Two Tier Security Enhancement for Wireless Protocol WEP (Wired Equivalent Privacy)

D. J. Evanjaline, P. Rajakumar, N. Kalpana

Abstract: A Wireless Local Area Network (WLAN) is a flexible data communication system implemented as an extension to or as an alternative for a wired Local Area Network (LAN). However, anyone can eavesdrop on information so that WLAN has the hidden security trouble such as leaking of electromagnetic wave or eavesdropping of data because WLAN adopts common electromagnetic wave as media to transmit data. Therefore, the security of WLAN is very important and outstanding. In IEEE 802.11, there are three security technologies used to ensure the data security in WLAN—SSID (Service Set Identifier), MAC (Media Access Control), WEP (Wired Equivalent Privacy). The proposed work falls on the third technology namely the WEP protocol. WEP suffered threats of attacks from hackers owing to certain security shortcomings in the WEP protocol. The proposed schemes implemented in two different layers of WLAN network architecture to strengthen the security of WLAN against the key stream reuse attacks and weak IV attacks.

Keywords: WLAN, WEP, Initialization Vector.

I. INTRODUCTION

The 802.11 standard defines the Wired Equivalent Privacy (WEP) protocol and encapsulation of data frames for security of the wireless LAN systems[4]. It is intended to provide data privacy to the level of a wired network. WEP uses the RC4 encryption algorithm, which is known as a stream cipher. A stream cipher operates by expanding a short key into an infinite pseudo-random key stream. The sender XORs the key stream with the plaintext to produce cipher text. The receiver has a copy of the same key, and uses it to generate an identical key stream. XORing the key stream with the cipher text yields the original plaintext. To avoid encrypting two cipher texts with the same key stream, an Initialization Vector (IV) is used to augment the shared secret key and produce a different RC4 key for each packet. The IV is also included in the packet. IV along with the WEP key is referred to as a secret key which is used for encrypting the transmitted frames. WEP key is also known as the shared key. The integrity check field is implemented as a Cyclic Redundancy Check-32 (CRC-32) checksum, which is part of the encrypted payload of the packet. WEP suffered threats of attacks from hackers owing to certain security shortcomings in the WEP protocol. Despite its shortcomings one cannot undermine the importance of WEP as it still remains the most widely used system. WEP suffers security pitfalls due to weak key management of the shared secret key and initialization vector (IV) repetitions and inappropriate RC4 and CRC-32 algorithms. All WEP weaknesses come from four main conception flaws:

Manuscript Received on February 2015.
Dr. D.J .Evanjaline Department of Computer Applications, Jayaram College of Engg & Technology, Anna University,Trichy, India.
Mr. P .Rajakumar Department of Computer Applications, Jayaram College of Engg & Technology, Anna University,Trichy, India.
Ms. N. Kalpana Department of Computer Applications, Jayaram College of Engg & Technology, Anna University,Trichy, India.

(i) The initialization vector is transmitted as clear text. (ii) The key is rarely renewed. (iii) The WEP has not planned a mechanism to ensure data source authentication. To overcome these problems, the existing WEP protocol is enhanced using our proposed model without changing the WEP mechanism. The proposed schemes implemented in two different layers of WLAN network architecture to strengthen the security of WLAN against the key stream reuse attacks and weak IV attacks. The first algorithm implemented in the application layer of WLAN. This algorithm shuffles the plain text using random addressing mechanism [2].

In the data link layer, the second algorithm implemented, where the actual WEP is implemented. The WEP uses 24-bit IV with shared secret key for WEP encryption as mentioned above. The IV space is limited; it will be exhausted within a minimum amount of time, after that the same IV will be repeated. The IV reuse problem eliminated by generating private IV using time difference and iteration of IV as a key to encrypt IV. Finally, the cryptanalysis is performed to evaluate the strength of proposed algorithms and is found to be competent with the WEP encryption mechanism.

II. RANDOM ADDRESSING MECHANISM (RAM)

The WEP protocol for WLAN networks has been proven to have several weaknesses. This chapter proposes a new security mechanism RAM which enhances the security of WEP protocol by increasing the diffusion characteristic. This RAM implemented in the application layer, and it is executed before entering in the WEP to protect information from eavesdropping and other types of attacks. The RAM shuffles the plain text based on the random addresses. The output produced by the RAM is taken as an input for WEP protocol [1].

A. Encryption Algorithm: RAM -I(Block Shuffling)

Input: Binary form of Plain Text.
Output: Shuffled bit pattern of plain text.

Step 1: Divide the source file into number of blocks (n bits/block)
Step 2: Number the blocks from 1ton
Step 3: Generate the random block from the random numbers S12 sub-key generation algorithm. Consider as key r.

Step 4: The secret key r is, then XORed with different blocks of the source file.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Sb = b1⊕ r, b2⊕ r, b3⊕ r…… bn⊕ r

Step 5: Generate random numbers controlled from 0.. n using the S12 key generation algorithm.
Step 6: Shuffle the blocks based on the random numbers.

B. Encryption Algorithm: RAM-II (Bits Shuffling)

Input: Output of RAM-I
Output: Shuffled Text

Step 1: Select any number of random numbers from as key r, where 0≤r≤7.
Step 2: Each round takes one number from the key to specify the bit location called 'rbit' in each byte of RC4 sub-key k2.
Step 3: A shuffle key is constructed by listing the numbers of bytes in the shuffle key with the value of bit number rbit equal to zero, followed by the numbers of bytes with the value of bit number rbit equal to one in the sub-key.
Step 4: The bits in the blocks are shuffled based on shuffled key.
Step 6: Rotate the blocks based on sum of shuffle keys.

C. *Decryption*

The decryption operation is similar to the encryption, but with the inverse of shuffle and rotate operations. First the receiver calculates the random numbers using the sub-key generation algorithm. Next the decryption of RAM-II performed. Last nth iteration with nth key is executed first; then n-1th iteration executed and so on. Finally, the inverse of rotation is performed. After that, the decryption process of the RAM –I performed.
The cipher text is re-shuffled with the random numbers to get the source bits get back in its original form. The receiver will generate the plain text by XOR ing the random block with every other block. This decryption restores the original plain text without loss of integrity.

D. *Experimental Results*

For the proposed algorithm implementation, laptop Intel core I3 with 1.86 GHz CPU used, in which performance data is collected. In the experiments, the laptop encrypts a different file size ranges from 350 KB to 7.139MB. 140MB for text data, from 350 KB to 8090 KB for audio data, and from 4015 KB to 5073 KB for video files. Several performance metrics are collected for the different size files.
The encryption time is considered the time that an encryption algorithm takes to produce a cipher text from a plaintext. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption.

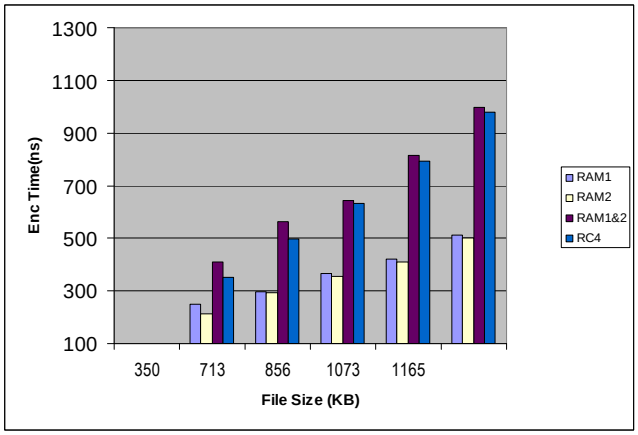

Fig .1 RAM Encryptions of different size of text files

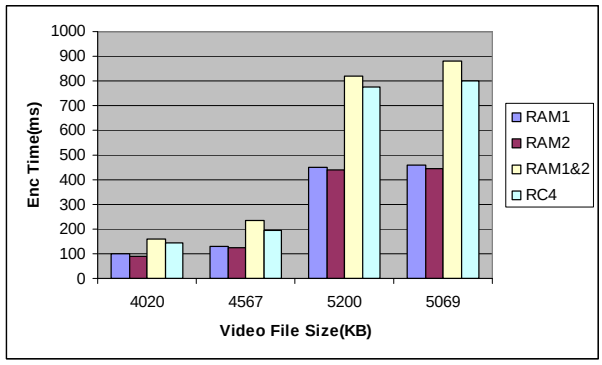

Fig.2 RAM Encryptions of different size of video files

Experimental results of the proposed algorithm for video files compared to RC4 algorithm shown in Figure 3.8 at encryption stage. When combining RAM-I & II algorithms it takes more time for encryption similarly for text files. RAM encryption of image files shown in Fig 3.

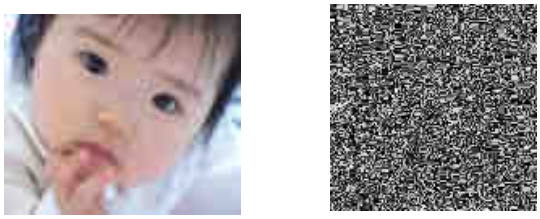

Fig.3 RAM Encryptions of image file

Fig.3 shows the performance comparison point is changing different keys for RAM-II. It always shows that when number of keys increased the encryption time also increased.

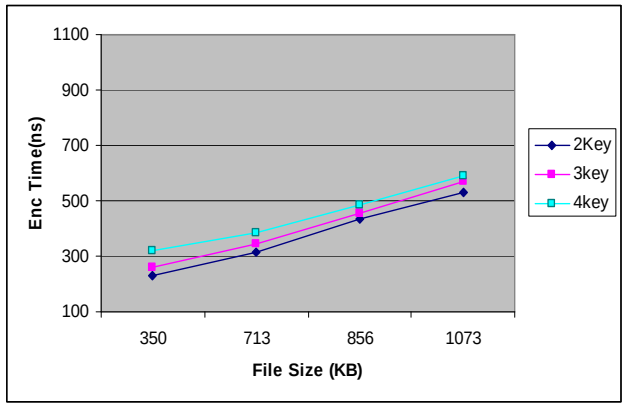

Fig 4 RAM-II Encryption time with different keys

E. Advantages

The proposed modification to the existing WEP protocol makes it more secure and robust in terms of Message Privacy. If one or more bits in the key are changed, a different shuffle bit is chosen, and the substitution is changed. There is K x 2b different possible shuffle vectors for an input of size b bytes encrypted in k iterations. So the brute force attack is impossible. When different keys were used with the same plain text, they produced different cipher texts. The fact that in the proposed mechanism frequently change the shared secret keys through the random numbers make any kind of cryptanalytic attack futile. The proposed system works well with the existing

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

hardware and gives an edge over the present WEP protocol.

III. PRIVATE IV GENERATION ALGORITHM

A well-known pitfall of stream ciphers is that encrypting two messages with the same key sequence can reveal information about both messages without any knowledge of the secret key. This could lead to a number of attacks. To prevent key sequence reuse, the WEP recommends varying key sequences for payload so that the WEP uses a 24-bit IV.

One significant design flaw of WEP concerns the length of the initialization vector (IV). The IV is 24 bits long; therefore, there are 224 different IVs. This may seem like a large number, but a simple analysis reveals that, even if a different IV is used for each successive packet, the entire IV space will be used up extremely quickly

The weakness of IV summarized as follows:

- The IV is too small and in clear text.
- The IV is static.
- The IV makes the key stream vulnerable.
- The IV is a part of the RC4 encryption key.

In order to overcome the above mentioned flaws the proposed mechanism enhances the current WEP protocol. To eliminate the IV reuse problem, the IV generated by the WEP protocol is made private by this mechanism.

The proposed mechanism is to ensure that it will disable an intruder's ability to easily map IVs to known key sequences without changing the IV space (i.e. 24 bits).

And also the proposed enhancement attempt to rectify the vulnerabilities to enhance the WEP with Private IV for improved authentication process.

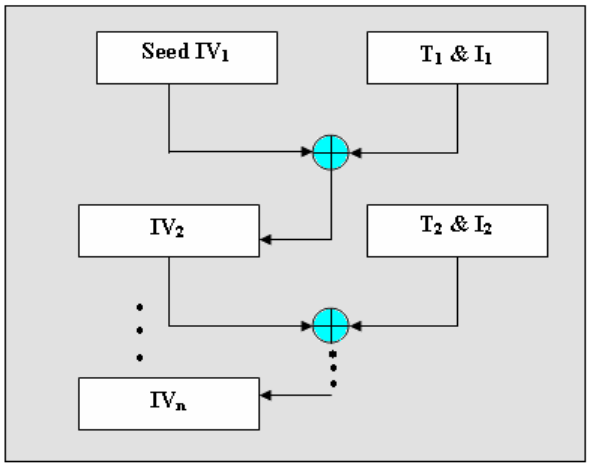

Fig.5 Private IV Generation Process

A. *Encryption*

The proposed scheme is similar to WEP, which has no change in the size of the IV. The difference is in the conventional WEP the IV is public and in the proposed scheme the IV is encrypted aims to hide it from eaves dropping. As Shown in Figure 4.1 the sender encrypts IVi+1 using time difference and IVi and counter value of Ii. Thus it is sufficient for the receiver to know the previous IV, time stamp and counter value to decrypt the next IV.

After that the sender receives the first IV and encrypts it with time stamp and counter value. Then the sender sends the IV to the receiver. Knowing the first time stamp and counter value the receiver decrypts the first IV and store in a table. The next IV encrypted by previous IV and the time stamp value of current IV and the counter value. The time difference sends as extra one byte in a payload section in the WEP frame. As a matter of fact, every frame contains the time difference used to generate the next time stamp in the receiver side to decrypt the IV. This encryption of IV makes no correlation between the current IV and the current cipher text in the WEP frame. Therefore, enhances resistance to brute force attack.

The Private IV generation process done in 3 steps described below.

1. The key idea of avoiding IV collision is to calculate the time stamp of each IV generated by the access point.
2. The timestamp, the difference between two successive IV time stamps, the iteration of current IV and previous IV are used to generate the private IV.
3. The private IV generation process done by two threads to increase the uniqueness of the IV without changing the size of the IV.

Algorithm 1: Algorithm for Time Stamp Calculation

1. ts = 0; Initialize the timestamp to 0.
2. for k = IV1 to IVm do ; Do this for all IV
3. If (k != 0) then tk =tk-1 +(Δtk - Δtk-1)
else Δtk = 0
4. end for;

The idea here is to disable intruders to know the actual IV used by the WEP for encryption, because the original IV generated by AP synchronously and periodically updated by the sender and receiver minimizing the chances of an attack.

Step 2 (The Private IV generation algorithm)

The private IV generated by encrypting each IV by the previous IV, time stamp tk of current IV and the iteration of IV that the AP generated for this particular session.

Algorithm 2: Algorithm for private IV generation

1. for each IV, do:
2. At time Δtk, updated the IV generated by the AP for each packet according to the following equation:
IVi = XOR [IVi ,(ti 2k)]
3. end do

In this algorithm, each IV regenerated by XORing the IV with the time stamp and the actual iteration of IV. The private IV generation sample code using a single thread as given in Figure 4.2. The following Java code generates a 8-bit random IV without repetitions using LFSR. Each random IV XORed with previous IV, the timestamp and the counter value of IV.

The sample output for private IV given in Fig 6. The receiver should maintain the table for timestamp value of each IV, the previous IV and the actual number of IV for the decryption process.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

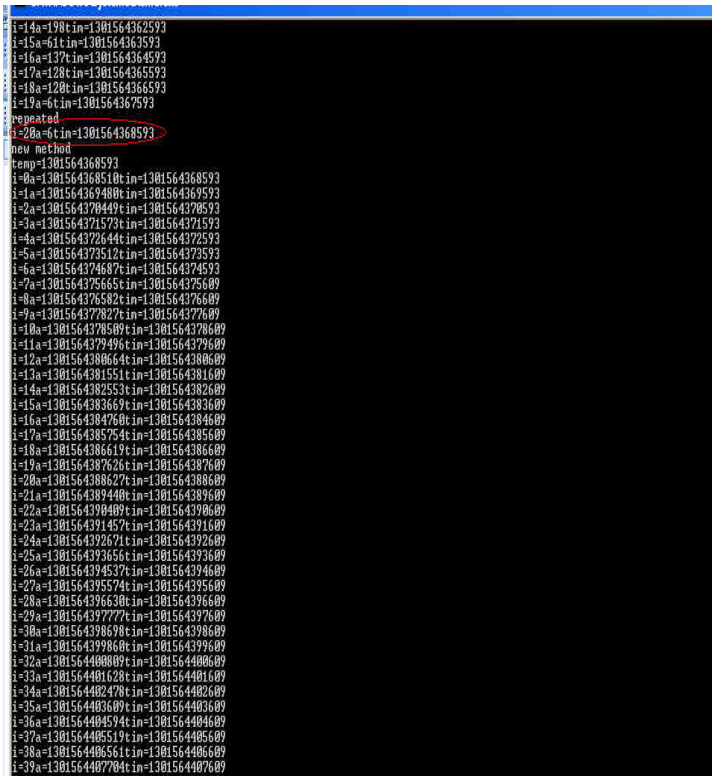

Fig 3.1.1 Sample output of Private IV Generations

In the proposed scheme, each IV encrypted by time stamp and the timestamp will be changed regularly for each transmission. So the intruder cannot get any useful information from the IV.

B. Decryption

Both sender and receiver must store the timestamp values for each IV and the iteration of IV. For the decryption the IV from the WEP frame extracted and it is XORed with first time stamp and incrementing the counter of iteration value.

C. Advantages

Since the IV space is limited (24 bits in length), the above mechanism helps to change the key to achieve the requirement of supplying unique pairs of key and IV to the RC4 algorithm, and therefore, the problem of key sequence reuse can be largely avoided.

IV. ANALYSIS OF PROPOSED ALGORITHMS

In the first proposed algorithm named RAM, there are two ways to shuffle the file. The intruder makes more attempts and creates more no of combinations to get the plain text.

Table 4.1 Maximum combinations for addresses with different file size in RAM

File Size (Bytes)	**No.of Blocks (16 bytes/block)**	**Combinations**	**Time needed for Brute Force Attack (ms)**
63	4	(4 × 16)!=64!	5
125	8	(8 × 16)!=128!	11
256	16	(16 ×16)!=256!	37
383	24	(24 × 16)!=384!	68

In the above table, the time needed for brute force attack to generate the combinations is directly proportional to the file size. In addition to that, this proposed algorithm maximum satisfies the criteria values discussed in the section 6.3.

In the Private IV generation algorithm (PIV) used because, in WEP the RC4 uses the key pair (iv, k) for encryption. This algorithm takes the 24-bit key for encrypting iv. The value of timestamp, the previous iv and the number iv is combined and form the 24-bit key. The original iv encrypted by this key to generate the private iv. The attacker has to try to find the original iv and the key value by 224 x 224 =248 combinations.

Table 4.2 Comparison of Conventional WEP and Proposed IV

Parameter	Conventional WEP	PIV
IV length	224	224
RC4 key	Fixed	Fixed
IV	Public	Private
Key to encrypt IV	No	24-bit key

V. CONCLUSION

This paper describes how the proposed algorithms are achieved the security goal of WEP. The strength of the proposed algorithms is compared with WEP protocol. It proved that the time to the ability of enduring attack, break or crack the cipher text is increased. Furthermore, the proposed algorithms efficiently withstand the IV reuse attacks. This makes the brute force attack futile. In the nutshell when implementing all the three proposed algorithms in different layers of WLAN thwarts all kind of cryptanalytic attacks.

REFERENCES

[1] Mohamed Juwaini, Raed Alsaqour, Maha Abdelhaq , “A Review On WEP Wireless Security Protocol,” Journal of Theoretical and Applied Information Technology, ISSN: 1992-8645, E-ISSN: 1817-3195 Vol. 40 No.1, 15 June 2012.

[2] Dr.R.N. Rajotiya, Pridhi Arora, “Enhancing Security of WI-FI Network”, International Journal of Computer Applications, ISSN: 2250 – 1797, Issue 2, Vol 3, June 2012.

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

[4] Lashkari, A.H.; Mansoor, M.; Danesh, A.S.; Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA). International Conference on Signal Processing System. IEEE, 2009

[5] Lashkari, A.H., A survey on wireless security Protocols (WEP, WPA and WPA2/802.11i), Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on 8-11 Aug 2009, E-ISBN: 978-1-4244-3878-5

[6] Sandirigama, M, Security weaknesses of WEP Protocol IEEE 802.11b and enhancing the Security with dynamic keys, Science and Technology for Humanity (TIC-STH), 2009, IEEE Toronto International Conference

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.