Journal of Theoretical and Applied Information Technology
31st December 2012. Vol. 46 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# ANALYSIS OF SECURITY MECHANISM IN WIRELESS CAMPUS NETWORK

**XIULI ZHU, JIEYING LI**
Zhoukou Normal University, Zhoukou 466001 Henan, China

**ABSTRACT**

With the rising number of schools going to built wireless campus networks, the current wireless campus networks cannot protect from increasing illegal network intrusion. This paper presented an improved security mechanism for wireless campus networks. It is based on the analysis of the shortages of current for security mechanism for wireless campus networks, and on the optimization and improvement of data confidentiality agreement, network authentication protocol and access control. And also use CCMP algorithm to encapsulate and encrypt data, present a fast authentication protocol based on public key cryptography and control access in wireless networks' port with the concept of virtual ports. The results show that the security mechanism put forward in this paper can not only protect the connection speed but at the same time increase the safety.

**Keywords:** *Wireless Campus Network, Security Mechanism, Data Security, Network Authentication, Access Control*

## 1. INTRODUCTION

With the development of information construction of colleges and universities, wireless campus network, as network infrastructure, has been gradually built in colleges and universities [1], in which the safety certificate might be the most important thing in planning and considerations [2]. Compared with mature wired network security mechanism, the wireless network is in lack of flexible and reliable safety certificate mechanism [3] [4]. It is quiet the puzzled for wireless network construction to take both the available acceptability of the users and rigorous safety precautions into account [5].

In current situation, many wireless access points in the campus network have not do well in the consideration of the security with wireless access, such as the authentication based on MAC address or shared secret key without authentication, and let alone the relatively difficult-set authentication method like 802.1x [6]. When hanging in the campus with a notebook computer in hand, we may find a lot wireless access point which is easy to get in, without any security precautionary measure [7]. If someone unknown comes into the campus network by getting in the wireless network, that would be a threat to our campus network [8].

This paper, base on the current situation of wireless campus network, presents an improved security mechanism for wireless campus network, with the optimization and improvement separately in data confidentiality agreement, network authentication protocol and access control.

## 2. THE CURRENT SITUATION OF SECURITY MECHANISM FOR WIRELESS CAMPUS NETWORKS

At present, the security mechanism for wireless campus networks includes the following two: WEP security mechanism and WPA security mechanism [9].

### 2.1 WEP Security Mechanism

WEP (Wired Equivalent Privacy) agreement is an encryption standard made to guarantee that data can pass through wireless networks safely, with the cooperation of the encryption algorithm in shared secret key RC4, so that access net resource can only be obtained with both users' encryption key and AP key, which also means to prevent the unauthorized users' monitoring and illegal users' access, with a key supporting 152-bit encryption [10] [11].

WUP standard have inherent vices in protecting net security. For example, since users in one service area share the same secret key, the whole network would be confronted with danger, once a user has lost or compromised the key [12]. WEP encryption has some security defects in itself. Come open and available tools for invading dangerous networks can be downloaded from the internet for free. And Hackers are very likely to find out the network transmission, and then use these tools to code the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

keys, to intercept network data package or unauthorized access [13].

### 2.2 WPA Security Mechanism

With the dissatisfaction for market demands in WEP shortages, the Wi-Fi alliance launched WPA tech, as the temporary succedaneum of WEP security standard protocols of wireless network to supply quite strong security performance for IEEE 802.11 Wireless Local Area Network. WPA is actually a subset of IEEE 802.11, whose kernel is IEEE 802.1x and Temporal Key Integrity Protocol (TKIP) [14].

Both TKIP and WEP are based on RC4 encryption algorithm, but improve the current WEP by using dynamic communication key. TKIP introduces 4 algorithms: new 48-bit initialization vector (IV) and order rules of IV, per-packet key construction, Michael message integrity codes, and key recover and distribution, which increase the security of data encryption in wireless network [15] [16].

IEEE 802.11i also definite a new encryption algorithm based on Advanced Encryption Standard (AES), to create more powerful encryptions and data integrality inspection. AES is a symmetrical-block encryption with a higher encryption performance than RC4 algorithm in WEP / TKIP. After being notarized in IEEE 802.11i, it has become a new encryptionof stronger security protection replacing WEP. But WPA security mechanism is inferior to WEP instability [17].

## 3. THE IMPROVED SECURITY MECHANISM FOR WIRELESS CAMPUS NETWORKS.

On the basis of the existing security mechanism for wireless campus networks, this paper makes optimization and improvement in data confidentiality agreement, network authentication protocol and access control [18].

### 3.1 Data Confidentiality Agreement Based on CCMP

CCMP is another encapsulation protocol supplying data confidentiality and integrity. Figure.1 is the CCMO encryption flow block diagram.

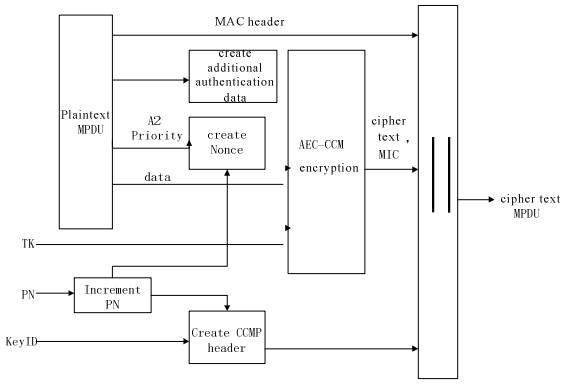


*Figure 1: CCMO Encryption Flow Block Diagram.*

The procedure of CCMO encryption algorithm is as follow:

The data package number (PN) pluses one, every MPDU needs a new and different PN;

Create additional authentication data ADD for OCM by MAC header;

Create current Nonce of CCM by PN, address A2 (TX-address of MPDU) and Priority;

Inset PN and key identifier to CCMP header (first 8 bytes in cipher text);

Import additional authentication data ADD, current Nonce, and MPDU data, encrypt AES-CCM under the control of temporary key TK, then get cipher text data and message integrity code MIC;

Combine CCMP header, Plaintext MAC header, cipher text data and MIC to cipher text MPDU with a certain format, and send cipher text MPDU.

The encapsulate objects in CCMP differ from those in TKIP. TKIP's message integrity code is for MSDU, encryption for MPDU, encapsulation for MSDU and MICMPDU after calculating MIC of the entire MSDU. And then translate MPDU into cipher text. The procedure of CCMP is just the opposite: get MPDU by segmenting MSDU. Then make separate encryption and integrity protection for each MPDU. CCMP's integrity code and encryption is all for MPDU. In general, CCMP is a strong data confidentiality agreement.

### 3.2 Rapid Authentication Protocol Based on Public Key Encryption

This paper presents a rapid authentication protocol and key agreement with the help of public key encryption and the tech of message authentication code. The protocol which uses modularized design, offers provable safety in CK model and has the security attribute of mutual entity authentication, forward security and so on, contenting the safety demands. For efficiency, only 2 communications is needed to complete. With small operand, it can be used as a sub-protocol of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

802.11i and WAPI, after appropriated encapsulation. The protocol is as follow:

Parameter Setting:

Set $p$ , $q$ as prime number. $q \mid p-1$ , $g$ is $q$ - order element in group $Z_p^*$ . $s$ is session identifier. Network identifier of the sender is $A$ . Network identifier of the receiver is $B$ . $H:\{0,1\}^{\infty} \rightarrow \{0,1\}^n$ is security Hash function. $E_p$ is safety public key encryption algorithm. $Mac$ is safety message authentication code algorithm. $E$ is safety symmetric encryption algorithm.

Authentication process as follow:

(1) T he sender choose a random $x \in Z_p^*$ , $a = g^x$ , and send $E_{P\_B}(A \| B \| s \| a)$ message to the receiver;

(2) The receiver receives and decodes it, and get $a$ . Choose randomly $y \in Z_p^*$ , $b = g^y$ , calculate $N = g^{xy}$ ,delete $y$ and send message $< E_{P\_A}(A \| B \| s \| b), Mac_N(b) >$ to the sender, as an output conversation key $K = (g^{xy} \| A \| B)$ ;

(3) The sender receives and decodes it, gets $b$ and checks the verification code. If receivable, delete $x$ , and get conversation code $K = H(g^{xy} \| A \| B)$ .

The sender and receiver can authenticate each other and at the same time, get the conversation key $K$ . That contributes a key agreement.

Key updating:

The sender chooses randomly $R \in \{0,1\}^k$ , calculate $K' = H(g^{xy} \| R \| K)$ s, $m = E_k(R \| Message)$ and then send the message $< m, Mac_{K'}(m) >$ to the receiver.

The receiver receives, decodes $m$ and gets $R$ , calculates $K' = H(g^{xy} \| R \| K)$ , and checks $Mac$ . If passed, receive new conversation key $Message$ .

The both sides of the conversation can get the conversation key $K'$ . The key updating finishes.

### 3.3 The Access Control Mechanism on Ports

IEEE 802.1x is the standard "of network access control based on port", with an original aim of access control on wire network. The authentication model of 802.1x includes 3 substances: supplicant, authenticator and authentication server AS.

With the concept of virtual port, this paper separately filters and controls the users control data and operating data, and defined the "controlled" and "uncontrolled" logical port edge of device in network (authenticator, such as concentrator and AP). After getting into the network, authenticators allow controlled reports of users to pass through uncontrolled ports, but obstruct in controlled ports. Only after checking users identities by authentication servers and be authenticated to, can authenticators let customer service data get through controlled ports.

## 4. EXPERIMENT SIMULATIONS

The two main performances of wireless networks are speed and security. This paper simulates a experiment of security mechanism of wireless campus networks focusing on these.

### 4.1 The Speed Test of Wireless Networks

In the area being experienced, set separately 10 various locations to test the speed of wireless networks. The experiment result is shown below.

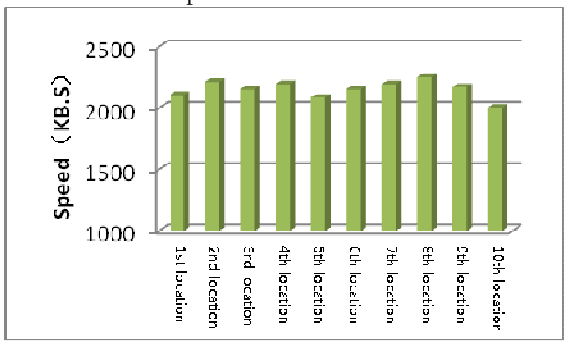


*Figure 2: The Wireless Network Speed Testing Statistics In The Original Scheme(Nst Location)*

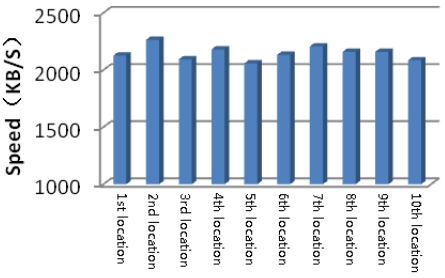


*Figure 3: The Speed Testing Statistics In The Present Scheme*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

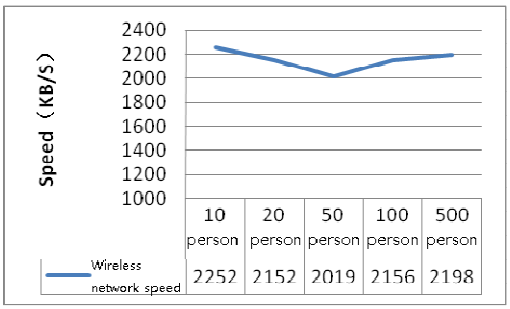


*Figure 4: The Average Speed Testing In The Present Scheme With A Increasing Number Of People(10)*

From Figure.2 to Figure.4, it can been seen that the security mechanism of wireless campus networks put forwards in this paper have little influence on the speed of wireless networks and difference in the speed of wireless networks between the original and the present one is small.

### 4.2 The Test on Wireless Network Security

Use the method of code exhaustion, code this wireless network and compare with WEP security mechanism and WPA security mechanism, as shown below.

*Table 1 : The Statistics Of Secrete Key Decoding Time*

| Key length | Decoding time | | |
|---|---|---|---|
| | WEP mechanism | WPA mechanism | Textual mechanism |
| 8 | 9.29H | 12.52H | 17.94H |
| 9 | 21.67H | 25.84H | 31.27H |
| 10 | 75.69H | 102.36H | 259.57H |
| 11 | 186.39H | 259.68H | 458.21H |
| 12 | 589.58H | 758.36H | 1258.36H |

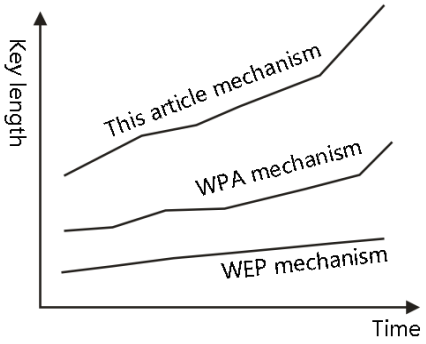


*Figure 5: The Test On Wireless Network Security*

From Figure.5, taking security into account, the security mechanism in this paper is much better than that of WEP security mechanism and WPA security mechanism.

## 5. CONCLUSIONS

The improved security mechanism for wireless campus network, on the basis of no influence on signal strength and speed of network, makes a optimization and 207-1221 separately in data confidentiality agreement, network authentication protocol and access control, and its security mechanism can prevent illegal network access invasion effectively, which is much better than that of WEP security mechanism and WPA security mechanism.

## ACKNOWLEDGEMENTS

The Project Supported by Natural Science Foundation of Henan Educational Committee（2011A520025）

## REFERENCES:

[1] Z.M. Chen, W. Liao, S.S. Chen, “The authentication agreement on wireless network under optimization of the PKI mechanism”, *Computer Engineering and Aesigning*, Vol. 9, No. 3, 2012, pp. 3297-3300.

[2] L. Zhang, J. W. Liu, H.C. Xu, “The research and design of routing protocol of networks multicast”, *Computer Engineering and Designing*, Vol. 9, No. 1, 2012, pp. 3347-3350.

[3] C.R. Zhang, Y. Liu, F. Li, “The summary on wireless network key technology”, *Computer Engineering and Designing*, Vol. 8, No. 9, 2012, pp. 2906-2910.

[4] Q. He, Z.Y. Feng, P. Zhang, “The decision algorithm on perceiving wireless network reconstruction based on artificial intelligence technology”, *Communication Journal*. Vol. 7, No. 3, 2012, pp. 96-102.

[5] M. Wei, P. Wang, J.T. Jin, “A delaminating detection for invading WIA-PA network”, *Instrument Journal*. Vol. 71, No. 1, 2012, pp. 1453-1459.

[6] B.Q. Kan, J.H. Wan, J.Y. Wang, “The information channel access agreement on cognitive wireless network”, *Software Journal*. Vol. 7, No. 10, 2012, pp. 1824-1837.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[7] Y.Q. Sun, X.D. Wang, X.M. Zhou, "The jamming attack in wireless network", *Software Journal*. Vol. 5, No. 5, 2012, pp. 1207-1221.

[8] T.T. Zhou, Q. Li, D. Zheng, "The analysis and improvement on wireless network moved authentication agreement", *Computer Usage and Software*. Vol. 3, No. 9, 2012, pp. 19-21.

[9] T. Hu, Z.H. Jing, F.J. Li, "A improved game playing algorithm on cognitive wireless network power control", *The Computer Science* . Vol. 2, No. 2, 2012, pp. 75-79.

[10] J.D. Hu, J.Z. Lu, "An anonymity authentication project in wireless network based on smart card", *Computer Engineering*. Vol. 201, No. 1, 2011, pp. 122-124.

[11] Z. Gao, "Guaranteed Cost Controller Design for Wireless Networked Control Systems Based on Dead band Scheduling". *Information and Control*. Vol. 41, No. 4, 2012, pp. 522-528.

[12] Li Z. "Stable enclosure based hybrid routing schema in heterogeneous wireless networks". *Journal on Communications*. Vol. 33, No. 9, 2012, pp. 95-104.

[13] H. Wang, "Research on a wireless network system in the intelligent office environment". *Computer Engineering & Science*. Vol. 34, No. 9, 2012, pp. 21-25.

[14] H. Wu, "Wireless network monitoring technology of cable-less stored seismic instrument". *Journal of Jilin University: Eng and Techno Ed*. Vol. 42, No. 5, 2011, pp. 1296-1301.

[15] F. Xiong, "Design and Realization of Node Location System in Wireless Networks". *Measurement & Control Technology*. Vol. 31, No. 8, 2012, pp. 71-74.

[16] Y. Ruan, "Station and relay node deployment strategy for optimizing performance and costs in heterogeneous wireless networks". *Chinese Scientific Papers*. Vol. 7, No. 7, 2012, pp. 518-522.\

[17] X. Zhou, "New problems of radio network optimization in dense urban areas". *Telecommunications Science*. Vol. 28, No. 5, 2012, pp. 151-154.

[18] J. Xu, "A routing metric for delay-sensitive applications in heterogeneous multi-radio Multi-channel wireless networks". *Mini-micro Systems*. Vol. 33, No. 8, 2012, pp. 1660-1664.