Security Enhancement of WEP Protocol IEEE802.11b with Dynamic Key Management


Abstract—Wireless network security has become a strong requirement for effective deployment of wireless communication applications. There are obviously some reasons for users who like to use wireless technology because of its various benefits. However, as the attacks against WLANs are easier than LANs, the security architectures in WLANs have been discussed frequently. In this paper, the vulnerabilities and weakness of WEP protocol which is used in IEEE 802.11b have been analyzed. A new dynamic key generation scheme that surely enhances the security of WEP (Wired Equivalent Privacy) has been proposed. The proposed method found to be more effective than conventional system.

Index Terms—Wireless Network, IEEE 802.11b, Dynamic Key, IV.

I. INTRODUCTION

A wireless LAN is the perfect way to improve data connectivity in an existing building without the expense of installing a structured cabling scheme to every desk. There are however, in most wired LANs the cables are contained inside the building, so a would-be hacker must defeat physical security measures (e.g. security personnel, identity cards and door locks). In WLANs, privacy is achieved by data content protection with encryption. Encryption is optional in 802.11 WLANs, but without it, any other standard wireless device, can read all traffic in network [1].

The designers of the IEEE 802.11b or Wi-Fi tried to overcome the security issue by devising a user authentication and data encryption system known as Wired Equivalent Privacy, or WEP. IEEE 802.11i [2], an IEEE standard ratified June 24, 2004, is designed to provide enhanced security in the Medium Access Control (MAC) layer for 802.11 Networks. There is some work on security weakness of WEP protocol and enhancing the security. Zhang Longjun et al [3] have worked on improved key management scheme emphasizing key decryption, using hash function of temporal key and

Manuscript received May 11, 2011; revised July 20, 2011. This work was supported in part by the U.S. Department of Commerce under Grant B512345G (sponsor and financial support acknowledgment goes here).

Mahmudur Rahman Author is with the Electronics and Telecommunication Engineering Department Daffodil International University, Dhaka, Bangladesh (e-mail: riyad_ete@yahoo.com).
Md. Asif Hassan Riyad Author is with the Electronics and Telecommunication Engineering Department Daffodil International University, Dhaka, Bangladesh (e-mail: asif_down@gmail.com).
Md. Ibn Sinha Author is with the Electronics and Telecommunication Engineering Department Daffodil International University, Dhaka, Bangladesh (e-mail: sinha_diu@yahoo.com).
A.K.M Fazlul Haque Author is with the Electronics and Telecommunication Engineering Department Daffodil International University, Dhaka, Bangladesh (e-mail: akfnhaque@daffodilvarsity.edu.bd).

based on table search. Maocai Wang et al [4] have worked on security analysis for IEEE802.11 and described the IV repetition issue.

Conventional WEP system cannot ensure data confidentiality and integrity due to its some security has vulnerability. To overcome this problem, WPA and WAP2 introduced the concept which generates dynamic keys, it uses 48 bit Initialization Vector (IV) compared to the 24 bit Initialization Vector in WEP. So a significant bandwidth is required. On the other hand the more we increase the security the performance will also be decreased. The implementation of WPA and WPA2 is not possible with the existing devices. So, the aim and objective is to enhance the security issues of WEP system by generating dynamic key which is also compatible with the existing device.

This paper focuses on several security issues of WEP and also proposes an improved key management scheme that reduces the IV repetition possibility issues.

II. BACKGROUND

WEP cannot meet the security requirement of WLAN because of the flaws in WEP. There are mainly five flaws [5, 6] in WEP as following:

A. RC4 Algorithm

RC4 is a kind of stream key algorithm widely used. RC4 is composed of key schedule algorithm (KSA) and pseudo-random generation algorithm (PRGA). Some researches indicate that the RC4 algorithm is vulnerable in the aspect that every 256 keys or less produce one weak key. This is called invariance weakness [7]. The data that are encrypted with these weak keys will become breakable.

B. Key Management

WEP requires each wireless connection share a secret shared key for encryption. But it does not define any key management technique [7, 8]. So each frame sent through the connection is using the same key, which will ease the task for the hackers to break the WEP encryption [9]. The use of static WEP keys—many users in a wireless network potentially sharing the identical key for a long period of time is well-known security vulnerability. There is no prescription for the generation and renew of key.

C. Repetition of Initialization Vector

IV space in WEP is 24 bits of length, which is so small. A 24 bits binary string has the total combination of $2^{24} = 16777216$ possible results. Consider wireless...
network traffic of 11Mbps. Now if sender sends 1200B packets then:
The numbers of packets are sent per second =
\[
\frac{11 \times 10^6}{1200 \times 10^3} \approx 1146
\]

So it is seen that sender uses 1146 IV per second. So after 4hrs the IV will repeat.
\[
16777216 \div 1146 = 14639.80
\]
\[
= 4.07 \text{ Hrs}
\]

Once the IV is being reused the attacker can capture two cipher texts with two different plain text but the same key sequence. Now if we XORED these two cipher text with same key sequence then the attacker gets the XOR results of two plain text. According to the XOR result of two plain text data packets can be decrypted.

\[P_1 = \text{plain text 1}\]
\[P_2 = \text{plain text 2}\]
\[IV = \text{initialization vector}\]
\[Sk = \text{secret WEP-Key}\]
\[C_1 = \text{cipher text 1} = P_1 \oplus RC4(IV,Sk)\]
\[C_2 = \text{cipher text 2} = P_2 \oplus RC4(IV,Sk)\]

Then,
\[C_1 \oplus C_2 = (P_1 \oplus RC4(IV,Sk)) \oplus (P_2 \oplus RC4(IV,Sk)) = P_1 \oplus P_2\]

From the above operation, it is observed that if an attacker knows a plaintext due to the repetition of IV, then attacker can know the other plain text although he doesn’t know the key sequence.

In case of busy network by injecting huge ARP request the attacker can force the repetition of IV within several minutes.

D. CRC

WEP uses CRC-32 algorithm to ensure the data integrity during transmission. This CRC information is a part of the encrypted payload. The problem with CRC-32 is that it is linear.

\[CRC(x \oplus y) = CRC(x) \oplus CRC(y)\]

Here \(x\) and \(y\) is our information. This means if an attacker changes the encrypted data packet he can figure out the value that needs to be changed for the checksum. This results in the receiver thinking that the data is valid. As for example:

Let,
\[C = [X,\text{crc}(X)] \oplus RC4(IV,Sk)\]

Now \(X\) is the message and \(\text{crc}(X)\) is the corresponding CRC-32 information of \(X\). if an attacker change the message \(X' = (X + V)\) where \(V\) is the modified part then he needs to change the CRC-32 information for the modified data.

Let \(\text{crc}(V)\) is the corresponding CRC-32 information of \(V\). Then:
\[C' = C \oplus [\nabla,\text{crc}(\nabla)] = [X,\text{crc}(X)] \oplus RC4(IV,Sk) \oplus [\nabla,\text{crc}(\nabla)]\]

This way the attacker can substitute the original plain text \(X, \text{crc}(X)\) with the modified plain text \(X', \text{crc}(X')\) by receiving the source station address. So the receiver identifies as a valid data.

E. Authentication

The authentication mechanism in WEP is unidirectional, the AP only authenticates the client but there is no way to authenticate the AP by client. This problem can cause Denial of Service attack (DoS).

III. PROPOSED SCHEME FOR WEP

In this part, a new approach to reduce the flaws which is occurred in Wired Equivalent Privacy (WEP) has been proposed

A. Proposed Solution

The proposed solution ensures a new era in the following services that WEP always try to provide:

Data Privacy:

In proposed solution, dynamic key for encryption which starts from the authentication process is introduced and based on which temporary shared key for further encryption, decryption process have been generated. It has also been proposed a different way of using IV which can reduce IV collision. As a result data privacy will be increased.

Data Integrity:

Here, a new way to implement the CRC-32 checksum algorithm in WEP encryption which will ensure better data integrity has been proposed.

The Proposed Scheme is started from the authentication process:

B. Dynamic Key Generation during Authentication Process

The authentication process (Fig. 1) works as follows: Let \(S\) be the station and \(R\) is the authenticator. As like as conventional WEP authentication process at first \(S\) sends the challenge text with a random number \(N_o\) to \(S\). same \(N_o\) is also stored in \(R\) when the \(S\) receives the challenge text with \(N_o\) then \(S\) stores \(N_o\) and calculate the following dynamic key:

\[k_1 = h(\text{Sk} \oplus N_0)\]

Where, \(K1 = \text{Dynamic key generated by S}\)
\(\text{Sk} = \text{Shared secret WEP key}\)
\(N_o = \text{Random number generated by authenticator}\)
\(h = \text{hash function [ref]}\)
S encrypts the challenge text with shared secret WEP key
and sends the challenge response to authenticator R. The R
decrypts the encrypted challenge text using shared secret
key, if they are same then the authenticator R authenticates
the station S and calculates the following dynamic key:

\[ K_1 = h(Sk \oplus N_0) \]

Where, \( K_1 \) = dynamic key generated by R
\( Sk \) = Shared secret WEP key
\( N_0 \) = Random number generated by authenticator
\( h \) = hash function

After successful authentication both the R and S side
has the same dynamic key which is used as shared key
for next encryption decryption process. The Length of
dynamic key is 128 bit.

### C. Proposed WEP Encryption

Here both the station S and the authenticator R have the
same initial shared key \( K_1 \) which is used for first
encryption decryption procedure. Based on the initial shared
key \( K_1 \) a new temporary dynamic key will be generated. So
for better understanding we have described our encryption
process in two steps:

**Step 1**

The first frame is encrypted using \( K_1 \). Let X is the message
and the checksum is crc(Xm). Here crc(Xm) will not only
compute over X but also include dynamic key \( K_1 \) with it.
That is crc(Xm) is the integrity check value of message X,
dynamic key \( K_1 \). So the plain text will become:

\[ P = [X, crc(Xm)] \]

**Step 2**

The first frame which is been encrypted using \( K_1 \) will be
decrypted at the client side (describe at the decryption
process), so we need a new dynamic shared key which is
used for next encryption process.

The step 2 (Fig. 3) works as follows:

Step2 encryption process is same as step 1 except the
creation of new dynamic key. Here the authenticator R
remembers the stored \( IV_1 \) and creates the new dynamic
key \( K_2 = h(K_1 \oplus IV_1) \). Now this dynamic key \( K_1 \) will be
used as shared key for encryption. The \( K_2 \) acts as the input
of RC4 algorithm and the key sequence will become:

\[ K_n = RC4 \{ h(K_1 \oplus IV_1) \} \]

Authenticator R generates another new \( IV \). Let \( IV \) be the generated
\( IV(i = 2) \) and cipher text C is sent with the \( IV \) as
conventional WEP algorithm. In this way the WEP
encryption process will be continued.

### D. Proposed WEP Decryption

Our proposed WEP decryption process is the reverse of
the encryption. As like as the encryption we have divided
the decryption process in two steps.

\[ IV_2 \]

for encryption process.
Step 1:

The step 1 (Fig. 4) works as follows:

The station S captures the WEP frame that has been sent by authenticator R at the step 1 of encryption process. Station S stores the IV, which will be used for next decryption purpose. Station S has the same dynamic shared key $K_1 = h(Sk \oplus No)$ which was generated at the authentication part. Using RC4 algorithm S will create key sequence $Kn = RC4/h(Sk \oplus No)$. By doing the XOR operation between Kn and received cipher text C station gets the plain text P.

$Pr = [ X, crc(Xm)] = [X, crc(Xm)] = P$

The receiving plaintext $Pr$ is divided into two parts $Pr=[X,crc(Xm)]$ where X is the received message and $crc(Xm)$ is the ICV of $X$ and $K_2$. Now receiver calculates $crc(Xc)$ by using the CRC-32 algorithm of $X$ and $K_2$. If this $crc(Xc)$ is matched with $crc(Xm)$ then it is ensured that the sending message is not tempered, in this way the data integrity is ensured.

Step 2

The step 2 (Fig. 5) works as follows:

Station S remembers the stored $IV_1$ and $K_1$. By using $IV_1$ and $K_1$ Station S will create the new dynamic key $K_2 = h(K_1 \oplus IV_1)$ which is used for this decryption purpose. As well as key sequence $Kn = RC4/h(K_1 \oplus IV_1)$. The Kn and the captured cipher text C which had been transmitted at step 2 of encryption process will be XORed to get the plain text P

$Pr = [ C \oplus Kn ] = [X, crc(Xm)] = [X, crc(Xm)] = P$

The receiving plaintext $Pr$ is divided into two parts $Pr=[X,crc(Xm)]$ where X is the received message and $crc(Xm)$ is the ICV of $X$ and $K_2$. Now receiver calculates $crc(Xc)$ by using the CRC-32 algorithm of $X$ and $K_2$. If this $crc(Xc)$ is matched with $crc(Xm)$ then it is ensured that the sending message is not tempered. Station S will store the $IV_2$ for next decryption process. The decryption mechanism will be continued in this way with the encryption process.

**IV. ANALYSIS**

In the next section, the proposed WEP scheme will be compared with the conventional WEP algorithm in two different criteria. The first level is data privacy and the second is data integrity.

---

**A. Data privacy**

The aim of data privacy is to ensure security during transmission that no illegal user can render the data. Conventional WEP algorithm does not ensure data security that has been discussed already. The proposed scheme ensures data security in the following way.

There is no proper key management in WEP algorithm. The proposed schemes suggest a new dynamic key management system where a temporary key is always generated based on the previous one which is used for encryption and decryption purpose. For example if we consider $K1$ is the dynamic key then after few seconds it will be replaced by another temporary key $K2$ and go on. So every time the previous dynamic key is replaced by a new one. So it is obvious that such a mechanism will be a harder task for attackers to break. In proposed scheme key sequence is the function of IV and dynamic key. So if IV is repeated after $2^{24}$ times but dynamic key will be repeated only after $2^{128}$ times. As a result it is said that key sequence will not be repeated even IV is repeated. Besides of that every frame carries the IV which is used for next encryption and decryption purpose. So, i number of IVs can decrypt i+1 number of frames. So, this encryption method enhances the resistance of the WEP frame against the attackers to obtain the plain text.

Here,

Length of the dynamic key= 128 bits

Total combination of dynamic key=$2^{128} = 3.4 \times 10^{38}$

Network traffic = 54 Mbits/S

Data packet size = 1500 Byte
Data packet send per second = \( \frac{54 \times 10^6}{1500 \times 8} \approx 4500 \)

So the number of dynamic keys used per second is 4500

Then after \( 2.1 \times 10^{31} \) hrs the dynamic key will repeat.

\[
(3.4 \times 10^{38}) \times 4500 = 7.66 \times 10^{34} \text{ seconds} = 2.13 \times 10^{31} \text{ hrs}
\]

Although the dynamic key will repeat after \( 2.13 \times 10^{31} \) hrs but there is no possibility for attacker to get the key sequence. Because our dynamic key is the function of future IV and the previous shared key. Here the IV is of 24 bits which will repeat after 4 hrs but the dynamic shared key is of 128 bits will repeat after \( 2.13 \times 10^{31} \) hrs. Among this \( 2.13 \times 10^{31} \) hrs the IV will repeat at least \( 5 \times 10^{30} \) times. So it will almost impossible to for attackers to get the key sequence.

B. Data Integrity

From section II.C we have seen that the conventional WEP algorithm does not insured data integrity. But our proposed scheme ensures the data integrity where CRC-32 is the function of plaintext and dynamic key.

Now if \( X \) is the message and \( \text{crc}(X_m) \) is the corresponding CRC-32 information of \( X \) and dynamic key \( K \). If attacker changes the message from \( X \) to \( X' \) then he needs to change the CRC-32 information for the modified data. Let \( \text{crc}(V) \) is the corresponding CRC-32 information of \( V \). Then:

\[
C' = C \oplus \{ \text{crc}(V) \}
\]

\[
= \{ X, \text{crc}(X_m) \} \oplus \text{RC4}(h(IV,SK)) \oplus \{ \text{crc}(V) \}
\]

\[
= \{ X \oplus \text{crc}(X_m) \oplus \text{crc}(V) \} \oplus \text{RC4}(h(IV,K))
\]

\[
= \{ X', \text{crc}(X_m') \oplus \text{crc}(V') \} \oplus \text{RC4}(h(IV,K))
\]

Here \( X' \) is the function of \( X \) and \( K \) where \( X \) is known and \( K \) is unknown for attacker. Even if the attacker can change the message from \( X \) to \( X' \) and calculate \( \text{crc}(X_m') \) which will be denied by receiving side. Because the receiver will calculate the ICV using \( X' \) and known \( K \) which will definitely not be matched with \( \text{crc}(X_m') \). In this way data integrity can be ensured.

V. Conclusion

In this paper, security holes in WEP have been analyzed in more convenient way. The structure of WEP in sender and receiver side and description about all steps has been reviewed. Comparing with the existing WEP encryption and decryption process, it is found that the proposed scheme works more precisely to minimize the IV repetition issues and even confirms that if IV repetition occurs then hacker won’t be able to do any harm because of new dynamic key. To verify the result, the proposed scheme has been examined by mathematical calculations and it is confirmed that the proposed modified scheme is better solution for security holes of WEP. Further works should focus on the problem on IV length and data integrity.

REFERENCES


