Secure and Efficient Communication Method in Rogue Access Point Environments

Bumjoo Park and Namgi Kim*

Dept. of Computer Science, Kyonggi Univ. Korea
parkbumjo@gmail.com, ngkim@kyonggi.ac.kr

Abstract

WiFi networks, which have been widely used along with the explosive increases in the supply of smartphones, can provide high network speeds but cannot prevent user information spills though rogue Access Points (APs). Therefore, the present paper proposes a method to exchange SSL session keys through more secure 3G networks to be used in WiFi networks in order to prevent such spills. In the proposed method, only those session keys to be used in SSLs are exchanged through 3G networks, and the remaining application data is transferred through WiFi networks. Therefore, attacks by rogue APs can be prevented with sufficient use of the speedy and efficient WiFi networks.

Keywords: *rouge AP, Secure Socket Layer, WiFi, 3G, wireless security*

1. Introduction

Along with the explosive increase in smartphones, users have come to install Access Points (APs) that enable easy and fast wireless access to the Internet at home or a place of business without any restrictions [1, 2, 9, 10]. However, as some wireless APs have been imprudently installed and used, the personal information of users with insufficuent security consciousness has come to be easily spilled by malicious users. In particular, rogue APs that are installed by attackers with a view to obtaining users' confidential information have become great threats to wireless Internet security [12].

A method that can be commonly used in web services to prevent hackers' attacks on WiFi networks with low security is encrypting the data exchanged in HTTP protocols using Secure Socket Layers (SSLs) to ensure data confidentiality in communication. However, even when SSLs are used, users' confidential information can be easily extracted using Man in the Middle (MITM) attacks: that is, making rogue APs, using a laptop with a wireless interface installed and seizing the information of users who use those APs. [3] Therefore, recently, studies to detect and block rogue APs have been actively conducted in order to prevent these security hazards. [4] However, this method has problems, because it involves additional overheads, since in order to detect rogue APs, wireless packets should be analyzed and AP lists should be managed, and even when these additional overheads have been added, rogue APs have not been perfectly detected [11-12].

Therefore, unlike previous studies that focused on on the detection and blocking of rogue APs, the present study proposes a method to make SSLs more secure when data is transferred even without detecting rogue APs. The proposed method is to exchange SSL session keys through 3G networks, which are more secure than WiFi networks. Then, it uses WiFi networks with the exchanged session keys so that data can be transferred

* Corresponding Author: Namgi Kim

securely though WiFi networks even without detecting rogue APs. Therefore, communcation can become secure and fast when the proposed method is used, since MITM attacks can be effectively blocked.

2. Background and Related Work

WiFi networks provide mobility and convenience to users by enabling wireless communication. However, they are vulnerable to hacking and information spills, because they provide open wireless communication. To make up for this weakness, web service data can be encrypted for confidentiality using SSLs in HTTPS protocols, as shown in Figure 1 [12].

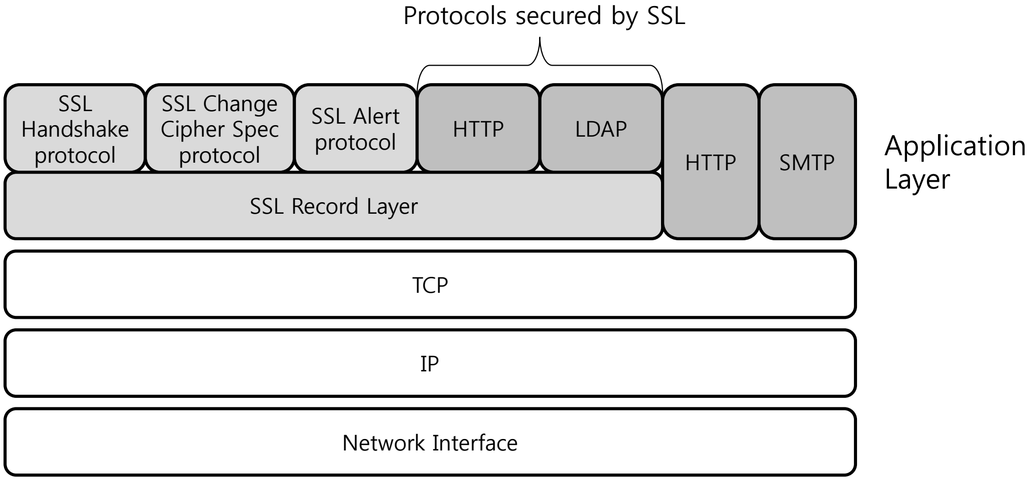


Figure 1. SSL Protocol Architecture

SSLs are protocols that create security connections between clients and servers to encrypt the data being exchanged so that malicious attackers cannot see the data in communication links. To ensure this confidentiality, clients and servers using SSLs exchange authentication keys and encrypt data with the exchanged authentication keys before transferring the data. However, recently, attack methods have been found that enable malicious rogue APs to illegally decrypt encrypted user data by manipulating, in the middle between clients and servers, the process through which authentication keys are transferred. Figure 2 shows a scenario that demonstrates this vulnerable point of SSLs. As can be seen from the figure, a rogue AP serves the role of a proxy in the middle of a client and a server, requesting the server for authentication keys to be used by the rouge APs and sending counterfeit authentication keys created by the rogue AP to the client. Thereafter, the client encrypts data using the counterfeit authentication keys transferred by the rogue AP, and thus the rogue AP can decrypt the data in the middle [12].

As such, if rogue APs are used, weak points in security can be used to hack important user data even when SSLs are used. To prevent this, many studies have been conducted on methods to detect rogue APs. Representative studied methods include methods to detect rogue APs through an AP authentication server [5], methods to detect rogue APs through traffic analysis [6], and methods to detect rogue APs through comparisons of server authentication certificates [7, 12].

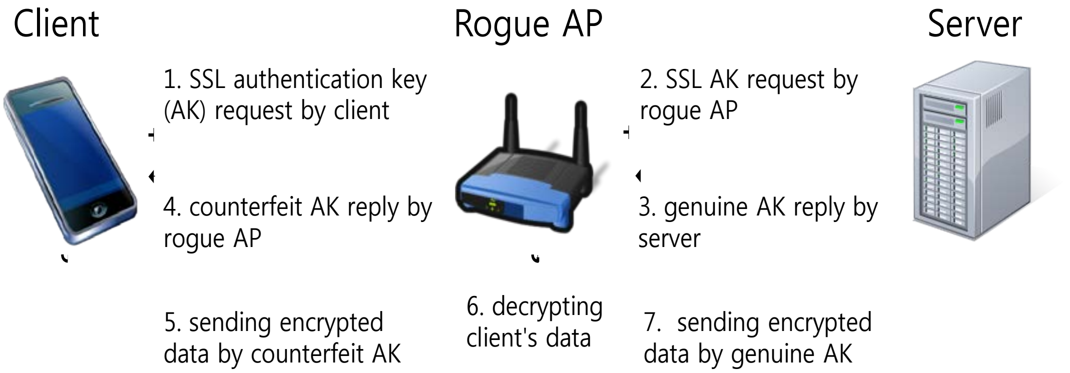

Client
Rogue AP
Server
1. SSL authentication key (AK) request by client
2. SSL AK request by rogue AP
3. genuine AK reply by server
4. counterfeit AK reply by rogue AP
5. sending encrypted data by counterfeit AK
6. decrypting client's data
7. sending encrypted data by genuine AK

Figure 2. Rogue APs' Attacking Method [12]

Rogue AP detection methods using a radius authentication server [5] reinforce security by storing the MAC addresses of authenticated APs in an authentication server and blocking those APs for which the users have not been registered in the authentication server. However, these methods are disadvantageous, in that the MAC addresses of APs that may be registered in the authentication server must be periodically maintained and managed, and none of the public APs that have not been maintained and managed can be used. In addition, these methods cannot detect rogue APs that have reproduced even the MAC addresses. Second, some methods [6] detect rogue APs by analyzing the characteristics of the traffic in routers. These methods scan the source IP address and source port number of the transferred data and judge whether the source host is an authenticated host or a rogue AP by analyzing the characteristics of wireless and wired packets. However, these methods are disadvantageous too, in that to detect and block rogue APs, a traffic analysis module should be installed in each router device, and information should be collected and analyzed every time through the traffic analysis module. Finally, there is a method to detect rogue APs by receiving a server's authentication keys through more secure networks such as 3G networks and comparing them with authentication keys received through WiFi networks [7]. This method is the most similar to the method proposed in the present paper. In this method, when the authentication keys of a server received through heterogeneous networks are different from each other, the AP used in the relevant WiFi network is judged to be a rogue AP and is not used. However, if an AP received through a WiFi network is judged to be a rogue AP, the WiFi network, which is fast, will not used anymore, and thus network efficiency will be decreased. On the contrary, in the case of our method, since authentication keys securely received by 3G networks are immediately used again in WiFi networks, WiFi networks can be securely utilized without detecting rogue APs that may be inaccurate while requiring large overheads [12].

3. Proposed Method

3G networks such as WCDMA provide user authentication security, network access control, data and signaling protection, and data integrity between users' USIMs and base stations [8]. Therefore, 3G networks that use base stations maintained and managed by mobile service providers can be said to provide much higher security than WiFi networks that use APs arbitrarily installed without any centralized control. In the present paper, a method is proposed that can solve rogue AP-related security problems by exchanging SSL session keys to be used in WiFi networks through 3G networks when web services are provided through SSLs. In the proposed method, users can employ WiFi networks more securely and efficiently, even without detecting rogue APs.

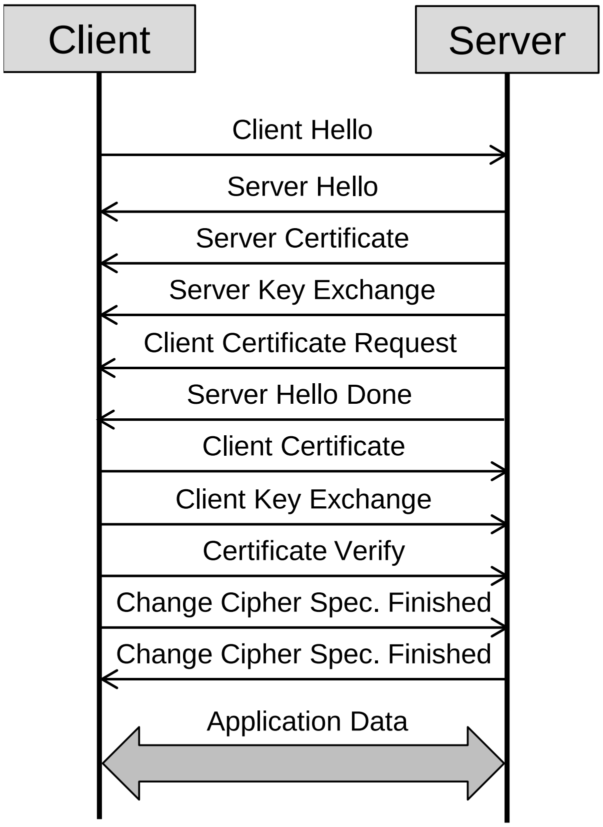


Figure 3. SSL Handshake Protocol

The proposed method exchanges session keys used in SSLs through 3G networks and reuses the exchanged session keys in WiFi networks in order to prevent MITM attacks by rogue APs. These SSL session keys are exchanged through SSL handshake protocols. A handshake protocol consists of Hello, Certificate, Key, and Finished message exchange procedures, as shown in Figure 3. In the protocol, if the client and server have not yet shared the session key, the session ID field in the Client Hello message will be set to 0 and delivered to the server. Then, the server will create a session ID and deliver it to the client through a Server Hello message. Thereafter, the server will share the session key with the client through the handshake protocol. If the client and the server have already shared a session key, the client will deliver the session ID through a Client Hello message to use the session key shared earlier. Therefore, the present paper provides a secure and fast communication method in rogue AP environments, since handshake protocols are implemented using 3G networks when session keys are shared, and the session keys created are reused in WiFi networks.

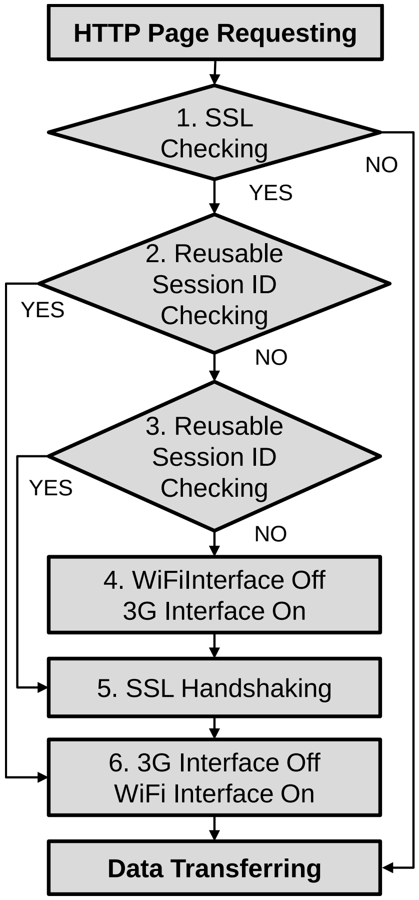

HTTP Page Requesting
1. SSL Checking
NO
YES
2. Reusable Session ID Checking
YES
NO
3. Reusable Session ID Checking
YES
NO
4. WiFiInterface Off 3G Interface On
5. SSL Handshaking
6. 3G Interface Off WiFi Interface On
Data Transferring

Figure 4. Flowchart of Proposed Method

The proposed method can be implemented in smart devices through network interface switching without changing SSL, 3G network, or WiFi network standards. Figure 4 shows a flowchart of the proposed communication method. If the use of any SSL is detected during wireless communication, the client will check if there has been any valid session ID created previously. If there is no valid session ID, the user will set the network interface to 3G network and follow SSL handshake procedures to obtain a valid session key and ID from the server. Thereafter, the user will switch the network interface to the WiFi network and encrypt the data through the session key shared with the valid session ID. Through these processes, the SSL authentication session key will be securely exchanged, and rogue APs will not be able to use MITM attacks to access any of data transferred through the WiFi network.

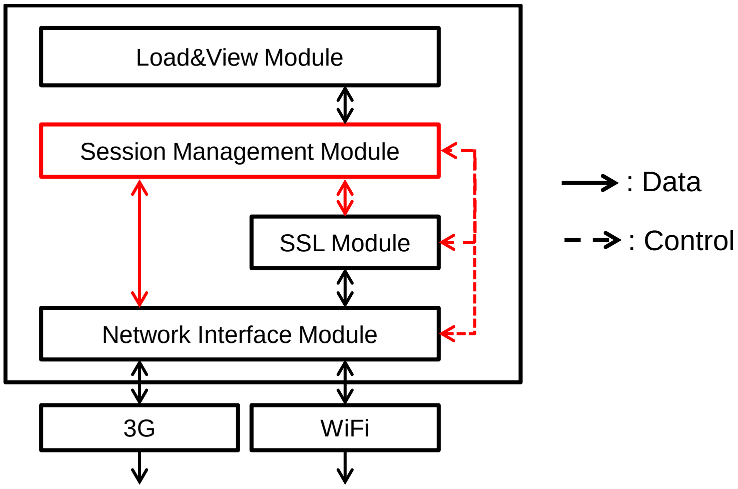


Figure 5. Browser Architecture for the Proposed Method

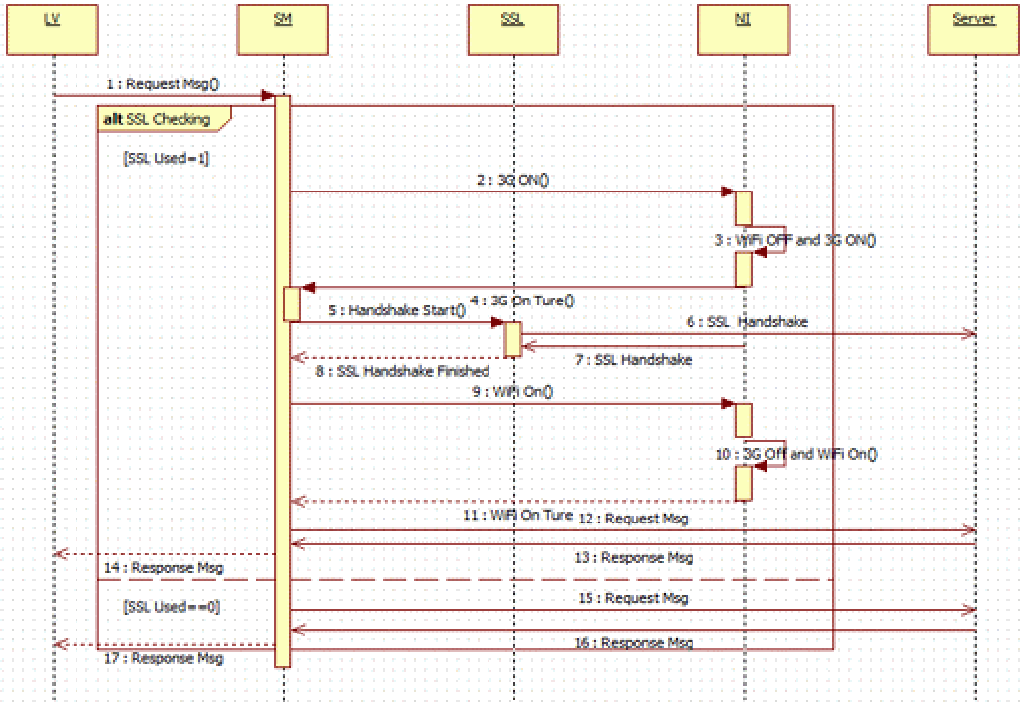


Figure 6. Sequence Diagram for Proposed Method

Figure 5 shows the browser architecture for implementing the proposed method. The Load&View (LV) module serves the role of showing the data received from a server through page loading on the screen, and the SSL module implements the SSL protocol. The Network Interface (NI) module serves the role of switching network interfaces to 3G or WiFi. The Session Management (SM) module is a core module for implementing the proposed method. It detects whether SSLs are used in browsers and issues commands to the NI module requesting a check of network interface statuses or switching network interfaces in accordance with the flowchart described earlier.

Figure 6, as a sequence diagram, shows the mutually exchanging actions of the four modules in the browser architecture described earlier.

4. Performance Evaluation

Figure 7 shows the results of an implementation of the proposed method. It can be seen that 3G networks are activated for key exchanges when the device logs in at the homepage http://www.naver.co.kr and that the device is connected to WiFi networks later when it receives data.

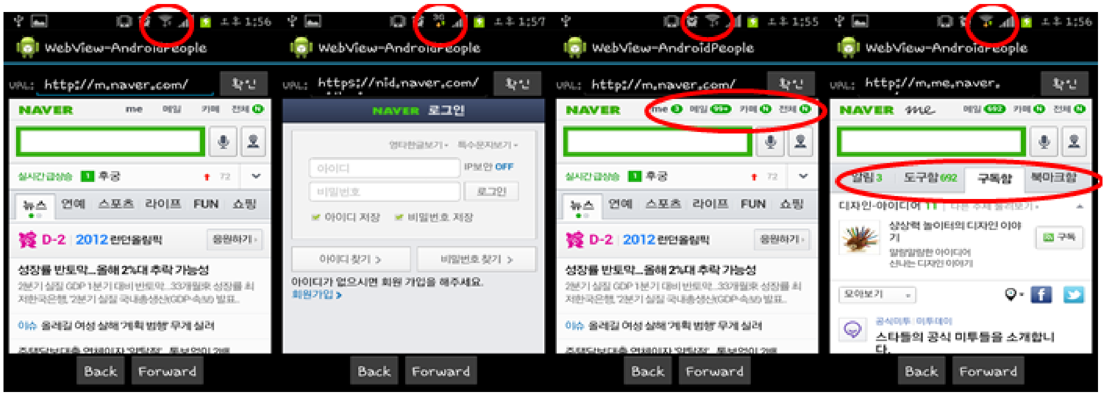


Figure 7. Example of Implemented Browser

Next, network performances were measured through actual experiments when the proposed method, a 3G network only, and WiFi network only were used. To this end, first, the performances were measured using a Samsung Galaxy S2 smartphone when the speeds of the 3G and WiFi networks were Low, Middle, and High, separately. Then, 2.6MB of experimental data was collected from two services, Facebook and Gmail, to measure the network performance in each environment.

Table 1 shows data loading times taken to receive 2.6 MB of data from Facebook at each network speed. As can be seen in the figure, WiFi Only shows the best performance in all sections, while 3G Only shows the poorest performance. The proposed method shows performances in between the performances of 3G Only and WiFi Only, because the proposed method exchanges SSL handshake data through 3G networks and application data through WiFi networks. In particular, the reason why these differences in performance appear, despite that the amount of SSL handshake data is much smaller compared to application data, is that the interface switching time between 3G and WiFi networks - 5 seconds in total (two instances of 2.5 seconds per time) is included. However, since the switching time varies with the kind of smart devices and will keep decreasing along with technical development, it is expected that the proposed method will be able to show gradually improving performances.

Table 1. Data Loading Time with Three Network Speeds

	Low	Middle	High
WiFi	1,284 KB/s	2,156 KB/s	3,086 KB/s
3G	260 KB/s	300 KB/s	468 KB/s
WiFi Only	2.12s	1.26s	0.88s
3G Only	10.45s	9.06s	5.81s
Proposed (5sec)	7.13s	6.27s	5.89s

Figure 8 shows data loading times in relation to network interface switching times that are different by smart device. As can be seen through the figure, the loading time of the proposed method decreases greatly as the switching time decreases.

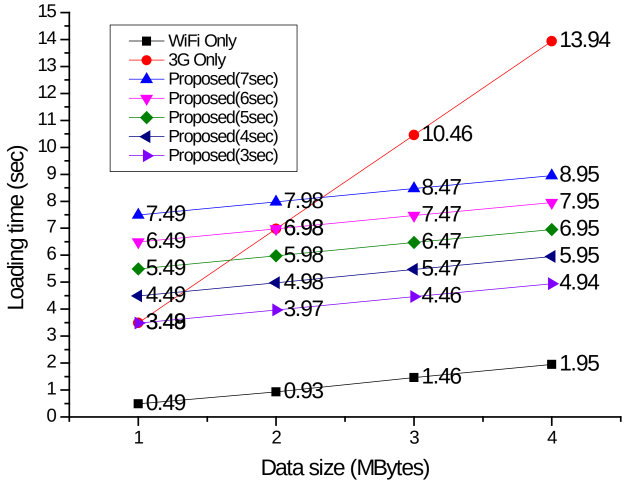


Figure 8. Loading Time

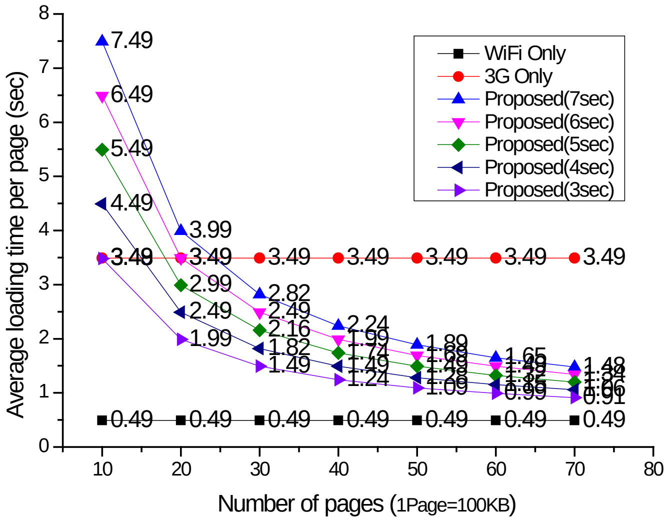


Figure 9. Average Page Loading Time

The proposed method requires network switching time only for the initial SSL connection, because after negotiating an SSL authentication key through initial switching, no more switching to 3G networks is necessary when using the relevant service. Figure 9 shows average page loading times by the number of pages. As can be seen from the figure, when 10 pages of data are loaded at a time, the initial network switching time occupies a large portion of the entire loading time, and thus the proposed method shows a poorer performance than 3G Only or WiFi Only. However, the proposed method is affected less by the initially spent network switching time as the number of loading pages increases, and thus application data increases. Therefore, the proposed method's performance becomes similar to that of WiFi Only as the amount of data increases.

4. Conclusion

The present paper proposes a method to communicate more securely while utilizing the efficiency of WiFi networks. The method exchanges session keys to be used in SSLs through 3G networks, which are more secure than WiFi networks and uses the keys in WiFi networks for transferring application data. So, through only simple network switching and no additional overhead for detecting rogue APs, the proposed method utilizes fast WiFi networks more securely where rogue APs may exist. For the future work, we will fully implement our proposed method into the popular web browsers in smartphones such as safari and chrome.

Acknowledgements

This work was supported by Kyonggi University Research Grant 2012.

References

[1] V. Shnayder, B. Chen, K. Lorincz, T. R. F. Fulford-Jones and M. Welsh, "Sensor Network for Medical Care", TR-08-05, Harvard Univ., **(2005)**.

[2] IEEE: Information technology-Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Standard 802.11, **(1999)**.

[3] B. P. Crow, I. Widjaja, J. G. Kim and P. T. Sakai, IEEE 802.11 Wireless Local Area Networks, IEEE Communications Magazine, vol. 35, no. 9, **(1997)**, pp. 116-126.

[4] Wikipedia: Rogue Access Point, http://en.wikipedia.org.

[5] R. Beyah, "Rogue Access Point Detection Challenges, Solutions, and Future Directions", IEEE Security and Privacy Article, IEEE, vol. 9, no. 5, **(2011)**, pp. 56-61.

[6] D. -P. Kim, Z. Jiang and S. -W. Kim, "Rogue AP Protection System based on Radius Authentication Server", in Proc. of KISS Spring Conferences (A), **(2004)**, pp. 316-318.

[7] S. Shetty, M. Song and L. Ma, "Rogue Access Point Detection by Analyzing Network Traffic Characteristics", Proc. of Milcom, **(2007)**.

[8] J. Lee, C. Tu and S. Jung, "Man-in-the-middle Attacks Detection Scheme on Smartphone using 3G Network", in in Proc. of IARIA, **(2012)**.

[9] S. -I. Jun, Y. -S. Kim, J. -H. Han, K. Chung and S. -W. Son, "Interworking Security for Public WLAN, WiBro and WCDMA: Mobile and Wireless Systems", Information and Communications Magazine, KICS, vol. 22, no. 8, **(2005)**, pp. 63-80.

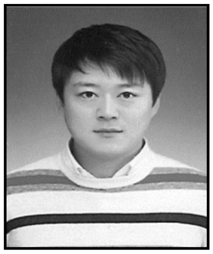
[10] C. -W. Lee, J. C. L. Liu, K. Chen, Y. -C. Tseng and S. P. Kuo, "System study of the wireless multimedia ad-hoc network based on IEEE 802.11g", International Journal of Security and Its Applications, vol. 2, no. 2, **(2008)** April, pp. 23-40.

[11] T. Janevski and I. Petrov, "Cross-layer analysis of transport control protocols over IEEE 802.11 wireless networks", International Journal of Advanced Science and Technology, vol. 26, **(2011)** January, pp. 1-18.

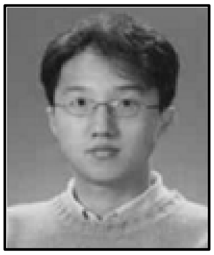
[12] A. Panch and S. K. Singh, "A novel approach for evil twin or rogue AP mitigation in wireless environment", International Journal of Security and Its Applications, vol. 4, no. 4, **(2010)** October, pp. 33-38.

[13] B. Park and N. Kim, "A Study of secure communications in WiFi networks", Proceedings of Advanced Science and Technology Letters, **(2013)** April.

Authors



Bumjo Park received the B.S. degree in Computer Science from Kyonggi University, Korea, in 2011, and the M.S. degree in Computer Science from Kyonggi University in 2013. His research interests include wireless systems and mobile communication.



Namgi Kim received the B.S. degree in Computer Science from Sogang University, Korea, in 1997, and the M.S. degree and the Ph.D. degree in Computer Science from KAIST in 2000 and 2005, respectively. From 2005 to 2007, he was a research member of the Samsung Electronics. Since 2007, he has been a faculty of the Kyonggi University. His research interests include sensor system, wireless system, and mobile communication.