2006

Burglarproof WEP Protocol on Wireless Infrastructure

Jin-Cherng Lin
Tatung University, jclin@ttu.edu.tw

Yu-Hsin Kao
Tatung University, hebe@dlit.edu.tw

Burglarproof WEP Protocol on Wireless Infrastructure

Jin-Cherng Lin
Department of Computer Science and Engineering, Tatung University
jclin@ttu.edu.tw

Yu-Hsin Kao
Department of Computer Science and Engineering, Tatung University
hebe@dlit.edu.tw

Abstract

With the popularization of wireless network, security issue is more and more important. When IEEE 802.11i draft proposed TKIP, it is expected to improve WEP (Wired Equivalent Privacy) on both active and passive attack methods. Especially in generating and management of secret keys, TKIP uses more deliberative attitude to distribute keys. Besides, it just upgrades software to accomplish these functions without changing hardware equipments. However, implementing TKIP on the exiting equipment, the transmission performance is decreased dramatically. This article presents a new scheme, Burglarproof WEP Protocol (BWP), that encrypt WEP key twice to improve the security drawbacks of original WEP, and have better performance on transmission. The proposed method is focus on modifying encryption sets to improve the low performance of TKIP, and provides better transmission rate without losing security anticipations base on current hardware configuration.

Keywords: WLAN, IEEE 802.11 Family, WEP, TKIP, BWP

1. Introduction

With the development of science and technology, people are deeper and deeper in reliance on the Internet. In 1999, IEEE released a series of wireless LANs (WLAN) standards, 802.11 [1]. Wireless network brings people a heavy one convenient is the user mobility. The modern WLANs offer many benefits to networking, such as mobility, scalability, flexibility, installation easily, and so on. From cost perspective, it can save installation cost for short term and maintenance expense for long term cost. It is especially attractive to those environments where physical Ethernet cable deployment is not favored.

As statement in wireless LAN specifications, the date frames of WLAN are similar to the ones of Ethernet. For WLAN, the data transmission media is air-waves via air. Therefore, the base station will receive all WLAN clients' information in one particular service area. Due to air-wares can pass through the barriers, such as ceiling, floor and wall, so data transmission might be received by unexpected receiver who from different floors or buildings. Therefore, setting up a WLAN just like place numerous Ethernet ports everywhere. For this reason, security is the most important major for wireless LANs.

In the definition of IEEE 802.11[1] standard, a WLAN must provide three base Networking security service: authentication, confidentiality, and integrity, but related

documents [4][5] indicate that it cannot guarantee the data confidentiality of WLAN transmission when using basic encryption of based Wireless Network security service, and invaders can use WEP(RC4) encryption's defects or destroy the related program of WEP to find the secret key, even more capture the content of transmission data.

To reinforce 802.11 series, Wireless Ethernet Compatibility Alliance (WECA) raised some proposals about secure suggestions of WLAN [6], such as management of secret KEY, installing VPN environment and so on. Institute of Electrical and Electronics Engineers, Inc. (IEEE) proposed 802.11i WLAN Draft standard specification and reformed known security loopholes of 802.11 WLAN standards which were established previously by IEEE. Nevertheless, this Draft's standard specification hasn't approved until now. However, the demand for improving WLAN transmission security is very urgent. Because WEP has loophole of encrypting, and TKIP will make efficiency bad, we hope to propose a schema that can give consideration to the security and transmit efficiency.

The remainder of this paper is organized as follows. The following section overviews WEP and TKIP mechanisms. Then, the third portion presents the proposed new protocol schema. Section four is the simulation results about the comparison of TKIP and BWP. This paper concludes in section 5 with a summary and brief discussion of related work and other potential applications

2. Current Security Schemes: WEP and TKIP

Because of the way of WLAN process message's transmission uses radio broadcast, so its data more easily to wiretap then common network. Therefore, IEEE designed an encryption's function and expects WLAN user can obtain privacy as same normal wired networking. This encryption function is called WEP (Wired Equivalent Privacy). WEP offers basic security protection for data transmission and prevents third party steal communication data. Fig. 1 and Fig. 2 describe the WEP encryption and integrity checking mechanisms. By now it is well-known that WEP is insecure and should not be counted on to provide any security. The vulnerabilities of WEP can be concluding on four design flaws: WEP does not specify a mechanism for key management; WP does not specify a mechanism for generating IVs; there s no replay protection; and CRC32 is not a cryptographic integrity checker. [27]

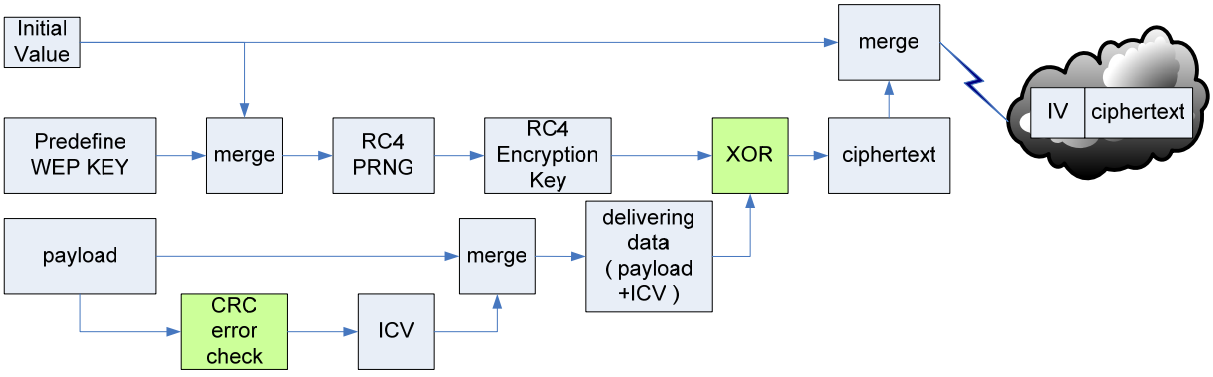

Figure 1: WEP Encryption Flowchart

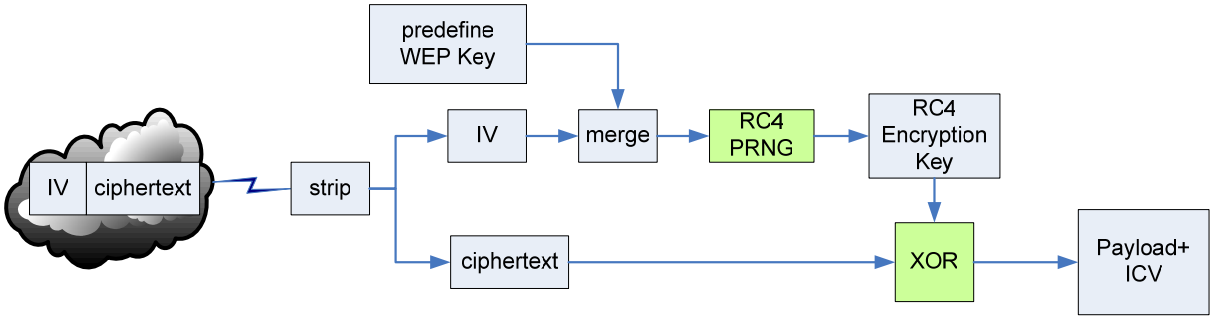

Figure 2: WEP Decryption Flowchart

At 2002, 802.11i [3] proposed TKIP protocol as temporary solution for the drawback of previous methods. It upgrades from WEP and quickly modifies current WEP loopholes. TKIP remains the method of WEP RC4 Encryption and improve the generation and management functions of WEP Key. TKIP uses MIC (Message Integrity Code) to protect transmission channel form auto-attack. The network security can be improved by upgrading software and leave the hardware to its original architecture.

To strengthen WEP encryption function, TKIP still uses original PRNG RC4 cipher of WEP, but added few steps before WEP PRING to strengthen the security of data transmission It can make each packet use different encryption secret key (Per-Packet Keying). The main characteristic of TKIP describes as below:

- Message Integrity Code (MIC)
- Sequence Counter
- Dynamic key management (Re-Keying)
- Countermeasures
- Key mixing

Because of TKIP changed the method of KEY generation and management, therefore, it can accomplish the safety function to reinforce the security of data transmission. However, the encryption algorithm is more complexity such that the performance of network throughput is seriously decreased. TKIP has three places which can discard received packet while decrypting procedure, as show in figure 4:

(1) Sequence is wrong.

(2) WEP engine cannot encrypt.

(3) MIC checking is not correct.

Each TKIP packet use two phases to generate 128Bits encrypted KEY. While identifying MIC information security, at the same time, it must compute each MSDU by MIC and bring TSC into Phase2's Mixing; The MIC of TKIP input is the sharing MIC Key of AP

and Client, and the 64 Bit MIC Key is generated by DA/SA/Payload of MSDU. It is equal to 20 Bit's key encrypt to MSDU. This action increases a lot of Overhead and increases transmission AP Throughput.

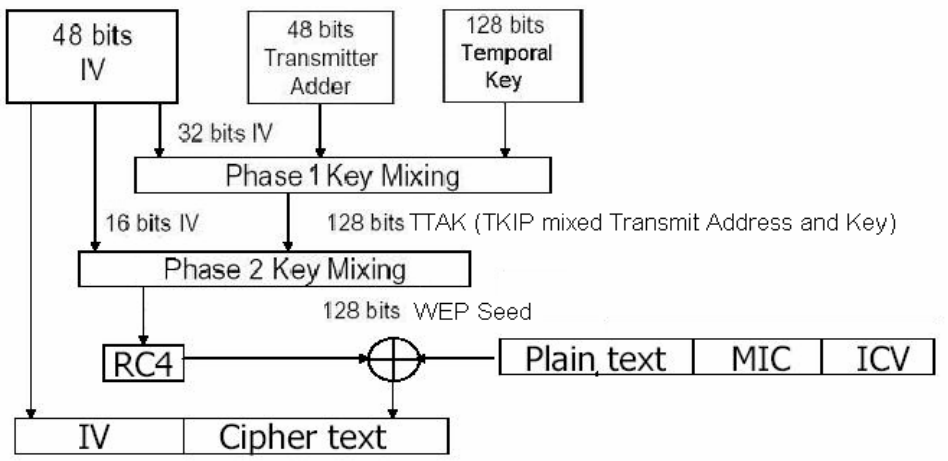

Figure 3: TKIP Key Mixing Encryption Flowchart

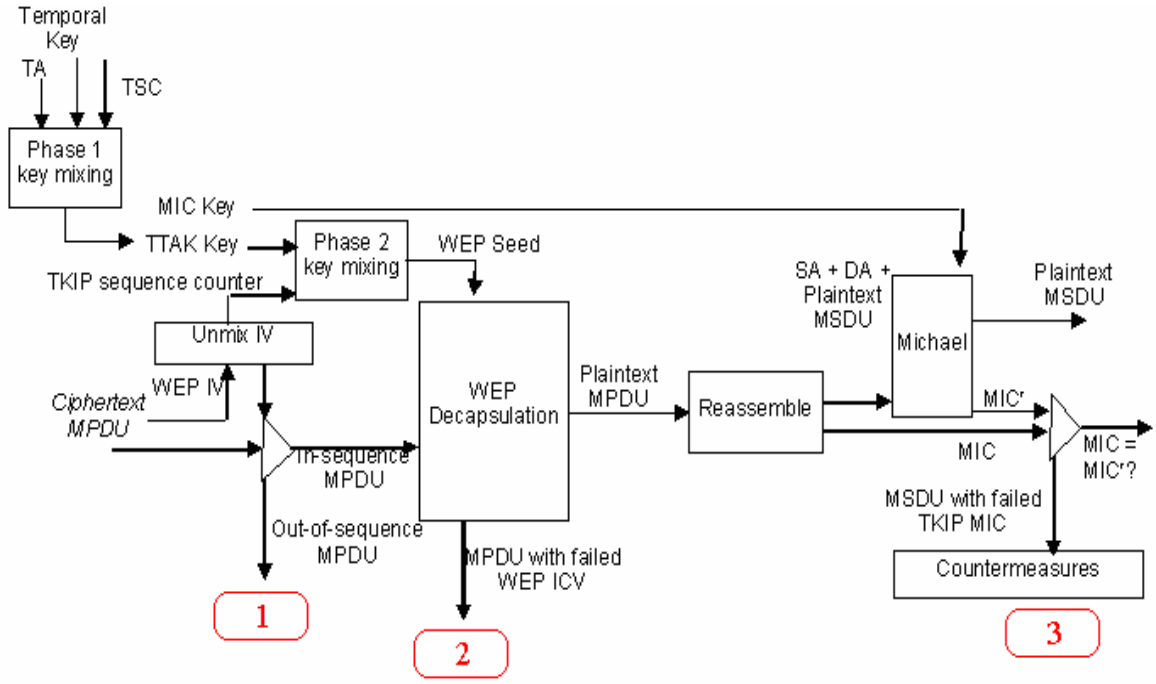

Figure 4: TKIP MSDU Decryption Flowchart

As Figure 5 shows, we experiment on practical environment. When using one 802.11g AP and one Notebook to connect 802.11g wireless NIC card of PCMCIA, which connect to 802.11g, 54 Mbps transmission mode; also use NetIO Corporation's Chariot version 4.0 software to test and observe the transmission flow without using TKIP encryption.

Figure 6 shows the average throughput between access point and client without TKIP encryption that using Chaiot to simulate traffic. As concludes from Figure 6, we can see that average throughput is 19.4 Mbps. Then enables TKIP function on AP and Notebook, and uses the same conditions to experiment the throughput on AP side. The result is shown in Figure 7. We can obtain the actual throughput is 12.4 Mbps. From the experiment result, we can conclude that the method of TKIP encryption seriously decreases the efficient throughput of AP.

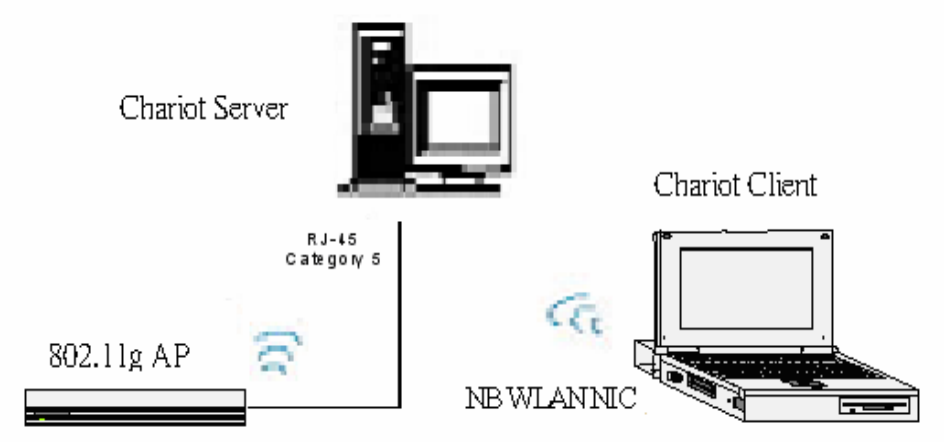

Figure 5: TKIP testing platform

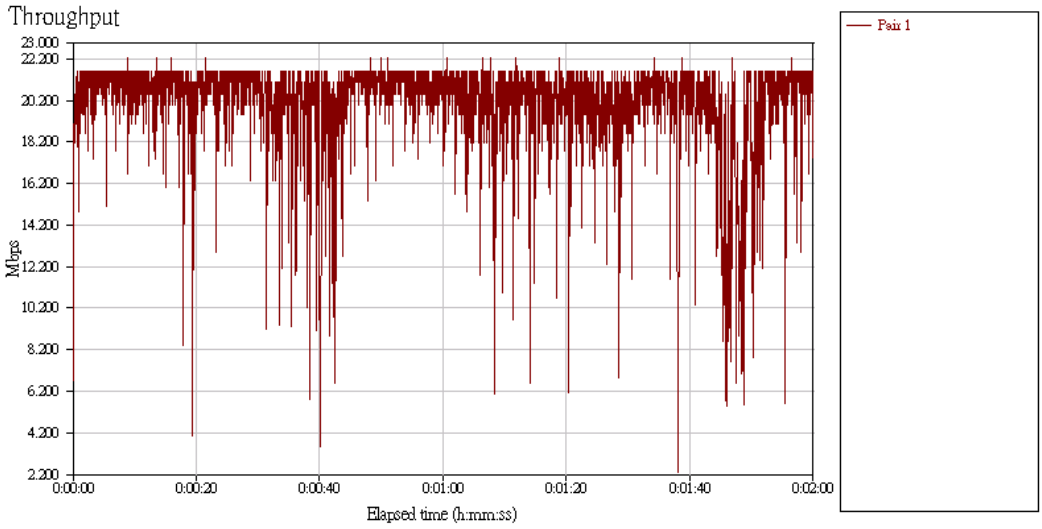

Figure 6: transmission flow at 802.11g without enable TKIP

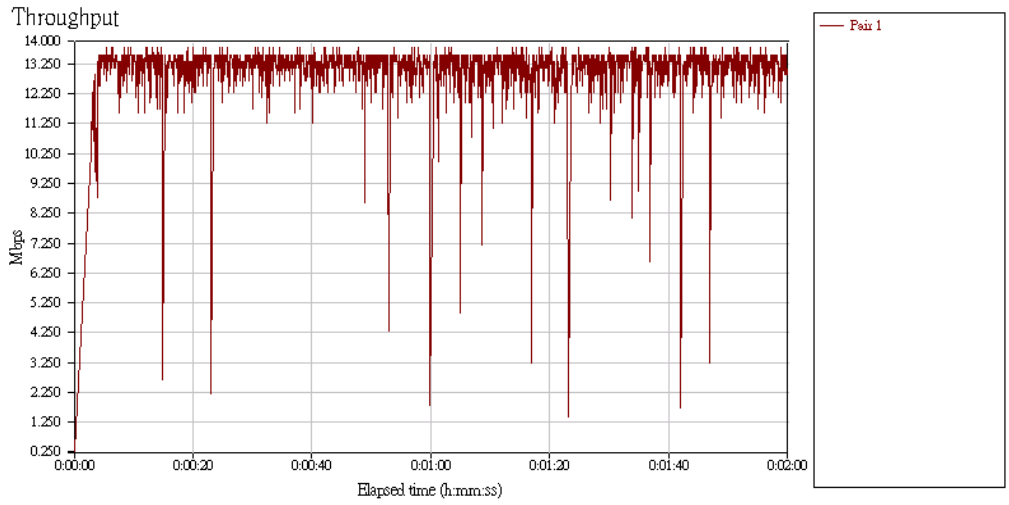

Figure 7: transmission flow at 802.11g that enable TKIP function

3. Proposed Method: Burglarproof WEP Protocol

As previous section described, TKIP resolve the security drawbacks of WEP, but it also causes serious throughput diminished. This section will propose a novel schema: Burglarproof WEP Protocol, BWP, which modifies the process of WEP Key generation on TKIP. Compare with TKIP, the proposed protocol neither change nor increase hardware cost, and narrow down hardware computing quantities. Further, BWP reduces authentication frequency but can provide security function as well as TKIP and will not affect the performance of throughput. The features of BWP include three parts: first, the process of WEP KEY generation, second, the form of Frame Integrity Code, FIC, and the last, user authorization.

The design principles of BWP must be satisfied as following rules:

(1) Use the simple schema to cover WEP drawbacks and provide the same secure transfer function as TKIP.
(2) All clients use the same secret key. The key will be easy to management, and it can speed up key updating synchronously for all users.
(3) Use the WEP RC4 encryption method. America restricts within export of encryption-decryption technique. For this issue, BWP continually uses RC4 encryption method to conform exporting criteria.
(4) Resolve the loopholes in the RC4 wake key.
(5) The IV field is 4 bytes to narrow down the length of packet header.
(6) The identical IV does not generate the same RC4 encryption seed so that to prevent packet collection attraction.
(7) After run out of 24 bits IV key, new WEP Key will be generated so that to prevent packet collection attraction.
(8) At the initial communication status, clients use the same default WEP key, but when they start to transfer data, they will use temporal key to avoid stealing of

default WEP key.

(9) When receiver finds the packet sequence number is the same or smaller, it discards packet to prevent active attack.

(10) The proposed protocol could be implemented on current hardware, ARM7 or ARM9 CPU, with update firmware.

(11) Use temporal key to make authentication that could resolve core error problem.

Figure 8 shows the frame structure of BWP MPDU. The length of IV field is 4 bytes that shorter than TKIP but the same with WEP. BWP adds 3 bytes Frame Integrity Code (FIC) field between Data field and ICV field. The frame structure of BWP is very similar with TKIP and WEP. BWP is draw up to use PRNG RC4 cipher as well as WEP and TKIP, but the generation steps of WEP key that before WEP PRNG are less than TKIP. The encryption fields of BWP protocol are Data, FIC, and ICV.

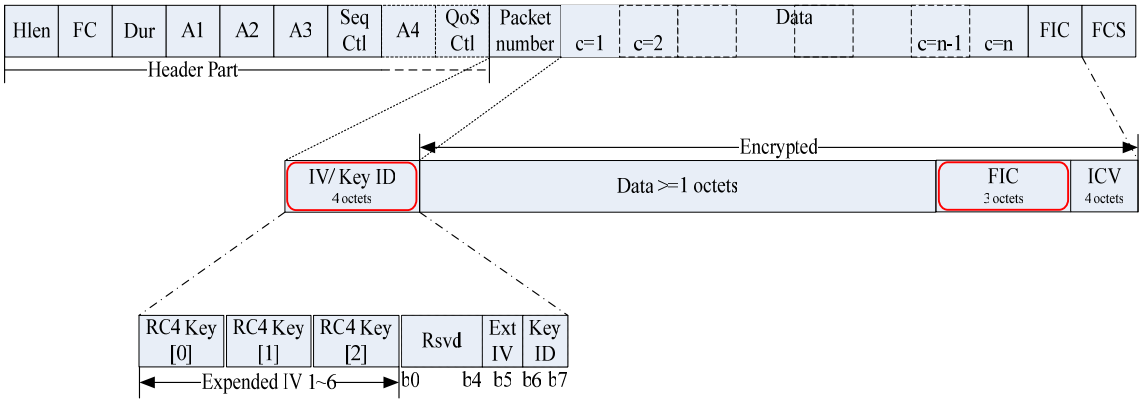

Figure 8 BWP MPDU Frame

As usual, BWP use TKIP RC4 cipher engineer to execute encryption, it contents three components: the generation of new secret WEP key, authentication of BWP and IV generation. The detail encryption flow is addressing as following:

Step 1. Generation of new secret WEP key

When client joins AP domain first time, it sends a random number to AP. Then, both AP and client sides do hashing function to product new secret key synchronously and records client MAC address at AP. This random number is for synchrony to notified AP that the client will send data. And then, AP generates another random number and sends it to client. Using this new secret key to be the new WEP key can avoid fixed default secret key (default WEP key) be founded. The process is shown in figure 9.

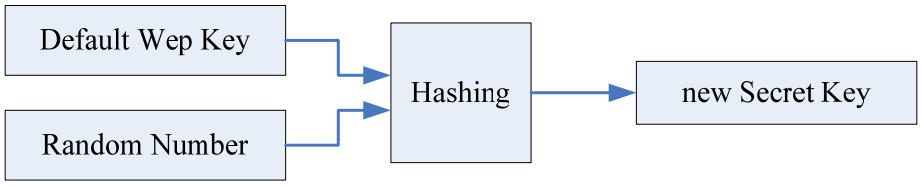

Figure 9: generation process of New Secret Key

Step 2. Authentication of BWP

After generate new secret key, AP sends random number to client. Then AP and client use new secret key (generated at step 1) and this random number (sent by AP) to hash another new secret key1, and use this new secret key1 as the authentication, as shown in figure 10. All BWP encryption actives will use this new secret key 1 to encrypt transformation data to instead of default WEP key. The new secret key is only for authentication. After pass authenticated, it will be discard. Even if the attacker uses core error that proposed by Marylan [5] to gain new secret key1, they cannot be backward to new WEP key and then cannot transfer data or detect packet content.

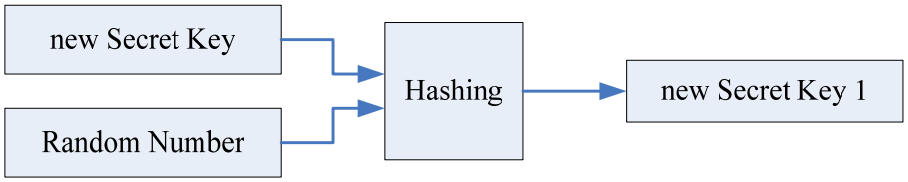

Figure 10: generation process of New Secret Key1

Step 3. IV Generation

IV Generator is to manage the generation of IV_{24Bits}. IV Generator will filter Strong IV Number and after run out of IV_{24Bits}, it will notify client and AP to update new WEP key. IV generator can avoid producing RC4 wake key, too. As example, when the first byte of IV value is between from 3 to 14 and the second byte is FF can be backward to secret key. Use IV generator can filter strong IV number and combines new secret key to generate RC4 cipher $seed_{64bits}$ (include IV).

Figure 11: the steps of IV generator

Step 4. Update steps of secret key:

When run out of IV_{24bits} value, secret key will update. The client send random number to AP and then AP and client do hashing function to product new secret key synchronously and records at both client and AP sides. The shorter the IV field is, the faster the secret key update. Show as figure 12.

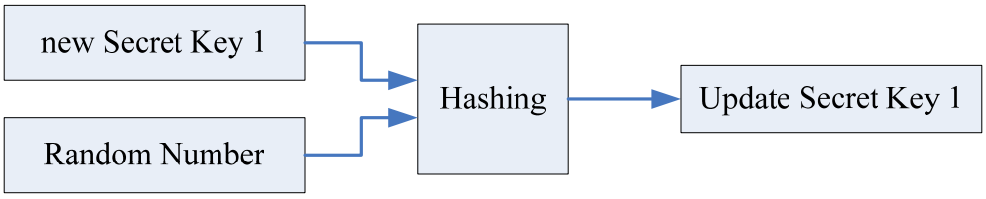

Figure 12: update steps of secret key

Step 5. Frame Integrity Code (FIC) : frame confidential detection

The FIC field is generated 24 bits initial sequence number by hashing with new secret key and sender's TA (transmitter MAC address). CRC32 frame check includes this field and the ICV (integrity check value) is locating after FIC field.

Generate steps of Sequence Number shows as follows:

Sequence Number $_{(24bits)}$ = SHA1 (newSecret $_{(40bits)}$, Random Number $_{(16bits)}$)

The output MPDU of BWP shows as follows:

Message: M; Sequence Number: N

Compute integrity checksum ICV = c(M+N), using CRC32

The plaintext P = { M+N || c(M+N) }

Encrypt P using RC4: cipher text C = (P ⊕ RC4 (IV, newSecret Key))

Transmit C' = IV, (P ⊕ RC4 (IV, newSecret Key))

BWP adds 24 bits sequence number field after data payload in the MPDU frame. It will accumulate this sequence number for the following MPDU frame. After runs out of IV and updating secret key, the sequence number will regenerate. The complete frame structure is shown in figure 8. If frame error occurs, AP will separate this user for one minute.

In order to get batter decryption performance, BWP use the same decryption method with 802.11 WEP. The FIC field records sequence number in each MPDU frame. When decryption progressing, SWTP compares sequence number in the frame. This can ensure the integrity of each frame and prevent active attack. Figure 13 and 14 shows the encryption and decryption flow chart of BWP.

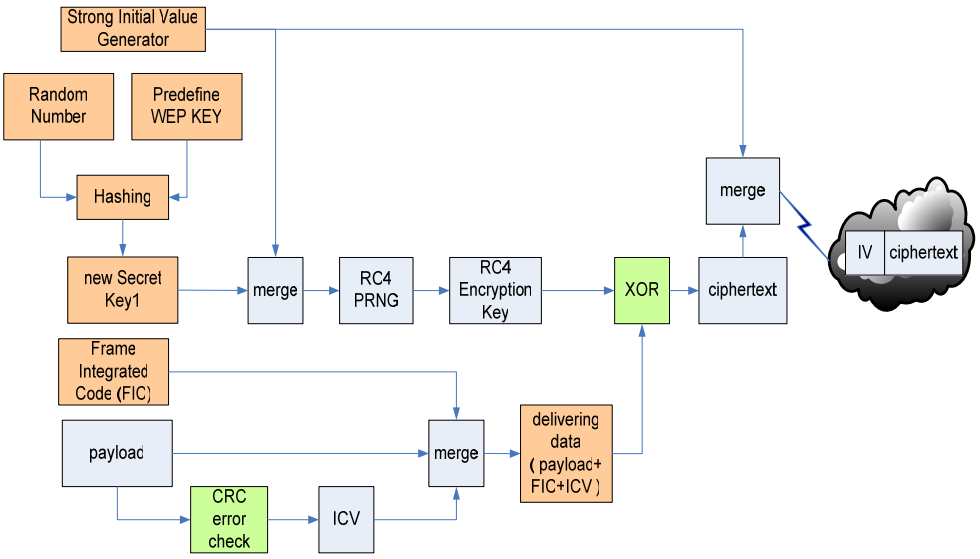

Figure 13: encryption steps of BWP

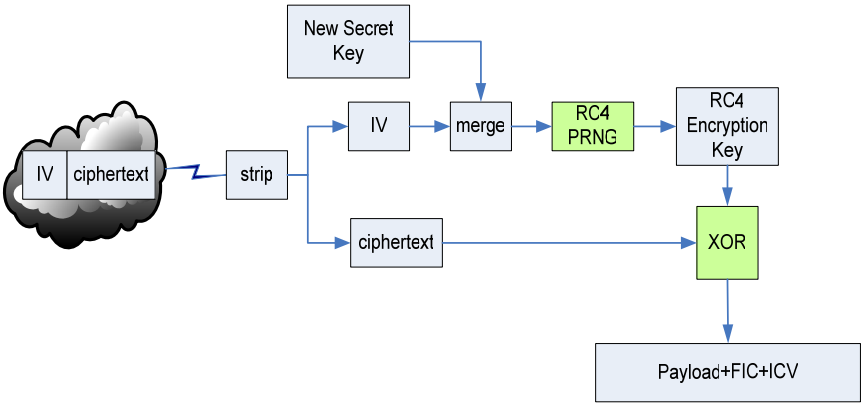

Figure 14: BWP Decryption Flowchart

4. Simulation and Results

BWP provide the same security rank with TKIP. But the different between BWP and TKIP are the ways of key generation and data confidential detection. Both BWP and TKIP can prevent current WEP attacks and drawbacks by upgrading firmware. Table 1 shows the mapping of attack methods versus protection schemas for BWP and TKIP. However, BWP has better throughput than TKIP.

As shown in figure 5, we construct an infrastructure wireless LAN to evaluate throughput practically. In this WLAN environment, there is an 802.11g AP with ARM9 100MHz CPU, and perform BWP and TKIP by software coding. The client is a notebook which using 802.11g PCMCIA wireless LAN adapter. The traffics are produced by Chariot, version 4.0, and uses maximum transmission speed to observe the throughput under three infrastructure modes: no data encryption, enable TKIP, and enable BWP.

Table 1: Protection schema for BWP and TKIP

Attack method	BWP protection schema	TKIP protection schema
Forgery (Bit-Flip)	FIC (Frame Integrity Code)	MIC(Message Integrity Code)
Weak-Key Attacks	Weak key will be filtered	Dynamic Key
Collision Attacks	Secret Key Update	Re-Keying
Replay Attacks	Sequence Number	Sequence Number

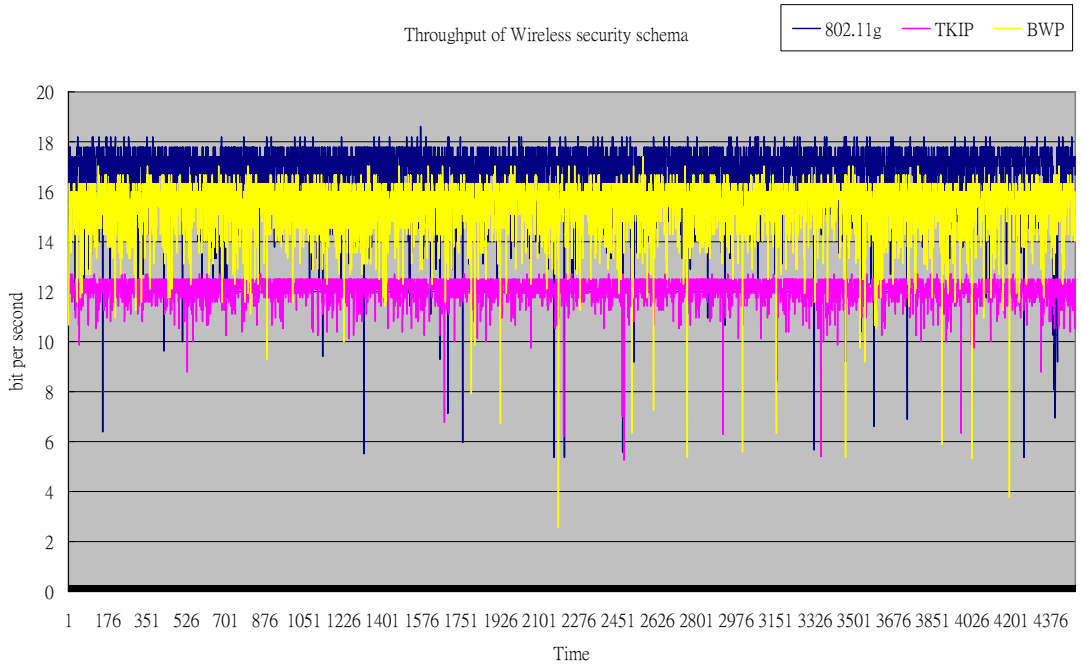

Figure 15: Throughput of BWP, TKIP and 802.11g

Figure 15 is the experiment results. Analyzing figure 15, we can find that if data delivers without any secure protection, the average throughput is 15.778Mbps. But once enable TKIP protocol, the average throughput is down to 9.301 Mbps. However, if enable BWP protocol, the average throughput is raising to 14.994Mbps. From this experimentation, we can find that the BWP is indeed improving the inefficiency throughput problem cause by TKIP.

From the simulation result we can find that BWP have better performance than TKIP. The performance of throughput just follows 802.11 that is no encryption schema enabled. The result is converged in table 2. It is very clearly to observe that the proposed schema have better performance. The Chariot generates whole wireless 802.11g frames with

complete header at full speed. The more the clients consume bandwidth, the more packets fill on the transmission channel. The packets collision and retransmission will increase due to WLAN employs CSMA/CA algorithm over layer 2 protocol. The total traffic increases but the efficient data throughput won't increase relatively. Even at this situation, BWP has better performance than TKIP when mentions about three clients. Also, the efficient throughput is greater than TKIP. Following, we will discuss more about the transfer appearance under BWP versus TKIP for multi-clients.

Table 2: Practical Lab testing of multi-clients

Average (Mbps)	One Client	Two Clients	Three Clients
No encryption	Pair1= 15.961 Totals= 15.778	Pair1= 8.955 Pair2= 8.940 Totals= 17.779	Pair1= 6.150 Pair2= 6.101 Pair3= 5.919 Totals= 17.890
BWP	Pair1= 14.994 Totals= 14.994	Pair1= 8.715 Pair2= 7.337 Totals= 15.947	Pair1= 6.207 Pair2= 6.147 Pair3= 6.004 Totals= 18.270
TKIP	Pair1= 9.362 Totals= 9.301	Pair1= 4.948 Pair2= 5.457 Totals= 10.364	Pair1= 3.950 Pair2= 3.212 Pair3= 3.883 Totals= 11.045

5. Conclusions

Unfortunately, at present wireless network environment, WEP and TKIP are unable to give consideration to the security and performance at the same time. Analyzing TKIP protocol, we inference that the critical reason of low throughput is TKIP's algorithm. In TKIP, the major algorithm of encryption is message integrity code, called Michael. It is too complexity to increase performance. Even though, it is still need a security scheme to improve network security efficiently. The most important thing is the manager should use appropriate encryption protocol to ensure their data transform security when communicate on wireless LAN. The proposed method, BWP, provide better performance and throughput to transfer data. The inductive reasons are two: first, at the same packet size, the BWP protocol overhead is shorter than TKIP; second, the TKIP encryption schema is much complexity than BWP. At the same time, it gives consideration to data delivering security. Data delivering from client to AP or from AP to client is the worst link for security issue, and a lot of attacks are occurred at this point. BWP not only avoids current security problems but also has better throughput. WEP and SSID can use to separate wireless domain.

For more advance application, the enterprise or security sensitive organizations, 802.1x or VPN are suggested to enhance user authentication and secure data

delivering. Although VPN can support better transmission protection, the traffic overhead is too large to utilize bandwidth efficiently. In practically, if IPSec function is enable, data throughput will cut down to 30% ~ 40%, and it will be worse when multiple client accesses. IEEE is now studying use 802.11i to replace of current WEP encryption. Wireless LAN manager can choice various specifications from different vendors on the market to protect their WLAN. But without identical standard, the compatible problem will persecute users when purchasing different brands. There are a lot of new protocols be provided to assist wireless network transformation security. But the 802.1x environment is very complicated for general users, and VPN will deliver a lot of conditions data to decrease throughput of valid data. BWP is easy to implement in every environment and will not raise hardware cost. It is suit for popular users.

6. References

[1] The Institute of Electrical and Electronics Engineers (IEEE), "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std 802.11, 1997.

[2] The Institute of Electrical and Electronics Engineers (IEEE), "IEEE 802.1X, http://standards.ieee.org/getieee802/ download/802.1X-2001.pdf" , 2001.

[3] The Institute of Electrical and Electronics Engineers (IEEE), "Draft Supplement to ISO/IEC 8802-11/1999(I) ANSI/IEEE Std 802.11, 1999 edition," IEEE Std 802.11i/D3.0, November 2002.

[4] Wireless Sniffers List http://www.personaltelco.net/ index.cgi/WirelessSniffers

[5] W. A. Arbaugh, N. Shankar, and Y. J. Wan. "Your 802.11 wireless network has no clothes". http://www.cs.umd.edu/~waa/wireless.pdf, Mar. 2001. University of Maryland report.

[6] Wireless Ethernet Compatibility Alliance (WECA) "WEP Security Statement" September 7,2001

[7] Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks Wi-Fi Alliance April 29, 2003

[8] Wireless Security and VPN: "Why VPN is Essential for Protecting Today's 802.11 Networks" by Intel

[9] Wireless network, Security, VPN "Wireless 802.11b Security in a Corporate Environment" Intel Information Technology White Paper March 2002