# Enhanced Wireless IEEE 802.11b Protocols Resistant to the Keystream Reuse Attack

*(Submitted to Cryptography and Information Security)*

*Ching-Nung Yang, Tsung-Yuan Cheng and Chen-Chin Kuo*

Department of Computer Science & Information Engineering,
National Dong Hwa University,
1, Sec. 2, Da Hsueh Rd., Shou-Feng, Hualien,
Taiwan, Republic of China
TEL: 886-3-8662500 Ext-22120 FAX: 886-3-8662781
E-mail: cnyang@mail.ndhu.edu.tw

## Abstract

The security mechanism of IEEE 802.11b wireless network standard is the Wired Equivalent Privacy (WEP) protocol. The WEP can be used to protect communications from eavesdropping and other attacks. In fact an effective attack, called as keystream reuse attack, that aims at a public value initialization vector (IV) in WEP header is proposed. Here, we propose enhanced protocols resistant to the attack by lengthening the reuse cycle of IV.

Keywords: IEEE 802.11b, Wireless Equivalent Privacy, RC4, keystream reuse attack.

Contact author: Ching-Nung Yang
E-mail: cnyang@mail.ndhu.edu.tw

## 1. Introduction

IEEE 802.11b is a wireless network standard. Users have the ability to access the Web, transfer files, and do other high bandwidth activities without cables. Because wireless medium is a public channel, the message over a wireless interface may be intercepted. Therefore, encryption/decryption and authentication are always considered when using this wireless networking system. IEEE 802.11b standard [1], [5] provides a security mechanism to encrypt the message and authenticate the access nodes by using the WEP protocol.

In wireless environment, the mobile device is battery-limited and thus it cannot provide complex computations. So, the WEP protocol does not use public key and block cipher but adopts the RC4 stream cipher. A keystream used in theP packet is generated by RC4. The inputs of RC4 are IV and the secret key. Since the value of IV is sent in the WEP header publicly. Thus, the keystream will be same for the same IV when secret key is not changed. Due to the encrypted result is only XOR-ed by keystream, thus the attacker can use a reused keystream to decrypt the ciphertext.

The paper is organized as follows. The WEP protocol and keystream reuse attack [2] are described in section 2. Section 3 shows our enhanced WEP protocols and gives the compared results. Finally, we give a conclusion in section 4.

## 2. The WEP Protocol and Keystream Reuse Attack in IEEE 802.11b

### 2.1 The Wireless Equivalent Privacy (WEP) protocol

WEP provides two features. One is to assure privacy through encryption and the other is to supply the access control in wireless access point (AP) [1], [3] using RC4 stream cipher. RC4 cipher operates by expanding a secret key to a random long pseudorandom bits (keystream). The secret key of RC4 is a public value IV *v* (24-bit) and a key *k* (40-bit) and the output is a long pseudorandom binary sequences. The key *k* must be shared by both the client and AP in advance. The Integrity Check Value (ICV) field is a 32-bit CRC check on the plaintext. The ICV will be appended to the end of the plaintext. Encryption is performed by XORing the generated keystream and the "plaintext+ICV" (see Figure 1). Then, concatenate IV and ciphertext to form a WEP packet. Consider description, we get the keystream using the received IV *v* and the shared key *k*. We can recover the plaintext by using bitwise addition of the ciphertext and keystream.

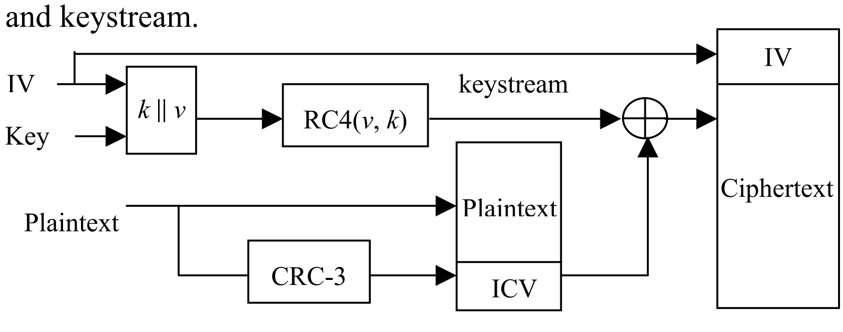

Figure 1. WEP Encryption

### 2.2 Keystream Reuse Attack in IEEE 802.11b

The keystream RC4 ($v$, $k$) is a function of the values $v$ and $k$. The key k will be same for all packets during the lifetime of key. The IV $v$ is different for each packet. Thus, the keystream varies with the value of IV that is sent in WEP header.

The WEP standard recommends (but does not require) that the IV needs to be changed for every packet. The IV is publicly sent (see Figure 1). So, the receiver know what IV used to derivive the keystream for decryption. The IV is also known to attacker, but the key remains secret and maintains the security of keystream.

The IV field used by WEP is only 24 bits, nearly assuring that the same IV will be reused for some packets. If we use sequential IV, i.e., we start from IV=0 and change IV with IV+1 for each packet until IV=$2^{24}$-1 and then reset IV to 0. A back-of-the-envelope calculation shows that a busy AP sending 1500 byte packets and achieving an average 5Mbps bandwidth will exhaust the available space in less than 11 hours (($2^{24}\times1500\times8/5\text{Mbps} \approx 11.1848$ hours). It means that every 11 hours, the keystream will repeat. Note that, reuse of the IV will cause the same value of keystream. The use of a per-packet IV was intended to prevent keystream reuse attacks. Nonetheless, WEP also has the keystream reuse attack problem [2].

When using sequential IV, some PCMCIA cards will reset the IV to 0 when they are re-initialized. If these cards re-initialize frequently, keystream corresponding to the low-valued IV may be reused many times.

The method of random IV was proposed to overcome the re-initialzed problem of PCMCIA card. Nevertheless, if the card uses a random 24-bit IV for each packet, then it will be expected to incur collisions after transmitting about 5000 packets (as described below), which is only a few minutes of transmission. It means that the problem of keystream reuse may be more serious. The random IV cannot conquer the problem.

$$(2^{24}/2^{24})\times((2^{24}-1)/2^{24}))\times((2^{24}-2)/2^{24}))\ldots\times((2^{24}-i)/2^{24}))\le 1/2 \qquad (1)$$

The smallest value of $i$ is 4823 satisfying the above equation such tat the collision probability will be about 1/2.

Figure 2 shows the two choices of IV, sequential IV and random IV.

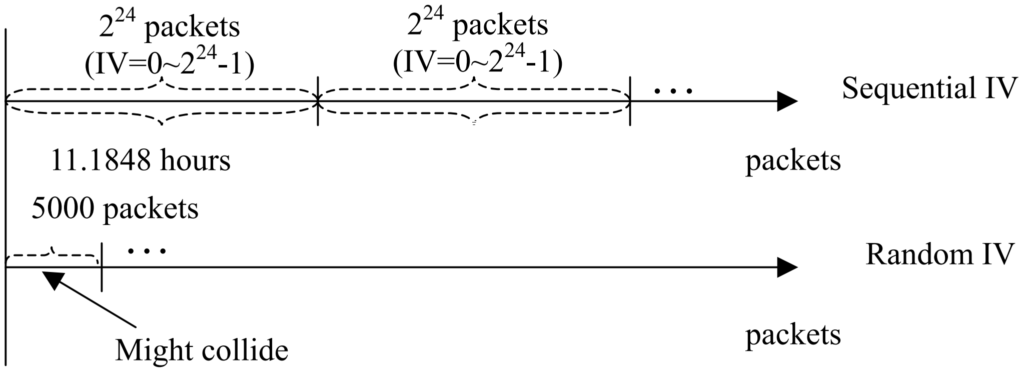

Figure 2. Sequential IV and Random IV

If the reused cycle of keystream is small, it will be reused frequently. The attacker can build a table the keystream and its corresponding IV. The full table has at least space requirements perhaps 1500 bytes for each of the $2^{24}$ possible IV, or roughly 24GB (1500-byte $\times 2^{24}$). At this time, it becomes possible to immediately decrypt the intercepted ciphertext.

Here, we provide four methods to increase the reused cycle of keystream and some methods can also solve the re-initialized problem.

## 3. Enhanced IEEE 802.11b Protocols

Rethinking the keystream RC4($v$, $k$), the inputs are $v$ and $k$. $v$ may be sequential or random and $k$ will be fixed during the life cycle of secret key. Now, if we choose the values of $v$ and $k$ using both "sequential" or "random" sequence, then there are four possible combinations (see table 1). We calculate the reused cycle of keystream for these four methods and also show whether they solve the re-initialized problem or not.

Table 1. Four possible choices of $v$ and $k$

| | Key ($k$) | IV ($v$) |
|---|---|---|
| Method 1 | Sequential | Random |
| Method 2 | Sequential | Sequential |
| Method 3 | Random | Sequential |
| Method 4 | Random | Random |

### Method 1:

The inputs of RC4 cipher are the public IV (24-bit) and key (40-bit). IV is random for and key is sequential for each packet in this method. The keystream is generated by RC4 and the key pair ($v$, $k$) is input. The range of the key is 0~($2^{40}$-1). In the first $2^{40}$- packets, if IV is reused, the keystream RC4($v$, $k$) would not be same, because the key is added 1 ($k$=$k$+1) for each packet. In the first $2^{40}$-packets, the value of RC4($v$, $k_i$) will not be equal to the value of RC4($v$, $k_j$), where $i \neq j$. Next, in the second $2^{40}$-packets, while choosing the IV, the IV might be in collision with IV for the same key in the first $2^{40}$-packets. The "$i$" indicates that there are "$i$" IV in the prior $2^{40}$-packets which have been selected. Therefore, there are only ($2^{24}$- $i$) IV left to use. The "$n_i$" less than $2^{40}$ indicates that there are $n_i$ key pairs ($v$, $k$) that would be selected in current $2^{40}$-packets.

When the IV is random and the key is sequential for each packet, the reused cycle of keystream can be calculated as follows. Find the smallest value of $i$ and $n_i$ satisfying Equation (2). Note that if the probability is less than 1/2, the key pair probably collides.

$$\prod_{j=1}^{2^{40}}(2^{24}/2^{24})^j \times \prod_{j=1}^{n_1}(2^{24}-1/2^{24})^j \times \prod_{j=1}^{n_2}(2^{24}-2/2^{24})^j \times \Lambda \times \prod_{j=1}^{n_i}(2^{24}-i/2^{24})^j \le 1/2 \qquad (2)$$

The final calculated result is that $i$=1 and $n_1$=11629080. So, the reused cycle of keystream approximates to $2^{40}$ +11629080 as shown in Figure 3.

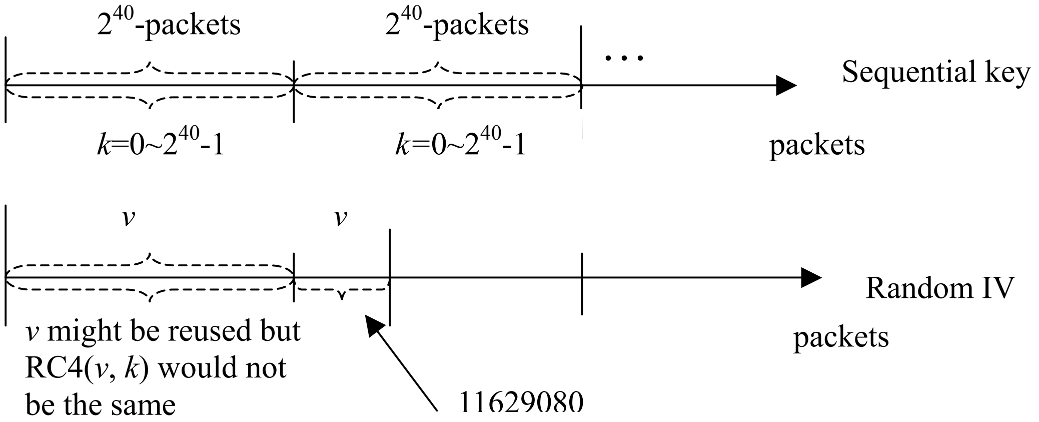

Figure 3. Random IV and Sequential key

**Method 2:**

The IV is sequential for each packet. Therefore, the range of the IV is 0~($2^{24}$-1). After encrypting $2^{24}$ packets, the key $k$ is changed to $k$+1. Initial value of the IV is 0. The keysream is generated as follows. RC4 ($v$, $k$ mod $2^{40}$), RC4($v$+1, $k$ mod $2^{40}$), …, RC4($v$+$2^{24}$-1, $k$ mod $2^{40}$), RC4($v$, ($k$+1) mod $2^{40}$), RC4($v$+1, ($k$+1) mod $2^{40}$), …, RC4($v$+$2^{24}$-1, ($k$+1) mod $2^{40}$), …, RC4($v$+$2^{24}$-1, ($k$+$2^{40}$-1) mod $2^{40}$).

Therefore, the reused cycle of keystream is $2^{24}$×$2^{40}$=$2^{64}$ as shown in Figure 4.

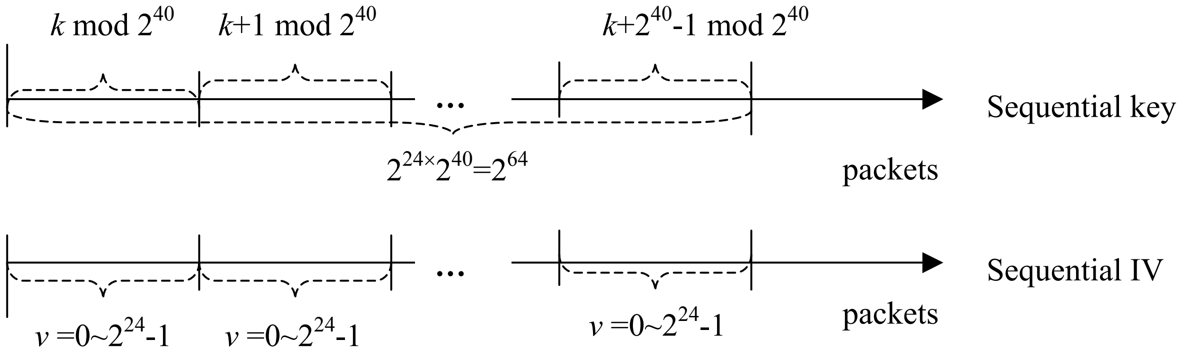

Figure 4. Sequential IV and Sequential key

**Method 3:**

In this Method, the IV is sequential and the key is random. We use hash function to generate random value from the key $k$ as follows. $k \rightarrow H(k) \rightarrow H^2(k) \rightarrow H^3(k) \rightarrow \ldots \rightarrow H^n(k)$, where $n$ is $2^{40}$-1 and H(·) is a hash function. The mobile device and AP can synchronize to share the same secret key. For example, for $i$-th packet, the secret key is $H^i(k)$. Same as the analysis in Method 1, the reused cycle of keystream can be calculated as follows.

$$\prod_{j=1}^{2^{24}}(2^{40}\big/2^{40})^{j}\times\prod_{j=1}^{n_1}(2^{40}-1\big/2^{24})^{j}\times\prod_{j=1}^{n_2}(2^{40}-2\big/2^{24})^{j}\times\Lambda\times\prod_{j=1}^{n_i}(2^{40}-i\big/2^{24})^{j}\leq 1/2 \qquad (3)$$

The final calculated result is that $i$=301 and $n_i$=15388777. So, the reused cycle of keystream approximates to $2^{24}$×301+15388777 shown in Figure 5.

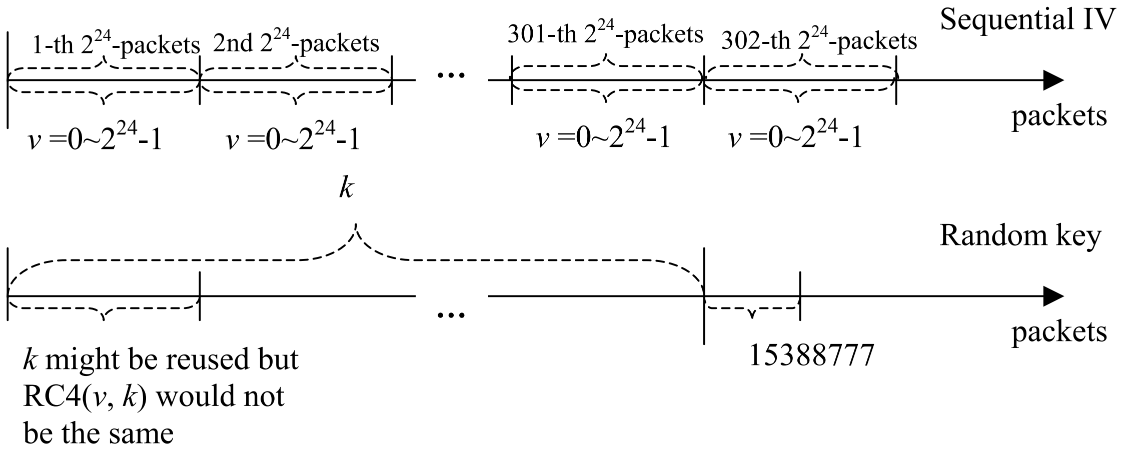

Figure 5. Sequential IV and Random key

**Method 4:**

IV and key are all random for this method. The random key shared by client and AP is obtained by hash function. The reused cycle of keystream is calculated as follows. It is described as follows:

$$(2^{64}/2^{64})\times((2^{64}-1)/2^{64}))\times((2^{64}-2)/2^{64}))\ldots\times((2^{64}-i)/2^{64}))\leq 1/2 \qquad (4)$$

When $i$=$2^{32}$+3532997052 the collision probability is less than 1/2. So, the reused cycle of keystream is $2^{32}$+3532997052.

## 4. Compared Results and Discussion

Table 2 shows the compared results for six methods, two original WEP methods (one uses sequential IV, the other uses random IV) and our proposed four methods.

Table 2. The reused cycle of keystream for different methods

| | Original WEP | Original WEP | Method 1 | Method 2 | Method 3 | Method 4 |
|---|---|---|---|---|---|---|
| IV | 0~$2^{24}$-1 sequential | 0~$2^{24}$-1 random | 0~$2^{24}$-1 random | 0~$2^{24}$-1 sequential | 0~$2^{24}$-1 sequential | 0~$2^{24}$-1 random |
| Key | Fixed | Fixed | 0~$2^{40}$-1 sequential | 0~$2^{40}$-1 sequential) | 0~$2^{40}$-1 random | 0~$2^{40}$-1 random |
| Keystream | $2^{24}$ | 5000 | $2^{40}$+11629080 ≈$2^{40}$ | $2^{64}$ | $2^{24}$×301+15388777 ≈$2^{32}$ | $2^{32}$+3532997052 ≈$2^{33}$ |
| solve the re-initialized problem | No | Yes (NOTE: the reused cycle of keystream is only 5000) | Yes | No | Yes | Yes |

From Table 2, our methods increase the reused cycle of keystream. Method 1, 3 and 4 can also solve the re-initialized problem. Method 2 will raise the reused cycle of keystream up to $2^{64}$.

In WEP protocol, the input of RC4 is 64-bit sequence and divided to 24-bit IV and 40-bit key. IV and key could be $m$, $n$ bits, respectively, and $m + n = 64$. If “$n$” is too small, it would be compromised by brute force attack and the key will be obtained easily. If the “$m$” is small, collisions will occur frequently and the WEP will be attacked using keystream reuse.

WEP also provides the 128-bit RC4 cipher to enhance the security in the system. The IV is 24-bit and the key is 104-bit. In original IEEE 802.11b standard, IV is still 24-bit. Here, we recommend that WEP can increase IV from 24-bit to 40-bit (or more) such that it can prevent the keystream reuse attack because the attacker now needs to build a large table to save the IV and keystream. At this time, the key is also large enough to resist brute force attack. However, even using long IV, the re-initialized problem still exists for 128-bit RC4. Our methods can be applied to avoid the problem.

## 5. Conclusion

The WEP protocol will be compromised by keystream reuse attack. It lets the attacker easily to attack the system without decrypt RC4 cipher. In this paper, we propose four possible combinations of IV and key. The optimal method that can resist the keystream reuse attack and re-initialized problem is Method 1 that uses random IV and sequential key.

## References

[1] IEEE Standard Board, “802 part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, 1999 Edition.

[2] N. Borisov. I. Goldberg. D. Wanger. “Interception Mobile Communications: The Insecurityof 802.11”. The Seventh Annual International Conference on Mobile Computing And Networking, July 16-21, 2001.

[3] Sultan Weatherspoon, Network Communications Group, Intel Corporation. “Overview of IEEE 802.11b Security”. Intel Technology Journal Q2, 2000.

[4] W.A. Arbaugh, N. Shankar, and Y. J. Wan. Your 802.11 Wireless Network Has No Clothes, March 2001.

[5] ANSI/IEEE Std 802.11b, 1999 Edition

[6] R. L. Rivest. The RC4 Encryption Algorithm. RSA Data Security, In c., Mar. 12, 1992

[7] 3COM Technical Paper “IEEE 802.11b wireless LANs: Wireless Freedom at Ethernet Speeds” [Online document], 25 April 2000. Available URL: http://www.3com.com/technology/tech_net/white_papers/503072.html

[8] "Introduction to IEEE 802.11," [Online document]. Available URL: http://www.intelligraphics.com/articles/80211_article.html