CHEMICAL ENGINEERING TRANSACTIONS

VOL. 51, 2016

A publication of
AIDIC
The Italian Association
of Chemical Engineering
Online at www.aidic.it/cet

Guest Editors: Tichun Wang, Hongyang Zhang, Lei Tian
Copyright © 2016, AIDIC Servizi S.r.l.,
ISBN 978-88-95608-43-3; **ISSN** 2283-9216

DOI: 10.3303/CET1651126

Security Mechanism Analysis of Wireless Local Area Network Based on WEP Protocol

Zaihui Cao*[a,c], Dongxian Yu[b], Qingtao Wu[c]

[a]Cooperative Innovation Center for Aviation Economy Development of Henan Province Zhengzhou, Henan 450046, China
[b]Department of Information Engineering, Henan Polytechnic College Zhengzhou, Henan 450046, China
[c]Department of Art and Design, Zhengzhou University of Aeronautics Zhengzhou, Henan 450046, China
czhhn@126.com

Due to the high rate, flexible of WLAN technology, it is easy to install, expand and economical advantages, which can meet virtually business or internet application needs. However, wireless network security problems in the process of rapid application brought in more and more people's attention. This paper introduces the concept and 802.11 WLAN security standards from the generation algorithm based --RC4 WEP security mechanism to explain the principles of the WEP security mechanism and processing. The decryption process was for analyzing the shortcomings of WEP security mechanism and vulnerabilities, the current attacks against WEP and intrusion methods. Finally, two improved methods TKIP protocol improvements and AES_CCM improved system for a detailed description. Security issues will continue to be the biggest obstacle to the wireless LAN industry.

1. Introduction

The wireless communication technology under no physical connection among plurality of devices can communicate with each other (Silva and A.Thakre, 2009). The wireless communication using radio waves to transmit data, while a wired communications using a cable (A.Kisliansky, 2007). Applications range wireless communication technology is very broad, from complex systems (such as wireless LAN and a cellular phone) to simple devices (such as wireless headphones, wireless LAN) can see the application of wireless communication technologies (Zhang, 2008). Infrared (IR) devices, such as a remote control with a wireless keyboard and mouse, wireless fidelity headphones, also belonging to the wireless communication devices, but these devices require the sender and receiver in a straight line visible range (Dongarsane, 2011). Target wireless communication technology provided users on the move can be anywhere access to the information function (Spencer, 2004).

Wi-Fi and traditional wired networks compared advantage is obvious, but due to its transport network and free to expand its features, security problems is also very prominent, especially in some networks attack is unique, such as roaming attacker, fraudulent access points and wireless LAN security encryption mechanism of congenital defects (Sadek, 2008). This gives us the use of wireless networks has brought a certain amount of risk, free to expand connections and user authentication management with respect to traditional wired network port management and user authentication management and existing wireless network encryption security mechanisms might have to rely on illegal invaders seemingly cover and bring legitimacy (Ackerman, 1990). How to strengthen the security management, how to make a wireless network to strike a balance between security and performance, which requires us to design the most appropriate and successful deployment of wireless network security solutions (Gao and Pandurang, 2015).

Wireless LAN is a computer network and wireless communication technology product of the combination, due to the unique wireless network open, and therefore the need for specialized research applies to wireless network security strategy (Hayajneh and Tanwar, 2015). Currently, there is a security mechanism for wireless LAN all the design flaws, affecting the range of applications and development prospects of the wireless LAN, the wireless LAN security study has very important significance. For vulnerabilities of WEP, WLAN security solutions are constantly evolving. While technologies such as 802.1x and VPN can greatly improve wireless

Please cite this article as: Cao Z.H., Yu D.X., Wu Q.T., 2016, Security mechanism analysis of wireless local area network based on wep protocol, Chemical Engineering Transactions, 51, 751-756 DOI:10.3303/CET1651126

network security and confidentiality, but as a security technology, they are not perfect, they can not make up for all of the vulnerabilities on network security. In today's rapid development of wireless technology, along with the further development of science and technology and wireless security mechanism, we will strengthen information security awareness continues to innovate and improve wireless security mechanism in the process of improving the level of prevention.

2. Related theory and method

2.1 WLAN security protocol

Since the wireless local area network communication is the way radio signals are transmitted, with respect to the wired network, a wireless LAN to send and receive data more vulnerable to eavesdropping (Iyer and Maallawi, 2015). Design a complete wireless LAN system, encryption and authentication are two essential factors to be considered safe, wireless LAN encryption and authentication technology applications the most fundamental purpose is to make wireless services can reach the same level of security and cable business. For this goal, and IEEE design a mechanism for encryption and decryption, the user can obtain the desired wireless network and the wired network is generally equivalent privacy, the encryption and decryption mechanism called WEP.

WEP encryption is a public key encryption algorithm, its code was shown in Figure 1.

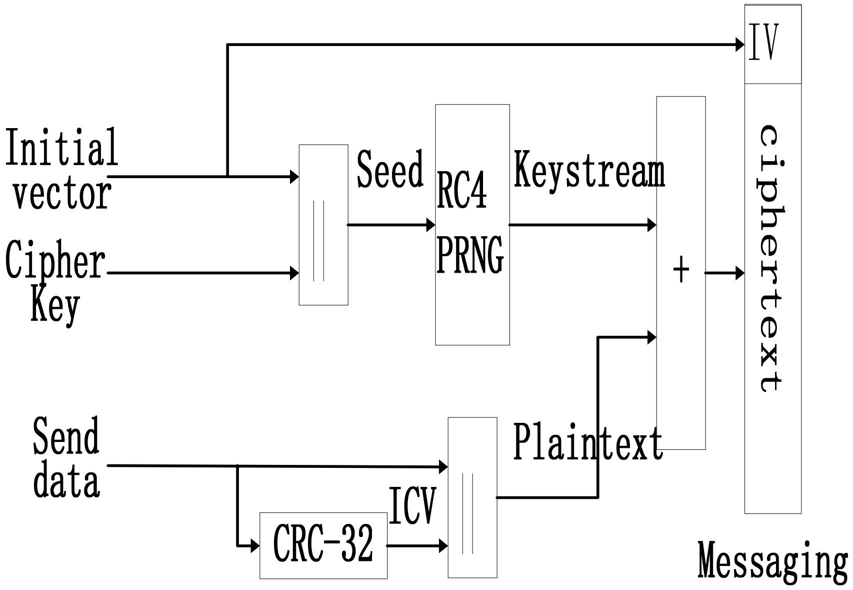


Figure 1: WEP encryption coding theory

Wherein the RC4 PRNG is a pseudo-random sequence generator, which is a key part of the algorithm, that is, it uses the RC4 algorithm to generate the key stream.

2.2 Wireless LAN encryption algorithm

RC4 size changes depending on the value of the parameter n varies. RC4 can achieve a secret internal state of n bits, there are N = 2n possible. Typically n = 8, which is the present value of the selected program, RC4 can generate a total of 256 of each output array S. RC4 (= 28) are elements in the array s a random element to achieve these, requires two processes: one is the key scheduling algorithm (KSA), to set the initial arrangement of S; a pseudo-random generation algorithm (PRGA), and random elements used to select the original order to modify the S sequence of KSA start initialization S, s (i) = i (where i = 0-255) by choosing. a series of numbers, and loaded into the key array K (0) a K (255) do not have to select the 256 number, as long as repeated until K S array is filled using the following procedures to achieve randomization:

```
j=0;
for(int i=0;i<256;i++)
{
j=i+S(i)+K(i)(mod 256);
swap(S(i),S(j));
}
```

Once completed the initial S KSA randomized, PRGA will take over the work, it is key to select byte stream that randomly selected elements from S, and modify S for the next selection. Selection process depends on the index i and j. the two index values are from 0, the following procedure is to select each byte of the key stream:

```
i=i+1(mod 256);
j=i+S(i)(mod 256);
swap(S(i),S(j));
t=S(i)+S(i)(mod 256);
k=S(t);
```

Specific RC4 encryption algorithm is shown in Figure 2.

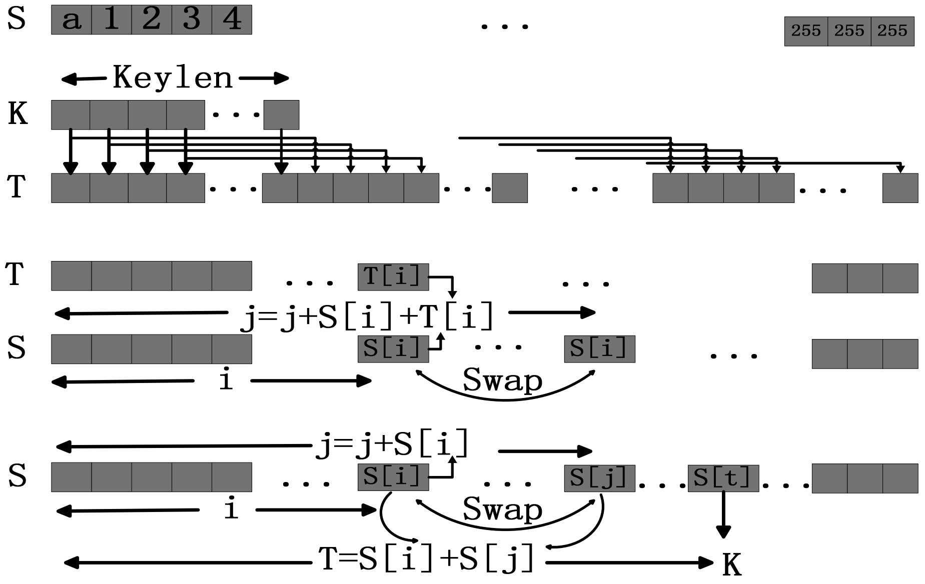


Figure 2: RC4 logical structure

RC4 algorithm output function is very simple, if we are to consider the S pseudo-random function, so long as we first find the two random numbers S [i] and S [j], then exchanged a S obtained by adding a new position to output value to this position. Such multiple use S has many advantages: First, S is not likely to be truly random, by a certain method can detect some of its deviations, these deviations will expose the internal state of RC4 some information, use many times S It can be reduced to some extent after the leak internal state information; secondly, we use the addition operation, linear operation to a randomly selected word to be output, increasing the difficulty of the operation after the nonlinear analysis.

Byte conversion is a non-linear byte substitution operation unit, substitution tables (S a Box) is established through two operation process, and is reversible. After an affine conversion operator:

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \tag{1}$$

In this conversion, the state exists as two GF (28) polynomial, and for a fixed polynomial c(x) for multiplication, if an overflow occurs, the remainder modulo x4 + 1, as follows:

$$c(x)='03'x^3+'01'x^2+'01'x+'02' \tag{2}$$

$$c(x) \text{ and } x^4+1 \text{ are coprime, let } b(x)=c(x)\otimes a(x) \tag{3}$$

In matrix multiplication, said:

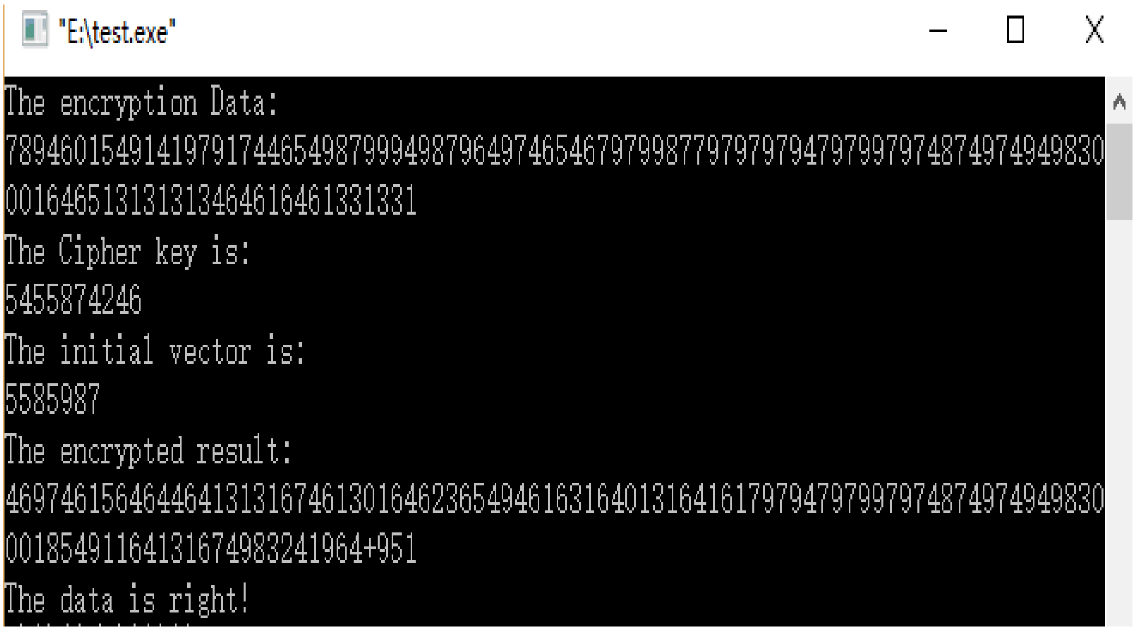
$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} \tag{4}$$

$$d(x)='0B'x^3+'0D'x^2+'09'x+'0E' \tag{5}$$

3. Experiments and results

3.1 Experimental results and analysis

Thorough grasp WEP, a WEP-AES, based on the realization of a WEP obit (ie core algorithm is RC4, the key is 4obit), WEP_lo4bit (ie core algorithm is RC4, the key is 104bit), WEP a ES_104bit (namely, the core algorithm to AES, the key is 104bit the C programming language. WEP_40 bit programming results were shown in Figure 3.



```
The encryption Data:
789460154914197917446549879994987964974654679799877979797947979979748749749498300
0016465131313134646164613313331
The Cipher key is:
5455874246
The initial vector is:
5585987
The encrypted result:
46974615646446413131674613016462365494616316401316416179794797997974874974949830
0018549116413167498324196 4+951
The data is right!
```

Figure 3: WEP_40 bit programming results

Due to the presence of the mathematical theory RC4 vulnerability has been completely broken, and AES in today's mathematical theory is safe, has not yet been completely broken, so using the AES algorithm to replace RC4 algorithm is of positive significance.

3.2 TCP protocol improvements

Temporary key integrity protocol (TKIP) to improve the use of WEP key security. It changes the way to get the key and spinning (change) key, and in order to prevent forgery package, it also increases the integrity checking of messages, so that the security of wireless networks has increased considerably Figure 4 is WEP and TKIP encryption for data comparison.

Compare TKIP WEP respect improvements:
(1) 48bit initial vector
In TKIP, the initialization vector from 24 bits to 48 bits, so that reduce the probability of conflict, greatly increasing security.
(2) Production and distribution each packet key
TKIP periodically generated for each client a new independent key, use this key to encrypt 802.11 each frame body, thus avoiding a few weeks when using WEP, or even months without more key case.
(3) Information integrity code
Use MIC to prevent hacker attacks, in the frame body in a 4bit additional check code, the sender to determine the MIC based on the frame body, and the body frame to fill the MIC. According to MIC receiving end to determine whether the frame is accepted, it first checks whether the information matches and the MIC, and then the message integrity check. If they match, then the complete information transfer, data normally accept.

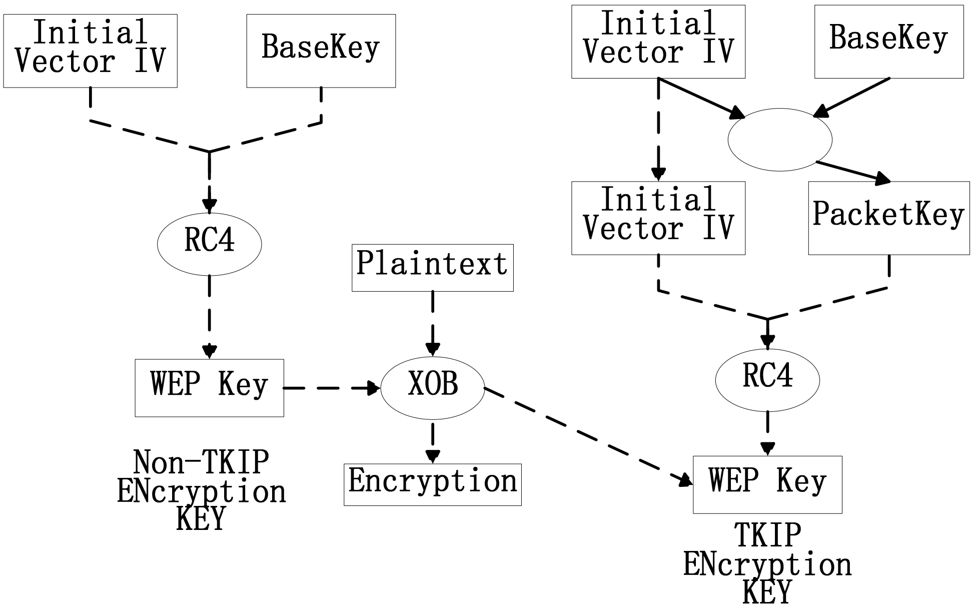


Figure 4: WPA and TKIP schematic comparison

4. Conclusions

Wireless LAN is a computer network and wireless communication technology product of the combination, due to the unique wireless network open, and therefore the need for specialized research applies to wireless network security strategy. Currently, there is a security mechanism for wireless LAN all the design flaws, affecting the range of applications and development prospects of the wireless LAN, the wireless LAN security study has very important significance. WLAN technology due to a high rate, access to flexible, easy to install, easy to expand and economical advantages can meet virtually any business or internet application needs, being more and more users of all ages. However, wireless network security problems in the process of rapid application brought in more and more people's attention. This paper introduces the concept and 802.11 WLAN security standards, and start from the generation algorithm based --RC4 WEP security mechanism to explain the principles of the WEP security mechanism and processing, the decryption process, and the process for analyzing the shortcomings of WEP security mechanism and vulnerabilities and the current attacks against WEP and intrusion methods.

Acknowledgments

This work is supported by the Educational Scientific Research Fund Project of Zhengzhou University of Aeronautics (No. zhjy15-20), and Youth Research Fund of Zhengzhou University of Aeronautics(No.2016143001).

Reference

Ackerman M.S., Malone T.W., 1990. Answer Garden: a tool for growing organizational memory. In: Proceedings of the ACM SIGOIS and IEEE CS TCOA Conference on Office Information Systems, Cambridge, MA, p 31–39. doi:10.1145/91474.91485.

Dongarsane C.R. and Jadhav A.N., 2011, “Simulation study on DOA estimation using MUSIC algorithm”, International Journal of Technology and Engineering System, vol.2, No.1, pp.54-57.

Gao W., Zheng X., & Lu B., 2015, IEEE 802.11 i WLAN Security Protocol Based On Genetic Software Engineering Model.

Hayajneh T., Ullah S., Mohd B. J., & Balagani K., 2015, An Enhanced WLAN Security System With FPGA Implementation for Multimedia Applications.

Kisliansky A., Shavit R. and Tabrikian J., 2007, “Direction of arrival estimation in the presence of noise coupling in antenna arrays”, IEEE Transactions on antennas and propagation, vol.55, No.7, pp.1940-1947.

Lyer P. J., & Narasimhan P., 2015, U.S. Patent No. 9,143,956. Washington, DC: U.S. Patent and Trademark Office.

Maallawi R., Agoulmine N., Radier B., & Meriem B.T., 2015, A comprehensive survey on offload techniques and management in wireless access and core networks. Communications Surveys & Tutorials, IEEE,17(3), 1582-1604.

Pandurang R.M., & Karia D.C., 2015, Performance measurement of WEP and WPA2 on WLAN using OpenVPN. In Nascent Technologies in the Engineering Field (ICNTE), 2015 International Conference on (pp. 1-4). IEEE.

Sadek M., Tarighat A., Sayed A.H., 2008, “A Leakage-based Precoding Scheme for Downlink multi-user MIMO Channels”, IEEE Transactions on Wireless Communications, vol. 26, no.8, pp.1505-1515.

Silva S., Goel L., Mousavidin E., 2009, Exploring the dynamics of blog communities: the case of MetaFilter. Inf Syst J 19:55–81. doi:10.1111/j.1365-2575.2008.00304.

Spencer Q.H., Swindlehurst A.L., Haardt M., 2004, “Zero-Forcing Methods for Downlink Spatial Multiplexing in Multiuser MIMO Channel”, IEEE Transactions on Signal Processing, vol.52, no. 2, pp.461-471, May 2004.

Tanwar S., Kumar N., & Rodrigues J. J., 2015, A systematic review on heterogeneous routing protocols for wireless sensor network. Journal of network and computer applications, 53, 39-56.

Thakre A., Haardt M. and Giridhar K., 2009, “Singal snapshot spatial smoothing with improved effective array aperture”, IEEE Signal Processing Letters, vol.16, No.6, pp505 -508.

Zhang Y., Wang Q. and Huang A.M., 2008, “Localization of narr- ow band sources in the presence of mutual coupling via sparse solution finding”, Progress in Electromagnetics Re- search, vol.86, pp.243-257.