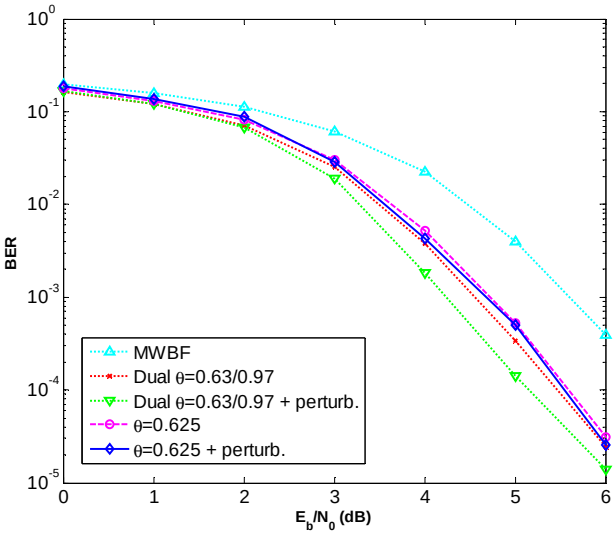


Fig. 17. BER versus E_b/N_0 (dB) for LDPC Code 2 with noise perturbation in AWGN.

VI. Conclusion

The error and convergence rates of adaptive threshold bit-flipping algorithms have been studied. A dual-scaling architecture was proposed that applies the hard bit estimates and thresholds at each iteration from either the fine or coarse step-size decode branch depending on its respective syndrome sum. The dual-scale architecture with θ=0.63/0.97 performed as well as that of the single step-size θ=0.97 decoder but the average number of iterations was reduced by 41% at 4 dB E_b/N_0. By adding a small noise perturbation the average iteration count of the dual-scale detector could further be reduced by 11 cycles at 4 dB E_b/N_0. An optimum value for the perturbation coefficient was found to be 1.6 for Uniform noise and applied after a delay of 20 iterations. Further work could investigate the optimum value as a function of the threshold step-size.

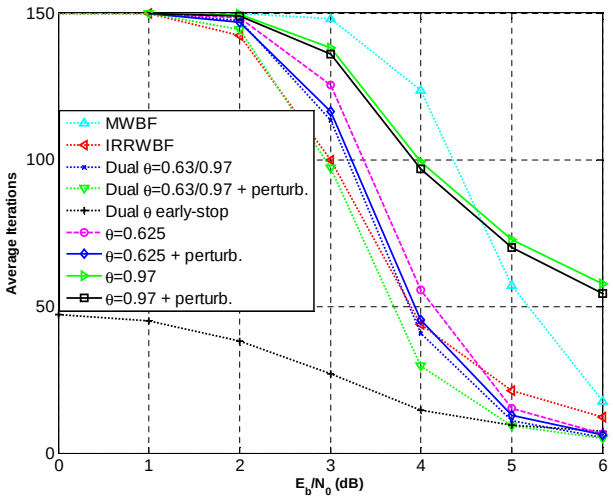


Fig. 18. Average number of iteration versus E_b/N_0 (dB) for Code 2 with perturbation.

REFERENCES

[1] R. Gallager, "Low Density Parity Check Codes (LDPC)," *Mass. Inst. Tech. Press*, Phd. Thesis, 1963.

[2] D. MacKay and R. Neal, 'Good error-correcting codes based on very sparse matrices," *Crypt. and Coding 5th IMA conf.*, Jul. 1995.

[3] W. Chung, and J. Cruz, "An improved belief-propagation decoder for LDPC-coded partial-response channels," *IEEE Trans. Magnetics*, vol. 46, no. 7, pp. 2639-2648, Jul. 2010.

[4] J. Webber, T. Nishimura, T. Ohgane, and Y. Ogawa, "A study on adaptive thresholds for reduced complexity bit-flip decoding," *International Conference on Advanced Communications Technology (ICACT'12)*, Phoenix Park, Pyeongchang, Korea, Feb. 2012.

[5] D. J. MacKay, "Information thoery, inference, and learning algorithms," *Cambridge University Press*, 2003.

[6] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol. 27, no. 5, pp. 533-547, Sep. 1981.

[7] M. Luby, M. Mitzenmacher, A. Shokrollahi, and D. Spielman, "Analysis of low density codes and improved designs using regular graphs," *IEEE Trans. on Inform. Theory*, vol. 47, pp. 585-598, 2001.

[8] Y. Kou, S. Lin, and M. Fossorier, "Low-density parity-check codes based on finite geometries: a rediscovery and new results," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 2711-2736, Nov. 2001.

[9] F. Guo and L. Hanzo, "Reliability ratio based weighted bit-flipping decoding for LDPC codes," *IEE Electron. Lett.*, vol. 40, no. 21, pp. 1356-1358, Oct. 2004.

[10] C. H. Lee and W. Wolf "Implementation-efficient reliability ratio based weighted bit-flipping decoding for LDPC codes," *IEE Electronics Lett.* vol. 41, no. 13, pp. 755-757, Jun. 2005.

[11] T. Wadayama, K. Nakamura, M. Yagita, Y. Funahashi, S. Usami, and I. Takumi, "Gradient descent bit-flipping algorithms for decoding LDPC codes," *International Symposium on Information Theory and its Applications (ISITA'08).*, Auckland, New Zealand, Dec. 2008.

[12] J. Cho and W. Sung, "Adaptive threshold technique for bit-flipping decoding of low-density parity-check codes," *IEEE Comm. Letts.*, pp. 857-859, col. 14, no. 9, Sep. 2010.

[13] M. Ismail, I. Ahmed, J. Coon, S. Armour, T. Kocak, and J.P. McGeehan, "Low latency low power bit flipping algorithms for LDPC decoding," *IEEE PIMRC10*, Sep. 2010.

[14] E. Psota, and L. Perez, "Iterative construction of regular LDPC codes from independent tree-based minimum distance bounds," *IEEE Comm. Letts.*, vol. 15, no. 3, Mar. 2011.

[15] D. MacKay, "Encyclopedia of sparse graph codes [Online]," *URL: http://www.inference.phy.cam.ac.uk/mackay/codes/data.html*, Accessed Feb. 2011.

Julian WEBBER Julian WEBBER received the M.Eng. and Ph.D. degrees from the University of Bristol, UK in 1996 and 2004 respectively. From 1996 to 1998, he was with Texas Instruments working on ASIC and DSP. From 2001-07 he was a Research Fellow at Bristol University working on real-time MIMO-OFDM test beds, and from 2007-2012 he was a Research Fellow with Hokkaido University working on MIMO signal processing. He currently is a researcher at ATR, Kyoto, Japan working on spectrally efficient modulation techniques and frequency recovery for satellite communications. His current research interests include synchronization, MIMO signal processing and coding. Dr Webber is a member of the IEEE and IEICE.

Toshihiko NISHIMURA Toshihiko NISHIMURA received the B.S. and M.S. degrees in physics and Ph.D. degree in electronics engineering from Hokkaido University, Sapporo, Japan, in 1992, 1994, and 1997, respectively. In 1998, he joined the Graduate School of Engineering (reorganized to Graduate School of Information Science and Technology at present) at Hokkaido University, where he is currently an Assistant Professor of the Graduate School of Information Science and Technology. His current research interests are in MIMO systems using smart antenna techniques. Dr. Nishimura received the Young Researchers' Award of IEICE Japan in 2000, and the Best Paper Award from IEICE Japan in 2007. Dr. Nishimura is a member of the IEEE.

Takeo OHGANE Takeo OHGANE received the B.E., M.E., and Ph.D. degrees in electronics engineering from Hokkaido University, Sapporo, Japan, in 1984, 1986, and 1994, respectively. From 1986 to 1992, he was with Communications Research Laboratory, Ministry of Posts and Telecommunications. From 1992 to 1995, he was on assignment at ATR Optical and Radio Communications Research Laboratory. Since 1995, he has been with Hokkaido University, where he is an Associate Professor. During 2005-2006, he was at Centre for Communications Research, University of Bristol, U.K., as a Visiting Fellow. His interests are in MIMO signal processing for wireless communications. Dr. Ohgane received the IEEE AP-S Tokyo Chapter Young Engineer Award in 1993, the Young Researchers' Award of IEICE Japan in 1990, and the Best Paper Award from IEICE Japan in 2007. Dr. Ohgane is a member of the IEEE.

Yasutaka OGAWA Yasutaka OGAWA received the B.E., M.E. and Ph.D. degrees from Hokkaido University, Sapporo, Japan, in 1973, 1975, and 1978, respectively. Since 1979, he has been with Hokkaido University, where he is currently a Professor of the Graduate School of Information Science and Technology. During 1992-1993, he was with ElectroScience Laboratory, the Ohio State University, U.S.A., as a Visiting Scholar, on leave from Hokkaido University. His interests are in adaptive antennas, mobile communications, super-resolution techniques, and MIMO systems. Dr. Ogawa received the Young Researchers' Award of IEICE Japan in 1982, and the Best Paper Award from IEICE Japan in 2007. Dr. Ogawa is a member of the IEEE.

Classification of N-Screen Services, Scenarios and its Standardization

Changwoo Yoon, Hyunwoo Lee, Won Ryu

*Electronics & Telecommunications Research Institute, Daejeon, Korea

cwyoon@etri.re.kr, hwlee@etri.re.kr, wlyu@etri.re.kr

***Abstract*—By the advent of IPTV and smart TV, the broadcasting is transmitted using Internet. Bi-directional programs are appeared on broadcasting services. The convergence service combining with communication, information and web service are appeared too.**

N-Screen service is a killer service of smart TV. It uses several terminals, either fixed or mobile, to provide bi-directional, convergence and personal services with broadcasting service.

N-Screen service can be classified into three categories: first, OSMU (One Source Multi Use) case, providing same contents to terminals having different capabilities such as screen size, CPU speed, memory, codec, network speed, etc. Second case is a vertical handover, continuous watching of content using different terminal. Third case is a collaborative service among multiple terminals. For example, a customer is watching soap opera using TV, while watching a specific scene related information or advertisement using his PAD or smart phone.

In ITU-T SG13, the Y.sof (Service Scenario over FMC) was standardized. It defined detailed overall service scenarios using feature extraction of seamless mobile convergence service on several networks such as WiFi, 3G, WiMAX/WiBro. This standard extracts key features of five key elements: person, terminal, network, content, and service. Then, it analyzes relationships among key elements and suggests overall service scenario model.

The service scenario model can be easily adopted on describing N-Screen service scenario because Y.sof handles scenario cases among several fixed or mobile terminals.

In this paper, I will introduce Y.sof and classification of N-Screen service scenarios described using the standard. Also I will refer the standardization issues of N-Screen and its technologies.

***Keywords*— IPTV, Smart TV, N-Screen, OSMU, FMC**

I. INTRODUCTION

Recently, the environment where consumers use multiple devices according to time and place is being created. In this situation, multi-device platforms are gaining attention for enabling users to enjoy the same content or services seamlessly, irrespective of which device / medium is used. N Screen which is recently getting attention falls into the broader concept of Multi-Device Service. N Screen is about enabling the user to use multiple devices, which means, it should be made up of integrated platforms for multi-devices. The core element of N Screen Service is a platform that mediates the use of content or services on multiple devices. [1,2]

N Screen Services and Multi-Device Services are often used in the same meaning. Technically speaking, however, Multi-Device Service is a broader concept that encompasses N Screen Service. Multi-Device Service is, literally, to provide the same content or services on a variety of devices. Along with the evolution of the ICT environment, Multi-Device Services have been evolving as well.

ITU-T Y.2720 Sup.14 describes overall scenario model for various services over FMC. In the overall scenario model, shown in Fig. 1, the red dotted box describes N- screen service scenario situation of an end user using his/her terminal devices while the features of service are operated on several devices synchronously. [3,4,5] An example is the case of displaying the same content on different types of terminals converting content quality. Another scenario is of an end user using his/her terminal devices while the unit feature of converged service is operated on separate devices synchronously. Examples are the case of displaying VOD on TV+STB, starting VOD using EPG displayed on mobile phone, and displaying VOD related information on a Notebook.

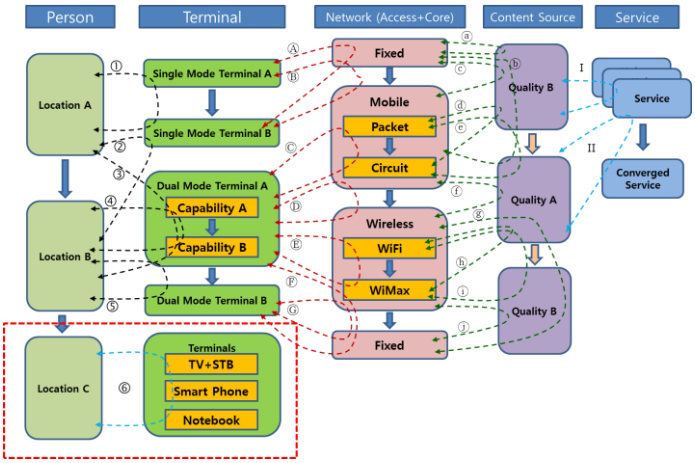


Figure 1. N-Screen part on Overall scenario model over FMC

Manuscript received September 15, 2012. This work was supported in part by the EU ITEA-2 project with Grant No.10028 "Web-of-Objects" (WoO) funded by MKE and supervised by KIAT.

Changwoo Yoon is Principle Researcher with the Electronics & Telecommunications Research Institute, Daejeon, Korea (Phone: +82-42-860-6543; fax: +82-42-860-5611; e-mail: cwyoon@etri.re.kr).

Hyunwoo Lee is Team Leader with the Electronics & Telecommunications Research Institute, Daejeon, Korea (Phone: +82-42-860-6526; fax: +82-42-861-1342; e-mail: hwlee@etri.re.kr).

Won Ryu is Director with the Electronics & Telecommunications Research Institute, Daejeon, Korea (Phone: +82-42-860-6290; fax: +82-42-861-1342; e-mail: wlyu@etri.re.kr).

In this paper, we describe various kinds of N-screen service scenarios based on overall scenario model over FMC.

II. General Description of N-Screen Services

By the advent of IPTV and smart TV, the broadcasting through Internet is generalized. The bi-directional service is introduced on broadcasting by using Internet's bi-directional transmission characteristic. The convergence services combined with telecommunication, information, web and personalized broadcasting services are appeared. Major feature of smart TV is intelligence such as smart search, extraction and UI technology providing customer targeted information on the limited size of TV screen. N-Screen service is a killer service of smart TV providing various kinds of bi-directional, converged, personalized and intelligent contents and services to multiple fixed or mobile devices

We can classify N-screen service scenarios as three cases. First case is sharing same content or service on more than one screen among multiple kinds of screen; For example, it is a service on which an end user can watch the same content on various terminals such as TVs with Setop, PCs, notebooks, PMPs, or smart phones.

Figure 2. Classification Case I of N-Screen Service: OSMU

Another example of OSMU is migration of service among terminals. Figure 3 shows an example of OSMU of service. User can use smart TV application showing maps of specific location, while the user want to send an e-mail to her/his friend. Because it is difficult to write an e-mail on smart TV, the user migrate the e-mail window to his smartphone.

Figure 3. Classification Case I of N-Screen Service: OSMU of service

Second case is consuming same contents on several devices continuously. . It is considered as one of the representative service supporting service mobility among multiple kinds of screens.

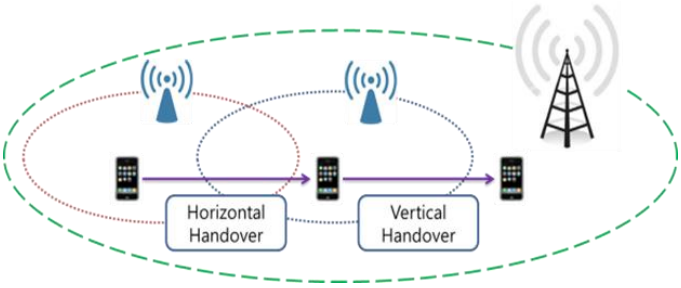


Figure 4. Classification Case II of N-Screen Service: Handover

Third case is providing collaborating service among multiple devices. The service provides to customer is consist of different shape of services that is operated on separate screen. For example, PAD operates as EPG terminal for an IPTV. A customer can select a program he wants to see and the selected program is displayed on TV screen with synchronous manner.

Figure 5. Classification Case I of N-Screen Service: Collaboration

More advanced example of case III collaboration is ASMD (Adaptive Source Multi-Device) shown on figure 6. In ASMD service scenario, user can divide and combine services making convergence services. In figure 6, three persons are watching TV while they are using their own handheld device such as mobile phone and pad. While watching music program, each person are using music program related services. Person A watches different angle scenes. Person B watches celebrity news about the singer who is showed in TV screen. Person C watches album about the singer. By a touch of each person's handheld device, the services shown in each person's device transmitted to big TV screen and displayed in combined mode.

This ASMD type of N-Screen service will bring new watching pattern on smart TV by providing collaborating TV services with mobile devices. There will bring new business

opportunities by providing convergence services combining broadcasting, telecommunications and web service freely.

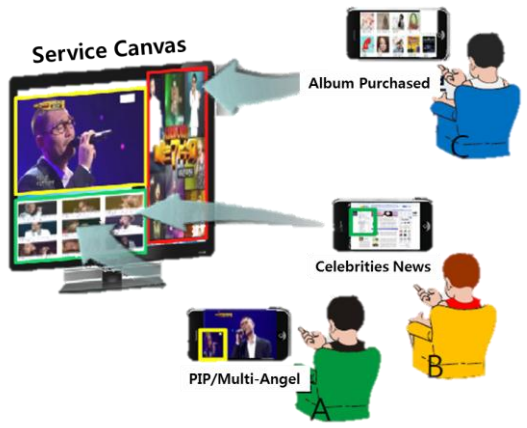


Figure 6. Classification Case III of N-Screen Service: ASMD

III. Y.SOF: SERVICE SCENARIOS OVER FMC

One of the essential benefits of the NGN is a supporting of convergences such as a fixed mobile convergence (called FMC), telecom-broadcasting converged service like IPTV. ITU-T produced several Recommendations on FMC and IPTV, especially in the ITU-T Y.2000 series of Recommendations. ITU-T is developing more detailed aspects of supporting the FMC, taking consideration of the fact that various services are waiting to utilize the FMC as their service infrastructure, which will extend their service coverage as well as give more benefits to the user.

This Supplement to the ITU-T Y.2000-series Recommendations on the scope of service scenarios over the FMC provides service scenarios which are used over FMC. This Supplement uses the features of involved key elements of FMC to guide how services can be provided in detail. This Supplement also introduces overall configurations and scenario models to identify service scenarios over the FMC.

There are five key elements to define: Person, Terminal, Network, Contents and Service.

- Person (End User): This is a key subject for consuming services over FMC. It is characterized by the location, that is, "Same Location" or "Change Location"
- Terminal: This is a key device supporting services for the person. The person can own multiple terminal devices either fixed, mobile or Wireless. The terminal can be classified into two categories (Single mode and Multi mode) by the number of network connection interfaces. As single mode terminal provides a single connection to the network that is either fixed or mobile or wireless. A multi-mode terminal provides several ways of connection to the networks. In this supplement, we use a dual mode terminal as an example of a multi mode terminal. The dual mode terminal provides dual connections to the network that are either fixed, mobile or wireless.
- Networks: This is a key part supporting mobility and FMC of the terminal. The network is composed of an access network and a core network. We can classify the access network by its technology basis, whether it is "Fixed", "Mobile" or "Wireless".
- Contents: This is a key part that is presented by media files and media processing. The contents form services for the end user.
- Service: This is a key part for the end users providing a set of functionalities enabled by a service provider.

I will describe the features of key element bellows.

A. *Behavioural aspect of Person*

A person will use terminal device either keeping the same location or changing location. Changing the location causes supporting of mobility if the person wishes to keep current services. So we can determine the features of the person's key element by the location, whether it is, "Same location" or "Change location".

Figure 7. Features of Person

B. *Capability aspect of Terminal*

The terminal is operated following the behaviour of the person while trying to keep the service continuity. As a result of following person's behaviour, it is decided whether the capability of the terminal should be changed or not.

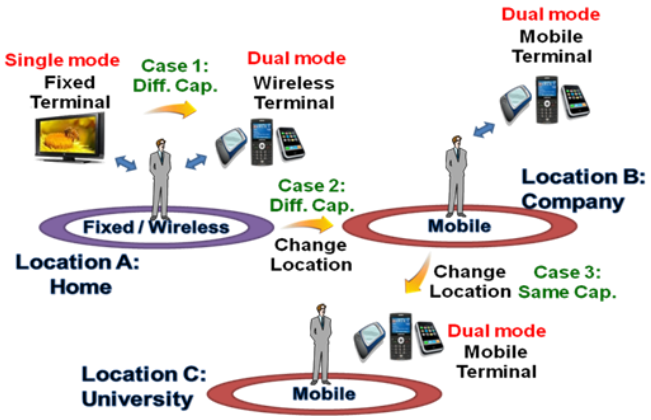


Figure 8. Example cases of Person's behaviour of terminal usage

For example, figure 8 shows three cases of the terminal capability change or no-change according to the behaviour of the person.

First case shows the situation of the person watching high quality IPTV at home. He has to go to his company and he wants to watch the program seamlessly using his mobile phone. In this case the capability of the terminal is changed: from single mode, fixed network TV to dual mode, wireless network mobile phone.

Second case shows the situation of the person moving his location from A (home, wireless network area) to B (company,

mobile network area), while continuing the service. In this case the capability of the terminal is changed: network mode change of mobile phone from wireless network to mobile network.

Third case shows the situation of the person moving his location from B (company, mobile network area) to C (university, mobile network area), while continuing the service. In this case, there is no terminal capability change because it is merely a change of mobile base station.

Therefore we can determine the features of the terminal key element by the capability, whether it is, the "Same capability" or "Different capability".

Figure 9. Features of Terminal

C. Capability aspect of Network

The features of access network needs to be considered by the technology basis: Fixed, Mobile and Wireless. For those networks, the network capability may vary from one network to another. For example, a fixed broadband network is able to support much higher bandwidth than cellular wireless.

Core network is a delivery part managing overall traffic transferring process such as re-routing, traffic congestion and failure in the routing path etc. The core network's capability should be impacted by end user behaviour such as changing access networks. Therefore, core network features can be determined by "Same Capability" and "Different Capability".

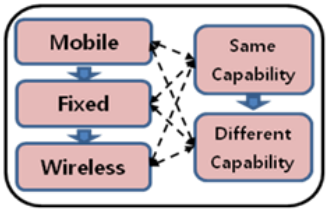


Figure 10. Features of Network

D. Quality aspect of Contents

We can determine features of the content by its quality such as trans-coding QoS parameters, such as encoding codec, resolution (CIF, SD, HD) or frame rate

- Same quality: This is the case in which the source of contents should maintain the quality. From the contents point of view, there is no need to change trans-coding QoS parameters such as codec, resolution or frame rate.
- Different quality: This is the case in which the source of contents should change the quality. From the contents point of view, there is a need to change the trans-coding QoS parameters such as codec, resolution or frame rate.

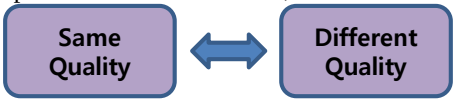


Figure 11. Features of Contents

There are two cases for the Different quality: upgrade or downgrade.

Example case for the upgrade is a handover from a mobile terminal to a TV requiring high quality video and network. The change of quality is required such as codec and resolution (CIF to HD).

Example case for the downgrade is a handover from a TV to a mobile terminal. The change of quality is required such as codec and resolution (HD to CIF).

E. Integration aspect of Service

Service feature can be classified by its integration, whether it is, "service" or "Converged service". A converged service can be composed of several services.

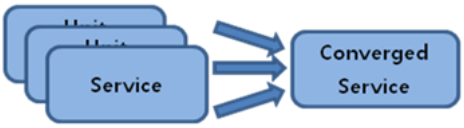


Figure 12. Features of Service

F. Overall FMC configuration model

This clause shows an overall high level configuration model over FMC. This is determined by considering the features of FMC key elements, and their characteristics.

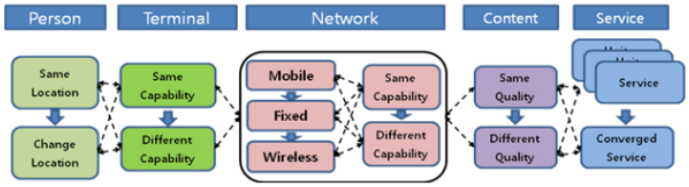


Figure 13. Overall configuration model using features of key elements

In this figure, a person will use his/her terminal device either maintaining the same location or changing the location. Changing the location demands support of mobility if the person wishes to keep services while moving.

Then, a terminal device (either single mode or multiple modes) is operated to follow the behaviour of the person while keeping the network connection as much as possible. As a result of following user behaviour (handover to other terminal or change of network connection), the capability of the terminal function should be changed.

In the case of access networks, it should be continuously changed according to the end user's behaviour such as moving or changing the connection among fixed, mobile and wireless access networks. One important thing here is that changing the access network causes change in the connecting capability like bandwidth, or overall traffic management process.

Sources of contents are influenced by the mobility, because the result of mobility either caused at terminal device or access network requires changing the QoS (downgrading or upgrading). Therefore this can be characterized by the quality: "Same Quality" or "Different Quality."

Service providers provide several types of service such as content on demand, real-time broadcasting IPTV service, IMS based caller ID service, information display etc. Service

providers can provide converged services by combining services such as displaying caller-ID, content related information while the customer is watching VOD.

Using overall FMC configuration model, we can derive overall scenario model over FMC shown in Figure 1.

In figure 1, scenario number 6 shows N-screen scenario case. This is a scenario of an end user using his/her terminal devices while the features of service are operated on several devices synchronously. An example is the case of displaying the same content on different types of terminals converting content quality. Another scenario is of an end user using his/her terminal devices while the unit feature of converged service is operated on separate devices synchronously. Examples are the case of displaying VOD on TV+STB, starting VOD using EPG displayed on mobile phone, and displaying VOD related information on a Notebook.

IV. N-SCREEN SERVICE SCENARIO: CASE I

Case I N-screen is a service on which an end user can watch the same content on various terminals such as TVs with Setop, PCs, notebooks, PMPs, or smart phones. Each screen of terminals is used in a cooperative and synchronous manner.

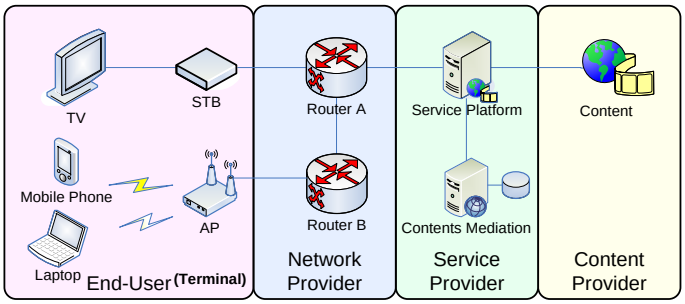


Figure 14. Overall configuration of N-screen case watching same content

Figure 14 is a 3-screen service with content sharing. Three screen service allows an IPTV service subscriber consume IPTV service contents on TV, PC, and wireless screens. The basic type of 3-screen service is sharing the same IPTV service contents on more than one screen among the three kinds of screens.

A. Service scenarios of N-screen service case watching same content on multi-devices

1. [Service Provider > End-user(Person): watching N-screen service on Terminal A] End-user(Person) is watching contents provided by content delivery functions of a service provider via network functions of a network provider using terminal A (For example, a TV with setop). The end-user may have a plan to watch the content using terminal B (For example, a Laptop) and Terminal C (For example, a mobile phone) at the same time.
2. [End-user(Person)-> Service Provider: request N-screen service to Terminal B,C] End user functions of the end-user request the terminal to provide current service to terminal B.
3. [Service Provider: preparing N-screen service for terminal B & C] The N-screen service requested to display same content of terminal A to terminal B, C is processed by service provider's service control function. The service control functions of the service provider adjust quality of contents to network bandwidth to be changed. The service control functions decide to transcode origin contents into suitable contents to be changed, considering display sizes to be changed. Application functions of the service provider may have contents mediation functions like codec convertors. The application functions converts content into small-size or big-size display, depending on the device profile and access network bandwidths.
4. [Service Provider -> Terminal B,C -> End user(Person): using N-screen service] The newly generated contents are delivered into designated storage managed by content delivery functions. The content delivery functions send adjusted contents to terminal B and C.

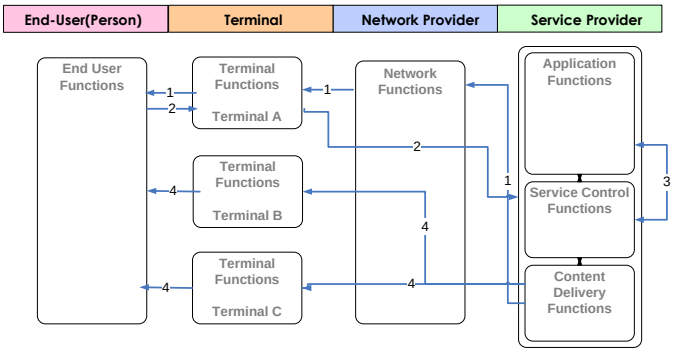


Figure 15. Service scenario of N-screen case watching same content

V. N-SCREEN SERVICE SCENARIO: CASE II

Case II N-screen is consuming same contents on several devices continuously. It is considered as one of the representative service supporting service mobility among multiple kinds of screens. Figure 16 is one of the examples of case II N-screen service. Below is the service scenario of case II N-screen: service continuity.

A. Service scenarios of N-screen service case consuming same content on multi-devices continuously.

1. [Service Provider-> End-user(Person): watching N-screen service on Terminal A] End-user (Person) is watching contents provided by content delivery functions of a service provider via network functions of a network provider using terminal A (For example, a TV with STB in a living room).

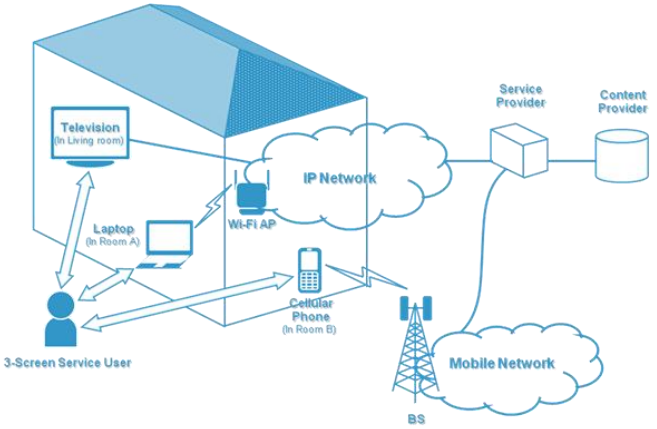


Figure 16. 3-screen service with service continuity

2. [End-user(Person): moving N-screen service on Terminal B] The end-user moves from living room to room A to watch the same content continuously using terminal B (For example, a Laptop).
3. [Terminal B-> Service Provider: request N-screen service to Terminal B] Terminal B is authenticated as an N-screen service and requests the service provider to send the same content.
4. [Service Provider: preparing N-screen service for terminal B] The N-screen service requested to display same content continuously on the terminal B is processed by service provider's service control function. The service control functions of the service provider adjust quality of contents to network bandwidth to be changed. The service control functions decide to transcode origin contents into suitable contents to be changed, considering display sizes to be changed. Application functions of the service provider may have contents mediation functions like codec convertors. The application functions converts content into small-size or big-size display, depending on the device profile and access network bandwidths.
5. [Service Provider -> Terminal B -> End user(Person): using N-screen service] The newly generated contents are delivered into designated storage managed by content delivery functions. The content delivery functions send adjusted contents to terminal B.
6. [End-user(Person): moving N-screen service on Terminal C] The end-user moves from room A to room B to watch the same content continuously using terminal C (For example, a Cellular phone). The terminal C shows the same content continuously through the same process as described above.

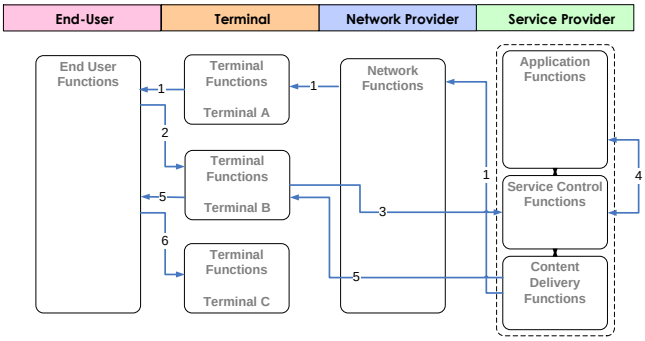


Figure 17. Service scenario of N-screen case consuming same content on multi-devices continuously

VI. Scenario for N-screen service case III scenario 1: Targeted advertising service to separate terminal

I will describe N-screen service scenario case III example, targeted mobile advertisement service that is a collaborative case.

Targeted advertisement service is providing Ad to person's mobile terminal while he is watching VOD on TV screen. During watching a VOD channel, logging and selecting keyword may be required to initiate the service. Choosing 'keyword' plus 'interests' among menus may load Ad service web pages, which gathers related Ad contents and metadata from Web and 3rd party Ad server. The login user's interests are dependent on user profile. In case that the keyword belongs to 'people', the person may appear in aggregated commercial advertisement. As supplementary Ads, banner advertisement, which is inserted by advertiser's request, is located near targeted advertising service or other convergence services.

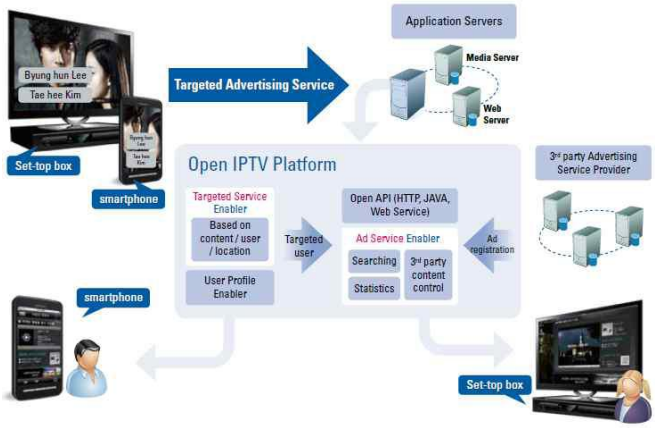


Figure 18. Targeted Advertising Service

The split EPG terminal has function to control IPTV service via home AP. A mobile user in the right of figure 18 watches golf sports channel in VOD service. He already gave his preference to the profile enabler via open service platform. For instance, since the profile enabler knows he enjoys golf as outdoor sports, when he detects golf driver on watching golf contents, the mobile ad process enabler may give him ad moving picture about newly released golf driver. Mobile ad

process enabler may give helpful information to him as well as connect to the purchase step by the mobile device.

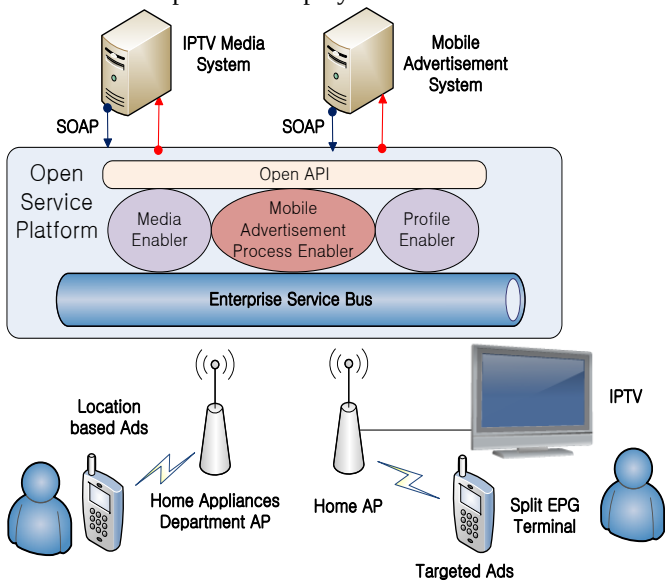


Figure 19. Example system of Targeted Advertising Service

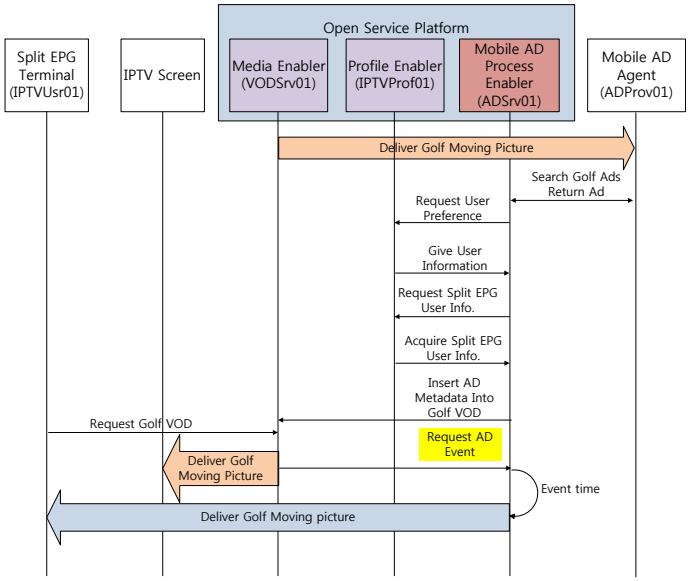


Figure 20. Service flows of Targeted Advertising Service

Figure 19 shows example of targeted advertisement using SDP. Mobile ad agent may be person or sub-system of an ad service provider. He also watches a golf VOD service via media enabler within open service platform. The mobile ad process enabler searches a golf ad among many ad contents of a mobile ad agent. That golf ad is related with revealed product in golf moving picture. The mobile ad process enabler acquires user preference and whether mobile users own split EPG terminals. The convergence enabler then inserts ad metadata into golf VOD. A mobile user with split EPG terminal requests to view that golf contents to open service platform. As soon as golf moving picture is delivered to an IPTV user, ad request event is generated.

A. Service scenarios of N-screen service case collaborating convergence service: targeted advertising service to separate terminal.

1. [Service Provider -> End-user(Person): watching VOD channel on Terminal A] End-User(Person) is watching VOD channel with Ad service which is provided content delivery functions of service provider via network functions of network provider using terminal A (For example, a TV with setop). We suppose that end-user with Terminal A is a woman in forties and she likes to collect jewelry.
2. [End-user(Person) -> Service Provider: initiate Targeted advertisement service on Terminal A] The end-user can login and select keyword to initiate the targeted advertisement service. By choosing ‘keyword’ plus ‘interests’ on menues of Terminal A, related Ad contents and metadata from Web and 3RD party Ad Server is gathered by service control functions of the service provider.
3. [Service Provider: prefaring and generate targeted web pages for Terminal A] Targeted advertised content is generated with gathering Ad contents , metadata and profile information of end-user with Terminal A
4. [Service Provider -> Terminal A-> End user(Person): using targeted advertised service with Terminal A] The newly generated content which has targeted information(For example, jewelry shops) for end-user with Terminal A is delivered to Terminal A by content delivery functions.
5. [End user(Person) -> Service Provider : initiate Targeted advertisement service on Terminal B] End-User(Person) has a hand-helded device such as smartphone. He lives with his mother who is end-user using Terminal A. Let’s suppose that end-user with Terminal B is a man in twenties and he is interested in car so much. He can also initiate targeted advertised service by logining and selecting keyword. At this time, user profile information of end-user with Terminal B is transmitted to the service control functions of the service provider. Related Ad contents and metadata for end-user with Terminal B from Web and 3RD party Ad Server is also gathered by service control functions of the service provider.
6. [Service Provider: prefaring and generate targeted web pages for Terminal B] Targeted advertised content is generated with gathering Ad contents , metadata and profile information of end-user with Terminal B

7. [Service Provider -> Terminal A-> End user(Person): using targeted advertised service with Terminal B] The newly generated content which has targeted information(For example, car Ad) for end-user with Terminal B is delivered to Terminal B by content delivery functions.

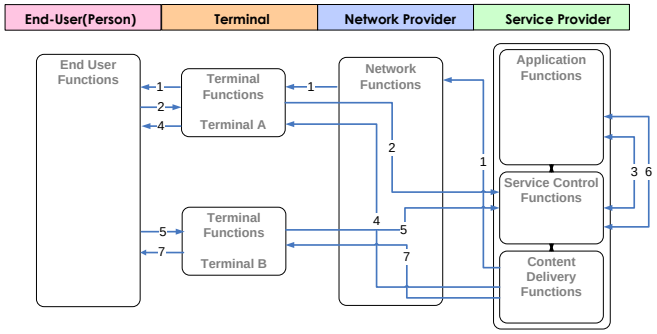


Figure 21. Service scenario of N-screen case using targeted advertising service

VII. N-SCREEN SERVICE SCENARIO CASE III SCENARIO 3: ASMD

ASMD (Adaptive Source Multi-Device) is a collaborative case of N-screen service. The concept of collaborative case of N-screen is an existence of collaboration among multi-screen showing different content or services for screens. The ASMD adds content/service adaption concept upon the collaboration. For example, if a user watching TV content related news using his mobile phone, then he wants to transfer the news to big TV screen to share the news with his family. Because the size and resolution is different between TV and mobile phone, proper adaption should be done on service presentation. In ASMD type of collaborative N-screen service, it is not sufficient to provide service only by collaboration.

A. Service scenarios of N-screen service case III collaborating: ASMD

1. [Service Provider > End-user(Person): watching TV program(baseball) on Terminal A(Big-screen TV)] User1, 2, 3 (3 Persons) are watching TV program on Terminal A(Big-screen TV) provided by content delivery functions of a service provider via network functions of a network provider.

2. [Service Provider > End-user(Person): using service on Terminal] User1, 2, 3 (3 Persons) are using services on their own handheld device (Terminal B, C, D). The services are related with TV program shown on Terminal A (Big-screen TV). For example, User 1 watches multi-angle scene of the baseball game on his smartphone. User 2 watches shorts news about the played baseball game on his tablet. User 3 uses baseball-game statistics service.

3. [End-user(Person)-> Service Provider: request sending their services to Terminal A] End user functions of the end-user requests their own terminal B, C, D to transfer current service to terminal A to discuss about the game by watching each person's service together. The N-screen service requested is to display combined contents of services of terminal B, C, and D. The N-screen Service control function receives the request.

4. [Service Provider: preparing N-screen service for terminal A] The N-screen service control functions of the service provider adjust quality of services to fit the capabilities of different terminals. The Application function receives adapted content from service control function then sends it to terminal A using collaboration function of N-screen service control function.

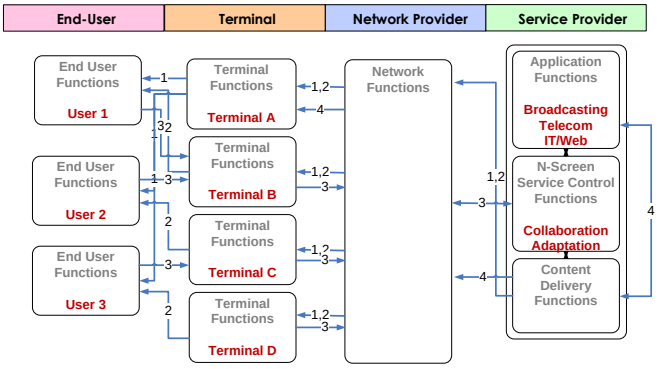


Figure 22. Service scenario of ASMD, N-screen collaborative case

VIII. CONCLUSIONS

The major keywords for N-screen service are cloud computing and social TV. The cloud computing is expending its technological importance and business area. It is possible to provide information synchronization service inside home and dynamic resource allocation using cloud computing's technologies such as virtualization, remote storage and mobile cloud [7]. Those kinds of services are closely related to N-screen service.

It is important to combine with social TV to invigorate N-screen service business. Using social TV concept, it is easy to introduce N-screen into IPTV or smart TV because the customer can use collaborative services with main VOD or channel content. We described the targeted advertisement service that the customer watches advertisement content on different screen while he watches TV. At that scenario, we used service delivery platform to deliver IPTV and advertisement [8, 9, 10]

N-screen service standardization is progressing through ITU-T Q24/SG13 for the service scenarios and use cases. The standardization of architecture and cloud computing related will be progressed.

In this paper, we described N-screen service concept, N-screen service classification, service scenario description method, and service scenarios. Among three cases of N-screen service classification, the case III, collaborative case among

several terminals is most importance in the aspect of business model. Right now, the telecommunication venders are focusing to provide OSMU and seamless case of N-screen. However the case III will catch user's attention because of its variety of service cases and features.

REFERENCES

[1] Changwoo Yoon, Hyunwoo Lee, Won Ryu, Bongtae Kim, "IPTV Service and Technology Evolutions," *Journal of Korea Information and Communication Society*, pp. 1-9, August, 2008.

[2] Changwoo Yoon, Shinmo Kim, Hyunwoo Lee, "Convergence Service Implementation based on Service Delivery Platform and Research Issues," *International Technical Conference on Circuits/Systems, Computers and Communications*, pp. 1080-1083, July 2009.

[3] ITU-T, Next Generation Network Global Standards initiative (NGN-GSI), http://www.itu.int/ITU-T/ngn/index.phtml

[4] "Service scenarios over FMC," ITU-T Recommendation Series Y.2720 Supplement 14, 2011.1.

[5] "Supplement on IPTV service use cases," ITU-T Recommendation Series Y Supplement 5, 2008.

[6] "Web-based IPTV brokering service models and scenarios," ITU-T Draft Recommendation Series Y.iptvbs, September 2010.

[7] Changwoo Yoon, Mohammad Mehedi Hassan, Biao Song, Hyunwoo Lee, Won Ryu and Eui-Nam Huh, "Dynamic Collaborative Cloud Service Platform: Opportunities and Challenges," *ETRI Journal*, Vol.32, No.4, pp. 634-637, August 2010.

[8] Changwoo Yoon, Hyunwoo Lee, Won Ryu, "Design of Layered service delivery platform for enabling I-centric convergence service," *Communications and Information Technology, 2009. ISCIT 2009. 9th International Symposium on*, pp. 243-247, September, 2009.

[9] Changwoo Yoon, Hyunwoo Lee, "Service delivery platform for convergence service creation and management," *Proceeding ICACT'10 Proceedings of the 12th international conference on Advanced communication technology*, pp.1335-1338 , Feb, 2010.

[10] Changwoo Yoon, Hyunwoo Lee, Won Ryu, "Next generation IPTV Platform," *2010 9th International Conference on Optical Internet (COIN)*, pp. 1-3, July 2010.

Changwoo Yoon received the B.S. degree from Sogang University, Seoul, Korea, in 1990. He received M.S. degree from POSTECH, Pohang, Korea, in 1992. He received Ph.D. degree in Computer & Information Science & Engineering from University of Florida, US, in 2005. Currently he is principal researcher in Creative Future Research team, ETRI and adjunct professor at UST. His current research interests include N-Screen, IPTV, Cloud computing, SOA, Service creation/delivery technology and information retrieval.

Hyunwoo Lee received M.S. and Ph.D. degrees in 1995 and 2005, respectively, in Korea Aerospace University (KAU). He is currently a principal research engineer and team leader in convergence service networking research team, smart screen convergence research department, ETRI. His main research interests include heterogeneous wireless access network, Mobile P2P, open IPTV platform in NGN. His current research interests include cloud computing and platform.

Won Ryu, Ph.D received the BS degree in computer science and statistics from Pusan National University, Busan, South Korea, in 1983, and the MS degree in computer science and statistics from Seoul National University, Seoul, South Korea, in 1987. He received his PhD degree in information engineering from Sungkyunkwan University, Kyonggi, South Korea, in 2000. Since 1989, he has been a managing director with the Smart screen convergence research department, ETRI, Daejeon, Korea. Currently, his research interests are IPTV, Smart TV, IMT-advanced, and convergence services and networks and etc.

Dempster-Shafer Evidence Theory Based Trust Management Strategy against Cooperative Black Hole Attacks and Gray Hole Attacks in MANETs

Bo YANG*, Ryo YAMAMOTO*, Yoshiaki TANAKA*,**

*Global Information and Telecommunication Institute, Waseda University, Japan

**Research Institute for Science and Engineering, Waseda University, Japan

yangbo_youhaku@ruri.waseda.jp, ryo_yamamoto@moegi.waseda.jp, ytanaka@waseda.jp

Abstract—**The MANETs have been experiencing exponential growth in the past decade. However, their vulnerability to various attacks makes the security problem extremely prominent. The main reasons are its distributed, self-organized and infrastructure independent natures. As concerning these problems, trust management scheme is a common way to detect and isolate the compromised nodes when a cryptography mechanism shows a failure facing inner attacks. Among huge numbers of attacks, black hole attack may collapse the network by depriving the route of the normal communication. The conventional proposed method achieved good performance facing black hole attack, while failing to detect gray hole attacks. In this paper, a Dempster-Shafer (D-S) evidence based trust management strategy is proposed to conquer not only cooperative black hole attack but also gray hole attack. In the proposed method, a neighbour observing model based on watchdog mechanism is used to detect single black hole attack by focusing on the direct trust value (DTV). Historical evidence is also taken into consideration to go against gray hole attacks. Then, a neighbour recommendation model companied with indirect trust value (ITV) is used to figure out the cooperative black hole attack. D-S evidence theory is implemented to combine ITVs from different neighbours. Some of the neighbour nodes may declare a false ITV, which effect can also be diminished through the proposed method. The simulation is firstly conducted in the Matlab to evaluate the performance of the algorithm. Then the security routing protocol is implemented in the GloMoSim to evaluate the effectiveness of the strategy. Both of them show good results and demonstrate the advantages of proposed method by punishing malicious actions to prevent the camouflage and deception in the attacks.**

Manuscript received July 25, 2012.

B. YANG is with the Global Information and Telecommunication Institute, Waseda University, Tokyo, 169-0051 Japan. phone: 090-0495-246104; fax: 090-0495-246104; e-mail: yangbo_youhaku@ruri.waseda.jp.

R. YAMAMOTO is with the Global Information and Telecommunication Institute, Waseda University, Tokyo, 169-0051 Japan. e-mail: ryo_yamamoto @moegi.waseda.jp.

Y. TANAKA is with the Global Information and Telecommunication Institute, Waseda University, Tokyo, 169-0051 Japan. He is also with the Research Institute for Science and Engineering, Waseda University, Tokyo, 162-0044 Japan. e-mail: ytanaka@waseda.jp.

Index Terms—**Dempster-Shafer evidence, Trust management, Direct trust value, Indirect trust value, Black hole attack, Gray hole attack, MANETs**

I. INTRODUCTION

The mobile ad hoc networks (MANETs) are flexible networks that inherit common characteristics found in wireless networks in general. However, it adds characteristics specific to ad hoc networks, such as distributed, self-organized infrastructure and mobility. MANETs have been primarily been implemented for tactical network related applications to improve battlefield communications and survivability. Later the technology of MANETs is introduced to some other scenarios such as disaster relief, chemical leakage monitoring, forest fire monitoring, etc. However, owing to its flexibility and infrastructure-independent nature, it is particularly vulnerable to various attacks compared with conventional networks. And security problems in MANETs are mainly aroused by its unique characteristic such as dynamic network topology, limited bandwidth and limited battery power. Concerning about these, cryptography mechanisms, intrusion detection system (IDS) and efficient routing protocols are used to ensure the security of MANETs. However, these conventional methods, especially cryptography method, fail to filter out compromised nodes or the legitimated ones with malicious actions. Although lots of efficient routing protocols are proposed to ensure the security, routing attacks aroused by legitimated nodes that will make the protocols effectiveness. Possible attacks include passive eavesdropping, denial of service (DoS) attacks, wormhole attacks, sybil attacks etc. As one type of DoS attacks, black hole attack can cause catastrophic damage to normal communication of a large area in the network. The black hole nodes can launch routing attacks to deprive the routing path and relative operation such as dropping packets. Most of the existing detection strategy either spends a large overhead or cannot prevent the cooperative black hole attack effectively. This paper focuses

on the black hole attack and gray hole attack that malicious nodes pretend as if they have the shortest path to the destination and then deprive the routing.

In order to detect a single black hole attack as well as a cooperative black hole attack, a neighbour nodes observation model (NNOM) and a neighbour recommendation trust model (NRTM) based on the former one is given in our previous study [1]. The method introduces a trust mechanism to detect inner attackers in ad hoc network. The NNOM is based on the watchdog mechanism [2] and each node keeps on watching its own neighbour nodes while judging its communication behaviour. These statistical data are used to compute a direct trust value (DTV) that would be compared with a predefined threshold to decide whether a neighbour node is a malicious node or not. Even if a neighbour node acts as a normal node, the node would not be trusted immediately since the next hop of the node considers the case that a cooperative black hole attack is hidden behind. That is, the NRTM is established among the nodes and the other neighbour nodes are asked to declare their opinion about the reputation of the two hop neighbour node. Furthermore, an indirect trust value (ITV) is computed and simply compared with a predefined threshold to decide whether there is a cooperative black hole attack.

Malicious nodes may act abnormally after a long period normal actions and their reputation still remains high. It is known as another type of black hole attack: gray hole attack, which is taken in certain time period or to certain data packets. This kind of attack is more harmful and even more difficult to detect because of their malicious behaviour.

In this paper, historical evidence based NNOM and DTV based on the Dempster-Shafer (D-S) evidence theory [3] are proposed to settle this problem. The proposed method makes it difficult for each node to get a high reputation after a long run, but easy to lose it. Moreover, the recommended reputation from some neighbour nodes with ulterior motives might confuse the final judgement of the mechanism. The proposed method considers the data distance between two reputation evidences [4] and that makes the cheating impact on ITV minimized.

The rest of this paper is organized as follows. In section II, the single black hole attack and the cooperative black hole attack are introduced firstly. Then related works are described. In section III the D-S evidence theory is introduced. Section IV describes the details of the proposed model and algorithms along with the processes step of the strategy. The numerical result of algorithms and the network simulation study of security protocol are evaluated in section V and section VI, accordingly. Finally, section VII concludes this paper.

II. Black Hole Attack and Related Works

A. Black Hole Attack and Gray Hole Attack

Varieties of routing protocol are implemented in the MANET that can be classified into three categories: proactive, reactive, and hybrid. Some famous and representative ones are destination sequence distance vector (DSDV) as proactive protocol, and dynamic source routing (DSR) along with ad hoc on-demand distance vector (AODV) as reactive protocol [5]. Reactive routing protocols such as AODV initiate a route discovery process at the beginning of a communication when there is no valid and fresh route from the source node to the destination node. In this process, destination sequence numbers and unique broadcast IDs are used to ensure that the routes are loop-free and freshness of the routes. The source node broadcasts route request (RREQ) packets to all its neighbour nodes and the packets are relayed to next hop node until legitimated destination node receives them. After receiving RREQ, the destination node or an intermediate node with fresh route to the destination responds it by unicasting a route reply (RREP) packet. When the source node receives the RREP packet, the route is established. Then communication between the source node and the destination node would be available though the route.

In this route discovery phase, two types of black hole attack can be found: single attack and cooperative attack. The attacks can be aroused in two phases: the RREQ phase and the RREP phase. In this paper, the proposed method focuses on the black hole attack in the RREQ phase and the behaviour of malicious nodes in the same period.

As is shown in Figure 1, a single black hole attack is done merely by one malicious node. When a malicious node M receives RREQ message from the source node S, it sends back fallacious RREP message immediately without relaying it to the real destination node D through node 3. Since the

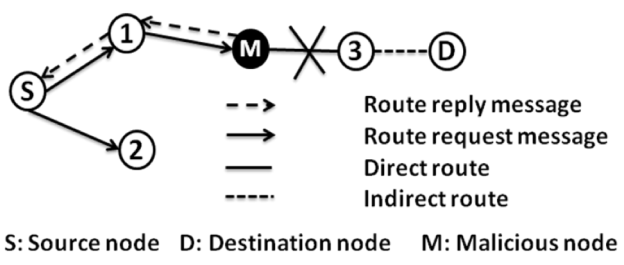


Fig. 1. Single black hole attack

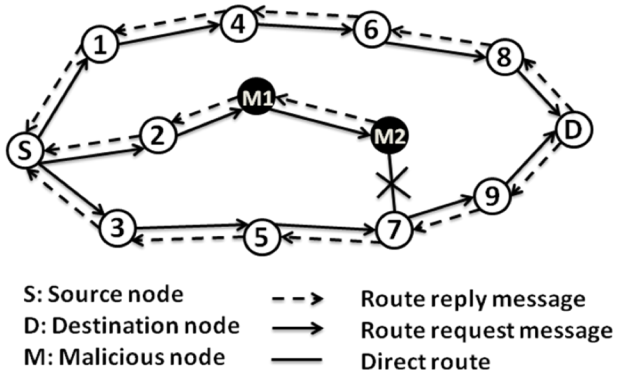


Fig. 2. Cooperative black hole attack

malicious nodes gerrymander the sequence number and the ID number, node S is convinced that node D is the next hop of node M. In this way, the malicious node is able to collect all the packets from the source node and do further actions such as dropping them or analysing the data. In order to tackle this problem, some conventional methods are proposed to settle this kind of problem by monitoring the neighbour nodes' activity. However, it does not work properly when two or more malicious nodes cooperate together.

Figure 2 illustrates an example of cooperative attack with malicious node M1 and M2. When the source node S tries to find a route to the destination node D, it broadcasts RREQ to the destination node. Since node 2 might watches the behaviour of node M1 closely, M1 tries to pretend to be a normal node and just relay the RREQ to node M2. After node M2 receives RREQ from node M1, it begins malicious action that is the same as the single attack. In this way, node M1 and M2 can hide in the network without being noticed by other normal nodes. For the cases of more than two malicious nodes in the network, the harmful influence becomes greater since the prevention becomes much difficult.

More harmful type of attacks in black hole attack is the gray hole attack [6]. The significant difference between the gray hole attack and black hole attack is that the former one only does the action in certain time period or to certain data. A gray hole attack node firstly exploits the route by advertising it has the shortest path to the destination node, then the node can establish the route through it. By doing this, it may be able to drop packets from a certain target node in certain time duration. However, it turns to normal behaviour for other nodes to hide its malicious presence for most of the time. In some other case, the malicious node may arouse attack to some certain data from the target node. Therefore, the gray hole attack becomes more difficult to detect than the ordinary black hole attack.

B. Related Works

In our previous work, each node implements a global agent acting as a watchdog that detects the packets relaying of neighbour nodes [7], [8]. The model is called NNOM as is seen in Figure 3. In this figure, node 1 keeps on watching node 2, 3, 4 and M. When node M drops packets, the observation nodes begin to observe its abnormal behaviour. The node 1 calculates DTV on node M based on the statistical data of node M's behaviour by using following Eq. (1):

$$D_i(j) = \frac{S}{S+F} \tag{1}$$

where:

$D_i(j)$: the DTV of node j judged by node i;
S: the number of successful packets relayed by node j;
F: the number of failed packets relayed by node j.

Once DTV becomes lower than a predefined threshold D_{th}, the node is treated as a malicious node. It is apparent that when the black hole node takes action all the way, S becomes smaller compared with F. That is, the DTV decrease sharply along with the passage of time.

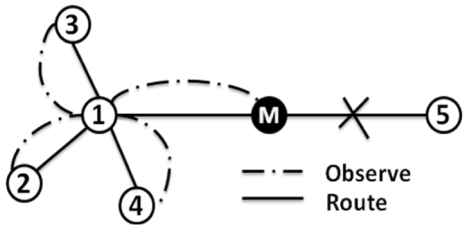


Fig. 3. Neighbour nodes observation model (NNOM)

For the case of gray hole attack, however, long terms of normal behaviour may help the malicious node to get a higher DTV. Since the attack nodes in a gray hole attack is intermittently, the malicious node act as normal as possible to earn higher DTV all the way. Irregular malicious behaviour does not decrease the DTV obviously, thus the node is treated as normal node.

In order to detect two cooperative malicious nodes, NRTM [9] is proposed as is shown in Figure 4. When M1 acts normal, node 1 does not trust it directly. However, it tries to get other neighbour nodes' opinion about node M2. Trust request (TREQ) message and trust reply (TREP) message are introduced to accomplish this requirement [10]. Firstly, the node 1 broadcasts TREQ messages to its neighbour nodes 2, 3. The nodes which receive TREQ reply TREP with $D_j(k)$ of M2 immediately. After a recommendation time to live (RTTL), the ITV is calculated using the following Eq. (2):

$$I_i(k) = \frac{\sum_{j \in N_i, j \neq m} D_i(j) D_j(k)}{|N_i| - 1} \tag{2}$$

where:

$I_i(k)$: the ITV of node k judged by node i;
$D_i(j)$: the DTV of node j judged by node i;
$D_j(k)$: the DTV of node k judged by node j;
N_i: the neighbour nodes' set of node i;
m: the suspicious node between node i and node k.

ITV is stored in an indirect trust table (ITT) and compared with a predefined threshold I_{th}. If ITV is lower than I_{th}, the node M1 along with node M2 are recognized as a malicious node. Then, the ID of node M1 and M2 are added to node 1's malicious table and restart the route discovery phase.

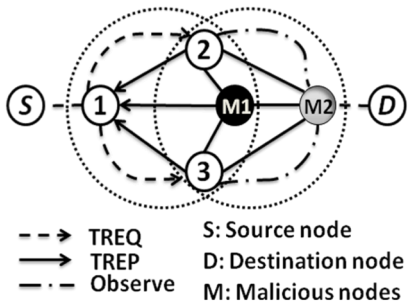


Fig. 4. Neighbour recommendation trust model (NRTM).

However, some intermediate neighbour nodes may lie to the observation node and affect the judgment of observation node on two-hop neighbour node. For example, node 2 may give a high reputation of node M2 compared with other recommender, which makes ITV insensitive to the attack actions of the malicious nodes. Then how to balance the ITVs from different sources is also a problem needs solving.

III. D-S Evidence Theory

The Dempster-Shafer evidence theory is not only a theory of evidence but also that of probable reasoning. It is a framework that can be deployed in diverse areas such as pattern matching, computer vision, expert systems and information retrieval. The D-S evidence theory can handle the randomness and subjective uncertainty together in the trust evaluation. By accumulating evidences, it can narrow down a hypothesis set which provides a powerful method for the representation and process of the trust uncertainty without the demand of prior distribution. Moreover, Dempster's rule of combination is the procedure to aggregate and summarize a corpus of evidence. In the section below, basic concepts in D-S evidence theory are reviewed and will be used to establish model in the proposed method in this paper.

Definition 1. Suppose Φ is a finite set of states, and Φ is defined as a frame of discernment $\{T, \neg T\}$ as the set of propositions under consideration where T and $\neg T$ mean that the given agent considers a given correspondent to be trustworthy or not to be trustworthy, respectively. The number of subsets is 2Φ, and 2Φ is defined as $\{ø, \{T\}, \{\neg T\}, \{T, \neg T\}\}$, where ø represent impossible events while $\{T\}$, $\{\neg T\}$ and $\{T, \neg T\}$ represent trust value, distrust value, and uncertain events respectively.

Definition 2. The mass value of an element A is defined as $m(A)$, and the value of m: 2Φ->[0, 1]. As is closed-world assumption, the mass value of null set is defined as $m(ø)=0$. The basic probability assignment function is defined using the following Eq.(3):

$$\begin{cases} \sum_{A\subseteq\Phi} m(A) = 1 \\ m(\phi) = 0 \end{cases} \tag{3}$$

As is in Definition 1, there has the relationship between $m(\{T\})$, $m(\{\neg T\})$ and $m(\{T, \neg T\})$: $m(\{T\})+m(\{\neg T\})+m(\{T, \neg T\}) = 1$.

Bel: 2Φ->[0, 1] is a belief function over Φ as is defined using the following Eq.(4):

$$Bel(A) = \sum_{B\subseteq A} m(B) \tag{4}$$

Pls: 2Φ->[0, 1] is a plausibility function over Φ as is defined using the following Eq.(5):

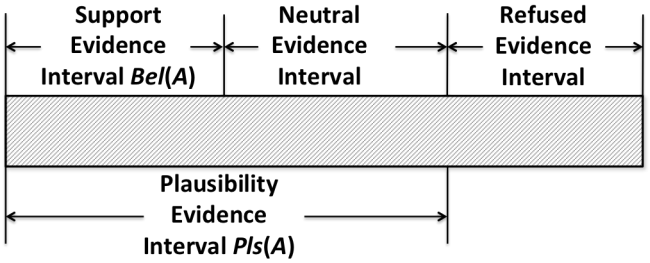


Fig. 5. Evidence interval illustration

$$\begin{cases} Pls(A) = \sum_{B\cap A\neq\phi} m(B) \\ Pls(A) = 1 - Bel(\overline{A}) \end{cases} \tag{5}$$

As is in Definition 1, there are $Bel(\{T\})=m(\{T\})$ and $Pl(\{T\})=m(\{\neg T\})+m(\{T, \neg T\})$.

The relationship between $Bel(A)$ and $Pls(A)$ can be illustrated as the figure in Figure 5.

Definition 3. Dempster's combination rule of two evidences: Suppose Bel_1 and Bel_2 are belief functions over the same frame Φ, with basic probability assignments m_1 and m_2, and focal elements $A_1,...,A_i$, and $B_1,...,B_i$, respectively. Then the function $m(C)$: 2Φ->[0, 1] is defined using the following Eq.(6):

$$\begin{cases} m(C) = m_1(A) \oplus m_2(B) = \dfrac{\sum_{A_i\cap B_j=C} m_1(A_i)m_2(B_j)}{1 - \sum_{A_i\cap B_j=\phi} m_1(A_i)m_2(B_j)} \\ m(\phi) = 0 \end{cases} \tag{6}$$

for all nonempty C, $m(C)$ is a basic probability assignment which describes the combined evidence.

Definiton 4. Dempster's combination rule of more than two evidences: Suppose there are k evidences that are independent with each other over the same frame Φ, with basic probability assignments m_1, m_2, ..., m_p, and focal elements C_1, C_2 and C_p, respectively. Then the function m: 2Φ->[0, 1] is defined using the following Eq.(7):

$$\begin{cases} m(C) = (m_1(C_1) \oplus m_2(C_2) \oplus ...) \oplus m_p(C_p) \\ m(\phi) = 0 \end{cases} \tag{7}$$

for all nonempty C, $m(C)$ is a basic probability assignment which describes the combined evidence.

The trust management strategy proposed in this paper is based on the D-S evidence theory. Firstly, it gives out a formal definition of the trust value. Then it quantifies the direct trust value with a basic confidence function. The direct trust value is used to decide whether a neighbour node is benevolent one. The indirect trust value comes from the

recommendation neighbour node. D-S combination rule is used to combine the indirect trust value together. Then, the combined trust value is compared with the predefined threshold to decide whether there is a cooperative black hole attack.

IV. Proposed Models and Algorithms

A. Proposed NNOM and DTV

As is in the previous work, it only considers about the communication factors such as routing packets as well as data packets. Moreover, it is supposed that each node only marks its neighbour nodes with cooperative and uncooperative by calculating DTV [11]. However, the watchdog mechanism usually considers about safety data fusion, which is used to make sure data's integrity that sent data and received data are exactly the same. In this case, a nodes' behaviour can be classified into three categories: normal, suspicious, and malicious. The proposed method supposes that each node watches its neighbour node and marks its behaviours as α, β and γ: the number of benevolent, malicious and suspicious respectively in a certain time period respectively. The target of the proposed method is to make it more difficult for a node to get a higher reputation in a long run while easy to lose it. The proposed method also takes historical evidence into consideration. It is inspired by the Dempster-Shafer (D-S) evidence theory, which is an effective method of combining accumulative evidences or for changing priors in the presence of new evidences [12]. The proposed DTV algorithm can be described in following Table 1. This algorithm decides whether a neighbour node is a malicious node or not.

From a time period [T_n, T_{n+1}], each node i will count the recent trust evidence of its neighbour node j. The trust evidence is refreshed form time T_n to T_{n+1} using the following Eq. (8) to Eq. (10). The refresh weight θ is decided by newly counted trust evidence using following Eq. (11). In order to prevent the camouflage and deception, lower θ_1 is used to lower the effect of the evidence supporting benevolent. In order to diminish the effect of malicious actions, a high value is given to θ_2. For the gay hole nodes, when it acts normal behaviour again after malicious actions, the value of θ is set to be θ_3. The value of θ_1, θ_2 and θ_3 is $0 < \theta_3 < \theta_1 < 0.5 < \theta_2 < 1$.

$$\alpha_{n+1} = (1-\theta)\alpha_n + \theta\Delta\alpha \tag{8}$$

$$\beta_{n+1} = (1-\theta)\beta_n + \theta\Delta\beta \tag{9}$$

$$\gamma_{n+1} = (1-\theta)\gamma_n + \theta\Delta\gamma \tag{10}$$

$$\theta = \begin{cases} \theta_1, & if \quad \Delta\alpha \geq \Delta\beta \\ \theta_2, & if \quad \Delta\alpha < \Delta\beta \\ \theta_3, & if \quad \Delta\alpha \geq \Delta\beta \quad then \quad \Delta\alpha < \Delta\beta \end{cases} \tag{11}$$

where:

$\Delta\alpha$: the number of the normal behaviours in [T_n, T_{n+1}];
$\Delta\beta$: the number of the malicious behaviours in [T_n, T_{n+1}];
$\Delta\gamma$: the number of the suspicious behaviours in [T_n, T_{n+1}];

TABLE 1
DTV Algorithm

DTV Algorithm

Step 1: Node i watches node j from T_n to T_{n+1}
Step 2: $(\Delta\alpha, \Delta\beta, \Delta\gamma)$ is calculated
Step 3: Compare $\Delta\alpha$ and $\Delta\beta$ to decide the value of θ using Eq. (11)
Step 4: Calculate the trust evidence $(\alpha_{n+1}, \beta_{n+1}, \gamma_{n+1})$ at T_{n+1} using Eq. (8)-(10)
Step 5: Calculate the DTV of node j using Eq. (12)-(15)
Step 6: if $B_{ij} - M_{ij} > \eta_1$ and $S_{ij} < \varepsilon_1$
node j is trusted
else if $B_{ij} - M_{ij} < \eta_2$ and $S_{ij} < \varepsilon_1$
node j is malicious node and put into MT.
else
node j is listed on ST
End.

MT stands for the malicious table. ST represents the suspicious table. The value of η_1, η_2 and ε_1 will be studied in the algorithm simulation.

α_n: the trust evidence of normal behaviour at T_n;
β_n: the trust evidence of malicious behaviour at T_n;
γ_n: the trust evidence of suspicious behaviour at T_n;
θ: the refresh weight.

Based on the trust evidence that cares about the historical data, DTV is calculated using following Eq. (12) to Eq. (15):

$$B_{i,j} = \frac{\alpha_n}{\alpha_n + \beta_n + \gamma_n} \tag{12}$$

$$M_{i,j} = \frac{\beta_n}{\alpha_n + \beta_n + \gamma_n} \tag{13}$$

$$S_{i,j} = \frac{\gamma_n}{\alpha_n + \beta_n + \gamma_n} \tag{14}$$

$$D_{i,j} = (B_{i,j}, M_{i,j}, S_{i,j}) \tag{15}$$

where:

$B_{i,j}$: the benevolent actions DTV of node j at T_n;
$M_{i,j}$: the malicious actions DTV of node j at T_n;
$S_{i,j}$: the suspicious actions DTV of node j at T_n.

DTV of node j calculated by node i is represented by $D_{i,j}$, which consists of three parts: $B_{i,j}$, $M_{i,j}$, $S_{i,j}$. Each node maintains two tables: Malicious Table (MT) and Suspicious Table (ST). If a neighbour node is considered to be malicious node, the observation node records its node ID in MT. If there is not enough evidence to make sure whether it is normal or malicious at the very moment, its ID is recorded in the ST of the observation node. Relative thresholds are described in the Step 6 of the DTV algorithm. DTV is stored in a Direct Trust-value Table (DTT) for further use in ITV.

B. Proposed NRTM and ITV

Although there is the proposed DTV, the route through one neighbour node is never set up directly when it is trusted by the observe nodes. As is shown in figure 6, node i tries to get other neighbour nodes' opinion about the next hop of node j, namely, node k. For this reputation, node i broadcasts TREQ

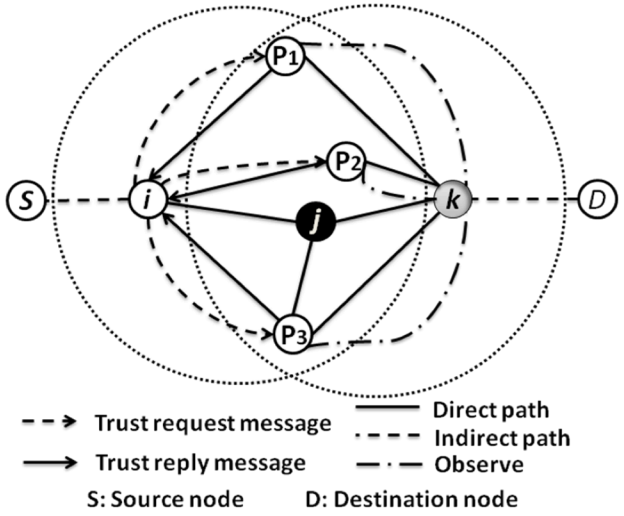


Fig. 6. Neighbour recommendation trust model (NRTM)

messages to get the DTV of node *k*.

In a predefined recommendation time to live (RTTL), the neighbour nodes such as nodes P_1, P_2 and P_3 send back TREP messages including DTVs of node *k*. Then, DTV of neighbour nodes and DTV of node *k* are used together to calculate ITV. However, some of the neighbour nodes may deceive node *i* by giving a high reputation of node *k*. Therefore, the proposed method tries to give each neighbour node an evaluation difference to balance the neighbour node's cheating enhancements on the value of ITV. The proposed ITV calculation algorithm is described in following Table 2 whether there is cooperative black hole attack or not.

The evaluation difference based on the data distance [13], which means each two data's difference, is calculated by following Eq. (16) to Eq. (17). The evaluation difference of each part in DTV is represented as d_B^p, d_M^p while the range is [0,1] and smaller difference makes them closer to 0.

$$d_B^P = \frac{\sum_{p,q\in N_i, p\neq j, q\neq p} \sqrt{\left|B_{i,q}B_{q,k} - B_{i,p}B_{p,k}\right|}}{\left|N_i\right| - 2} \tag{16}$$

$$d_M^P = \frac{\sum_{p,q\in N_i, p\neq j, q\neq p} \sqrt{\left|M_{i,q}M_{q,k} - M_{i,p}M_{p,k}\right|}}{\left|N_i\right| - 2} \tag{17}$$

where:

d_B^p : the evaluation difference of *B* in DTV;
d_M^p : the evaluation difference of *M* in DTV;
N_i : the neighbour nodes set of node *i*.

Based on the evaluation difference, each neighbour node can be given a different trust weight to calculate the ITV. Take d_B for example, if a given $B_{i,p}B_{p,k}$ is more different from other $B_{i,q}B_{q,k}$, the d_B of this recommendation reputation is larger than other ones. Then, this recommendation reputation may be given by a deceiving nodes and a low trust weight is used to decrease its impact on total ITV as is shown in the following Eq. (18) to Eq. (21):

TABLE 2
ITV ALGORITHM

ITV Algorithm

Step 1: Do DTV algorithm on node *j*, if it acts normal go on to step 2
Step 2: Node *i* asks nodes *p*'s DTV on node *j*
Step 3: Calculate the evaluation difference using Eq. (16)-(17)
Step 4: Calculate the ITVs of node *j* using Eq. (18)-(21)
Setp 5: Combine different ITVs using Eq. (22)-(25)
Step 6: if $b_{i,k} - m_{i,k} > \delta_1$ and $s_{i,j} < \varepsilon_2$
node k is trusted
else if $b_{i,k} - m_{i,k} < \delta_2$ and $s_{i,j} < \varepsilon_2$
node *k* is malicious node and put into MT.
else
node *k* is listed on ST
End.

MT stands for the malicious table. ST represents the suspicious table. The value of δ_1, δ_2 and ε_2 will be studied in the algorithm simulation.

$$b_{i,k}^p = B_{p,k}\left(1 - \frac{d_B^p}{Max\sqrt{\left|B_{i,q}B_{q,k} - B_{i,p}B_{p,k}\right|}}\right) \tag{18}$$

$$m_{i,k}^p = M_{p,k}\left(1 - \frac{d_M^p}{Max\sqrt{\left|M_{i,q}M_{q,k} - M_{i,p}M_{p,k}\right|}}\right) \tag{19}$$

$$s_{i,k}^p = 1 - b_{i,k}^p - m_{i,k}^p \tag{20}$$

$$I_{i,k}^p = (b_{i,k}^p, m_{i,k}^p, s_{i,k}^p) \tag{21}$$

where:

$b_{i,k}^p$: the benevolent actions ITV of node *k* through node *p* at present T_n;
$m_{i,k}^p$: the malicious actions ITV of node *k* through node *p* at present T_n;
$s_{i,k}^p$: the suspicious actions ITV of node *k* through node *p* at present T_n;
$I_{i,k}^p$: the ITV of node *k* through node *p* at present T_n.

According to the Dempster's combination rule of more than two evidences, the ITVs are combined together to calculate a combined ITV and the ITV is calculated using the following Eq.(22) to Eq.(25):

$$b_{i,k} = b_{i,k}^1 \oplus b_{i,k}^2 \oplus b_{i,k}^3 \oplus \cdots \oplus b_{i,k}^p \tag{22}$$

$$m_{i,k} = m_{i,k}^1 \oplus m_{i,k}^2 \oplus m_{i,k}^3 \oplus \cdots \oplus m_{i,k}^p \tag{23}$$

$$s_{i,k} = s_{i,k}^1 \oplus s_{i,k}^2 \oplus s_{i,k}^3 \oplus \cdots \oplus s_{i,k}^p \tag{24}$$

$$I_{i,k} = (b_{i,k}, m_{i,k}, s_{i,k}) \tag{25}$$

where:

$b_{i,k}$: the benevolent actions ITV of node *k* at present T_n;
$m_{i,k}$: the malicious actions ITV of node *k* at present T_n;
$s_{i,k}$: the suspicious actions ITV of node *k* at present T_n;
$I_{i,k}$: the ITV of node *k* at present T_n.

ITV of node *k* calculated by node *i* is represented by $I_{i,k}$, which consists of three parts: $b_{i,k}$, $m_{i,k}$, $s_{i,k}$. The value of ITV is stored in an Indirect Trust-value Table (ITT). According to the Step 5 in the ITV algorithm, if node *k* is trusted, the source

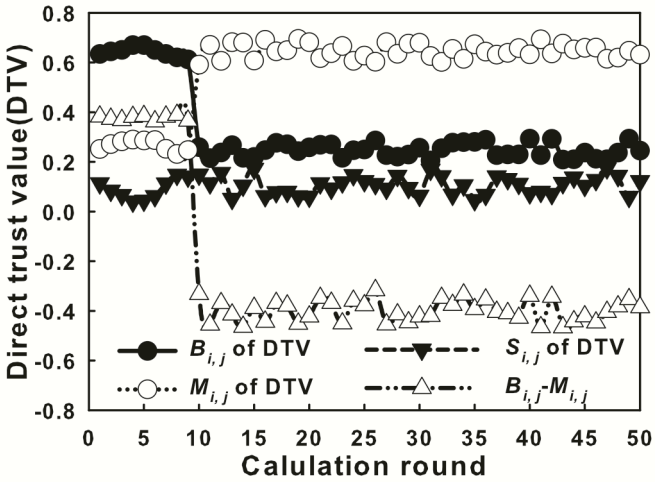


Fig. 7. Transition of DTV on black hole nodes.

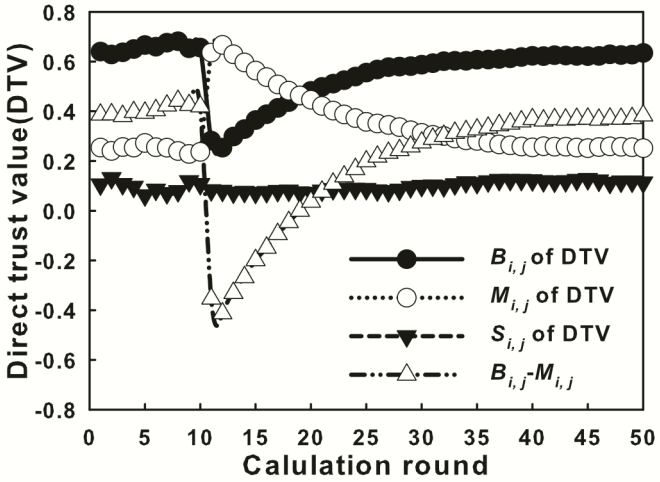


Fig. 8. Transition of DTV on gray hole nodes.

node establishes the route though node *j* and node *k*. If not, node *k* is stored in the MT as a malicious node.

V. Numerical Evaluation

Performance evaluation is firstly conducted to study the proposed DTV and ITV from the aspect of numerical analysis. Matlab is used as the analyser tool. For DTV algorithm, α_0=1, β_0=1 and γ_0=1 are set at initial phase. The historical evidence is given a high weight by assign a low value to θ_1=0.4, a high value to θ_2=0.9 to punish the nodes taking malicious action, and a punish value to θ_3=0.1. In each time period [T_n, T_{n+1}], a set of evaluation evidences is given for three kinds of nodes: normal nodes, black hole nodes, gray hole nodes.

1) For each normal node, a random function is exploited to generate a random number *B* with the probability between [0.6, 0.7] to represent its normal action rate. A random number *M* between [0.2, 0.3] is generated to represent its malicious action rate while the last number *S* between [0, 0.2] is left for the uncertain action rate. The relation between *B*, *M* and *S* is *S*=1-*B*-*M*.
2) For each back hole node, a random function is exploited to generate a random number *B* between [0.2, 0.3] to represent its normal action rate. A random number *M* between [0.7, 0.8] is generated to represent its malicious action rate while the last number *S* between [0, 0.2] is left for the uncertain action rate. The relation between *B*, *M* and *S* is also *S*=1-*B*-*M*.
3) For each gray hole node, firstly it acts as a normal node and all the action rates are generated as in 1), while it acts as a black hole node for a certain time and also follow the action rates in 2), then it acts as a normal node again.

For the ITV algorithm, it is supposed that each recommendation node is given a high reputation because they are all supposed to have been trusted. However, their reputations are different values generated randomly.

1) For normal recommendation node, it will observe the two-hop node based on its own observation. The reputation of the node under observation is given as defined in the front according to its behaviours.
2) If a malicious recommendation node is trying to deceive, it scores a low reputation to a normal node same as what is define as a black hole node or gray hole node, while a high reputation to a malicious node.

A. DTV Performance Evaluation

Figure 7 shows the performance of DTV with the black hole node. The black hole node acts as a malicious node from the 11st round until the last 50th round. As is described previously, the DTV of a neighbour node *j* calculated by node *i* consists of three parts: $B_{i,j}$, $M_{i,j}$ and $S_{i,j}$. It is apparent that $B_{i,j}$ decreases sharply from 0.6 and is stable at about 0.2, meanwhile, $M_{i,j}$ increases suddenly from 0.3 and finally rests at around 0.7. $B_{i,j}$-$M_{i,j}$ also drops from minus 0.4 to around minus 0.4. Based on the explanation of Figure 7, some key parameters in the decision part of the DTV algorithm can be set as: η_1 and η_2 is around minus 0.5 and minus 0.2, while ε_1 is around 0.3. In this case, the black hole node is very easy to be filtered out.

Figure 8 shows the performance of DTV with the gray hole node. As is described in the simulation environment, the gray hole node firstly acts as a normal node in the first 10 rounds. The malicious node takes action from 10th round to 12th round. After that, the gray hole node acts as normal as possible. It is apparent that $B_{i,j}$ decreases sharply while $M_{i,j}$ increases immediately. Meanwhile, $B_{i,j}$-$M_{i,j}$ also drops from 0.4 to minus 0.5 at the same time. However, $B_{i,j}$-$M_{i,j}$ along with $B_{i,j}$ increase at a very low speed compared with their decrease of the value. It is easy to find that the proposed method makes it difficult for the gray hole node to get a high reputation on DTV. The mechanism is so sensitive that DTV changes dramatically whenever the node drops packets. However, it is difficult to restore its former reputation in a short time period. Based on the previous explanation of Figure 8, some key parameters in the decision part of the DTV algorithm can be appropriate as follows: η_1 to be around 0.55, η_2 to be around minus 0.3, and ε_1 to be around 0.15. In this case, the gray hole node is very easy to be filtered out.

Based on the numerical analysis of both black hole attack and gray hole attack, the key parameters in the decision part of the DTV algorithm are set to be: η_1=0.55, η_2=-0.25 and ε_1=0.2.

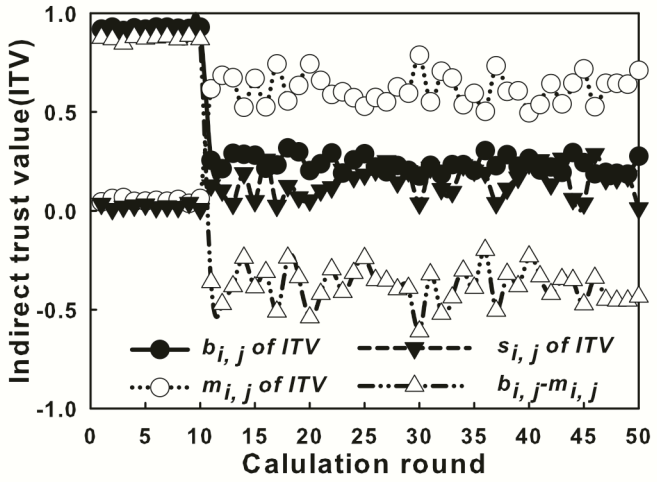


Fig. 9. Transition of ITV on black hole node with 2 benevolent recommenders and 1 deceiving recommender.

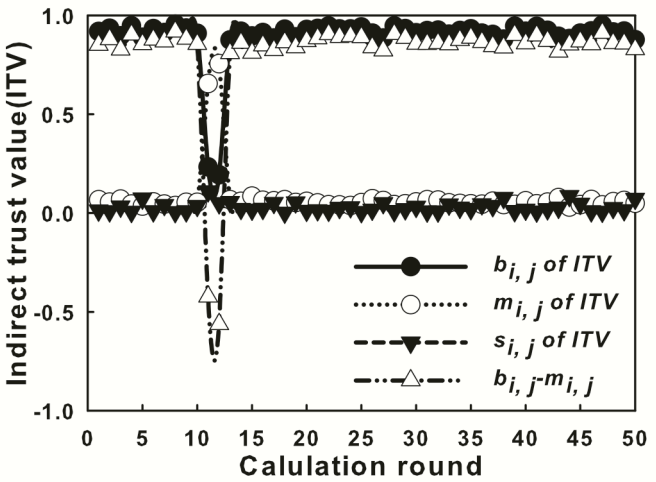


Fig. 10. Transition of ITV on gray hole node with 2 benevolent recommenders and 1 deceiving recommender.

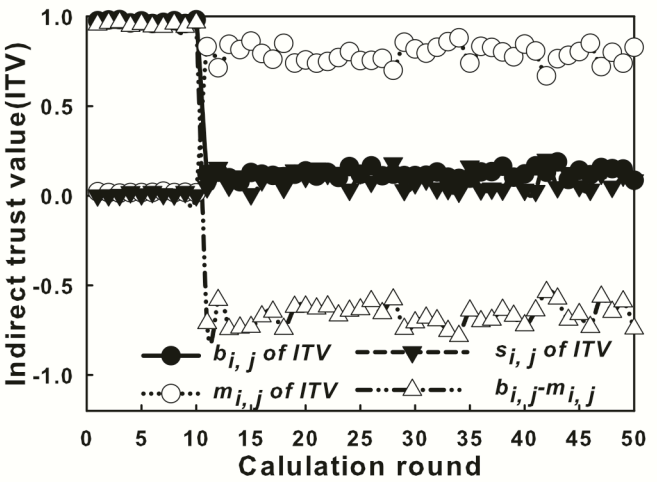


Fig. 11. Transition of ITV on black hole node with 3 benevolent recommenders and 1 deceiving recommender.

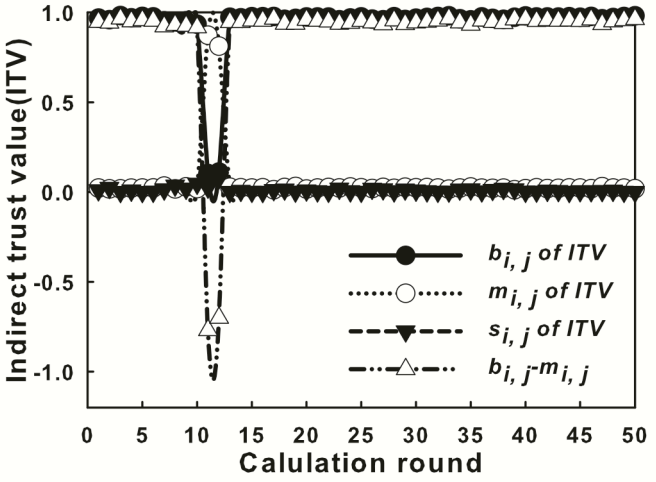


Fig. 12. Transition of ITV on gray hole node with 3 benevolent recommenders and 1 deceiving recommender.

B. ITV Performance Evaluation

Figure 9 shows the performances of ITV influenced by the deceiving nodes under black hole node. For the proposed ITV, it is set that there are totally 3 nodes acting as the recommendation nodes, among which 1 node is cheating. The two-hop node takes black hole action from round 11 to the end. As is described previously, the ITV of a two-hop neighbour node k calculated by node i consists of three parts: $b_{i,k}$, $m_{i,k}$ and $s_{i,k}$. $b_{i,k}$ is decreasing from the level of 0.9 to around 0.2. $m_{i,k}$ increases from 0.05 but always maintains about 0.9. $s_{i,k}$ changes sharply from 0.05 to 0.2, approximately. After the proposed ITV is implemented, although the deceiving node keep on cheating, the values of $b_{i,k}$, $m_{i,k}$, and $s_{i,k}$ change slowing. The enhancement of the false recommended reputation is minimized. Based on the Figure 9, some key parameters are set to be: δ_1 about 0.9, δ_2 around minus 0.5 and ε_2 is around 0.3.

Figure 10 shows the performances of ITV influenced by the deceiving nodes under gray hole node. For the proposed ITV, it is set that there are totally 4 nodes acting as the recommendation nodes and 1 node is cheating among them. From the result, $b_{i,k}$ first changes in a low speed while still no more than 0.8, then it drops sharply when the two-hop takes malicious action. $m_{i,k}$ increases sharply from 0.05 while always maintains more than 0.9. $s_{i,k}$ changes slightly from 0.05 to 0.2, approximately. Under the proposed ITV, although the deceiving node keeps on cheating, the values of $b_{i,k}$, $m_{i,k}$, and $s_{i,k}$ change slowly. The gray hole node acts as a normal node in the first 10 rounds. The malicious node takes action from 10th round to 12th round. After that, the gray hole node acts as normal as possible. It is apparent that $b_{i,j}$ increases sharply to nearly 0.9, while $m_{i,j}$ decreases immediately to nearly 0.05. Meanwhile, $b_{i,j}$-$m_{i,j}$ also drops from 0.9 to minus 0.7 at the same time. Thus, the enhancement of the falsely recommended ITV is minimized. Based on the analysis of Figure 10, some key parameters are set to be: δ_1 is around 0.8, δ_2 is around minus 0.5 and ε_2 is around 0.1.

Figure 11 and figure 12 are the performances of ITV influenced by deceiving nodes under black hole and gray hole, respectively. Same as what is analysed in figure 9 and figure 10, it is easy to find key parameters to be set. In Figure 11, key parameters are set to be: δ_1 is around 0.9, δ_2 is around minus 0.5 and ε_2 is around 0.25. In Figure 12, δ_1 is around 0.9, δ_2 is around minus 0.5 and ε_2 is around 0.25.

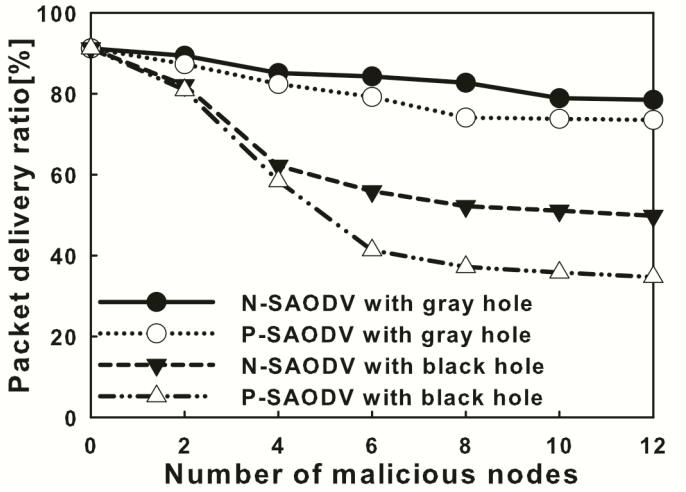


Fig. 13. Packet delivery ratio with single-attack malicious nodes.

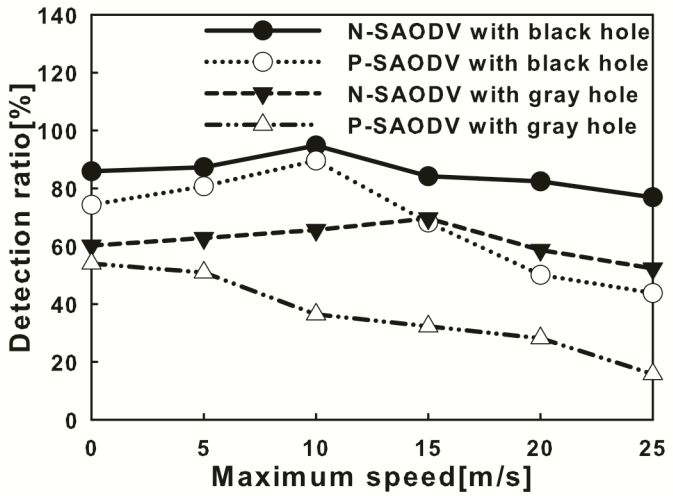


Fig. 14. Packet delivery ratio with single-attack malicious nodes.

Based on the numerical analysis of both black hole attack and gray hole attack, some key parameters in the decision part of the ITV algorithm are set to be: δ_1=0.7, δ_2=-0.3 and ε_2=0.35.

VI. Network Simulation Evaluation

As a second evaluation, the proposed mechanism is implemented in AODV using simulator GloMoSim2.03 to study the packet delivery ratio and detection rate. The parameters are set as in Table 3.

A. Single Attack Performance Evaluation

Figure 13 shows the packet delivery ratio with single-attack black hole node or gray hole node. P-SAODV stands for the AODV protocol with the security mechanism in the previous work. N-SAODV stands for the newly proposed method in this paper. The packet delivery ratio decreases with the increase of the number of malicious nodes in the network. Newly proposed SAOVE detection mechanism will increase the packet delivery ratio more than that of the previous work, in both cases of black hole node and gray hole node. What's more, the black hole case, packet delivery rate decreases more sharply than that in the gray hole case, for the reason that black hole node takes action persistently while gray hole node takes action selectively. Figure 14 shows the detection ratio of P-SAODV and N-SAODV with single-attack black hole node or gray hole node. The detection ratio firstly increases with the increase of the maximum speed of each node, but then it decrease, which is caused by the increase of the packets dropping between nodes. Form these two aspects, it is easy to find that new method shows better performance compared with previous one.

TABLE 3
Simulation Parameters

Parameters	Setting
Simulator	GloMoSim2.03
Routing protocol	P-SAODV／N-SAODV
Mac protocol	IEEE 802.11
Simulation area	1000m×1000 m
Node placement	Random
Number of nodes	50
Transmission range	180m
Maximum speed	10m/s
Traffic type	CBR (UDP)
Packet rate	2 packets/s
Data payload	512bytes/packets
Pause time	10s
Simulation time	1000s
Mobility model	Random waypoint

B. Cooperative Attack Performance Evaluation

Figure 15 shows the packet delivery rate with cooperative attack malicious nodes. The packet delivery ratio decreases with the increase of the number of malicious nodes in the network. Newly proposed SAOVE detection mechanism will increase the packet delivery ratio more than that of the previous work, in both cases of black hole node and gray hole node. Figure 16 shows the detection ratio of P-SAODV and N-SAODV with cooperative-attack black hole node or gray hole node. The detection ratio firstly increases slightly with the increase of the maximum speed of each node, but then it decrease. The strategy can also reduce the impact from the deceiving neighbour nodes and take advantages of the recommended reputation to make the detection determination more rationally. Form the two aspects, it is easy to find that new method shows better performance compared with the previous one. However, compared with the single-attack, the cooperative-attack is harder to detect even with the new method.

VII. Conclusions

In this paper, the problem of black hole attack and gray hole attack are discussed and two algorithms, NNOM-based DTV and NRTM-based ITV are proposed. The proposed DTV can be used to detect the gray hole attacks in the networks. The proposed ITV aims at the recommendation of cheating neighbour nodes. If there is no such recommendation node or

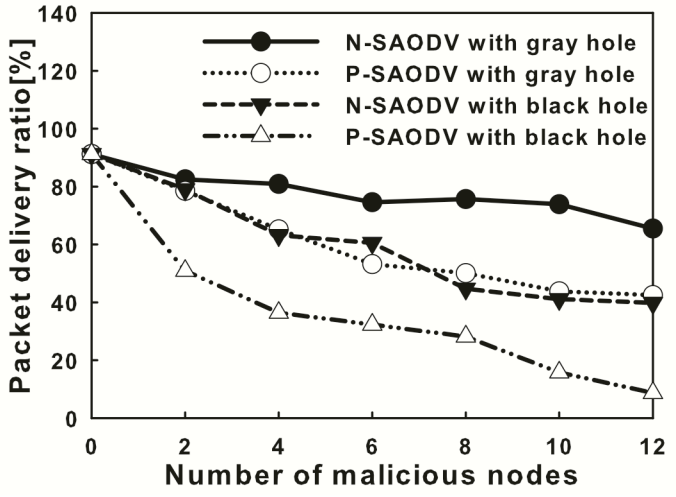


Fig. 15. Packet delivery ratio with cooperative-attack malicious nodes.

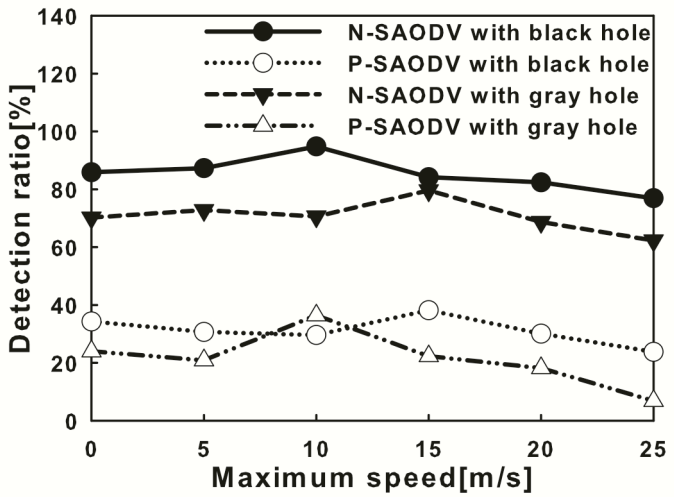


Fig. 16. Detection ratio with cooperative-attack malicious nodes.

the cheating nodes are too many, the proposed ITV may not take effects. For the future study, it may find another better method instead of the evaluation difference method. Furthermore, we would like to apply this trust management strategy into wireless sensor network (WSN) where the network structure is similar to MANET. Some other problems such as energy should also be taken into consideration.

REFERENCES

[1] B. Yang, R. Yamamoto, and Y. Tanaka, "A Trust-aware management strategy against black hole attacks in MANET," IEICE Commun. Society Conf., no. BS-6-39, pp S-106-S-107, Sept. 2011.

[2] S. Ganeriwal, L. K. Balzano, M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," ACM Trans. Sensor Netw., vol. 4, pp. 1-37, June 2008.

[3] A. P. Dempster, "Upper and lower probabilities induced by a multivalued mapping," The Annals of Mathematical Statistics, vol. 38, no.2, pp.325-339, April 1967.

[4] A. L. Jousselme, D. Grenier, E. Bosse, "A new distance between two bodies of evidence," Information Fusion Journal by Elsevier, vol. 2, pp.91-101, June 2001.

[5] D. Djenouri, L. Khelladi, A. N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," IEEE Commun. Surveys and Tutorials, vol. 7, pp. 2-28, fourth quarter 2005.

[6] A. D. Wood, J. A. Stankovic, "Denial of service in sensor networks," Computer Society by IEEE , vol. 35, pp. 54-62, Oct. 2002.

[7] S. D. Roy, S. A. Singh, S. Choudhury, "Countering sinkhole and black hole attacks on sensor networks using dynamic trust management," Comput. and Commun. by Elsevier, pp. 537-542, July 2008.

[8] T. Zahariadis, P. Trakadas, S. Maniatis, "Efficient detection of routing attacks in Wireless Sensor Networks," Systems, Signals and Image Processing IWSSIP, pp. 1-4, June 2009.

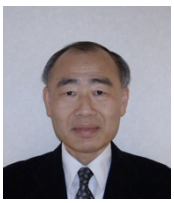
[9] H. Chen, "Task-based trust management for wireless sensor network," Int. J. of Security and Its Applications SERSC, vol. 3, No. 2, April 2009.

[10] P. B. Velloso, R. P. Laufer, D. de O Cunha, O. C. M. B. Duarte, G. Pujolle, "Trust management in mobile ad hoc networks using a scalable maturity-based model," IEEE Trans. on Netw. and Service Management, vol. 7, pp. 172-185, Sept. 2010.

[11] B. Y. Yan, F. Y. Liu, M. J. Deng, J. L. Zhou, W. Lu. "Trust model based on risk evaluation in wireless sensor networks," J. of Central South University, vol. 42, no. 6, pp. 1657-1662. June 2011.

Bo Yang received his B. E. degree in computer science and technology from Xi Dian University, Xi'an, China, in 2009. He received his second B.E. degree in economics from Xi'an Jiaotong University, China, 2012. Currently, he is working toward the M.E. degree in the Global Information and Telecommunication Studies, Waseda University, Tokyo, Japan. He won the ICACT best paper award in Feb. 2012. His present research emphasizes on the study of security problems in the wireless networks, such as ad hoc networks, MANETs, WSNs etc.

Ryo Yamamoto received his B.E. and M.E. degree in electronic information systems from Shibaura Institute of Technology, Tokyo, Japan, in 2007 and 2009. He is presently a research associate of Global Information and Telecommunication Institute, Waseda University. He received the IEICE young researcher's award in 2010. His current research interests are mobile ad hoc networks and cross-layered protocols.



Yoshiaki Tanaka received the B.E., M.E., and D.E. degrees in electrical engineering from the University of Tokyo, Tokyo, Japan, in 1974, 1976, and 1979, respectively. He became a staff at Department of Electrical Engineering, the University of Tokyo, in 1979, and has been engaged in teaching and researching in the fields of telecommunication networks, switching systems, and network security. He was a guest professor at Department of Communication Systems, Lund Institute of Technology, Sweden, from 1986 to 1987. He was also a visiting researcher at Institute for Posts and Telecommunications Policy, from 1988 to 1991, and at Institute for Monetary and Economic Studies, Bank of Japan, from 1994 to 1996. He is presently a professor at Global Information and Telecommunication Institute, Waseda University, and a visiting professor at National Institute of Informatics. He received the IEEE Outstanding Student Award in 1977, the Niwa Memorial Prize in 1980, the IEICE Achievement Award in 1980, the Okawa Publication Prize in 1994, the TAF Telecom System Technology Award in 1995 and in 2006, the IEICE Information Network Research Award in 1996, in 2001, in 2004, and in 2006, the IEICE Communications Society Activity Testimonial in 1997 and in 1998, the IEICE Switching System Research Award in 2001, the IEICE Best Paper Award in 2005, the IEICE Network System Research Award in 2006, in 2008, and in 2011, the IEICE Communications Society Activity Award in 2008, the Commendation by Minister for Internal Affairs and Communications in 2009, and the APNOMS Best Paper Award in 2009. He is a Fellow of IEICE.

A Global Mobility Scheme for Seamless Multicasting in Proxy Mobile IPv6 Networks

Hwan-gi Kim*, Jong-min Kim*, Hwa-sung Kim*

** Dept. of Electronics and Communications Engineering, Kwangwoon University, Seoul, Korea*

Hwangi9999@gmail.com, sazemic@kw.ac.kr, hwkim@kw.ac.kr

***Abstract*— Recently, Proxy Mobile IPv6 (PMIPv6) has been drawing attention as a mobility management protocol to effectively use the limited wireless resources. And, there have been some researches to apply PMIPv6 to multicasting, which is core technology of Internet broadcast system. However, PMIPv6 based multicasting cannot support the global mobility directly between different PMIPv6 domains because PMIPv6 is basically designed for local mobility in single PMIPv6 domain. Moreover, PMIPv6 based multicasting causes the disconnection of services because it does not solve problems of packet loss during binding and group joining procedure. In this paper, we propose a global mobility scheme that supports the seamless multicasting service in PMIPv6 networks. The proposed scheme supports the global mobility due to the addition of extra signalling messages between LMAs. Also, it achieves low latency because it performs fast binding and group joining procedure. We present the simulation results which show that the proposed scheme achieves the global mobility with low latency through the NS-2 simulation.**

***Keywords*— Proxy Mobile IPv6, Multicast Mobility, Global Mobility, Seamless Service, Packet loss**

I. INTRODUCTION

Recently, communication business is rapidly changed from wired network market to wireless mobile network market. Especially, mobile network environment is gaining attention nowadays, as the portable device such as smart phones and PDAs have been popular recently. In mobile networks, VOD and VoIP have been the main services. But recently, mobile broadcast services like a mobile IPTV are gaining attention in mobile networks.

Mobile IPTV is an IP-based service unlike existing mobile services such as DMB, and it is suitable service to All-IP next generation networks. Mobile IPTV service has weakness in that it has service disconnection problem due to the IP address change while the mobile terminal moves. In order to solve this problem, IETF(Internet Engineering Task Force) proposed Mobile IPv6(MIPv6)[1] to support mobility regardless of IP address change.

MIPv6 is a mobile-controlled mobility management protocol in that mobile node recognizes the handoff by itself and it performs the handoff procedure. But MIPv6 needs to be implemented in the mobile node and it needs many signalling in order to provide the mobility of the mobile devices. These problems make limited link resource overloaded. In order to solve these problems, IETF NETLMM (Network-based Localized Mobility Management) WG (Working Group) proposed Proxy Mobile IPv6 (PMIPv6)[2].

Basically, PMIPv6 is a network-controlled mobility management protocol. PMIPv6 provides mobility to Mobile Node(MN) using two kinds of routers: Mobile Access Gateway(MAG) and Local Mobility Anchor(LMA). MAG performs signalling procedure for MN's movement. LMA performs agent role of MNs. When MN moves, MAG recognizes that MN is moving, and MAG decides if means handover or not. If it is handover, MAG performs handover procedure with LMA. This handover procedure could reduce many signals between MAG and MN. But if PMIPv6 domain gets too wider, routing overhead gets too bigger. So, PMIPv6 assumes that the movements occur only in a PMIPv6 domain[2]. This problem is a critical weakness when adopting the multicast to PMIPv6 networks in order to provide next generation multimedia service. Therefore PMIPv6 needs to provide global mobility as well as local mobility without binding delay and packet loss due to the mobility. In this paper, we propose a seamless multicast scheme which supports global mobility in PMIPv6 networks.

The remainder of the paper is organized as follows. In section 2, as the related works, we will explain about the PMIPv6 and PMIPv6 based global multicast schemes. In section 3, we will explain about the proposed global mobility scheme for seamless multicast service in PMIPv6 networks. Next, in section 4, Simulation results of the proposed scheme will be explained. And then, in section 5, we will conclude this paper.

II. RELATED WORKS

A. Proxy Mobile IPv6

PMIPv6 was designed to provide the network-based IP mobility to MN in a topologically localized domain, without

Manuscript received June 30, 2012. This work was supported in part by the Kwangwoon University Industry-Academic Collaboration Foundation, 2012.

Hwan-gi Kim is with the Dept. of Electronic and communications Engineering, Kwangwoon University, Seoul, Korea (e-mail: hwangi9999@gmail.com)

Jong-min Kim was with the Dept. of Electronic and communications Engineering, Kwangwoon University, Seoul, Korea (sazemic@kw.ac.kr)

Hwa-sung Kim is a professor at Dept. of Electronics and communications Engineering, Kwangwoon University, Seoul, Korea (Tel: +82-02-940-5442; e-mail: hwkim@kw.ac.kr).

requiring the MN to participate in any IP mobility related signalling. Existing host based mobility protocols have some weaknesses in that it needs many signalling between MN and network in order to provide the mobility of the MN, and this makes limited link resource overloaded. In order to remedy the weaknesses of MIPv6, PMIPv6 makes the network mainly perform the signalling that is needed to provide the mobility instead of MN. So, MN can be provided the mobility without implementation of the complicated signalling function.

The core functional components used to support mobility in PMIPv6 are the Policy Store (PS), Local Mobility Anchor (LMA), and Mobile Access Gateway (MAG). Figure 1 shows the PMIPv6 network. PS is the entity that manages an MN's authentication and maintains the MN's profile which is a set of parameters configured for a given MN. Meanwhile, MAG performs the role of typical access router that detects the movement of MN and performs the MN's location update by sending mobility related signals to the MN's LMA on behalf of the MN. Also, the MAG ensures that an MN can obtain an address from its Home Network Prefix (HNP) and receive its HNP anywhere within the PMIPv6 domain. As a result, the MN believes it is using the same link obtained with its initial address configuration, even after changing its point of attachment within the network. On the other hand, LMA is similar to HA (Home Agent) in MIPv6, however, it has additional capabilities required to support PMIPv6. The main role of the LMA is to maintain reachability to the MN's address while the MN moves around within the PMIPv6 domain. The LMA includes a Binding Cache Entry (BCE) for each currently registered MN.

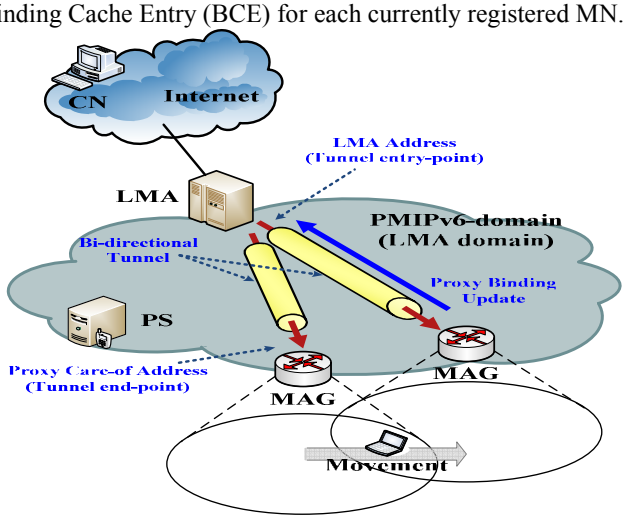


Figure 1. PMIPv6 network

B. *Supporting Global Mobility in PMIPv6*

As mentioned in introduction, PMIPv6 was designed to provide the network-based IP mobility to MN in a topologically localized domain[2]. However, MN can move out to other domain frequently in real situation. Therefore, the research for global mobility in PMIPv6 is required because there is no protocol definition to support the global mobility. IETF NETLMM WG has researched this problem.

C. *Interaction between PMIPv6 and MIPv6*

IETF NETLMM WG is standardizing the interaction method between PMIPv6 and MIPv6 to support the global mobility [3]. In this method, a HA is designated in the PMIPv6 domain where MN enters for the first time. Thereafter, LMA in the domain, where MN moves, sends the binding request massage to MN's HA. Figure 2 shows the detail interaction method between PMIPv6 and MIPv6.

At first, MN is connected to MAG1. MAG1 that recognizes the connection of MN by link layer signal, sends PBU(Proxy Binding Update) massage to LMA1 for Binding Update. Then LMA1 completes Binding Update by registering MN's address. This procedure is sufficient for Binding Update in existing PMIPv6 protocol. In the case of PMIP-MIP interaction for global mobility, however, LMA1 has to perform binding Update for MIPv6 with HA. After Binding Update between HA and LMA1, LMA1 need to send PBA massage to MN through MAG1 in order to complete Binding Upadate procedure. Thereafter, MN can be serviced.

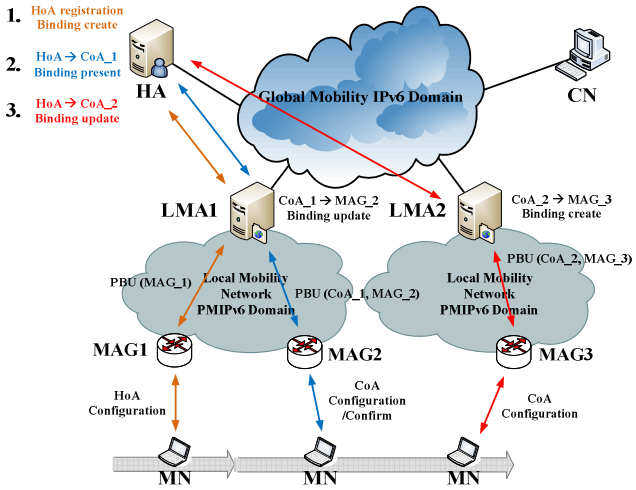


Figure 2. PMIP-MIP Interaction

If MN moves to MAG2, Binding Update is not required because it is not global mobility. But MN's COA(Care-of-Address) has to be changed to MAG2's address. Therefore MAG2 performs Binding Update by sending PBU message to LMA1. Then LMA1 requests Binding Update to HA for COA change.

If MN moves to MAG3, LMA2 requests Binding Update to HA because PMIPv6 domain is changed. HA, which received Binding Update, recognizes that the path to MN was changed. Also it recognizes that COA was changed to MAG3's address. HA redirects the packets destined to MN to new domain. Therefore, MN can be serviced even in case of global mobility without performing any signalling according to MN's movement.

D. *Definition of new agent*

PMIP-MIP interaction is a global mobility method proposed by IETF NETLMM WG, in which PMIPv6 is combined with MIPv6 signalling.

This method has a problem in that unnecessary delay is occurred by additional signals between LMA and HA even though the advantage of PMIPv6 protocol is maintained because MN does not participate to the binding update procedure. Therefore new method called I-PMIP that add the new agent function to router, was proposed for solving unnecessary delay problem[4]. I-PMIP provides the global mobility by giving the role of HA to the first LMA connected for the first time instead of using the separate HA[4].

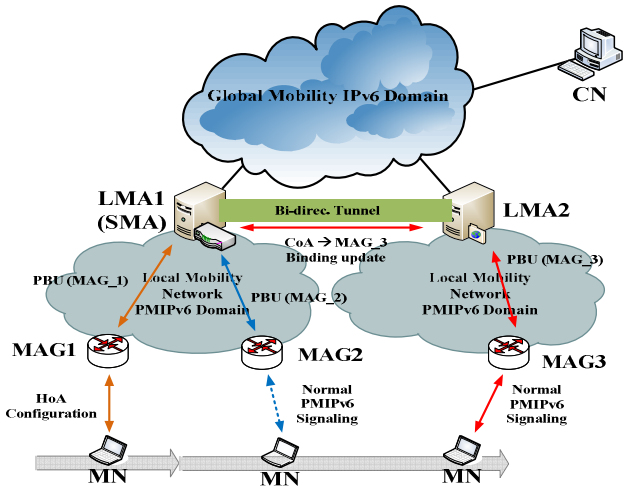


Figure 3. I-PMIP operation

Figure 3 shows the I-PMIP operation. When MN is connected to first LMA, MN receive the service according to PMIPv6 protocol. As shown in figure 3, the location of MN is registered using PMIPv6 signalling messages when a MN is connected to MAG1. Also, the mobility is supported using PMIPv6 signalling messages when MN moves to MAG2. On the other hand, LMA2 requests the binding of MN to LMA1, when MN moves continuously and finally connects to MAG3. This is the core aspect of I-PMIP operation. The first LMA, to which MN is connected for the first time, is called SMA (Session Mobility Anchor) and it provides seamless session to MN even in the case of global mobility..

The first LMA, to which MN is connected for the first time, carries the role of SMA that is similar to HA of MIPv6. Therefore, all packets destined to MN from outside pass through SMA. And, LMA of new PMIPv6 domain requests the binding to this SMA when MN moves away from PMIPv6 domain where SMA resides. After the binding, the bi-directional tunnel is established between SMA and new LMA. Thereafter, all packets destined to MN are transmitted to new LMA through bi-directional tunnel. If MN moves continuously and is connected to LMA of another PMIPv6 domain, bi-directional tunnel is established again.

E. Problems of PMIP-MIP Interaction and I-PMIP

PMIP-MIP Interaction adds the MIPv6 signalling to PMIPv6 signals to provide the global mobility. But adding MIPv6 signal occur unnecessary delay because of binding between LMA and HA. This unnecessary delay causes the problem when PMIP-MIP Interaction is applied to multicasting. When a MN receiving multicast service, is connected to LMA of new PMIPv6 domain but LMA is not a member of multicast group, group joining procedure is occurred. In this case, new LMA requests the binding to HA, and group joining procedure is performed in turn. This leads to the delay of group joining and service disconnection because MN is not able to receive any packet before group joining procedure is completed.

In contrast to PMIP-MIP interaction, I-PMIP does not incur unnecessary delay because it does not require signalling with HA. But, I-PMIP causes the delay if global mobility occurs frequently because the continued bindings to SMA are required. Also, it does not solve the service disconnection problem caused by group joining operation after the binding, because it still needs the binding for global mobility, it reduces the unnecessary signalling with HA by using SMA though.

In this paper, we propose an effective global mobility scheme, which performs the fast binding and group joining procedure, without binding to HA or new agent. Also, the proposed scheme does not incur any packet loss.

III. PROPOSED SCHEME FOR GLOBAL MOBILITY AND SEAMLESS MULTICAST IN PMIP

A. LMA option massage for global mobility

In this section, we explain newly added massage for supporting global mobility without HA and new agent. Using this added massage, each LMA identifies each other without HA and new agent.

Type	Length	Dist.	Pref.	r	Reserved
Valid lifetime					
LMA's Global Address (128 bits)					

Figure 4. LMA option massage format

A router sends RA(Router Advertisement) massage to all other routers for sharing its information. In the newly added massage shown in Figure 4, a LMA's global address option is added. Using this option, LMA configures the LMA entries of other LMA's global addresses in the same manner as their own MAG entry. LMA's global addresses are selectively stored as LMA entry by configuring based on Hop Count according to the distance field in the massage format because the distant LMA's global addresses does not need to be stored. Using this massage, LMAs are able to share each address and inform MN's movement.

B. global mobility for Seamless multicast service

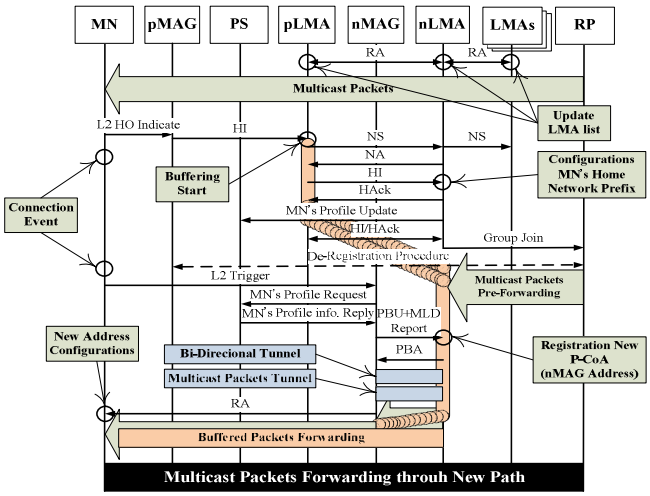


Figure 5. Seamless multicast for global mobility

Figure 5 shows the sequence diagram of global mobility for seamless multicast service. MN first joins to MAG, then its LMA(Previous LMA, p-LMA) provides multicast service to MN via MAG. It assumes LMAs have LMA entry by using new option massage in RA.

When MN moves away from p-MAG to other domain, it performs Figure 5 procedure.

MN recognizes decreasing signal strength from current AP. MN informs handover to its p-MAG via AP. Then p-MAG sends HI(Handover Initiate) massage to p-LMA about MN's handover. This This HI massage includes n-MAG's address as MN's new MAG. A p-LMA checks its own MAG entry whether n-MAG's address is included same domain. If n-MAG's address is not same domain, p-LMA pretends MN's global mobility. Then p-LMA sends NS(Neighbor Solicitation) massage to LMAs that it is included a list of LMA entry. And LMAs that received NS from p-LMA, check each own LMA entries. If one of LMAs discovers n-MAG's address from its own MAG entry, it sends NA(Neighbor Advertisement) massage to p-LMA. Then p-LMA knows MN moves which LMA. And p-LMA sends HI massage to n-LMA for fast handover procedure. In this HI massage, includes MN's ID and multicast information. After receiving HI massage from p-LMA, n-LMA sends HACK(Handover Acknowledgement) and pretends MN's handover.

On the other hand, p-LMA starts buffering multicast data that will forward to MN, when receive HI massage from p-MAG.

It is for seamless multicast service without data loss. P-LMA continues buffering until n-LMA send Hack massage to p-LMA. If p-LMA receives Hack massage, p-LMA sends buffered data to n-LMA.

During buffered data is transmitted to n-LMA, n-LMA updates newly configured MN's information to PS(Policy Store) server. After updating, n-LMA informs that update procedure is completed to p-LMA by HI massage. After that, n-LMA performs group rejoining procedure. Then n-LMA receives multicast data from source. And n-LMA also buffered data from p-LMA sending.

When MN handovers to n-MAG, n-MAG accesses to PS server and request MN's information. After that, n-MAG sends PBU massage to n-LMA for MN's binding update. At this time, n-MAG sends MLD(Multicast Listener Discovery) report massage[5](n-MAG could know MN's multicast information through PS server) to n-LMA at same time. After receiving PBU and MLD massages, n-LMA could know MN is joined its own domain then send PBA massage to n-MAG. And n-LMA starts two channel configuration procedure. One of them is Bi-Directional Tunnel for existed PMIPv6 protocol, another tunnel is Multicast Packet Tunnel as we defined.

After channel configuration procedure, n-LMA sends buffered data to MN through n-MAG. Finally, MN has been moved global mobility and received seamless multicast service.

IV. SIMULATION

In order to evaluate the performance of proposed handover scheme, we use the NS-2 network simulator[6]. Figure 6 shows the topology used for the simulation. In Figure 6, MN starts moving from AP1 and moves to AP4 with constant velocity, 60m/s. And, MN is connected to MAG through layer 2 handover at intervals of about 60 sec. The parameters used for the simulation are shown in Table 1.

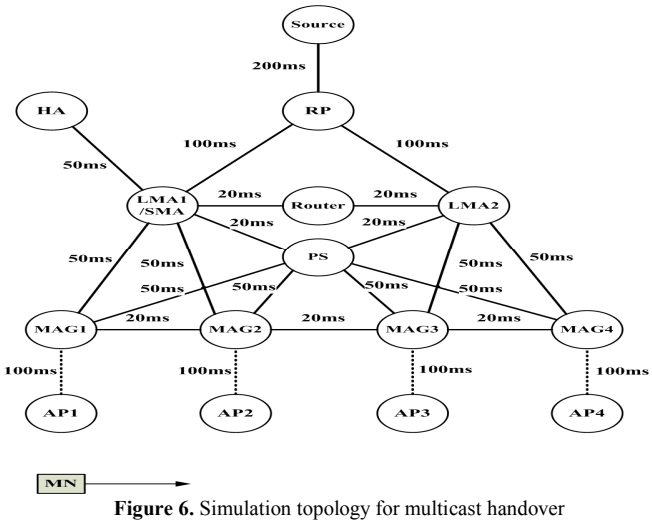


Figure 6. Simulation topology for multicast handover

Table 1. Simulation Parameter

Parameter	Value
Simulation time	300 sec
Distance between MAGs	5km
Link bandwidth	2Mbps
Velocity of MN	60m/s
Bit rate	CBR
Packet size	1Kbyte
Multicast routing protocol	PIM-SM

In order to evaluate that the proposed scheme can provide the seamless multicast service when the global mobility occurs, we measured the UDP Datagram ID, TCP Sequence Number, UDP and TCP Throughput during MN moves from MAG2 to MAG3.

Figure 7 shows the simulation results on UDP datagram ID that MN receives when source node sends the UDP traffic. As shown in Figure 7, PMIP-MIP interaction-based multicast cannot receive the UDP datagram from 120.2 second to 122.5 second. This data loss occurs because of the global binding delay among LMA2, LMA1 and HA after the layer 2 handover between APs and multicast group joining procedure delay. In case of I-PMIP-based multicast, packet loss occurs from 120.2 second to 122.1 second that is shorter than PMIP-MIP interaction-based multicast. This result is caused by the faster binding procedure of I-PMIP because binding is completed at LMA1 unlike PMIP-MIP Interaction. But, as shown in Figure 7, packet loss still occurs from datagram ID 62231 to 62250 in case of I-PMIP.

On the other hand, the proposed scheme can receive the UDP datagram during disconnection period from 120 second to 120.7 second by using buffering. That is, proposed scheme does not experience the packet loss thus provides the seamless service because the datagrams that are generated while MN is moving is saved and retransmitted.

This result affects the UDP throughput as shown in figure 8. The UDP throughput in PMIP-MIP Interaction scheme drops to zero for about 2000ms because of the effect of the global handover, which incurs the binding procedure with HA and group joining procedure after binding. Also, the UDP throughput in I-PMIP-MIP scheme drops to zero for about 1600ms because of the effect of the global handover, which incurs the binding procedure with SMA and group joining procedure after binding. However, the UDP throughput in the proposed scheme drops just for about 790ms because it processes the binding procedure and group joining procedure at the same time. We can also notice that the proposed scheme prevent the throughput from dropping to zero because it performs the buffering.

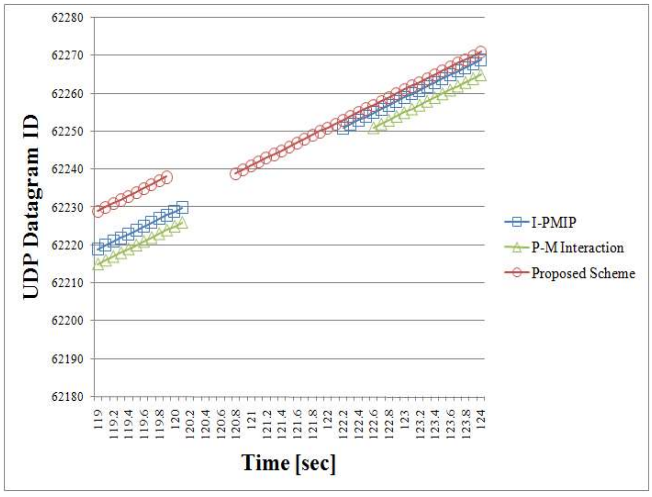


Figure 7. Comparison of UDP datagram ID

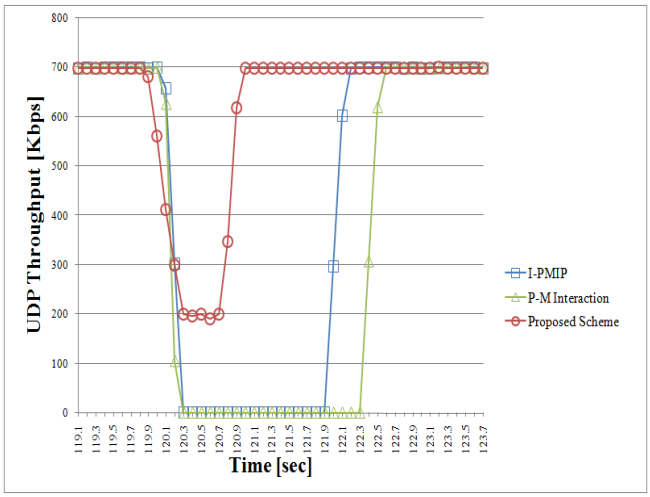


Figure 8. Comparison of UDP Throughput

Figure 9, 10 and 11 shows TCP sequence numbers that MN received. Figure 9 shows received TCP sequence number when P-M Interaction is used. When MN's global mobility is performed, binding delay with HA and group joining delay is occurred during 1990ms that is similar to UDP case. During this delay time, the packets sent by the source cannot be delivered to MN and these undelivered packets are retransmitted by TCP algorithm. These retransmission causes additional delay for packet delivery. Therefore TCP packets experience more delay than UDP packets. Figure 10 shows the received TCP sequence numbers that MN received when I-PMIP is used. I-PMIP also has binding and group joining delay during 1550ms and additional retransmission delay. As shown in Figure 11, however, the proposed low latency global mobility scheme shows relatively short delay due to the fast binding. Also, using buffering scheme, there is no need to retransmit the packets, which leads to seamless multicast service without additional delay.

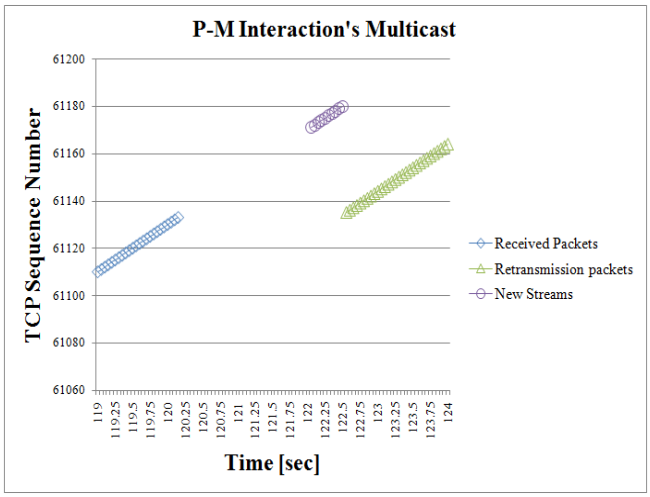


Figure 9. TCP sequence numbers in P-M Interactio

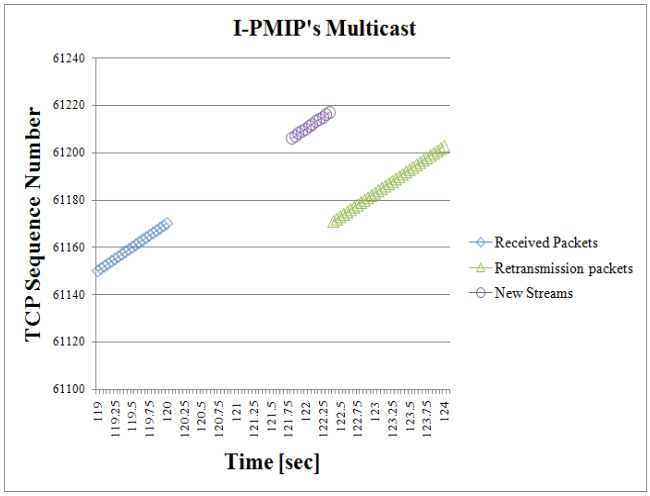


Figure 10. TCP sequence number in I-PMIP

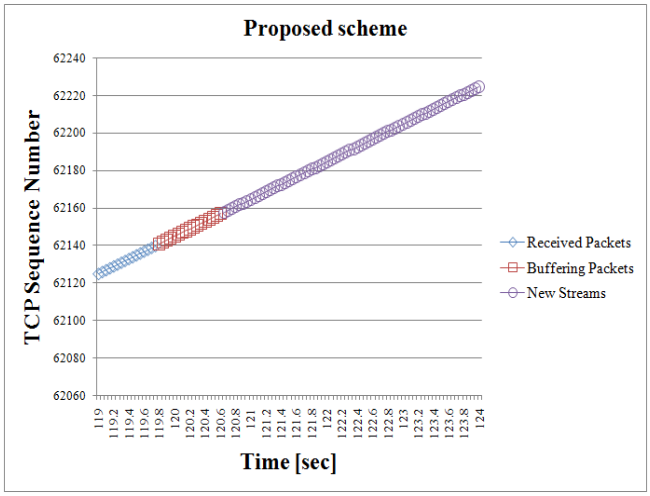


Figure 11. TCP sequence number in proposed Inter mobility scheme

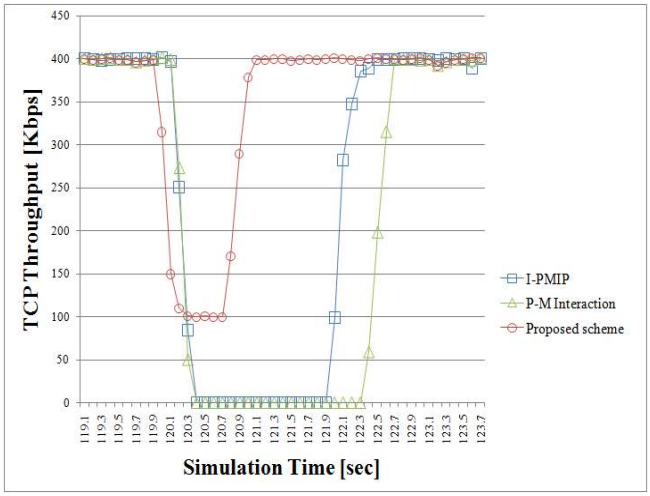


Figure 12. Comparison of TCP Throughput

Figure 12 shows comparison of TCP throughput for three methods. TCP throughput result is very similar to UDP throughput. P-M Interaction is falling down to 0 during 2000ms. And I-PMIP is falling down to 0 during 1600ms. But in proposed scheme, it shows that is not falling down to 0, even if throughput is falling down during 800ms. As a result, these throughput results show the proposed scheme is more effective than other two methods.

V. CONCLUSION

In this paper, we propose a new low latency global mobility scheme which supports seamless multicast service without out-of-sequence problem and packet loss in PMIPv6 networks. Before discussing the proposed scheme, the existing global mobility schemes in PMIPv6 networks are explained. The multicasting based on existing global mobility schemes has the problem in that it causes the unnecessary delay and service disconnection because the global binding to HA or new agent and the group joining procedure has to be occurred in turn. In the proposed scheme, however, the global mobility can be supported without extra global binding because each LMA can identify each other using LMA global address option added to RA massage format. Additionally, LMA could prevent the packet loss using buffering procedure during the global mobility procedure …..

Using the NS-2 simulation, we showed that the proposed scheme reduces the unnecessary delay that the existing global mobility methods have.

REFERENCES

[1] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6," IETF RFC 3775, Jun. 2004.
[2] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, "Proxy Mobile IPv6," IETF RFC 5213, Aug, 2008.
[3] G. Giaretta, "Interactions between PMIPv6 and MIPv6: scenarios and related issues," <draft-ietf-netlmm-mip-interactions-06>, May. 2010.
[4] N. Neumann, J. Lei, X. Fu, G. Zhang, "I-PMIP: An Inter-Domain Mobility Extension for Proxy-Mobile IP," IWCMC' 09, Jun. 2009
[5] R. Vida, L. Costa, "Multicast Listenet Discovery Version 2 (MLDv2) for IPv6," IETF RFC 3810, Jun. 2004
[6] "The Network Simulator-ns (version 2) website," http://www.isi.edu/nsnam.

Hwan-gi Kim is currently enrolled in M.Sc. program at the Dept. of Electronics and communications Engineering, Kwangwoon University, Seoul, Korea. His research interests include mobile network protocol, sensor network, context reasoning, augmented reality.

Jong-min Kim received the M.Sc degree at the Dept. of Electronics and communications Engineering, Kwangwoon University, Seoul, Korea. . His research interests include mobile network protocol, sementic web, context reasoning.

Hwa-sung Kim received Ph.D degree at the Dept. of Computer Science, Lehigh University, Bethlehem, PA 18015 USA. He is now a professor at the Dept. of Electronics and communications Engineering, Kwangwoon University, Seoul, Korea. His research interests include mobile network protocol, mobile web computing, embedded software

Alternatives to Network Selection in Heterogeneous Wireless Environments

Vinícius de Miranda Rios*, Claudio de Castro Monteiro**, Vanice Canuto Cunha***

**Information Systems Department, University of Tocantins, Palmas - TO - Brazil*

***Federal Institute of Education, Science and Technology of Tocantins, Computing Science Department, Palmas - TO - Brazil, ACM member*

****University of Brasilia, Electrical Engineering Department, Brasilia - DF - Brazil*

vinicius.mr@unitins.br, ccm.monteiro@acm.org, vanicecunha@gmail.com

***Abstract*—This article presents two proposals in order to solve the problem of choosing the best access network available in the environment where the user is located. One based on a combination of fuzzy logic technique with two decision-making methods, AHP (Analytic Hierarchy Process) and GRA (Grey Relation Analysis), and the other based only on fuzzy logic technique. In order to demonstrate the effectiveness of these proposals, they were compared with a third one, of the authors in [7], which uses a combination of AHP method with a cost function. The obtained results show that the two proposals presented in this paper are more efficient in sorting and selecting the best access network when compared to the third.**

***Index Terms*—Network selection, AHP, GRA, Fuzzy logic**

I. INTRODUCTION

With the emergence of wireless networks, users have become able to move into many different environments. This mobility has brought some challenges such as [1]: choosing the best access network, keeping the session to data transmission and allowing the mobile user to be always best connected anywhere and anytime on the best available access network (ABC conception – Always Best Connected).

In this sense, the next-generation wireless networks (NGWN) focus on the free users' movement between heterogeneous networks through mobile terminals (Notebooks, Netbooks, PDA - Personal Digital Assistant, cell phones, etc.) with network interfaces of different technologies (WWAN - Wireless Wide Area Network, WLAN - Wireless Local Area Network, WMAN - Wireless Metropolitan Area Network, etc.) allowing continuous access to real or not real time services, always aiming at the continuity of the service (seamless).

Keeping the service active while switching access networks is the function of one of the key parts of mobility management, called handover [2]. The handover function is to control exchanges between users' access points during a data transmission [1].

Manuscript received July 30, 2012. This work was supported in part by the UnB – University of Brasilia.

Vinícius de Miranda Rios is with the UNITINS – University of Tocantins, BR Brazil (+55 (63)-3218-4926; e-mail: vinicius.mr@unitins.br).

Claudio de Castro Monteiro is with the IFTO – Federal Institute of Education, Science and Technology of Tocantins, BR Brazil (+55 (63)-3229-2200; e-mail: ccm.monteiro@ acm.org).

Vanice Canuto Cunha is with the IFB – Federal Institute of Education, Science and Technology of Brasilia, BR Brazil (+55 (61)-2103-2154; e-mail: vanicecunha@gmail.com).

It can be classified into two types [3]: horizontal and vertical. The horizontal handover is designed to manage switching between similar network technologies (e.g. wi-fi (Wireless Fidelity) to wi-fi) during a data transfer, in which only the signal loss is the motivation for the exchange of access points, whereas the vertical handover aims to manage switching between different access technologies (e.g. wi-fi to 3G) during a data transmission, in which the use of preferred applications requiring certain thresholds for each requirement of QoS (Quality of Service) or the user preferences are the motivators for exchanging access points [4].

This access network exchange happens in three distinct steps, which are [2]:

- finding networks in the environment in which the mobile device is located;
- approaches to decision making/selection of the best available access network;
- the implementation of the change of the access points.

Therefore, the network selection, as an integrating and indispensable part of the handover management, aims to provide the mobile user with the best traffic condition access point, allowing applications, whether voice, data or video, to be transmitted with the required quality from source to destination.

The remainder of this paper is organized as follows: section 2 presents related work to the techniques used; section 3 describes the proposed network selection; the characterization of the experiments is shown in section 4; in section 5, the obtained results are displayed stating which proposal is the best; and finally, section 6 presents the conclusion and future work.

II. RELATED WORK

The authors in [11] make a comparison among the MADM, SAW, WP and TOPSIS methods, whose goal is to classify access networks in three different scenarios. In the first scenario, TOPSIS and SAW methods proved similar in classification of networks, while the WP method showed a slight variation in its classification. In the second scenario, where two networks are removed from the classification, the SAW and WP methods proved similar, while the TOPSIS method obtained a change in its classification for suffering from the problem of abnormality ranking. Finally, a distinction between the classifications obtained in the previous scenarios is presented in the third scenario, where the TOPSIS method proves to be more consistent in the variations, while the SAW and WP methods are constant with little variability in the classification of networks.

The network selection made by the authors in [12] is based on a fuzzy multiple criteria decision-making, where all the selected criteria are normalized by a normalization function and the result is fuzzified, generating a degree of membership between 0 and 1, which will be used to give weights to these criteria. Finally, the selection of the best access network is made by a cost function.

The network selection algorithm of the authors in [7] is premised on originally giving preference to the UMTS (Universal Mobile Telecommunications System) in case the wi-fi is not available, since the former has a larger geographical coverage and does not allow the mobile device to run out of connection. Thus, the environment where the terminal is located is composed of four networks: three wi-fi access points and a 3G base station (cellular network). Therefore, the mobile terminal is shifted 1000m, at an average speed of 1m/s, with 3G coverage during all its path, while the wi-fi network coverage is segmented.

Therefore, the mobile device only initializes the data collection in order to select the best access network when there is at least one wi-fi network available, when the signal limit is greater than the established limit and when it may possibly stay longer in this environment, avoiding the ping-pong effect, thus. After confirmation, the mobile device initiates the data collection.

The final decision on network selection shall be taken by the cost function (4), in which the weights used by w_j are given through the AHP method. In this way, the authors standardized parameters using the following assumptions:

The bigger, the better:

$$S(x_{ij}) = \frac{x_{ij}}{\max\{x_{ij} \mid i = 1,2,...,m\}} \quad (1)$$

The smaller, the better:

$$S(x_{ij}) = \frac{\min\{x_{ij} \mid i = 1,2,...,m\}}{x_{ij}} \quad (2)$$

Where x_{ij} express parameter *j* in network *i*.

The normalization of the parameters is:

$$N(x_{ij}) = \frac{S(x_{ij})}{\sum_{j=1}^{n} S(x_{ij})} \qquad i = 1,2,...,m \quad (3)$$

Therefore, the rate of network decision-making can be calculated as:

$$I_i = \sum_{j=1}^{n} w_j N(X_{ij}) \qquad i = 1,2,...,m \quad (4)$$

The values of each parameter used to select the best access network are characterized in Table I.

TABLE I.
NETWORK PARAMETERS

Parameters		UMTS	WLAN1	WLAN2	WLAN3
QoS	Available	0,4	20	10	30
factors	bandwidth				
	Delay	20	30	50	40
	Jitter	5	10	10	10
Cost		1	0,01	0,01	0,01
	Bit error rate	10^{-9}	10^{-6}	10^{-6}	10^{-5}
Reliability	Packet Loss	0,01	0,1	0,2	0,1
	Cell load	0,3	0,8	0,1	0,8
Securit		8	4	2	4

The entire article was implemented by using the EXCEL spreadsheet. There the data provided by the authors were inserted, as well as the values of the collected parameters and also the implementation of the AHP method and the above equations, which reached the same values of weights and results presented in the article.

The exception of results could be noticed in the normalization of parameters of the scenario when the mobile is in the area of WLAN2, WLAN3 and 3G network coverage. The parameters α, β, γ and δ, express the QoS factors, cost, reliability and security respectively. The values generated by our implementation differ from those provided by the article, as shown in tables II and III below.

TABLE II.
NORMALIZATION OF NETWORK PARAMETERS

Simulation Scenarios	α			β	γ			δ
UMTS	0.01	0.48	0.50	0	1	0.87	0.23	0.57
WLAN2	0.33	0.32	0.25	0.50	0	0.09	0.09	0.29
WLAN3	0.66	0.20	0.25	0.50	0	0.04	0.68	0.14

TABLE III.
OUR NORMALIZATION OF NETWORK PARAMETERS

Simulation Scenarios	α			β	γ			δ
UMTS	0.01	0.53	0.50	0	1	0.87	0.23	0.57
WLAN2	0.25	0.21	0.25	0.50	0	0.04	0.69	0.14
WLAN3	0.99	0.33	0.33	0.99	0	0.09	0.27	0.33

A big difference between the values generated by the normalization equation (3) of the authors in [7] in Table II can be observed in relation to our values presented in Table III. Therefore, the result we reached was that, in the scenario where the preference is for reliability and security, the mobile selected the 3G network all the times, whereas in the article there is a selection for WLAN2 network.

In addition, when we implement the article in a real testbed, we can observe that if there is a value of the collected parameters equal to 0, its final result will also be 0, thus affecting the choice of the best access network, as it is shown in section 5.

III. PROPOSALS

The proposals of this work are presented here with the intention of using the fuzzy logic, AHP and GRA for the composition of an architecture of network selection in heterogeneous wireless network environments.

A. Proposal 1- Network selection by using Fuzzy logic

The first network selection proposal aims to using only the technique of fuzzy logic considering the accurate output provided upon the input of raw data collected by the system, as it is illustrated in Figure 1.

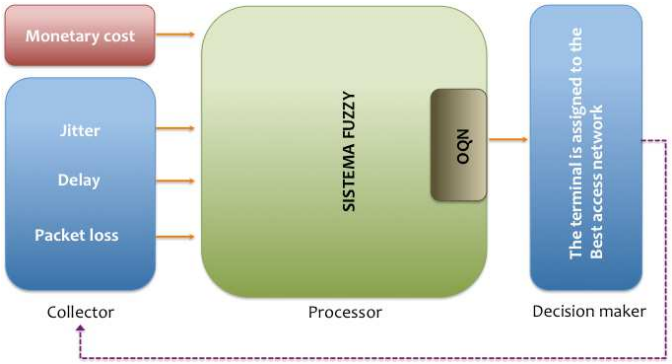


Figure 1. Architecture of proposal 1 using only fuzzy logic only.

Thus, the system is divided into three functional blocks, which are: the collector, processor and decision-maker.

Collector

The collector aims to collecting data on delay, jitter and packet loss, provided by the ping application, as it can be seen in Figure 2. The monetary cost parameter is fixed, so there is no need to be collected, but only informed by the mobile operator, taking the value of wi-fi networks equal to zero real and the values in networks 1 and 2 base stations equal to 89.9 and 79.9 brazilian reals, respectively, since only the access from the terminal to the access point is considered, i.e., the ICMP (Internet Control Message Protocol) requisitions of the ping (packet internet grouper) application will be transmitted from the client terminal to the interface output gateway, passing only by the access point it is connected.

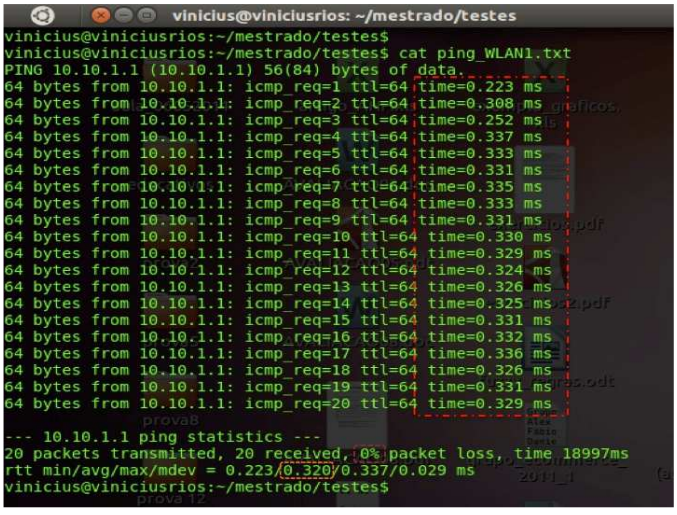


Figure 2. File with the collection of ICMP requisitions.

This collection takes place through two rounds of 10 ICMP requisitions, and because we are dealing with the sum of all end-to-end delay [8], the average RTT (Round Trip Time) values are also stored in each round.

TABLE IV.
PSEUDOCODE FOR COLLECTOR FUNCTION

```
collector(redes, iteracoes, rounds, ICMP, custo)
{
   while(n < rounds)
   {
      while(m < iteracoes)
      {
         redes.dados = requisicoes.ICMP;
         delay = f(redes.dados.delay);
         jitter = f(redes.dados.jitter);
         perda = f(redes.dados.perda);
         processor(redes, delay, jitter, perda, custo);
         n = n + 1;
      }
      m = m + 1;
   }
}
```

Processor

The processor aims to manipulate the data that is collected through the fuzzy logic technique in order to classify access networks in the environment the terminal is located. For this, audio thresholds were used in the fuzzy system, because they are already well known and documented and they also state that in an audio transmission (VoIP), the delay cannot be greater than 300ms, the jitter cannot be greater than 150ms and the packet loss may not exceed over 3% [9], [10], which makes the sound unintelligible to the human ear in such cases.

Under this assumption, each linguistic variable (jitter, delay, packet loss and monetary cost) has three linguistic terms in the fuzzy system, which are: low, medium and high, where the universe of discourse of each of them is within the thresholds of the audio traffic. Each of these terms was fuzzified with the function of triangular relevance and in accordance with the Mandani method inference on the obtained result, as it can be seen in Figure 3.

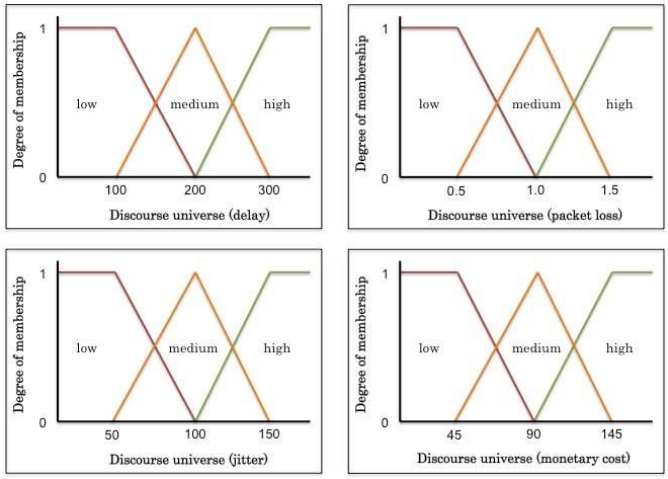


Figure 3. Fuzzification.

Each fuzzy subset within the discourse universe associated with the delay is composed of:

- low, between 0 and 200;
- medium, between 100 and 300;
- high, above 300.

But the discourse universe associated with the jitter is composed of:

- low, between 0 and 100;
- medium, between 50 and150;
- high, above 150.

The same happens in the discourse universe associated with the packet loss:

- low, between 0 and 1;
- medium, between 0.5 and 1.5;
- high, above 1.5.

And finally, the discourse universe associated with the monetary cost:

- low, between 0 and 90;
- medium, between 45 and 145;
- high, above 145.

Figure 4 illustrates the rules used in this proposal.

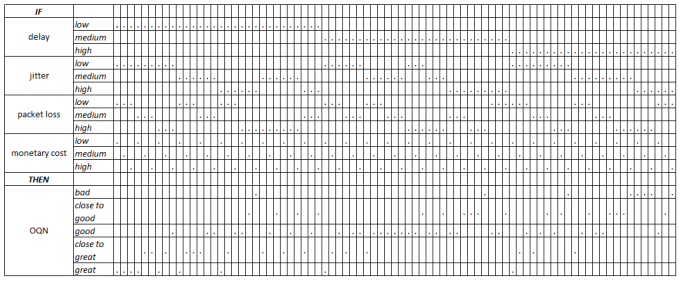


Figure 4. Rule Base.

Finally, in the fuzzification, there is the linguistic variable called OQN (Objective Quality of Network) which has five linguistic terms: bad, close to good, good, close to great and great, as it can be seen in Figure 5. The final result is calculated by the center of maximum defuzzification method.

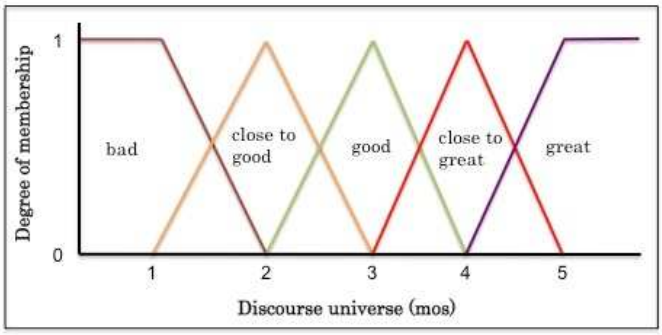


Figure 5. Defuzzification.

Each fuzzy subset within the discourse universe associated with OQN is composed of:

- bad, between 0 and 1;
- close to good, between 1 and 3;
- good, between 2 and 4;
- close to great, between 3 and 5;
- great, above 5.

TABLE V.
PSEUDOCODE FOR PROCESSOR FUNCTION

```
processor(redes, delay, jitter, perda, custo)
{
   redes.analise[]=delay, jitter, perda;
   OQN=fuzzy(redes.analise.delay, redes.analise.jitter,
   redes.analise.perda, redes.custo);
   decisor(OQN);
}
```

Decision-Maker

The decision-maker module checks, every 60 seconds, the total time of iteration, the highest score access point generated by the processor module, then stores it in a text file, thereby allowing any mobility management solution on layer 3 to read it and to take the decision to perform the handover to the network stored in its content. Then, as it can be seen, the proposed fuzzy system consists of four inputs and one output, the latter stating how much quality each network has using the OQN variable.

TABLE VI.
PSEUDOCODE FOR DECISION FUNCTION

```
decisor(OQN)
{
  if(WLAN1.OQN > WLAN2.OQN)
  {
    if(WLAN1.OQN > 3G1.OQN)
    {
      if(WLAN1.OQN > 3G2.OQN)
      {
        altera_rede(WLAN1);
      }
      else
      {
        altera_rede(3G2);
      }
    }
    else
    {
      if(3G1.OQN > 3G2.OQN)
      {
        altera_rede(3G1);
      }
      else
      {
        altera_rede(3G2);
      }
    }
  }
  else
  {
    if(WLAN2.OQN > 3G1.OQN)
    {
      if(WLAN2.OQN > 3G2.OQN)
      {
        altera_rede(WLAN2);
      }
      else
      {
        altera_rede(3G2);
      }
    }
    else
    {
      if(3G1.OQN > 3G2.OQN)
      {
        altera_rede(3G1);
      }
      else
      {
        altera_rede(3G2);
      }
    }
  }
```

```
}
```

Main

The algorithm is modularized and parameterized, i.e., it enables the user to perform the experiments with the necessary amount of ICMP repetitions and requisitions. The algorithm below is started to pass on the information the collector module will need to gather the values to be processed by the processor module.

TABLE VII.
PSEUDOCODE FOR MAIN FUNCTION

```
main()
{
   read(redes);
   while (redes >= 2 && redes <= 4)
   {
     read(host);
     read(gateway);
     read(custo[]);
   }
   read(iteracoes);
   read(rounds);
   read(ICMP);
   collector(redes, iteracoes, rounds, ICMP, custo);
}
```

B. Proposal 2 - Network Selection using Fuzzy Logic, AHP and GRA

The aim of the second proposal of network selection is to use the combination of two strategies: fuzzy logic, which is alike the first proposal, combined with two MADM methods, AHP and GRA. This combination aims to propose a different vision of combination between decision-making methods and artificial intelligence techniques.

The choice of AHP was motivated by being an efficient method to generate weights for objective data, while the choice of GRA was motivated by being a very efficient method in sorting alternatives to meet a particular purpose, in this case, the choice of the best access network, as it can be noted in the authors' article [4], and [11]. Figure 6 illustrates this proposal.

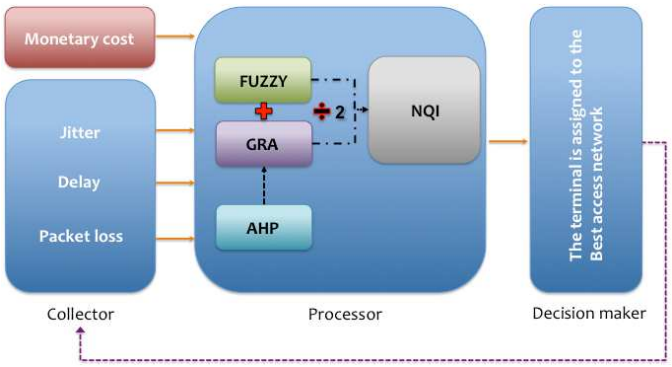


Figure 6. Architecture of Proposal 2 using fuzzy logic, AHP and GRA.

Just as in proposal 1, the system is divided into three functional blocks, which are: the collector, the processor and the decision-maker.

Collector

The collector module works the same way as in the first proposal.

Processor

The processor module uses all the features of the fuzzy logic of the first proposal and, in parallel, it uses the GRA method, which will also receive the same collected values of jitter, delay, packet loss and monetary cost. The generated result will be the rank (score) of each network. This classification is possible due to the weights provided by the AHP, according to each criterion. The weights generated by the AHP for jitter, delay, packet loss and monetary cost criteria are 0.18, 0.25, 0.05 and 0.52, respectively.

These weight values were based on the importance of each QoS criterion of network for audio transmission, i.e., for voice traffic the jitter has a bit greater importance than the delay and they have far greater importance than the packet loss [10], while the monetary cost to the user's preference has much greater importance than the previous criteria, since it is assumed that the user will always opt for the cheapest access network when a change in the access network is necessary.

TABLE VIII.
PSEUDOCODE FOR PROCESSOR FUNCTION

```
processor(redes, delay, jitter, perda, custo)
{
     ahp[]=peso.delay, peso.jitter, peso.perda,
     peso.custo;
     redes.analise[]=delay, jitter, perda;
     gray=GRA(redes.analise.delay,redes.analise.jitter,r
     edes.analise.perda,redes.custo);
     OQN=FUZZY(redes.analise.delay,redes.analise.jitter,
     redes.analise.perda,redes.custo);
     NQI=(gray + OQN)/2;
     decisor(NQI);
}
```

The decision-maker module checks, every 60 seconds, the total time of iteration, the highest score access point generated by the processor module, then stores it in a text file, thereby allowing any software to read it and to take the decision to perform the handover to the network stored in its content. Then, as it can be seen, the proposed fuzzy system consists of four inputs and one output. This output informs how much quality each network has using the NQI (Network Quality Index) variable. The value of this variable is the result of the arithmetic average of the OQN variable value with the GRA value.

TABLE IX.
PSEUDOCODE FOR DECISION FUNCTION

```
decisor(iQR)
{
  if(WLAN1.iQR > WLAN2.iQR)
  {
    if(WLAN1.iQR > 3G1.iQR)
    {
      if(WLAN1.iQR > 3G2.iQR)
      {
        altera_rede(WLAN1);
      }
      else
      {
        altera_rede(3G2);
      }
```

```
    }
    else
    {
      if(3G1.iQR > 3G2.iQR)
      {
        altera_rede(3G1);
      }
      else
      {
        altera_rede(3G2);
      }
    }
  }
  else
  {
    if(WLAN2.iQR > 3G1.iQR)
    {
      if(WLAN2.iQR > 3G2.iQR)
      {
        altera_rede(WLAN2);
      }
      else
      {
        altera_rede(3G2);
      }
    }
    else
    {
      if(3G1.iQR > 3G2.iQR)
      {
        altera_rede(3G1);
      }
      else
      {
        altera_rede(3G2);
      }
    }
  }
}
```

Main

The algorithm is modularized and parameterized, i.e., it enables the user to perform the experiments with the necessary amount of ICMP repetitions and requisitions. The algorithm below is started to pass on the information the collector module will need in order to gather the values to be processed by the processor module.

TABLE X.
PSEUDOCODE FOR MAIN FUNCTION

```
main()
{
   read(redes);
   while(redes <= 2)
   {
      read(host);
      read(gateway);
      read(custo);
   }
   read(iteracoes);
   read(rounds);
   read(ICMP);
   collector(redes, iteracoes, rounds, ICMP);
}
```

IV. METHODOLOGY

Here the necessary procedures to implement the proposals outlined above are presented in order to demonstrate the effectiveness in the proposed scenarios.

C. Experiments without mobility

To assess the impact of network parameters (QoS), jitter, delay and packet loss, besides the monetary cost parameter in the network selection process without mobility, a scenario involving two computers and two wi-fi access points was set up, structured as shown in Figure 7 and with the following function:

- Computer 1: Client;
- Computer 2: Router;
- wi-fi access point 1: 802.11b;
- wi-fi access point 2: 802.11g;
- 3G Base Station 1: UMTS;
- 3G Base station 2: UMTS.

The client computer has two USB (Universal Serial Bus) network interfaces and two USB 3G network interfaces, each previously connected to its respective access point. Therefore, the wi-fi interfaces are connected to access points 1 and 2, while the 3G interfaces are connected to base stations 1 and 2 of distinct cellular operators.

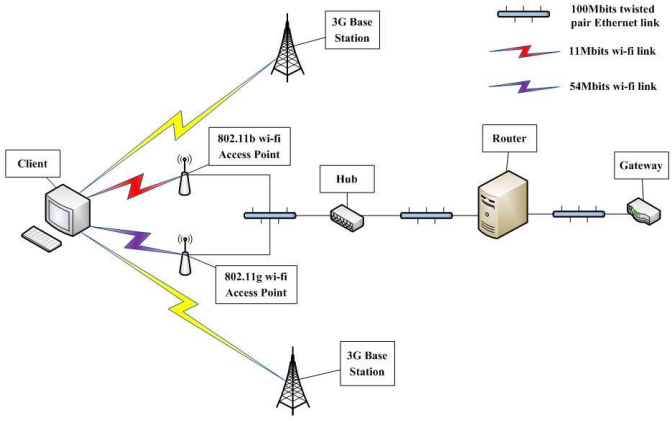


Figure 7. Representation of the scenario structure of the tests without mobility.

All computers used in the assembly of this scenario have the same configuration: Intel Atom Dual Core processor, 2GB RAM and 500GB hard drive. Table 10 shows the list of software and hardware installed and used on the computers.

TABLE XI.
LIST OF SOFTWARE AND HARDWARE USED IN THE SCENARIO FOR THE EXPERIMENTS

Computer	Software	Hardware
1	- Linux Ubuntu v. 11.04 Natty Narwhal Operating System; - gcc v. 4.5.2	- Two wi-fi network cards: * Tenda 802.11N pattern. - Two 3G network cards: * ONDA MAS190UP model; * HUAWEI E173 model.
2	- FreeBSD v. 8.2 operating system. - ipfw dummynet v. 4.	- Three network cards: * 100Mbits Ethernet.

Thus, the experiment consisted of 35 iterations. Each iteration is composed of two rounds and each turn consists of 10 ICMP requisitions from the client bound to the network gateway where the interface is connected. The values of jitter, delay and packet loss generated in these two turns were collected during a whole week, in the morning, afternoon and

evening, totaling 420 iterations on a single day. Each item of this experiment has the following characteristics:

- iteration: includes the whole process, i.e., collection, processing and decision;
- turn: is the action of collecting the data for each network criterion;
- collection: consists of sending ICMP requisitions to the gateways of each network interface;
- collection time: is the time at which the collection is performed.

It is noteworthy that the best access network is selected in each iteration (60 seconds). The competing traffic generated by the server through ipfw (ipfirewall) command was only for wi-fi networks, since telecommunication operators do not allow access to the infrastructure core of 3G networks.

D. Experiments with mobility

To assess the impacts of network parameters (QoS), jitter, delay and packet loss, in addition to the monetary cost parameter in the network selection process with mobility, a scenario with a notebook, access point and a 3G operator was set up, structured as shown in Figure 8 and having the following function:

- notebook;
- wi-fi access point: 802.11g pattern;
- 3G Base station: UMTS.

The client computer contains a wi-fi network interface and a USB 3G network interface, which are previously connected, each to its respective access point. The wi-fi interface is connected to the access point, while the 3G interface is connected to a base station of a mobile operator.

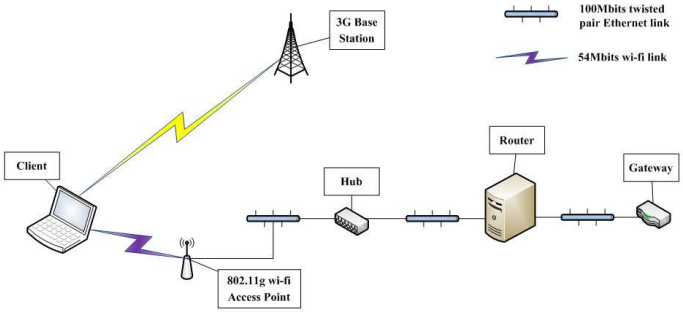


Figure 8. Representation of the structure of the test scenario with mobility.

The notebook used in this scenario has the following configuration: Intel Core 2 Duo 2.4 Ghz processor, 4GB RAM and 250GB hard drive. Table 16 shows the list of installed and used software and hardware.

TABLE XII.
LIST OF SOFTWARE AND HARDWARE USED IN THE SCENARIO FOR THE EXPERIMENTS

Computer	Software	Hardware
1	- Linux Ubuntu v. 11.04 Natty Narwhal Operating System; - gcc v. 4.5.2.	- One wi-fi network card: * Broadcom model BCM4328 802.11b/g pattern. - One 3G network card: * ONDA MAS190UP model;

Thus, the experiments consisted of 358 iterations generated during the one hundred (100) drives, in which fifty (50) from the starting point toward the edge of the wi-fi access point cell and fifty (50) from the edge of the wi-fi access point cell to the starting point, at an average speed of 1m/s straight, as it can be seen in Figure 9.

Each iteration is composed of two turns and each turn consists of 10 ICMP requisitions from the client bound only to the gateway of each one of the access networks. It collects the values of jitter, delay and packet loss generated in these two turns. It is important to stress that the best access network is selected in each iteration (60 seconds). Each item of this experiment has the following characteristics:

- iteration: includes the whole process, i.e., collection, processing and decision;
- turn: is the action of collecting the data for each network criterion;
- collection: consists of sending ICMP requisitions to the gateways of each network interface.
- collection time: is the time at which the collection is performed.

Figure 9. Trajectory of the mobile.

Based on the experiments of these two scenarios, some analyses were necessary to validate the proposals presented in this article.

V. RESULTS

E. Results of the experiments without mobility

The result obtained with each of the proposals in the scenario without mobility is characterized in the following figures, in which charts 1, 2 and 3 represent the collector and the processor modules, while charts 4, 5 and 6 represent the decision-maker module. In each examination, a universe of 420 collection iterations of network variables (delay, jitter and

packet loss) was observed and also the amount of times a particular network was selected by each of the proposals. This amount is expressed in percentage in charts 4 to 6, while in charts 1 (P1), 2 (P2) and 3 (P3) the averages of these selected network variables are shown considering the set of samples which resulted in the selection of that particular network. This methodology was followed for the presentation of other results.

No competing traffic on WLAN1 and WLAN2 networks

Figure 10 shows that proposals 2 and 3, charts 5 and 6 respectively, have succeeded in obtaining great performance in selecting the best access network, within the given characteristics.

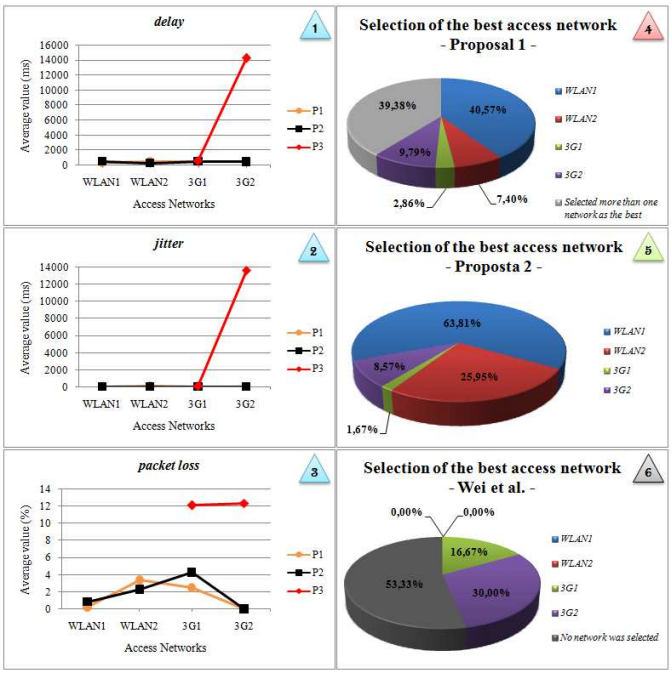


Figure 10. No competing traffic on the WLAN1 and WLAN2 networks.

As it can be seen in chart 5, WLAN1 network has got 63.81% of choice, averaging its delay network parameter around 500ms, jitter around 30ms and packet loss around 1%. The WLAN2 network has obtained 25.95% of choice, averaging its delay network parameter around 300ms, jitter around 60ms and packet loss around 2%. The 3G1 network has obtained 1.67% of choice, averaging its delay network parameter around 500ms, jitter around 60ms and packet loss around 4%. And finally, the 3G2 network has obtained 8.57% of choice, averaging its delay network parameter around 450ms, jitter around 60ms and packet loss around 0%.

In the first proposal, represented by the fourth chart, there is 39.38% of choice in the selection of more than one access network, which is a problem, since the handover has to happen for the best network selected. The WLAN1 network has got 40.57% of choice, averaging its delay network parameter around 350ms, jitter around 50ms and packet loss around 0%. The WLAN2 network has obtained 7.40% of choice, averaging its delay network parameter around 500ms, jitter around 150ms and packet loss around 3%. The 3G1 network has obtained 2.86% of choice, averaging its delay network parameter around 450ms, jitter around 60ms and packet loss around 3%. Finally, the 3G2 network has got 9.79% of choice, averaging its delay network parameter around 550ms, jitter around 60ms and packet loss around 0%.

The authors' proposal in [7], represented by chart 6, has not selected any network in 53.33% of total iterations, because in addition to the criterion of packet loss that can have a value of 0, the monetary cost criterion has a value of 0 real in the WLAN1 and WLAN2 networks. The 3G1 network has obtained 16.67% of choice, averaging its delay network parameter around 600ms, jitter around 180ms and packet loss around 12%. The 3G2 network has got 30% of choice, averaging its delay network parameter around 14000ms, jitter around 13500ms and packet loss around 13%.

Moderate competing traffic in the WLAN1 network

Figure 11 shows that proposals 2 and 3, charts 5 and 6 respectively, have succeeded in obtaining great performance in selecting the best access network, within the given characteristics.

As it can be seen in chart 5, the WLAN2 network obtained 61.19% of choice, averaging its delay network parameter around 400ms, jitter around 60ms and packet loss around 1%. The 3G1 network has obtained 9.29% of choice, averaging its delay network parameter around 400ms, jitter around 70ms and packet loss around 0%. And finally, the 3G2 network has obtained 29.52% of choice, averaging its delay network parameter around 400ms, jitter around 60ms and packet loss around 0%. It may be observed that because the WLAN1 network parameters are above the audio traffic parameters considered as good or great, it was not selected in any of the iterations.

In the first proposal, represented by chart 4, there is 0.24% of choice in selecting more than one access network, which causes a problem, since the handover has to happen for the best network selected. The WLAN2 network has obtained 55.24% of choice, averaging its delay network parameter around 400ms, jitter around 60ms and packet loss around 1%. The 3G1 network has obtained 11.19% of choice, averaging its delay network parameter around 400ms, jitter around 70ms and packet loss around 0%. And finally, the 3G2 network has obtained 33.33% of choice, averaging its delay network parameter around 400ms, jitter around 60ms and packet loss around 0%.

The authors' proposal in [7], represented by chart 6, has not selected any network in 75.95% of total iterations, because in addition to the criterion of packet loss that can have a value of 0, the monetary cost criterion has a value of 0 real in the WLAN1 and WLAN2 networks. The 3G1 network has obtained 6.19% of choice, averaging its delay network parameter around 700ms, jitter around 300ms and packet loss around 8%. The 3G2 network has obtained 17.86% of choice, averaging its delay network parameter around 4800ms, jitter around 4100ms and packet loss around 3%.

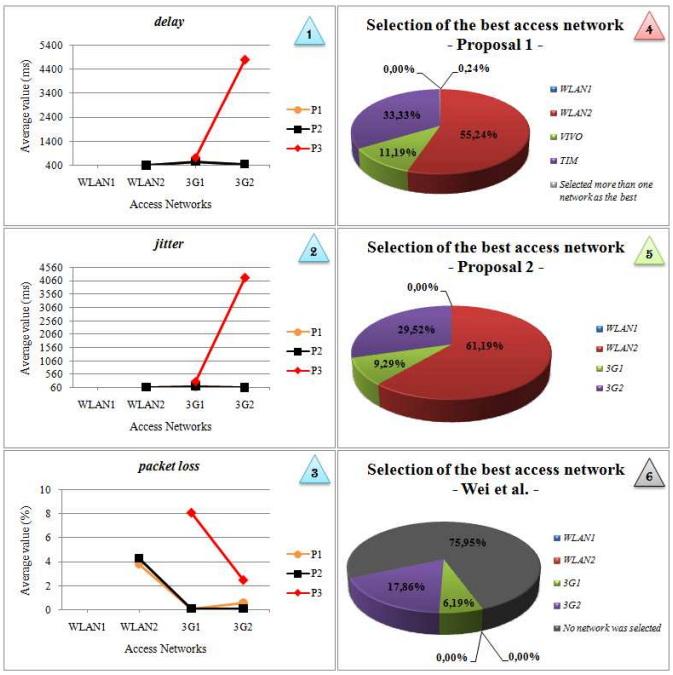


Figure 11. Moderate competing traffic in the WLAN1 network.

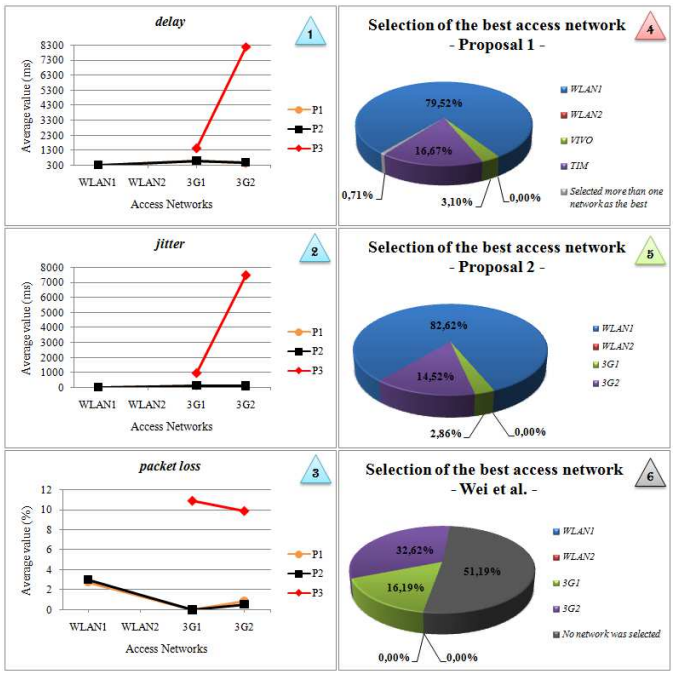


Figure 12. Moderate competing traffic in WLAN2 network.

Moderate competing traffic in the WLAN1 network

Figure 12 shows that proposals 2 and 3, charts 5 and 6 respectively, have succeeded in obtaining great performance in selecting the best access network, within the given characteristics.

As it can be seen in chart 5, the WLAN1 network has got 82.62% of choice, averaging its delay network parameter around 300ms, jitter around 20ms and packet loss around 2%. The 3G1 network has obtained 2.86% of choice, averaging its delay network parameter around 400ms, jitter around 120ms and packet loss around 0%. And finally, the 3G2 network has obtained 14.52% of choice, averaging its delay network parameter around 400ms, jitter around 110ms and packet loss around 2%. It may be observed that because the WLAN2 network parameters are above the audio traffic parameters considered as good or great, it was not selected in any of the iterations.

In the first proposal, represented by chart 4, there is 0.71% of choice in the selection of more than one access network, which causes a problem, since the handover has to happen for the best network selected. The WLAN1 network has got 79.52% of choice, averaging its delay network parameter around 300ms, jitter around 20ms and packet loss around 2%. The 3G1 network has obtained 3.10% of choice, averaging its delay network parameter around 400ms, jitter around 120ms and packet loss around 0%. And finally, the 3G2 network has obtained 16.67% of choice, averaging its delay network parameter around 400ms, jitter around 110ms and packet loss around 2%.

The authors' proposal in [7], represented by chart 6, has not selected any network in 51.19% of total iterations, because in addition to the criterion of packet loss that can have a value of 0, the monetary cost criterion has a value of 0 real in the WLAN1 and WLAN2 networks. The 3G1 network has obtained 16.19% of choice, averaging its delay network parameter around 1400ms, jitter around 900ms and packet loss around 10%. The 3G2 network has obtained 32.62% of choice, averaging its delay network parameter around 8000ms, jitter around 7500ms and packet loss around 9%.

Moderate competing traffic in the WLAN1 and WLAN2 networks

Figure 13 shows that proposals 2 and 3, charts 5 and 6 respectively, have succeeded in obtaining great performance in selecting the best access network, within the given characteristics.

As it can be seen in chart 5, the 3G1 network has obtained 29.52% of choice, averaging its delay network parameter around 500ms, jitter around 60ms and packet loss around 0%. And finally, the 3G2 network has obtained 70.48% of choice, averaging its delay network parameter around 400ms, jitter around 50ms and packet loss around 2%. It may be observed that because the WLAN1 and WLAN2 network parameters are above the audio traffic parameters considered as good or great, they were not selected in any of the iterations.

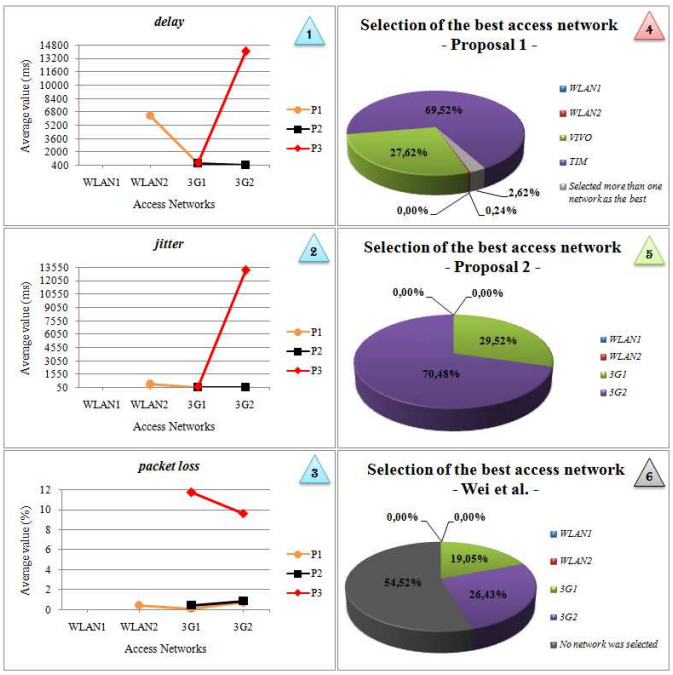


Figure 13. Moderate competing traffic in the WLAN1 and WLAN2 networks.

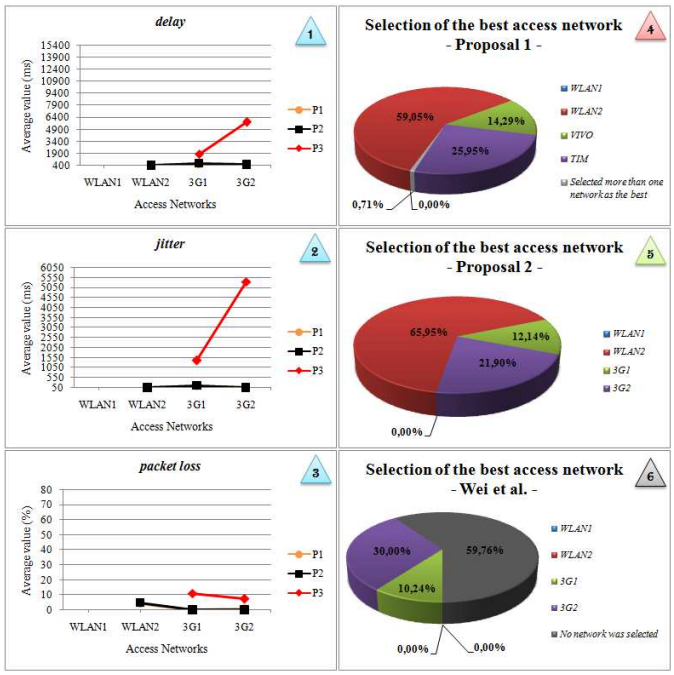


Figure 14. Competing traffic in the WLAN1 network.

In the first proposal, represented by chart 4, there is 2.62% of choice in selecting more than one access network, which is considered a problem, since the handover has to happen for the best network selected. The WLAN2 network has obtained 0.24% of choice, averaging its delay network parameter around 6700ms, jitter around 500ms and packet loss around 0%. The 3G1 network has obtained 27.62% of choice, averaging its delay network parameter around 500ms, jitter around 60ms and packet loss around 0%. And finally, the 3G2 network has obtained 69.52% of choice, averaging its delay network parameter around 400ms, jitter around 50ms and packet loss around 2%.

The authors' proposal in [7], represented by chart 6, has not selected any network in 54.52% of total iterations, because in addition to the criterion of packet loss that can have a value of 0, the monetary cost criterion has a value of 0 real in the WLAN1 and WLAN2 networks. The 3G1 network has obtained 19.05% of choice, averaging its delay network parameter around 700ms, jitter around 200ms and packet loss around 11%. The 3G2 network has obtained 26.43% of choice, averaging its delay network parameter around 14000ms, jitter around 13000ms and packet loss around 9%.

High competing traffic in the WLAN1 network

Figure 14 shows that proposals 2 and 3, charts 5 and 6 respectively, have succeeded in obtaining great performance in selecting the best access network, within the given characteristics.

As it can be seen in chart 5, the WLAN2 network has obtained 65.95% of choice, averaging its delay network parameters around 400ms, jitter around 50ms and packet loss around 4%. The 3G1 network has obtained 12.14% of choice, averaging its delay network parameter around 400ms, jitter around 190ms and packet loss around 0%. And finally, the 3G2 network has obtained 21.90% of choice, averaging its delay network parameter around 400ms, jitter around 50ms and packet loss around 0%. It may be observed that because the WLAN1 network parameters are above the audio traffic parameters considered as good or great, it was not selected in any of the iterations.

In the first proposal, represented by chart 4, there is 0.71% of choice in the selection of more than one access network, which is considered a problem, since the handover has to happen for the best network selected. The WLAN2 network has obtained 59.05% of choice, averaging its delay network parameter around 400ms, jitter around 50ms and packet loss around 4%. The 3G1 network has obtained 14.29% of choice, averaging its delay network parameter around 400ms, jitter around 190ms and packet loss around 0%. And finally, the 3G2 network has obtained 25.95% of choice, averaging its delay network parameter around 400ms, jitter around 50ms and packet loss around 0%.

The authors' proposal in [7], represented by chart 6, has not selected any network in 59.76% of total iterations, because in addition to the criterion of packet loss that can have a value of 0, the monetary cost criterion has a value of 0 real in the WLAN1 and WLAN2 networks. The 3G1 network has obtained 10.24% of choice, averaging its delay network parameter around 1900ms, jitter around 1550ms and packet loss around 10%. The 3G2 network has got 30% of choice, averaging its delay network parameter around 6400ms, jitter around 5550ms and packet loss around 8%.

High competing traffic in the WLAN2 network

Figure 15 shows that proposals 2 and 3, charts 5 and 6 respectively, have succeeded in obtaining great performance in selecting the best access network, within the given characteristics.

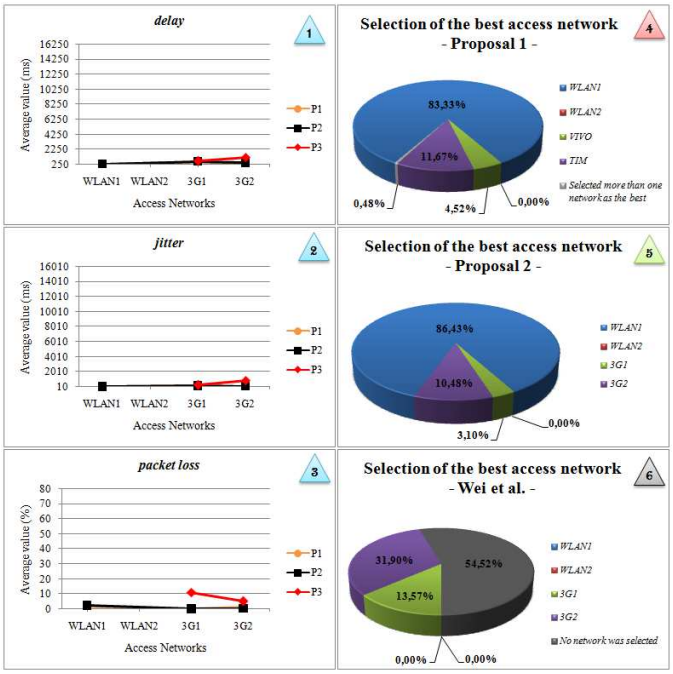


Figure 15. Competing traffic in WLAN2 network.

As it can be seen in chart 5, the WLAN1 network has got 86.43% of choice, averaging its delay network parameter around 250ms, jitter around 10ms and packet loss around 2%. The 3G1 network has obtained 3.10% of choice, averaging its delay network parameter around 260ms, jitter around 10ms and packet loss around 0%. And finally, the 3G2 network has obtained 10.48% of choice, averaging its delay network parameter around 250ms, jitter around 10ms and packet loss around 0%. It may be observed that because the WLAN2 network parameters are above the audio traffic parameters considered as good or great, it was not selected in any of the iterations.

In the fourth graph representing the first proposal, there is 0.48% of choice in the selection of more than one access network, which is a problem, since the handover has to happen for the best network selected. The WLAN1 network has got 83.33% of choice, averaging its delay network parameter around 250ms, jitter around 10ms and packet loss around 2%. The 3G1 network has obtained 4.52% of choice, averaging its delay network parameter around 260ms, jitter around 10ms and packet loss around 0%. And finally, the 3G2 network has obtained 11.67% of choice, averaging its delay network parameter around 250ms, jitter around 10ms and packet loss around 0%.

The authors' proposal in [7], represented by chart 6, has not selected any network in 54.52%of total iterations, because in addition to the criterion of packet loss that can have a value of 0, the monetary cost criterion has a value of 0 real in WLAN1 and WLAN2 networks. The 3G1 network has obtained 13.57% of choice, averaging its delay network parameter around 250ms, jitter around 10ms and packet loss around 10%. The 3G2 network has obtained 31.90% of choice, averaging its delay network parameter around 300ms, jitter around 15ms and packet loss around 7%.

High competing traffic in WLAN1 and WLAN2 networks

Figure 16 shows that the second proposal, chart 5, has performed well in selecting the best access network when compared to the first proposal, but a little worse than the third proposal.

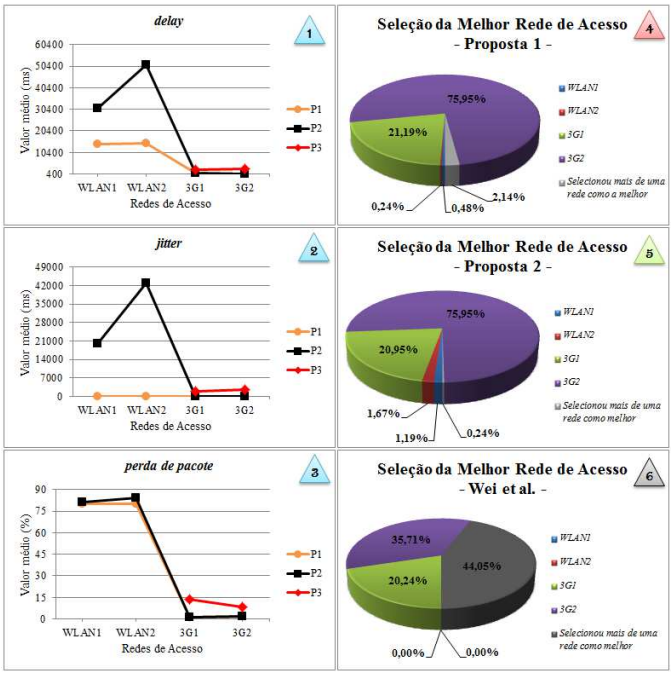


Figure 16. Competing traffic in the WLAN1 and WLAN2 networks

As it can be seen in chart 5, there is 0.24% of choice in the selection of more than one access network, which is a problem, since the handover has to happen for the best network selected. The WLAN1 network has got 1.19% of choice, averaging its delay network parameter around 30400ms, jitter around 21000ms and packet loss around 80%. The WLAN2 network has obtained 1.67% of choice, averaging its delay network parameter around 50400ms, jitter around 42000ms and packet loss around 80%. The 3G1 network has obtained 20.95% of choice, averaging its delay network parameter around 400ms, jitter around 10ms and packet loss around 0%. And finally, the 3G2 network has obtained 75.95% of choice, averaging its delay network parameter around 400ms, jitter around 10ms and packet loss around 2%.

In the first proposal, represented by chart 4, there is 2.14% of choice in the selection of more than one access network, which is considered a problem, since the handover has to happen for the best network selected. The WLAN1 network has obtained 0.48% of choice, averaging its delay network parameter around 15400ms, jitter around 10ms and packet loss

around 80%. The WLAN2 network has obtained 0.24% of choice, averaging its delay network parameter around 15400ms, jitter around 10ms and packet loss around 80%. The 3G1 network has obtained 20.95% of choice, averaging its delay network parameter around 400ms, jitter around 10ms and packet loss around 0%. And finally, the 3G2 network has obtained 75.95% of choice, averaging its delay network parameter around 400ms, jitter around 10ms and packet loss around 2%.

The authors' proposal in [7], represented by chart 6, has not selected any network in 44.05% of total iterations, because in addition to the criterion of packet loss that can have a value of 0, the monetary cost criterion has a value of 0 real in the WLAN1 and WLAN2 networks. The 3G1 network has obtained 20.24% of choice, averaging its delay network parameter around 400ms, jitter around 10ms and packet loss around 14%. The 3G2 network has obtained 35.71% of choice, averaging its delay network parameter around 400ms, jitter around 15ms and packet loss around 12%.

Result of the experiments with mobility

To obtain the results presented in this scenario a set of 358 collection iterations of the network variables was considered during the 50 drives/shifts from the access point to the edge and vice versa.

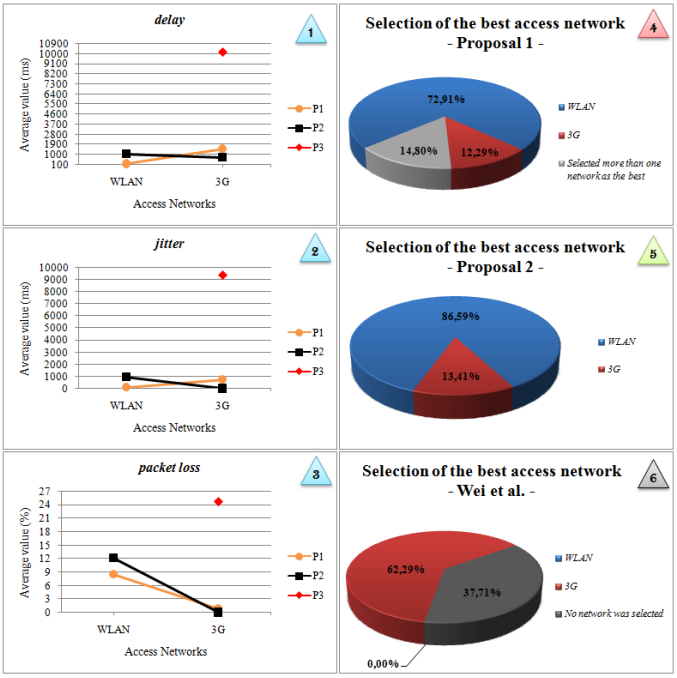


Figure 17. Traffic in the environment with mobility.

As it can be seen in chart 5, the WLAN network has obtained 86.59% of choice, averaging its delay network parameter around 1000ms, jitter around 1000ms and packet loss around 12%. The 3G network has obtained 13.41% of choice, averaging its delay network parameter around 900ms, jitter around 10ms and packet loss around 0%. Although the 3G network parameters are smaller than the WLAN network, the monetary cost parameter in the WLAN is 0 real and in the 3G network 89.90 reais, leading to a preference for the WLAN network.

In the first proposal, chart 4, there is 14.80% of choice in the selection of more than one access network, which is considered a problem, since the handover has to happen for the best network selected. The WLAN network has obtained 72.91% of choice, averaging its delay network parameter around 100ms, jitter around 10ms and packet loss around 8%. The 3G network has got 12.29% of choice, averaging its delay network parameter around 1700ms, jitter around 900ms and packet loss around 1%.

The authors' proposal in [7], represented by chart 6, has not selected any network in 44.05% of total iterations, because in addition to the criterion of packet loss that can have a value of 0, the monetary cost criterion has a value of 0 real in WLAN network. The 3G network has obtained 62.29% of choice, averaging its delay network parameter around 10000ms, jitter around 9500ms and packet loss around 25%.

VI. Conclusions and Future Work

The network selection is a very important step, or even the most important, in the handover process, since it will make every effort in implementing the handover so that the terminal can connect to the selected network through decision-making techniques that best meet the user's access point preferences.

Therefore, we can see that the decision-making methods are useful in sorting alternatives in order to achieve a goal, and together with an artificial intelligence technique, the result becomes even more accurate.

As future work, we intend to integrate these proposals with handover software by encompassing the whole process of mobility management.

References

[1] Kassar, M., Kervella, B., and Pujolle, G. An overview of vertical handover decision strategies in heterogeneous wireless networks. Computer Communications, 31(10):2607–2620, 2008.

[2] Singhrova, A. and Prakash, N. Adaptive Vertical Handoff Decision Algorithm forWireless Heterogeneous Networks. In Proceedings of the 2009 11th IEEE International Conference on High Performance Computing and Communications, volume 0, pages 476–481. IEEE Computer Society, 2009.

[3] Ciccarese, G., De Blasi, M., Marra, P., Mighali, V., Palazzo, C., Patrono, L., and Stefanizzi, M. Vertical handover algorithm for heterogeneous wireless networks. In 2009 Fifth International Joint Conference on INC, IMS and IDC, pages 1948–1954, 2009.

[4] Stevens-Navarro, E. and Wong, V. Comparison between vertical handoff decision algorithms for heterogeneous wireless networks. In Vehicular Technology Conference, volume 2, pages 947–951, 2006.

[5] Godor, G. and Detari, G. Novel network selection algorithm for various wireless network interfaces. In Mobile and Wireless Communications Summit, 2007. 16th IST, pages 1–5, 2007.

[6] Alkhawlani, M. and Ayesh, A. Access network selection based on fuzzy logic and genetic algorithms. Advances in Artificial Intelligence, 8(1):1–12, 2008.

[7] Wei, Y., Hu, Y., and Song, J. Network selection strategy in heterogeneous multi-access environment. The Journal of China Universities of Posts and Telecommunications, 14:16–49, 2007.

[8] Kurose, J. and Ross, K. Redes de Computadores e a Internet: uma abordagem top-down. 5. ed. - São Paulo: Addison Wesley, 2010.

[9] ITU-T, R. G. 114. One-way transmission time, 18, 2000.

[10] Silva, D. J. Análise de qualidade de serviço em redes corporativas. Dissertação de Mestrado, Instituto de Computação, Universidade Estadual de Campinas (UNICAMP), 2004.
[11] Tran, P. and Boukhatem, N. Comparison of madm decision algorithms for interface selection in heterogeneous wireless networks. In Software, Telecommunications and Computer Networks, 2008. SoftCOM 2008. 16th International Conference on, pages 119–124, 2008.
[12] Radhika, K.; Reddy, A. V. Network selection in heterogeneous wireless networks based on fuzzy multiple criteria decision making. International Journal of Computer Applications, Foundation of Computer Science (FCS), v. 22, n. 1, p. 7–10, 2011.

Vinícius Rios is assistant professor at the University of Tocantins (UNITINS) in distance education mode and face. He is Graduated in Information Systems from the Lutheran University of Brazil (ULBRA) (2005), specialization in Management and Consulting in Telecommunications from the Brazilian Institute of Postgraduate Studies and Extension (IBPEX) (2006) and Master's degree in Electrical Engineering from the University of Brasilia (UNB) (2012). He has experience in Information Systems with emphasis in Computer Networking, Operating Systems, Wi-Fi Networks, Mobility Management and Artificial Intelligence.

Claudio Monteiro is a full professor at the Federal Institute of Education, Science and Technology of Tocantins, Computing Science Department, Palmas – TO, ACM member and leader of the Research Group on Networks Computers (GREDES - gredes.ifto.edu.br). He graduated in data processing technology from the University of Amazonia (1990) and Masters in Computer Science from Federal University of Paraíba (1997) and Ph.D. in Electrical Engineering from the University of Brasilia - UNB (2012). Actualy, has been developed a framework for reduce the latency of the handover between heterogeneous wireless networks. In addition, a. He has experience in computer science, with emphasis on wireless networks, network protocols, QoS/QoE and operating systems.

Vanice Cunha was born in Brasília, Federal District (Brazil) on august 24, 1984. She became Master degree in Electrical Engineering from the University of Brasilia in 2012. Her research project involved QoV (Quality of Video) and QoS (Quality of Service) in wireless networks of 3rd Generation. Currently she is a female teacher at the Instituto Federal de Brasilia.

Volume 2 Issue 3, May 2013, ISSN: 2288-0003

ICACT-TACT JOURNAL

Global IT Research Institute

1713 Obelisk, 216 Seohyunno, Bundang-gu, Sungnam Kyunggi-do, Republic of Korea 463-824

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