International Journal of Information and Electronics Engineering, Vol. 4, No. 5, September 2014

Modeling and Evaluation for Proxy Mobile IPv6 Protocol

Ye Wang, Yanming Cheng, Xiaoyan Huang, Xiaolei Zhang, and Jang-Geun Ki

***Abstract*—This paper is addressed to develop a simulation node model to support the Proxy Mobile IPv6 (PMIPv6) protocol. The PMIPv6 related process node models were developed based on the Mobile IPv6 (MIPv6) process models by using simulation software, such as pmipv6_pmn.pr.m, pmipv6_mgr.pr.m and pmipv6_ra_gtwy.pr.m. In order to verify the developed process models, the several simulation scenarios were designed and constructed under the various traffic environments. In this paper, we provided two simulation scenarios: one is that the basic terminology of PMIPv6 network and the other is that comparison performance between MIPv6 and PMIPv6 network. From the simulation results can be seen, the Local Mobility Anchor (LMA) manages and intercepts all data packets from CN to proxy_MN, and each Mobile Access Gateway (MAG) encapsulates and decapsulates all data packets from LMA or proxy_MN. Moreover, the packet network delay presented higher in MIPv6 scenario than in PMIPv6 network. In wireless Local Area Network (LAN) load evaluation performance, the packet size of PMIPv6 is lower than that of the MIPv6 by outer IPv6 header length in 40 bytes. It can be concluded that the developed simulation models for PMIPv6 are logically correct and very useful to understand the fundamental features of mobility management in future networks.**

***Index Terms*—MIPv6, model, PMIPv6, simulation.**

I. Introduction

Mobility management of the device is the one of the major functions in the LTE and 3G networks that allows mobile phones to move around. The goal of mobility management is to chase where the subscribers are and support the mobile phone services such as calls and short messages, to be kept without break. Mobility management has been recognized that using global mobility protocol causes a number of problems, such as a long registration delay. To overcome these problems, Proxy Mobile IPv6 is proposed, which can avoid tunneling overhead over the air and support for hosts without an involvement in the mobility management [1].

Proxy Mobile IPv6 (PMIPv6) [2] is being actively standardized by the IETF netext (Network-Based Mobility Extensions) working group. The objective of this paper is to create a simulation program to support the proxy mobile IPv6 protocol. The implementation and performance analysis of this protocol is essential to understand the fundamental feature. Therefore, our goal is to develop the PMIPv6 protocol model in the simulation tool in order to study further and research in the future work. In this paper, the simulation models and environments for proxy mobile IPv6 protocols were developed according to the standard documents in Internet Engineering Task Force (IETF). Moreover, we designed and constructed several simulation scenarios under the various traffic environments. The simulation results show that the developed models are useful for mobility management studies in various integrated wireless networks.

II. Overview of Proxy Mobile IPv6 Protocol

A. *Overview of Mobile IPv6 Protocol*

To better understanding PMIPv6 protocol, the Mobile IPv6 (MIPv6) [3] protocol should be studied at first. As discussed in [4], Fig. 1 illustrates the basic operation of MIPv6. As shown in Fig. 1, there are three cases as follows:

1) While MN is in its home network, all data packets destined to the MN will reach through the normal routing process without any tunnelling process, as shown in Fig.1 (1).
2) Once MN moves into the visited network, MN will attach the access router and delegate the new IP address (e.g. CoA) by using a statefull auto-configuration (DHCPv6) or an IPv6 stateless address auto-configuration (router advertisement) mechanism. Then MN will send Binding Update and Binding Acknowledgement to and from the HA, to create a bi-directional tunnel between MN and HA, as shown in Fig.1 (2).
3) Another case is using route optimization to avoid the routing triangular problem as explained previous, the binding information will be exchanged between the MN and CN, as can be seen in Fig. 1 (3).

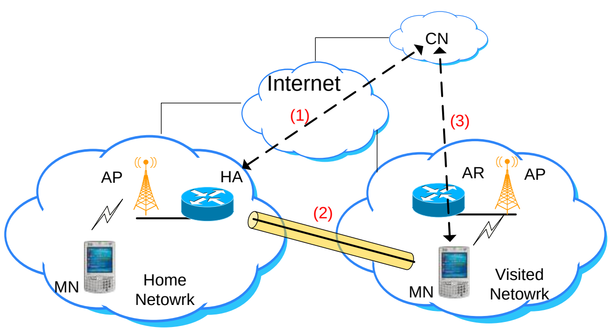


Fig. 1. Mobile IPv6 basic operation.

Manuscript received February 21, 2014; revised May 30, 2014.

Ye Wang and Xiaoyan Huang are with the Department of Electronic and Information Engineering, Lishui University, Lishui City, Zhejiang Province, China (e-mail: wychina_2007@ hotmail.com, lsxyhxy@126.com).

Yanming Cheng is with the Department of Electric and Information Engineering, Beihua University, Jilin City, Jilin Province, China (e-mail: mycheng2005@hotmail.com).

Xiaolei Zhang is with the Communication and Automation Centre, Sichuan Electric Power Corporation, Chengdu City, China (e-mail: mumulei0411@126.com).

Jang-Geun Ki is with the Department of Electrical, Electronics and Control Engineering, Kongju National University, Budae-dong, Cheonan, 330-717, Korea (corresponding author: Jang-Geun Ki; e-mail: kjg@kongju.ac.kr).

DOI: 10.7763/IJIEE.2014.V4.472

B. *Overview of Proxy Mobile IPv6 Protocol*

Unlike MIPv6, where the mobile node signals its location changes to the HA, a PMIPv6 [2], which is a network-based mobility to solving the IP mobility challenge, has been developed to support IP mobility for a MN. It is possible to support mobility for IPv6 nodes without mobile host involvement by extending mobile IPv6 signalling messages between a network node and a home agent. In order to facilitate such network-based mobility, the PMIPv6 protocol defines a Mobile Access Gateway (MAG), which acts as a proxy for the mobile IPv6 signalling, and the Local Mobility Anchor (LMA) which acts similar to a HA. Upon exchanging Proxy Binding Update (PBU) message and Proxy Binding Acknowledgement (PBA) message, the LMA and the MAG establish a bi-directional tunnel for forwarding all data traffic belonging to the mobile nodes.

A description of the basic terminology of Proxy Mobile IPv6 is illustrated in Fig. 2 [4]. As shown in Fig. 2, the LMA includes the Binding Cache Entry (BCE) and the MAG includes the Binding Update List (BUL) information, respectively. The BCE has the fields MN-ID, MAG proxy-CoA and MN-prefix. The BUL is a cache maintained by the MAG that contains the needed information about the attached MNs. The following procedure is shown:

1) While MN initially attaches to the MAG1 by presenting MN-ID to process an access authentication.
2) After successful AAA operation, the MAG1 sends a PBU message with MN-ID to the LMA on behalf of the MN to update the MN's new location, see Fig. 2-(1).
3) After receiving PBA message from LMA, the tunnel is set up between LMA and MAG1. Upon exchanging PBU and PBA message, the BCE and BUL are created. See Fig. 2.
4) Once MN is moving away from MAG1 and attaches to the MAG2, the new tunnel between LMA and MAG2 is created for data packet transmission, see Fig. 2-(2) [5].

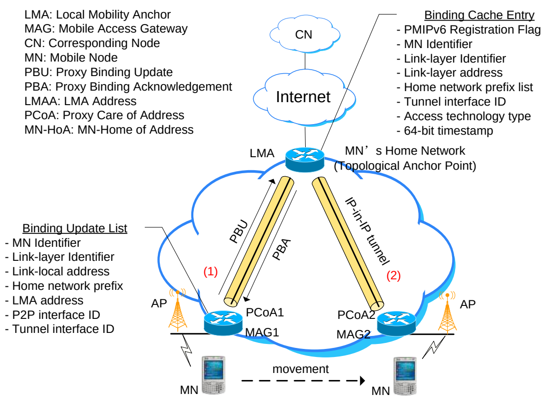


Fig. 2. Basic terminology overview of PMIPv6 domain.

III. PROXY MIPV6 NODE MODELS

The PMIPv6 process models are developed based on the MIPv6 process models in OPNET [6], such as mipv6_mgr.pr.m, mipv6_mn.pr.m, etc. According to the basic terminology of PMIPv6 [2], each node should include and present the different functions and process models, which can see in Fig. 3- Fig. 4.

From the Fig. 3 can be seen, the MAG should detect the MN's attachment by receiving Router Solicitation message in order to send PBU message in time. However, we adopt the MAC_Network algorithm to detect the MN's attachment procedure. This algorithm is seen in Fig. 4 and explained as follows:

1) The data link layer (wlan_mac layer) in both MN and MAG is required to support WLAN AP association procedure.
2) Once MN enters a new network, MN's wlan_mac layer will do a scan procedure to find out an AP if MN has no AP to connect.
3) While connecting an AP (MAG), MN should negotiate with this AP in wlan_mac layer. After that, AP will obtain a MN's MAC address (mn_mac_addr) by association procedure.
4) Then, AP (MAG)'s wlan_mac layer will delivery the interrupt process code with mn_mac_addr to invoke the pmipv6_pmn.pr.m for generating a PBU message.

It can be seen form Fig. 3 and Fig. 4 that once LMA receives the PBU message, LMA will invoke the pmipv6_mgr.pr.m to handle this PBU message and create or update BCE. In MAG, the pmipv6_pmn.pr.m will handle the PBA message and invoke the pmipv6_ra_gtwy.pr.m to generate and send Router Advertisement message with Home Network Prefix information.

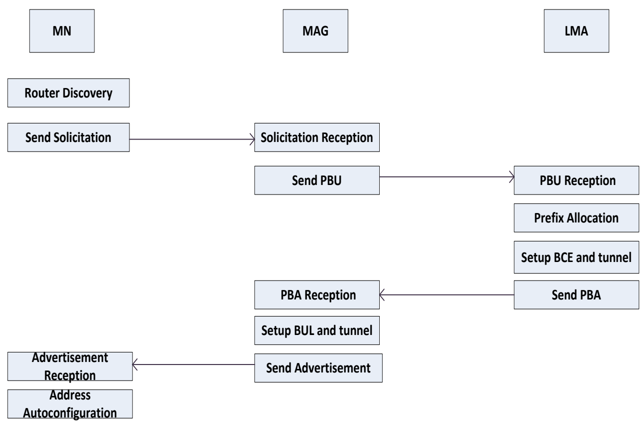


Fig. 3. PMIPv6 each node function.

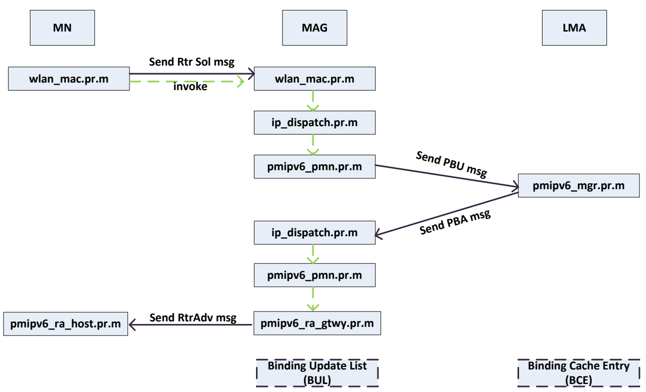


Fig. 4. Process models developed for PMIPv6 operation.

IV. Simulation Results Analysis and Discussion

In Fig. 5, there are two network scenarios: one is that basic PMIPv6 scenario, and the other is that MIPv6 network architecture. In the previous scenario, we will show the UDP and TCP traffic, and then the comparison performances between PMIPv6 and MIPv6 scenarios are illustrated.

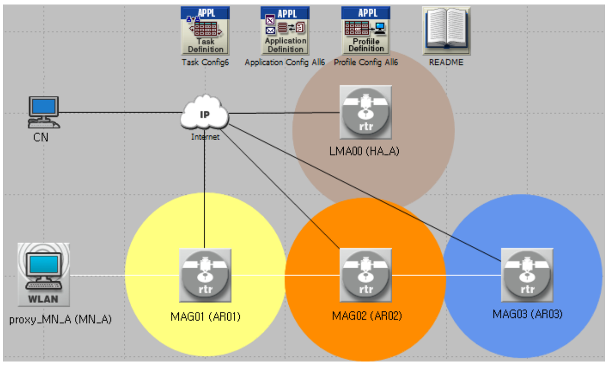


Fig. 5. The basic PMIPv6 & MIPv6 network architecture.

A. UDP and TCP Traffic in PMIPv6 Network

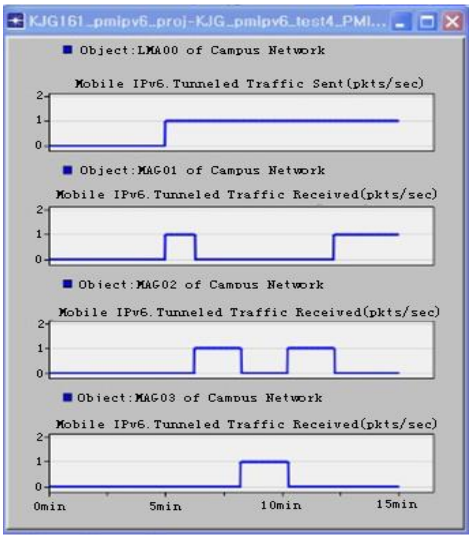
In this section, the UDP and TCP packets are generated and delivered to the proxy_MN_A from CN with 1024 bytes and 500000 bytes, respectively.

Fig. 6(a) shows the PMIPv6 tunneled UDP traffic statistics between LMA and MAG in the scenario. More specifically, it depicts the tunneled traffic sent from LMA and tunneled traffic received by each MAG nodes. With the change of the MN's attachment point to the MAG, the LMA sends tunneled traffic to each MAG node during the simulation time.

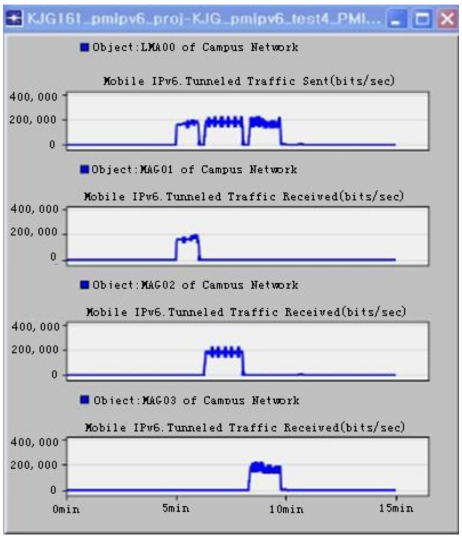
Fig. 6(b) shows the tunneled TCP traffic sent and received. Because TCP traffic only sent one time and also it will be segmented by the network and sent separately. From the Fig. 6b, the LMA00 intercepted all TCP data packets for proxy_MN_A and then tunneled those segmented data packets to MAG01, MAG02 and MAG03.

B. Comparison Performance with MIPv6 Network

In the previous Fig. 5, the same network scenario between PMIPv6 and MIPv6 is shown. In this scenario, the UDP data traffic with 1024 bytes will be generated from CN to proxy_MN_A and MN_A.

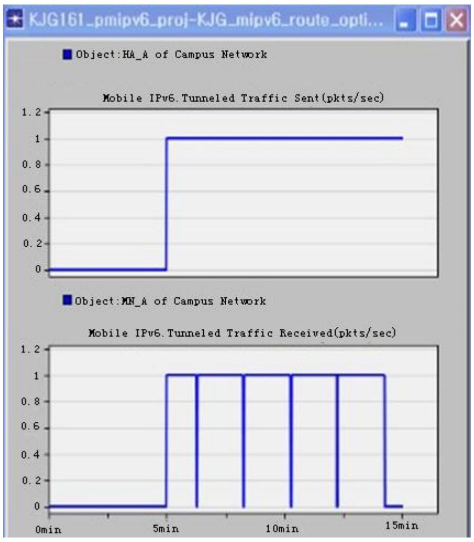


(a) UDP tunneled traffic

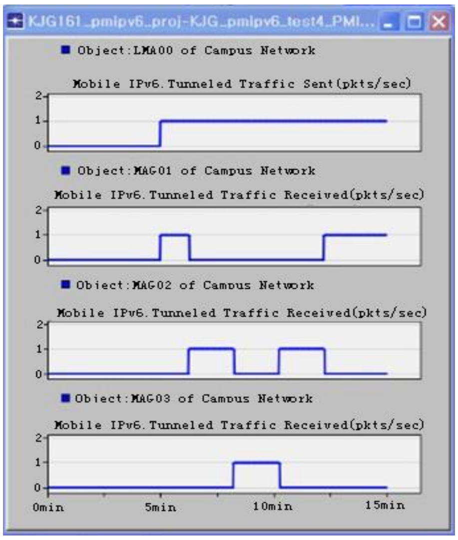


(b) TCP tunneled traffic

Fig. 6. PMIPv6 tunneled traffic sent/received with UDP/TCP packet.



(a) MIPv6: HA-> MN



(b) PMIPv6: LMA->MAG

Fig. 7. Tunneled traffic sent/received in MIPv6 and PMIPv6 scenario.

From Fig. 7(a) - Fig. 7(b), it can be known there is no tunneling overhead at proxy_MN_A in PMIPv6 scenario. It means the MAG will manage all data packets on behalf of MN in PMIPv6 domain. In Fig. 8, the packet network delay in MIPv6 presents higher than in PMIPv6 network, because

LMA and MAG will manage all the data packets instead of proxy_MN_A.

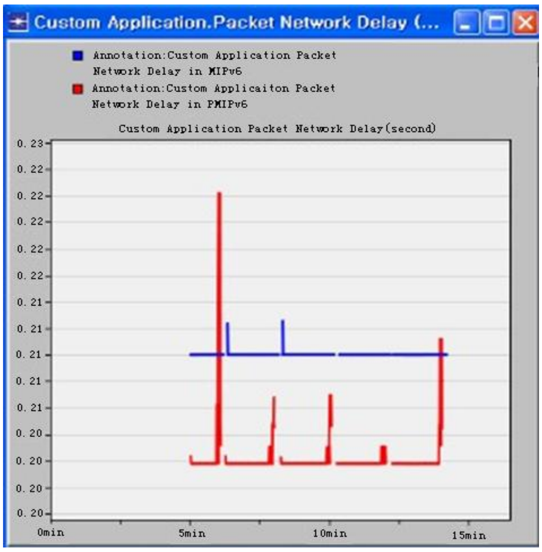
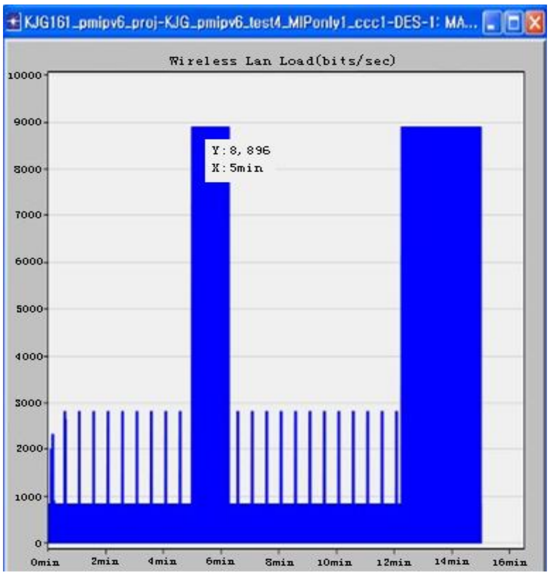
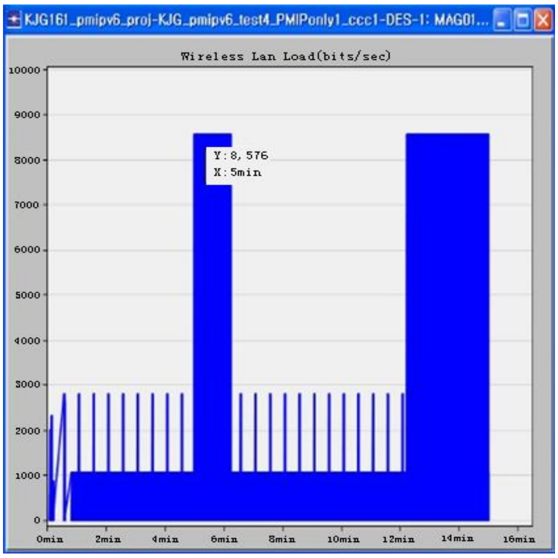


Fig. 8. Application packet network delay.



(a) WLAN load in MIPv6



(b) WLAN load in PMIPv6

Fig. 9. Wireless LAN load in MIPv6/PMIPv6 network.

Fig. 9 shows the wireless LAN loads in the Access Router (AR) of the MIPv6 and in the MAG of the PMIPv6 scenario. Because we choose the same network architecture between MIPv6 and PMIPv6, also the same UDP data packets are delivered, in Fig. 9(a)- Fig. 9(b), the WLAN load shows 8896 bits/sec and 8576 bits/sec in 5 minute, respectively. The reason also can be seen from the Table I.

Table I compares the packet size of each scenario in the wireless LAN network. In case of the MIPv6, the encapsulated packet is delivered to the MN through wireless network. On the other hand, data packet in the PMIPv6 is de-capsulated at the MAG node and then delivered to the MN through wireless network. Therefore, the packet size of the PMIPv6 is shorter than that of the MIPv6 by outer IPv6 header length (40 bytes), which also can be seen in Fig. 9.

TABLE I: PACKET SIZE FOR WIRELESS LAN LOAD

	MIPv6	PMIPv6
Data	8192bits (1024 bytes)	8192bits (1024 bytes)
UDP header	64 bits (8 bytes)	64 bits (8 bytes)
IPv6 header	320 bits (40 bytes)	320 bits (40 bytes)
Outer IPv6 header	320 bits (40 bytes)	
Total	8896 bits (1112 bytes)	8576 bits (1072 bytes)

V. CONCLUSIONS

In this paper, we developed the simulation node models and environments for Proxy Mobile IPv6 protocol. The implementation and performance analysis of this protocol is essential to understand the fundamental features of mobility management in future networks.

After simulating the whole scenarios and analyzing the results, we conclude that the developed simulation models are logically correct and very useful for studying PMIPv6 protocol.

This paper attempts to compare host-based mobility management protocol with network-based mobility management protocol. Since MIPv6 is the most widely researched protocol, we have used MIPv6 as the host-based protocol to compare the performance of PMIPv6 in our comparison scenarios. The PMIPv6 presents some good advantages and other features over MIPv6 in our simulation results.

The future research must be conducted and more extensive simulations and develop network-based distributed mobility management architecture by using PMIPv6 protocol.

REFERENCES

[1] J. Lei and X. M. Fu, "Evaluating the benefits of introducing PMIPv6 for localized mobility management," in *Proc. Wireless Communications and Mobile Computing Conference*, Crete Island, 2008, pp. 74-80.

[2] *Proxy Mobile IPv6*, IETF Network Working Group, RFC 5213, August 2008.

[3] *Mobility Support in IPv6*, IETF, RFC 6275, July 2011.

[4] I. Al-Surmi, M. Othman, and B. Mohd Ali, "Mobility management for IP-based next generation mobile networks: Review, challenge and perspective," *Journal of Network and Computer Applications*, vol. 35, no. 1, pp. 295-315, January 2012.

[5] I. Soto and M. Calderón, "PMIPv6: A network-based localized mobility management solution," *The Internet Protocol Journal*, vol. 13, no. 3, September 2010.

[6] OPNET. [Online]. Available: http://www.riverbed.com/products-solutions/.

Ye Wang received the B.S. in electrical engineering and automation from Beihua University, China in 2003. He joined Zhuhai Wanlida Electric Co., LTD. in 2003 China, and also received his M.S., Ph.D in information and communication engineering from Kongju National University in Korea in 2009, 2013, respectively.

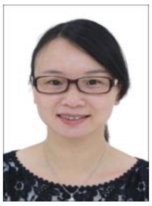
Since then, He has been a lecturer in Lishui University, Zhejiang Province in China.

His main research interests include mobile wireless networks, mobile Internet architecture and NGN mobility management.

Yanming Cheng received the B.S degree in electrical engineering and automation from Jilin Institute, China in 2006 and M.S., Ph.D degree in information and communication engineering from Kongju National University in Korea in 2007 and 2011, respectively.

Since then, he has been a lecturer of College of Electrical & Information Engineering, Beihua University, Jilin, China. He was past-time researcher in mobile RF team in Electronics Technology Research Institute (ETRI) in Korea in 2010.

His areas of research interest are compatibility between wireless communications system, smart antenna technology, simulation & modeling and internet of things.



Xiaoyan Huang was born in Lishui, Zhejiang Province, China, 1972, and received her B.S. in physics from Zhejiang Education College, in 1999, and her M.S. in electronics and communication engineering from Zhejiang University, China in 2008.

Since 2004, she has been a lecture in Lishui University, Zhejiang Province in China.

Her main research interests include electronic circuit and system.

Xiaolei Zhang received B.S. degree in the automation from Beihua University, China, in 2007, and received her M.S., Ph.D in information and communication engineering from Kongju National University in Kongju, Korea in 2009, 2013 respectively.

Since then, she has been a researcher in Communication and Automation Centre, Sichuan Electric Power Corporation, China.

Her main research interests include MANET, MIPv6 and internet protocol suite.

Jang-Geun Ki received the B.S., M.S., Ph.D. in electronics from Korea university, Korea in 1986, 1988, 1992 respectively.

Since then, he has been a professor in Kongju National University.

His main research interests include telecommunication protocols and network architectures.