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

Mahmudur Rahman, Md. Asif Hassan Riyad, Md. Ibn Sinha, A.K.M Fazlul Haque

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 LAN, 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 contents 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 based on table search. Maocai Wang et al [4] have worked on security analysis for IEE802.11 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 WAP2introduced 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

Manuscript received May 11, 2011; revised July 20, 2011. This work was supported in part by the U.S. Department of Commerce under Grant BS123456 (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: akmfhaque@daffodilvarsity.edu.bd).

network traffic of 11Mbps. Now if sender sends 1200B packets then:
The numbers of packets are sent per second =

$$\frac{11\ X\ 10^6}{1200\ X\ 8} \approx 1146$$

So it is seen that sender uses 1146 IV per second. So after 4hrs the IV will repeat.

$16777216 \div 1146 = 14639.80$ Seconds

$= 4.07$ 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.
P1 = plain text 1
P2 = plain text 2
IV = initialization vector
Sk = secret WEP-Key
C1 =cipher text 1 = $P1 \oplus RC4(IV, Sk)$
C2 =cipher text 2 = $P2 \oplus RC4(IV, Sk)$
Then, $C1 \oplus C2 = (P1 \oplus RC4(IV,Sk)) \oplus (P2 \oplus RC4(IV,Sk))$
$= P1 \oplus P2$
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,

$$C = [X, crc(X)] \oplus RC4(IV, Sk)$$

Now X is the message and crc(X) is the corresponding CRC-32 information of X. if an attacker change the message $X = (X + \nabla)$ where ∇ is the modified part then he needs to change the CRC-32 information for the modified data.
Let crc(∇) is the corresponding CRC-32 information of ∇. Then:
$C' = C \oplus [\nabla, crc(\nabla)]$
$= [X, crc(X)] \oplus RC4(IV, Sk) \oplus [\nabla, crc(\nabla)]$
$= [X \oplus \nabla, crc(X) \oplus crc(\nabla)] \oplus RC4(IV, Sk)$
$= [X', crc(X \oplus \nabla)] \oplus RC4(IV, Sk)$
$= [X', crc(X')] \oplus RC4(IV, Sk)$
This way the attacker can substitute the original plain text X, crc(X) with the modified plain text X', 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 probe request to R for accessing the network. Then R sends a 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:

$$k_1 = h(Sk \oplus N_0)$$

Where, K1= Dynamic key generated by S
Sk = Shared secret WEP key
N_o = Random number generated by authenticator
h = hash function [ref]

ISBN: 978-988-18210-9-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

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

S_k = 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

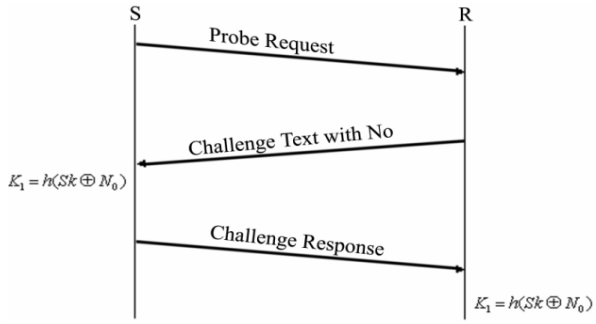

Fig. 1 Dynamic Key Generation during Authentication Process

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 step 1 (Fig. 2) works as follows:

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)]. Now K_1 will act as the input of RC4 algorithm which results the key sequence (Kn) of 128 bits length so,

Kn = RC4 (K_1)

= RC4 [$h(Sk \oplus N_0)$]

Now by XOR operation of Kn and P we get the cipher text

$C = P \oplus Kn$

= [X,crc(Xm)] $\oplus$ RC4[$h(Sk \oplus N_0)$]

After this authenticator R generates IV randomly and sends as plaintext with the cipher text to the station S like the conventional WEP algorithm. Let the authenticator generates i number of initialization vectors, if $i=1$ then the first $IV = IV_1$. The authenticator stores the IV_1 for encryption process.

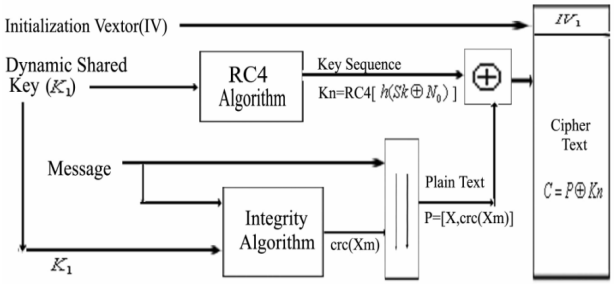

Fig. 2: Proposed WEP Encryption (Step1)

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 Kn= RC4 [$h(K_1 \oplus IV_1)$]. Here crc(Xm) is also calculated which is the function of message X and dynamic key K_2 Then the key sequence Kn will be XORED with the new plain text P=[X,crc(Xm)] and generates cipher text C=[X,crc(Xm)] $\oplus$RC4[$h(K_1 \oplus IV_1)$]. Authenticator R generates another new IV. Let IV_2 be the generated $IV(i=2)$ and cipher text C is sent with the IV_2 as conventional WEP algorithm. In this way the WEP encryption process will be continued.

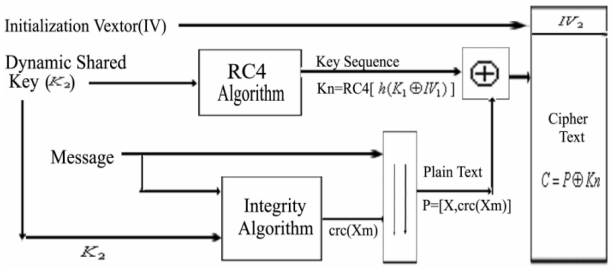

Fig. 3: Proposed WEP Encryption (Step2)

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.

ISBN: 978-988-18210-9-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

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 step1 of encryption process. Station S stores the IV_1, 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 $K_n = RC4[h(Sk \oplus No)]$. By doing the XOR operation between Kn and received cipher text C station gets the plain text P.

C station gets the plain text P.

$Pr = [\, C \oplus Kn \,]$

$=[\, X, crc(Xm)] \oplus RC4[h(Sk \oplus No)] \oplus RC4[h(Sk \oplus No)]$

= [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_1. Now receiver calculates crc(Xc) by using the CRC-32 algorithm of X and K_1. 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.

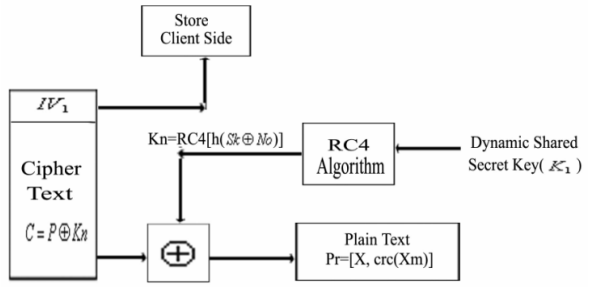

Fig. 4 Proposed Decryption process (Step 1)

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 step2 of encryption process will be XORED to get the plain text Pr

$Pr = [\, C \oplus Kn \,]$

$= [\, X, crc(Xm)] \oplus RC4[h(K_1 \oplus IV_1)] \oplus RC4[h(K_1 \oplus IV_1)]$

= [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 modified. Station S will store the IV_2 for next decryption process. The decryption mechanism will be continued in this way with the encryption process.

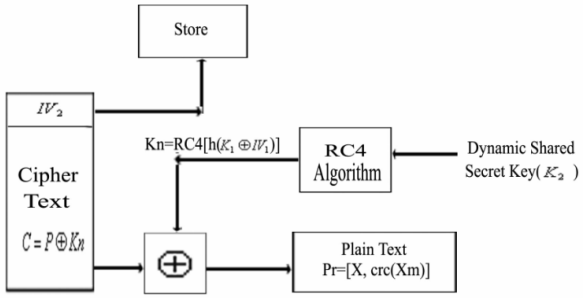

Fig. 5 Proposed WEP decryption (Step 2)

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= $2^{128} = 3.4 * 10^{38}$

Network traffic = 54 Mbits/S

Data packet size = 1500 Byte

ISBN: 978-988-18210-9-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Data packet send per second = $\frac{54\ X\ 10^6}{1500\ X\ 8} \approx 4500$

So the number of dynamic keys used per second is 4500

Then after 2.1×10^{31} hrs the dynamic key will repeat.

$(3.4\times10^{38}) \div 4500 = 7.66\ 10^{34}$ seconds

$= 2.13\times10^{31}$ hrs

Although the dynamic key will repeat after 2.13×10^{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 2.13×10^{31} hrs. Among this 2.13×10^{31} hrs the IV will repeat at least 5×10^{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 crc(Xm) is the corresponding CRC-32 information of X. and dynamic key K. If attacker changes the message $X = (X + \nabla)$ where ∇ is the modified part then he needs to change the CRC-32 information for the modified data. Let $crc(\nabla)$ is the corresponding CRC-32 information of ∇. Then:

$C' = C \oplus [\nabla, crc(\nabla)]$

$= [X, crc(Xm)] \oplus RC4[h(IV,Sk)] \oplus [\nabla, crc(\nabla)]$

$= [X \oplus \nabla, crc(Xm) \oplus crc(\nabla)] \oplus RC4[h(IV,K)]$

$= [X', crc(Xm \oplus \nabla)] \oplus RC4[h(IV,K)]$

$= [X', crc(Xm')] \oplus RC4[h(IV,K)]$

Here $crc(X_m)$ 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 crc (Xm') 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 crc(Xm'). 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

[1] Arash Habibi Lashkari, Farnaz Towhidi, Raheleh Sadat Hosseini. "Wired Equivalent Privacy (WEP)". 2009 International Conference on Future Computer and Communication.

[2] IEEE P802.11i/D10.0. Medium Access Control (MAC) Security Enhancements, Amendment 6 to IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications. April, 2004.

[3] Zhang Longjun and Zou Tao. An improved key management scheme for WEP. IEEE/IFIP International Conference on Embedded and Ubiquitous Computing 2008.

[4] Maocai Wang, Guangming Dai, HanpingHu,Lei Pen. Security Analysis for IEEE802.11. © 2008 IEEE

[5] S.Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling ALGORITHM OF rc4", eigth annual workshop on selected areas in cryptography, August 2001.

[6] Sadia Arefin, MD.Faroque Hossain"An Enhanced Security Scheme Based On the Analysis of IEEE802.11 Wireless Network Security: Wired Equivalent Privacy"Daffodil International University, supervised by Prof. Dr. M. Lutfar Rahman.

[7] Scott Fluhener, Itsik Mantin, Adi Shamir, Weaknesses of key scheduling algorithm of RC4.

[8] Jumnit hong Raid Lemachheche, WEP protocol Weaknesses and Vulnerabilities –spring 2003.

[9] Jose Perez, A Survey of Wireless Network Security Protocol.