Substitutive Mutual Authentication between Mobile Base Stations in Tactical Networks

Yu-Jin Son, Taeshik Shon and Young-Bae Ko

Graduate School of Information and Communication, Ajou University, Korea
yujin@uns.ajou.ac.kr, tsshon@ajou.ac.kr, youngko@ajou.ac.kr

Abstract

This paper proposes a cooperated mutual authentication scheme for mobile base stations (MBS) that construct a Wireless Mesh Network (WMN) in the Tactical Information Communication Networks (TICN). To enhance the fighting capabilities and survivability of soldiers in battlefields, it is crucial to secure the communication and commands between soldiers and commanders. To achieve this goal, a reliable mutual authentication method is required to approve between MBS and the soldiers in the network. We apply EAP-TLS (Extensible Authentication Protocol – Transport Layer Security) for mutual authentication between mobile base stations that each hold authentication servers [1]. Also, we propose a cooperative authentication scheme that can substitute the authentication process between MBS and ultimately reduce the authentication overhead. We evaluate the proposed scheme using the Qualnet 5.0 simulator to verify the performance of our proposed schemes in Tactical Networks.

Keywords: *Node Cooperation, Mutual Authentication, Wireless Mesh Networks, Tactical Communication and Networks*

1. Introduction

The next generation of tactical communication and networks include lightweight, independent communication capabilities of soldiers that are managed and controlled by a centralized communication command system. Already, much research and development have been under progress, such as Joint Tactical Radio System (JTRS) [2, 3] in America and the recent TICN project [4, 5] in Korea. In the near future, these systems are destined to be successfully implemented to reinforce the combat and communication capabilities of the whole tactical system.

In these tactical networking systems, it is most important to provide seamless and reliable multimedia transmission to all mobile soldiers deployed in the battlefield. To provide these functionalities for example, TICN utilizes some of the commercial technologies such as IEEE 802.16 based cellular systems [6] to maintain high performance communication capabilities between mobile terminals (the soldiers) and the base stations (vehicles or access points that act as the backbone infrastructure). However, in contrary to the applications of these commercial cellular systems, tactical environments must provide means to cope with the dynamic mobility and wide coverage of the battlefield. Therefore, it is required for the base stations to also have full, unlimited mobility to follow and provide communication means to soldiers.

One of the main issues to cope with in these tactical environments is managing network security. In traditional authentication schemes such as EAP in 802.16, a master base station that has a link to the exterior networks will be responsible for managing the Authentication, Authorization, and Accounting (AAA) server to authenticate all the nodes in the network.

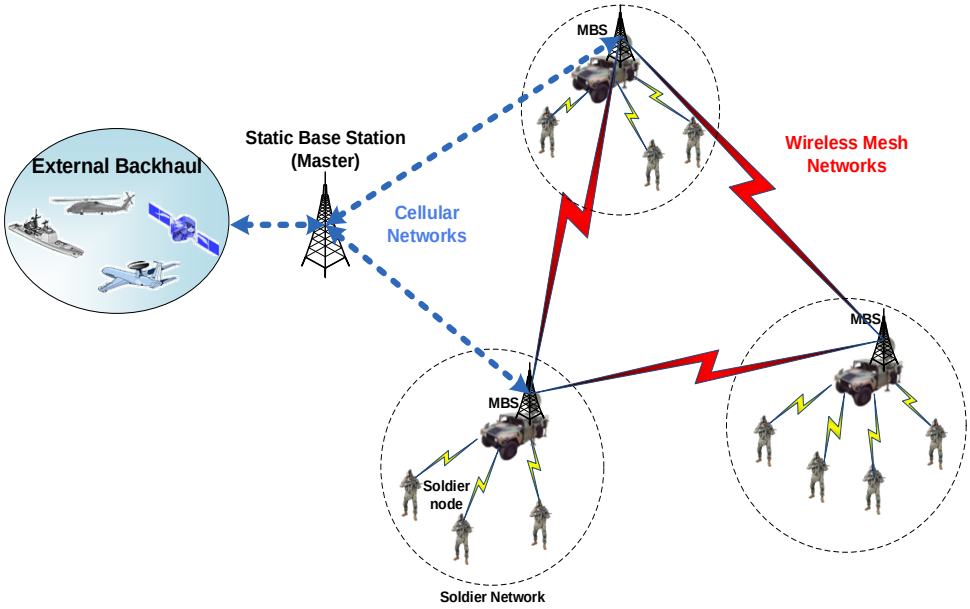


Figure 1. The assumed tactical network scenario where MBS forms WMN

Even though EAP can provide powerful means of authentication, this may cause problems in the dynamic tactical environment, shown in Figure 1. In Figure 1, MBS can connect to the external backhaul through cellular network, while connecting with other MBS via independent mesh network. The soldier nodes maintain single-hop communication with the closest MBS. If EAP is utilized, nodes must relay the authentication information between the base station managing the AAA server, other base stations, and the mobile soldier terminals because of the mobile multi-hop characteristics. This may result in excessive authentication overhead affecting data transmission in the tactical network.

To solve this problem, this paper proposes a method of migrating AAA servers to each mobile base station for more efficient authentication between the stations. To account for rogue base stations [6], we propose a method of mutual authentication that can effectively utilize the existing EAP-TLS between the AAA servers by using the WMN. We also propose a substitute node authentication using distributed methods that can reduce the number of transmitted control packets by simplifying the authentication operations. Via simulation through Qualnet 5.0, we show that our proposed scheme can reduce the overall overhead of the network while maintaining reliable level of security.

2. Background and Related Works

2.1. Background on EAP-TLS

The IEEE 802.16 standard defines the Privacy Key Management version 2 (PKMv2) as the mutual authentication method between base station and the mobile terminals. Through the PKMv2, the base station can re-authenticate, reauthorize, distribute, and refresh traffic keys to the mobile terminals. One of the main options of PKMv2 is to utilize the EAP-TLS for mutual authentication between base stations, which is also standardized [7]. The base station with the EAP-TLS will authenticate other stations through X.509 certification, while the other stations also maintain the certificates to allow mutual authentication. Through this process, the base station and the terminal will mutually share a private key that will be later used to

encrypt and transmit data. The algorithm of the traditional EAP-TLS authentication method can be summarized as shown below:

Step 1. System Initializing Phase & User Register Phase: Each node in the network will initiate the ranging process that provides link synchronization, initial negotiation, and identification.

Step 2. Mutual Authentication Phase: The authentication through TLS is attempted, creating the Premaster Secret Key and the TLS master secret key, which are used to generate the Master Session Key (MSK).

Step 3. Key Derivate and 4-way Handshaking Phase: After the initial authentication, the terminal will transmit its MSK to the base station so that any data encrypted through the MSK can be decrypted by either node.

One of the most critical problems in these authentication processes is that excessive numbers of control packets are shared between the base station and the terminals. The dynamic mobility of base stations that may enforce re-authentication process can further deteriorate the network.

2.2. Related Works

There have been several approaches on improving the security of network in mobile multi-hop relay scenarios. For example, Huang [6] provides a more reliable mutual authentication in the 802.16j MMR environments, which strengthens the mutual multi-hop authentication process. Work by Jin [8] provides improvement in mutual authentication by reinforcing the reliability of X.509 certificate and readjusting the authentication process. Even though these works can improve the level of security, they do not consider reducing the overhead that may occur from multi-hop authentication. Related standards [9, 10] also provide methods of mutual authentication between multi-hop mesh nodes in the LAN. In 802.11s, Mesh Points become responsible for authenticating mesh routers and mesh clients, utilizing similar methods to 802.16 such as EAP-TLS. However, the standard also defines only one AAA server at the mesh point, causing multi-hop authentications between servers and clients, inducing overhead in the process. There are also more works in sensor networks that allow mutual authentication between sink nodes and sensor nodes, which have to eventually deal with the same problems that MBSs have when utilizing EAP-TLS for mutual authentication. However, to the best of our knowledge, there has been minimal work on where each wireless sensor node maintains same-level authentication servers and attempt to mutually authenticate each other.

3. Proposed Scheme

The proposed mutual authentication scheme between the MBS assumes that each MBS in the network maintains an AAA server that is traditionally used for authentication of mobile soldier nodes. In the proposed scheme, this AAA server will be used to mutually authenticate between each MBS. Each MBS can utilize the cellular network to connect and communicate with external backhaul, which may include connection between other networks. On the other hand, MBS can connect with each other through the utilization of WMN module. The main objective of the mutual authentication between MBS is to distinguish and exclude rogue MBS that may attempt to associate and participate in the network. Also, another objective of the proposed scheme will be to reduce the overall overhead that may occur from the mutual authentication process.

3.1. Mutual Authentication based on EAP-TLS

Figure 2 shows the EAP-TLS authentication of two MBSs using the WMN module. The WMN module is responsible for transmitting and receiving the EAP messages, while managing the X.509 certificates. Therefore, most of the mutual authentication process can be done by the WMN module, while the AAA server is only occasionally referenced to reduce computational complexity of the process. The overall process can be divided into three steps:

Step 1. System Initializing Phase & User Register Phase: The initial registration phase involves the transmission of authenticator MBS1 to request identity of MBS2.

MBS1 WMN → MBS2 WMN :

PKMv2-RSP/EAP-Transfer(EAP-Request/ Identity) (1)

Upon reception of the request, MBS2 will transmit its ID back to the MBS1, which will forward the data to the AAA server for identification.

MBS2 WMN → MBS1 AAA Server:

PKMv2-REQ/EAP-Transfer(EAP-Response/ Identity) (2)

Step 2. Mutual Authentication Phase: Upon successful identification by the AAA server, MBS1 WMN initiates the EAP-TLS process and transmits its first message to the WMN module of MBS2.

MBS1 AAA Server → MBS2 WMN :

PKMv2-RSP/EAP-Transfer(EAP-Request/EAP-TLS.Start) (3)

Without referring to its AAA server, MBS2 can transmit back a response message including the information shown in (4) of Fig. 2.

MBS2 WMN → MBS1 WMN: PKMv2-REQ/EAP-Transfer(EAP-TLS.Client_Hello) (4)

Using the X.509 certificates that each WMN module holds, MBS1 and MBS2 can share the TLS server key, as shown in (5) and (6).

MBS1 WMN → MBS2 AAA Server:

PKMv2-RSP/EAP-Transfer(EAP-TLS.Server_Hello) (5)

MBS2 AAA Server → MBS1 AAA Server:

PKMv2-REQ/EAP-Transfer(EAP-TLS.Finished) (6)

Once the MBS WMN module receives the final EAP response from MBS2, it will transmit the certificate to the AAA server. From the certificate of MBS2, the AAA server of MBS1 must be able to retrieve the MAC address and model name from the X.520 Common Name RDN and try to approve it.

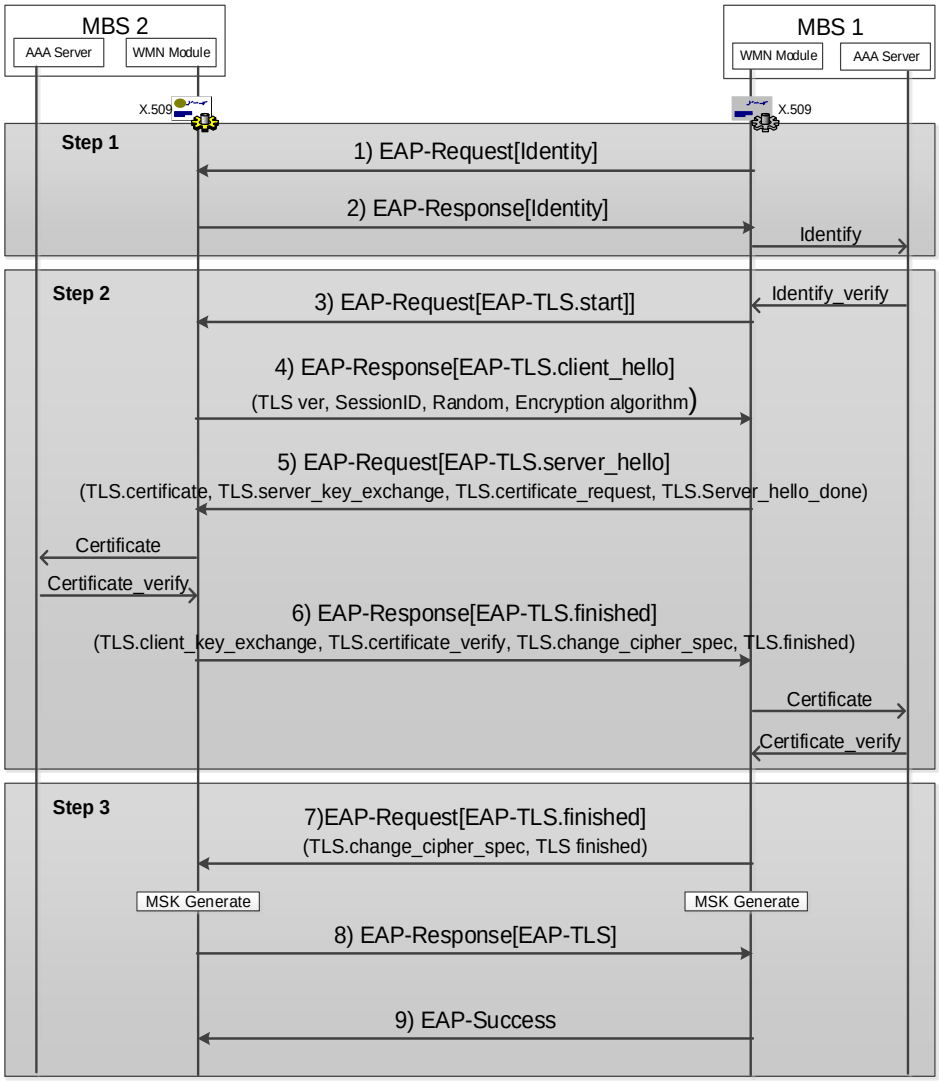


Figure 2. The proposed scheme operating between two MBSs

Step 3. Key Derivate and 4-way Handshaking Phase: Once the approving is complete, the MBS1 will create a TEK from the Premaster Secret key and use the TEK to transmit EAP-TLS.finished message back to MBS2.

MBS1 AAA Server →MBS2 WMN:

PKMv2-RSP/EAP-Transfer(EAP-TLS.Finished) (7)

Then, MBS1 and MBS2 can generate the MSK, which will eventually be used to encrypt and decrypt data transmission between the two devices. After successful generation of the MSK, the final handshake between the two devices are made to finalize the authentication process. Firstly, the WMN module of the MBS2 generates the EAP-Response/EAP-TLS message and transmits it to MBS1, as shown in (8).

MBS2 WMN →MBS1 WMN:

PKMv2-REQ/EAP-Transfer(EAP-Response/EAP-TLS) (8)

Upon receiving the EAP-Response/EAP-TLS message by the WMN module of MBS1, it generates the EAP-Success message and transfers it back to the WMN module of MBS2. This can be seen in (9).

MBS1 WMN →MBS2 WMN:

PKMv2-RSP/EAP-Transfer(EAP-Success) (9)

Only after when the WMN module of MBS2 receives the EAP-Success message can it be declared that the whole authentication process have succeeded. After the authentication, each MBS can now use the generated key to encrypt and transmit their data securely.

The advantage of using our proposed mutual authentication method is that each mobile base station can manage its own AAA server; considerably reducing overhead that may severely occur in multi-hop authentication scenarios. Furthermore, we reduce the computational complexity by reducing the reference to the AAA server. However, due to the mobility of MBS, we believe that installing AAA servers on each MBS will not be enough to reduce overhead induced from frequent re-authentication.

3.2. Substitutive Authentication Scheme

The cooperated substitute authentication method is aimed to further reduce the overhead induced from the algorithm by simplifying some of the process while maintaining the security level. Scheme 1 will be used as the basis of the scheme, but conditions will be given to make the scheme more efficient.

Initial State: For any MBS attempting authentication, if it does not contain MSK to any other MBS, it will undergo full authentication process in scheme 1. In other words, this condition applies for any MBS that has not attempted authentication or if all of its keys are expired.

Authentication of $n > 1$ MBS: Once a MBS successfully generates more than one MSK, that MBS will broadcast its owned MSKs to all other authenticated MBSs in single-hop range, using the public session key to encrypt it. Since it is encrypted, any rogue MBS will not be able to receive it while the authenticated node can receive this key. The transmitted *key_notify* message will contain {*Key_identifier, MSK, Node_ID, Key_hop_count*} for each key that will be transmitted. The *Key_identifier* will inform the destination MBS that the key will be used for. *Key_hop_count* will be accumulated every time it is transmitted.

Reception and maintenance of *key_notify* message: Any neighbor MBS that receives the *key_notify* message will decrypt and store the information on the *received_key* table. If any MSK has a *Key_hop_count* over *hop_threshold*, it will be deleted from the table because a MSK of a far MBS may not be used for an extended period of time.

Substitute authentication using *received_key* table: If an authenticated MBS receives authentication request from a suspicious MBS that has not yet been authenticated by the MBS itself, it will check the *Node_ID* that is transmitted in step 1 of Figure 2. If the Node_ID matches an entry in the *received_key* table, this means that the suspicious MBS has been

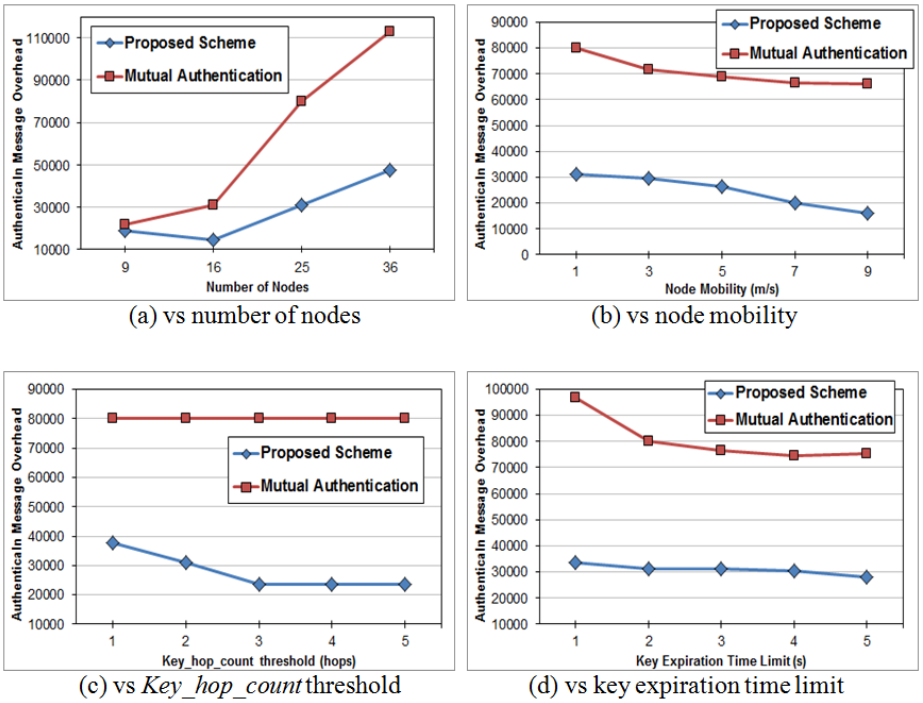
previously authenticated by another trusted MBS. Therefore, the authenticated MBS will initiate the MSK handshake process to match the key between each other. In a case where multiple MBS have transmitted multiple MSKs to the same suspicious MBS, the authenticated MBS will randomly select one MSK and use it to establish secure data connection. If the *Node_ID* does not match any entry in the *received_key* table, then the original full authentication process explained above is initiated.

Since the MSKs are shared only between trusted and authenticated MBSs, we believe that this can be used instead to greatly simplify the whole authentication process. In overall, the proposed mutual authentication method and the cooperated substitute authentication scheme can effectively reduce the authentication overhead in the network. Even though this may come at the expense of sharing keys, the overhead is very small compared to the overhead reduction gained from the proposed schemes.

4. Performance Evaluation

In this section, the proposed scheme is evaluated via QualNet 5.0 simulator. The proposed scheme is configured on top of the IEEE 802.11 MAC using a 2.4GHz single interface with data rate of 11Mbps. The transmission coverage of each node is 250 meters, and 9 to 36 nodes are randomly deployed inside a 1500 * 1500 m network. Each node starts roaming the network at a preconfigured speed from 1 to 9 m/s, using random waypoint mobility model. Each scenario was simulated and averaged 10 times, with each simulation running for duration of 1000 seconds. The interval for authentication beaconing is 1 second. The proposed scheme is compared with the original EAP-TLS mutual authentication scheme. The authentication message overhead count is compared, which represents the total control packet message overhead induced in the network to maintain connection between nodes. The results can be seen in Figure 3. Since the performance of centralized server based authentication is essentially worse compared to the mutual authentication schemes, they are omitted from comparison.

In Figure 3 (a), we compare the performance of two schemes while increasing the number of nodes, node mobility fixed to 1 m/s, *Key_hop_count* threshold to 2 hops, and key expiration time limit to 2 seconds. We can observe that as the number of nodes increases in the network, the performance of the propose scheme increases dramatically, as it can guarantee overhead decrease of more than 55%. This is because the cooperated mutual authentication scheme can effectively reduce the authentication process. As the number of nodes increase, the secure key broadcast can reduce the number of handshaking while the original EAP-TLS attempts handshaking for each node in the one-hop vicinity. We can observe that the message overhead count value with 16 nodes is actually smaller than that with 9 nodes. This is because when there are only 9 nodes in the network, not many nodes can benefit from substitute authentication. However, when there are 16 or more nodes in the network, the substitute authentication can simplify the overall authentication process, reducing the total overhead induced from control messages.



(a) vs number of nodes (b) vs node mobility

(c) vs *Key_hop_count* threshold (d) vs key expiration time limit

Figure 3. Evaluation of proposed scheme (Comparison of authentication overhead)

In Figure 3 (b), the mobility of nodes is changed while number of nodes is fixed to 25. We can observe that the overhead of authentication reduces while the mobility of nodes increases. This is because the increase in the mobility disconnects the connectivity between nodes and prevents any more authentication process between them. Therefore, the overall authentication process in the network also decreases. We can observe that the benefit of the mobility is much greater in our proposed scheme, performing better than its counterpart by more than 3 times at best. We can see that the overall overhead decreases when the mobility increases.

Figure 3 (c) shows the performance of the two schemes while varying the *key_hop_count* threshold. As the original authentication does not attempt cooperated authentication, this value does not have any effect on its performance. However, we can see that the increasing this value for the propose scheme can improve its performance greatly. It can be observed that in the network of 25 nodes in a 1500 * 1500 network area, the *key_hop_count* threshold of 3 can be empirically thought as the ideal value. While the threshold of 5 can also provide identical results, it can also increase the complexity of the key sharing scheme as useless keys may be propagated too much.

Figure 3 (d) shows that the variation of key expiration time limit can also affect the performance of the two schemes. Regardless of the time limit, the performance of our proposed scheme is superior, thereby providing better support for various security parameters that may be needed depending on the network environment. In overall, the proposed scheme manages to successfully decrease the total security overhead in the wireless network, providing better wireless environments while also guaranteeing security.

5. Conclusion

We have proposed a cooperated mutual authentication scheme in tactical networks that can maintain high level of security while reducing the overhead in the network to provide more reliable networking between soldiers on battlefield. The main contribution of our work is that we have reduced the authentication overhead (complexity and transmission overhead) through our proposed cooperated mutual authentication scheme. The main application of our proposed scheme is mainly focused on the MBS of tactical systems such as the Wideband Network Waveform (WNW) in JTRS or the Mobile Subscriber Access Point (MSAP) in the TICN. However, it can also be applied in different applications and areas of network. In the future, we will attempt to utilize the mobility information and design mobility models and prediction algorithms to further reduce authentication overhead. Also, we will undergo more extensive evaluation studies to better analyze our scheme.

Acknowledgements

This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency (NIPA-2012-(H0301-12-2003)) and National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (2012-003573)

References

[1] Y. Son, K. Lim, T. Shon and Y. Ko, Proceedings of the 2012 International Conference on Information Science and Technology, Edited by A. Stoica and J. Kang, Shanghai, China, **(2012)** April 28-30.
[2] A. Feickert, "UNT Digital Library", Congressional Research Service, Library of Congress, Washington D.C., **(2005)**.
[3] B. Kimura, C. Carden and R. North, Proceedings of the IEEE Military Communications Conference, edited by P. Bocon, San Diego, CA, **(2008)** November 17-19.
[4] K. T. Nath, D. Kim and S. Choi, Proceedings of the IEEE 71st Vehicular Technology Conference – Spring, edited by J. Wu, Taipei, Taiwan, **(2010)** May 16-19.
[5] D. Kim and S. Choi, Proceedings of the 2011 IEEE Wireless Communications and Networking Conference, edited by M. Addali, Cancun, Mexico, **(2011)** March 28-31.
[6] J Huang and C. Huang, Proceedings of the IEEE International Conference on Communications, edited by N. Uji, Kyoto, Japan, **(2011)** June 5-9.
[7] B. Aboba, D. Simon, IETF RFC, 2716, **(1999)**.
[8] H. Jin, L. Tu, G. Yang and Y. Yang, Proceedings of the IEEE International Conference on Computer and Electrical Engineering, edited by K. Jusoff, L. Capretz and R. Voyles, Phuket, Thailand, **(2008)** December 20-22.
[9] M. Lee, J. Zheng, Y. Ko and D. Shrestha, IEEE Wireless Communications, vol. 13, no. 56, **(2006)**.
[10] B. O'Hara and A. Petrick, IEEE 802.11 Handbook: A Designer's Companion, Wiley-IEEE Press, New Jersey, **(2005)**.

Authors

Yu-Jin Son received B.S. in information and computer engineering from Ajou University, Korea in 2010. She has recently received her M.S. in computer engineering in 2012. She is now a researcher in LG U-Plus. Her research interests are in the areas of wireless networking, tactical networks, and wireless security.

Taeshik Shon received his Ph.D. degree in Information Security from Korea University, Korea. From Aug. 2005 to Feb. 2011, Dr. Shon had been a senior engineer in the Convergence S/W Lab, DMC R&D Center of Samsung Electronics Co., Ltd. He is currently a professor at the Division of Information and Computer Engineering, at Ajou University, Korea. He is serving in editorial activities in journals published by Elsevier, Springer, Wiley InterScience, and KIISC. His research interests include Convergence Platform Security, Mobile Cloud Computing Security, Mobile/Wireless Network Security, WPAN/WSN Security, anomaly detection algorithms, and machine learning applications. Information on his various achievements and best paper awards can be found at http://ics.ajou.ac.kr.

Young-Bae Ko is currently a Professor in the School of Information and Computer Engineering at Ajou University, Korea, leading the Ubiquitous Networked Systems Lab. Prior to joining Ajou University in 2002, he was with the IBM T. J. Watson Research Center, New York, as a research staff member in the Department of Ubiquitous Networking and Security. He received his Ph.D. degree in computer science from Texas A&M University. His current research interests are in ad hoc/mesh networks and content centric networks. He was the recipient of a Best Paper award from ACM Mobicom 1998. He has served in various activities, most notably as general chair in IEEE SECON 2012 and as editorial board of ACM Mobile Computing and Communications Review. See http://uns.ajou.ac.kr for further details.