Campus Wireless Network Coverage and Analysis of Its Security Based on Big Data

Yang Chen, Yingyun Wang, and Fenfei Gu
(Corresponding author: Yang Chen)
Institute of Information Engineering, Anhui Xinhua University, Hefei, Anhui 230088, China
No. 555, Wangjiang West Road, Hefei, Anhui 230088, China
Email: bochen19137542@163.com
(Received Apr. 1, 2019; Revised and Accepted June 24, 2020; First Online June 10, 2021)

Abstract

Under the background of big data, the wired network has not met the campus's needs; therefore, it needs to cover the wireless network. Taking the wireless local area network (WLAN) coverage of Institute of Information Engineering of Anhui Xinhua University as an example, this study firstly analyzed the characteristics of campus WLAN and the security technology of WLAN, improved the wired equivalent privacy (WEP) protocol in IEEE802.11, and strengthened the security of RC4. Then, a specific coverage scheme of campus WLAN was designed. After testing, it was found that the operation efficiency of the improved RC4 algorithm decreased slightly, and the designed WLAN could defend most of the network attacks, had high signal intensity, and operated stably, meeting the needs of teachers and students. Thus, this study contributes to the further research of WLAN and provides some guidance for constructing campus WLAN.

Keywords: Big Data; Security; Wireless Network

1 Introduction

With the development of technology, people's demands on the Internet has improved, and their dependence on wireless local area network also has been strengthened [4, 6]. In the current campus, the wired network is mainly used, which provides great convenience for teachers and students. However, the wired network has some limitations. For example, it can not meet the needs of teachers and students to use the network at any time in the classroom, library, outdoor, etc. Also, with the development of science and technology, equipment, such as tablet computers, mobile phones, and laptops, has become more and more popular.

In order to satisfy the demands of teachers and students, covering WLAN on campus has become an important part of campus construction. With the popularity of WLAN on campus [10], how to build campus WLAN and realize the safe transmission of information has been widely studied. Zhang *et al.* [21] designed a campus network management method based on the runtime model to manage the network equipment uniformly. They found through the experiment that the designed method could save energy by 16.7% and manage the network more efficiently and orderly compared with the traditional method.

Nonum *et al.* [16] studied WLAN in Nigerian tertiary institutions, proposed an autonomous web service architecture, which could not only manage the performance of service users but also manage the interconnection of WiMax-WiFi infrastructure and service coverage network, to improve the network flexibility and overall performance.

Zhang *et al.* [20] designed an encryption-based method to protect user privacy and carried out experiments on the method in the intelligent campus. It was found that the method provided a more powerful security guarantee and weighed the storage, bandwidth, and computing costs, which had high practicability. Ooko *et al.* [18] pointed out that there have been increasing hacking cases because of the uncontrolled medium of WLAN. They investigated the security of WLAN in Kenyan University and found through literature analysis, interviews, and experiments that campus WLAN was not secure.

2 Campus Wireless Network Under Big Data

In the era of big data, the number and types of information have become more and more, which brings great challenges to the security of the network [11]. A school is a place with a large number of people and frequent exchanges. In the campus wireless network, teachers and students are producing data almost every moment. These data packets contain a variety of content, including text, video, audio, etc., and the data contain very important information, such as the identity information, major, and

performance of students, the teaching courseware and research paper of teachers, etc. Mass data have higher requirements on the network; therefore, a network environment with higher processing speed and safety is needed. In campus WLAN, the existing problems mainly include:

Equipment Safety. In order to ensure the physical security of the network, it is necessary to ensure the operation security of wireless devices and detect these devices to avoid equipment failure and protect the wireless network;

Information Security. Under the background of big data, information spreads very fast, and it is easy to leak and lose information. In the process of information transmission, there may be various loopholes, which will cause damages to network security under the attack of viruses or hackers. Also, imperfect and incomplete network management will also cause security problems.

Compared with the wired network, WLAN is more vulnerable and prone to problems because of its openness [7]. Also, wireless devices have some limitations in storage, power supply, etc. Many security technologies that can be applied in the wired network can not be applied in the security protection of WLAN. At present, the main security problems faced by WLAN are as follows.

The wired network has fixed boundaries; therefore, attackers need to go through defense lines, such as firewalls, gateways, etc., to enter the network. WLAN has no clear defense boundary; therefore, attackers can attack the network from any node. Wired network terminals can not move on a large scale, so that it is easy to manage, while WLAN terminals are mobile and vulnerable to eavesdropping and hijacking because of insufficient protection [13]. Also, the topology of WLAN is dynamic and changeable; therefore, it is difficult to carry out centralized management, but many security algorithms require the participation of all nodes, which is difficult to achieve in WLAN [14]. Finally, with the movement of users, the channel of WLAN is affected by interference and fading, leading to a large fluctuation in signal quality, i.e., the robustness problem.

3 Overview of Wireless Network

3.1 Composition of WLAN

WLAN refers to the local area network established using wireless communication [9, 12]. It has fast transmission speed and has been widely used in scenes such as personal, enterprise, school [19]. It takes up a small space and covers a wide range. It can also be used in areas such as forests and deserts with constant communication. The main components of WLAN include:

1) Station (STA, pp. a data exchange equipment, such as desktop, notebook, mobile phone, etc.;
2) Wireless medium (WM, pp. the medium that can transmit radio frequency (RF) signal or infrared signal;
3) Access point (AP, pp. realize the exchange of wireless data;
4) Distributed system: realize the connection between different services.

3.2 WLAN Security Technology

3.2.1 IEEE 802.11 Standard

In order to realize the communication and data sharing of WLAN, it should follow some protocols. WLAN protocols have good security and stability. At present, the most commonly used is the IEEE 802.11 standard [1, 15].

IEEE802.11 is an open-band network with a data transmission rate of 1 Mbit/s-2 Mbit/s and a working frequency band of 2.4 GHz. In addition to IEEE802.11, there are 802.11a, 802.11b, 802.11g, and 802.11n. The latter four networks are the upgrading and improvement of 802.11. Its security technologies include:

1) Service set identification (SSID, pp. SSID is a string. As long as the SSID is remembered, it can access WLAN to avoid unauthorized users accessing the network.
2) WEP: WEP is used for WLAN encryption and authentication [2]. The encryption algorithms used are RC4 (Rivest cipher) and CRC-32. The former is used for ensuring data security, and the latter is used for ensuring data integrity.
3) Physical address filtering (MAC, pp. only the site registered with MAC address can be connected. Each network card corresponds to a unique MAC address, which can prevent some low-level intrusion.
4) Identity authentication: there are two methods: open system authentication (OSA) and shared key authentication (SKA). The former is the default method, and the latter is optional. If the request fails to pass the authentication, it will be rejected.

3.2.2 WEP Protocol and Improvement

In WEP, the data frame consists of three parts, 32-bit initialization vector (IV), transmitted data (≥ 1 bit), and 32-bit integrity check value (ICV). IV is transmitted in plaintext, and the last two parts are transmitted in the ciphertext. WEP uses the RC4 algorithm for encryption [17]. It generates a key sequence based on a large array, called S-box, and its value range is 0-255. The encryption process mainly consists of two parts [3]:

1) Key scheduling algorithm (KSA, pp. a secrete key (Key) is randomly selected. S-box is initialized. It is assumed that there are parameters i_t and j_t pointing

to the S-box. Let i_t traverse every position of the S-box to make j_t generate a new value. Then, the bytes corresponding to j_t and i_t in the S-box are exchanged. After N times of traversal, the initial state S_0 of RC4 is obtained.

2) Pseudo-random key sequence generation algorithm (PRGA, pp. according to S_0, i_t and j_t are initialized. Then j in the algorithm is updated. The bytes corresponding to i_t and j_t are exchanged. The position of the bytes in the S-box is conversed through the pseudo-random number generator (PRNG) [5]. After every time of conversion, the 8-bit key stream is output and processed by xor encryption with the plaintext and by xor decryption with the ciphertext.

The key stream in RC4 is generated by PRNG. By analyzing the first byte of the key stream, the first byte of the original key can be found out, and then the other bytes are gradually deduced [8]. Therefore, in order to increase the security of the algorithm, the process of PRNG generating the initial random number is improved. 0-255 is converted to hexadecimal numbers and arranged in a table of 16×16 in the order from small to large, as shown in Table 1.

Table 1: Initialized random number table

	0	1	2	⋮	E	F
0	00	01	02	⋮	0E	0F
1	10	11	12	⋮	1E	1F
2	20	21	22	⋮	2E	2F
⋮	⋮	⋮	⋮	⋮	⋮	⋮
E	E0	E1	E2	⋮	EE	EF
F	F0	F1	F2	⋮	FE	FF

The improved RC4 method improves security by exchanging bytes. It is assumed that the byte of the position where $S\lfloor i_t \rfloor$ locates is $X_{mt}Y_{mt}$ and the byte of the position where $S\lfloor j_t \rfloor$ locates is $X_{nt}Y_{nt}$. The row is moved to the right gradually, and the distance is $|X_{nt} - X_{mt}|$. When $S\lfloor i_t \rfloor$ and j_t are in the same column, the column is moved downward to make $S\lfloor i_t \rfloor$ reach the position of j_t, and the distance is $|Y_{bt} - Y_{mt}|$, where j_t locates is also moved to make $S\lfloor j_t \rfloor$ reach the position of $S\lfloor i_t \rfloor$ according to the same method; the moving distance of the row and column is $(16 - |X_{nt} - X_{mt}|)$ and $(16 - |Y_{nt} - Y_{mt}|)$ respectively. The other steps are the same as the original RC4 algorithm.

4 Coverage Design of Campus WLAN

By February 2020, there were more than 3400 students and 120 teachers in the Institute of Information Engineering of Anhui Xinhua University, including 24 professional laboratories for wireless sensor network and software engineering, six campus practice bases, 11 computer basic experimental training rooms, six embedded experimental rooms, etc. The original wireless network of the school covered a few apartments and teaching buildings, which could not meet the needs of teachers and students. The requirements for WLAN coverage in different places of the college are shown in Table 2.

In the college, the architecture of thin AP was adopted to manage user data uniformly, and the WLAN supporting 802.11n was constructed. RG-WS5708 product was used as the wireless controller; the controller adopted the MIP64 multi-core processor architecture, which could break through the three-tier network to maintain communication with AP and support 768 wireless access points at most. The wireless AP adopted RG-AP220-E, which could provide sixfold bandwidth. The network management system adopted RG-SNV, which could maintain and manage the network remotely and make a timely response if there was an abnormality in the network. Based on the investigation of the actual situation of the college, it was estimated that 123 AP was needed to cover the whole college.

5 Wireless Network Security Analysis

Firstly, the performance of the improved RC4 algorithm was analyzed. The times of operation was compared between the original RC4 algorithm and the improved RC4 algorithm. The results are shown in Tables 3 and 4.

It was seen from Table 3 that the improved RC4 algorithm needed one more row shift and column shift every time when encrypting one byte compared to the original RC4 algorithm. Table 4 shows the operation times of the two algorithms under different byte numbers. It was found that the operation times of the improved RC4 algorithm were slightly more than that of the original RC4 algorithm, 5000, 10000, 15000 and 20000 times respectively, i.e., when improving the security of the algorithm, the operation efficiency of the algorithm decreased slightly.

The method of active analysis was used to test the security of WLAN. A pretended attacker interacted with STA and AP and then attacked WLAN. Whether WLAN could defend against this attack was determined. Test cases were written using Tcl. The test cases were expanded into commands using the C/C++ interface to simulate the attack behavior. Whether it was successful or not, AP will return the results to the host side. The test results are shown in Table 5.

Table 2: Coverage requirements of campus WLAN

Place	Coverage Requirements	Frequency Band Planning
Dense office area	The number of online users shall not be less than 100% of the seats, and the rate per user shall not be less than 2 Mbps	Dual-frequency
Classroom	The number of online users shall not be less than 30% of the seats, and the rate per user shall not be less than 1 Mbps	Single-frequency 2.4 GHz
Library	The number of online users shall not be less than 60% of the seats, and the rate per user shall not be less than 2 Mbps	Dual-frequency
Laboratory	The number of online users shall not be less than 100% of the seats, and the rate per user shall not be less than 1 Mbps	Single-frequency 2.4 GHz
Restaurant	The number of online users shall not be less than 15% of the seats, and the rate per user shall not be less than 1 Mbps	Single-frequency 2.4 GHz
Student apartment	The number of online users shall not be less than 100% of the seats, and the rate per user shall not be less than 2 Mbps	Single-frequency 2.4 GHz
Outdoor playground	The number of online users shall not be less than 80, and the rate per user shall not be less than 1 Mbps	Dual-frequency

Table 3: Comparison of operation times (1)

	Original RC4 Algorithm	Improved RC4 Algorithm
Number of modular addition operations	$5n$	$5n$
Byte conversion times	$2n$	n
Number of row shift operations	-	n
Number of column shift operations	-	n

Table 4: Comparison of operation times (2)

Number of Bytes	Original RC4 Algorithm	Improved RC4 Algorithm
5000	35000	40000
10000	70000	80000
15000	105000	120000
20000	140000	160000

Table 5: Attack test results

Attack Modes	Attack Results
WEP Share Key attack	The attack failed
WEP Weak Key attack	The attack failed
Association Request Frame Flood attack	The attack failed
Virtual Carrier Sense attack	The attack failed
NAV DOS attack	The attack was successful
Beacon Flood attack	The attack failed
EAP Failure attack	The attack failed
Probe Request Frame Flood attack	The attack was successful
Spoof of Sleep State Indication Frame attack	The attack failed
Spoof of No Data TIM Frame attack	The attack failed

It was seen from Table 5 that only the NAV DOS attack and Probe Request Frame Flood attack were successful, and the other eight attacks failed, which showed that the WLAN established in this study had a good performance in security and could resist most of the attacks. Also, for the successful cases of attacks, managers should pay attention to them and further strengthen the security of WLAN by combining with methods such as intrusion detection.

The other performances of the designed WLAN were tested. The testing content is as follows.

1) The signal strength in the classroom installed with AP was analyzed. A laptop was put in the classroom and installed with the wirelessmon software. The laptop was moved freely in the classroom, and the signal data of different positions were recorded. After testing, it was found that the signal strength in the classroom was - 32 dB ¿ 50 dB, which showed good quality.

2) The download rate of AP was tested. In the classroom, five laptops were connected with AP, and large files were downloaded through Thunder 7. After 20 minutes, the download stopped, and the total download amount was calculated. The test showed that the download rate of AP was 800 kb/s, which could meet the needs of teachers and students.

3) The response of AP in case of failure was tested. In the classroom, large files were downloaded via a laptop connected to AC. Whether the download of the laptop interrupted was tested after two running AC was turned off. After testing, it was found that the download did not interrupt, indicating that the AP could automatically carry out local forwarding and had a stable data forwarding function.

4) The warning function of WLAN was tested. A wireless AP was added as an illegal AP, and its SSID was set as wlanx. Then, a laptop was connected to observe whether it could connect successfully. After testing, the terminal connecting to the AP was forcibly interrupted, indicating that WLAN could prevent the access of illegal AP.

6 Conclusion

This paper analyzed the security problems of WLAN. An improved RC4 algorithm was proposed to enhance the security of WLAN. The campus WLAN coverage scheme was designed, and the WLAN was tested. It was found that the WLAN had good signal strength, a high download rate, a stable data transmission function, a stable alarm function, and a strong defense against network attacks. This work makes some contributions to the construction of campus WLAN.

References

[1] A. S. M. Anuar, W. N. W. Muhamad, D. M. Ali, S. Seroja, N. A. Wahab, "A review on link adaptation techniques for energy efficiency and QoS in IEEE802.11 WLAN," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, no. 1, pp. 331, 2020.

[2] A. Aziz, M. R. Abd Razak, N. E. A. Ghani, "The performance of different IEEE802.11 security protocol standard on 2.4ghz and 5GHz WLAN networks," in *International Conference on Engineering Technology and Technopreneurship (ICE2T'17)*, Kuala Lumpur, pp. 1-7, 2017.

[3] S. Chugh, "Kamal. Securing data transmission over wireless LAN (802.11) by redesigning RC4 Algorithm," in *International Conference on Green Computing & Internet of Things*, pp. 1436-1441, 2015.

[4] Z. Guo, "Cryptanalysis of a certificateless conditional privacy-preserving authentication scheme for wireless body area networks," *International Journal of Electronics and Information Engineering*, vol. 11, no. 1, pp. 1-8, 2019.

[5] D. Han, L. Min, G. Chen, "A stream encryption scheme with both key and plaintext avalanche ef-

fects for designing chaos-based pseudorandom number generator with application to image encryption," *International Journal of Bifurcation & Chaos*, vol. 26, no. 05, pp. 1650091, 2016.

[6] D. P. Huangfu, X. P. Tian, X. J. Wang, P. Chen, "Research and mass deployment of non-cognitive authentication strategy based on campus wireless network," *ITM Web of Conferences*, vol. 17, pp. 01013, 2018.

[7] M. S. Hwang, C. C. Lee, S. K. Chong, J. W. Lo, "A key management for wireless communications", *International Journal of Innovative Computing, Information and Control*, vol. 4, no. 8, pp. 2045–2056, 2008.

[8] R. Ito, A. Miyaji, "Refined construction of RC4 key setting in WPA," *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, vol. 100, no. 1, pp. 138-148, 2017.

[9] C. C. Lee, M. S. Hwang, I. E. Liao, "A new authentication protocol based on pointer forwarding for mobile communications", *Wireless Communications & Mobile Computing*, vol. 8, no. 5, pp. 661-672, 2008.

[10] Q. Liao, X. R. Luo, A. Gurung, W. Shi, "A holistic understanding of non-users' adoption of university campus wireless network: An empirical investigation," *Computers in Human Behavior*, vol. 49, pp. 220-229, 2015.

[11] L. Liu, Z. Cao, C. Mao, "A note on one outsourcing scheme for big data access control in cloud," *International Journal of Electronics and Information Engineering*, vol. 9, no. 1, pp. 29–35, 2018.

[12] J. W. Lo, C. C. Lee, M. S. Hwang, Y. P. Chu, "A secure and efficient ECC-based AKA protocol for wireless mobile communications", *International Journal of Innovative Computing, Information and Control*, vol. 6, no. 11, pp. 5249-5258, 2010.

[13] J. W. Lo, J. Z. Lee, M. S. Hwang, Y. P. Chu, "An advanced password authenticated key exchange protocol for imbalanced wireless networks", *Journal of Internet Technology*, vol. 11, no. 7, pp. 997-1004, 2010.

[14] J. W. Lo, S. C. Lin, M. S. Hwang, "A parallel password-authenticated key exchange protocol for wireless environments", *Information Technology and Control*, vol. 39, no. 2, pp. 146-151, 2010.

[15] W. N. W. Muhamad, J. Y. Khan and J. Brown, "Energy efficient contention window adaptation algorithm for IEEE 802.11 WLAN," in *22nd International Conference on Telecommunications (ICT'15)*, pp. 54-59, 2015.

[16] E. O. Nonum, P. O. Otasowie, K. C. Okafor, "Campus wireless network classification for enterprise adoption: perspectives and dimensions for large scale computing," *International Journal of Computer Applications*, vol. 142, no. 12, pp. 19-31, 2016.

[17] T. Ohigashi, T. Isobe, Y. Watanabe, M. Morii, "Full plaintext recovery attacks on RC4 using multiple biases," *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, vol. 98, no. 1, pp. 81-91, 2015.

[18] O. S. Ooko, M. Shadrack, E. Ataro, "Security of wireless campus networks in selected public and private universities in Kenya," *International Journal of Engineering and Management Sciences*, vol. 2, no. 1, pp. 1-10, 2017.

[19] A. Pandey, P. K. Pant, R. C. Tripathi, "A system and method for authentication in wireless local area networks (WLANs)," *Proceedings of the National Academy of Sciences, India Section A: Physical Sciences*, vol. 86, no. 2, pp. 149-156, 2016.

[20] L. Q. Zhang, O. Oksuz, L. Nazaryan, C. Q. Yue, B. Wang, A. Kiayias, A. Bamis, "Encrypting wireless network traces to protect user privacy: A case study for smart campus," in *IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'16)*, New York, NY, pp. 1-8, 2016.

[21] P. Zhang, J. Wang, "Management of intelligent campus wireless sensor networks based on runtime model," *Journal of Computer & Communications*, vol. 03, no. 7, pp. 22-31, 2015.

Biography

Yang Chen, born in June 1980, has received the master's degree from Hefei University of Technology. She is an associate professor. Her research directions are wireless sensor network, network security, and artificial intelligence.

Yingyun Wang, born in November 1982, has received the master's degree from Anhui University. She is an associate professor. She is interested in network security and artificial intelligence.

Fenfei Gu, born in September 1982, has received the master's degree from Hefei University of Technology. He is associate professor. He is interested in deep learning and privacy protection.