Study on a Secure Wireless Data Communication in Internet of Things Applications

Chibiao Liu, Jinming Qiu

IOT Application Engineering Research Center of Fujian Province Colleges and Universities,
School of Information Engineering, Sanming University, Sanming 365004, China

Summary
Internet of Things (IOT) applications are being widely deployed in many industrial and social fields, and guarantee of the safety of IOT related data transmission is the key for successful IOT related businesses. Our study provides a new way to secure the data transmission of the Wireless Local Area Network (WLAN) related IOT applications. The WLAN-based IOT application is mainly composed of WLAN sensor nodes, the WLAN gateway, transmission networks and the data service center. The WLAN gateway collects data from sensor nodes in real-time and sends the collected data to the data service center via the transmission network. Since many WLAN-based IOT applications involve critical services, such as power, water, industry productions and health care, the data transmission between the wireless gateway and the data service center is required to be secured for preventing crypto attacks, such as traffic analysis, man in the middle, session hijack, unauthorized access, masquerading, eavesdropping, replay, tampering and forgery. In this paper, we propose an integrated approach to secure the data transmission of the WLAN-based IOT applications. Meanwhile, we conduct experiments and theoretical analysis to study the performance of the proposed integrated security approach; it shows that the integrated approach is a new and effective way to secure the data transmission of the WLAN related IOT applications.

Key words:
Internet of things, Wireless security attacks, Secure data transmission, Performance overhead

1. Introduction

Since 2009, Internet of Things (IOT) applications have been used in many fields closely related to industry, agriculture, business, education, healthcare and finance [1-8]. As shown in Figure 1, due to its low cost, long transmission distance, high bandwidth, easy networking and low power consumption, the WLAN data communication has been widely used in many kinds of IOT applications, such as industrial production line monitoring, city safety inspection, food logistics monitoring, fire rescue monitoring, power monitoring, oil monitoring, environmental monitoring, school safety monitoring and community safety monitoring [9-12]. An IOT application is mainly composed of nodes, gateways, data transmission networks and the data service center.

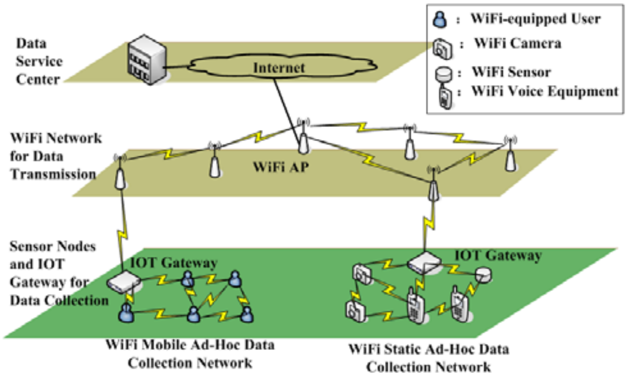
WiFi-equipped User
WiFi Camera
WiFi Sensor
WiFi Voice Equipment
Data Service Center
Internet
WiFi Network for Data Transmission
WiFi AP
Sensor Nodes and IOT Gateway for Data Collection
IOT Gateway
IOT Gateway
WiFi Mobile Ad-Hoc Data Collection Network
WiFi Static Ad-Hoc Data Collection Network

Fig. 1 WiFi-based IOT applications

IOT nodes refer to those devices that can generate real-time environmental data, such as voice, image, noise, temperature, humidity, power, emission, light and pressure. Nodes connect with the gateway through wired or wireless media, and the gateway collects various kinds of data from nodes. Meanwhile, as shown in Figure 2, the IOT gateway can send the collected data to the data service center through the data transmission network, such as WLAN, wired LAN and 3G/4G mobile networks.

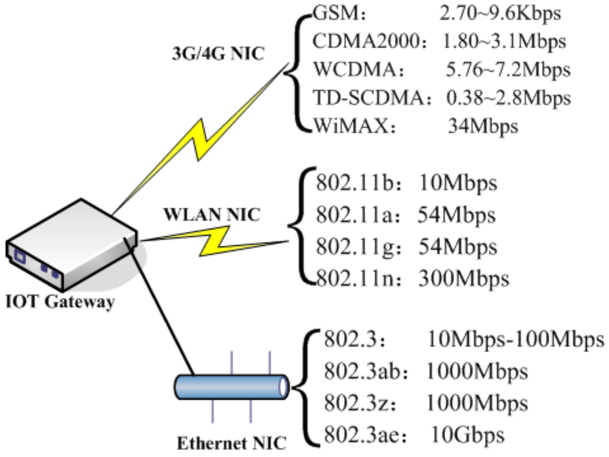

Fig. 2 Network interface cards (NIC) for an gateway

Since many WLAN-based IOT applications involve critical services, the data transmission between the IOT

Manuscript received February 5, 2015
Manuscript revised February 20, 2015

gateway and the data service center is required to be secured to prevent from crypto attacks, such as traffic analysis, man-in-the-middle, session hijack, unauthorized access, masquerading, eavesdropping, replay, tampering and forgery [13-16]. The wireless security technologies of Wired Equivalent Privacy (WEP), WEP-802.1X, Virtual Private Network (VPN) /WEP-802.1X or 802.11i alone is not sufficient to address all major WLAN crypto attacks of eavesdropping, tampering, masquerading, replay and forgery, and there is an urgency to find new way to protect the wireless data transmission in IOT applications.

As shown in Figure 3, in this paper, we propose an integrated approach of VPN over 802.11i (Temporal Key Integrity Protocol: TKIP or Counter CBC-MAC Protocol: CCMP) to secure the IOT data transmission between the wireless gateway and the IOT data service center, and this securing approach can prevent wireless attacks, such as traffic analysis, man-in-the-middle, session hijack, unauthorized access, masquerading, eavesdropping, replay, tampering and forgery.

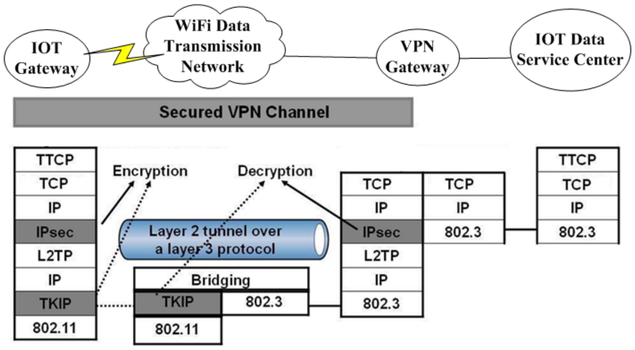

Fig. 3 Protocol stack of VPN/TKIP secured TCP traffic for an IOT application

We conduct experiments and theoretical analysis to study the performance of VPN, and VPN/802.11i to evaluate their impacts on the WLAN-based IOT applications. The study shows that the integrated security approach can provide strong protection for the WLAN-based IOT applications without causing obvious performance overheads, which shows that VPN over 802.11i is a new and effective way to secure the data transmission of the WLAN related IOT applications.

The rest of this paper is organized as follows. In section 2, we present the experiments and the methodologies. In section 3, we discuss the performance overheads of the TCP data communication between the wireless gateway and the IOT data service center. Theoretical analysis of performance overheads is given in section 4. The conclusions are given in section 5.

2. Experiments and Methodologies

We implemented a prototype at the lab to study the performance of the integrated approach of VPN over 802.11i for securing the data communication between the wireless gateway and the IOT data service center. This prototype consists of one access point (AP), one VPN gateway, one RADIUS server, two Ethernet switches, and three workstations (WS) as illustrated in Figure. 4.

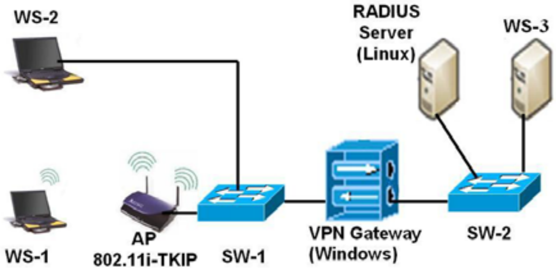

Fig. 4 Experimental design for performance measurements on the IOT data transmission

The VPN gateway is running on a Windows 2008 Enterprise Sever, and it is configured with the options of IPSec/L2TP and Point to Point Tunneling Protocol (PPTP). IPSec/L2TP and PPTP use MS CHAP v2 for user authentications. PPTP VPN uses Microsoft Point to Point Encryption (MPPE) 128 to encrypt data. To secure data communication, IPSec/L2TP uses Encapsulating Security Payload (ESP) and Triple Data Encryption Standard (3DES). The freeRadius server is running on a Linux machine. The RADIUS server is for user authentication of both 802.1X and VPN. The AP is a Netgear WNDR3700, and it supports 802.1X, 802.11i-TKIP and other security protocols. WS-1 represents a wireless IOT gateway, which is equipped with a Linksys 802.11 b/g wireless adapter that supports data encryption (TKIP) and user authentication (802.1X). WS-2 is for baseline measurements, and it is a Windows 7 machine with PPTP and L2TP VPN clients. WS-3 is a Windows 7 machine representing a server at the IOT data service center.

3. Performance Overheads of the TCP Data Communication

In this section, it first presents the TCP throughput results of different security approaches to secure the TCP data communication between the IOT gateway and the IOT data service center, and the performance study also includes the baseline data of the WLAN-based IOT applications with no security protections (None Encryption: Nonenc). The TCP throughputs under the protections of different security approaches are shown as Table 1.

In Table 1, the security approach of "*Nonenc*" means that there is no protection for the data transmission between the IOT gateway and the data service center. The protocol stack for the "*Nonenc*" wireless configuration is shown in Figure 5. Figure 5 shows that the IOT gateway sends TCP data to the data service center without protection of TKIP or the VPN security approach. As shown in Table 1, without any protection, the data transmission might have better TCP throughputs; however, it has the highest security vulnerabilities.

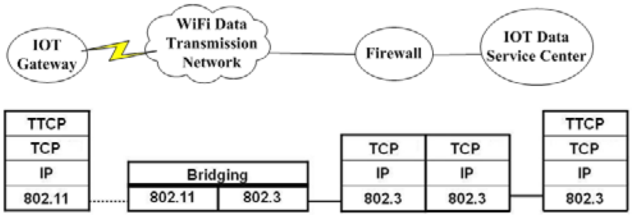

Fig. 5 Protocol stack of the TCP traffic for an IOT application without protection

In Table 1, the security approach of TKIP means that the data transmission the IOT gateway and the IOT data service center is protected only with TKIP. The protocol stack of the TKIP secured wireless TCP communication is shown in Figure 6.

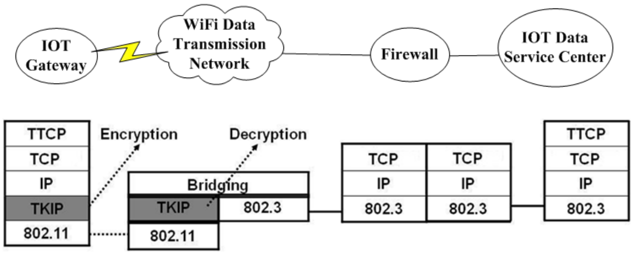

Fig. 6 Protocol stack of the TCP traffic for an IOT application with TKIP protection

Table 1: TCP throughputs under the protections of different security approaches

Network type	Security approach	TCP throughput (Mbps)
802.11b	Nonenc	5.43
802.11b	TKIP	5.26
802.11b	PPTP	5.24
802.11b	L2TP	5.06
802.11b	TKIP /PPTP	4.67
802.11b	TKIP /L2TP	4.66
802.11g	Nonenc	18.07
802.11g	TKIP	17.24
802.11g	PPTP	16.21
802.11g	L2TP	14.65
802.11g	TKIP /PPTP	15.43
802.11g	TKIP /L2TP	14.49

Meanwhile, the security approach of PPTP or L2TP means that the data transmission between the IOT gateway and the IOT data service center is protected with the VPN approach of PPTP or L2TP. The protocol stack of the VPN secured data communication is shown in Figure 7.

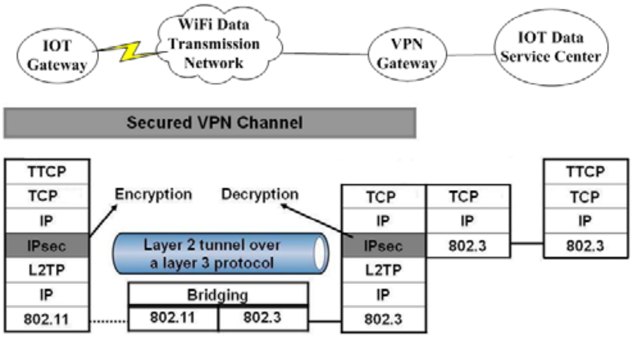

Fig. 7 Protocol stack of the TCP traffic for an IOT application with VPN protection

We use VPN approaches of PPTP and L2TP to secure TCP traffic. Without protection, the TCP throughput for 802.11b and 802.11g are 5.43 Mbps and 18.07 Mbps, respectively. These values are consistent with other published results [17-19]. Furthermore, Table 1 shows that the adoption of PPTP or L2TP has little impact on the performance of the 802.11b/g wireless data communication. With enabling the integrated approach of TKIP and VPN, we further measured TCP throughputs of TKIP and VPN/TKIP. Compared with TKIP, the integrated security approach does not cause much performance degradation.

We use TH_enc and TH_nonenc to represent the TCP throughput with and without security protection, respectively. The performance overhead of a security approach can be defined as Eq. (1). The comparison of performance degradation due to security protection is summarized in Table 2.

$$Overhead(\%) = \frac{(TH\_nonenc - TH\_enc)}{TH\_nonenc} * 100\% \quad (1)$$

Table 2: TCP performance overheads of different security approaches

Network type	Security approach	TCP performance overhead (%)
802.11b	L2TP	6.8
802.11b	PPTP	3.4
802.11b	TKIP	3.1
802.11b	TKIP /L2TP	14.2
802.11b	TKIP /PPTP	14.0
802.11g	L2TP	18.9
802.11g	PPTP	10.3
802.11g	TKIP	4.6
802.11g	TKIP /L2TP	19.8
802.11g	TKIP /PPTP	14.6

Table 2 shows that the overhead of VPN on the wireless network (e.g. 802.11b/g) is small. For example, the performance overhead of L2TP for 802.11b is 6.8%, which shows that the integrated security approach can provide strong protection for the WLAN-based IOT applications without causing obvious performance overheads. In the following section, we will theoretically analyze the performance overheads of different security approaches.

4. Theoretical Analysis of Performance Overheads

4.1 TCP Throughput Analysis

In this section, we first derive the equation to calculate the TCP throughput. Then, we combine the throughput equations with Eq. (1) to calculate the overhead under different security configurations. Based on similar model as described in the published literatures [19-21], the TCP data exchange between the TCP data sender and the TCP data receiver is illustrated in Figure 8.

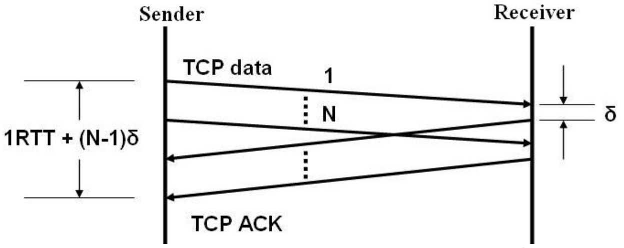

Fig. 8 TCP communication with the window size of N

In Figure 8, the RTT refers to the round trip time(RTT), and δ refers to the protocol processing time at the receiver. The RTT is equal to the total time for sending one TCP data packet from the Sender to the Receiver, and sending the TCP ACK packet from the Receiver to the Sender. Fig. 2 shows that there are N TCP data packets exchanged between the Sender and the Receiver within the time of 1 RTT + (N-1)δ. Then, the TCP throughput can be expressed as Eq. (2). In Eq. (2), TH is the TCP throughput in million bits per second (Mbps), MSS is the number of data bits in a maximum segment size (MSS) (units=bits), RTT and δ have a unit of second, N is the TCP window size, which has a value of 2 or 3 in our measurements. Assuming that the value of RTT is much bigger than that of (N-1)δ, Eq. (2) can be further derived as Eq. (3). Two cases of TCP throughput derivations will be discussed as follows.

$$TH = \frac{MSS * N}{RTT + (N-1)\delta} \qquad (2)$$

$$TH = \frac{MSS * N}{RTT} \qquad (3)$$

Case 1) Throughput derivation for the non-secured wireless TCP data communication. The TCP RTT time components for normal wireless communication mainly include propagation time and wireless transmission time. The transmission time at the wireless station is denoted as T_tr(wlan). Assuming that the propagation time of TCP data and ACK packets over the air and the wire is negligible, applying T_tr(wlan) into Eq. (3), the TCP throughput is derived as Eq. (4).

Case 2) Throughput derivation for the VPN-secured wireless TCP communication. For this scenario, the RTT time components for processing TCP packets include propagation time, wireless transmission time, and VPN processing time. At the wireless station, the encryption time is T_vpn. The wireless transmission time is T_tr(wlan). Assuming that the propagation time is negligible, the RTT for the VPN-secured wireless TCP data communication is equal to T_tr(wlan) + T_vpn. Applying this RTT into Eq. (3), the throughput for the VPN-secured wireless TCP traffic is derived as Eq. (5).

$$TH\_nonenc\_wireless = \frac{MSS * N}{T\_tr(wlan)} \qquad (4)$$

$$TH\_\mathrm{enc}\_wireless = \frac{MSS * N}{T\_vpn + T\_tr(wlan)} \qquad (5)$$

4.2 TCP Data Encryption and Transmission Time

As discussed above, throughputs for wireless data communications can be calculated with the transmission time and encryption time. The encryption time is closely related to encapsulation and encryption overhead, which is different for different encryption algorithms. The data structures of L2TP and PPTP are illustrated in Figure 9.

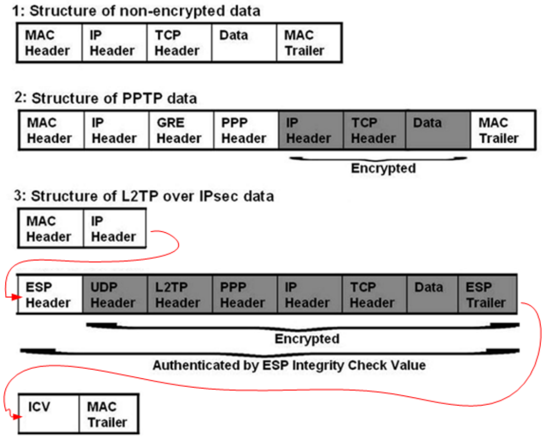

Fig. 9 Data structures used by different security approaches

Figure 9 shows that the VPN security approaches of L2TP and PPTP have different protection mechanisms. The encryption algorithm and the implementation method are two major factors determining encryption time. For different encryption algorithms, a slower one leads to a longer encryption time. PPTP uses RC4 encryption algorithm, which is much faster than the triple Data Encryption Standard (3DES) encryption algorithm used by L2TP VPN [21]. Meanwhile, PPTP adds fewer headers than L2TP does. Let T_vpn(pptp) and T_vpn(l2tp) represent the packet encryption time for PPTP and L2TP-IPsec, respectively, and we have the sequence of encryption time as T_ vpn(pptp) < T_ vpn(l2tp).

The transmission time is related with the packet size and network capacity. For an 802.11b WLAN, the average TCP throughput is 5.5Mbps [17]. For a TCP packet of 1460 bytes, the average transmission time for the 802.11b WLAN, is (1460*8bits)/5.5Mbps as 2124 µs. For an 802.11g WLAN, the reported average TCP throughput is 18.8 Mbps [18]. The average 802.11g transmission time for a TCP packet of 1460 bytes, is (1460*8bits)/18.8 Mbps as 621 µs.

4.3 Analysis of VPN Overhead on 802.11 Wireless Network

As discussed in section 4.1, the throughput for the wireless TCP traffic without protection is expressed as Eq. (4). Meanwhile, the TCP throughput with VPN protection is expressed as Eq. (5). Applying TH_nonenc_wireless from Eq. (4) and TH_enc_wireless from Eq. (5) into Eq. (1), the overhead of VPN is derived as Eq. (6). Applying the transmission time of T_tr(wlan-802.11b) of 0.002124 second into Eq. (6), we derive the VPN overhead as Eq. (7). Applying the transmission time of T_tr(wlan-802.11g) of 0.000621 second into Eq. (6), the overhead for the 802.11g WLAN is derived as Eq. (8). The values of T_vpn(l2tp) and T_vpn(pptp) are 0.0001479 second and 0.00007 second, respectively[22]. Applying the values of T_vpn(l2tp) and T_vpn(pptp) in Eq. (7) and Eq. (8), VPN overheads of 802.11 are calculated. The comparison of analytical results and the empirical results is shown in Table 3.

$$Overhead\_vpn(wlan)(\%) = 100*(1-\frac{1}{1+\frac{T\_vpn}{T\_tr(wlan)}}) \quad (6)$$

$$Overhead\_vpn(802.11b)(\%) = 100*(1-\frac{1}{1+471*T\_vpn}) \quad (7)$$

$$Overhead\_vpn(802.11g)(\%) = 100*(1-\frac{1}{1+1610*T\_vpn}) \quad (8)$$

Table 3: Comparison of analytical results and the empirical results of VPN overheads

VPN overheads	Empirical value (%)	Analytical value (%)
Overhead_l2tp(802.11b)	6.8	6.5
Overhead_l2tp(802.11g)	18.9	19.2
Overhead_pptp(802.11b)	3.4	3.2
Overhead_pptp(802.11g)	10.3	10.1

Table 3 shows that the analytical values are close to the empirical values, which means that the theoretical model can be used to explain overheads of VPN for protecting the data transmission of the WLAN related IOT applications.

5. Conclusion

This paper presents both empirical and theoretical analysis of VPN overheads for protecting the data transmission of the WLAN related IOT applications, which provides a justification to use VPN for protecting against wireless attacks of traffic analysis, man-in-the-middle, session hijack, unauthorized access, masquerading, eavesdropping, replay, tampering and forgery. Applying the proposed integrated security approach for protecting the WLAN-based IOT applications will guarantee a higher safety and a higher quality IOT service.

Acknowledgment

This work is supported by the science and technology project of Fujian Province (2013N0031), the Provincial Universities Scientific Research Special Plan of the Education Department of Fujian Province (No. JK2012051), the Fujian Provincial Natural Science Foundation (No. 2012J01283, 2012J01282), and the Provincial Teaching Quality Reform Project - Network Engineering Major Comprehensive Reform (ZL2012ZG4).

References

[1] C.S. Bontu, S. Periyalwar and M. Pecen, “Wireless Wide-Area Networks for Internet of Things: An Air Interface Protocol for IoT and a Simultaneous Access Channel for Uplink IoT Communication,” IEEE Vehicular Technology Magazine, vol.9,pp. 54-63,2014.

[2] O. Bello and S. Zeadally, “Intelligent Device-to-Device Communication in the Internet of Things,” IEEE Systems Journal. vol.PP, pp.1-11, 2014.

[3] J. Jin, J. Gubbi, S. Marusic and M. Palaniswami, “An Information Framework of Creating a Smart City through Internet of Things,” IEEE Internet of Things Journal. vol.1,pp.112-121,2014.

[4] L. Atzori, A. Iera and G. Morabito, “From "Smart Objects" to "Social Objects": The Next Evolutionary Step of the Internet of Things,” IEEE Communications Magazine,vol.52,pp.97-105,2014.

[5] W. He, G. Yan and L. Xu, “Developing Vehicular Data Cloud Services in the IoT Environment,” IEEE Transactions on Industrial Informatics, vol.10,pp.1587-1595,2014.

[6] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi and G. Marrocco, “RFID Technology for IoT-based Personal Healthcare in Smart Spaces,” IEEE Internet of Things Journal, vol.1,pp.144-152,2014.

[7] C. Perera, A. Zaslavsky, C. H. Liu, M. Compton, P. Christen and D. Georgakopoulos, “Sensor Search Techniques for Sensing as a Service Architecture for the Internet of Things,” IEEE Sensors Journal, vol.14,pp.406-420,2014.

[8] V. K. Sehgal, A. Patrick and L. Rajpoot, “A Comparative Study of Cyber Physical Cloud, Cloud of Sensors and Internet of Things: Their Ideology, Similarities and Differences,” 2014 IEEE International Advance Computing Conference (IACC), pp.708-716, 2014.

[9] Li Li, Hu Xiaoguang, Chen Ke and He Ketai, “The Applications of WLAN-based Wireless Sensor Network in Internet of Things and Smart Grid,” 6th IEEE Conference on Industrial Electronics and Applications (ICIEA), pp.789-793, 2011.

[10] S. Tozlu, “Feasibility of Wi-Fi Enabled Sensors for Internet of Things,” 7th International Wireless Communications and Mobile Computing Conference (IWCMC), pp.291-296, 2011.

[11] Chongjoon You, Jaeyoung Lee, Jinyoung Kim and Jun Heo, “Efficient Cooperative Spectrum Sensing for Wi-Fi on TV Spectrum,” 2011 IEEE International Conference on Consumer Electronics (ICCE), pp.903-904, 2011.

[12] Keun-Woo Lim, Young-Bae Ko, Sung-Hee Lee, and Sangjoon Park, “Congestion-aware Multi-gateway Routing for Wireless Mesh Video Surveillance Networks Sensor,” 8th Annual IEEE Communications Society Conference on Mesh and Ad Hoc Communications and Networks (SECON), pp.152-154, 2011.

[13] R. K. Jha, U. D. Dalal and I. Z. Bholebawa, “Performance Analysis of Black Hole Attack on WiMAX-WLAN,” Third International Conference on Interface Network Computer and Communication Technology (ICCCT), pp.303-308, 2012.

[14] A. M. Alabdali, L. Georgieva and G. Michaelson, “Modelling of Secure Data Transmission over a Multichannel Wireless Network in Alloy,” 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp.785-792, 2012.

[15] S. Fahmy, A. Nasir and N. Shamsuddin, “Wireless Network Attack: Raising the Awareness of Kampung WLAN Residents,” 2012 International Conference on Computer & Information Science (ICCIS), vol.2,pp.736-740, 2012.

[16] S. M. K. M. A. Ahmad, E. G. Rajan and A. Govardhan, “Route Optimized Secured and Improved Encryption Protocol for Wireless Ad Hoc Network,” 2012 International Conference on Advances in Mobile Network Communication and its Applications (MNCAPPS), pp.34-38, 2012.

[17] S. Choi, K. Park and C. Kim, “On the Performance Characteristics of WLANs: Revisited,” Proceedings of the 2005 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems, vol.33,pp.97-108, 2005.

[18] J. Gretarsson, F. Li, M. Li, A. Samant, H. Wu, M. Claypool and R. Kinicki, “Performance Analysis of the Intertwined Effects between Network Layers for 802.11g Transmissions,” Proceedings of the 1st ACM Workshop on Wireless Multimedia Networking and Performance Modeling, pp.123-130, 2005.

[19] D. A. Menascé and V. A. F. Almeida, Capacity Planning for Web Performance: Metrics, Models, and Methods, Prentice Hall, 1998.

[20] D. A. Menascé, V. A. F. Almeida and L.W. Dowdy, Performance by Design: Computer Capacity Planning by Example, Prentice Hall PTR, 2004.

[21] D. Menasce, “Security Performance,” IEEE Internet Computing, vol.7,pp.84-87, 2003.

[22] Chibiao Liu, “Empirical Analyses and Queuing Models of Security Attacks Against 802.11 Wireless Local Area Networks,” PhD diss., DePaul University, 2010.

Chibiao Liu is the associate dean of School of Information Engineering, Sanming University. He received Ph.D. degree in computer science from College of Computing and Digital Media at DePaul University, Chicago, USA, in 2010. He has been performing research in the area of wireless security, wireless sensor networks and various applications of Internet Of Things(IOT).

Jinming Qiu, professor, received his M.S. in computer science from Fuzhou University, Fuzhou, China, in 2005. He has been performing research in the area of network security, information fusion, data mining and rough set theory. Currently, professor Qiu is serving as the dean of School of Information Engineering, Sanming University.