Mobile Information Systems

Innovative Mobile Internet Services and Applications

Guest Editors: Ilsun You, Francesco Palmieri, and Leonard Barolli

Innovative Mobile Internet Services and Applications

Innovative Mobile Internet Services and Applications

Guest Editors: Ilsun You, Francesco Palmieri,
and Leonard Barolli

Contents

Hindawi Publishing Corporation
Mobile Information Systems
Volume 2015, Article ID 280275, 2 pages
http://dx.doi.org/10.1155/2015/280275

Editorial

Innovative Mobile Internet Services and Applications

Ilsun You,[1] Francesco Palmieri,[2] and Leonard Barolli[3]

[1] *Department of Computer Software, School of Information Science, Korean Bible University, 16 Danghyun 2-gil, Nowon-gu, Seoul 139-791, Republic of Korea*
[2] *Department of Industrial and Information Engineering, Second University of Naples, Via Roma 29, 81031 Aversa (CE), Italy*
[3] *Department of Information and Communication Engineering, Faculty of Information Engineering, Fukuoka Institute of Technology (FIT), 3-30-1 Wajiro-Higashi, Higashi-Ku, Fukuoka 811-0295, Japan*

Correspondence should be addressed to Ilsun You; ilsunu@gmail.com

Received 1 September 2014; Accepted 1 September 2014

1. Introduction

Mobile Internet technology has moved the digital world frontiers much far beyond what was even imaginable a few years ago. Such unprecedented revolution affected many sectors of modern society, ranging from business, culture, education, and social life, by also significant enhancing productivity for both public and private organizations. In particular, the convergence of mobile communications technologies and ubiquitous Internet coverage is introducing alternative business models, together with new applications, devices services, protocols, and security/performance issues. Day-to-day activities and operations in many areas ranging from healthcare to energy and transportation management can be significantly influenced by the availability of cheap, high-performance ubiquitous connections to the Internet. In addition, mobile broadband technologies such as WiFi, LTE, and WiMax together with advances in cheap sensor equipment and energy-efficient processing devices are fostering the integration of the Internet with an ever increasing quantity of smart objects deployed around us, leading to a new convergence between physical space and cyberspace. This also implies a shift in communication dynamics from person-to-person to machine-to-machine, resulting in the emerging Internet of Things paradigm, where the emerging active objects will largely outnumber (of several orders of magnitude) the actually connected devices, with the obvious consequences in terms of address space requirements and the need of new IPv6-based mobility services.

The evolution of mobile Internet will have as its most significant follow-up much more than improving the Web surfing or mobile access experience: new networking architectures, protocols, and paradigms such as software defined and cognitive networks are incessantly emerging, with obvious effects on a wide range of Internet-enabled services, activities, and transactions. The diffusion of these new network services, models, and architectures opens new security challenges to be faced by using flexible and effective methods that should be able to operate with very different and heterogeneous devices and technologies.

All the above issues are now considered as topics of paramount importance for research/academia, industry, and government as well as policy makers. Clearly this implies increased investments, enhanced productivity, and more job opportunities. Accordingly, this special issue is intended to foster the dissemination of state-of-the-art research in the aforementioned scenario, ensuring that the above technologies could reach their full potential, so that all the digital citizens can fully experience the benefits made possible by the mobile broadband economy. Original research articles have been selected by covering several aspects of innovative mobile Internet technologies, including emerging services and applications, theoretical studies, and experimental prototypes.

2. Special Issue Contents

This Special Issue is composed of five contributions, carefully selected according to their subject and accepted based on merit contents. These works cover a variety of topics, including mobile IPv6, advanced network architectures and services, and, finally, communications security.

In the new service environments empowered by mobile Internet connectivity Proxy Mobile IPv6 (PMIPv6) emerged as a promising network-based mobility management protocol, which does not need any participation of the involved Mobile Nodes. In this scenario, the contribution presented by L. Wang et al. proposed two efficient PMIPv6 based mobile multicast sender support schemes, namely, PMIP bidirectional tunneling (PMIP-BT) and PMIP direct routing (PMIP-DR), that can transparently support the multicast sender mobility in PMIPv6 networks.

Furthermore, the contribution presented by M. Song et al. proposes several cost-optimized mobility management schemes based on pointer forwarding for PMIPv6 networks with the aim of reducing the overall network traffic due to mobility-related signaling and packet delivery. When the MN moves in both intradomain and interdomain handoff, their schemes can reduce high-signaling overhead by using pointer chains to connect the local mobility anchor (LMA) and the mobile access gateway (MAG). All the schemes are independent, dynamical, and per-user-based, taking into account the optimal threshold of the forwarding chain length, as well as the mobility of each user, and the service patterns for minimizing overall network traffic.

From a completely different perspective, the article authored by G. Sato et al. introduces a disaster resilient network integrating various wireless networks into a cognitive network that can be used as an access network to the Internet in presence of severe disaster occurrence. We designed and developed such a disaster resilient network based on software defined network (SDN) technology in order to automatically select the best network link and route among the possible access resources to Internet by periodically monitoring their operating status.

On the other hand, the article by L.-F. Huang et al. presents a synchronous cognitive MAC protocol (distributed-antenna based heterogeneous cognitive wireless network synchronous MAC protocol), exploiting CSMA/CA mechanism in the 802.11DCF, for heterogeneous cognitive radio networks, aiming at combining the advantages of cognitive radio and distributed antennas to fully utilize the licensed spectrum and broaden the communication range. The use of distributed antennas to sense spectrum and transmit data significantly improves the sensing performance and increases network throughput.

Regarding security issues, the work by G. Vitello et al. proposes a novel embedded automatic fingerprint authentication system (AFAS) for mobile devices improving the performance of standard AFAS hardware implementations in order to enable its deployment in mobile architectures. The system exhibits an interesting trade-off between the needed resources, authentication time, and accuracy rate.

Finally, the contribution from K. Singh and P. Rangan presents an improved construction for lattice based universal reencryption scheme that can replace the existing universal reencryption schemes used in postquantum cryptography to ensure location privacy in mobile system.

We are sure that the experiences presented in this Special Issue may significantly contribute to the literature and the efforts conducted by academic people, industry professionals, and everyone interested in the covered areas, by also inspiring readers to find sources of new innovative insights that will benefit their future research.

Acknowledgments

We would like to express our sincere appreciation of the valuable contributions made by all the authors and our deep gratitude to all the highly qualified anonymous reviewers who have carefully analyzed the assigned papers and significantly contributed to improve their quality.

Ilsun You
Francesco Palmieri
Leonard Barolli

Hindawi Publishing Corporation
Mobile Information Systems
Volume 2015, Article ID 401975, 13 pages
http://dx.doi.org/10.1155/2015/401975

Research Article

Fingerprint Quality Evaluation in a Novel Embedded Authentication System for Mobile Users

Giuseppe Vitello,[1] Vincenzo Conti,[1] Salvatore Vitabile,[2] and Filippo Sorbello[3]

[1] *Faculty of Engineering and Architecture, University of Enna Kore, 94100 Enna, Italy*
[2] *Department of Biopathology and Medical Biotechnologies, University of Palermo, 90127 Palermo, Italy*
[3] *Department of Chemical Engineering, Management, Computer Science, and Mechanics, University of Palermo, 90128 Palermo, Italy*

Correspondence should be addressed to Giuseppe Vitello; giuseppe.vitello@unikore.it

Received 1 September 2014; Accepted 1 September 2014

Academic Editor: Ilsun You

The way people access resources, data and services, is radically changing using modern mobile technologies. In this scenario, biometry is a good solution for security issues even if its performance is influenced by the acquired data quality. In this paper, a novel embedded automatic fingerprint authentication system (AFAS) for mobile users is described. The goal of the proposed system is to improve the performance of a standard embedded AFAS in order to enable its employment in mobile devices architectures. The system is focused on the quality evaluation of the raw acquired fingerprint, identifying areas of poor quality. Using this approach, no image enhancement process is needed after the fingerprint acquisition phase. The Agility RC2000 board has been used to prototype the embedded device. Due its different image resolution and quality, the experimental tests have been conducted on both PolyU and FVC2002 DB2-B free databases. Experimental results show an interesting trade-off between used resources, authentication time, and accuracy rate. The best achieved false acceptance rate (FAR) and false rejection rate (FRR) indexes are 0% and 6.25%, respectively. The elaboration time is 62.6 ms with a working frequency of 50 MHz.

1. Introduction

The growing number of mobile users has deeply influenced scenarios such as commercial, banking, and government applications. Due to the increasing security requirements, the way people access information resources, data communication and processing, is radically changing [1, 2]. In this field, biometric recognition systems are a good solution for mobile users authentication [3, 4].

Depending on the application context, a biometric recognition system may be used as verification or identification system. A verification system checks the person's identity by comparing the captured biometric characteristic with his/her own biometric template enrolled in the system. It conducts a one-to-one comparison to determine whether the identity claimed by the individual is true. An identification system recognizes the subject by searching the entire template database for a match. It conducts one-to-many comparisons and establishes person's identity or fails if he/she is not enrolled in the system database, without the subject having to claim an identity. A biometric recognition system may be further classified as unimodal, when one or more instances of a single biometric trait (e.g., multiple impressions of a finger) are processed. The system is classified as multimodal, when it uses one or more instances of multiple biometric characteristics (e.g., fingerprint and face images) [5]. Multialgorithmic systems represent a particular multimodal systems class, where the same biometric trait is processed with different algorithms [4].

To reduce the processing time in identification systems, biometric characteristics can be classified in an accurate and consistent way such that the input needs to be matched only with a database subset. Fingerprint classification, for example, can be performed using a wide variety of algorithms, almost all based on one or more of the following features: neural network [6], Gabor filter and support vector machine [7], genetic programming [8], singular points [9], and so forth. Unfortunately, singular points are not always present in a fingerprint image (e.g., in the partially fingerprint image acquisition). In that case, the approach proposed in [10] may be useful, where pseudosingularity points are detected and extracted for fingerprints classification and matching.

Biometric systems are a rapidly evolving technology in mobile devices, with a very strong potential to be widely adopted in a broad range of human scenarios. However, there are many challenges to overcome in designing completely automatic and reliable systems, especially when input data are of poor quality. For example, fingerprint acquisitions not correctly performed, because of skin humidity, impressing pressure, large translation on sensor area, sensing mechanism, and so on, could lead to the following issues [11]:

(i) quite different ridges quality;

(ii) ridges and valleys pattern deformation;

(iii) insufficient contrast;

(iv) small foreground area;

(v) inadequate overlapping area between different images although they are captured from the same finger.

In this paper, a novel embedded automatic fingerprint authentication system (AFAS) for mobile users is described. The goal of the proposed approach is to improve the performance of a standard embedded AFAS, in terms of used resources, execution time, and working frequency, in order to enable its employment in mobile devices architectures. Starting from the work described in [12], focused only on an advanced matching technique for partial fingerprints, the novel embedded AFAS has been prototyped adding the proposed fingerprint image quality evaluation module. This module is designed to find a measure that can characterize the quality of raw fingerprint images, only using the information achieved in the acquisition step. The quality index calculates and merges six different global quality indexes based on image contrast, ridges orientation certainty level, fingerprint's center position, impressing pressure, and fingerprint size over the entire image. It is also specialized in identifying areas of poor quality. If the image overcomes the quality constraints only good areas are processed reducing the potential false minutiae. Otherwise, if the image is rejected, the system suggests to user a set of information about the not correct acquisition step, helping him to follow correct guidelines to obtain a better image quality in the next fingerprint acquisition task (Figure 1).

The proposed AFAS architecture, designed for field programmable gate array (FPGA) devices using pipeline techniques and parallelisms to reduce the execution time, has been prototyped on the Agility RC2000 development board, equipped with a Xilinx Virtex-II xc2v6000 FPGA [13]. To evaluate the effectiveness of the proposed approach, three tests have been conducted starting from two different free databases, chosen for their different characteristics in terms of resolution and quality.

The AFAS described in [14] has been extended with the proposed fingerprint image quality evaluation module. Experimental trials on the FVC2002 DB2-B database [15] show that the accuracy performance has been strongly increased. Then, the matching algorithm has been replaced with the advanced technique for partial fingerprints proposed in [12]. Experimental results on the PolyU database [16] show an interesting trade-off between required hardware resources, authentication time, and accuracy rate. Finally, the fingerprint image quality evaluation module has been replaced with a preprocessing task to enhance fingerprint images, a Gabor filter, and the system has been tested on the same PolyU database. The obtained experimental results show the validity of the proposed novel AFAS.

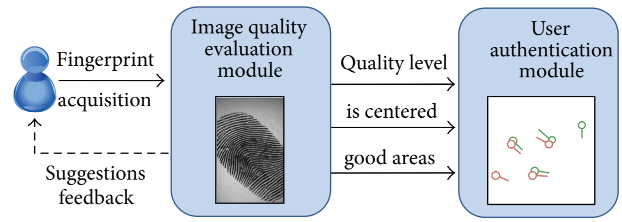


Figure 1: Image quality evaluation module classifies the fingerprint image quality and identifies high quality areas. It checks if the fingerprint is centered over the image. If an image is rejected, a suggestions feedback is given, to the user for the next fingerprint acquisition tasks.

The paper is structured as follows. Section 2 reports the main literature works on fingerprint image quality evaluation methods. Section 3 describes the proposed novel fingerprint authentication system. Section 4 outlines the experimental results. Finally, conclusions are reported.

2. Remarks on Fingerprint Image Quality Evaluation Methods

One of the main techniques to test the performance of an automatic fingerprint recognition system relies heavily on the quality analysis of the acquired fingerprint image [17]. In literature many researchers have studied, proposed, and implemented different methods for evaluating the images quality, using, for example, artificial neural networks, micro- and macrofeatures analysis, and texture feature estimates.

In [11] the authors propose a hybrid scheme to measure the quality of fingerprint images by combining both local and global characteristics. It uses not only local texture features but also some global factors such as the standard deviation of Gabor features, the foreground area and central position, the number of minutiae, and the existence of singular points. The authors define seven quality indexes and also two weighting methods, an overlapping area based method and a linear regression method, for computing the correlation between the final quality value and each quality index.

In [18] the authors present a fast fingerprint enhancement algorithm, based on the estimated local ridge orientation and frequency, which can adaptively improve the clarity of ridge and valley structures of input fingerprint images. It models the ridge and valley patterns as a sinusoidal wave and then calculates the amplitude, frequency, and variance of the wave to determine the quality of the fingerprint regions.

In [19] the authors define a method not aimed at selecting images of good visual appearance but aimed at identifying poor quality as well as invalid fingerprints for automatic fingerprint identification systems. It analyzes the image in the spatial domain and uses the orientation certainty to certify the localized texture pattern, while it uses ridge and valley structure to detect invalid images.

In [20] the authors implement an effective quality classification method for fingerprint images based on neural networks. It uses effective area, energy concentration, spatial consistency, and directional contrast as quality indexes. A comparison with individual quality index thresholding and linear weighted sum method, on a private database, shows the higher quality classification accuracy of their method.

In [21] the authors describe a novel method for estimating the quality of fingerprint images using both local and global analyses. They propose a fusion method mixing the information from ridge and valley line resolution, fingerprint area, and gray levels average and variance, using the golden section method to select the relevant weights value.

In [22] the authors propose a novel quality-checking algorithm which considers the condition of the input fingerprints and the orientation estimation errors. First, the 2D gradients of the fingerprint image is separated into two sets of 1D gradients, and then the shape of the probability density functions of these gradients is measured in order to determine the fingerprint quality.

In [23] the authors present an image quality assessment technique for a novel fingerprint multimodal algorithm to provide high accuracy under nonideal conditions. It uses the redundant discrete wavelet transform to assess the image quality, for high resolution fingerprint databases, by determining the presence of noise, smoothness, and edge information in a fingerprint image. Successively, in [24] the authors extend this technique designing a local image quality assessment algorithm. They use it as the first step of a novel algorithm for fast extraction and identification of level-3 features, such as pores, ridge contours, dots, and incipient ridges.

After an exhaustive analysis of the above described methods for fingerprint image quality evaluation and in order to achieve the best trade-off between execution time and used resources for embedded devices, a mixed method has been designed and integrated in the proposed novel embedded AFAS. It is based on a fingerprint image global analysis in the spatial domain and inspired by works described in [11, 19].

3. The Proposed Novel Embedded Fingerprint Authentication System

The proposed minutiae based AFAS is focused on the acquired raw image quality evaluation identifying poor quality areas, such as dry and moist portions, in order to overcome the common problems in wrong acquisitions on mobile devices. The system checks if the distance between image center and the fingerprint center coordinates is lower than an experimental fixed threshold in order to extract the maximum number of corresponding minutiae. If this condition is verified and the image overcomes the quality constraints, only high quality image portions are processed. Otherwise, the image is rejected and the system gives to the user suggestion feedbacks about the wrong acquisition step, helping him to obtain a better image quality in the next fingerprint acquisition task. In addition, an advanced matching technique for user recognition, based on partial fingerprints, is performed to improve system accuracy [12]. This technique calculates a likelihood ratio by trying every possible overlap of the acquired fingerprint with the enrolled one. The rototranslation parameters computation is based on the similar minutiae pairs identification belonging to both fingerprints.

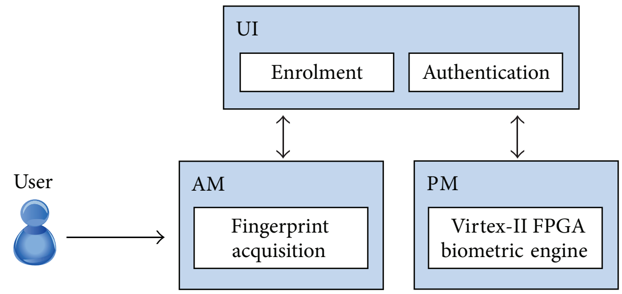


Figure 2: System's components: the user interface (UI), the acquisition module (AM), and the processing module (PM).

Considering the functionalities of the proposed system, three main components can be identified: the interface module (IM), which enables the user to interact with the system, the acquisition module (AM), which deals with the fingerprint image acquisition, and the processing module (PM), based on the FPGA processing engine implementing the authentication phase (Figure 2).

Using the proposed PM, no image enhancement after fingerprint acquisition is performed. Therefore, a considerable saving in terms of execution time and hardware resources has been achieved with respect to a standard AFAS implementation. With more details, the proposed AFAS requires an image quality evaluation module, including a binarization module, a thinning module, a feature extraction module, an alignment module, and, finally, a matching module. Despite a standard AFAS implementation no normalization, enhancement, field orientation, filtered orientation and, smoothing tasks are required (Figure 3).

In the following subsections the main submodules of the proposed novel AFAS will be described.

3.1. Image Quality Evaluation Module. This module, inspired by works described in [11, 19], evaluates the fingerprint image quality through a global analysis in the spatial domain. With more details, it analyzes the image by blocks, calculates the fingerprint central position, identifies the dry and moist blocks, and classifies the image quality into two levels.

Figure 4 shows the architecture of the proposed module, while the following subsections describe each submodule.

3.1.1. Blocks_Generator Submodule. This submodule reads a gray levels fingerprint image from the on-board memory, divides it into an ideal grid of $N = N_x * N_y$ nonoverlapping blocks, and sends them, pixel by pixel, to the Fingerprint_Quality_Level_Evaluator submodule. Each block has a fixed size depending on the used database: 30×30 and

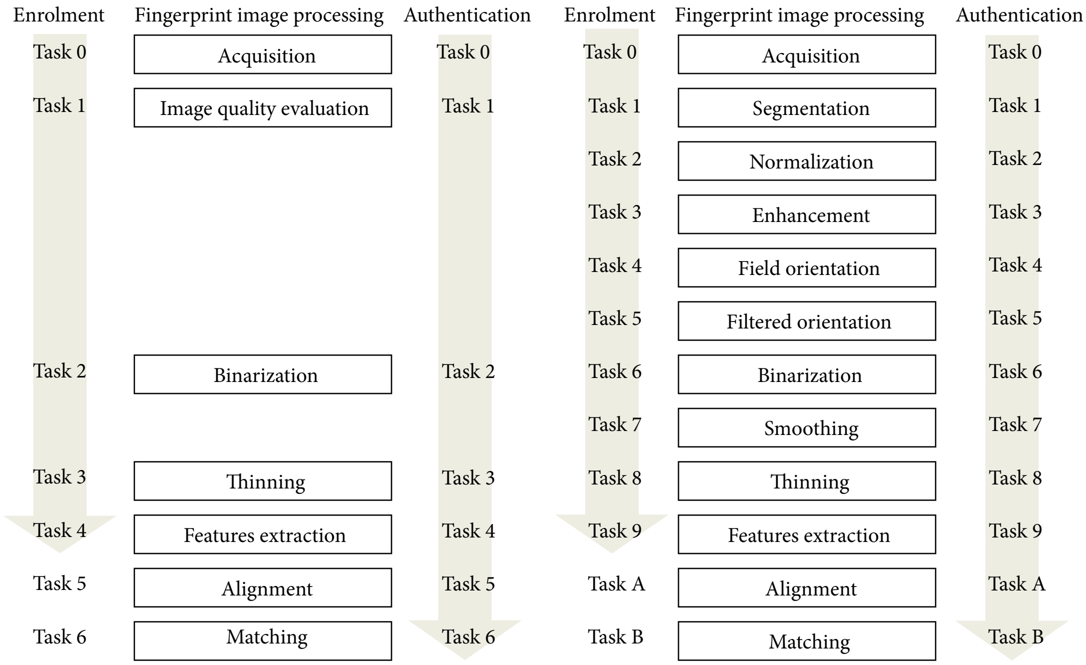


Figure 3: Comparison between the proposed AFAS (on the left) and the standard AFAS (on the right).

40 × 40 pixels for the FVC2002 DB2-B and the PolyU database, respectively. This system also counts the blocks sent and sets the *new_block* signal when the last pixel of the current block is sent.

3.1.2. Fingerprint_Quality_Level_Evaluator Submodule. This submodule identifies the dry and moist fingerprint portions allowing the subsequent features extraction task to discard them in order to reduce the potential false minutiae number. In concurrent way, the submodule checks if the fingerprint is centered over the image and calculates six indexes, each measuring an image qualitative characteristic. It performs a linear combination of them obtaining the final quality index. Finally, it classifies the image quality into two classes.

In the following subsections, the Fingerprint_Quality_Level_Evaluator submodules are described.

(1) Image_Blocks_Analyzer Submodule. This submodule is able to process block by block the fingerprint image. For each block it calculates, in a concurrent way, the following features:

(i) max and min gray level: these local values are used to calculate the global max and min gray level of the entire image;

(ii) gray levels average and variance: these values are used to classify blocks as foreground/background and as dry/moist/good;

(iii) ridges orientation certainty level (ocl): this value, only for foreground blocks, is added to the ocl_accumulator signal, subsequently used for the calculation of the 2nd index.

After that, in a concurrent way, it identifies the fingerprint high quality areas and calculates the fingerprint central position. The following subsections describe the main submodules of the proposed Image_Blocks_Analyzer submodule.

Orientation_Certainty_Level_Calculator Submodule. A fingerprint image block generally consists of ridges separated by valleys with the same orientation. Ridges and valleys constant structure and regular orientation can be used to evaluate the quality of each considered block. They are analytically calculated through the gradient of the gray levels along the x and y directions of a pixel [19]. The covariance matrix C of the gradient vector for an image block of M points is given by

$$C = E\left\{\begin{bmatrix} dx \\ dy \end{bmatrix}\begin{bmatrix} dx & dy \end{bmatrix}\right\} = \begin{bmatrix} a & c \\ c & b \end{bmatrix}, \quad (1)$$

where

$$E\{\bullet\} = \frac{1}{M}\sum_{M} \bullet . \quad (2)$$

The ridges orientation certainty level (ocl) is calculated as shown in

$$\text{ocl} = 100 * \frac{(a+b) - \sqrt{(a-b)^2 + 4c^2}}{(a+b) + \sqrt{(a-b)^2 + 4c^2}}. \quad (3)$$

With low (high) ocl values, the local structure and orientation of ridges and valleys are very regular (irregular), and therefore the block has good (wrong) quality (Figure 5). With more details, this submodule is further composed of two submodules, implementing a two-stage pipeline (Figure 6). While the first submodule calculates the covariance matrix C of block j, the second submodule calculates the ocl value of j-1 block.

Average_Calculator and Variance_Calculator Submodules. Average and variance are important characteristics for

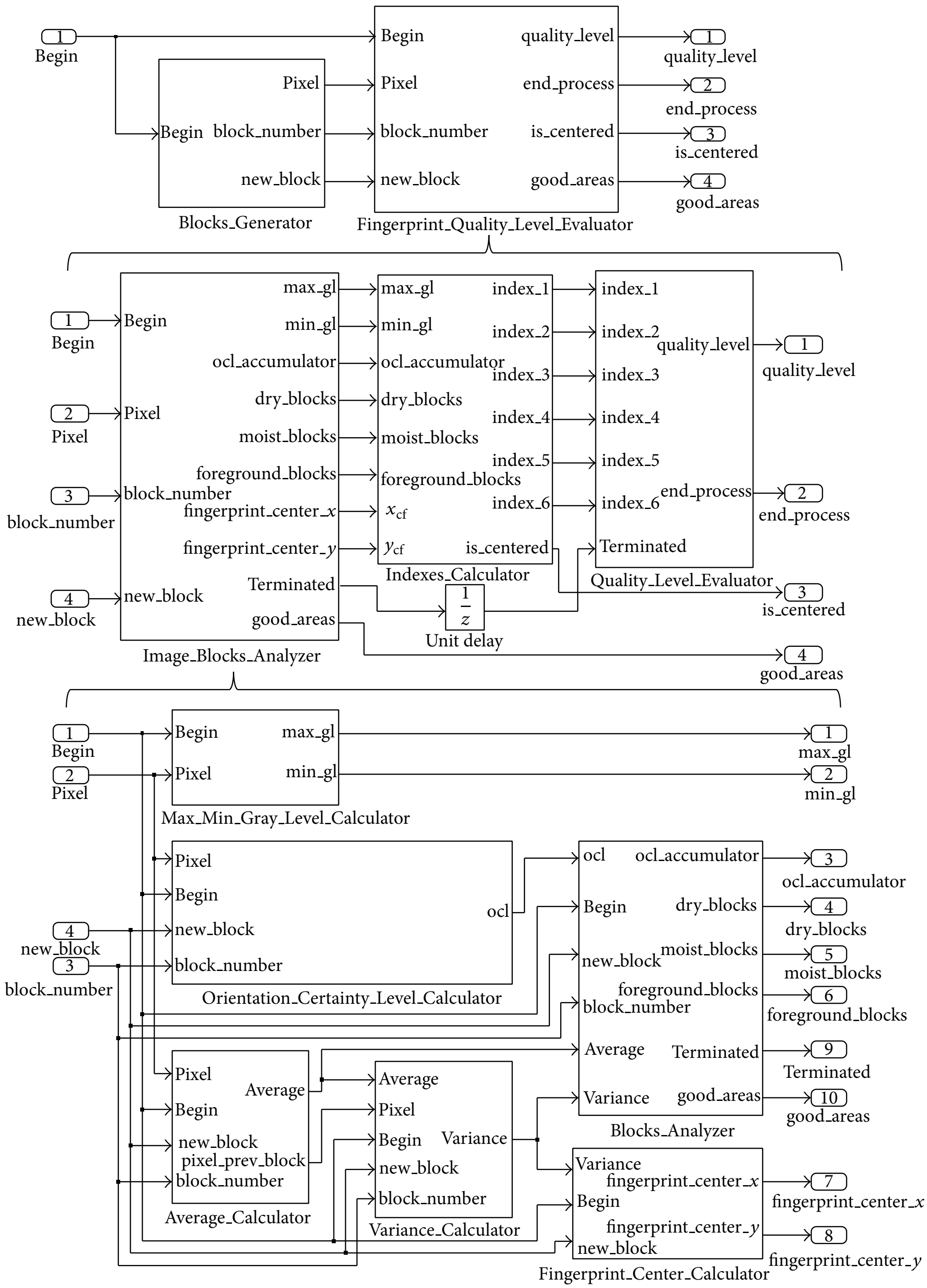


Figure 4: The proposed architecture evaluates the fingerprint image quality level. Fingerprint quality evaluator module is composed of image blocks analyzer submodule, indexes calculator submodule, and quality level evaluator submodule. The Image Block Analyzer submodule is composed of Max Min Level Calculator submodule, Orientation Certainty Level Calculator submodule, Average Calculator submodule, Variance Calculator submodule, Block Analyzer submodule, and Fingerprint Center Calculator submodule.

evaluating the block quality: average measures the luminosity, while variance measures the contrast. A low average value is linked to a block prevalently containing ridges (because it is dark), while a low variance value entails that the block does not contain any useful portion of the fingerprint (because it has a low contrast).

The Average_Calculator submodule stores the incoming block pixels on a shift register and sends the pixels of

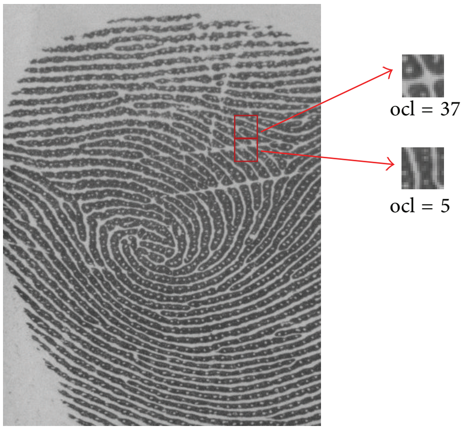


Figure 5: Examples of different ocl values.

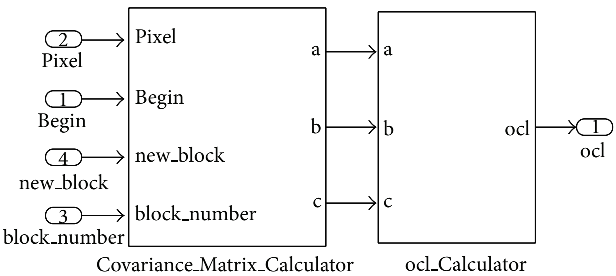


Figure 6: Orientation_Certainty_Level_Calculator submodule.

the previous block in order to achieve the best trade-off between requested resources and execution time.

Block_Analyzer Submodule. The ocl characteristic is not sufficient to quantify the clearness of the fingerprint ridges and valleys pattern when the skin humidity is also considered. For a moist block the ridges are too thick, since it has low average value. On the other hand, the ridges are too thin for a dry block, since it has a high average value. So, the average value is heavily influenced by the background gray level intensity (Figure 7). In this work, the gray level intensity of the image background is fixed to be the average value of the first image block, since it does not usually contain part of the fingerprint. If the block contains part of the fingerprint (i.e., the fingerprint covers the entire image) the background gray level is assumed as dark.

This submodule compares the average value of the first block with an experimental fixed threshold classifying the background as dark or bright and setting moist and dry thresholds. These values are experimentally fixed and depend on the used database. For example, on the FVC2002 DB2-B, the dry thresholds are 140 and 180 for bright and dark background, respectively, while the moist thresholds are 80 for dark background and 100 otherwise. Successively, it classifies each block as foreground or background using the incoming variance value. The foreground threshold is not influenced by the background gray level and it is experimentally fixed to 190.

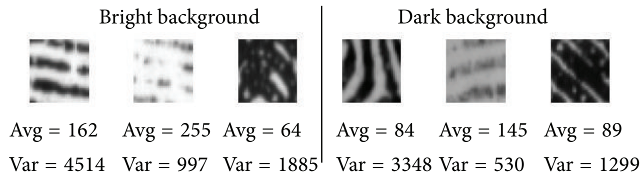


Figure 7: Examples of average and variance values with dark and bright background.

Fingerprint_Center_Calculator Submodule. This submodule calculates, in a concurrent way, the fingerprint central position (Figure 8). It checks if the considered block belongs to the column $N_x/2$, $N_x/4$, or $3N_x/4$. If so then, if it is of foreground, a value equal to the block size is added to the relevant column foreground accumulator (an accumulator for each considered column); otherwise only if this accumulator value is zero, the same value is added to the relevant column background accumulator (i.e., the background blocks below the fingerprint are discharged). Concurrently, the same check is performed on the rows $N_y/2$, $N_y/4$, or $3N_y/4$, and, in the same way, the relevant row background or foreground accumulator is increased. Finally, for the last block, the column foreground accumulator with the highest value is selected and the y-coordinate of the fingerprint's center is calculated as the sum of the half value stored in the selected foreground accumulator and the relevant column background accumulator value. Concurrently, the x-coordinate of the fingerprint's center is calculated in the same way.

(2) Indexes_Calculator Submodule. Among common quality indexes present in literature and reported in the related works section, this subsystem concurrently calculates six global indexes, designed in order to realize a module reducing used resources and execution time. To make all indexes compatible, they have normalized in the range of $[0, 100]$. High index value entails a good image quality.

Index1_Calculator Submodule. The first index measures the contrast between fingerprint and background. This value is calculated as the difference between the maximum and the minimum gray level value of the entire image:

$$\text{index\_1} = 100 * \frac{(\max\text{\_gl} - \min\text{\_gl})}{255}. \quad (4)$$

Index2_Calculator Submodule. The second index extends to the whole image the considerations about the block orientation certainty level estimation, thus globally measuring the clarity and continuity of ridges and valleys orientation. It is calculated by averaging all the ocl values relating to only foreground blocks:

$$\text{index\_2} = 100 - \frac{\text{ocl\_accumulator}}{\text{foreground\_blocks}}. \quad (5)$$

Index3_Calculator Submodule. The third index measures the humidity of the entire image and it is calculated as the ratio

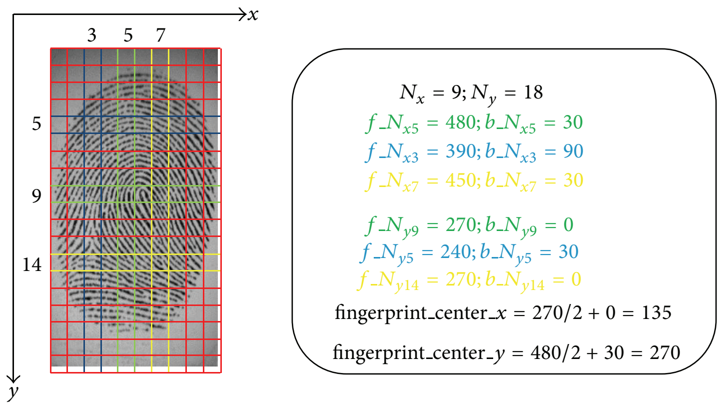


Figure 8: Example of a FVC2002 fingerprint's center calculation.

between the number of moist blocks and the number of foreground blocks:

$$\text{index\_3} = 100 - \left(100 * \frac{\text{moist\_blocks}}{\text{foreground\_blocks}}\right). \quad (6)$$

Index4_Calculator Submodule. The fourth index measures the dryness of the entire image and it is calculated as the ratio between the number of dry blocks and the number of foreground blocks:

$$\text{index\_4} = 100 - \left(100 * \frac{\text{dry\_blocks}}{\text{foreground\_blocks}}\right). \quad (7)$$

Index5_Calculator Submodule. The fifth index measures the image area occupied by the foreground blocks. It is an estimate of the fingerprint size over the entire image and it is calculated as the ratio between the number of foreground blocks and the total number of blocks:

$$\text{index\_5} = 100 * \frac{\text{foreground\_blocks}}{N}. \quad (8)$$

Index6_Calculator Submodule. The sixth index measures the position of the fingerprint over the entire image: too large translation caused by human behavior can generate an insufficient overlapping area between images captured from the same finger. It is calculated as the average of two values, $i6_x$ and $i6_y$:

$$\text{index\_6} = \frac{i6_x + i6_y}{2} \quad (9)$$

with

$$i6_x = 100 - \left(100 * \frac{|x_{cf} - x_{ci}|}{x_{ci}}\right),$$
$$i6_y = 100 - \left(100 * \frac{|y_{cf} - y_{ci}|}{y_{ci}}\right), \quad (10)$$

where x_{cf} and y_{cf} are the coordinates of the fingerprint's center, while x_{ci} and y_{ci} are the coordinates of the image's center.

In addition, this subsystem checks if the distance between the respective coordinates of the image's center and the fingerprint's center is lower than a threshold (experimentally fixed to 100) and then sets the *is_centered* signal.

(3) Quality_Level_Calculator Submodule. First, this subsystem calculates the final fingerprint quality index as linear combination of the previous six indexes. As described in [11], a linear regression method is used for weights calculation. They are experimentally determined by performing tests to observe the behavior of the change in the final quality index while one index is changing and the others are constant. Experimental results show that the most relevant indexes are ocl, fingerprint moisture, and fingerprint dryness. Then, by comparing the final quality index value with a threshold (experimentally fixed to 65), this subsystem classifies the image quality level as *Good* or *Bad*. Finally, the subsequent tasks are performed only if the quality is *Good* and the fingerprint is centered over the image.

3.2. Binarization Module. This module gives out an image where pixels assume a binary value: white as background and black as foreground (Figure 9). Binarization is performed using the local gray range technique described in [25]. In this adaptive technique the threshold is set at the average of the maximum and minimum gray values in a local window of size 9 × 9.

3.3. Thinning Module. This module reduces the ridge thickness to the unitary value (Figure 10), using the Zhang-Suen algorithm described in [26]. For the realization of the thinning algorithm on FPGA, a 3 × 3 mask has been used in order to implement a two-stage pipeline.

3.4. Features Extraction Module. For the minutiae extraction, the algorithm proposed in [14] has been optimized and extended: in order to reduce the system execution time and the potential false minutiae, only the good areas, computed by the image quality evaluation module, of a central area of 240 × 320 pixels, are processed. The proposed approach improves the performance of a standard embedded AFAS, such as

Figure 9: Example of fingerprint binarization.

Figure 10: Example of fingerprint thinning.

would a Gabor filtering process in order to reconstruct the poor quality areas. Figure 11 shows the minutiae extracted using the Gabor filter, to reconstruct image areas of poor quality, and using the image quality evaluation, to discard those areas. As depicted, the Gabor filter approach introduces two false bifurcations and discards two terminations, while the proposed approach discards two bifurcations and one termination.

3.5. Alignment and Matching Modules. The computation of a likelihood ratio in fingerprint authentication is obtained by trying all the possible overlapping of the acquired fingerprint with the one enrolled in the system [12]. The rototranslation parameters computation is based on the identification of two similar pairs of minutiae belonging to both fingerprints (Figure 12). A threshold (experimentally fixed to 175) based on Euclidean distance is used to generate the minutiae pairs.

First, rototranslation parameters are computed only if the value of Euclidean distance between each minutiae pair of both fingerprints is lower than a threshold (experimentally fixed to 20). The rotation parameter is based on the differences between the corresponding angles in the selected minutiae pairs. If the gap between each of these differences with respect to the other is lower than a threshold (experimentally fixed to 1.5) the rotation parameter is the average of the calculated differences. In the same way, the translation parameter is based on the differences between the respective Cartesian coordinates in the selected minutiae pairs. If the gap between each coordinate distance is lower than a threshold (experimentally fixed to 30) the translation parameter is the average of the respective calculated differences.

Then, the rototranslation is performed and, for each minutia, differences between respective coordinates x-y (diff_{xy}) and angles ($\text{diff}_{\text{theta}}$) are calculated. Only when these differences are lower than two thresholds ($xy_{\text{threshold}}$ and $\text{theta}_{\text{threshold}}$, experimentally fixed to 15 and 0.785, resp.) a first partial score is obtained and normalized in the range of $[0, 1]$. The complete score is calculated as

$$s_i = 0.75 * \left(1 - \frac{\max\left(\text{diff}_{xy}\right)}{xy_{\text{threshold}}}\right) + 0.25 * \left(1 - \frac{\max\left(\text{diff}_{\text{theta}}\right)}{\text{theta}_{\text{threshold}}}\right), \qquad (11)$$

where higher importance has been made to the differences between respective coordinates rather than to angles, due to rounding problems on data.

Finally, among all complete scores, only the greater is considered. Therefore, the final matching score is calculated adding the 12 highest obtained scores. In accordance with the USA guidelines in the forensic field, when two fingerprints have a minimum of 12 corresponding minutiae, these are regarded as coming from the same finger [27].

4. Experimental Results

The proposed approach introduces interesting characteristics for mobile devices. The architectural implementation on FPGA, considering its working frequency (50 MHz), achieves the performance of the highly competitive systems, realizing a good trade-off between accuracy rate, used resources, and execution time. To evaluate the accuracy performances of the proposed authentication system, the well-known false recognition rate (FRR) and false acceptance rate (FAR) indexes have been used and two different free databases with different characteristics in terms of resolution and quality have been used.

The following subsections report the used databases and datasets description, the execution time, the required hardware resources, and the authentication performance of the proposed AFAS.

4.1. Databases Description

4.1.1. FVC2002 DB2-B Database. This free downloadable database has been made available for the second edition of the international fingerprint verification competition [28]. It contains 80 fingerprint images of 296 × 560 pixels, with

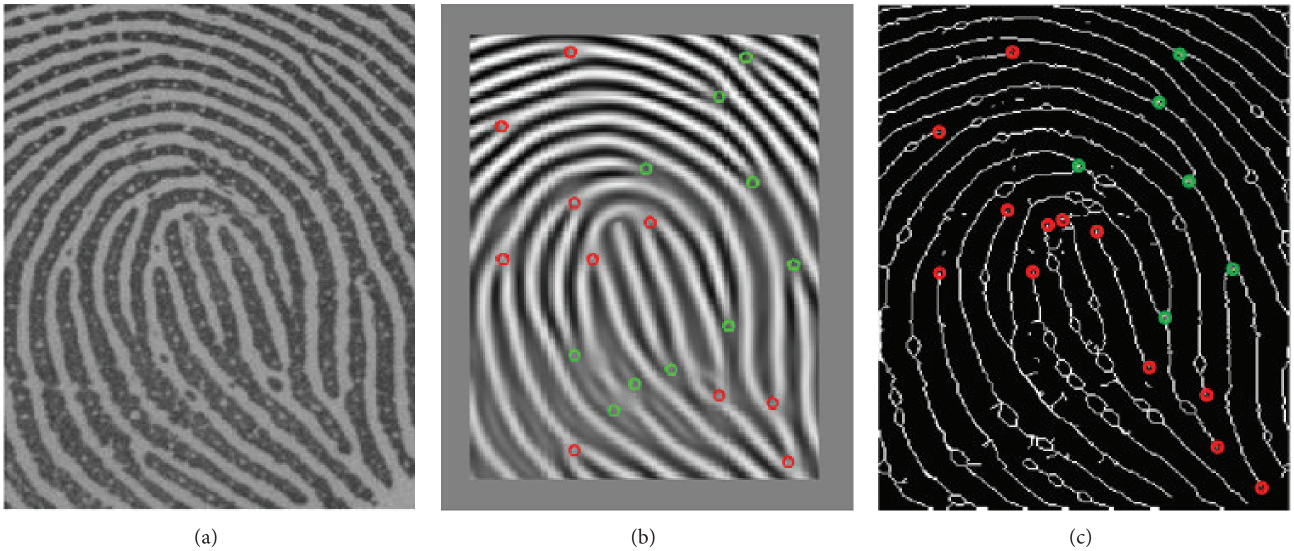


Figure 11: (a) Image 2_1_5 from PolyU database; (b) minutiae extracted with a Gabor filter and without the image quality evaluation; (c) minutiae extracted with the image quality evaluation and without a Gabor filter.

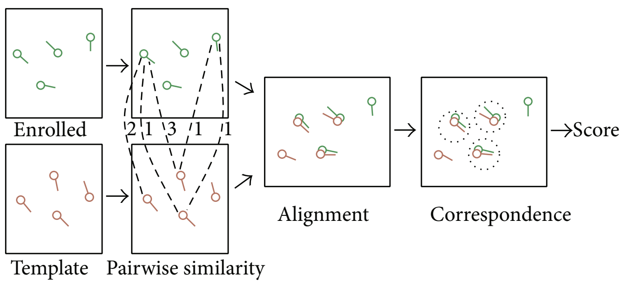


Figure 12: Rototranslation parameters computation.

a resolution of 569 dpi. The images has been acquired from 10 users (8 acquisitions for user of the same finger), via the scanner Biometrika FX2000 [29], with a maximum rotation of about 35 degrees between impressions (Figure 13).

4.1.2. PolyU Database. This free downloadable database has been built at the Hong Kong Polytechnic University [16]. It contains 1480 fingerprint images of 480 × 640 pixels, with a resolution around 1,200 dpi of 148 users (10 acquisitions for user of two fingers, Figure 14). Each image name has been described using three numbers in the following way: first number represents the user, second number represents the finger, and third number represents the different acquisition.

4.1.3. Datasets Description. Starting from the above description databases, two different datasets have been built:

(i) the *dataset1* has been generated using the entire FVC2002 DB2-B database (10 users, 8 acquisitions for user);

(ii) the *dataset2* has been generated using a consistent subset of the PolyU database (100 users with 5 acquisitions for user of the same finger).

Table 1: FAR and FRR indexes of the three performed tests.

Test number	FAR	FRR
1.	0%	6.25%
2.	0%	8.00%
3.	0%	9.00%

4.2. Authentication Performance. Starting from the AFAS described in [14] and used as comparison, three different tests have been conducted:

(1) the AFAS has been extended with the proposed fingerprint image quality evaluation module and tested on the *dataset1*;

(2) the AFAS has been extended with the proposed fingerprint image quality evaluation module and, moreover, the matching algorithm has been replaced with the advanced technique, based on partial fingerprints, proposed in [12] and tested on the *dataset2*;

(3) the AFAS has been extended with a preprocessing task, based on the Gabor filter, to enhance fingerprint images and, moreover, the matching algorithm has been replaced with the advanced technique, based on partial fingerprints, proposed in [12] and tested on the *dataset2*.

Table 1 illustrates the authentication performance in terms of FAR and FRR indexes for the three performed tests.

4.3. Execution Time. The following tables (Tables 2, 3, and 4) and Figure 15 illustrate the elaboration times, for the three performed tests, required by each single task, with a working frequency of 50 MHz.

(a) (b)

Figure 13: Two example images of the FVC2002 DB2-B acquired by Biometrika FX2000 sensor.

(a) (b)

Figure 14: Two example images of the Hong Kong Polytechnic University.

Table 2: Execution times of test number 1.

Task	Execution time (msec)
Image quality evaluation	3.9
Binarization	2.2
Thinning	39.0
Minutiae extraction	13.7
Matching	3.8
Total	62.6

Table 3: Execution times of test number 2.

Task	Execution time (msec)
Image quality evaluation	3.9
Binarization	2.2
Thinning	39.0
Minutiae extraction	13.7
Matching	2.35×10^3
Total	2.4×10^3

4.4. Hardware Resources. The following tables (Tables 5, 6, and 7) depict the required hardware resources, for the three performed tests, used by each single task on the Agility RC2000 development board. Figure 16 illustrates the total used hardware resources for the three performed tests.

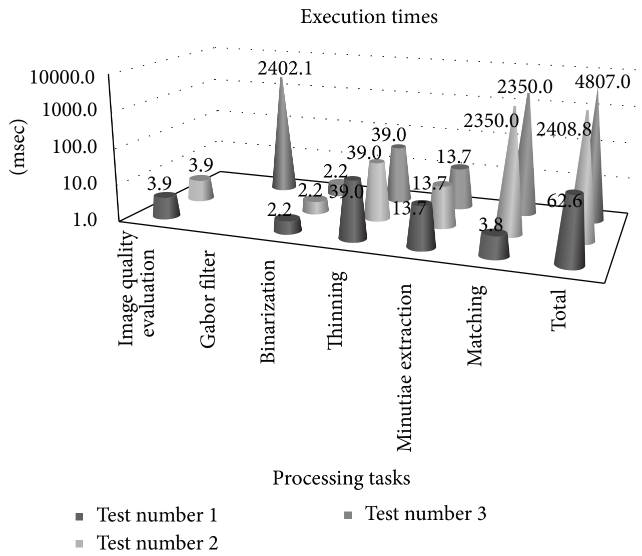


Figure 15: Elaboration times required by each processing task for the three performed tests.

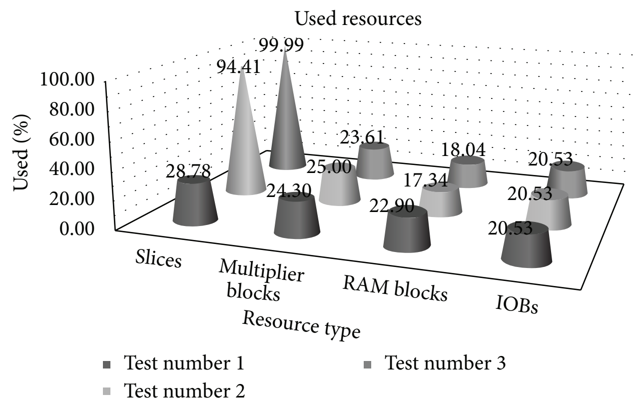


Figure 16: Used hardware resources, for the three performed tests.

Table 4: Execution times of test number 3.

Task	Execution time (msec)
Gabor filter	2.4×10^3
Binarization	2.2
Thinning	39.0
Minutiae extraction	13.7
Matching	2.35×10^3
Total	4.8×10^3

4.5. Discussion and Comparisons. User authentication is one of the most challenging issues for system and network security. A robust authentication mechanism is based on the use of biometric access control methods, processing one or more biometrics (such as a fingerprint). There are many approaches to deal with fingerprint verification. In recent literature publications, few findings have been on design and prototyping of an embedded biometric recognizer. For example, in [30] the authors proposed an implementation of a hardware identification system. However, the fingerprint matching phase was not developed and presented, so that no direct comparison with this work can be addressed. The remaining fingerprint processing tasks had been implemented in a FPGA device with a clock frequency of 27.65 MHz and a processing time of 589.6 ms. Compared with this system, the achieved execution times denote high performance levels. In [11] the authors use local texture features as well as some global factors such as the standard deviation of Gabor features, the foreground area and central position, the number of minutiae, and the existence of singular points. They produce a good analysis about equal error rate (EER) for three databases: FVC2002 DB2A, Fujitsu database, and FVC2002 DB4A. In [18] the authors have developed a software fast fingerprint enhancement algorithm which can adaptively improve the clarity of ridge and valley structures based on the local ridge orientation and ridge frequency. Experimental results show that their enhancement algorithm is capable of improving both the goodness index and the verification performance. The whole execution time of the enhancement algorithm on a Pentium 200MHZ is 2.49 sec, with FAR = 0.01% and FRR = 27% (without enhancement) and FRR = 9% (with enhancement) using the MSU fingerprint database (700 live-scan images; 10 per individual each). In [23, 24] the authors present an image quality assessment software technique for a novel fingerprint multimodal algorithm to provide high accuracy under nonideal conditions. Their study was based on a small number of minutia features. This is likely to be the case with latent fingerprints collected at a crime scene. Specifically, the performance of their fusion algorithm is studied when the number of minutiae is between 5 and 10. Experimental results show that while the performance of existing fusion algorithm decreases if compared to the performance of complete rolled fingerprints, the proposed approach is able to compensate for the limited partial information. The approach shows FRR between 91.35% and 97.98% with FAR = 0.01%, using a comprehensive database with rolled and partial fingerprint images of different quality and arbitrary number of features.

5. Conclusion

In this work a novel embedded AFAS improving the performance in terms of both used resources and execution time has been proposed. It is focused on the raw image quality evaluation of the acquired fingerprint, identifying areas of poor quality. It is designed to find a measure to characterize the quality of raw fingerprint images, using only the information obtained in the acquisition step. In addition, an advanced matching technique for user recognition using partial fingerprints has been developed to increase system accuracy. The best achieved FAR and FRR indexes are 0% and 6.25%, respectively. The required elaboration time is 62.6 ms with a working frequency of 50 MHz.

Table 5: Used resources of test number 1.

Resource type	Image quality evaluation	Binarization	Thinning	Minutiae extraction	Matching
Slices	5.83%	0.14%	0.67%	21.80%	0.34%
Multiplier blocks	4.17%	0.00%	0.00%	19.44%	0.69%
RAM blocks	0.69%	0.69%	0.69%	14.58%	6.25%
IOBs	4.98%	4.98%	0.00%	0.00%	10.57%

Table 6: Used resources of test number 2.

Resource type	Image quality evaluation	Binarization	Thinning	Minutiae extraction	Matching
Slices	5.83%	0.14%	0.67%	21.80%	65.97%
Multiplier blocks	4.17%	0.00%	0.00%	19.44%	1.39%
RAM blocks	0.69%	0.69%	0.69%	14.58%	0.69%
IOBs	4.98%	4.98%	0.00%	0.00%	10.57%

Table 7: Used resources of test number 3.

Resource type	Gabor filter	Binarization	Thinning	Minutiae extraction	Matching
Slices	11.41%	0.14%	0.67%	21.80%	65.97%
Multiplier blocks	2.78%	0.00%	0.00%	19.44%	1.39%
RAM blocks	1.39%	0.69%	0.69%	14.58%	0.69%
IOBs	4.98%	4.98%	0.00%	0.00%	10.57%

The proposed prototype has been implemented on the Agility RC2000 development board, addressing interesting characteristics for security in mobile device applications and enabling its use in commercial, banking, and government scenarios.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] Apple Inc., http://support.apple.com/kb/HT5883.

[2] Samsung, http://www.samsung.com/it/consumer/mobile-devices/smartphones/smartphones/SM-G900FZKAITV-spec.

[3] C. Militello, V. Conti, F. Sorbello, and S. Vitabile, "An embedded iris recognizer for portable and mobile devices," *International Journal of Computer Systems Science and Engineering*, vol. 25, no. 2, pp. 119–131, 2010.

[4] V. Conti, C. Militello, F. Sorbello, and S. Vitabile, "A multimodal technique for an embedded fingerprint recognizer in mobile payment systems," *International Journal of Mobile Information Systems*, vol. 5, no. 2, pp. 105–124, 2009.

[5] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, New York, NY, USA, 2003.

[6] V. Conti, C. Militello, F. Sorbello, and S. Vitabile, "An embedded fingerprints classification system based on weightless neural networks," *Frontiers in Artificial Intelligence and Applications*, vol. 193, no. 1, pp. 67–75, 2009.

[7] D. Batra, G. Singhal, and S. Chaudhury, "Gabor filter based fingerprint classification using support vector machines," in *Proceedings of the IEEE 1st India Annual Conference (INDICON '04)*, pp. 256–261, December 2004.

[8] J. Hu and M. Xie, "Fingerprint classification based on genetic programming," in *Proceedings of the 2nd International Conference on Computer Engineering and Technology (ICCET '10)*, vol. 6, pp. 193–196, Chengdu, China, April 2010.

[9] A. Tariq, M. U. Akram, and S. A. Khan, "An automated system for fingerprint classification using singular points for biometric security," in *Proceedings of the International Conference for Internet Technology and Secured Transactions (ICITST '11)*, pp. 170–175, December 2011.

[10] V. Conti, C. Militello, F. Sorbello, and S. Vitabile, "A frequency-based approach for features fusion in fingerprint and iris multimodal biometric identification systems," *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews*, vol. 40, no. 4, pp. 384–395, 2010.

[11] J. Qi, D. Abdurrachim, D. Li, and H. Kunieda, "A hybrid method for fingerprint image quality calculation," in *Proceedings of the 4th IEEE Workshop on Automatic Identification Advanced Technologies*, pp. 124–129, October 2005.

[12] V. Conti, G. Vitello, F. Sorbello, and S. Vitabile, "An advanced technique for user identification using partial fingerprint," in *Proceedings of the 7th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS '13)*, pp. 236–242, July 2013.

[13] Xilinx Inc, http://www.xilinx.com/support/documentation/data_sheets/ds031.pdf.

[14] V. Conti, S. Vitabile, G. Vitello, and F. Sorbello, "An embedded biometric sensor for ubiquitous authentication," in *Proceedings of the AEIT Annual Conference: Innovation and Scientific and Technical Culture for Development*, October 2013.

[15] FVC Databases, http://bias.csr.unibo.it/fvc2002/databases.asp.

[16] PolyU Database, http://www4.comp.polyu.edu.hk/~biometrics/HRF/HRF_old.htm.

[17] E. Tabassi, C. Wilson, and C. Watson, "Fingerprint image quality," NIST Research Report NISTIR7151, 2004.

[18] L. Hong, Y. Wan, and A. Jain, "Fingerprint image enhancement: algorithm and performance evaluation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 8, pp. 777–789, 1998.

[19] E. Lim, X. D. Jiang, and W. Y. Yau, "Fingerprint quality and validity analysis," in *Proceedings of the International IEEE Conference on Image Processing*, vol. 1, pp. 469–472, September 2002.

[20] X. Yang and Y. Luo, "A classification method of fingerprint quality based on neural network," in *Proceedings of the International Conference on Multimedia Technology (ICMT '11)*, pp. 20–23, IEEE, Hangzhou, China, July 2011.

[21] F.-J. An and X.-P. Cheng, "Approch for estimating the quality of fingerprint Image based on the character of ridge and valley lines," in *Proceedings of the International Conference on Wavelet Active Media Technology and Information Processing (ICWAMTIP '12)*, pp. 113–116, Chengdu, China, December 2012.

[22] S. Lee, H. Choi, K. Choi, and J. Kim, "Fingerprint-quality index using gradient components," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 4, pp. 792–800, 2008.

[23] M. Vatsa, R. Singh, A. Noore, and M. M. Houck, "Quality-augmented fusion of level-2 and level-3 fingerprint information using DSm theory," *International Journal of Approximate Reasoning*, vol. 50, no. 1, pp. 51–61, 2009.

[24] M. Vatsa, R. Singh, A. Noore, and S. K. Singh, "Quality induced fingerprint identification using extended feature set," in *Proceedings of the 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems*, pp. 1–6, October 2008.

[25] J. Bernsen, "Dynamic thresholding of gray-level images," in *Proceedings of the 8th International Conference on Pattern Recognition*, pp. 1251–1255, Paris, France, 1986.

[26] T. Y. Zhang and C. Y. Suen, "A fast parallel algorithm for thinning digital patterns," *Communications of the ACM*, vol. 27, no. 3, pp. 236–239, 1984.

[27] NSCT, "Fingerprint Recognition," http://www.biometrics.gov/documents/fingerprintrec.pdf.

[28] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC: The Second International Competition for Fingerprint Verification Algorithms," http://bias.csr.unibo.it/fvc2002/.

[29] Biometrika FX2000, http://www.biometrika.it/eng/fx2000.html.

[30] V. Bonato, R. F. Molz, J. C. Furtado, M. F. Ferrão, F. G. Moraes, and M. F. Ferrão, "Propose of a hardware implementation for fingerprint systems," in *Field Programmable Logic and Application: 13th International Conference, FPL 2003, Lisbon, Portugal, September 1–3, 2003 Proceedings*, vol. 2778 of *Lecture Notes in Computer Science*, pp. 1158–1161, 2003.

Hindawi Publishing Corporation
Mobile Information Systems
Volume 2015, Article ID 308194, 11 pages
http://dx.doi.org/10.1155/2015/308194

Research Article

Resilient Disaster Network Based on Software Defined Cognitive Wireless Network Technology

Goshi Sato,[1] Noriki Uchida,[2] and Yoshitaka Shibata[1]

[1]*Iwate Prefectural University, 152-52 Takizawa, Iwate 0200173, Japan*
[2]*Saitama Institute of Technology, Fukaya, Saitama Prefecture 369-0203, Japan*

Correspondence should be addressed to Goshi Sato; g236l001@s.iwate-pu.ac.jp

Received 1 September 2014; Accepted 1 September 2014

Academic Editor: Ilsun You

In order to temporally recover the information network infrastructure in disaster areas from the Great East Japan Earthquake in 2011, various wireless network technologies such as satellite IP network, 3G, and Wi-Fi were effectively used. However, since those wireless networks are individually introduced and installed but not totally integrated, some of networks were congested due to the sudden network traffic generation and unbalanced traffic distribution, and eventually the total network could not effectively function. In this paper, we propose a disaster resilient network which integrates various wireless networks into a cognitive wireless network that users can use as an access network to the Internet at the serious disaster occurrence. We designed and developed the disaster resilient network based on software defined network (SDN) technology to automatically select the best network link and route among the possible access networks to the Internet by periodically monitoring their network states and evaluate those using extended AHP method. In order to verify the usefulness of our proposed system, a prototype system is constructed and its performance is evaluated.

1. Introduction

As advent of recent wireless communication technology, many applications on various fields such as public wireless networks, disaster information networks, or intelligent traffic transportation systems are developed [1–3]. In particular, wireless communication system plays a very important role as disaster use. In fact, in the Great East Japan Earthquake on March 11, 2011, the communication access networks to the Internet in disaster areas were recovered by the 3G mobile communication vehicles and satellite communication system. However, those used networks were introduced individually and operated by each of the mobile phone companies; some mobile phones could not be used on different company's network. The handover function between the different company's networks could not be supported even though one network is very congested and the others have enough available network resources.

In this paper, we introduce a novel cognitive wireless network system which is able to select the best link and route that can provide the best network performance among possible networks by integrating the different type of wireless networks such as 3G, LTE, WiMAX, Wi-Fi, and satellite networks with the different network characteristics such as throughput, RTT, and packet loss rate and periodically monitoring those network states [4, 5]. By exchanging the disaster information through this stratified network, the system can persistently continue to provide communication capability and can automatically perform handover to the other access networks which have enough available network resources by wireless cognitive network functions even if some network node and line failures occur in a part of the network infrastructure. We designed and developed our system as a prototype system based on the SDN technology [6] by integrating 3G, LTE, WiMAX, and satellite network and constructed a testbed disaster network as access network by connecting three different locations in our Iwate prefecture which were seriously damaged by the tsunami from the Great East Japan Earthquake on March 11, 2011.

Required information varies in time before/after disaster

Bandwidth-oriented period

Objects	Required information	t_1	t_2	t_x	t_3	t_4	t_5	t_6
Stricken area resident	Forecast	△	○	Disaster				
	Evacuation		○		◎			
	Resident safety				◎	◎	○	△
	Disaster status				◎	○		
	Traffic				○	◎	◎	
	Supplied materials					◎	○	
	Public service					○	◎	
	Life line					○	◎	
	Local government					○	◎	
Relatives	Resident safety				◎	◎	○	
	Disaster status				◎	○	△	
	Supplied materials					○	◎	

Connection-oriented period

Figure 1: Required disaster information.

2. Disaster Information

From the investigation of the previous large natural disasters, the required information varies in time before and after disaster as shown in Figure 1 [7]. Just before the disaster, the forecast and evacuation information are required while, just after the disaster evacuation, resident safety and disaster status information are required where t_1 is normal time, t_2 is estimated period, t_x is time at disaster, t_3 is the period just after the disaster, t_4 is stable period, t_5 is recovery period, and t_6 is recovered time.

Just after disaster happened, the communication network around the disaster area maybe damaged and must be quickly recovered although the required network throughput is small; while being at stable and recovery period, the required throughput will be increased as the time elapsed. Thus, in order to achieve the emergency communication immediately after a disaster, quick recovery of the information network must be made.

3. System Configuration

Figure 2 shows our proposed disaster information network which consisted of wireless cognitive network switches combined with multiple different networks and a cognitive wireless controller. Wired networks can be also used as access networks. The cognitive wireless switches periodically monitor their network states at the several locations and send the monitored network states data to the cognitive wireless controller at the disaster headquarter. All of the received data are accumulated in the cognitive wireless controller and evaluated to select the best access network by weighting those possible access networks. The satellite network is used as a control channel for SDN to exchange the data between the cognitive switches. Each cognitive switch determines the suitable outgoing network for the packets to be send from the incoming network based on the message from the cognitive controller. In order to determine the best performance network, the following techniques perform important roles:

(i) network monitoring technology to detect the change of network performance states;

(ii) optimal selection method to decide the best access network;

(iii) packet control technology by OpenFlow [8] which changes the link and route to the switch to the best access network.

As monitoring the packet delay, ping tool is used between the observation server and the cognitive wireless switch in a specified time period by averaging the round trip time (TTL) of the proved packets. With packet loss rate monitoring, ping tool is also used by counting the nonreplying packets.

In our system, in order to detect the change of the network states, the wireless cognitive switch has network monitoring function.

The monitored states include the following parameters:

(i) link-up/down signal of network link;

(ii) throughput;

(iii) RTT between the observation server and each of the wireless cognitive switches;

(iv) packet loss rate between the observation server and each of the cognitive switches.

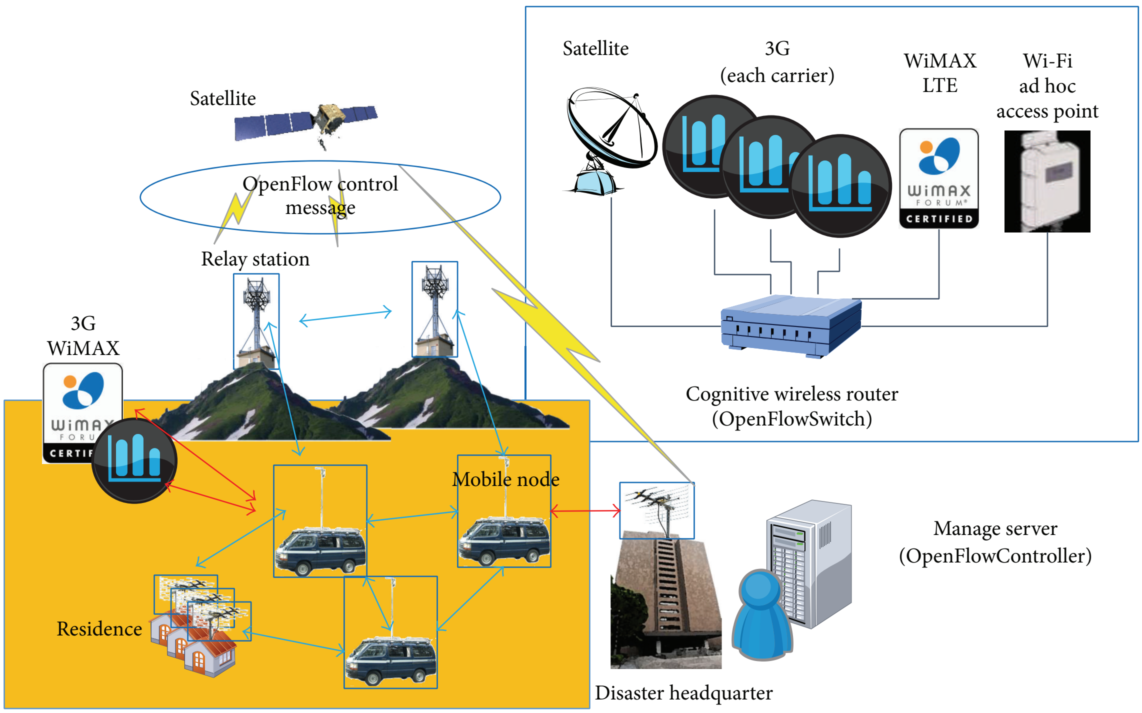


Figure 2: System configuration.

With monitoring the network throughput, two methods including passive and active methods are possible [9]. In passive methods, the throughput is calculated by implementing the monitoring function at all of the routers which the packets pass through. In active method, on the other hand, proved packets are transmitted between the end-to-end terminals [10]. In passive method, the monitoring functions have to be installed on all of the routers where packets pass through. This is very difficult because the Internet is huge and managed by different organizations. Therefore, for this reason, in our system, the active method is applied. Furthermore, there are two active methods including available bandwidth measuring methods such as *Iperf* and packet train methods such as *pathChirp* and *PathQuick* [11, 12]. In the available bandwidth measuring method, a large number of packets are inserted, while, in the packet train method, only a limited number of the probe packets are used in a limited period. For this reason, the packet train method is applied in our system.

At monitoring the packet delay, *ping* tool is used between the observation server and the cognitive wireless switch in a specified time period by averaging the round trip time (TTL) of the probe packets. With packet loss rate monitoring, *ping* tool is also used by counting the nonreplying packets.

4. Link Selection Method

4.1. Proposed Method Overview. Our cognitive radio router is equipped with a multiple access network. The system periodically monitors the performance of the wireless network access multiple links and calculates the priority of each access network by extending AHP method based on the parameter values obtained as results of the monitoring. Thus, the system determines the link of an access network based on the priority [13, 14] as shown in Figure 3.

4.2. AHP Method Overview. In this section, we describe the detail of AHP to be used in the decision-making in the access network switching. AHP is one of the decision-making processes and a more structural approach is used when performing a complicated decision. AHP was proposed in the 1970s by Satty et al. AHP [15] is capable of evaluation of alternatives and quantification of elements by performing the structure of the decision problem. The calculation process is performed in the order of "hierarchy of the problem," "pair comparative evaluation for criteria," "pair comparative evaluation of alternatives," and "the calculation of the total value."

Figure 4 is an example of a layered hierarchy by AHP and is a case of selecting the optimal wireless link between adjacent nodes. In order to solve the problem caused by AHP, it is necessary to stratify the problem first. In this study, we set a goal such as "select the best radio link in video communication" or "select the best radio link of connectivity." Next, in order to select the link that is the most suitable one for a user's request, appropriate network state values (throughput, delay, and packet loss rate) are set. And p_1 priority is determined based on the pairwise comparison of the evaluation criteria. On the other hand, p_2 priority is determined from the measured value of each alternative.

After that, the hierarchical priorities for evaluation criteria are calculated. As an example, we describe a method of calculating the priority by the measuring network performance. The number of evaluation criteria is defined as n, the weight of each term is defined as "$w_1, w_2, \ldots, w_n$," and pair comparison

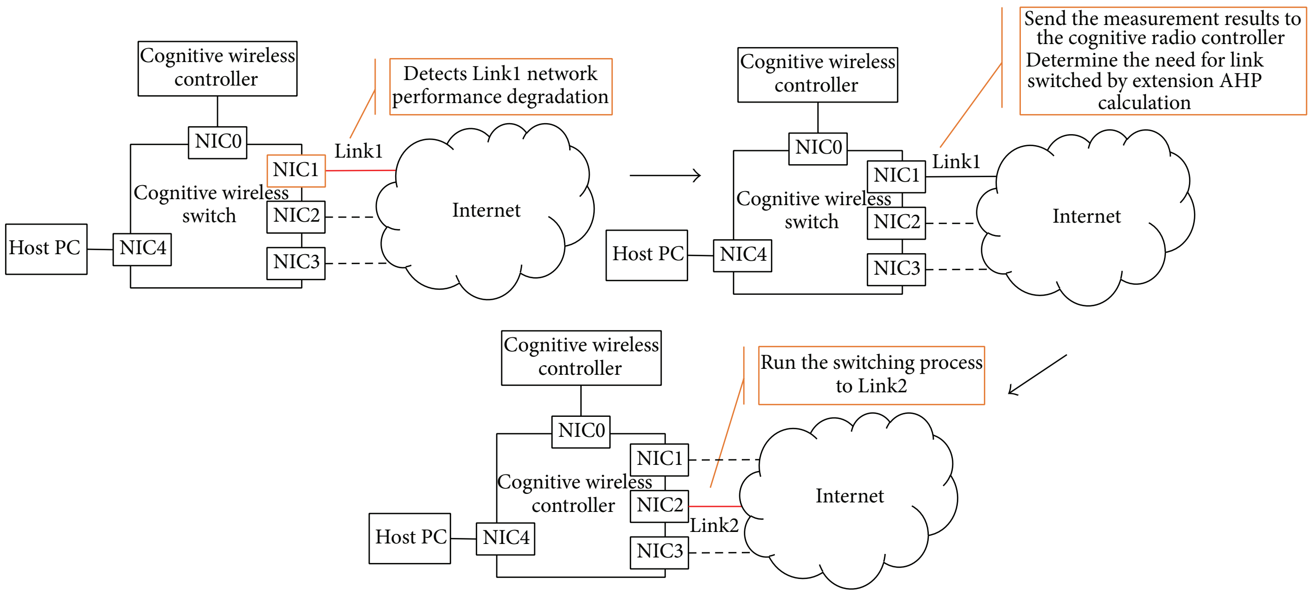


Figure 3: Link selection method overview.

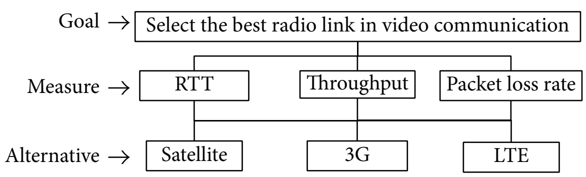


Figure 4: Examples of AHP hierarchy.

of each element is expressed as $a_{ij} = w_i/w_j$. Furthermore, these pair comparisons can be expressed as A:

$$A = \begin{bmatrix} \frac{w_1}{w_1} & \cdots & \frac{w_1}{w_j} & \cdots & \frac{w_1}{w_n} \\ \vdots & & \vdots & & \vdots \\ \frac{w_i}{w_1} & \cdots & \frac{w_i}{w_j} & \cdots & \frac{w_i}{w_n} \\ \vdots & & \vdots & & \vdots \\ \frac{w_n}{w_1} & \cdots & \frac{w_n}{w_j} & \cdots & \frac{w_n}{w_n} \end{bmatrix} \equiv \begin{bmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ a_{i1} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn} \end{bmatrix}. \quad (1)$$

A_{norm} normal matrix can be expressed as follows:

$$A_{\text{norm}} = \begin{bmatrix} b_{11} & \cdots & b_{1j} & \cdots & b_{1n} \\ \vdots & & \vdots & & \vdots \\ b_{i1} & \cdots & b_{ij} & \cdots & b_{in} \\ \vdots & & \vdots & & \vdots \\ b_{n1} & \cdots & b_{nj} & \cdots & b_{nn} \end{bmatrix}, \quad (2)$$

Table 1: Pairwise comparison matrix of evaluation.

	PER	RTT	Throughput
Goal 1 (video)			
PER	1	3	1/2
RTT	1/3	1	1/5
Throughput	2	5	1
Goal 2 (VoIP)			
PER	1	1/2	3
RTT	2	1	5
Throughput	1/3	1/5	1
Goal 3 (text)			
PER	1	5	5
RTT	1/5	1	1
Throughput	1/5	1	1

where

$$b_{ij} = \frac{a_{ij}}{\sum_{k=1}^{n} a_{kj}}. \quad (3)$$

In addition, each priority P_i of evaluation criteria is calculated by the following equation:

$$p_i = \frac{\sum_{l=1}^{n} b_{il}}{n}. \quad (4)$$

Weight w_n of each evaluation criterion with the range 1–9 is used to compute priority P_i and pairwise comparison matrix a_{ij}. Table of evaluation criteria for each purpose is shown in Table 1.

Therefore, priorities $P_1 \sim P_3$ of evaluation criteria for each goal are shown in Table 2.

Next, alternatively, priority is calculated for each alternative with the weight. In this paper, the priority calculation of alternative considers a change in the wireless network.

Table 2: Result of evaluation priority.

Propose	PER	RTT	Throughput
Goal 1 (video)	0.3092	0.1096	0.5813
Goal 2 (VoIP)	0.3092	0.5813	0.1096
Goal 3 (text)	0.7143	0.1429	0.1429

Therefore, after calculating the weight w_n using the measured values of the network state, this weight is applied to calculate the priority of each alternative.

Then, the total value is calculated using the priority of each alternative with the evaluation criteria. Total value is determined by the sum of the products of the priority of alternatives and weights of the evaluation criteria. Finally, the maximum total value of alternatives is selected for optimal wireless access network.

4.3. Extended AHP Method. In this study, we introduce an extension of AHP to determine the wireless access network by the cognitive radio device. To respond to the network state changes caused by the movement or external factors of network environment, the measured value of the network states is used for the calculation of the weights of alternatives. The weight of each alternative is defined as S_i. u_i is defined as the upper limit of each alternative. l_i is defined as the lower limit. Further, n_i is defined as the moving average of the measurement period and is determined by the weight (5) for PER (packet error rate) and RTT (round trip time).

On the other hand, the scale of the alternatives is different as shown in (6), and the upper limit of the throughput is defined as $u_{\max}$. Furthermore, in order to smooth the fluctuation by the measuring, the moving average of the measured values is defined as "$n_i = 0.6x_i + 0.3x_{i-1} + 0.1x_{i-2}$" (where x_i is defined as a network measurement value of i second time):

$$S_i = \begin{cases} \left\lceil 1 - \dfrac{n_i - l_i}{u_i - l_i} \right\rceil \times 10; & l_i < n_i < u_i \\ 1; & n_i \geq u_i \\ 9; & n_i \leq l_i, \end{cases} \tag{5}$$

$$S_i = \left\lceil \frac{n_i - l_i}{u_{\max} - l_i} \right\rceil \times 10, \quad u_{\max} = \max(u_i). \tag{6}$$

As an example of the throughput of LTE network where the moving average of measurement n_i is 5.2 Mbps, the lower limit l_i is 0 Mbps, and the maximum value in the measurement history $u_{\max}$ is 24 Mbps; then the weight $S_{i_{\text{LTE}}}$ is calculated as

$$S_{i_{\text{LTE}}} = \left\lceil \frac{5.2 - 0}{24 - 0} \right\rceil \times 10 \approx 0.45. \tag{7}$$

Table 3 is shown as an example of a pairwise comparison matrix for video communication and Table 4 shows its priority alternatives.

Therefore, the overall result is shown in Table 5 by calculating the sum of the products of the priority of each alternative of Table 4 on the priority of the evaluation criteria in Table 2.

Table 3: Pairwise comparison matrix example of alternative.

	Satellite	LTE	3G
PER			
Satellite	1	1/2	1/2
LTE	2	1	1
3G	2	1	1
RTT			
Satellite	1	1/5	1/3
LTE	5	1	2
3G	3	1/2	1
Throughput			
Satellite	1	1/6	1/2
LTE	6	1	3
3G	2	1/3	1

Table 4: Priority of alternative.

	PER	RTT	Throughput
Satellite	0.2	0.1096	0.1137
LTE	0.4	0.5813	0.6647
3G	0.4	0.3091	0.2216
Propose			
Goal 1 (video)	0.2346	0.0819	0.4480

Table 5: Overall result.

Goal 1 (video)	PER	RTT	Throughput	Combined value
Satellite	0.0618	0.0121	0.0661	0.1399
LTE	0.1237	0.0637	0.3864	**0.5737**
3G	0.1237	0.0339	0.1288	0.2863

Finally, if the purpose is video communication, the priority is set to LTE > 3G > satellite. Therefore, LTE is determined as the optimal wireless link. Thus, it is possible to continue to select an optimal access network by periodically calculating a moving average value of the network status.

4.4. Route Selection. This system introduces "Extended AODV [16] which adopted extended AHP in AODV (Ad Hoc On-Demand Distance Vector) which is one of the conventional ad hoc network routing protocols." By Extended AODV, this system supports a change of neighboring communication environment reactively and realizes the construction of the network where QoS control is possible. The routing in Extended AODV is implemented based on the following algorithm. Specifically, an agent investigates all "the AHP calculation result between nodes existing between candidate routes" and finally really uses the highest route of the bottleneck score between the routes.

In the conventional AODV protocol [17], a route of the number of the smallest hops is chosen, but this may not be necessarily the most suitable root. In Extended AODV, each node adds the calculation result of the priority of each wireless link by the extended AHP to RREQ and RREP and finally makes the most suitable route choice by the min-max

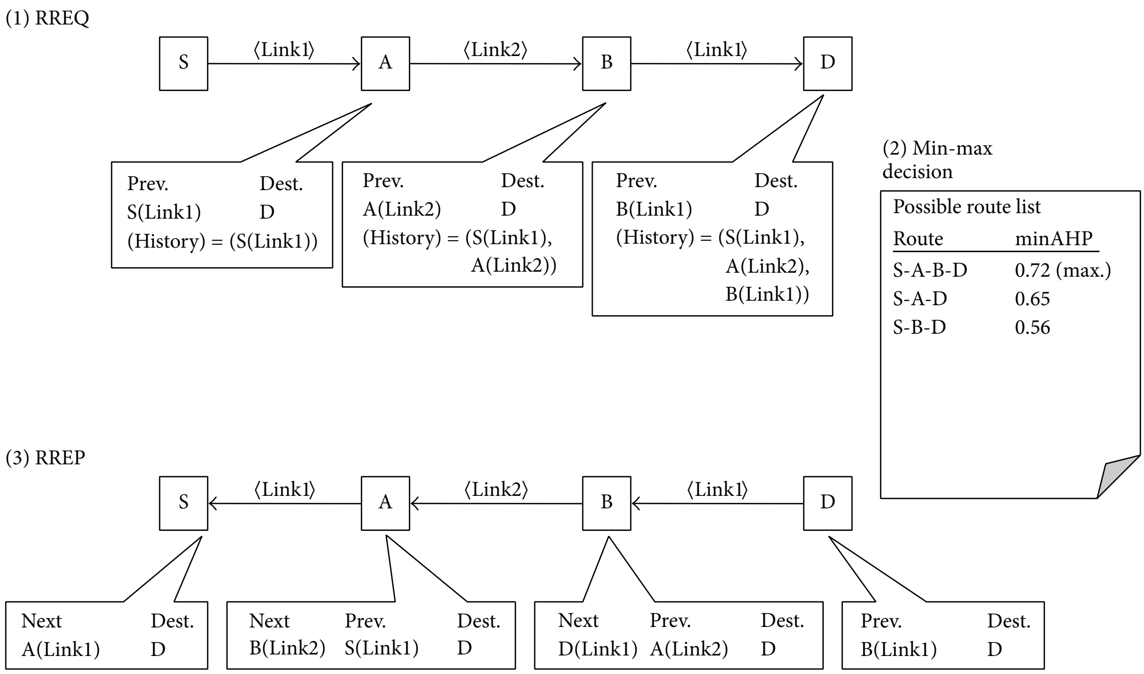


Figure 5: Message flow of Extended AODV.

method. The destination node finally sends out RREP packet from the reception side towards an origin of transmission and notifies you of the route decision.

The message flow of Extended AODV is shown in Figure 5. When data are sent to address node D by transmission former node S, at first it is delivered a broadcast to the RREQ packet like the normal AODV method by node S. Adjacent broadcast node A adds a postscript to adjacent node ID in front, the used most suitable wireless link ID, the value of the priority by the extended AHP in a route history of RREQ.

Then, in broadcast node A, broadcloth casts an adjacent node as RREQ packet equally, and similar processing is carried out in adjacent node B. Processing is repeated until RREQ packet finally arrives at objective transmission node D. When RREQ packet reaches transmission node, the transmission node waits for the arrival of the RREQ packet at constant time and destination node making the list of the candidate routes with route information and the priority information by the AHP chooses the most suitable route using the following min-max method from a candidate route list.

(1) Destination node compares the AHP information in each candidate route.
(2) The smallest AHP level is extracted by every candidate route.
(3) The minimum every candidate route is compared, and a route that has the maximum in the inside is chosen as the most suitable route.

And, along a route chosen by this min-max method, node D replies to the transmission in RREP packet. The broadcast node replies while referring to an adjacent transmission node made at the time of the RREQ packet transmission, and each broadcast node in this way knows the adjacent transmission, the reception node in this occasion.

5. Packet Control by OpenFlow

In this system, in order to flow the packets to the selected access network, OpenFlow as one of the SDN frameworks is used. In OpenFlow, OpenFlowController receives various messages from OpenFlowSwitches and executes the events corresponding to the message by event driven method [18]. In our system, the following events are used.

(i) *Switch_Ready*. This event is called when the link between OpenFlowController and OpenFlowSwitch has been established.
(ii) *Feature_Reply*. This event is called when the OpenFlowController received a reply from OpenFlowSwitch corresponding to the *Feature_Request* message.
(iii) *Access_Change*. This event is called when the current access network is needed to be changed due to network states change. Using the control channel, the *FlowMod* command in OpenFlow protocol is issued to the related OpenFlowSwitches.

By combining those events, the flows of the data packets can be controlled. The message flows between OpenFlowSwitch and OpenFlowController are shown in Figure 6.

First, OpenFlowSwitch issues *Switch_Ready* message to OpenFlowController to inform that the OpenFlowSwitch joins to the access network. Then, the OpenFlowController detects this new join from the OpenFlowSwitch and sends

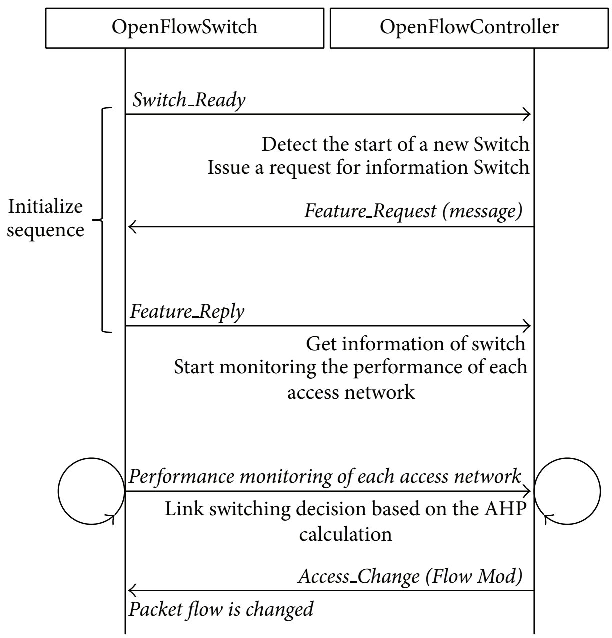


Figure 6: OpenFlow message flow.

the request message to reply to the message with the OpenFlowSwitch itself, such as the switch ID, the number of admissible access networks, and the MAC addresses of equipped NICs. The OpenFlowSwitch completes the initialization process by notifying this information to OpenFlowController. The initialized OpenFlowSwitches start monitoring network states and those monitored data are sent to the OpenFlowController. This process is repeated for all of the related OpenFlowSwitches.

The OpenFlowController can decide whether or not to change the current access network to the selected access network by issuing the *Flow_Mod* message to the corresponding OpenFlowSwitch.

6. System Architecture

The proposed system consisted of an OpenFlowController and multiple OpenFlowSwitches as shown in Figure 7. Furthermore, the OpenFlowSwitch consisted of three components including message exchange layer, monitoring layer, and flow table [19, 20].

The message exchange layer performs exchanging the monitored data and the control messages to the OpenFlowController. OpenFlow message is executed on software on OpenFlowSwitch. The monitoring layer monitors the network state of own OpenFlowSwitch.

The flow table is located in a stack of OpenFlowSwitch. The flow of the packet is defined by a command from OpenFlowController. The OpenFlowController consisted of two components including message exchanging layer and decision-making layer. The message exchanging layer performs exchanging control messages and receiving monitoring data from the OpenFlowSwitch. Exchanging OpenFlow message is executed on a framework on OpenFlowController.

In the decision-making layer, the priority process of the access network is carried out using the extended AHP method. The determined result is notified to all of the related OpenFlowSwitches. By this operation, the flow table of each OpenFlowSwitch is updated.

7. Prototype System

7.1. Device Construction. We describe the two main devices of the present prototype system including OpenFlowController and OpenFlowSwitch. OpenFlowController is implemented by Trema [21] which runs on Linux OS based PC. OpenFlowSwitch is implemented by OpenVSwitch [22] which runs on the Linux based PC. In addition, OpenFlowSwitch is connected to various wireless access networks through the NIC/USB connectors [23].

7.2. System Construction. We describe a prototype system to evaluate the proposed method. This prototype system is constructed for the purpose of demonstration and evaluation of dynamic access network switching function to ensure the communication between physically distant locations in an emergency. Therefore, we build a prototype system at three locations including inland site, northern coastal site, and southern coast site of Iwate prefecture which were seriously damaged by the Great East Japan Earthquake on March 11, 2011, as shown in Figure 8.

In each site, we set the OpenFlowSwitch equipped with a variety of wireless access devices for prototype system. Wireless access networks to be used in the present prototype system are as follows:

(i) satellite;

(ii) 3G/LTE;

(iii) WiMAX;

(iv) FTTH.

It is necessary to prepare the OpenFlow channel to control each OpenFlowSwitch using OpenFlow protocol. Therefore, the OpenFlowSwitch performs network configuration function to allow TCP connection to OpenFlowController which is disposed on the main site in advance. Furthermore, in order to always open OpenFlow channel, we use the satellite communication network channel for control link. Each OpenFlowSwitch provides a LAN port to control all of the packets by the OpenFlow.

8. Performance Evaluation

In order to verify usefulness and effects of our proposed system, the performance evaluation of switching link network connectivity was evaluated in the experimental environment as shown in Figures 9 and 10. In the actual disaster situations, physical connection problems occur such as the physical destruction of network equipment, lack of power, and breaking of the cable. Therefore, before making a decision based on the network performance, it is necessary to recognize the

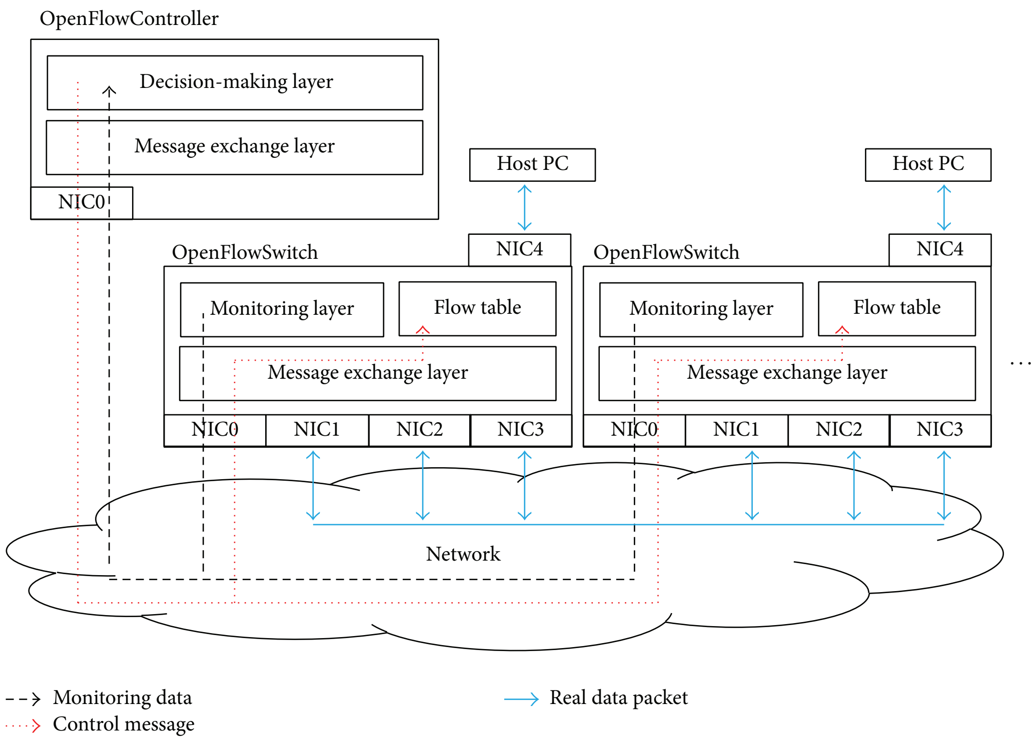


Figure 7: System architecture.

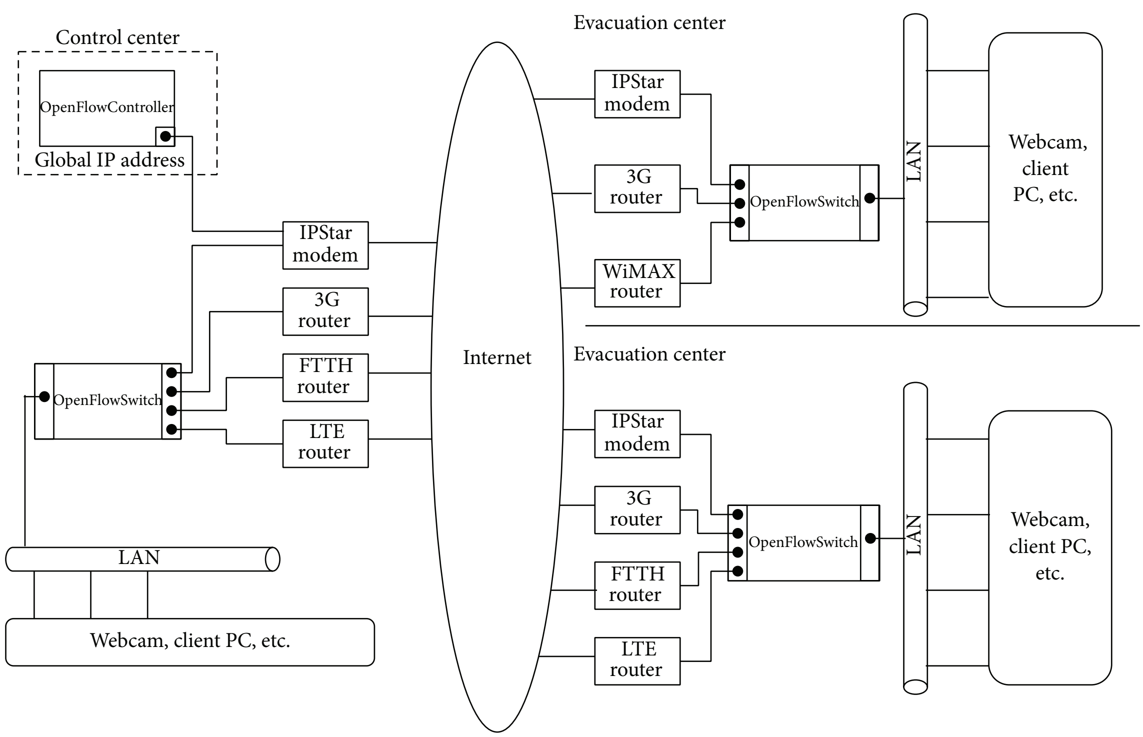


Figure 8: Prototype system.

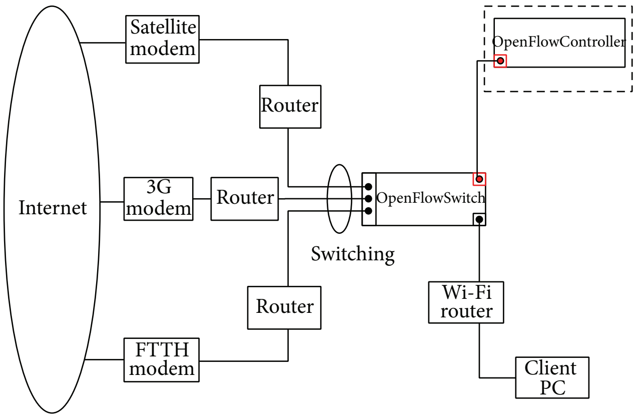


Figure 9: Performance evaluation environment.

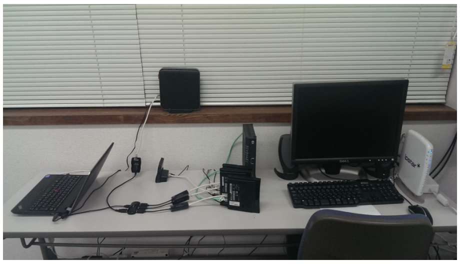


Figure 10: Performance evaluation devices.

availability of each link. In this prototype system, the availability of each link is recognized by monitoring the link state of each NIC. Link state of each NIC is determined by *status* member belonging to the *message* object which is retrieved by *Feature_Reply* event of OpenFlow. If the value of the status member is 0, the link of NIC is available. On the other hand, if value of the status member is 1, the link of the NIC is not available. In that case, the system switches to another available link of NIC immediately.

First we measured the time required to switch from one wireless access network link to another link of the prototype system and then measured the changes of the end-to-end throughput and packet loss performance. For the first case, we measured the switching performance when switching packet flow by OpenFlow protocol. In order to measure the exact switching performance, the delay of OpenFlow channel has to be close to zero. Therefore, OpenFlowController is directly connected to the OpenFlowSwitch by Ethernet. Since OpenFlowSwitch is operated by the very simple mechanism, it cannot obtain the event of rewriting completion of the flow timing and the flow-mod timing. For this reason, the switching performance measurement program is needed to be implemented on the OpenFlowController.

As the measurement procedure of switching time, first, OpenFlowController starts the timer at the transmission timing of "Flow Mod message." At the same time, OpenFlowController sends a "Barrier Request message." Then, OpenFlowController stops the timer upon receiving the "Barrier Reply message" from OpenFlowSwitch. Thus, it is possible to measure the switching time. We implemented the switching

Table 6: Switching process time.

	Maximum	Minimum	Average
Switching time	196 ms	67 ms	80 ms

time measurement program, ran 100 times switching every 10 seconds in the evaluation, and measured the maximum/minimum/average switching time at that time. The results are shown in Table 6.

The average switching time 80 ms is short enough to switch the link among possible access networks without significant packet loss. However, the maximum value was significantly out of normal distribution because the window manager is running on OpenFlowSwitch in order to perform a visual demonstration. That is, a processing time is increased by the control of the process such as interrupts at the OS level. It is considered that, in order for the operations to be more stable, it is necessary to introduce a dedicated OpenFlowSwitch machine not PC based or reduce the background process as much as possible.

Next we evaluated the end-to-end throughput and packet loss as network performance based on the disaster occurrence scenario. The scenario is as follows. Initially all three access networks including satellite network with average 1.29 Mbps throughput, 3G/LTE network with average 7.20 Mbps, and FTTH with average 25.01 Mbps are alive and the FTTH link is selected. Then a disaster occurred after 20 sec and both the FTTH and 3G/LTE network stopped due to power supply failure. Then link of the FTTH network is automatically switched to the satellite network. After 40 sec elapses, 3G/LTE network is recovered and the network link is automatically switched from satellite to 3G/LTE network. Finally, 60 sec elapses, the FTTH is recovered, and the network link is automatically switched from 3G/LTE to the FTTH. We measured the end-to-end network throughput and packet loss using *Iperf*.

The result of end-to-end throughput and packet loss is shown in Figure 11. After 20 sec from the starting time, the end-to-end throughput suddenly decreased from average 25 Mbps throughput to average 1.29 Mbps by satellite link. After 40 sec, the network link was switched to 3G/LTE network with average 7.1 Mbps. Finally, the 3G/LTE link was switched to the FTTH link with the original 25 Mbps. The packet loss at the switching times of 20 sec, 40 sec, and 60 sec was only under 5%. Thus, even though the disaster occurred and all of the networks were failed, the satellite network could be always alive and maintained the communication link to the Internet and realized resilient disaster network.

9. Conclusion and Future Work

In this study, we have implemented a cognitive radio system using the SDN technology. Cognitive wireless device is equipped with LTE and WiMAX, 3G mobile telephone network, and a satellite communication network. We have created a prototype system by placing the three based in cognitive radio devices. Furthermore, we constructed a testbed environment to evaluate the performance and functionality

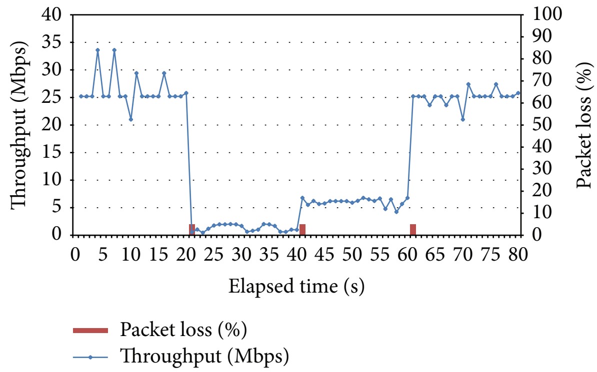


FIGURE 11: Result end-to-end throughput and packet loss.

of the system. Eventually we could verify the usefulness and effects of our proposed system.

In the future, we will implement immediately the expansion of AHP module which is the proposed method and network performance monitoring module. Then, by improving from manual to automatic switching process and evaluating the proposed method, we always activate a prototype system in three locations. By using continuous improvement, we will build a practicable system.

Disclosure

This paper is an extended version of the work originally presented at the 7th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS2013), Taichung, Taiwan, July 3–5, 2013.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] Y. Shibata, D. Nakamura, N. Uchida, and K. Takahata, "Residents oriented disaster information network," in *Proceedings of the Symposium on Applications and the Internet Workshops (SAINT '03)*, pp. 317–322, January 2003.

[2] D. Sakamoto, K. Hashimoto, K. Takahata et al., "Performance evaluation of evacuation information network system based on wireless wide area network," in *Proceedings of the DPS*, pp. 100–112, November 2000, (Japanese).

[3] K. Ito, K. Tsuda, N. Uchida, and Y. Shibata, "Wireless networked omni-directional video distribution system based on delay tolerant network," in *Proceedings of the 7th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS '13)*, July 2013.

[4] J. Mitola III and G. Q. Maguire Jr., "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[5] N. Uchida, K. Takahata, X. Zhang, and Y. Shibata, "Min-max based AHP method for route selection in cognitive wireless network," in *Proceedings of the 13th International Conference on Network-Based Information Systems (NBiS '10)*, pp. 22–27, September 2010.

[6] Open Networking Foundation, SDN, https://www.opennetworking.org/.

[7] D. Nakamura, N. Uchida, H. Asahi, K. Takahata, K. Hashimoto, and Y. Shibata, "Wide area disaster information network and its resource management system," in *Proceedings of the 17th International Conference on Advanced Information Networking and Applications (AINA '03)*, pp. 146–149, March 2003.

[8] OpenFlow, https://www.opennetworking.org/sdn-resources/openflow.

[9] A. A. Ali, F. Michaut, and L. Francis, "End-to-end available bandwidth measurement tools: a comparative evaluation of performances," in *Proceedings of the IPS-MoMe IEEE/ACM International Workshop on Internet Performance, Simulation, Monitoring and Measurement*, Salzburg, Austria, February 2006.

[10] A. Gerber, J. Pang, O. Spatscheck, and S. Venkataraman, "Speed testing without speed tests: estimating achievable download speed from passive measurements," in *Proceedings of the 10th Internet Measurement Conference (IMC '10)*, pp. 424–430, November 2010.

[11] V. J. Ribeiro, R. H. Riedi, and R. G. Baraniuk, "pathChirp: efficient available Bandwidth estimation for network paths," in *Proceedings of the Passive and Active Monitoring Workshop (PAM '03)*, San Diego, Calif, USA, July-August 2003.

[12] T. Oshiba and K. Nakajima, "Quick end-to-end available bandwidth estimation for QoS of real-time multimedia communication," in *Proceedings of the IEEE Symposium on Computers and Communications (ISCC '10)*, pp. 162–167, Riccione, Italy, June 2010.

[13] A. Awajan, K. Al-Begain, and P. Thomas, "Quality of service routing for real-time applications using the analytical hierarchy process," in *Proceedings of the 10th International Conference on Computer Modeling and Simulation (UKSIM '08)*, pp. 70–75, Cambridge, UK, 2008.

[14] T. Ahmed, K. Kyamakya, and M. Ludwig, "Design and implementation of a context-aware decision algorithm for heterogeneous networks," in *Proceedings of the ACM Symposium on Applied Computing (SAC '06)*, pp. 1134–1138, Dijon, France, April 2006.

[15] T. L. Saaty, "How to make a decision: the analytic hierarchy process," *European Journal of Operational Research*, vol. 48, no. 1, pp. 9–26, 1990.

[16] N. Uchida, G. Sato, Y. Shibata et al., "Selective routing protocol for cognitive wireless networks based on user's policy," in *Proceedings of the 12th International Workshop on Multimedia Network Systems and Applications (MNSA '10)*, pp. 112–117, June 2010.

[17] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) routing," Tech. Rep. RFC3561, IETF, 2003.

[18] S. Kinoshita, T. Watanabe, J. Yamato, H. Goto, and H. Sone, "Implementation and evaluation of an OpenFlow-based access control system for wireless LAN roaming," in *Proceedings of the 36th Annual IEEE International Computer Software and Applications Conference Workshops*, pp. 82–87, July 2012.

[19] K. Hashimoto and Y. Shibata, "Design of a middleware system for flexible intercommunication environment," in *Proceedings of the 17th International Conference on Advanced Information Networking and Applications (AINA '03)*, pp. 59–64, March 2003.

[20] C. W. Pyo and M. Hasegawa, "Minimum weight routing based on a common link control radio for cognitive wireless ad hoc networks," in *Proceedings of the International Conference on Wireless Communications and Mobile Computing (IWCM C '07)*, pp. 399–404, Honolulu, Hawaii, USA, 2007.

[21] http://www.trema.info/.

[22] OpenVSwitch, http://openvswitch.org/.

[23] "USB 3.0 Gigabit LAN Adapter," UE-1000T-G3, PLANEX, http://www.planex.net/product/adapter/ue-1000t-g3.htm.

Hindawi Publishing Corporation
Mobile Information Systems
Volume 2015, Article ID 963628, 9 pages
http://dx.doi.org/10.1155/2015/963628

Research Article

Lattice Based Mix Network for Location Privacy in Mobile System

Kunwar Singh,[1] C. Pandu Rangan,[2] and A. K. Banerjee[3]

[1]*Computer Science and Engineering Department, NIT Trichy, Tiruchirappalli 620015, India*
[2]*Computer Science and Engineering Department, IIT Madras, Chennai 600036, India*
[3]*Mathematics Department, NIT Trichy, Tiruchirappalli 620015, India*

Correspondence should be addressed to Kunwar Singh; kunwar@nitt.edu

Received 1 September 2014; Accepted 1 September 2014

Academic Editor: Ilsun You

In 1981, David Chaum proposed a cryptographic primitive for privacy called *mix network* (Mixnet). A mixnet is cryptographic construction that establishes anonymous communication channel through a set of servers. In 2004, Golle et al. proposed a new cryptographic primitive called universal reencryption which takes the input as encrypted messages under the public key of the recipients not the public key of the universal mixnet. In Eurocrypt 2010, Gentry, Halevi, and Vaikunthanathan presented a cryptosystem which is an additive homomorphic and a multiplicative homomorphic for only one multiplication. In MIST 2013, Singh et al. presented a lattice based universal reencryption scheme under learning with error (LWE) assumption. In this paper, we have improved Singh et al.'s scheme using Fairbrother's idea. LWE is a lattice hard problem for which till now there is no polynomial time quantum algorithm. Wiangsripanawan et al. proposed a protocol for location privacy in mobile system using universal reencryption whose security is reducible to Decision Diffie-Hellman assumption. Once quantum computer becomes a reality, universal reencryption can be broken in polynomial time by Shor's algorithm. In postquantum cryptography, our scheme can replace universal reencryption scheme used in Wiangsripanawan et al. scheme for location privacy in mobile system.

1. Introduction

In 1981, Chaum [1] proposed a cryptographic primitive for privacy called *mix network* (Mixnet). A mixnet is cryptographic construction that establishes anonymous communication channel through a set of servers. One type of mixnets accepts encrypted messages under the public keys of all intermediate mixnet nodes and outputs randomly permuted corresponding plaintexts. Sender encrypts the message using public keys of the mixnet nodes in some order. Ciphertext is concatenation of n-encryptions which can be seen as building up of a n layered onion. Mixnet receives these ciphertexts from many senders. Mixnet nodes decrypt the ciphertexts using its private keys (remove outer layer of the onion) in reverse order of the encryption and permute them before forwarding to the next mixnet node. Finally, the nth mixnet node sends the messages to the respective receivers. In this way, adversary like eavesdropper (external) and mail server (internal) will find it hard to guess who is communicating. Mixnet preserves anonymous communication even with one honest mixnet node. A drawback of decryption type of mixnet is that if one server fails then mixnet fails.

Choonsik et al. [2] proposed a reencryption mixnet which is robust. A reencryption mixnet accepts the encrypted massages under the public key of the mixnet. Mixnet node reencrypts the encrypted message and broadcasts this reencrypted to other mixnet nodes. There is no order of reencryption. Any mixnet node can reencrypt first and broadcast reencrypted to other nodes. Also it is not required that reencryption has to be done by all the mixnet nodes. The private key corresponding to the public key of the mixnet is distributed among all reencryption mixnet nodes [3]. Set of ciphertexts produced by last reencryption mixnet node is decrypted by group of t nodes using a (t, n) threshold scheme [3]. For privacy, it is required that adversary cannot distinguish between the reencrypted ciphertext and a random ciphertext with size being the same as the size of the reencrypted ciphertext.

Both the mixnets discussed above accept encrypted messages under the public key of the mixnet. In 2004, Golle et al. [4] proposed a new cryptographic primitive called universal reencryption which takes the input as encrypted messages under the public key of the recipients not the public key of the universal mixnet. So it dispenses with the complexities of the key generation, key distribution, and key maintenance of the public key of mixnet. A mixnet based on universal reencryption is called universal mixnet. Universal mixnet takes the input as encrypted messages under the public key of the recipients. These encrypted messages are universally reencrypted and permuted by each universal mixnet node before forwarding them to the next node. Finally the output from a universal mixnet is set of universal reencrypted ciphertexts. Potential recipient must perform to decrypt all the ciphertexts to identify messages sent for them. This is a disadvantage of the universal reencryption.

Lattice based cryptography has bloomed in recent years because of the following advantages.

(i) Once quantum computer comes into reality, all the cryptosystem based on prime factorization and discrete logarithm problem can be solved in polynomial time by Shor's algorithm [5]. But till now there is no polynomial time quantum algorithm for lattice hard problems.

(ii) Security of the cryptosystem depends on the hardness of the problem in the average case. Ajtai in his seminal result [6] has shown that lattice based cryptosystems are secure on the assumption of lattice based hard problems in the worst case. It gives strong hardness guarantee.

(iii) Lattice based cryptosystems are efficient and parallelizable.

(iv) Powerful primitives like fully homomorphic encryption [7] and multilinear maps [8] are realized using lattices.

A drawback of lattice based cryptosystem is that it has large key size and ciphertext size. Recently Regev [9] defined the learning with error (LWE) problem and proved that it also enjoys similar average case/worst case equivalence hardness properties under a quantum reduction.

Location privacy is the ability to prevent adversaries from knowing one's current or past location [10]. Advances in mobile networks have made location information a useful information in many applications. However location information can be used to know about person's medical condition, alternating lifestyle, and so forth. This information can be used for blackmail by malicious user. Wiangsripanawan et al. [11] proposed a protocol for location privacy in mobile system using universal reencryption [4] whose security is reducible to Decision Diffie-Hellman assumption. Once quantum computer becomes a reality, universal reencryption can be broken in polynomial time by Shor's algorithm [5].

Our Contributions. Universal reencryption has simple idea. In an additive homomorphic cryptosystem, a new ciphertext (encryption of zero) can be appended to the ciphertext. The new ciphertext can be used to reencrypt (change the encryption factor) the ciphertext such that the reencrypted ciphertext and the ciphertext decrypt to the same plaintext because, in an additive homomorphic, $E(M+0) = E(M) + E(0)$.

In Eurocrypt 2010 Gentry, Gentry et al. [12] presented a cryptosystem which is an additive homomorphic and a multiplicative homomorphic for only one multiplication. In MIST 2013, Singh et al. [13] presented lattice based universal reencryption scheme using learning with error (LWE) problem based on [12]. In this paper, we have improved Singh et al.'s scheme [13] in terms of ciphertext size and computational cost using Fairbrother's idea [14]. The idea is simple: ciphertext in scheme [13] has two parts and second part of the ciphertext is encryption of zero. Larger files can be split into many segments and the second part of the ciphertext (encryption of zero) can be made the same for all the segments. By this way, size of the ciphertext is reduced by approximately half and it also reduces the computational cost.

In post quantum cryptography, our scheme can replace universal reencryption scheme used in Wiangsripanawan et al. [11] protocol for location privacy in mobile system.

Paper Outline. Rest of the paper is organized as follows. In Section 2, we give some preliminaries including security models and hard problems. In Section 3, we describe different types of mixnet. We describe GHV public key cryptosystem [12] in Section 4. In Section 5, we review Singh et al.'s scheme [13]. In Section 6, we give our improved construction and in Section 7 we give conclusion and related open problems.

2. Preliminaries

2.1. Notation. We denote $[j] = \{0, 1, \ldots, j\}$, set of real numbers by R and the set of integers by Z. We assume vectors to be in column form which are written using small letters, for example, x. Matrices are written as capital letters, for example, X. We denote $R \leftarrow \psi_\beta(q)_q^{m\times m}$ as matrix R whose elements are chosen from the Gaussian distribution ψ_β over Z_q and $S \leftarrow Z_q^{n\times m}$ as matrix S whose elements are chosen uniformly over Z_q. $\|S\|$ denotes the Euclidean norm of the longest (maximum Euclidean norm) vector in matrix S; that is, $\|S\| := \max_i \|s_i\|$ for $1 \le i \le k$.

We say that $\mathrm{negl}(n)$ is a negligible function in n if it is smaller than the inverse of any polynomial function in n for sufficiently large n.

2.2. Universal Reencryption Scheme (URe). Universal Reencryption Scheme consists of four algorithms [4]. We denote M, C, and R as message space, ciphertext space, and set of encryption factors, respectively.

Universal KeyGen(n). On the input of a security parameter n, this algorithm outputs the public key pk and secret key sk pair.

Universal Encryption(pk, m, r). On the input of public key pk, a message $m \in M$, and an encryption factor $r \in R$, this algorithm outputs a ciphertext $C \in \mathbf{C}$.

Universal Decryption(C, sk). On the input of a secret key sk and a ciphertext C, this algorithm outputs message m.

Universal Reencryption(C, r). On the input of a ciphertext C and reencryption factor $r \in R$, but no public key, this algorithm outputs ciphertext C' where $C' \in \mathbf{C}$.

2.3. Universal Semantic Security Model for Universal Reencryption Scheme (IND-URe-CPA). Universal security model is variant of semantic security model and is adapted from [4]. In this model, adversary is allowed to construct universal ciphertexts under randomly generated public key pk. The challenger reencrypts the ciphertext. The goal of the adversary is to distinguish between the reencrypted ciphertext and the random ciphertext with the size of the random ciphertext being the same as size of the universally reencrypted ciphertext. Here, security model is defined using the following game played between the challenger and an active adversary.

KeyGen. The challenger runs the key generation algorithm and gives public parameters to the adversary.

Challenger. The adversary submits messages $m \in M$ and $r \in R$ (adversary can construct ciphertext). Challenger sets $C \leftarrow$ Universal Encryption(m, r, pk) and chooses a random bit $b \in \{0, 1\}$ and a random ciphertext C with the size of the random ciphertext being the same as size of the universally reencrypted ciphertext. If $b = 0$, it assigns the challenge ciphertext to $C^* =$ Universal Reencryption(C, r'). If $b = 1$, it assigns the challenge ciphertext to $C^* = C$. Challenger sends challenge ciphertext C^* to the adversary.

Guess. The adversary outputs a guess $b' \in \{0, 1\}$ and wins the game if $b' = b$.

An IND-URe-CPA adversary is referred to as an adversary $\mathscr{A}$. We define the advantage of the adversary $\mathscr{A}$ in attacking universal reencryption scheme ξ as $\mathrm{Adv}_{\xi,A}(n) = |\Pr[b = b'] - 1/2|$.

Definition 1. One says that universal reencryption scheme ξ is universal semantic secure if for all probabilistic polynomial time adversaries A, one has $\mathrm{Adv}_{\xi,A}(n)$ which is a negligible function.

2.3.1. Semantically Secure Elgamal Cryptosystem [15]. Semantically secure Elgamal cryptosystem consists of three algorithms.

Setup. Two primes p and q are randomly selected such that $p = 2q + 1$. Pick a random generator $h \in Z_p$ and set $g = h^2 (\mathrm{mod}\, p)$. g is generator of subgroup G (Schnorr group) of size q. Message m is also element of subgroup G. Since $g \in QR_p$ so $m \in QR_p$ (Quadratic residue modulo p). Pick a random number $x \in Z_{p-1}$ as private key and public key $y = g^x (\mathrm{mod}\, p)$.

Encryption. To encrypt a message $m \in G$, sender picks a random number $r \in Z_{p-1}$ and computes a ciphertext pair as follows:

$c_1 = g^r \bmod p$ and $c_2 = y^r m \,(\mathrm{mod}\, p)$. Output ciphertext $C = (c_1, c_2)$.

Decryption. To decrypt a ciphertext (c_1, c_2), receiver computes $m = c_2 / c_1^x (\mathrm{mod}\, p)$.

2.3.2. Homomorphic Encryption. A encryption scheme is multiplicative homomorphic encryption scheme if encryption of xy is equal to encryption of x into encryption of y; that is, $E(xy) = E(x)E(y)$.

A encryption scheme is additive homomorphic encryption scheme if $E(x + y) = E(x) + E(y)$.

It can be easily proved that Elgamal encryption scheme is multiplicative homomorphic encryption.

2.4. Integer Lattices [16, 17]. Let $B = \{b_1, \ldots, b_n\} \subset R^n$ consist of n linearly independent m-dimensional vectors as column vectors; the lattice generated by the matrix B is

$$\wedge = L(B) = \{Bx : x \in Z^n\}. \tag{1}$$

The column vectors of matrix $B = \{b_1, \ldots, b_n\}$ are called a basis for the lattice. n and m are called the rank and dimension of the lattice, respectively. When $n = m$, the lattice is called full-rank lattice but generally $n \le m$. The determinant of a lattice is the absolute value of the determinant of the basis matrix $\det(L(B)) = |\det(B)|$.

q-Ary Lattices. Generally cryptographic constructions based on lattices use q-ary lattices. Lattice L which satisfies the condition $qZ^n \subseteq L \subseteq Z^n$ for some prime q is called q-ary lattices. In other words, any vector $x \in L'$ if and only if $x \bmod q \in L'$, where L' is a q-ary lattices.

For prime q, $A \in Z_q^{n\times m}$, and $u \in Z_q^n$, three m-dimensional q-ary lattices are defined as follows:

$$\Lambda_q(A) := \{e \in Z^m \text{ s.t. } \exists s \in Z_q^n \text{ where } A^T s = e \,(\mathrm{mod}\, q)\}$$
$$\Lambda_q^{\perp}(A) := \{e \in Z^m \text{ s.t. } Ae = 0 \,(\mathrm{mod}\, q)\}$$
$$\Lambda_q^{u}(A) := \{e \in Z^m \text{ s.t. } Ae = u \,(\mathrm{mod}\, q)\}. \tag{2}$$

Since first q-ary lattices are generated by rows of matrix A and second is set of vectors orthogonal to rows of matrix A so these two q-ary lattices are dual to each other:

$$\Lambda_q^{\perp}(A) = q \cdot \Lambda_q(A)^*, \qquad \Lambda_q(A) = q \cdot \Lambda_q^{\perp}(A)^*. \tag{3}$$

2.5. Gram Schmidt Orthogonalization. $\widetilde{S} := \{\widetilde{s_1}, \ldots, \widetilde{s_k}\} \subset R^m$ denotes the Gram-Schmidt orthogonalization of the set of linearly independent vectors $S = \{s_1, \ldots, s_k\} \subset R^m$, which is defined as follows:

$$\widetilde{s_i} = s_i - \sum_{j=1}^{i-1} \mu_{i,j} \widetilde{s_j} \quad \text{where } \mu_{i,j} = \frac{\langle s_i, \widetilde{s_i} \rangle}{\langle \widetilde{s_j}, \widetilde{s_j} \rangle}. \tag{4}$$

In other words, $\widetilde{s_1} = s_1$ and $\widetilde{s_i}$ is the component of s_i orthogonal to $\mathrm{span}(s_1, \ldots, s_i)$ where $2 \le i \le k$. Since $\widetilde{s_i}$ is the component of s_i so $\|\widetilde{s_i}\| \le \|s_i\|$ for all i.

We refer to $\|\widetilde{S}\|$ as the Gram-Schmidt norm of S.

2.6. Discrete Gaussians. Let L be a subset of Z^m. For any vector $c \in R^m$ and any positive parameter $\sigma \in R > 0$, define:

$\rho_{\sigma,c}(x) = \exp(-\pi(\|x - c\|/\sigma^2))$: a Gaussian-shaped function on R^m with center c and parameter σ,

$\rho_{\sigma,c}(L) = \sum_{x \in L} \rho_{\sigma,c}(x)$: over L,

$D_{L,\sigma,c}$: the discrete Gaussian distribution over L with parameters σ and c,

$$\forall y \in L, \quad D_{L,\sigma,c}(y) = \frac{\rho_{\sigma,c}(y)}{\rho_{\sigma,c}(L)}. \tag{5}$$

Theorem 2 (see [6, 18]). *Let $q \ge 3$ be odd and $m := \lceil 6n \log q \rceil$. There is PPT algorithm TrapGen(q,n) that generates a pair ($A \in Z_q^{n \times m}, T \in Z^{n \times m}$) such that T is a basis for $\Lambda_q^{\perp}(A)$ and A is statistically close to a uniform matrix in $Z_q^{n \times m}$ satisfying*

$$\|\widetilde{T}\| \le O\left(\sqrt{n \log q}\right), \quad \|T\| \le O(n \log q) \tag{6}$$

with overwhelming probability in n.

2.7. Decision Diffie-Hellman Problem. Let us consider a finite cyclic group Z_p with generator g, where p is a prime number. g^a, g^b, and g^c are given for some random $a, b, c \in Z_p$. The goal of the adversary is to decide whether $c = ab$ or not.

2.8. The LWE Hardness Assumption [9, 19]. In 2004, Regev [9] proposed the LWE hard problem.

Definition 3. For a security parameter n, let $m = \mathrm{poly}(n)$, modulus $q = \mathrm{poly}(n)$, and a Gaussian distribution χ^m over Z_q^m. For a uniformly chosen vector $s \in Z_q^n$, let $A_{s,\chi}$ be the distribution on $Z_q^n \times Z_q$ of the variable $(a, \langle a, s \rangle + e)$ where a vector $a \in Z_q^n$ is chosen uniformly at random and $e \in Z_q$ is chosen according to χ.

Search LWE. The search $\mathrm{LWE}_{q,\chi}$ problem is to find $s \in Z_q^n$ with probability exponentially close to one, given m samples from $A_{s,\chi}$.

Decision LWE. Decision LWE is to distinguish with nonnegligible probability between the distribution $A_{s,\chi}$ for some uniform $s \in Z_q^n$ and a random distribution on $Z_q^n \times Z_q$.

In above, s is uniformly chosen from the random distribution. Even, if s is chosen from the Gaussian distribution still decision LWE is hard [20, 21].

Gaussian Distribution ψ_α. For $\alpha \in R^+$, the distribution ψ_α on $T = [0, 1)$ is obtained by sampling a Gaussian distribution with mean 0 and variance $\alpha^2/2\pi$ and reducing the result modulo 1. The probability density function is given by the following equation:

$$\psi_\alpha(x) = \sum_{k \in Z} \frac{1}{\alpha} \exp\left(-\pi\left(\frac{x-k}{\alpha}\right)^2\right). \tag{7}$$

In other words, distribution is obtained by "folding" a Gaussian distribution $N(0, \alpha^2/2\pi)$ on R into the interval $T = [0, 1)$ [22].

Discrete Gaussian Distribution $\overline{\psi}_\alpha$. This distribution is obtained by "folding" a Gaussian distribution ψ_α on $T = [0, 1)$ into the interval Z_q. It is a discrete distribution over Z_q of the random variable $\lfloor qX \rceil \bmod q$ where the random variable $X \in T$ has distribution ψ_α.

The following theorem shows that LWE problem is reducible to some lattice problems in the worst case using the quantum algorithm.

Theorem 4 (see [9]). *For security parameter n, Let $\alpha = \alpha(n) \in (0, 1)$ and $q = \mathrm{poly}(n)$ be a prime integer such that $\alpha \cdot q > 2\sqrt{n}$. If there exists an efficient, possibly quantum algorithm for deciding the $(Z_q, n, \overline{\psi}_\alpha)$-LWE problem for $q > 2\sqrt{n}/\alpha$, then there exists an efficient quantum algorithm for approximating the SIVP and GapSVP problems, to within $O(n/\alpha)$ factors in the l_2 norm, in the worst case.*

3. Mix Network

A mix network is a multistage system that offers anonymous communication. Here, we describe three types of mixnets: decryption mixnet, reencryption mixnet, and universal reencryption mixnet.

3.1. Decryption Mixnet [1, 23]. Each mixnet node has its own public key and private key. We denote public and private key of ith mixnet node by $(\mathrm{pk}_i, \mathrm{sk}_i)$.

Encryption. Sender first encrypts the message using public key of the nth mixnet node. First encryption is

$$C_n = E_{\mathrm{PK}_n}(m \parallel B) \parallel r_n, \tag{8}$$

where B is the address of the receiver and r is the random number concatenated with the encryption. Similarly, sender again encrypts C_n with the public key of $(n-1)$th mixnet node. Second encryption is

$$C_{n-1} = E_{\mathrm{PK}_{n-1}}(C_n) \parallel r_{n-1}. \tag{9}$$

Finally, sender sends the ciphertext C to the mixnet as

$$C = E_{\mathrm{PK}_1}\left(E_{\mathrm{PK}_2}\left(E_{\mathrm{PK}_3}, \ldots, \parallel r_3\right) \parallel r_2\right) \parallel r_1. \tag{10}$$

Above ciphertext is concatenation of n-encryptions which can be seen as building up of a n layered onion.

Decryption. First mixnet node receives ciphertext from many senders. It will decrypt all the ciphertexts using its private key (remove outer layer of the onion) and permute them before forwarding to the second mixnet node. Finally, the nth mixnet node sends the messages to the respective receivers.

Chaum's mixnet [1] preserves anonymous communication even with one honest mixnet node. But it has the following disadvantages.

(1) Mixnet is not robust because if one mixnet node fails, whole mixnet fails.

(2) Encryption cost is very high which grows with the number of mixnet nodes.

(3) Decryption has to be performed in reverse order of the encryption.

3.2. Reencryption Mixnet [2, 23]. All three weaknesses of the decryption mixnet are removed in reencryption mixnet. Reencryption mixnet node is based on Elgamal cryptosystem [24] and Shamir's secret sharing [3].

Secret key of the mixnet is d and public key is $K = g^d$. Secret key d is distributed among n mixnet nodes in such a way that, at least, t mixnet nodes are required to compute secret key d but no group of $t - 1$ nodes can compute secret key d.

Encryption. Sender encrypts the using public key K of the mixnet. Ciphertext is

$$C = E_K(m, r) = g^r \parallel (B \parallel m) k^r. \tag{11}$$

Sender sends the ciphertext C to the mixnet.

Reencryption. Mixnet node j reencrypts the encrypted message as follows:

$$\begin{aligned}\text{Reencryption} &= E_K(C, r_j) = g^{r_j}(g^r \parallel (B \parallel m) K^r K^{r_j}) \\ &= g^{r+r_j} \parallel (B \parallel m) K^{r+r_j},\end{aligned} \tag{12}$$

where r_j is random number. Mixnet node broadcasts this reencrypted to other mixnet nodes. There is no order of reencryption. Any mixnet node can reencrypt first and broadcast reencrypted to other nodes. It is also not required that reencryption has to be done by all the mixnet nodes.

Decryption. Now, in decryption phase, any t mixnet nodes can participate to compute secret key d:

$$\begin{aligned}&D_d(g^{r+r_1+r_2+\cdots+r_m} \parallel (B \parallel m) K^{r+r_1+r_2+\cdots+r_m}) \\ &\quad = \frac{(B \parallel m) K^{r+r_1+r_2+\cdots+r_m}}{(g^{r+r_1+r_2+\cdots+r_m})^d} = B \parallel m,\end{aligned} \tag{13}$$

where $m \le n$ and B is address of the receiver.

3.3. Universal Reencryption Mixnet [4]. In 2004, Golle et al. [4] presented a new primitive called universal reencryption based on the Elgamal public key cryptosystem [24]. Universal mixnet is a mixnet based on universal reencryption which takes the input as encrypted messages under the public key of the recipients not the public key of the universal mixnet. Even, there is no term like the public key of the universal mixnet. So it dispenses with cost of establishing public key infrastructure for mixnet nodes.

The idea for universal reencryption is simple. In an additive homomorphic cryptosystem, we append a second ciphertext (encryption of zero) to the ciphertext. Since, in an additive homomorphic, $E(M + 0) = E(M) + E(0)$, we can use the second ciphertext to reencrypt (change the encryption factor) the first ciphertext such that the reencrypted ciphertext and the ciphertext decrypt the same plaintext.

Key Generation. It is the same as key generation algorithm in Elgamal cryptosystem.

Universal Encryption. On the input of a message m, a public key y, and a random encryption factor $r = (k_0, k_1) \in Z_q^2$, ciphertext C is computed as follows:

$$C = [(c_0, c_1); (c_2, c_3)] = [(my^{k_0}, g^{k_0}); (y^{k_1}, g^{k_1})]. \tag{14}$$

Here ciphertext (c_2, c_3) is for message m.

Universal Decryption. Here, the decryption is done by the receiver. Compute $m_0 = c_0/c_1^x$ and $m_1 = c_2/c_3^x$. If $m_1 = 1$, then the output is $m = m_0$. Otherwise, decryption fails.

Universal Reencryption. On the input of a $C = [(c_0, c_1); (c_2, c_3)]$ and a random reencryption factor $r' = (k'_0, k'_1) \in Z_q^2$, reencrypted ciphertext C' is computed as follows:

$$C' = [(c'_0, c'_1); (c'_2, c'_3)] = [(c_0 c_2^{k'_0}, c_1 c_3^{k'_0}); (c_2^{k'_1}, c_3^{k'_1})]. \tag{15}$$

4. Gentry, Halevi, and Vaikunthanathan (GHV) Cryptosystem [12]

GHV cryptosystem [12] is an additive homomorphic and multiplicative homomorphic for only one multiplication. Here, message space $M \in Z_2^{m\times m}$ (the set of binary m-by-m matrices) and ciphertex space $C \in Z_q^{m\times m}$ (the set of m-by-m matrices). Here, we briefly describe the GHV homomorphic cryptosystem because our scheme is based on it.

KeyGen(n). On the input of a security parameter n, set the parameters $q = \text{poly}(n)$ and $m = O(n \log q)$ and a Gaussian distribution $\psi_\beta(q)_q^{m\times m}$ with Gaussian error parameter $\beta = 1/\text{poly}(n)$. Uniform matrix $A \in Z_q^{m\times n}$ together with the trapdoor $T \in Z^{m\times m}$ is obtained by running algorithm TrapGen of Theorem 2. The public key is A and the secret key is T.

Encrypt($A, M \in \{0, 1\}^{m\times m}$). To encrypt message $M \in \{0, 1\}^{m\times m}$, do the following steps.

(1) A random matrix $S \leftarrow Z_q^{n\times m}$ and an error matrix $X \leftarrow \psi_\beta(q)_q^{m\times m}$ are chosen uniformly.

(2) Output the ciphertext

$$C = AS + 2X + M \,(\text{mod } q)\,. \tag{16}$$

Decrypt(T, C). To decrypt C, do the following steps.

(1) Set $E = TCT^t \bmod q$.

(2) Output the matrix $B = T^{-1}E(T^t)^{-1} \bmod q$.

Correctness. Since $T \cdot A = 0$, therefore $E = TCT^t = T(2X + M)T^t \bmod q$. Now, if $T(2X+M)T^t \bmod q$ is equal to $T(2X + M)T^t$, then $T^{-1}ET \bmod q = M$. So for correct decryption, one has to set the parameter β small enough so that all the entries of $T(2X + M)T^t$ are smaller than $q/2$ with high probability.

Additive Homomorphic. Let $C_1 = AS_1 + 2X_1 + M_1$ and $C_2 = AS_2 + 2X_2 + M_2$ be ciphertexts for messages M_1 and M_2 under public key A. Then,

$$C = C_1 + C_2 = A(S_1 + S_2) + 2(X_1 + X_2) + M_1 + M_2 \tag{17}$$

would be decrypted to $M_1 + M_2$ as long as all the entries in $T(2(X_1 + X_2) + M_1 + M_2)T^t$ are smaller than $q/2$.

Multiplicative Homomorphic. The product of C_1 and C_2 is

$$\begin{aligned} C &= C_1 \cdot C_2^t \\ &= (AS_1 + 2X_1 + M_1) \cdot (AS_2 + 2X_2 + M_2)^t \\ &= A \cdot \left(S_1 C_2^t\right) + 2 \cdot \left(X_1 (2X_2 + M_2) + M_1 X_2^t\right) \\ &\quad + M_1 M_2^t + (2X_1 + M_1) S_2^t \cdot A^t. \end{aligned} \tag{18}$$

Product ciphertext C has the form $AS + 2X + M + S'A^t$. Ciphertext would be decrypted to $M_1 \cdot M_2^T$ as long as all the entries in $T(2X + M)T^t$ are smaller than $q/2$.

For our scheme, we will use variant of GHV cryptosystem which is only additive homomorphic. For this variant, decryption algorithm will not have right multiplication of T^t.

5. Lattice Based Universal Reencryption [13]

Singh et al.' scheme [13] is based on GHV cryptosystem which is explained in Section 4 (Table 1).

The idea for universal reencryption is to append a new ciphertext (encryption of zero) to the GHV cryptosystem ciphertext. The new ciphertext can be used to reencrypt (change the encryption factor) the ciphertext such that the reencrypted ciphertext and the ciphertext decrypt the same plaintext because the GHV public key cryptosystem is additive homomorphic; that is, $(E(M + 0) = E(M) + E(0))$.

Universal KeyGen(n). On the input of a security parameter n, we set the parameters $q = \text{poly}(n)$ and $m = O(n \log q)$ and a Gaussian distribution $\psi_\beta(q)_q^{m\times m}$ with Gaussian error parameter $\beta = 1/\text{poly}(n)$. Uniform matrix $A \in Z_q^{m\times n}$ together with the trapdoor $T \in Z^{m\times m}$ is obtained by running algorithm TrapGen of Theorem 2. The public key is A and the secret key is T.

Table 1: We compare our scheme with Singh et al.' scheme [13] for plaintext size of $k(m \times m)$ bits.

	Plaintext size	Ciphertext size
Singh et al.' scheme [13]	$k(m \times m)$ bits	$2k(m \times m)$ bits
Our scheme	$k(m \times m)$ bits	$(k + 1)(m \times m)$ bits

Universal Encryption(A, M). To encrypt message $M \in \{0, 1\}^{m\times m}$, we do the following steps.

(i) We choose random matrices $S_1, S_2 \leftarrow Z_q^{n\times m}$ and error matrices $X_1, X_2 \leftarrow \psi_\beta(q)_q^{m\times m}$.

(ii) Compute $C_1 = AS_1 + 2X_1 + M \in Z_q^{m\times m}$ and $C_2 = AS_2 + 2X_2 + 0^{m\times m}$(zero matrix) $\in Z_q^{m\times m}$.

(iii) Output the ciphertext $C = (C_1, C_2)$.

Universal Decryption$(T, C = (C_1, C_2))$. To decrypt C, we do the following steps.

(i) Set $E_1 = TC_1$.

(ii) Compute $M_1 = T^{-1}E_1 \bmod 2$.

(iii) Similarly, set $E_2 = TC_2$.

(iv) Compute $M_2 = T^{-1}E_2 \bmod 2$.

(v) If $(M_2 = 0^{m\times m})$, then output message $M = M_1$. Otherwise, decryption fails and output is $\perp$.

Universal Reencryption$(C = (C_1, C_2))$. To reencrypt ciphertext $C = (C_1, C_2)$ without using public key, we do the following steps.

(i) Choose two matrices $R_1, R_2 \leftarrow \psi_\beta(q)_q^{m\times m}$. We also choose error matrices $X_3, X_4 \leftarrow \psi_\beta(q)_q^{m\times m}$.

(ii) Compute

$$\begin{aligned} C_1' &= C_1 + C_2 R_1 + 2X_3 \\ &= (AS_1 + 2X_1 + M) + (AS_2 + 2X_2 + 0^{m\times m}) R_1 \\ &\quad + 2X_3 \\ &= A(S_1 + S_2 R_1) + (2(X_1 + X_2 R_1) + 2X_3) + M. \end{aligned} \tag{19}$$

(iii) Compute

$$\begin{aligned} C_2' &= C_2 R_2 + 2X_4 \\ &= (AS_2 + 2X_2 + 0^{m\times m}) R_2 + 2X_4 \\ &= AS_2 R_2 + 2X_2 R_2 + 0^{m\times m} + 2X_4. \end{aligned} \tag{20}$$

(iv) Output the ciphertext $C' = (C_1', C_2')$.

It is required that above universal reencryption scheme has the correctness property; that is, decryption of C' and decryption of C give the same message M. It is only possible when all the entries in $T2(X_1 + X_2R_1) + 2X_3 + M$ and $2X_2R_2+2X_4+0^{m\times m}$ are less than $q/2$. Since X_1, X_2, X_3, X_4, R_1, and R_2 are small, we can set parameter β small enough so that, with the probability exponentially close to 1, all the entries in $T2(X_1 + X_2R_1) + 2X_3 + M$ and $2X_2R_2 + 2X_4 + 0^{m\times m}$ are less than $q/2$.

Theorem 5. *Lattice based universal reencryption scheme is IND-URe-CPA (semantic) secure assuming that the $LWE_{q,\chi}$ is hard or $Adv_{B,LWE_{q,\chi}}(n) = Adv_{\chi,A}(n)$.*

Proof. It is the same as proof of [13]. □

6. Lattice Based Efficient Universal Reencryption

We use Fairbrother's idea [14] to reduce the size of the ciphertext by half. It also reduces the computational cost. The idea is that larger files can be split into k segments and size of each segment is $m \times m$ bits. In Singh et al.'s universal reencryption scheme [13], size of the plaintext is $(m\times m)$ and second part of the ciphertext is encryption of zero. In this scheme, size of the plaintext is $k(m \times m)$ and, for all these k segments, second part of the ciphertext (encryption of zero) is made the same.

In [13], size of the ciphertext for plaintext of size $k(m\times m)$ bits is $2k(m \times m)$ bits. With our efficient universal reencryption scheme size of the ciphertext for plaintext of size $k(m\times m)$ bits is $(k + 1)(m\times m)$ bits. Since second part of the ciphertext is same for all the segments, there is also some improvement in computation cost. Now, we describe our efficient scheme which is similar to [13].

Universal KeyGen(n). It is same as Universal KeyGen(n) algorithm of our scheme given in Section 5.

Universal Encryption(A, M). To encrypt message $M = (M_1, M_2, \ldots, M_k) \in \{0, 1\}^{k(m\times m)}$, we do the following steps.

(i) We choose random matrices $S_1, S_2, \ldots, S_{k+1} \leftarrow Z_q^{n\times m}$ and error matrices $X_1, X_2, \ldots, S_{k+1} \leftarrow \psi_\beta(q)_q^{m\times m}$.

(ii) For $i = 1$ to k, compute $C_i = AS_i + 2X_i + M_i \in Z_q^{m\times m}$.

(iii) Compute $C_{k+1} = AS_{k+1}+2X_{k+1}+0^{m\times m}$(zero matrix) $\in Z_q^{m\times m}$.

(iv) Output the ciphertext $C = (C_1, C_2, \ldots, C_{k+1})$.

Universal Decryption $(T, C = (C_1, C_2, \ldots, C_{k+1}))$. To decrypt C, we do the following steps.

(i) For $i = 1$ to k, set $E_i = TC_i$.

(ii) For $i = 1$ to k, compute $M_i = T^{-1}E_i \bmod 2$.

(iii) Similarly, set $E_{k+1} = TC_{k+1}$.

(iv) Compute $M_{k+1} = T^{-1}E_{k+1} \bmod 2$.

(v) If $(M_{k+1} = 0^{m\times m})$, then output message $M = M_1\| \cdots \|M_k$. Otherwise, decryption fails and output is $\perp$.

Universal Reencryption$(C = (C_1, C_2, \ldots, C_{k+1}))$. To reencrypt ciphertext $C = (C_1, C_2)$ without using public key, we do the following steps.

(i) Choose matrices $R_1, R_2, \ldots, R_{k+1} \leftarrow \psi_\beta(q)_q^{m\times m}$. We also choose error matrices $Y_1, Y_2, \ldots, Y_{k+1} \leftarrow \psi_\beta(q)_q^{m\times m}$.

(ii) Compute

$$\text{For } i = 1 \text{ to } k,$$

$$\begin{aligned} C_i' &= C_i + C_{k+1}R_i + 2Y_i \\ &= (AS_i + 2X_i + M_i) \\ &\quad + (AS_{k+1} + 2X_{k+1} + 0^{m\times m}) R_i + 2Y_i \\ &= A(S_i + S_{k+1}R_i) + (2(X_i + X_{k+1}R_i) + 2Y_i) + M_i. \end{aligned} \tag{21}$$

(iii) Compute

$$\begin{aligned} C_{k+1}' &= C_{k+1}R_{k+1} + 2Y_{k+1} \\ &= (AS_{k+1} + 2X_{k+1} + 0^{m\times m}) R_{k+1} + 2Y_{k+1} \\ &= AS_{k+1}R_{k+1} + 2X_{k+1}R_{k+1} + 0^{m\times m} + 2Y_{k+1}. \end{aligned} \tag{22}$$

(iv) Output the ciphertext $C' = (C_1', C_2', \ldots, C_{k+1}')$.

Correctness property is similar to correctness of previous scheme [13].

Theorem 6. *The lattice based improved universal reencryption scheme is IND-URe-CPA (semantic) secure assuming that the $LWE_{q,\chi}$ is hard or $Adv_{B,LWE_{q,\chi}}(n) = Adv_{\chi,A}(n)$.*

Proof. We now show universal semantic security of the universal reencryption scheme. We will show that if there exists a PPT adversary $\mathscr{A}$ that breaks universal reencryption scheme with nonnegligible probability then there must exist a PPT challenger $\mathscr{B}$ that solves decision LWE hard problem with nonnegligible probability by simulating views of A.

Adversary $\mathscr{A}$ constructs the ciphertext $C = (C_1, C_2, \ldots, C_k, C_{k+1})$ for message m and sends to the challenger $\mathscr{B}$. Ciphertext C_{k+1} is statistically close to uniform.

For $i = 1$ to k,

{challenger $\mathscr{B}$ obtains m LWE samples (for vector $r_{i,1}$), m LWE samples (for vector $r_{i,2}$), $\ldots$, m LWE samples (for vector $r_{i,m}$) where vectors $r_{i,1}, r_{i,2}, \ldots, r_{i,m}$ are from Gaussian (error) distribution ψ^m and matrix $R_i = [r_{i,1} \cdots r_{i,m}]$. It parsed as $C_{k+1}R_i + 2X_{3,i}$ and then challenger computes $C_i' = C_{k+1}R_i + 2X_{3,i} + C_i$}.

Similarly, challenger again obtains m LWE samples (for vector r_1'), m LWE samples (for vector r_2')$\cdots$ m LWE samples (for vector r'_m) where vectors $r'_1, r'_2, \ldots, r'_m$ are from Gaussian (error) distribution ψ^m and matrix $R_{k+1} = [r'_1 \cdots r'_m]$. It parsed as $C_{k+1}R_{k+1} + 2X_4$, and then challenger assigns $C'_{k+1} = C_{k+1}R_{k+1} + 2X_4$. Here, matrices $X_{3,1}, \ldots, X_{3,k}, X_4 \leftarrow \psi_\beta(q)_q^{m\times m}$.

Challenger $\mathscr{B}$ sends $C^* = (C'_1, \ldots, C'_k, C'_{k+1})$ to the adversary $\mathscr{A}$.

When Oracle O is a pseudorandom LWE oracle, then C^* is a valid universal reencryption of ciphertext C. When Oracle O is a random oracle, then C^* is a uniform. Finally, adversary $\mathscr{A}$ terminates with some output; challenger $\mathscr{B}$ terminates with same output and ends the simulation. So if adversary $\mathscr{A}$ breaks the scheme, then there exists challenger $\mathscr{B}$ which solves decision LWE hard problem.

$\mathrm{Adv}_{B,\mathrm{LWE}_{q,\chi}}(n) = \mathrm{Adv}_{\chi,A}(n)$. Hence, our scheme is universal semantic secure. □

7. Conclusion

We have presented an improved construction for lattice based universal reencryption. Disadvantage of universal reencryption is that receiver has to decrypt all the ciphertexts to identify message for him. A lattice based universal reencryption scheme improving this cost in the receiver side is an open problem.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors would like to thank one of the anonymous reviewers of the MIST 2013 for pointing out a mistake in our scheme. This paper is extended version of our paper published in MIST 2013.

References

[1] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, 1981.

[2] P. Choonsik, I. Kouichi, and K. Kurosawa, "Efficient anonymous channel and all/nothing election scheme," in *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 185–194, Springer, New York, NY, USA, 2007.

[3] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[4] P. Golle, M. Jakobsson, A. Juels, and P. Syverson, "Universal reencryption for mixnets," in *Topics in Cryptology—CT-RSA 2004: Proceedings of the Cryptographers' Track at the RSA Conference 2004, San Francisco, CA, USA, February 23–27, 2004*, vol. 2964 of *Lecture Notes in Computer Science*, pp. 163–178, Springer, Berlin, Germany, 2004.

[5] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[6] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)," in *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC '96)*, pp. 99–108, ACM, 1996.

[7] C. Gentry, *A fully homomorphic encryption scheme [Ph.D. thesis]*, Stanford University, 2009.

[8] S. Garg, C. Gentry, and S. Halevi, "Candidate multilinear maps from ideal lattices," in *Advances in Cryptology—EUROCRYPT 2013: Proceedings of the 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26–30, 2013*, vol. 7881 of *Lecture Notes in Computer Science*, pp. 1–17, Springer, Berlin, Germany, 2013.

[9] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC '05)*, pp. 84–93, ACM, 2005.

[10] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46–55, 2003.

[11] R. Wiangsripanawan, R. Safavi-Naini, and W. Susilo, "Location privacy in mobile IP," in *Proceedings of the IEEE 7th Malaysia International Conference on Communication and the 13th IEEE International Conference on Networks*, pp. 16–18, IEEE, 2005.

[12] C. Gentry, S. Halevi, and V. Vaikuntanathan, "A simple BGN-type cryptosystem from LWE," in *Advances in Cryptology—EUROCRYPT 2010*, Lecture Notes in Computer Science, pp. 506–522, Springer, Berlin, Germany, 2010.

[13] K. Singh, C. Pandu Rangan, and A. K. Banerjee, "Lattice based universal re-encryption for mixnet," in *Proceedings of the 5th International Workshop on Managing Insider Security Threats (MIST '13)*, pp. 1–11, Pukyung National University, Busan, South Korea, 2013.

[14] P. Fairbrother, "An improved construction for universal re-encryption," in *Privacy Enhancing Technologies: 4th International Workshop, PET 2004, Toronto, Canada, May 26–28, 2004. Revised Selected Papers*, vol. 3424 of *Lecture Notes in Computer Science*, pp. 79–87, Springer, Berlin, Germany, 2004.

[15] W. Mao, *Modern Cryptography Theory and Practice*, Pearson Education, Upper Saddle River, NJ, USA, 2002.

[16] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*, The Springer International Series in Engineering and Computer Science, Kluwer Academic, 2002.

[17] V. Vaikunthanathan, *Topics in Applied Discrete Mathematics: Lattices in Computer Science*, Lecture Series, CSC2414, 2011.

[18] J. Alwen and C. Peikert, "Generating shorter bases for hard random lattices," in *Proceedings of the International Symposium on Theoretical Aspects of Computer Science (STACS '09)*, IBFI Schloss Dagstuhl, pp. 75–86, 2009.

[19] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (H)IBE in the standard model," in *Advances in Cryptology—EUROCRYPT 2010*, vol. 6110 of *Lecture Notes in Computer Science*, pp. 553–572, Springer, Berlin, Germany, 2010.

[20] B. Applebaum, D. Cash, C. Peikert, and A. Sahai, "Fast cryptographic primitives and circular-secure encryption based on hard learning problems," in *Advances in Cryptology—CRYPTO 2009*, vol. 5677 of *Lecture Notes in Computer Science*, pp. 595–618, Springer, Germany, Berlin, 2009.

[21] R. Lindner and C. Peikert, "Better key sizes (and attacks) for LWE-based encryption," in *Topics in Cryptology—CT-RSA 2011*, vol. 6558 of *Lecture Notes in Computer Science*, pp. 319–339, Springer, Heidelberg, Germany, 2011.

[22] K. Xagawa, *Cryptography with lattices [Ph.D. thesis]*, Department of Mathematical and Computing Sciences, Tokyo Institute of Technology, 2010.

[23] K. Sampigethaya and R. Poovendran, "A survey on mix networks and their secure applications," *Proceedings of the IEEE*, vol. 94, no. 12, pp. 2142–2180, 2006.

[24] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

Hindawi Publishing Corporation
Mobile Information Systems
Volume 2015, Article ID 741460, 17 pages
http://dx.doi.org/10.1155/2015/741460

Research Article

Design, Implementation, and Performance Evaluation of Efficient PMIPv6 Based Mobile Multicast Sender Support Schemes

Lili Wang,[1,2] Yajuan Qin,[1] Huachun Zhou,[1] Jianfeng Guan,[3] and Hongke Zhang[1]

[1] *National Engineering Lab for NGI Interconnection Devices, Beijing Jiaotong University, Beijing 100044, China*
[2] *Research Institute of China Electronics Equipment System Engineering Corporation, Beijing 100141, China*
[3] *State Key Lab of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*

Correspondence should be addressed to Lili Wang; liliwang@bjtu.edu.cn

Received 1 September 2014; Accepted 1 September 2014

Academic Editor: Ilsun You

Proxy Mobile IPv6 (PMIPv6) is proposed as a promising network-based mobility management protocol, which does not need any participation of mobile nodes. PMIPv6 does not support the multicast well and most of the current research concentrates on the mobile multicast receiver. However, the mobile multicast sender is also very important and challenging, which has not been addressed well. Therefore, in this paper we propose two efficient PMIPv6 based mobile multicast sender support schemes which are PMIP bidirectional tunneling (PMIP-BT) and PMIP direct routing (PMIP-DR). In the PMIP-BT, the multicast traffic can be delivered through the PMIPv6 bidirectional tunnel, while, in the PMIP-DR, the multicast data can be transmitted via an optimized direct multicast routing. Both of them can support the multicast sender mobility transparently enabled in the PMIPv6 networks. We evaluate the performance of the proposed schemes by theoretical analysis, and the numerical results show that the proposed schemes have a better performance in terms of the signaling cost than the current schemes. Meanwhile, the proposed schemes are also implemented on the test bed, and the experimental results not only verify the validity and feasibility of our proposed schemes, but also conclude the different scenarios to which they are applicable.

1. Introduction

With the development of the wireless and mobile communication technology, the mobile Internet has been popular and become the focus of the development of information and communication industry [1–3]. As an extension of mobile Internet, mobile multicast has become a research hotspot, such as [4, 5], and has drawn significant attention over a decade [6]. Until now, a variety of solutions have been proposed, but most of them are based on the host-based mobility approach [6, 7], such as Mobile IPv6 (MIPv6) [8]. Besides, it is pointed out that the performance of mobile multicast depends upon that of mobility management protocols [6]. As a network-based mobility support protocol, Proxy Mobile IPv6 (PMIPv6) [9] has a smaller handover delay and higher quality of service (QoS) than the host-based mobility solutions and does not require any participation of mobile nodes (MNs) in mobility-related signaling. Therefore, PMIPv6 is believed to be one of the promising solutions for the future all-IP wireless network [10] and is adopted in the 3GPP (3rd Generation Partnership Project) LTE (Long Term Evolution) and SAE (System Architecture Evolution) architecture [11]. However, the basic PMIPv6 does not provide the multicast communication schemes. As a result, a new development boom for IP mobile multicast based on PMIPv6 has been launched.

At the same time, the mobile multicast technology generally focuses on the multicast receiver mobility [12] and the Internet community has made great efforts to support mobile receivers in multicast sessions [7]. Comparing with the multicast receiver mobility, there is less interest in mobile multicast senders. However, the area of the multicast sender mobility has been accompanied by the development of mobile multicast [7], and this issue is highly critical for the deployment of the multicast service. For example, there is an advanced concept based on the Intelligent Transport Systems

(ITS) service. In this concept, all the vehicles on the same route are identified by using a GPS or a car-navigation system. The vehicles multicast real-time video information about the transportation through the communication infrastructure like 3G, WiFi to the other vehicles interested in it [13]. Besides, in the mobile social network services especially the user generated content (UGC) services [14], most users want to publish their contents at anytime and anywhere and many users want to acquire these contents, so it is important to provide the mobility support to meet the requirements for large number of users. The multicast sender mobility is one of the core supporting schemes to realize the above functions.

In addition, due to the fact that the mobility of the multicast receivers only affects the reception of data for the node itself and the multicast sender mobility directly results in the failure of the entire multicast tree, the processing of the sender mobility will be more complex than the receiver mobility [6]. Until now, the mobile multicast for mobile receiver based on PMIPv6 has been published as RFC6224 in IETF [4]; however, the multicast sender mobility is still in the early stage [5]. Even though the IETF MULTIMOB working group [5] and Wang et al. [15] have proposed methods for multicast sender mobility in PMIPv6 networks, they all need the additional multicast listener discovery (MLD) proxy functions [16] and have the inefficient routing issue. Therefore, efficient multicast sender mobility schemes for PMIPv6 are needed urgently.

In this paper, we make some extensions of the PMIPv6 protocol to support the multicast communication in PMIPv6 networks and propose PMIP bidirectional tunneling (PMIP-BT) and PMIP direct routing (PMIP-DR) as two efficient PMIPv6 based mobile multicast sender support schemes. The PMIP-BT scheme supports the multicast data transmitted through the PMIPv6 bidirectional tunnel, while the PMIP-DR mechanism delivers the multicast packets through a direct multicast routing. Both of them can enable the multicast sender mobility transparently in the PMIPv6 networks and can solve the inefficient routing issue existing in [5, 15]. The performance evaluation is performed by the theoretical analysis, and the numerical results show that our proposed schemes significantly decrease the signaling cost. In addition, we implement the proposed schemes in the test-bed, which verifies their validity and feasibility. Furthermore, from the experimental results, we can obtain that the proposed two schemes are suited for distinct scenarios.

The remainder of this paper is organized as follows: Section 2 briefly reviews the related work. Section 3 describes the proposed PMIP-BT and PMIP-DR schemes in detail. Section 4 presents the performance evaluation and the numerical results in terms of signaling costs. Section 5 presents the implementation overview and the experimental results on the performance of multicast handover latency. Section 6 concludes the paper.

2. Related Work

Till now, a variety of mobile multicast mechanisms have been raised, in which most schemes commit to solve the multicast receiver mobility problem. Therefore, we mainly focus on the schemes for the multicast sender mobility support. There are two types of mobility support protocols proposed by the IETF, which are host-based and network-based mobility management architectures. Thus, current mobile multicast sender technologies are divided into the host-based and network-based categories in analogy, which is shown in Table 1. From Table 1, we can conclude that current mobile multicast sender supporting schemes mostly are based on MIPv6 and there are few technologies based on PMIPv6.

Table 1: Current mobile multicast sender schemes.

Schemes	Multicast sender mobility
Host-based	[8, 17–22]
Network-based	[5, 15, 23]

In the host-based mobility management architecture, the issue of multicast sender mobility has been widely recognized and studied. A variety of solutions have been proposed for mobile multicast sender support, which mainly followed the basic method for mobile multicast receivers, that is, mobile IP bidirectional tunneling approach (MIP-BT) and mobile IP remote subscription approach (MIP-RS) [8, 17]. In addition, there are also some extension methods, such as MRP [18] and MSSMS [19].

In [8, 17], two essential host-based multicast mobility approaches, which are MIP-BT and MIP-RS, are proposed. However, lots of disadvantages still exist in both of the schemes, such as the triangle routing issue [24] in the MIP-BT mechanism and higher handover delay and "out-of-synch" problem [25] in the MIP-RS scheme. Therefore, many researches such as MoM [26] and RBMoM [27] focused on solving the problem existing in the two basic approaches to improve the overall performance. Besides, there are also some extension methods proposed for the mobile multicast sender support, including tree morphing approach [20] and state update mechanism [21].

In [20], a tree morphing protocol for multicast sender mobility is proposed, in which the existing source-based distribution trees are reused and modified to continuously serve for the multicast data delivery of mobile senders. In this scheme, all nodes can identify (CoA,G) based tree topology and (HoA,G) based group membership by maintaining (CoA,G,HoA) address-triples in router states. Therefore, it is required that all the routers need to be extended, which not only increases the complexity but also introduces an expensive signaling overheads and state refresh costs. In addition, it is a host-based scheme and then will inherit all the disadvantages of MIPv6.

In [21], the authors introduced a state update mechanism which reuses the major parts of prior established multicast trees. However, the reconstruction of the multicast tree in this scheme is initiated by the multicast sender instead of the multicast receiver, which needs lots of changes for multicast.

In [18], the case that an MN is working as a sender and simultaneously a receiver for the multicast group is considered. In this mechanism, a combination of the MIP-BT and MIP-RS scheme is adopted. For the sender, to forward the multicast traffic, a reverse tunnel from the MN's current point of attachment to its home agent (HA) is utilized. For the receiver, to receive the multicast data, the MIP-RS scheme is used. A multicast join message as well as a notification message from the sender to its HA or foreign agent (FA) is needed, which indicates that higher requirements will be needed for the hosts and the bandwidth resources as well as signaling costs will increase.

In [22], the authors introduced a scheme that is an extension to the MLD multicast protocol, in which a new entity called MDA (multicast delivery agent) is added. In this scheme, the tunnel is established between the MDA and the HA. Thus, the multicast traffic originated from the sender is transmitted to the HA through the MDA. Due to the fact that the route of this scheme is more optimized than that of the MIP-BT scheme and the delay of the tree reestablishment is lower than that of the MIP-RS scheme, it is a compromise of the MIP-BT scheme and the MIP-RS scheme. However, the signaling interaction between the multicast sender and the MDA will bring extra network traffic loads. Besides, the check of the direct connection between the multicast sender and the MDA is still up in the air.

All the above schemes are host-based, which will have the deployment limitation issue. In recent years, with the release of the network-based mobility protocol in the IETF, a new development boom of IP mobile multicast has been launched [15]. The MULTIMOB working group was established by the IETF in 2009 to provide guidance of multicast support in PMIPv6 networks and the base deployment for multicast receiver mobility in PMIPv6 domains has been released as RFC6224 [4]. However, there are only a few mobile multicast sender support schemes which are based on PMIPv6 and Von Hugo et al. propose that the mobile multicast sender support in PMIPv6 networks is needed to solve in the future [28].

In [23], two PMIPv6 multicast methods, called the LMA-based (local mobility anchor-based) method and MAG-based (mobile access gateway-based) method, are proposed. However, our experiments verify the infeasibility of the two methods. For the LMA-based method, it is infeasible that the source address of the report message sent by the multicast receiver is a globally routable address, because it is specified in RFC3810 [29] that the source address of the report message should be link address. Besides, the multicast packets sent by the multicast sender can not be transmitted to the PMIPv6 bidirectional tunnel; that is due to the fact that PMIPv6 specification does not provide the multicast communication scheme. For the MAG-based approach, the join message from the multicast receivers can not be directly delivered to the MAG, since the topological anchor of the MN in PMIPv6 networks is the LMA and thereby the join message will not be sent to the MAG but the LMA.

In [5, 15], two multicast sender mobility schemes for PMIPv6 are proposed, which are the BS (base solution) and the DMRS (direct multicast routing scheme). The BS can support the multicast data delivered to the receivers through the PMIPv6 tunnel firstly, while the DMRS can provide a direct optimized routing for the multicast traffic. The two proposed schemes can not only provide multicast communications but also support the multicast sender mobility in PMIPv6 networks. However, the additional MLD Proxy functions [16] are needed for these schemes, which increases the complexity. Meanwhile, there is inefficient routing issue in the BS.

3. Efficient PMIPv6 Based Mobile Multicast Sender Support Schemes Design

3.1. Design Goals. According to the goals for PMIPv6 described in [30] and the various problems existing in the host-based multicast sender mobility schemes, we firstly overview the design goals for PMIPv6 based multicast sender mobility schemes.

First of all, we must follow the principle of PMIPv6 that is supporting unmodified MN, which makes PMIPv6 avoid the deployment issue in MIPv6. In this way, when MN moves from one MAG to another MAG, the MN does not need any modification, which indicates that the MN always remains agnostic of multicast mobility operations and the handover is transparency to the mobile sender MN.

Secondly, the handover performance must be improved, such as multicast handover delay and packet loss. The reason is that the mobility of a multicast sender will result in the failure of the entire multicast tree [6]. Therefore, the multicast handover delay should be minimized under the movement of a multicast sender.

Last but not least, the routing inefficiency problem illustrated in [5] must be solved to enhance the multicast routing performance. We must achieve the multicast services at the least cost of the network resources, which can meet the requirements of low power for smart city in the future.

3.2. Design and Function Implementation. According to the forwarding rules described in RFC5213, when an MAG receives packets from an MN connected to its access link, to a destination that is not directly connected, the packets must be forwarded to the LMA through the bidirectional tunnel established between the MAG and the LMA (MAG-LMA). Besides, it is assumed that the link between the MN and the MAG has multicast capability. However, there is no scheme for the multicast data forwarding. Thus, when the multicast traffic flows sent by the mobile sender arrive at the MAG, these packets will be simply discarded by the MAG, which has been verified by our experiments in the test-bed. The reason is that there is no multicast forwarding information base (MFIB) on the MAG.

Therefore, in order to make the multicast data be forwarded or transmitted through the MAG-LMA bidirectional tunnel in PMIPv6 network, some extensions on the PMIPv6 protocol are required. The MAG should make some extensions to establish the corresponding multicast forwarding states for the multicast data transmission through the MAG-LMA tunnel. Then, when a mobile sender MN accesses to an MAG, this MAG should not only build the PMIPv6 bidirectional tunnel and add route for the unicast data destined to or originated from the MN, but also update the multicast forwarding cache (MFC) for the multicast traffic. In this way, the PMIPv6 protocol could support the delivery of the multicast packets.

0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
	Sequence #
A H L K M R P S D Reserved	Lifetime
Multicast group address option	
Multicast sender address option	

Figure 1: Extended PBU message.

0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
	Status K R P S D Res.
Sequence #	Lifetime
Multicast group address option	
Multicast sender address option	

Figure 2: Extended PBA message.

In order to support the multicast communication in PMIPv6 networks, the proxy binding update (PBU) message and proxy binding acknowledgement (PBA) message are extended, which are shown in Figures 1 and 2. From Figures 1 and 2, we can see that a one-bit "S" flag and "D" flag as well as two new mobility options are added, in which the "S" flag is a multicast sender identification flag and is used to identify whether this MN is a mobile multicast sender. When the "S" flag in the PBU and PBA message is set to "1," the multicast group address related to the multicast session provided by the mobile multicast sender should be attached in the multicast group address option. Besides, the "S" flag in the PBA message is set to "1" only if the corresponding PBU message has the "S" flag set to "1." A one-bit "D" flag is used to identify whether the MAG has the ability to support the direct routing for multicast data. When the "D" flag in the PBA message is set to "1" as the same value in the PBU message, the MAG will not deliver the multicast packets to the PMIPv6 tunnel but directly send them to the multicast domain. However, when the "D" flag in the PBA message is set to "0" but its value in the PBU message is "1," the direct routing for multicast data is not allowed by the LMA. Since one multicast packet transmission path is through the PMIPv6 bidirectional tunnel, we call the scheme PMIP-BT, while since the other path for the multicast data is direct routing, this mechanism is denoted as PMIP-DR for simplicity, which will be described in detail in the following sections.

3.2.1. PMIP-BT Scheme. Figure 3 shows the detailed procedure of the mobile multicast sender's attachment and multicast communication in PMIP-BT scheme. As illustrated in Figure 3, when a mobile sender MN connects to an MAG, the MAG detects the attachment of the MN firstly and then obtains some information from the policy profile, including the MN-identifier (MN_ID), multicast group address, and the LMA address. Then an extended proxy binding update (PBU) message with both the "S" flag and the "D" flag set to value of 1 is sent to the LMA. Receiving this extended PBU message, the LMA decides whether this MN is authorized to send multicast data for the group address in the multicast group address option. If the MN is certified, the LMA sends back an extended proxy binding acknowledgement (PBA) message with the "S" flag set to "1," "D" flag set to "0," and the home network prefix (HNP) assigning for the MN to the MAG. Afterwards, the tunnel is established in the LMA. On receiving the PBA message, the MAG establishes its endpoint of the bidirectional tunnel to the LMA and also sets up the forwarding routes for the MN's unicast traffic. At the same time, the MAG also updates the MFC in the kernel for supporting the multicast communication. After that, the MAG sends router advertisement (RA) message to the MN on the access link for advertising the MN's HNP as the hosted on-link prefix. In this way, when the MAG receives a multicast packet from a mobile sender MN connected to its access link, to a multicast destination that has been authorized by the LMA, the MAG will forward this packet to the LMA through the bidirectional tunnel established between itself and the LMA, which is just the same as the unicast data transmission specified in RFC5213.

When the mobile multicast sender hands over from one MAG to another, it can continue to send multicast data as soon as the network connectivity is reconfigured. At this time, the new MAG performs the binding registration to the LMA and updates the corresponding unicast routes and MFCs for the mobile multicast sender. In this way, the multicast packets arriving at this new MAG will be forwarded again to the LMA according to the MFC and eventually to the receivers.

The detailed handover process is illustrated in Figure 4, in which MN1 is the mobile multicast sender and the MN2 and correspondent nodes (CNs) are both the multicast receivers. Besides, the MN2 attaches to the same MAG (MAG1) with the mobile sender MN1 but associates with a different LMA (LMA2). For simplicity, we abbreviate the "MLD Membership Report" as "Join" in Figure 4. As shown in Figure 4, when the MN1 accesses to the MAG1, the multicast packets could be transmitted to the CN through the PMIPv6 tunnel and directly sent to the MN2 via the MFC at the MAG1. When the MN1 moves to the MAG2, as soon as the binding registration to the LMA1 and the establishment of multicast forwarding states for the MN1 at the MAG2 has been completed and also the IP address of the MN1 has been configured, the multicast data could be successfully delivered by the MAG2 to the LMA1 and eventually to the receivers CN and MN2. Therefore, the multicast sender mobility is transparently enabled in the PMIPv6 networks.

3.2.2. PMIP-DR Scheme. Figure 5 illustrates the detailed procedure of the mobile multicast sender's attachment and multicast communication in PMIP-DR scheme. Compared with Figure 3, the difference of the attachment for the mobile sender is the "D" flag in PBA message. As shown in Figure 5, the value of the "D" flag in the extended PBA message is "1" in this scheme, while the value is set to "0" in PMIP-BT

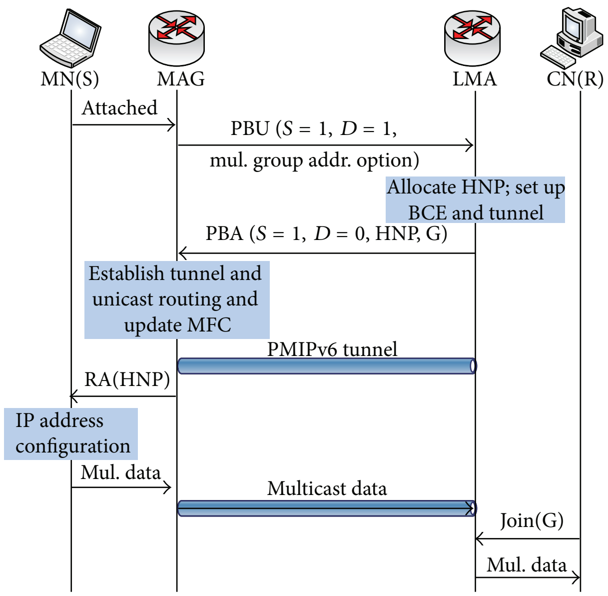


Figure 3: Call flow of the mobile multicast sender's attachment and multicast communication in PMIP-BT scheme.

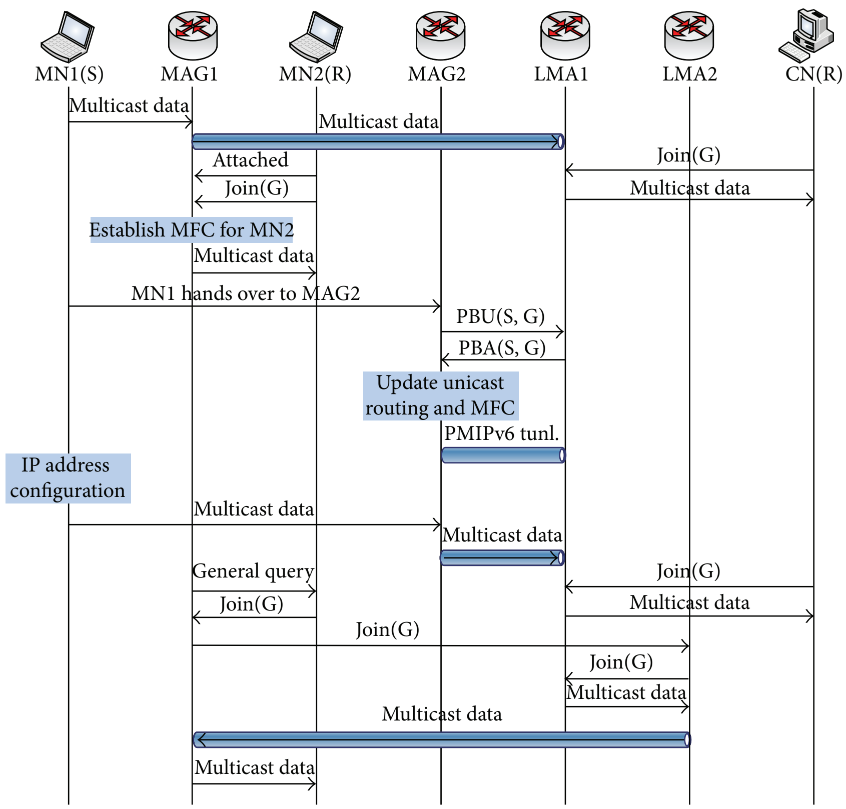


Figure 4: Call flow of the multicast communication for multicast sender handover in PMIP-BT scheme.

scheme. That means the direct routing for the multicast data transmission will be adopted. After the PMIPv6 registration of the mobile sender, the sender begins to send multicast data to the MAG. The receiver CN sends join message to the sender and finally arrives at the MAG which is the designated router (DR) of the multicast sender. At this time, the MAG establishes the multicast forwarding states for the CN. Then, the multicast data is delivered to the CN through a direct routing from the MAG.

When the mobile multicast sender moves from one MAG to another, it can continue to send multicast traffic once the PMIPv6 registrations have been successfully completed.

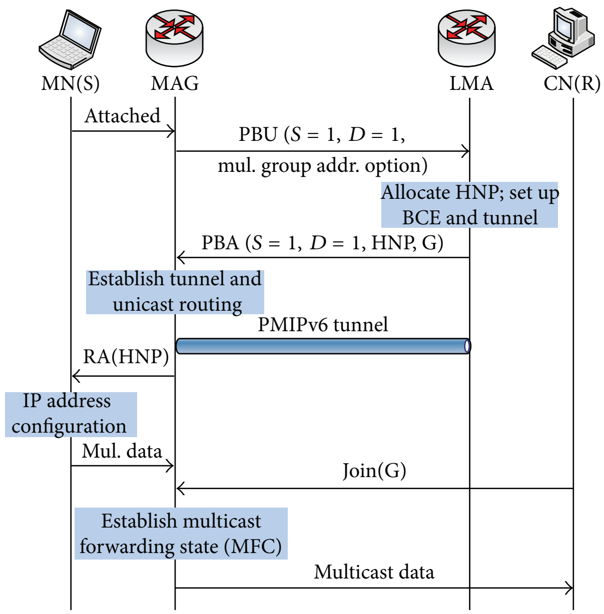


Figure 5: Call flow of the mobile multicast sender's attachment and multicast communication in PMIP-DR scheme.

At this time, the new MAG will act as the new DR for the mobile multicast sender and establish the multicast forwarding states for all the receivers who subscribe to the multicast service provided by the mobile sender. In this way, according to the MFC of the new MAG, the multicast packets arriving at this new MAG will be transmitted again to the multicast domain via a direct routing and eventually to the receivers.

The detailed handover process is shown in Figure 6. Similar to Figure 4, the MN1 is the mobile multicast sender, while both MN2 and CN are the multicast receivers. Additionally, the MN2 attaches to the same MAG (MAG1) with the MN1 but associates with a different LMA (LMA2). Also, "MLD Membership Report" is abbreviated as "Join" for simplicity in Figure 6. As shown in Figure 6, when the MN1 accesses to the MAG1, the multicast data could be directly delivered to the CN and the MN2 by the MAG1 via the MFC. When the MN1 hands over to the MAG2, after the completion of the binding registration for the MN1 and the establishment of multicast forwarding states at the MAG2 for the receivers, the multicast data could be successfully transmitted by the MAG2 to the receivers CN and MN2 through a direct routing. Thus, the multicast sender mobility is also transparently enabled in the PMIPv6 networks by this scheme.

3.2.3. Operations of the MN. There are not any additional functionalities or modifications required for the MN, which meets one of the design goals for this scheme. Therefore, an MN serving as a mobile multicast source will send multicast data as if attached to the fixed Internet.

3.2.4. Operations of the MAG. In order to provide the multicast service in PMIPv6 networks, the MAG must recognize the MN attached to it is a multicast sender firstly. Then, the corresponding multicast group address of which the multicast sender MN provides multicast service must also be learned. The MAG can learn these pieces of information during the authentication phase for example. Therefore, the PBU message should be extended, including the multicast sender identification flag "S", direct routing identification flag "D", multicast group address option, and multicast sender address option. Figures 7 and 8 show the format of these two mobility options. When the MAG finds that the attached MN is a multicast sender, it should send the extended PBU message to the LMA. In the extended PBU message, a one-bit "S" flag is set to "1" and the multicast group address is contained in the multicast group address option. Besides, a one-bit "D" flag indicates whether the MAG supports the direct routing scheme. When the MAG receives the extended PBA message with the "D" flag set to "1," it will forward the multicast data through a direct multicast routing. Otherwise, the multicast service must be provided via the PMIPv6 bidirectional tunnel.

In PMIP-BT scheme, on the arrival of a mobile multicast sender MN, the MAG should not only set up the unicast route for the MN, but also establish the multicast forwarding state and update the MFC for the MN. Besides, the establishment of the multicast forwarding states for the receivers is required for a MAG in PMIP-DR scheme. Thus, the MAG should participate in multicast routing functions, such as Protocol Independent Multicast-Sparse Mode (PIM-SM). Besides, the MAG serves as the DR of the multicast sender MN. According to RFC4601 [31], it is required that the DRs should directly connect with the senders. However, the LMA, not the MAG, advertises the HNP of the mobile sender to the network in PMIPv6 networks. Therefore, to address this issue, the MAGs should be set as PIM border routers and the border-bit should be activated, or the MAGs run the Bidirectional Protocol Independent Multicast (BIDIR-PIM) [15, 32].

3.2.5. Operations of the LMA. Similar to the extensions of the PBU message, the PBA message should also add the "S" flag, "D" flag, multicast group address option, and multicast sender address option. If the LMA receives the extended PBU message with "S" flag and "D" flag set to value of "1," it should judge whether the MAG could adopt the direct multicast routing scheme and indicate this to the MAG by the extended PBA message with the "D" flag. However, if the "D" flag is set to "0" in the extended PBU message, the LMA will set the "D" flag to value "0" in the extended PBA message.

In PMIP-BT scheme, as the persistent HA and the DR of the multicast sender MN, the LMA should not only establish a tunnel to the MAG and update the unicast route table for the MN, but also manage and maintain a MFIB for all group traffic arriving from its mobile senders. At the same time, the LMA should participate in multicast routing functions, such as PIM-SM, that enable traffic redistribution to all adjacent routers and thereby ensure a continuous session when the multicast sender is in motion. As described above, the DRs require the senders to be directly connected with itself based on RFC4601 [31]. However, since the MAGs are routers intermediate to the multicast senders (MNs) and the LMAs

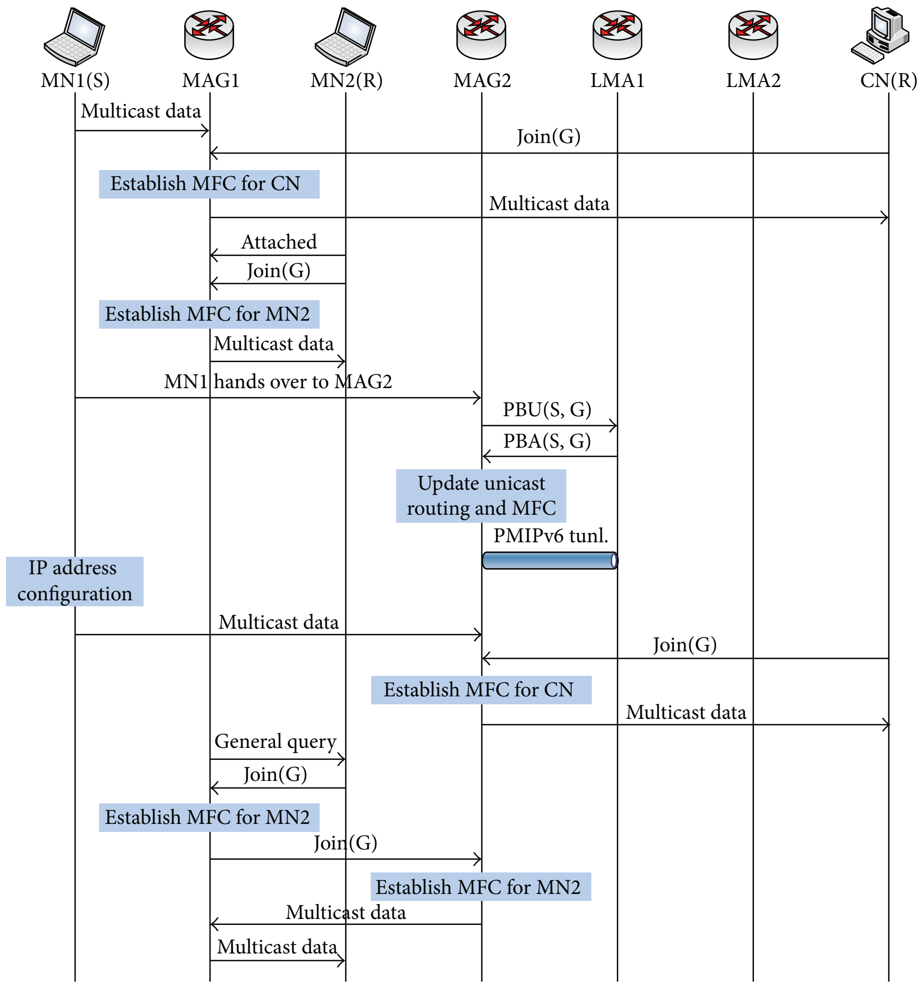


Figure 6: Call flow of the multicast communication for multicast sender handover in PMIP-DR scheme.

0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	
Type	Length	State	Prefix length	Res.
Multicast group address				

Figure 7: Multicast group address option.

0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
Type	Length	Reserved
Multicast sender address		

Figure 8: Multicast sender address option.

who are serving as DRs of the MNs in PMIPv6 domain, there exists the check of direct connection issue specified in [15]. Therefore, to address this issue, the LMAs should be set as PIM border routers and the border-bit should be activated, or the LMAs run the BIDIR-PIM [15, 32].

4. Performance Evaluation

This section evaluates the performance of the two proposed multicast sender mobility schemes which are PMIP-BT and PMIP-DR. In the analysis, we compare our schemes with HMIP bidirectional tunneling (HMIP-BT) and HMIP remote subscription (HMIP-RS) [8] and mainly concern on the signaling cost. In this paper, we define the signaling cost as hops × signaling message size [33].

4.1. Analytical Mobility Model. In [34], a new two-dimensional hexagonal random walk model in personal communication services (PCS) system had been presented. Due to the large number of states, an improved random walk model was proposed in [35]. Given the fact that one MAP or PMIPv6 domain is usually composed of several subnets, we present a modified two-dimensional hexagonal random walk model to analyze the signaling cost.

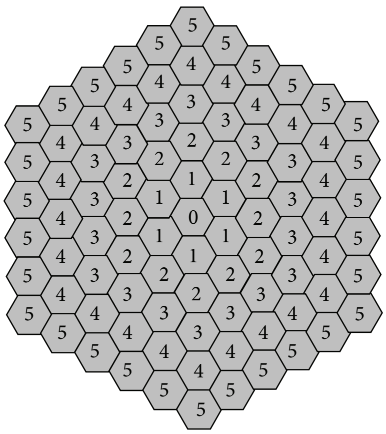


Figure 9: Six-layer analytical mobility model.

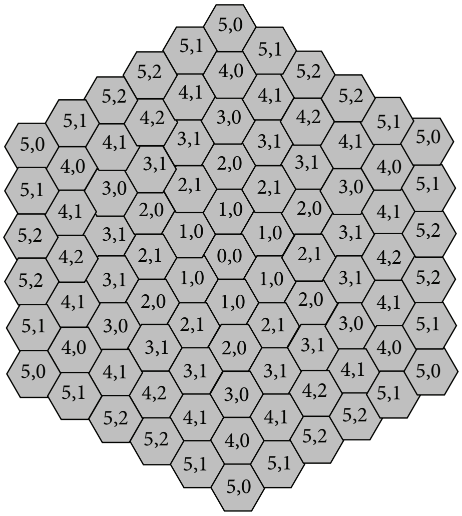


Figure 10: Type classification for the six-layer analytical mobility model.

Figure 9 shows the six-layer hexagonal analytical mobility model. In this model, each ring is labeled according to its distance from the center. The innermost cell "0" is called the center cell; the cells labeled "1" form the first ring around the center cell; the cells labeled "2" form the second ring around the center cell and so on. Each ring r ($r \geq 0$) consists of $6r$ cells. Based on this model, each cell represents an MAG or AR subnet, and a PMIPv6 domain or MAP domain includes six layers.

Figure 10 illustrates the type classification for the six-layer analytical mobility model. The subnets in a domain are classified into different types. The form $\langle x, y\rangle$ is used to distinguish the different subnets, where x indicates that this subnet is in ring x, and y indicates the $y + 1$st type in ring x. The subnets which are at the symmetrical positions on the hexagonal domain will have same type and same traffic flow pattern.

Suppose that an MN resides in a MAG/AR subnet for a period and moves to one of its six neighbors with equal probability (1/6). Figure 11 presents the state transition diagram for the six-layer random walk model, in which state (x, y) represents the MN is in one of the subnets of type $\langle x, y\rangle$ and state $(n, 0)$ is absorbing state, where $0 \leq x < n$, $0 \leq y \leq \lfloor x/2 \rfloor$, and n is the layers of a domain. In our presented random walk model, the numbers of states are $(n^2 + 2n + 5)/4$ when n is odd and $(n^2 + 2n + 4)/4$ when n is even, which significantly reduces the number of states when compared with that in [34] $(n(n + 1)/2)$. The corresponding one step state transition matrix is as follows, in which the elements are in the following order: (0, 0), (1, 0), (2, 0), (2, 1), (3, 0), (3, 1), (4, 0), (4, 1), (4, 2), (5, 0), (5, 1), (5, 2), (6, 0):

$$P = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{6} & \frac{1}{3} & \frac{1}{6} & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \frac{1}{6} & 0 & \frac{1}{3} & \frac{1}{6} & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \frac{1}{3} & \frac{1}{3} & 0 & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \frac{1}{6} & 0 & 0 & \frac{1}{3} & \frac{1}{6} & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & 0 & \frac{1}{6} & \frac{1}{6} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \frac{1}{6} & 0 & 0 & \frac{1}{3} & 0 & \frac{1}{6} & \frac{1}{3} & 0 & 0 \\
0 & 0 & 0 & 0 & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & 0 & \frac{1}{6} & 0 & \frac{1}{6} & \frac{1}{6} & 0 \\
0 & 0 & 0 & 0 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 & 0 & 0 & \frac{1}{3} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{6} & 0 & 0 & 0 & \frac{1}{3} & 0 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{6} & \frac{1}{6} & 0 & \frac{1}{6} & 0 & \frac{1}{6} & \frac{1}{3} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{6} & \frac{1}{6} & 0 & \frac{1}{6} & \frac{1}{6} & \frac{1}{3} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}. \quad (1)$$

In order to compute the k steps state transition matrix, the Chapman-Kolmogorov equation [36] can be used. The k steps state transition matrix can be derived as follows [34]:

$$P^{(k)} = \begin{cases} P, & \text{if } k = 1, \\ P \times P^{(k-1)}, & \text{if } k > 1. \end{cases} \quad (2)$$

Let t_s represent the subnet residence time of an MN and t_d denote the domain residence time of an MN, which are both independently and identically distributed random variables. Suppose that the density functions of t_s and t_d are $f_s(t)$ and $f_d(t)$, respectively. In this paper, we choose Gamma distribution for the subnet residence time and the domain residence time of the MN to analyze the total number of subnet handover and domain handover and also compute the total signaling cost. The reason of the Gamma distribution is specified in [37]. The subnet residence time of the MN has

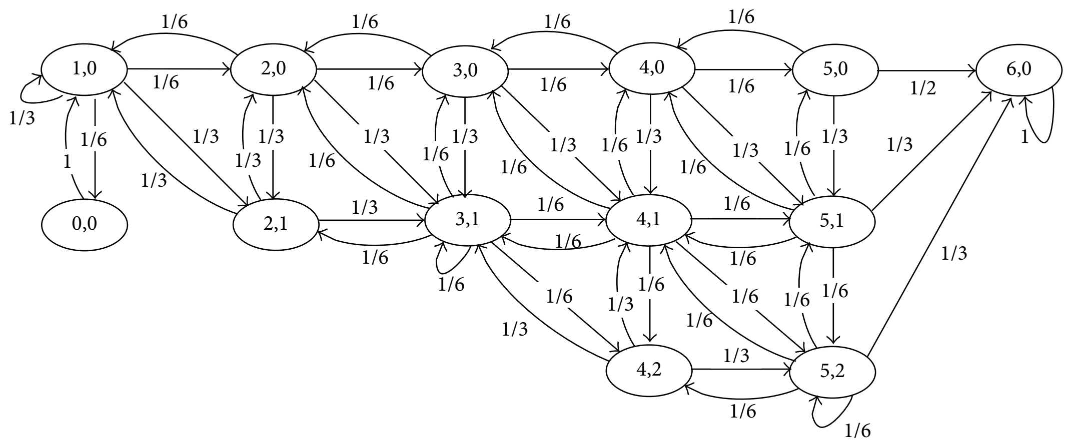


Figure 11: State transition diagram for six-layer random walk mobility model.

Gamma distribution with mean $E(t_s) = 1/\lambda_s$ and variance V, whose Laplace-Stieltjes transform is expressed as follows:

$$f_s^*(s) = \left(\frac{\lambda_s \gamma}{s + \lambda_s \gamma}\right)^{\gamma}, \quad \text{where } \gamma = \frac{1}{V\lambda_s^2}. \tag{3}$$

Besides, suppose that the expected value of a call hold time is $E(t_c) = 1/\lambda_c$. Therefore, the probability that an MN moves across M subnets in a call hold time can be calculated as follows [34]:

$$\alpha_s(M) = \begin{cases} 1 - \dfrac{1}{\rho}\left[1 - f_s^*(\lambda_c)\right], & M = 0 \\ \dfrac{1}{\rho}\left[1 - f_s^*(\lambda_c)\right]^2 \left[f_s^*(\lambda_c)\right]^{M-1}, & M > 0, \end{cases} \tag{4}$$

where $\rho = E(t_s)/E(t_c) = \lambda_c/\lambda_s$ is the call-to-mobility ratio (CMR).

Then, the average number of subnets that the MN traverses in a call hold time can be derived as

$$E(N_s) = \sum_{M=0}^{\infty} M\alpha_s(M). \tag{5}$$

Similarly, the probability that an MN moves across M domains in a call hold time is

$$\alpha_d(M) = \begin{cases} 1 - \dfrac{1}{\omega}\left[1 - f_d^*(\lambda_c)\right], & M = 0 \\ \dfrac{1}{\omega}\left[1 - f_d^*(\lambda_c)\right]^2 \left[f_d^*(\lambda_c)\right]^{M-1}, & M > 0, \end{cases} \tag{6}$$

where $\omega = E(t_d)/E(t_c)$, in which $E(t_d)$ can be obtained from the following equation [38]:

$$\begin{aligned} E[t_d] &= (-1)\frac{df_d^*(s)}{ds}\bigg|_{s=0} \\ &= -\sum_{k=1}^{\infty}\sum_{y=0}^{l}\sum_{j=0}^{l} q_{(n-1,y)} p_{k,(n-1,y)(n-1,j)(n,0)} \\ &\quad \cdot k\left[f_p^*(0)\right]^{k-1} \frac{df_s^*(s)}{ds}\bigg|_{s=0}, \end{aligned} \tag{7}$$

where $l = \lfloor (n-1)/2 \rfloor$, $f_d^*(s)$ is the Laplace transform of $f_d(t)$, $q_{(n-1,y)}$ denotes the probability that an MN moves into the domain through the $\langle n-1, y\rangle$ type subnet at the first step, and $p_{k,(n-1,y)(n-1,j)(n,0)}$ represents the probability that an MN resides at $\langle n-1, y\rangle$ type subnet initially, then moves to $\langle n-1, j\rangle$ type subnet through $k-1$ steps, and finally moves out of the domain at the kst step.

Thus, the average number of domains that an MN moves across in a call hold time can be derived as

$$E(N_d) = \sum_{M=0}^{\infty} M\alpha_d(M). \tag{8}$$

4.2. Signaling Cost Analysis. Signaling cost contains two major components which are the signaling cost related to the mobility management and the packet transmission [39]. In our analysis, we omit the signaling cost required for authentication and for L2 handoff, because they are the same for all protocols. Therefore, the total signaling cost consists of location update signaling cost and packet delivery cost. C_{location} and C_{packet} represent the location update cost and the packet delivery cost, respectively. Then, the total signaling cost can be expressed as follows:

$$C_{\text{total}} = C_{\text{location}} + C_{\text{packet}}. \tag{9}$$

4.2.1. Location Update Cost. Because an MN moves between different subnets either within a domain or out of a domain, two types of binding update will be performed, which are the intersubnet binding update and the interdomain binding update. We denote C_s and C_d as the signaling cost for the intersubnet binding update and the interdomain binding update, respectively. Based on the analytical mobility model specified above, the location update cost per unit time can be derived as follows:

$$C_{\text{location}} = \left[E(N_s) - E(N_d)\right] \cdot C_s + E(N_d) \cdot C_d. \tag{10}$$

The packet transmission cost in IP networks is proportional to the distance in hops between source and destination nodes [40]. Besides, the transmission cost in a wired link is generally lower than the transmission cost in a wireless link [41]. Let τ be the unit transmission cost over wired link and κ the weighting factor for the wireless link unit transmission cost. The signaling cost for the binding update includes the signaling transmission cost and the signaling processing cost at different entities. Besides, we also consider the route optimization (RO) case in the interdomain handover and suppose ω be the probability that an MN executes the RO process. Therefore, C_s and C_d can be derived from the following equations [15, 42]:

$$
\begin{aligned}
C_s^{\text{PMIP-BT}} &= \left(S_{\text{pbu}} + S_{\text{pba}}\right) \cdot \tau \cdot D_{\text{ml}} + \text{PC}_{\text{mag}} + \text{PC}_{\text{lma}}, \\
C_d^{\text{PMIP-BT}} &= (1-\omega) \\
&\quad \cdot \Big\{\left(S_{\text{pbu}} + S_{\text{pba}}\right) \cdot \tau \cdot D_{\text{ml}} + \text{PC}_{\text{mag}} + \text{PC}_{\text{lma}} \\
&\qquad + \left(S_{\text{bu}} + S_{\text{ba}}\right) \cdot \left[\kappa + \tau \cdot \left(D_{\text{ml}} + D_{\text{lh}}\right)\right] \\
&\qquad + \text{PC}_{\text{mn}} + \text{PC}_{\text{ha}}\Big\} + \omega \\
&\quad \cdot \Big\{\left(S_{\text{pbu}} + S_{\text{pba}}\right) \cdot \tau \cdot D_{\text{ml}} + \text{PC}_{\text{mag}} + \text{PC}_{\text{lma}} \\
&\qquad + \left(S_{\text{bu}} + S_{\text{ba}}\right) \cdot N_r \cdot \tau \cdot \left(D_{\text{ml}} + D_{\text{lr}}\right) \\
&\qquad + \left[\kappa + \tau \cdot \left(D_{\text{ml}} + D_{\text{lh}}\right)\right] + \left(N_r + 1\right) \\
&\qquad \cdot \text{PC}_{\text{mag}} + \text{PC}_{\text{lma}} + N_r \cdot \text{PC}_r + \text{PC}_{\text{mn}} + \text{PC}_{\text{ha}}\Big\}, \\
C_s^{\text{HMIP-BT}} &= \left(S_{\text{lbu}} + S_{\text{lba}}\right) \cdot \left(\kappa + \tau \cdot D_{\text{am}}\right) \\
&\quad + \text{PC}_{\text{mn}} + \text{PC}_{\text{map}}, \\
C_d^{\text{HMIP-BT}} &= (1-\omega) \\
&\quad \cdot \left\{\left(S_{\text{lbu}} + S_{\text{lba}}\right) \cdot \left(\kappa + \tau \cdot D_{\text{am}}\right) + \text{PC}_{\text{mn}}\right. \\
&\qquad + \text{PC}_{\text{map}} + \left(S_{\text{bu}} + S_{\text{ba}}\right) \\
&\qquad \left.\cdot \left[\kappa + \tau \cdot \left(D_{\text{am}} + D_{\text{mh}}\right)\right] + \text{PC}_{\text{mn}} + \text{PC}_{\text{ha}}\right\} \\
&\quad + \omega \cdot \Big\{\left(S_{\text{lbu}} + S_{\text{lba}}\right) \cdot \left(\kappa + \tau \cdot D_{\text{am}}\right) + \text{PC}_{\text{mn}} \\
&\qquad\quad + \text{PC}_{\text{map}} + \left(S_{\text{bu}} + S_{\text{ba}}\right) \cdot N_r \\
&\qquad\quad \cdot \left[\kappa + \tau \cdot \left(D_{\text{am}} + D_{\text{mr}}\right)\right] \\
&\qquad\quad + \left[\kappa + \tau \cdot \left(D_{\text{am}} + D_{\text{mh}}\right)\right] + \left(N_r + 2\right) \\
&\qquad\quad \cdot \text{PC}_{\text{mn}} + \text{PC}_{\text{map}} + N_r \cdot \text{PC}_r + \text{PC}_{\text{ha}}\Big\},
\end{aligned}
\tag{11}
$$

where S_{pbu}, S_{pba}, S_{bu}, S_{ba}, S_{lbu}, and S_{lba} are the size of the signaling messages for the location update in PMIPv6 and MIPv6, respectively. D_{ml} is the hop distance between the MAG and the LMA, D_{am} is the hop distance between the AR and the MAP, D_{lh} is the distance between the LMA and the home agent (HA), D_{mh} is the distance between the MAP and the HA, D_{lr} is the distance between the LMA and the receiver, and D_{mr} is the distance between the MAP and the receiver. N_r is the number of the receivers communicating with the MN. PC_{mag}, PC_{lma}, PC_{ha}, PC_{mn}, and PC_r are the processing costs for binding update procedure at the MAG, the LMA, the HA, the MN, and the receiver, respectively.

Since the PMIP-BT and the PMIP-DR are all based on the PMIPv6 mobility protocol, the location update cost for the PMIP-BT is equal to that for the PMIP-DR; that is,

$$C_{\text{location}}^{\text{PMIP-BT}} = C_{\text{location}}^{\text{PMIP-DR}}. \tag{12}$$

Similarly, the HMIP-BT and the HMIP-RS have an equal location update cost, which is as follows:

$$C_{\text{location}}^{\text{HMIP-BT}} = C_{\text{location}}^{\text{HMIP-RS}}. \tag{13}$$

4.2.2. Packet Delivery Cost. The cost for packet delivery procedure can be derived as follows [41, 42]:

$$C_{\text{packet}} = T_{S\text{-}R} + P_{\text{mag}} + P_{\text{lma}}, \tag{14}$$

where $T_{S\text{-}R}$ denotes the transmission cost of packet delivery from the mobile multicast sender to the receiver and P_{mag} and P_{lma} represent the processing cost of packet delivery at the MAG and the LMA, respectively.

The multicast packets are transmitted through the bidirectional tunnel firstly and then to the receiver based on the multicast tree in the PMIP-BT and HMIP-BT schemes, while they are delivered from the MAG/AR directly to the receiver according to the corresponding multicast states in the PMIP-DR and HMIP-RS schemes. Besides, in the PMIP-BT and HMIP-BT schemes, suppose that only the first packet of a session transits to the HA in order to detect whether or not an MN moves into foreign networks as assumed in [42], and all the successive packets are directly routed to the receiver through the MAP/LMA. Thus, the transmission cost of packet delivery from the mobile multicast sender to the receiver can be calculated as follows:

$$
\begin{aligned}
T_{S\text{-}R}^{\text{PMIP-BT}} &= \lambda_m \cdot S_p \cdot \left(1 + \frac{S_h}{S_p}\right) \\
&\quad \cdot \Big\{\omega \cdot \Big[\left(\overline{S} - 1\right) \cdot \tau \cdot \left(D_{\text{ml}} + D_{\text{lr}}\right) + \tau \\
&\qquad \cdot \left(2D_{\text{ml}} + D_{\text{lh}} + D_{\text{hr}}\right)\Big] \\
&\qquad + (1-\omega) \cdot \overline{S} \cdot \tau \cdot \left(2D_{\text{ml}} + D_{\text{lh}}\right)\Big\} \\
&\quad + \lambda_m \cdot S_p \cdot \omega \cdot \overline{S} \cdot \kappa + \lambda_m \cdot S_p \cdot (1-\omega) \\
&\quad \cdot \overline{S} \cdot \left(\kappa + \tau \cdot D_{\text{hr}}\right), \\
T_{S\text{-}R}^{\text{PMIP-DR}} &= \lambda_m \cdot \overline{S} \cdot S_p \cdot \left(\kappa + \tau \cdot D_{\text{mr}}\right),
\end{aligned}
$$

$$T_{S\text{-}R}^{\text{HMIP-BT}} = \lambda_m \cdot S_p \cdot \left(1 + \frac{S_h}{S_p}\right) \cdot \{\omega \cdot [(\overline{S} - 1) \cdot (\kappa + \tau \cdot (D_{\text{am}} + D_{\text{mr}})) + (2\kappa + \tau \cdot (2D_{\text{am}} + D_{\text{mh}} + D_{\text{hr}}))] + (1 - \omega) \cdot \overline{S} \cdot [2\kappa + \tau \cdot (2D_{\text{am}} + D_{\text{mh}})]\} + \lambda_m \cdot S_p \cdot (1 - \omega) \cdot \overline{S} \cdot \tau \cdot D_{\text{hr}},$$
$$T_{S\text{-}R}^{\text{HMIP-RS}} = \lambda_m \cdot \overline{S} \cdot S_p \cdot (\kappa + \tau \cdot D_{\text{ar}}), \quad (15)$$

where λ_m denotes the multicast session arrival rate, $\overline{S}$ is the average session size in the unit of packet, S_p is the multicast packet size, S_h denotes the size of the extra header for the packet encapsulation, and D_{ar}, D_{hr} represent the distance of the shortest path from the AR, the HA to the receiver, respectively.

The processing cost of packet delivery includes the mapping table lookup cost (C_{lookup}) and the routing cost (C_{routing}) [41, 42]. Therefore, the processing cost for the PMIP-BT scheme can be calculated as follows [15, 41, 42]:

$$P_{\text{mag}}^{\text{PMIP-BT}} = \lambda_m \cdot \overline{S} \cdot (C_{\text{lookup}} + C_{\text{routing}}) = \lambda_m \cdot \overline{S} \cdot (\alpha N_{\text{mn}} + \beta \log(L_{\text{mag}})),$$
$$P_{\text{lma}}^{\text{PMIP-BT}} = \lambda_m \cdot \overline{S} \cdot C_{\text{routing}} = \lambda_m \cdot \overline{S} \cdot \beta \log(L_{\text{lma}}), \quad (16)$$

where N_{mn} is the average number of MNs located in the coverage of an MAG subnet, α and β are the weighting factors of the mapping table lookup and the routing table lookup, respectively. L_{mag} and L_{lma} are the length of the routing table at the MAG and the LMA, respectively.

In the PMIP-DR scheme, the MAG directly forwards the multicast packets to the multicast domain. Therefore, there is processing cost only at the MAG and the MAG has no mapping table lookup cost. Thus, the processing cost at the MAG in the PMIP-DR scheme can be derived as follows:

$$P_{\text{mag}}^{\text{PMIP-DR}} = \lambda_m \cdot \overline{S} \cdot C_{\text{routing}} = \lambda_m \cdot \overline{S} \cdot \beta \log(L_{\text{mag}}). \quad (17)$$

Similarly, we can get the the processing cost for the HMIP-BT and HMIP-RS scheme, which will not be described here.

4.3. Numerical Results. This subsection presents various analysis results based on the above analytical mobility model. Table 2 shows the parameter values for the analysis, which are referenced from [15, 41, 42].

4.3.1. Location Update Cost versus Average Cell Residence Time. Figure 12 illustrates the impact of average cell residence time on location update cost. As shown in Figure 12, all the location update costs decline with the increased average cell residence time and the costs of PMIP-BT/PMIP-DR are lower than HMIP-BT/HMIP-RS. As the longer time an MN resides in a subnet, the lower frequencies the MN hands over. Besides, HMIPv6 is a host-based mobility management protocol, while PMIPv6 is a network-based mobility scheme and thereby when the MN performs handover, the MN does not need to participate in the location update procedures in PMIPv6 networks. In addition, from Figure 12, we can see that the location update cost with a higher probability of RO is higher. The reason is that the increased signaling cost is induced due to the increased binding update process between the MN and the receiver.

TABLE 2: Performance analysis parameters.

Parameter	Value	Parameter	Value
κ	2	τ	1
α	0.1	β	0.2
S_{pbu}	64 bytes	S_{pba}	64 bytes
$S_{\text{bu}}/S_{\text{lbu}}$	64 bytes	$S_{\text{ba}}/S_{\text{lba}}$	64 bytes
PC_{lma}	12	PC_{mag}	12
PC_{mn}	12	PC_r	6
PC_{ha}	24	PC_{map}	12
$D_{\text{ml}}/D_{\text{am}}$	2 hops	$D_{\text{lh}}/D_{\text{mh}}$	6 hops
$D_{\text{ar}}/D_{\text{mr}}$	8 hops	$D_{\text{lr}}/D_{\text{mr}}$	8 hops
D_{hr}	6 hops	$D_{\text{mh}}/D_{\text{ah}}$	7 hops
N_r	2	S_h	40 bytes
$\overline{S}$	10	S_p	1500 bytes
λ_m	0.1	λ_c	1/300

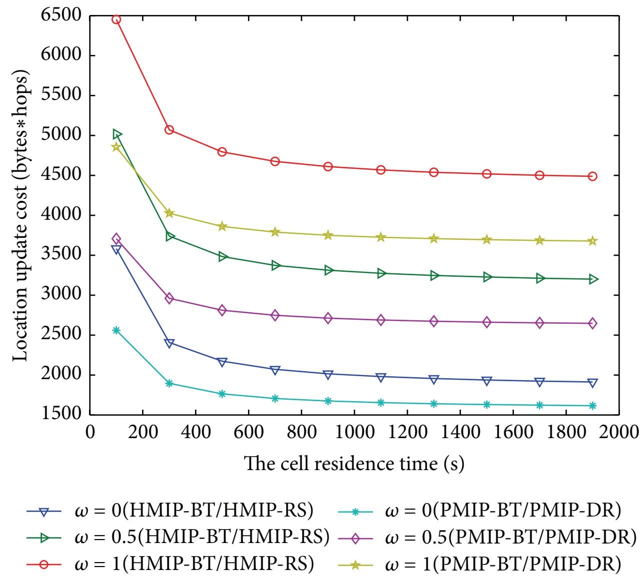


FIGURE 12: Impact of average cell residence time (t_s) on location update cost.

4.3.2. Location Update Cost versus Call-to-Mobility Ratio (CMR). Figure 13 presents the location update cost with the

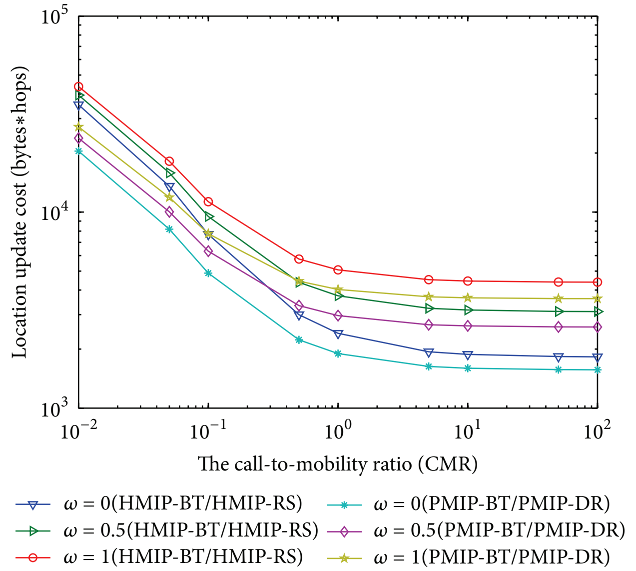


FIGURE 13: Impact of call-to-mobility ratio (CMR) on location update cost.

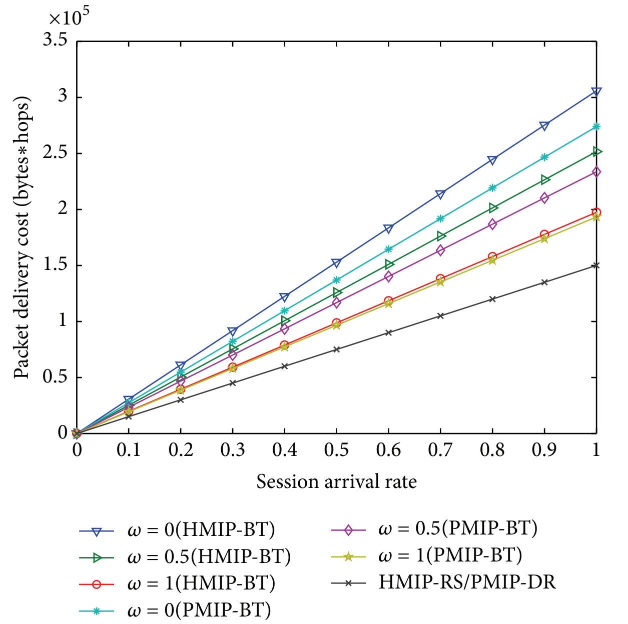


FIGURE 14: Impact of multicast session arrival rate (λ_m) on packet delivery cost.

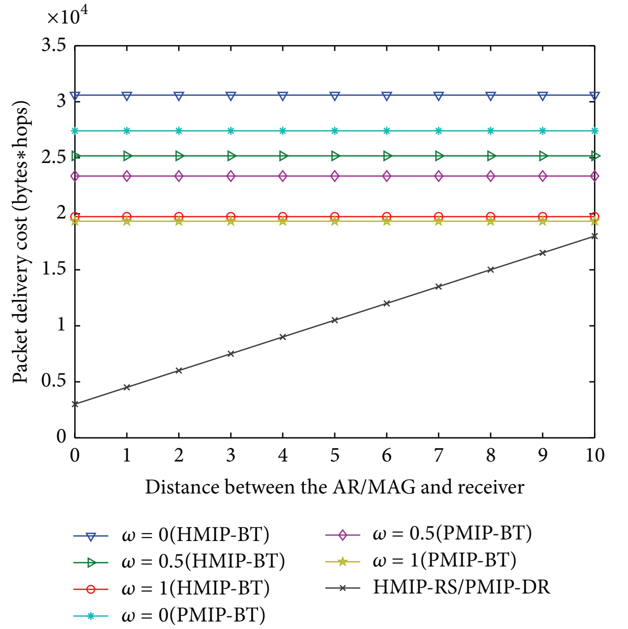


FIGURE 15: Impact of hop distance between the AR/MAG and receiver (D_{ar}/D_{mr}) on packet delivery cost.

impact of call-to-mobility ratio (CMR) for intra-PMIPv6/MAP domain roaming. From Figure 13, we can get that with the increase of the CMR, all the location update costs are decreased and the PMIP-BT/PMIP-DR has a lower location update cost than HMIP-BT/HMIP-RS. Since when CMR is small, the session arrival rate is smaller than mobility rate and then an MN will perform handoffs between different subnets frequently due to its mobility, which indicates that the location update cost increases. However, when the mobility rate is lower than the session arrival rate (i.e., CMR is greater than 1), the binding update will be less often performed and the location update cost will decline due to the fact that the frequency of subnet changes decreases. Besides, Figure 13 indicates that when the probability of RO is smaller, the location update cost is lower.

4.3.3. Packet Delivery Cost versus Multicast Session Arrival Rate. Figure 14 shows the packet delivery cost as a function of the multicast session arrival rate. In Figure 14, with the increased multicast session arrival rate, all the packet delivery costs increase; that is because in this case more packets should be transmitted. Meanwhile, the packet delivery cost of PMIP-BT/PMIP-DR is lower than that of HMIP-BT/HMIP-RS, and HMIP-RS/PMIP-DR has the lowest packet delivery cost for its more optimized routing than HMIP-BT and PMIP-BT. In addition, the packet delivery cost with a higher probability of RO is lower. The reason is that a higher probability of RO indicates that more optimized path routes will be provided for these schemes.

4.3.4. Packet Delivery Cost versus Hop Distance between the AR/MAG and Receiver. Figure 15 compares the results of packet delivery cost under the hop distance between the AR/MAG and receiver. From Figure 15, we observe that all the results for the HMIP-BT and PMIP-BT keep unchanged and the packet delivery cost of the HMIP-RS/PMIP-DR increases with the increased hop distance between the AR/MAG and receiver. That is due to the fact that more optimized routing for the HMIP-RS and PMIP-DR will be brought by the shorter hop distance between the AR/MAG and receiver, and thereby less signaling cost will be required. Besides, HMIP-BT and PMIP-BT transmit multicast data via bidirectional tunnel, while HMIP-RS and PMIP-DR do not need the encapsulation overhead.

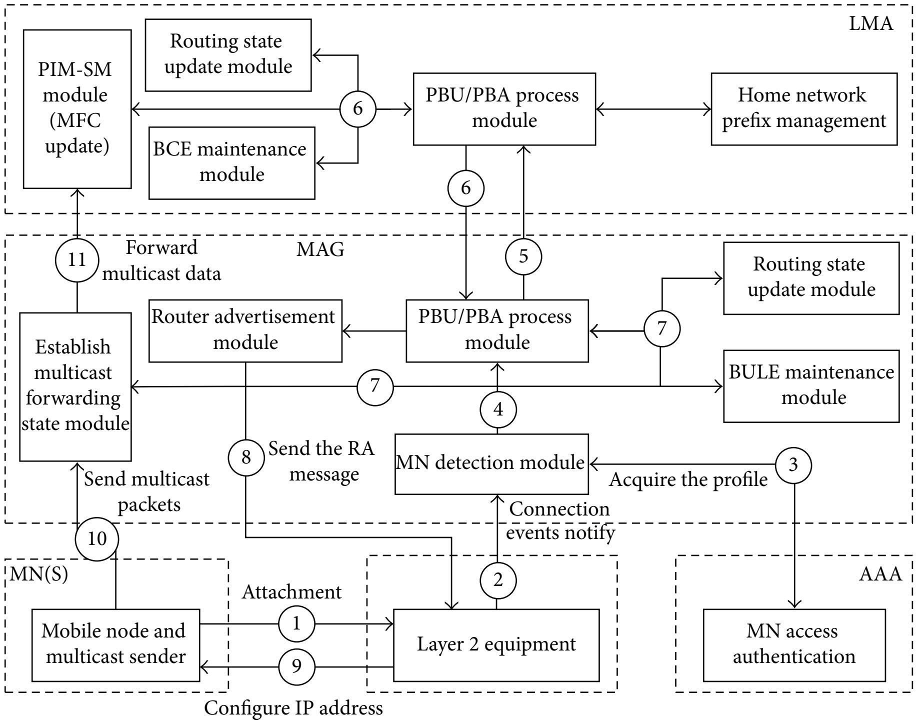


Figure 16: Implementation modules for PMIPv6 based mobile multicast sender support scheme.

5. Experimental System Development

In this section, we implement the proposed schemes and analyze the experimental evaluation results which mainly focus on the multicast handover latency.

5.1. Implementation Overview. Figure 16 illustrates the whole implementation framework for the proposed schemes, which mainly contains two parts: PMIPv6 and PIM-SM. In our implementation, PMIPv6 is based on the MIPL2.0 (MIPv6 for Linux) [43] and the detailed PMIPv6 module is shown in Figure 16.

The PMIPv6 implementation includes the LMA, the MAG, and the AAA. The modules in the MAG consist of modules MN detection, PBU/PBA process, routing state update, BULE maintenance and establish multicast forwarding state and router advertisement. The MN detection module monitors the MN attachment and detachment events through the link layer technologies (the syslog function is used in our implementation). The PBU/PBA process module generates and processes the mobility signaling messages including the (extended) PBU and PBA. The routing state update module sets up the tunneling routing between the LMA and the MAG. BULE maintenance module sets up and maintains the BU list in the MAG. Establishing multicast forwarding state module is extended to establish the multicast forwarding state for the multicast data originated from the MN. Router advertisement module emulates the home link by sending the home network prefix from the LMA. The modules in the LMA consist of the PBU/PBA process module similar to that of MAG, the routing state update module similar to that of MAG, BCE maintenance module, home network prefix management module, and PIM-SM module for PMIP-BT scheme. The BCE maintenance module records the BU in the LMA. The home network prefix management module allocates the IPv6 prefixes for the MNs belonging to the PMIPv6 domain. The PIM-SM module is used to update the MFC and this module is only needed in the PMIP-BT scheme. Besides, the AAA module is used to authenticate the MN, which is implemented in the MAG in our implementation.

PIM-SM routing protocol design is divided into two parts, which are kernel space and user space. The kernel space is responsible for the multicast packets forwarding. When the multicast router receives the multicast packets, it can forward those data according to the multicast routing information stored in the MFC. And the user space is in charge of establishing multicast route table (MRT) and updating the MFC in kernel. The PIM-SM system model is shown in Figure 17, where the functional modules of the user space include modules MRT, inner control message process, PIM and MLD protocol message process, timer, virtual interface, and kernel interface, while the kernel space includes PIM message process module, multicast packets process module, and support user space set socket option module. The user space modifies and updates the MRT based on the process results and also reflects the relevant changes to the kernel space via the system call.

Figure 16 also shows the detailed operation flow of PMIPv6 based mobile multicast sender support scheme, which will be described as follows. When a multicast sender MN attaches to the layer 2 equipment (Cisco 1200 AP) (1), the attachment event is firstly detected and then notified to

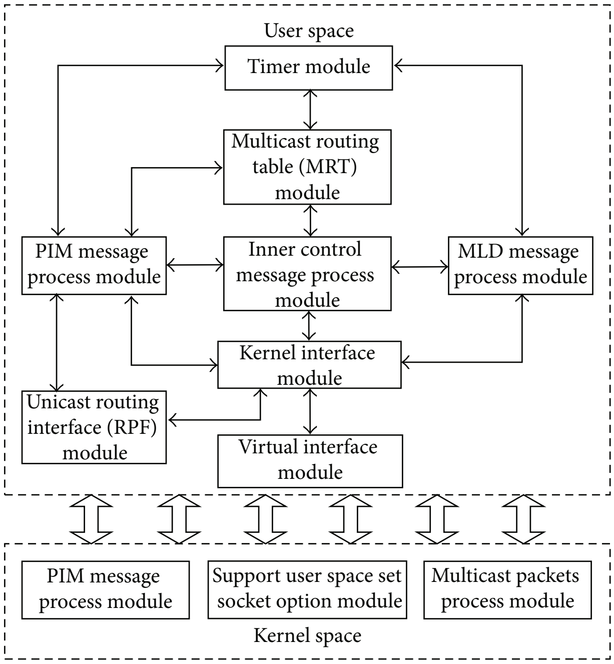


Figure 17: PIM-SM system module.

Table 3: Configuration parameters.

Parameter	Value
Audio bit rate	48 kb/s
Video bit rate	344 kb/s
Size of image	640 × 480
Sampling rate	44100 Hz
AP	Cisco Aironet 1200
MAG	NEL NGIID MA 2600/2601
LMA	NEL NGIID HA 2600/2601
DR/RP	NEL NGIID WR 2600/2601
ROUTER1/2	NEL NGIID A3600

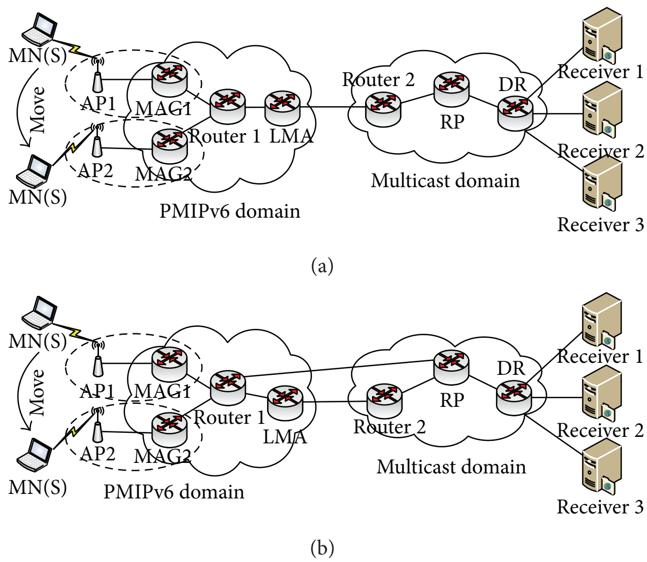
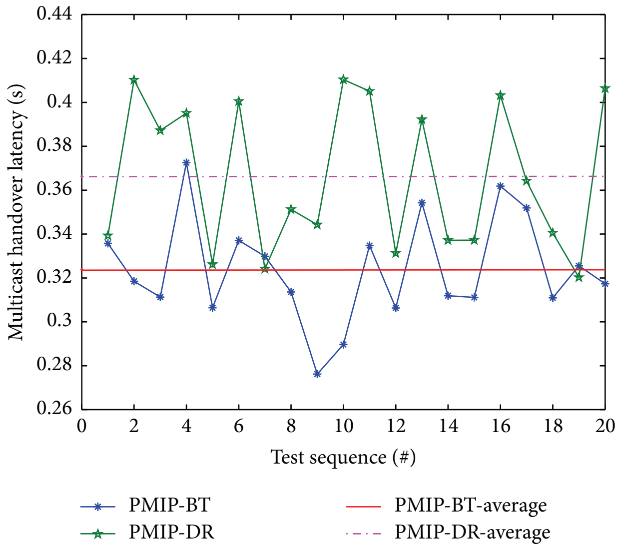


Figure 18: The experimental test-bed topology.

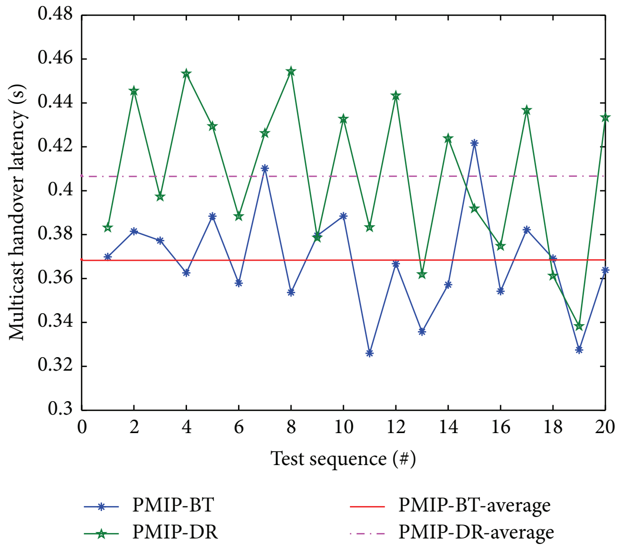
the MAG by the equipment (2). Thus, the layer 2 address of the MN is derived by the MAG from the notified message. Meanwhile, the MAG acquires the MN-identifier and policy profile from the policy server, in which the profile is stored in the local store for simplicity in our implementation (3). After the MAG gets the MN-identifier and AAA information, it sends the extended PBU message with both the "S" flag and the "D" flag set to value of 1 to the LMA (4). After receiving this extended PBU message from the MAG, the LMA not only updates the unicast routing states and the multicast forwarding states, but also maintains the binding caches (5). Then, the LMA judges whether the MAG could adopt the direct multicast routing scheme and indicate this to the MAG by the extended PBA message with the "D" flag (6). Just like the LMA, the MAG receiving the extended PBA message not only performs the PBU/PBA module to maintain the binding update lists and update the unicast routing states, but also establishes the multicast forwarding states for the MN (7). After that, the MAG advertises the HNP to the MN by sending the router advertisement (RA) message (8), and then the MN configures its address (9). Acting as a multicast sender, the MN begins to send multicast data to the MAG (10). Then the MAG forwards the multicast packets either to the LMA through the PMIPv6 bidirectional tunnel or directly to the multicast domain (11).

5.2. Experimental Setup. In order to analyze the two proposed schemes in detail, we set up two experimental test-bed topologies which are illustrated in Figure 18. The main difference between Figures 18(a) and 18(b) is the distance between the MAG/LMA and the multicast domain. In Figure 18, there are one multicast sender MN, two access points (AP), two MAGs, one LMA, one RP, one DR, two Routers, and three multicast receivers. The multicast sender MN provides multicast video services by running VLC (VideoLAN Client) media player. The MAG and the LMA run extended PMIPv6 protocol and PIM-SM protocol. Routing Information Protocol (RIP), RIP next generation (RIPng), and PIM-SM routing protocols are performed on all the other routers in the test-bed. Table 3 presents the experimental configuration parameters.

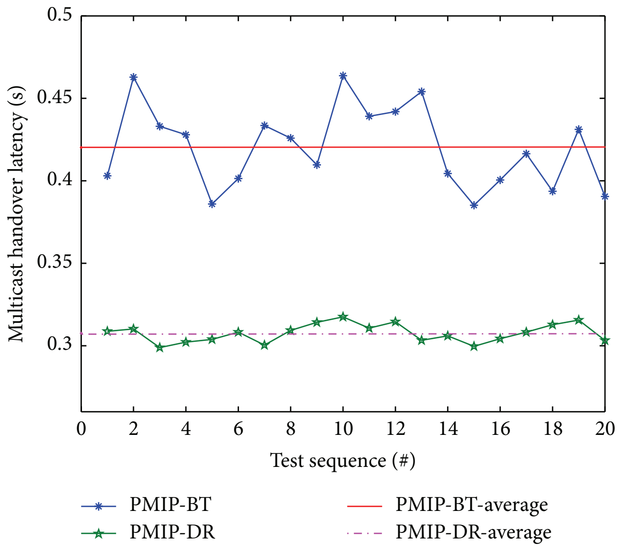
In order to evaluate the performance in different environments, we set up different test scenarios and perform three kinds of experiments. The first and the second experimental scenarios are both based on the topology in Figure 18(a), while the first scenario does not introduce any additional delay and the second scenario uses the WANem to introduce transmission delay and packet loss among the LMA and the RP in order to emulate the wide area networks. The third scenario uses the WANem to set up one case that the MAG is near to the multicast domain and the LMA is far away from the multicast domain, which is based on the topology in Figure 18(b) and is different from the former scenarios.



(a) Scenario 1



(b) Scenario 2



(c) Scenario 3

Figure 19: Multicast handover latency of the PMIP-BT and PMIP-DR schemes.

5.3. Experimental Results. We use the VLC media player to provide multicast data for a certain group and test the intra-PMIPv6 domain handover performance for both the PMIP-BT and the PMIP-DR schemes. Figure 19 presents the experimental results in terms of the multicast handover latency of the PMIP-BT and the PMIP-DR schemes for 20 times handovers.

Figures 19(a) and 19(b) display the multicast handover latency in Scenarios 1 and 2, respectively. In Figures 19(a) and 19(b), we can see that PMIP-BT has a lower latency than PMIP-DR. The reason is that the path route from the multicast sender to the receiver is the same for these two proposed schemes; that is, the data transmission of the PMIP-DR scheme must also pass through the LMA. In this case, the advantage of the optimized multicast routing for the PMIP-DR scheme is not represented and that of the unchanged DR for the PMIP-BT scheme is good at the improvement of the handover performance. Since the DR in the PMIP-DR scheme changes from the previous MAG to the new MAG whenever the multicast sender handovers, whereas the LMA acting as the DR keeps unchanged in the PMIP-BT scheme, thereby the multicast tree from the DR to the RP needs to be reconstructed for the PMIP-DR scheme but need not for the PMIP-BT scheme. Therefore, we can conclude that the PMIP-DR scheme is suitable for the lower multicast sender handover frequency scenarios, while the PMIP-BT scheme is suitable for the higher multicast sender handover frequency scenarios. Besides, we can see that the average multicast handover latency for both the PMIP-BT and PMIP-DR scheme in Scenario 1 is larger than that in Scenario 2, because Scenario 2 has more transmission delay than Scenario 1.

However, it can be seen from Figure 19(c) that PMIP-DR has a lower latency than PMIP-BT. That is due to the fact that the LMA is far away from the multicast domain and the MAG is near to the multicast domain in this scenario. Thus, the PMIP-DR scheme can transmit the multicast data through a direct multicast routing, which is a much more optimized path route than the PMIP-BT scheme. Based on the experimental results, we can get that the PMIP-DR scheme is suitable for the more optimized routing from the MAG/AR to the multicast domain scenarios, whereas the PMIPv6-BT scheme is suitable for the less optimized routing scenarios.

6. Conclusion

In this paper, PMIP-BT and PMIP-DR are proposed to support the multicast sender mobility in PMIPv6 networks efficiently. The PMIP-BT scheme inherits the transmission path of the unicast data in PMIPv6 domain, in which the multicast data must be transmitted through the PMIPv6 tunnel. However, the PMIP-DR scheme can provide a local optimized multicast routing, but the multicast tree needs to be reestablished whenever the multicast sender moves. Therefore, they are suited for the different application scenarios. We not only evaluate the proposed schemes' performance in terms of signaling cost by numerical analysis, but also analyze their performance of multicast handover latency via implementation and practical tests. The theoretical results and experimental results show that our proposed schemes are feasible and outperform the current schemes. Meanwhile, the evaluation experiments also indicate that the PMIP-BT scheme is suitable for the higher multicast sender handover frequency and less optimized routing from the MAG/AR to the multicast domain circumstances, while the PMIP-DR scheme is suitable for the lower multicast sender handover frequency and more optimized routing scenarios.

As part of future work, we plan to expand our current simple test-bed to a complex experimental scenario to further verify the feasibility and validity of our proposed schemes. Besides, we will set up the simulations to get a more comprehensive performance evaluation for the schemes proposed in this paper. Moreover, we will also study the combination of PMIP-BT and PMIP-DR under practical circumstances and continue to deeply study on this PMIPv6 based mobile multicast sender support issue to obtain a much more better handover performance.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work is supported by the National Basic Research Program of China (973 program) under Grant no. 2013CB329101, the National Key Technology R&D Program under Grant no. 2012BAH06B01, the National Natural Science Foundation of China (NSFC) under Grant no. 61271201, 61271202, 61003283, and Beijing Natural Science Foundation under Grant No. 4122060.

References

[1] P. Newman, "In search of the all-IP mobile network," *IEEE Communications Magazine*, vol. 42, no. 12, pp. 3–8, 2004.

[2] J. P. Wu, H. W. Li, W. Q. Sun, Q. Wu, Z. Jiang, and W. Zhao, "Technology trends and architecture research for future mobile internet," *China Communications*, vol. 10, no. 6, pp. 14–27, 2013.

[3] C. Q. Xu, T. J. Liu, J. F. Guan, H. K. Zhang, and G.-M. Muntean, "CMT-QA: quality-aware adaptive concurrent multipath data transfer in heterogeneous wireless networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 11, pp. 2193–2205, 2013.

[4] T. C. Schmidt, M. Waehlisch, and S. Krishnan, "Base deployment for multicast listener support in PMIPv6 domains," IETF RFC 6224, 2011.

[5] T. C. Schmidt, S. Gao, H. K. Zhang, and M. Waehlisch, "Mobile multicast sender support in proxy mobile IPv6 (PMIPv6) domains. IETF draft-ietf-multimob-pmipv6-source-09," IETF RFC 7287, 2014.

[6] M. Kellil, I. Romdhani, H.-Y. Lach, A. Bouabdallah, and H. Bettahar, "Multicast receiver and sender access control and its applicability to mobile IP environments: a survey," *IEEE Communications Surveys and Tutorials*, vol. 7, no. 2, pp. 46–70, 2005.

[7] T. C. Schmidt, M. Waehlisch, and G. Fairhurst, "Multicast mobility in mobile IP version 6 (MIPv6): problem statement and brief survey," IETF RFC 5757, Internet Research Task Force, 2010.

[8] C. Perkins, D. Johnson, and J. Arkko, "Mobility support in IPv6," IETF RFC 6275, 2011.

[9] S. Gundavelli, K. leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy mobile IPv6," IETF RFC 5213, 2008.

[10] K.-S. Kong, W. Lee, Y.-H. Han, M.-K. Shin, and H. You, "Mobility management for all-IP mobile networks: mobile IPv6 vs. proxy mobile IPv6," *IEEE Wireless Communications*, vol. 15, no. 2, pp. 36–45, 2008.

[11] 3GPP TS 23.402 v12.4.0, "Architecture Enhancements for non-3GPP accesses (Release 12)," 2014, http://www.3gpp.org/ftp/Specs/archive/23_series/23.402/23402-c40.zip.

[12] G. Xylomenos and G. C. Polyzos, "IP multicast for mobile hosts," *IEEE Communications Magazine*, vol. 35, no. 1, pp. 54–58, 1997.

[13] K. Sato, M. Katsumoto, and T. Miki, "Future vision distribution system and network," in *Proceedings of the IEEE International Symposium on Communications and Information Technology (ISCIT '04)*, vol. 1, pp. 274–279, October 2004.

[14] C. Q. Xu, F. T. Zhao, J. F. Guan, H. K. Zhang, and G.-M. Muntean, "QoE-driven user-centric vod services in urban multihomed P2P-based vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2273–2289, 2013.

[15] L. Wang, S. Gao, H. Zhang, T. C. Schmidt, and J. Guan, "Mobile multicast source support in PMIPv6 networks," *Eurasip Journal on Wireless Communications and Networking*, vol. 2013, no. 1, article 152, 2013.

[16] B. Fenner, H. He, B. Haberman, and H. Sandick, "Internet group management protocol (IGMP)/multicast listener discovery

(MLD)- based multicast forwarding ('IGMP/MLD Proxying')," IETF RFC 4605, 2006.

[17] C. Perkins, "IP mobility support for IPv4," IETF RFC 3344, 2002.

[18] H. Gossain, S. Kamat, and D. P. Agrawal, "A framework for handling multicast source movement over mobile IP," in *Proceedings of the International Conference on Communications (ICC '02)*, pp. 3398–3402, May 2002.

[19] C. S. Jelger and T. Noel, "Supporting mobile SSM sources for IPv6," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '02)*, pp. 1693–1697, November 2002.

[20] T. C. Schmidt and M. Wählisch, "Morphing distribution trees-on the evolution of multicast states under mobility and an adaptive routing scheme for mobile SSM sources," *Telecommunication Systems*, vol. 33, no. 1–3, pp. 131–154, 2006.

[21] H. Lee, S. Han, and J. P. Hong, "Efficient mechanism for source mobility in source specific multicast," in *Information Networking. Advances in Data Communications and Wireless Networks: Proceedings of the International Conference, ICOIN 2006, Sendai, Japan, January 16–19, 2006*, vol. 3961 of *Lecture Notes in Computer Science*, pp. 82–91, Springer, Berlin, Germany, 2006.

[22] B. Park and C. Lim, "An efficient source mobility-based multicast scheme for mobile hosts in mobile-IPv6 networks," in *Proceedings of the 1st International Symposium on Wireless Pervasive Computing*, IEEE, New York, NY, USA, January 2006.

[23] J. Guan, H. Zhou, C. Xu, H. Zhang, and H. Luo, "The performance analysis of the multicast extension support for proxy MIPv6," *Wireless Personal Communications*, vol. 61, no. 4, pp. 657–677, 2011.

[24] V. Chikarmane, C. L. Williamson, R. B. Bunt, and W. L. Mackrell, "Multicast support for mobile hosts using mobile IP: design issues and proposed architecture," *Mobile Networks and Applications*, vol. 3, no. 4, pp. 365–379, 1998.

[25] J.-R. Lai and W. Liao, "Mobile multicast with routing optimization for recipient mobility," *IEEE Transactions on Consumer Electronics*, vol. 47, no. 1, pp. 199–206, 2001.

[26] T. G. Harrison, C. L. Williamson, W. L. Mackrell, and R. B. Bunt, "Mobile multicast (MoM) protocol: multicast support for mobile hosts," in *Proceedings of the 3rd Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'97)*, pp. 151–160, September 1997.

[27] C. R. Lin and K.-M. Wang, "Scalable multicast protocol in IP-based mobile networks," *Wireless Networks*, vol. 8, no. 1, pp. 27–36, 2002.

[28] D. Von Hugo, H. Asaeda, B. Sarikaya, and P. Seite, "Evaluation of Further Issues on Multicast Mobility: Potential Future Work for WG MultiMob," IETF draft-von-hugo-multimob-future-work-02, 2010.

[29] R. Vida and L. Costa, "Multicast listener discovery version 2 (MLDv2) for IPv6," IETF RFC 3810, 2004.

[30] J. Kempf, "Goals for network-based localized mobility management (NETLMM)," IETF RFC 4831, 2007.

[31] B. Fenner, M. Handley, H. Holbrook, and I. Kouvelas, "Protocol independent multicast—sparse mode (PIM-SM): protocol specification (Revised)," IETF RFC 4601, 2006.

[32] M. Handley, I. Kouvelas, T. Speakman, and L. Vicisano, "Bidirectional protocol independent multicast (BIDIR-PIM)," IETF RFC 5015, 2007.

[33] A. S. Reaz, P. K. Chowdhury, M. Atiquzzaman, and W. Ivancic, "Signalling cost analysis of SINEMO: seamless end-to-end network mobility," in *Proceedings of the 1st ACM/IEEE International Workshop on Mobility in the Evolving Internet Architecture (MobiArch '06)*, San Francisco, Calif, USA, December 2006.

[34] I. F. Akyildiz, Y. B. Lin, W. R. Lai, and R. J. Chen, "New random walk model for PCS networks," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 7, pp. 1254–1260, 2000.

[35] G. Xue, "An improved random walk model for PCS networks," *IEEE Transactions on Communications*, vol. 50, no. 8, pp. 1224–1226, 2002.

[36] S. M. Ross, *Stochastic Processes*, Wiley Series in Probability and Mathematical Statistics: Probability and Mathematical Statistics, John Wiley & Sons, New York, NY, USA, 1983.

[37] Y. B. Lin, "Reducing location update cost in a PCS network," *IEEE/ACM Transactions on Networking*, vol. 5, no. 1, pp. 25–33, 1997.

[38] H. Zhang and H. K. Zhang, "Multicast fast handover algorithm based on neighbor information exchange," *Journal of Software*, vol. 19, no. 10, pp. 2648–2658, 2008.

[39] Y. Fang, "Movement-based mobility management and trade off analysis for wireless mobile networks," *IEEE Transactions on Computers*, vol. 52, no. 6, pp. 791–803, 2003.

[40] C. Makaya and S. Pierre, "An analytical framework for performance evaluation of IPv6-based mobility management protocols," *IEEE Transactions on Wireless Communications*, vol. 7, no. 3, pp. 972–983, 2008.

[41] J. Xie and I. F. Akyildiz, "A novel distributed dynamic location management scheme for minimizing signaling costs in mobile IP," *IEEE Transactions on Mobile Computing*, vol. 1, no. 3, pp. 163–175, 2002.

[42] S. Pack and Y. Choi, "A study on performance of hierarchical mobile IPv6 in Ip-based cellular networks," *IEICE Transactions on Communications E*, vol. 87, no. 3, pp. 462–469, 2004.

[43] Helsinki University of Technology, "MIPL-Mobile IPv6 for Linux," http://mobile-ipv6.org.

Hindawi Publishing Corporation
Mobile Information Systems
Volume 2015, Article ID 868346, 10 pages
http://dx.doi.org/10.1155/2015/868346

Research Article

A Study on the Distributed Antenna Based Heterogeneous Cognitive Wireless Network Synchronous MAC Protocol

Lian-Fen Huang,[1] Sha-Li Zhou,[1] Yi-Feng Zhao,[1] and Han-Chieh Chao[2,3]

[1] *Department of Communication Engineering, Xiamen University, Xiamen, Fujian 361005, China*
[2] *Institute of Computer Science & Information Engineering and Department of Electronic Engineering, National Ilan University, I-Lan, Taiwan*
[3] *Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan*

Correspondence should be addressed to Yi-Feng Zhao; zhaoyf@xmu.edu.cn

Received 1 September 2014; Accepted 1 September 2014

Academic Editor: Ilsun You

This paper introduces distributed antennas into a cognitive radio network and presents a heterogeneous network. The best contribution of this paper is that it designs a synchronous cognitive MAC protocol (DAHCWNS-MAC protocol: distributed antenna based heterogeneous cognitive wireless network synchronous MAC protocol). The novel protocol aims at combining the advantages of cognitive radio and distributed antennas to fully utilize the licensed spectrum, broaden the communication range, and improve throughput. This paper carries out the mathematical modeling and performance simulation to demonstrate its superiority in improving the network throughput at the cost of increasing antenna hardware costs.

1. Introduction

DAS (distributed antenna system) is used as an extension of the outdoor cellular mobile system in early stage, which is widely used for indoor or blind spot coverage. However the research of MIMO (multiple input multiple output) technology has become more and more sophisticated, which provides a broader space for the further development of DAS. This network structure can improve the wireless signal covering ability and system capacity and obtain high power efficiency. Because of these advantages, the DAS has been considered to be a key way of multiple antennas accessing in future mobile communication. Most current researches on the distributed antenna are focused on how distributed antennas can be used in the cellular mobile network physical layer to improve network capacity. Introducing DAS into WLAN (wireless local area network) can fully utilize its physical advantages to greatly improve the performance of WLAN, which is an attractive research area in the future. However there is scant literature on how distributed antenna can be used in WLANs. Reference [1] thinks that the fixed channel allocation method is not flexible and fair enough for multicell WLAN. New systems replace APs (access points) with distributed antennas using a control center. The control center dynamically adjusts the channel assignment scheme according to a judgment standard determined by the throughput, fairness, and other factors. Reference [2] designs the control center internal structure used in the distributed antenna WLAN system. The author thinks that each channel needs a corresponding processing unit. The more nodes the antenna services, the more channels it needs. The antenna therefore allocated more processing units.

This paper studies distributed antenna applications in the MAC (media access control) layer and designs a distributed antenna-based synchronous MAC protocol to sense the spectrum and transmit data.

Numerous literatures have studied spectrum sensing, producing some novel algorithms. References [3, 4] proposed a multitaper method (MTM) to detect the spectrum, with the advantages of low complexity and high detection accuracy. References [5, 6] proposed a detection method based on the signal covariance matrix. The ratio of two statistics is used to judge if the primary user appears. References [7, 8] studied the generalized likelihood ratio test method. To eliminate the influence of noise uncertainty, it first uses the maximum likelihood algorithm to estimate the unknown noise power and then completes the detection algorithm.

In addition to spectrum sensing we can further use distributed antennas to locate the primary user and adopt different access methods according to positioning information. Reference [9] studied the power allocation problem under overlay/underlay hybrid access mechanism. Reference [10] introduced the distributed antenna into the cognitive radio network. It utilizes the distributed antenna to sense the spectrum and locate the primary user. The author designed an asynchronous cognitive MAAC-MAC protocol (multi-antenna asynchronous cognitive MAC).

This paper focuses on how the distributed antenna can be used in data transmission and does not explore its usage in spectrum sensing and positioning. In future studies we can continue this research in different directions.

In order to design an appropriate network architecture for DAS, this paper studies the hybrid wireless networks. Many documents have studied hybrid wireless networks [11–14]. Adding AP/BSs (access point/base stations) into an ad hoc network can combine the network advantages with ad hoc infrastructure. Currently related literatures are focused on a cellular network and ad hoc network combination. In [15] the whole area is partitioned into many cells and all cells use the TDMA (time division multiple access) scheme. The author proposes two hybrid routing strategies that combine direct transmission (ad hoc mode) and forwarding data through base stations (infrastructure mode). Reference [16] proposes a protocol to judge whether data needs to be forwarded or not in the hybrid network.

This paper introduces the distributed antenna into the cognitive radio network and designs a heterogeneous network consisting of an ad hoc network and a sparse network of distributed antennas. The new network utilizes the distributed antennas to sense the spectrum and transmit data. We design a synchronous cognitive MAC protocol (DAHCWNS-MAC protocol) that can improve the sensing performance and also broaden the communication range to increase the throughput compared to the original single-hop network.

2. Heterogeneous Network Model

2.1. Communication Scenario. The distributed antenna layout is shown in Figure 1. Distributed antennas are uniformly placed throughout the region. Seven antennas are used to cover the entire communication scenario. The seven antennas are connected to a control center via an optical fiber. Distributed antennas forward data only with the other complex processing work completed by the control center.

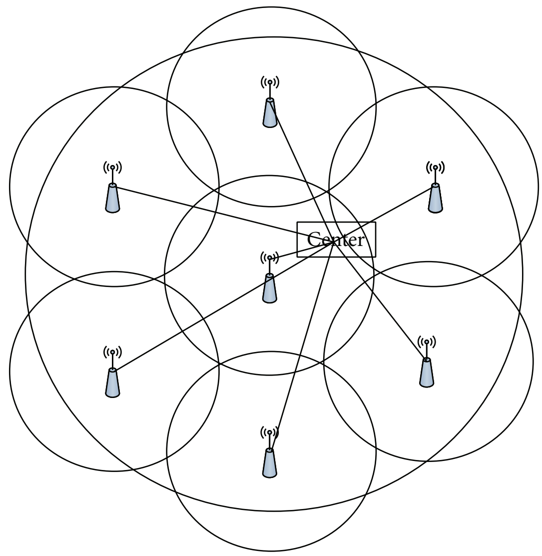


Figure 1: The layout of distributed antennas.

2.2. Network Architecture. In an 802.11DCF network with infrastructure all data is forwarded by the access point (AP). After adding distributed antennas the original AP coverage is divided into seven smaller cells, each of which is covered by an antenna. Within the coverage of each antenna the distance between nodes can be regarded as one hop and they can send data to each other directly. A node cannot communicate directly with its destination node when its destination node is not located in the same cell. In this case distributed antennas are used to forward data. We assume that nodes are uniformly placed in the region and each node accesses its nearest antenna. When a node and its destination node are located in the same antenna coverage they can send data directly. However, if a node and its destination node are not located in the same cell, they have to use distributed antennas to forward data. This is a heterogeneous network consisting of an ad hoc mode and infrastructure mode.

This heterogeneous network combines the advantages of two different networks. The network with infrastructure is easy to manage and does not have to exchange messages among nodes as in the ad hoc network. This reduces the extra overhead. It can also broaden the communication range through forwarding data by infrastructure. Under the ad hoc mode direct data transmission decreases the time consumed by forwarding, so the throughput can be improved.

The DAHCWNS-MAC protocol is designed for cognitive radio networks where nodes use idle licensed bands to communicate. The spectrum sensing is an important part of the protocol. What is different from the previous cognitive MAC protocols is that the DAHCWNS-MAC protocol uses distributed antennas instead of nodes to sense the spectrum. Results at all the antennas will be submitted to the control center for a final judgment result. The idle bands will be allocated to nodes by the control center. Nodes do not have to sense the spectrum by themselves as in the self-organized network, which reduces the exchanging sensing results overhead and decreases the node hardware requirements. Furthermore, the sensing performance is improved while utilizing the distributed antennas' macrodiversity.

We can utilize distributed antennas to locate primary users and adopt overlay/underlay hybrid access schemes through power control for more effective licensed band usage.

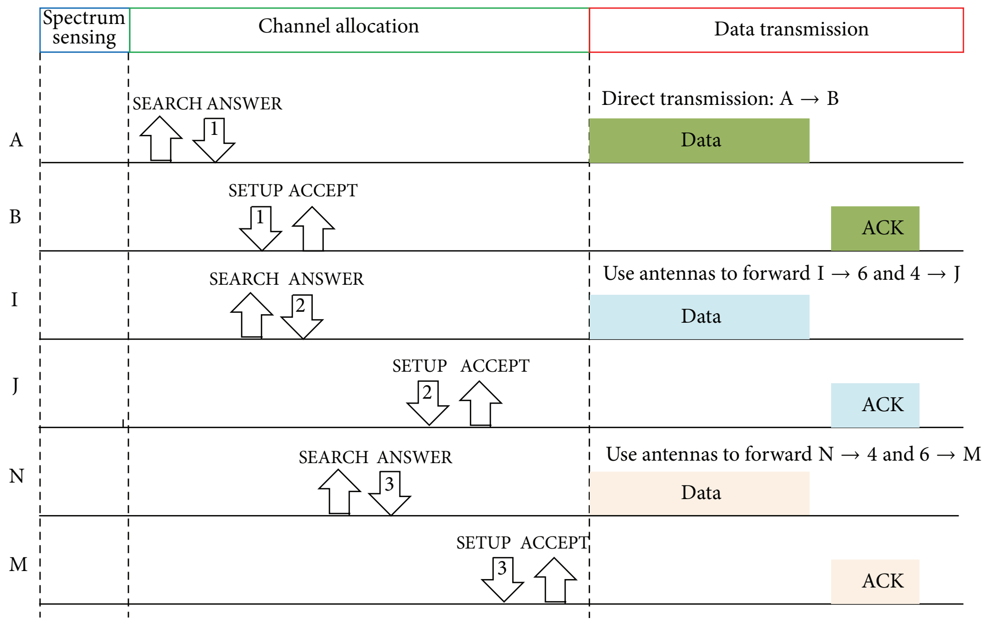


Figure 2: The time frame of DAHCWNS-MAC protocol.

Section 1 introduces some novel sensing algorithms and hybrid access schemes that are very useful in completing the DAHCWNS-MAC protocol in future research. Because this paper aims mainly at exploring how distributed antennas are used for data transmission, we no longer repeat the spectrum sensing and positioning parts of the protocol in the next article.

3. The Distributed Antenna Based Heterogeneous Cognitive Wireless Network Synchronous MAC Protocol (DAHCWNS-MAC Protocol)

In this section the DAHCWNS-MAC protocol will be described in detail.

3.1. Assumptions. Before presenting the specific protocol some necessary assumptions are summarized as follows.

(a) There are $N+1$ licensed channels for use, all of which have the same bandwidth. Since no overlap occurs among channels, packets transmitted on different channels will not affect each other. The control center knows how many licensed channels can be used in advance.

(b) One of $N+1$ licensed channels is used as the control channel. This can be the unlicensed band in practice and thus free from interference from the primary users.

(c) Each CU (cognitive user) is equipped with a single cognitive radio. This radio can either transmit or receive, but it cannot do both simultaneously.

(d) All antennas can forward data correctly. The control center has different processing units corresponding to different antennas, so it can parallel process data from different antennas. The control center also knows which nodes exist within the antenna coverage.

(e) All nodes are strictly synchronous. They always start and finish a beacon interval at the same time.

(f) Distributed antennas can sense the spectrum precisely to obtain all idle channels.

3.2. Protocol Design. The DAHCWNS-MAC protocol is a synchronous MAC protocol. The whole time can be divided into frames with fixed length. The time frame can be separated into three parts: sensing, channel allocation, and transmission phases. The DAHCWNS-MAC time frame is depicted in Figure 2.

(1) The first part of the DAHCWNS-MAC protocol is the sensing phase. Distributed antennas sense spectrum during this period. Each antenna detects N channels independently and submits its result to the control center. The control center will get final judgment result through data fusion and allocates idle channels to nodes to communicate in the next part of the protocol.

(2) The second part of the DAHCWNS-MAC protocol is the channel allocation phase. This phase is based on the CSMA/CA mechanism. All nodes contend with each other for the right to use channels. Since this network is a heterogeneous network it is necessary to determine whether nodes need distributed antennas to forward data. The specific process is as follows. Nodes that have data to transmit contend to send SEARCH frames to their nearest antenna on the control channel. If the competition succeeds, the corresponding antenna will submit the frame to the control center and then stores it. At the same time the control center

will reply with an ANSWER frame to the node which includes the number of allocated channels (randomly selected from the remaining channels until no idle channels remain). The above is the uplink part of this phase.

Upon receiving the SEARCH frame the control center will find the number of distributed antennas to which the destination node belongs and check if the sending and receiving nodes are located in the same antenna coverage area. If so, then in the next data transmission phase there is no need for distributed antennas to forward data. The sending and receiving nodes can communicate directly. If not, data packets are forwarded by distributed antennas. The control center records the result if a pair of nodes need data forwarding and in the next data transmission phase it can use the result to judge whether to forward data packets from this node. Next the control center checks if the antenna to which the receiving node belongs is idle. If the antenna is idle a SETUP frame will be sent to the receiving node immediately which contains the same channel number as the ANSWER frame. Otherwise, the SETUP frame will be sent until the antenna becomes idle. Upon the receiving node getting the SETUP frame it will reply with an ACCEPT frame, which means the handshake is completed. The above is the downlink part of the channel allocation phase.

Because the uplink and downlink capacity are unbalanced in networks with infrastructure, to ensure downlink transmission completion, the protocol does not use a competition scheme during the downlink, which means the nodes do not need to perform backoff. Specifically, there is no need for backoff before sending the SETUP frame.

The transceiver node pair completes any message exchange necessary for the data transmission phase through a four-way handshake. As shown in Figure 3 the four-way handshake includes two parts: the uplink part and downlink part.

The DAHCWNS-MAC protocol makes the collision domain narrow to the antenna coverage. Cells covered by different antennas are independent and do not affect each other. Each antenna can work in parallel with others, which means different antennas can be in different transmission/receiving stages at the same time.

All operations during this phase are carried out on the control channel. The control channel may also be used for data transmission.

(3) The third part of the DAHCWNS-MAC protocol is the data transmission phase. The transceiver node pair which completes the four-way handshake can send data on the channel allocated to them. If they need help from distributed antennas in forwarding data the corresponding antenna will forward their data automatically. Otherwise, they will communicate directly until this time frame ends. A transceiver node pair that does not complete the four-way handshake cannot enter the data transmission phase.

The time frame is divided into three parts. As illustrated there are three pairs of nodes communicating: A to B, I to J, and N to M. For example, A wants to communicate with B and it sends SEARCH frame to the center. Then the center replies with ANSWER frame which allocates channel 1 to A. At the same time the center sends SETUP frame to B to tell B that

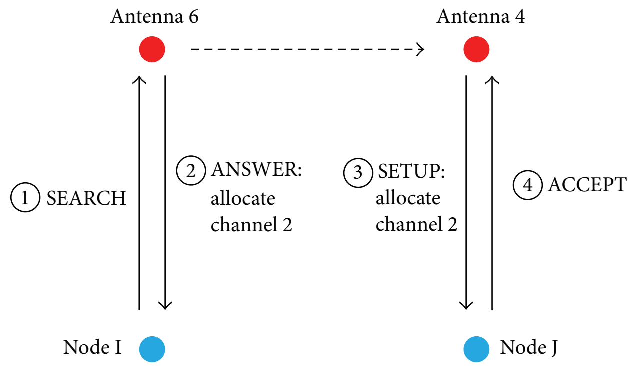


Figure 3: The four-way handshake.

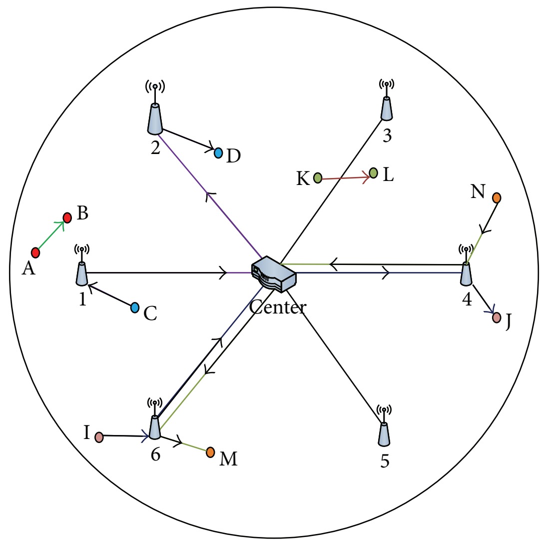


Figure 4: Transmission example.

the allocated channel is 1 and then B replies with ACCEPT frame to complete four-way handshake. Because nodes A and B are in one-hop distance, they can transmit directly in channel 1. I and J communicate on channel 2 through antenna forwarding. N and M communicate on channel 3 through antenna forwarding.

A specific transmission case is presented in Figure 4. For example, nodes A and B are located in antenna 1 coverage area. They can communicate directly because the control center allocated channel 1 to them. Nodes I and J are located in different antenna coverage areas, so they need antennas 4 and 6 to forward data with channel 2 assigned to them.

This figure uses the communication process between nodes I and J to explain how the four-way handshake works. The first step: node I sends SEARCH frame to antenna 6. The second step: the center replies with ANSWER frame which allocates channel 2 to I. The third step: at the same time antenna 4 sends SETUP frame to node J to tell J that the allocated channel is 2. The last step: node J replies with ACCEPT frame to complete four-way handshake.

3.3. The DAHCWNS-MAC Protocol Model. In this section a mathematical model for the DAHCWNS-MAC is presented to theoretically calculate its saturated throughput.

Since only transceiver nodes that complete a handshake can enter the data transmission phase, the key in calculating throughput is to calculate how many pairs of transceiver nodes complete the handshake during the channel allocation phase. The channel allocation phase is divided into uplink and downlink parts. How many times the downlink part is finished represents how many pairs of transceiver nodes complete the handshake. Therefore the objective is to calculate the downlink part throughput during the channel allocation phase.

Whether frames are sent in the downlink part depends on the uplink part. The SETUP frame is sent only when the SEARCH frame has been successfully received. Since seven distributed antennas operate independently, the uplink and downlink transmissions in different cells are independent of each other. Therefore, the average throughput for the seven cells should be the same. It is feasible to calculate the downlink throughput of one cell first and then multiply it by seven.

We assume that sending nodes always have data to transmit. Nodes contend to send frames in uplink and the transmission probability in each slot can be calculated using the two-dimension Markov chain model. Since there is no competition during downlink, the downlink transmission probability is equal to the probability of generating downlink data.

Several necessary variables are defined as follows. τ^{up} and τ^{down} represent the transmission probability in each slot of uplink and downlink, respectively. The average number of sending nodes in each cell is n.

In 802.11DCF network, the transmission probability in each slot can be calculated using the two-dimension Markov chain model according to [17]. The transmission probability of the uplink part should be the same. So

$$\tau^{\text{up}} = \frac{2(1-2p)}{(1-2p)(\text{CW}+1) + p\text{CW}\left[1-(2p)^{m}\right]}, \tag{1}$$

where CW is the size of the smallest contention window and m is the maximum backoff stage. The collision probability of uplink is

$$p = 1 - \left(1-\tau^{\text{up}}\right)^{n-1}\left(1-\tau^{\text{down}}\right). \tag{2}$$

There is no need in downlink for backoff before sending data. Frames are sent out as soon as the channel is idle. Therefore, the transmission probability of downlink is equal to the probability of generating downlink data. The probability depends on the uplink transmission success. Only when the uplink transmission succeeds, which means the SEARCH frame has been successfully stored in center cache, will the corresponding exit antenna have data to send. So the downlink transmission probability is assumed to be equal to the probability of successful uplink transmission:

$$\tau^{\text{down}} = p_s^{\text{up}} p_{\text{tr}}^{\text{up}} = n\tau^{\text{up}}\left(1-\tau^{\text{up}}\right)^{n-1}\left(1-\tau^{\text{down}}\right). \tag{3}$$

Combining (1), (2), and (3), the τ^{up} and τ^{down} can be solved.

According to [18] the probability that at least one uplink frame is in transmission at some slot is

$$p_{\text{tr}}^{\text{up}} = 1 - \left(1-\tau^{\text{up}}\right)^{n}. \tag{4}$$

Under the case that uplink frames exist which are in transmission, the probability that only one uplink frame is being transmitted is

$$p_s^{\text{up}} = \frac{n\tau^{\text{up}}\left(1-\tau^{\text{up}}\right)^{n-1}\left(1-\tau^{\text{down}}\right)}{1-\left(1-\tau^{\text{up}}\right)^{n}}. \tag{5}$$

Likewise, under the case that downlink frames exist which are in transmission, the probability that only one downlink frame is being transmitted is

$$p_s^{\text{down}} = \frac{\tau^{\text{down}}\left(1-\tau^{\text{up}}\right)^{n}}{\tau^{\text{down}}}. \tag{6}$$

Four possible states exist in one slot as follows.

(1) The channel is idle and the probability is $(1-p_{\text{tr}}^{\text{up}})(1-\tau^{\text{down}})$. The length of a slot is σ.

(2) The uplink frame is transmitted successfully and the probability is $p_s^{\text{up}}\tau^{\text{down}}$. The average transmission time is T_s^{up}.

(3) The downlink frame is transmitted successfully and the probability is $p_s^{\text{down}}\tau^{\text{down}}$. The average transmission time is T_s^{down}.

(4) When a collision happens the probability is $p_{\text{tr}}^{\text{up}}(1-p_s^{\text{up}}) + \tau^{\text{down}}(1-p_s^{\text{down}}) - p_{\text{tr}}^{\text{up}}\tau^{\text{down}}$. The average time is T_c.

The downlink throughput is

$$s = \frac{\tau_{\text{down}} P_s^{\text{down}} E^{\text{down}}}{\left(1-P_{\text{tr}}^{\text{up}}\right)\left(1-\tau_{\text{down}}\right)\sigma + P_{\text{tr}}^{\text{up}} P_s^{\text{up}} T_s^{\text{up}} + \tau_{\text{down}} P_s^{\text{down}} T_s^{\text{down}} + \left(P_{\text{tr}}^{\text{up}}\left(1-P_s^{\text{up}}\right) + \tau_{\text{down}}\left(1-P_s^{\text{down}}\right) - P_{\text{tr}}^{\text{up}}\tau_{\text{down}}\right) T_c}. \tag{7}$$

The denominator of the above formula is the average length of one slot where the downlink transmission occupies a proportion:

$$r = \left(\tau_{\text{down}} P_s^{\text{down}} T_s^{\text{down}}\right)$$

$$\times\left(\left(1-P_{\text{tr}}^{\text{up}}\right)\left(1-\tau_{\text{down}}\right)\sigma + P_{\text{tr}}^{\text{up}} P_s^{\text{up}} T_s^{\text{up}}\right.$$

$$+ \tau_{\text{down}} P_s^{\text{down}} T_s^{\text{down}}$$

$$+ \left(P_{\mathrm{tr}}^{\mathrm{up}}\left(1-P_{s}^{\mathrm{up}}\right)+\tau_{\mathrm{down}}\left(1-P_{s}^{\mathrm{down}}\right) - P_{\mathrm{tr}}^{\mathrm{up}}\tau_{\mathrm{down}}\right)T_{c}\Big)^{-1}. \tag{8}$$

So the total number of transceiver nodes that can complete a handshake during the channel allocation phase is

$$\mathrm{num} = 7 * \mathrm{CA\_window\_length} \times \frac{r}{T_{s}^{\mathrm{down}}}, \tag{9}$$

where CA_window_length is the length of the channel allocation phase.

The final saturation throughput is

$$s = \left(\frac{1}{7} \times \mathrm{num} \times \frac{\mathrm{data\_window\_length}}{T_{\mathrm{data}}} \times l \times 8 + \frac{6}{7} \times \mathrm{num} \times \frac{\mathrm{data\_window\_length}}{2 \times T_{\mathrm{data}}} \times l \times 8\right) \times (\mathrm{interval\_length})^{-1}, \tag{10}$$

where data_window_length is the length of the data transmission phase, T_{data} is the transmission time of a data packet, l is the real payload in a data packet, and interval_length is the length of a time frame.

As nodes are randomly placed, the probability that sending and receiving nodes are located in the same cell is $1/7$ at which time they can send data directly. However, the probability that sending and receiving nodes are located in a different cell is $6/7$ at which time distributed antennas should help in forwarding data. The time required for forwarding data is doubled compared to that of sending directly.

4. Performance Simulation and Analysis

In this section we present the DAHCWNS-MAC protocol simulation results. We assume a time frame is fixed at 100 ms and the state of licensed channels changing at the beginning of each time frame and remaining unchanged until the time frame ends up. The related parameters are shown in Table 1. This paper uses C language and MATLAB 7.0 as simulation tools. The simulation results come from C language programming and the theoretic results come from MATLAB programming.

4.1. The Comparison of Mathematical Model and Simulation Throughput. The channel allocation phase length is fixed to 10 ms and the number of idle channels is unlimited (all the transceiver nodes pairs which complete four-way handshake can be assigned a channel). A comparison between the mathematical model and simulation results is shown in Figure 5. We can see that the outcome for the two is quite close. This demonstrates the accuracy of the mathematical model. As the number of sending nodes increases, the throughput first increases and then decreases. This is because when the number of nodes increases the collision probability increases as well. The increasing collision probability results in a decreasing number of nodes that can complete a handshake and enter the transmission phase. Therefore, the throughput eventually decreases.

Table 1: The main simulation parameters.

Data channel rate	1 Mb/s
Control channel rate	1 Mb/s
Transmission delay	1 us
DIFS	50 us
SIFS	10 us
Slot time	50 us
Maximum backoff state (m)	4
Data packet length	512 bytes
Time frame length	100 ms
Simulation time	100 s

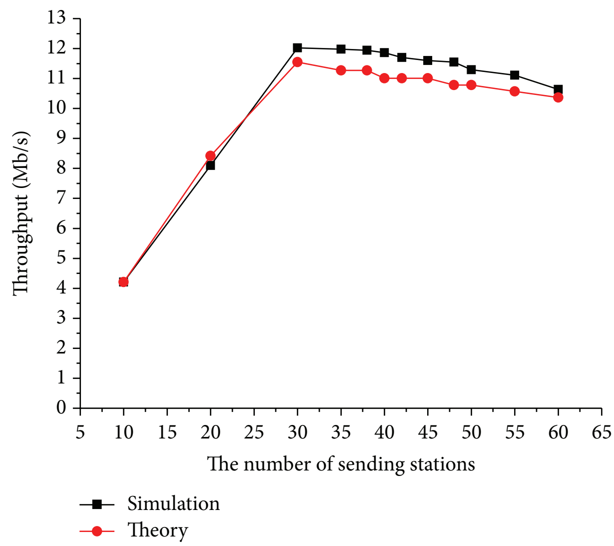


Figure 5: The saturation throughput of mathematical model and simulation.

4.2. The Relationship between Throughput and Channel Allocation Phase Length. Now let us analyze the channel allocation phase length effect on the saturation throughput. With 50 sending stations and 50 licensed channels, as shown in Figure 6, the saturation throughput increases as the time increases from 5 ms to 20 ms when the primary users' activity rate is 0. However, the saturation throughput decreases after 20 ms. This is because the number of nodes that complete a handshake is limited when the length is smaller than 20 ms. As the length becomes larger, the number of nodes that can complete a handshake to get a channel becomes larger, which results in an increase in the saturation throughput. However, the length of the time frame is fixed in the DAHCWNS-MAC protocol, which means the data transmission time will decrease when the channel allocation time increases. As the throughput reaches peak when the time is 20 ms because all transceiver nodes can get idle channels at this moment, increasing the channel allocation time results in the data

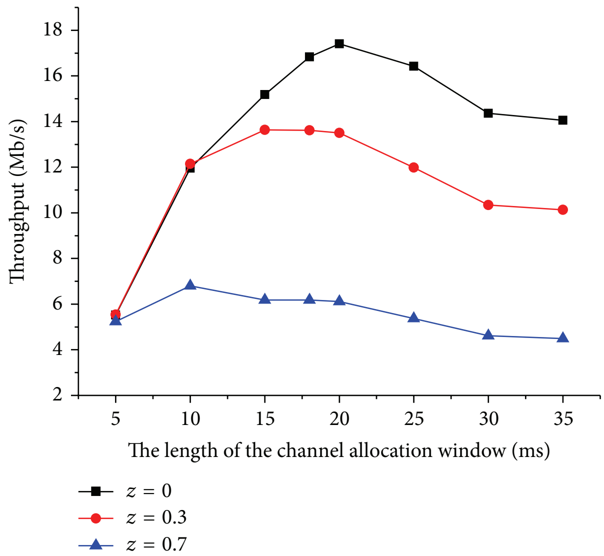


FIGURE 6: The relationship between throughput and channel allocation phase length.

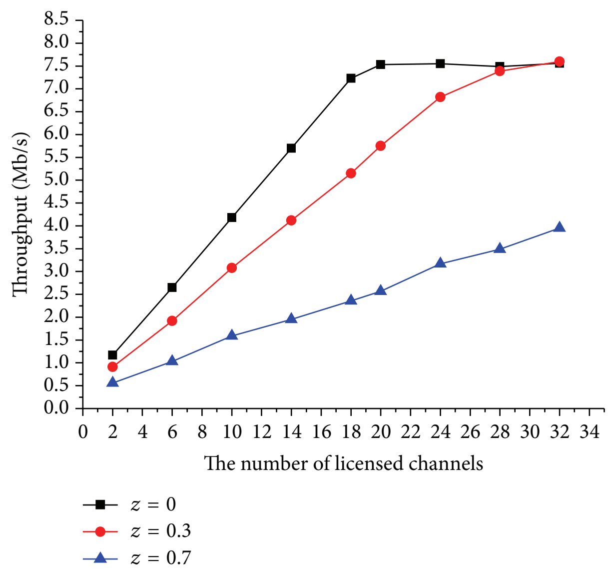


FIGURE 7: The relationship between throughput and number of licensed channels.

transmission time being reduced and the saturation throughput decreasing. When the primary users' activity rate gets higher, fewer idle channels become available. Idle channels are therefore assigned soon when the channel allocation time is small. For example, the throughput reaches the maximum when the channel allocation phase length is short.

4.3. The Relationship between Throughput and Number of the Licensed Channels. The relationship between the number of licensed channels and throughput in the DAHCWNS-MAC protocol is shown in Figure 7. The number of sending stations is 20 and the channel allocation phase length is 15 ms. When the number of licensed channels increases, the saturation throughput increases under different primary users' activity rate, which means the proposed protocol can fully utilize licensed channels to communicate without interrupting primary users.

4.4. The Relationship between Throughput and Number of Sending Stations. Figure 8 shows the impact of the number of sending stations on the DAHCWNS-MAC protocol's throughput. The number of licensed channels is 20 and the channel allocation phase length is 15 ms. As the number of sending stations increases, the throughput will increase and then remain stable when the primary users' activity rate is 0. This is because the number of node pairs that can complete a handshake is larger than 20 when the number of licensed channels is 20. The saturation throughput will reach the maximum when all channels are assigned. After this, because there are no more available channels, an increase in the number of sending stations will not result in an increase in the throughput. So the throughput remains stable.

4.5. Comparison to the C-MMAC Protocol. Reference [19] proposes the C-MMAC (cognitive-multichannel MAC) protocol. This protocol is also a synchronous MAC protocol for

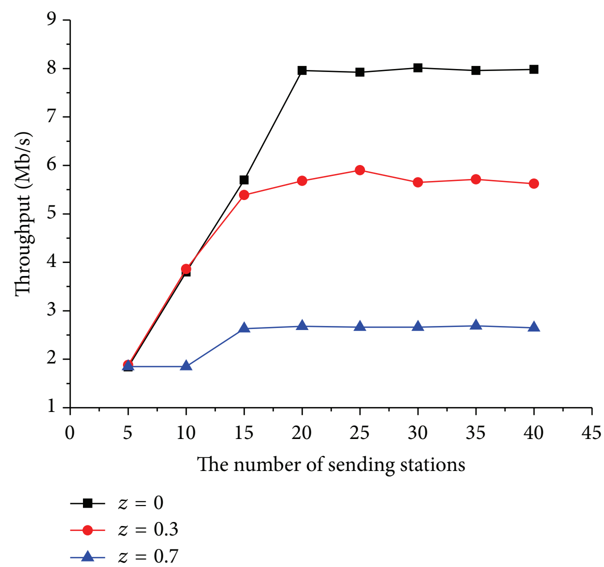


FIGURE 8: The relationship between throughput and number of sending stations.

cognitive radio network. The C-MMAC has some similarities with the DAHCWNS-MAC protocol: (1) The time frame of the C-MMAC protocol is divided into several parts (also include sensing phase, channel allocation phase, and data transmission phase) too and (2) all the nodes are strictly synchronous. The idea of designing DAHCWNS-MAC protocol is inspired by the C-MMAC protocol. However, the biggest difference between the two protocols is the network architecture. The C-MMAC protocol sets a single-hop network. The distance between two arbitrary nodes is within single-hop transmission range, and nodes can communicate directly. The network is self-organized, without infrastructure. Nodes have to sense the spectrum, exchange results, and negotiate channels by themselves. However, the protocol proposed in this paper is a hybrid network design. So this paper put these two protocols together to compare.

The two protocols are compared next through simulation. Since C-MMAC protocol is designed for the single-hop scenario, the scheme used in C-MMAC protocol is assumed to be a one-cell DAHCWNS-MAC protocol network. We compare the performance under the single-hop setting first (in one cell). The performance under a multiple cells network will be compared later.

4.5.1. Comparison in Single Cell. Nodes are placed randomly in one cell and communicate directly.

(1) 10 pairs of nodes are randomly placed in a cell, forming 10 communication streams. The number of licensed channels is 4. As shown in Figure 9 the throughput varies as the channel allocation phase length changes. When the primary user activity rate is 0 the C-MMAC protocol throughput is larger than that for the DAHCWNS-MAC at the beginning. This is because the C-MMAC protocol requires a three-way handshake (ATIM frame, ATIM-ACK frame, and ATIM-RES frame) to complete channel allocation while the DAHCWNS-MAC protocol requires a four-way handshake (SEARCH frame, ANSWER frame, SETUP frame, and ACCEPT frame). Under the same channel allocation window the C-MMAC protocol allows more nodes to complete a handshake to get available channels, which results in higher throughput. When the channel allocation window gets larger it allows most nodes to complete a handshake. The C-MMAC protocol also adopts a competition scheme during the data transmission phase, which results in a longer time to send data packets than the DAHCWNS-MAC protocol. The C-MMAC throughput is therefore smaller than that of the DAHCWNS-MAC protocol.

(2) 10 pairs of nodes are randomly placed in a cell, forming 10 communication streams. The channel allocation window length is fixed at 30 ms which is sufficient for 10 pairs of nodes to complete a handshake to get available channels. As shown in Figure 10 the throughput varies as the number of licensed channels changes. When the primary user activity rate is 0 all licensed channels are idle and the control channel can also be used to transmit data. The throughput of the DAHCWNS-MAC protocol reaches the maximum when the number of licensed channels is 9 and then remains stable. However, the nodes must sense the spectrum by themselves in the C-MMAC protocol. Not all channels are detected in order to save power. Each node randomly selects a channel to sense and exchange its results with other nodes to obtain the entire sensing results. Whether all channels can be sensed depends on the number of nodes. According to [19], the probability that all channels can be detected is 0.95 when there are 10 licensed channels and 50 nodes. When the number of licensed channels is equal to the number of nodes the probability falls to 0.036. This is why the C-MMAC throughput does not reach the maximum when the number of licensed channels increases to 9 (not all 9 channels have been detected). The maximal throughput does not come up until the number increases to 16 when the nodes can detect 10 idle channels. The DAHCWNS-MAC protocol is free from this problem because distributed antennas undertake the spectrum sensing job and are able to detect all channels. The curve has the same trend when the primary user activity rate is 0.5.

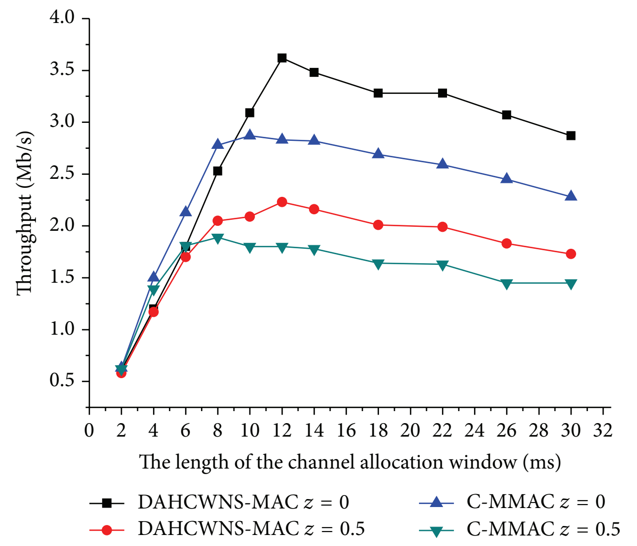


FIGURE 9: The comparison between the DAHCWNS-MAC protocol and the C-MMAC protocol as the channel allocation window length varies.

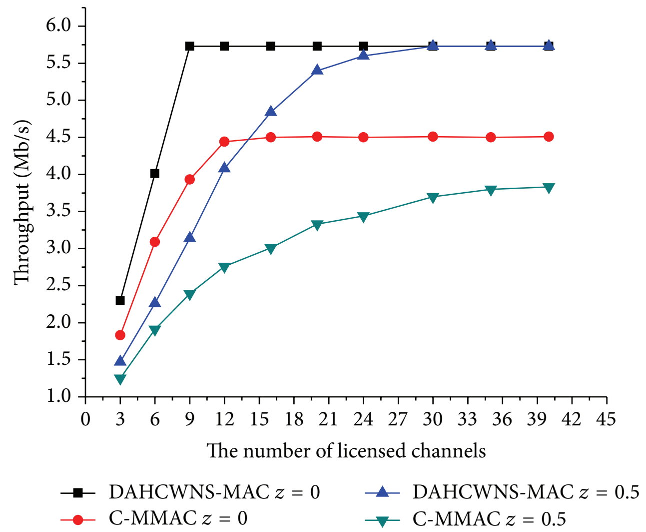


FIGURE 10: The comparison between the DAHCWNS-MAC protocol and the C-MMAC protocol as the number of licensed channels varies.

4.5.2. Comparison in Multiple Cells. The DAHCWNS-MAC protocol scheme is changed to seven cells while the C-MMAC protocol scheme remains the same.

(3) The number of nodes in the DAHCWNS-MAC protocol multiple cells scheme is more than seven times that of the C-MMAC single cell protocol. Assume that 35 pairs of nodes exist in the former scene and 5 pairs in the latter

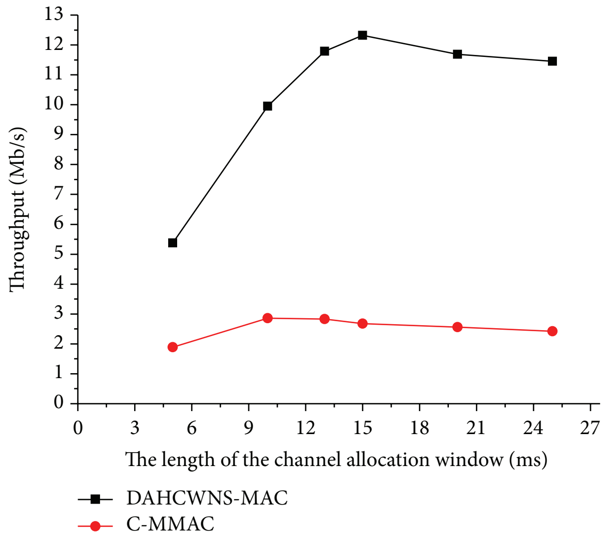


Figure 11: Comparison in multiple cells with different numbers of nodes.

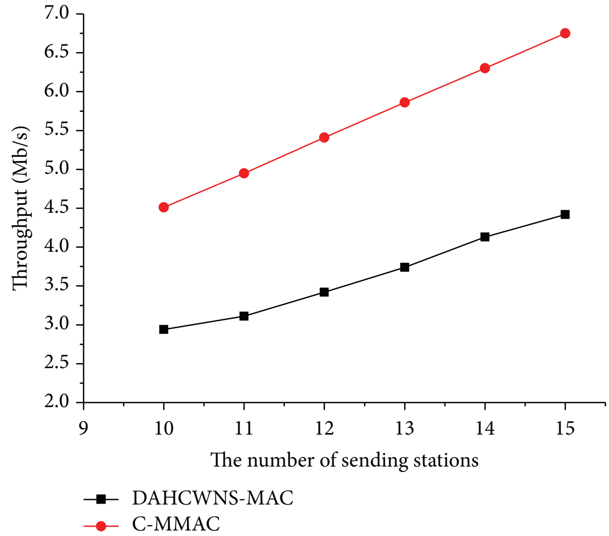


Figure 13: Comparison of multiple cells with the same number of nodes as the number of sending stations varies.

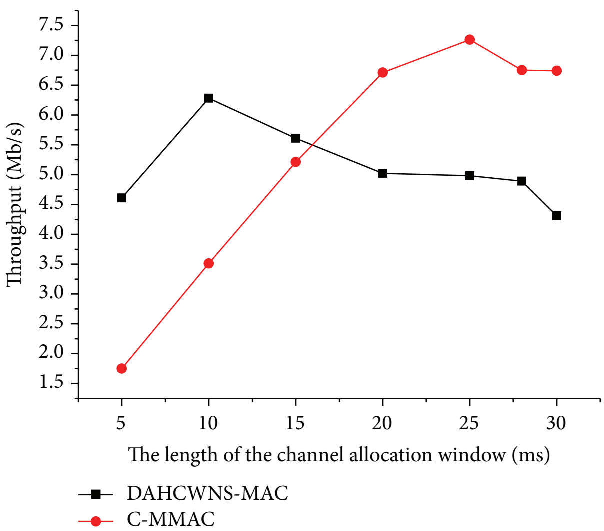


Figure 12: Comparison in multiple cells with the same number of nodes.

scheme. Ensure that nodes can be assigned channels as long as they complete a handshake. As shown in Figure 11, the DAHCWNS-MAC protocol throughput is not exactly seven times as large as that of the C-MMAC protocol. This is because the case nodes require distributed antennas to forward data which takes double the time of direct transmission.

(4) Assume 15 pairs of nodes are randomly placed in the two protocols, which means the number of nodes is the same in both schemes. Ensure that nodes can be assigned channels as long as they complete a handshake. As shown in Figure 12, the DAHCWNS-MAC protocol throughput is larger than that of the C-MMAC protocol when the channel allocation window length is relatively small. This is because operations in seven cells can be conducted in parallel, which leads to more nodes being able to complete a handshake. Since seven cells can work independently, 15 pairs of nodes can complete a handshake within 10 ms and the throughput reaches peak at this moment. After this moment the increase in channel allocation window length only leads to a decrease in the DAHCWNS-MAC protocol throughput. As the window becomes larger the number of nodes that finish a handshake becomes larger in C-MMAC. Since nodes can communicate directly, not like the DAHCWNS-MAC where antennas are required to forward data, the throughput becomes gradually higher than that of the DAHCWNS-MAC and reaches the maximum at 25 ms.

(5) Assume the number of nodes in the two schemes is the same. The channel allocation window is fixed at 30 ms. The number of licensed channels is sufficient. As shown in Figure 13, because the case exists where nodes need antennas to forward data in DAHCWNS-MAC, the throughput is absolutely less than that of the C-MMAC protocol where nodes are put together in a single cell.

5. Conclusion

The paper introduced distributed antennas into the cognitive wireless network. The cognitive wireless network is designed to be a heterogeneous network consisting of an ad hoc network with a sparse network with infrastructure. A distributed antenna based synchronous MAC protocol (DAHCWNS-MAC protocol) is also presented for the proposed network. This protocol utilizes distributed antennas to sense the spectrum and transmit data, which can improve the sensing performance and increase network throughput. Every part of the protocol was described in detail and a mathematical model and performance simulation were presented. The proposed protocol combines the advantages of the ad hoc network and the network with infrastructure to fully utilize idle licensed channels to increase throughput. We compared the proposed protocol with the C-MMAC protocol to demonstrate that the

DAHCWNS-MAC protocol can broaden the communication range and increase the network throughput compared with the original single-hop network at the cost of increasing antenna hardware costs.

The introduction of distributed antennas into spectrum sensing can fully utilize the spatial resources at the expense of increasing the antenna hardware costs. It can also overcome hidden/exposed terminal problems to a certain extent and improve sensing performance.

In addition to the spectrum sensing, we can further let the distributed antennas be used to locate the primary user and adopt different access methods according to positioning information. For example, the hybrid underlay/overlay access scheme can be adopted through power control, which can greatly improve the channel utilization ratio and increase network throughput.

Furthermore, in the DAHCCWNS-MAC protocol the center allocates the same channel to communication pair which is not flexible enough. In future work we can take the channel state information into consideration and allocate different channels to sending node and receiving node, respectively, according to in-time channel state to further improve network performance.

This paper focused on how the distributed antenna can be used in data transmission and did not explore its usage in spectrum sensing and positioning. In future studies we can continue to study on these aspects to complete the DAHCWNS-MAC protocol.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The work presented in this paper was partially supported by 2011 National Natural Science Foundation of China (Grant no. 61172097), 2014 National Natural Science Foundation of China (Grant no. 61371081), and 2012 Natural Science Foundation of Fujian (Grant no. 2012J01424).

References

[1] P. Yue, X. Yi, and Z.-J. Liu, “A novel wireless network architecture and its radio frequency assignment mechanism for WLAN based on distributed antenna system using radio over free space optics,” in *Proceedings of the International Conference on Information Science and Technology (ICIST ’11)*, pp. 488–492, March 2011.

[2] Z. Xu, C. Zhou, and J. Wang, “A novel cell architecture based on distributed antennas for mobile WiMAX systems,” in *Proceedings of the 4th IEEE International Conference on Circuits and Systems for Communications (ICCSC ’08)*, pp. 172–176, May 2008.

[3] D. J. Thomson, “Spectrum estimation and harmonic analysis,” *Proceedings of the IEEE*, vol. 70, no. 9, pp. 1055–1096, 1982.

[4] S. Haykin, D. J. Thomson, and J. H. Reed, “Spectrum sensing for cognitive radio,” *Proceedings of the IEEE*, vol. 97, no. 5, pp. 849–877, 2009.

[5] Y. Zeng, C. L. Koh, and Y.-C. Liang, “Maximum eigenvalue detection: theory and application,” in *Proceedings of the IEEE International Conference on Communications (ICC ’08)*, pp. 4160–4164, Beijing, China, May 2008.

[6] Y. Zeng and Y.-C. Liang, “Eigenvalue-based spectrum sensing algorithms for cognitive radio,” *IEEE Transactions on Communications*, vol. 57, no. 6, pp. 1784–1793, 2009.

[7] A. Taherpour, M. Nasiri-Kenari, and S. Gazor, “Multiple antenna spectrum sensing in cognitive radios,” *IEEE Transactions on Wireless Communications*, vol. 9, no. 2, pp. 814–823, 2010.

[8] R. Zhang, T. J. Lim, Y. C. Liang, and Y. Zeng, “Multi-antenna based spectrum sensing for cognitive radios: a GLRT approach,” *IEEE Transactions on Communications*, vol. 58, no. 1, pp. 84–88, 2010.

[9] H. Yao, *Research on the Spectrum Sensing and Resource Allocation in Cognitive Radio Networks*, Beijing University of Posts and Telecommunications, 2011.

[10] C. Zhao, L. Huang, Z.-L. Gao, S. Zhou, D. Guo, and H.-C. Chao, “performance analysis of the multiple antenna asynchronous cognitive MAC protocol in cognitive radio network for IT convergence,” *Intelligent Automation and Soft Computing*, vol. 20, no. 1, pp. 61–75, 2014.

[11] E. Y. Kang, H. Park, and J. Chae, “A hybrid message delivery scheme for improving service discovery in mobile ad-hoc networks,” *Journal of Internet Technology*, vol. 13, no. 6, pp. 879–890, 2012.

[12] Y.-X. Lai, C.-F. Lai, Y.-M. Huang, and H.-C. Chao, “Multi-appliance recognition system with hybrid SVM/GMM classifier in ubiquitous smart home,” *Information Sciences*, vol. 230, pp. 39–55, 2013.

[13] L. Zhou, H.-C. Chao, and A. V. Vasilakos, “Joint forensics-scheduling strategy for delay-sensitive multimedia applications over heterogeneous networks,” *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 7, pp. 1358–1367, 2011.

[14] C.-W. Chiang, “Two novel genetic operators for task matching and scheduling in heterogeneous computing environments,” *Journal of Internet Technology*, vol. 13, no. 5, pp. 773–784, 2012.

[15] B. Liu, Z. Liu, and D. Towsley, “On the capacity of hybrid wireless networks,” in *Proceedings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Societies*, vol. 2, pp. 1543–1552, April 2003.

[16] R. S. Chang, W. Y. Chen, and Y. F. Wen, “Hybrid wireless network protocols,” *IEEE Transactions on Vehicular Technology*, vol. 52, no. 4, pp. 1099–1109, 2003.

[17] G. Bianchi, “Performance analysis of the IEEE 802.11 distributed coordination function,” *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, pp. 535–547, 2000.

[18] N. Liu, *Wireless Local Area Networks (WLAN)—Principle,Technique and Application*, Xidian University Press, Xi’an, China, 2007.

[19] M. Yu, The Study of Cognitive Multi-Channel MAC Protocol Based on Spectrum Sensing, 2009.