Security Improvement for Management Frames in IEEE 802.11 Wireless Networks

Mina Malekzadeh[1], Abdul Azim Abdul Ghani[2], Zuriati Ahmad Zulkarnain[3] and Zaiton Muda[4]

University of Putra Malaysia

Summary
IEEE 802.11 Wireless LAN (WLAN) has gained popularity. WLANs use different security protocols like WEP, WPA and WPA2. The newly ratified WPA2 provides the highest level of security for data frames. However WPA2 does not really mention about protection of management frames. In other words IEEE 802.11 management frames are always sent in an unsecured manner. In fact the only security mechanism for management frames is CRC-32 bit algorithm. While useful for unintentional error detection, CRC-32 bit is not safe to completely verify data integrity in the face of intentional modifications. Therefore an unsecured management frame allows an attacker to start different kinds of attack. This paper proposes a new model to address these security problems in management frames. First we summarize security threats on management frames and their influences in WLANs. Then based on these security threats, we propose a new per frames security model to provide efficient security for these frames. Finally simulation methodology is presented and results are provided. Mathematical probabilities are discussed to demonstrate that the proposed security model is robust and efficient to secure management frames.

Key Words:
Management frames, security, wireless networks, cyclic redundancy check, IEEE 802.11.

1. Introduction

Over the past several years, wireless technology has changed the way people communicate. Among the wireless network technologies, Wireless Local Area Network (WLAN) or IEEE 802.11 is most popular. A WLAN uses radio frequency technology to transmit and receive data over the air by exchanging three kinds of frames: control frame, data frame and management frame. With rapidly growing of the WLANs, a strong security was vital for a safe communication between wireless stations. Therefore different protocols were designed to provide security for all IEEE 802.11 standards. Unfortunately these protocols only put much attention on securing data frames, and less on securing management frames and control frames. Currently, management frames use Cyclic Redundancy Check (CRC) algorithm for security but CRC is useful only for error detection of the management frames and can not provide any security in form of authentication or privacy. Hence, an unprotected management frame can be used by intruders to launch different types of attack such as man-in-the-middle-attack, frame injection, frame modification, and denial of service attacks.

In this paper, we present the current security threats on management frames and consider their influences on the WLANs. We propose a security enhancement on the management frames to overcome common known vulnerabilities and thus to provide better management frame authentication and integrity. In the enhancement, a keyed-message authentication code that prevents an intruder from tempering with management frames in transit as well as inserting a forged management frames into WLAN is adopted.

The rest of this paper is organized as follows. Section 2 presents some related works that have been done to make a secure management frames. In section 3 we describe management frames structure. The security threats on management frames are summarized in section 4. Security enhancement and the proposed model are presented in section 5. Section 6 describes implementation of the proposed model. In section 7 evaluation of the proposed model is done, then this section discuss the results. Finally section 8 concludes the paper.

2. Related Works

An unprotected management frames can lead to serious threats on WLANs. In this case providing a security mechanism to protect management frames is important in WLANs. This section describes some of the previous works have been done to provide the security on WLANs.

Faria and Cheriton [4] considered the authentication flooding attack and they proposed a new authentication framework to address authentication DoS attack. Their architecture is composed of the Secure Internet Access Protocol (SIAP) and the Secure Link Access Protocol (SLAP). They show that SIAP-SLAP can be used to implement a secure association service and avoid the DoS attacks. SIAP and SLAP rely on the security of robust constructions and encryption algorithms. In addition to, SLAP implements a link-layer independent access verification mechanism using HMAC-MD5. Ding [3] in his paper has used the sensors hardware to detection DoS attacks as a Central Manager (CM) to consider the amount

Manuscript received June 5, 2007
Manuscript revised June 20, 2007

of the observed traffic on the channels. Liu [6] in his paper to address the problem of management frames proposed disabling IEEE 802.11 disassociation functions to avoid its related attacks. Also Bellardo et al. [1] investigated the problem of management frames. In their paper they proposed a method for queuing IEEE 802.11 disassociation frames so that access point queuing disassociation requests for 5-10 seconds. If a data packet arrives after a disassociation request is queued, that request is discarded since a legitimate client would never generate packets in that order. As another approach Guo and Chiueh in their paper [5] mentioned spoofing is possible in WLAN, because the IEEE 802.11 standard does not provide per-frame source authentication. The key idea of this paper is using the sequence number field in the header of IEEE 802.11 frames without modifying clients or APs. They design and implement a sequence number-based MAC address spoof detection system, whose effectiveness is demonstrated in their paper.

All these methods are considered as a short term solution to prevent an attack and compared these papers, we proposed a new model to protection all unicast management frames which can prevent many of the mentioned attacks on 802.11 media access control layer.

3. Management Frames

General format of management frames is shown in Fig.1.

Frame Ctl	Dur.	Dest. Adr.	Srs. Adr.	BSSID	Seq. Ctl.	Body	FCS
Bytes:2	2	6	6	6	2	0-2312	4

Fig.1 IEEE 802.11 Management Frame Structure

A) Duration

It contains the amount of time the current transmission will keep the medium busy.

B) Destination, Source and BSSID Address

These address fields are 48-bit IEEE 802.11 address. The BSSID is address of the AP in a BSS. The Source Address (SA) identifies the originator of the data being transmitted. The Destination Address (DA) is the individual physical address of the entity to which the data is to be ultimately delivered.

C) Sequence control

This field is subdivided into two fields [14], the sequence number (12 bits) and the fragment number (4 bits). Fragment number shows the number of fragmentation of the frames and sequence number is used to frame duplication detection.

D) Management Frame Body

Management frame has different subtypes so that all of them are the same in the header but are different in the body and the body identifies the type of management frames. This paper considers unicast management frames includes: authentication request and response, association request and response, reassociation request and response, deauthentication and disassociation.

E) FCS

The Frame Check Sequence (FCS) field is a 32-bit field containing a 32-bit Cyclic Redundancy Check (CRC) algorithm which is calculated over all the fields of header and body of the management frame. CRC algorithm has two serious problems; data modification and data injection. In first problem because of the linear structure of CRC polynomials, it is extremely easy to intentionally changing data without modifying its CRC value by intruders. CRC is just useful for error detection but it cannot be safe to verify data integrity and authentication.

CRC originally has been designed to see if noise or common errors in transmission, have modified the data, and is not a cryptographic checksum to protect against malicious tampering. An attacker can change both the data and the CRC-32 value while the CRC-32 matches the altered data, because the checksum is a linear function of the data [9], [2]. The second problem with CRC is because it is a keyless algorithm. As a result, it can also be computed by the adversary who knows the data. As it mentioned earlier, management frames are transmitted clearly and all their information is visible to intruders, therefore this property of the CRC, allows attacker to make a legitimate CRC value for his illegitimate management frame and in this case he is capable to injecting arbitrary forgery management frames into the WLAN to start some mentioned attacks in next section.

4. Attacks on Management Frames

An intruder can use an insecure management frame to produce different kinds of attacks so that the whole wireless network will be unusable [1], [10]. Common recently attacks on management frames are as follow.

A) MAC Address Spoofing

MAC address is a vital piece of information that helps clients understand which AP they are talking to and vise versa. Unfortunately MAC address is not encrypted and spoofed easily which is one of common attacks on management frames whereby the intruders configure their wireless client to appear to have the same MAC address as an authorized access point or wireless client. When a legitimate client is not transmitting, the intruder will first reconfigure his terminal with the known information. Once this is done, the intruder's terminal will appear as the authorized terminal and will be able to access most of the resources. There are different known attacks using MAC address spoofing [1], [11] as follow:

1) Forged Deauthentication

After an IEEE 802.11 client selected an AP for communication, it must first authenticate itself to the AP before starting further communication and to do this it has to send authentication request. But unfortunately, this management frame is not authenticated using any algorithm. Consequently, the attacker can spoof this frame, either pretending to be the access point or the client. In response, the access point or client will exit the authenticated state and will refuse all further frames until authentication is reestablished. By repeating the attack persistently, a client can not access to WLAN at all.

2) Forged Disassociation

A very similar vulnerability like forged deauthentication may be found in the association management frame which occurs after authentication according to the state machine [6]. Since a client may be authenticated with multiple APs at the same time, therefore, the IEEE 802.11 provides a special association management frame to allow the client and AP to agree which AP is better for which client. IEEE 802.11 provides a disassociation management frame similar to the deauthentication described earlier. The vulnerability in disassociation frames is like deauthentication because this management frame also is not protected in WLAN.

B) Denial of Service (DoS) Attack

In this attack, the intruder sends a continually stream of different kinds of management frames to the WLAN [12], [13]. An attacker can spoof MAC address of AP or client and flood the WLAN with different kinds of forgery deauthentication, disassociation, association, authentication or bacon management frames by using both directions of the communication. In this case the WLAN overloads and will be unusable for even legitimate users.

C) Session Hijacking

Session hijacking combines denial of service and MAC spoofing attacks. Typically an intruder forces a legitimate client to terminate its connection to an AP by sending it a forgery disassociation or deauthentication management frame with the MAC address spoofed of the AP, therefore the client will be disconnected from the network. The intruder can now associate with the AP, to forge the MAC address of the client, and hence captures its session.

D) Man-in-the-Middle Attack

For Man-in-the-Middle attack, intruders insert themselves between an AP and a client to capture management frames in transmission. The idea behind this attack is to enter between the sender and the recipient, access to the management frame, modify it and forward it to the recipient. The client sees the intruder as an authorize AP, while the AP sees the intruder as an authorize client. Both authorize devices fail to detect the intruder and continue transmitting information.

As a result, all these mentioned attacks are because there is no any security mechanism to check integrity and authentication of the management frames (MF) in none of IEEE 802.11 standards, therefore these standards are vulnerable to such mentioned attacks. Hence in next section, this paper proposes a new model to provide security for management frames to protect against all the mentioned attacks.

5. Security Enhancement

The proposed enhancement attempts to rectify the vulnerabilities and make the attacks futile. By using keyed message authentication code algorithm we propose Management Frames with Authentication and Integrity (MFIA). As a keyed message authentication code algorithm, this research uses the HMAC-SHA1 to protect MF because IEEE 802.11i uses HMAC-SHA1 for data frame protection, therefore using the HMAC-SHA1 for MF does not need to any new algorithm and with a small change in the wireless network cards the proposed model can be implemented.

This research bases the proposed model on a shared key (k) among the legitimate devices and is presumed it has been delivered to the legitimate devices through a secure way. To being easier, this research summarizes the name of HMAC-SHA1 algorithm to MAC algorithm and its output to code. In order to adequately protect management frames, the proposed model covers the management frame body and header fields, including the frame control, duration, destination address, source address, access point address, fragment number and the sequence number. According to the proposed model, when a sender wants to send each kind of management frame, first by using MAC algorithm, key (k), header and body of the MF, the Sender Code (S-code) is computed and is connected to the MF then this new protected MF is transmitted (FCS is appended after S-code). When receiver takes this protected MF, first computes Receiver Code (R-code), by using the received MF, k and MAC algorithm. If S-code and R-code match together, so receiver understands the management frame has not been changed during transmission and also understands it has been transmitted by a legitimate user who knows the key, so will implement the MF. The proposed model is shown in Fig.2.

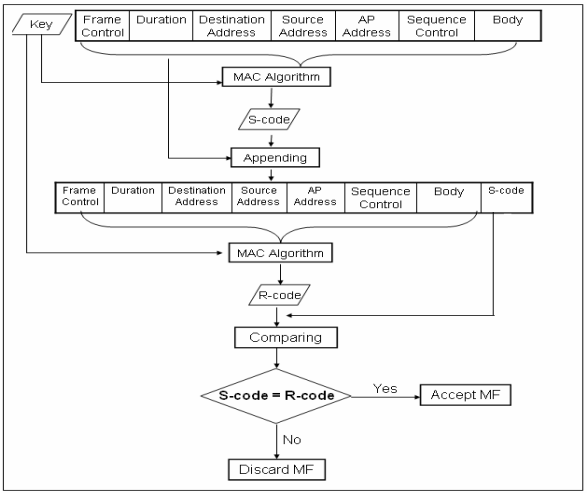

Fig.2 the Proposed Model (MFIA)

6. Implementation of the Proposed Model

To implement the proposed model, a program is designed with JavaScript and HTML in Microsoft FrontPage XP on a win32 platform with a Pentium IV processor. The program has two entities: a sending station module and a receiving station module. First to compute the S-code the sender station module determines kind of management frame that it needs to transmit and after that the program makes a simulated management frame based on type of the selected management frame. The program uses the simulated management frame, MAC algorithm and the shared key to compute the value of the S-code. Now S-code is appended to the management frame to transmit to the receiving station module. The receiver by using the received management frame, MAC algorithm and the key computes the value of the R-code. Finally the program by using a comparison function compares the values of S-code and R-code together to check the validation of the management frame.

7. Evaluation of the Proposed Model and Discussion of the Results

The results aim to quantify the security enhancements of the proposed model and enable comparisons between the original security of management frame and the proposed scheme. To evaluate the security effectiveness of the proposed model this research defines the security effectiveness of the proposed model as the low probability of successful operation of the most common existing management frames attacks on the proposed model. Therefore this research quantifies the security of both MFIA and CRC in term of attack probability on them and compares the obtained results to show the strength of the proposed model to prevent the attacks in WLANs.

1) Forgery Attack Probability

A dangerous situation on the proposed model can be when an adversary has obtained a particular code from an earlier transmitted management frame (x) and he makes a fake management frame (y) so that its code ($H_k(y)$) is matched with that legitimate particular code ($H_k(x)$). By using this attack the intruder sends his forgery management frame with a legal code which is quite acceptable for receiver. This situation is dangerous because it leads to another situation where an attacker replaces the original management frame contents with his forgery management frame. The general format of the attack is shown as follow:

$$x \in Legal\ , y \in Intruder \therefore H_k(x) = H_k(y) \quad (1)$$

To do this kind of attack the intruder has to send several forgery management frames to find his desired MF. This research considers these frames that intruder sends, belong to a set which is called E with F elements. Therefore to find the probability of this attack, here is computed the number of required MFs that an intruder has to send to find a MF that has a particular code. If x is the legitimate MF with code1, now it is necessary to compute the F so that E contains at least one MF with code2 so that code1=code2. With n-bit length of code, the amount of possible codes will be $N=2^n$. So the probability that code2 has any particular value is $\frac{1}{N}$.

$$p(\text{code1=code2}) = \frac{1}{N} \quad \therefore \overline{p}(\text{code1} \neq \text{code2}) = 1 - \frac{1}{N} \quad (2)$$

From the above formula it is derived that the probability in the E with F independent elements is $\overline{P} = \left(1 - \frac{1}{N}\right)^F$.

Therefore, the probability that at least one of the E elements has a code equal to code1 is:

$$P = 1 - \overline{P} \ \rightarrow P = 1 - \left(1 - \frac{1}{N}\right)^F \quad (3)$$

After simplifying of this formula, the probability is:

$$p_{forgery} = \frac{F}{N} \quad (4)$$

Now to compute the F with probability of p it is considered three common probabilities it means 25%, 50%, 75%. Now for n=160 in MFIA and n=32 in CRC the results of this computation are shown in Table1.

Table1: Number of Required MFs for Forgery Attack

Security	No. F with p= 25%	No. F with p= 50%	No. F with p= 75%
MFIA	3.65×10^{47}	7.3×10^{47}	1.10×10^{48}
CRC	1.07×10^{9}	2.15×10^{9}	3.22×10^{9}

From the observations in Table1, it can be concluded that the required resources to do the attack are bigger for MFIA, than CRC which is because of output size of their underlying algorithms. It shows MFIA needs more operations by intruder to find his proper management frame corresponding to a legitimate special code than CRC. Allocating these amounts of management frames is both cost and time consuming for the intruder in MFIA which makes it more powerful against this attack, but in CRC intruder with a low attempts can insert his forgery management frames to the WLAN to start his attack.

2) Collision Attack Probability

Another attack on MFIA can be when an intruder produces any two different forgery management frames with same codes which is called collision attack. The general structure of this attack is shown as follow:

$$x, y \in Intruder \therefore H_k(x) = H_k(y) \quad (5)$$

The intruder motivates the legitimate user to implement one of his forgery management frames (x) to produce a legitimate code, after that the intruder uses this legitimate code for his second forgery management frame (y) and sends it to the receiver part and receiver will accept this forgery MF because of its legal code. Now to understand the probability of such an attack, here is computed the number of required MFs that an intruder has to send to find his desired pair of MF. Like before, this research uses the set of E with F elements. To compute the probability, first must be computed the probability that a pair of MFs have the same code. It needs to compute two new variables W_1 and W_2. The W_1 is total number of ways that an intruder can make the set of E without duplicate codes and W_2 is the total number of ways that an intruder can construct the set of E while allowing for duplicates.

For W_1 there is different probability for each MF in the E, therefore:

$$W_1 = N \times (N-1) \times ... \times (N-F+1) = \frac{N!}{(N-F)!} \quad (6)$$

For W_2 there is equal probability for each element in the set of E therefore:

$$W_2 = N \times N \times ... \times N = N^F . \quad (7)$$

Thus, the probability of constructing the set of E without duplicate code is $\overline{P} = \frac{W_1}{W_2} = \frac{N!}{(N-F)!N^F}$.

Hence the probability of constructing the set of E with at least one duplications in the code values is $P = 1 - \frac{N!}{(N-F)!N^F}$ and after simplifying, the probability that at least two MFs have same code is $P = 1 - e^{-\frac{F(F-1)}{2N}}$ now it is computed the value of the F with probability of P. Like before, is considered three common probabilities it means 25%, 50%, and 75%. The number of MF that an intruder has to send to obtain a collision with these probabilities is: $F = 0.72 \times 2^{\frac{n}{2}}$, $F = 1.18 \times 2^{\frac{n}{2}}$ and $F = 1.67 \times 2^{\frac{n}{2}}$ respectively. Now for n=160 in MFIA and n=32 in CRC the result of this computation is shown in Table2.

Table2: Number of Required MFs for Collision Attack

Security	No. F with p= 25%	No. F with p= 50%	No. F with p= 75%
MFIA	8.70×10^{23}	1.43×10^{24}	2.02×10^{24}
CRC	4.71×10^{4}	7.73×10^{4}	1.09×10^{5}

As the Table2 shows, in MFIA intruder has to send a large number of management frames to find his desire management frames. From the probability of 50% for both approaches, the number of required management frames for MFIA is about 1.43×10^{24} operations and for CRC this number is about 7.73×10^{4} operations for the same probability. So it is clear that with this high difference values the intruder can break CRC with a less attempts but he needs more resources to do a successful attack on MFIA. As it mentioned before the amounts of resources directly is concerned to output size of the underlying algorithms.

3) Overhead Calculation of Management Frames

When a sender wants to send a frame to a receiver, from MAC layer to physical layer, some information as overhead are attached to the frame. In MAC layer a header and FCS attached to data and in physical layer Physical Layer Convergence Protocol (PLCP) overheads are attached to the MAC frame. All these overheads increase period of time between frames transmission hence they decrease the total number of transmitted management frames in WLAN [7], [8]. So to compute the number of frames that a WLAN can transmit in one second it is essential to consider the amounts of these overheads. To do this, first it is necessary to compute the length of MF in both proposed and current models which this research calls them LOF_{MFIA} and LOF_{CRC} respectively. As it mentioned before, the header length of MF is 24 bytes and its FCS is 4 bytes. Now at the bellow there is computation of the average length of its body. Because the proposed model is based on an open system authentication so the body of the authentication request is not included the challenge text therefore the length of body for authentication request and answer is 6 octets. The length of body for disassociation and deauthentication, because

they have only reason code, is 2 octets. Maximum association request length of body is 48 octets and reassociation request is 54 octets. The length of association response and reassociation response is 16 octets. So to compute the average of management frames body length:

$$MF_{bl} = \frac{2+48+16+54+16+6+2+6}{8} = \frac{150}{8} \approx 19byte \quad .$$

Now to compute LOF_{MFIA} it is necessary to sum the length of header, body, and trailer together as well the 160 bits length of the MAC output so: $LOF_{MFIA} = 24+19+4+20 = 67byte = 536bit$. In the current algorithm there is no extra 20 bytes hence to compute length of that: $LOF_{CRC} = 24+19+4 = 47byte = 376bit$

As a result average length of a management frame in the proposed model is 536 bits and in the current model is 376 bits. On the other hand, as it was mentioned before, each transmitted frame to PHY layer has some different delay times (overhead) before transmission, which include DCF Interframe Space (DIFS), Backoff random (BO), Short Interframe Space (IFIS), PLCP preamble and PLCP header. Therefore we can describe all these overheads as Fig.3.

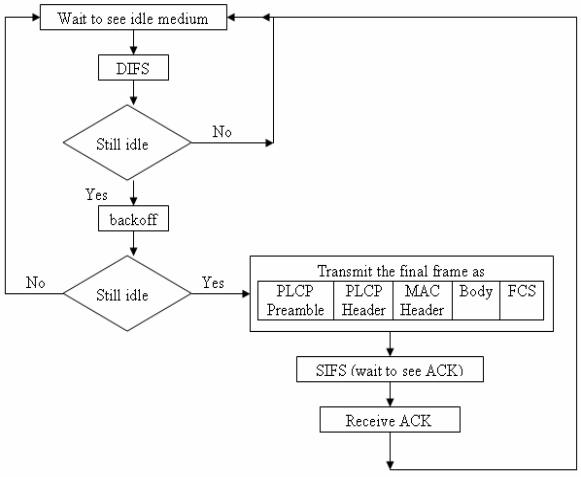

Fig.3: Frame Overheads

On the other hands Management frames have response frames instead of Acknowledge (ACK) frame like probe request with probe response and association request with association response. So to calculate total delay time, in the above figure the SIFS will be discarded because there is now any ACK frame transmission. Therefore according to [15], [16], [17] and [18] four main overheads for MAC frames in IEEE 802.11a and b are summarized in Table 3.

Table 3: IEEE 802.11Frame Overheads Value

Standard	Delay	Value (μs)
IEEE 802.11b (11 Mbps)	DIFS	50
	PLCP Preamble	144
	PLCP Header	48
	BO	15.5
IEEE 802.11a (54 Mbps)	DIFS	34
	PLCP Preamble	16
	PLCP Header	4
	BO	67.5

If $Otime_b$ is minimum transmission overhead for each frame in IEEE 802.11b then:

$Otime_b$ =DIFS+PLCP preamble + PLCP header + BO = 50+144+48+15.5=257.5

$Otime_a$ =34+16+4+67.5=121.5

On the other hand calculation of the required time for transmission one frame, without considering any overhead, uses its related data rate as follow:

$$\text{frame rate} = \frac{\text{data rate}}{\text{frame lenght}} \Rightarrow \text{IEEE 802.11b MFIA frame rate} = \frac{11\times 2^{20}}{536} = 21519$$

$$\text{frame rate} = \frac{\text{data rate}}{\text{frame lenght}} \Rightarrow \text{IEEE 802.11a MFIA frame rate} = \frac{54\times 2^{20}}{536} = 105640$$

Since in 802.11b transmission time of 21519 frames is one second so transmission time of one frame is: $\frac{1}{21519} = 46\mu s$. As well in 802.11a it is $\frac{1}{105640} = 9\mu s$

IEEE 802.11b total transmission time of one frame with its overhead=257.5+46=303.5μs.

IEEE 802.11a total transmission time of one frame with its overhead=121.5+9=130.5μs.

Finally to calculate number of frame per second (frame rate) in 802.11b with related overheads since one frame can transmit in $303.5\times 10^{-6} s$ hence frame rate= $\frac{1}{303.5\times 10^{-6}} = 3295$.

As well to calculate number of frame per second in 802.11a with related overheads since one frame can transmit in $130.5\times 10^{-6} s$ hence frame rate= $\frac{1}{130.5\times 10^{-6}} = 7663$

Now the same process will be done to calculate actual frame rate in CRC. This result is summarized in Table 4.

Table 4: Total Management Frame Rate in WLAN

Standard	Model	LOF (bit)	MAC over head (μs)	PHY Over head (μs)	Frame Rate
802.11b	MFIA	536	46	257.5	3295
	CRC	376	33	257.5	3442
802.11a	MFIA	536	9	121.5	7663
	CRC	376	7	121.5	7782

4) Required Time for Forgery Attack

One of important components to determine the effectiveness of the model is time. It is clear as the required time to do the attacks increases, the strength of the model to prevent the attacks increases. Therefore this research as well computes the required time to carry out this forgery attack in IEEE 802.11a and b. As it was mentioned in Table 1, the intruder has to send F management frames to do this attack. Since in one second number of transmission management frames is as Table4 therefore to transmit F management frame the required time is computed as follow:

In IEEE 802.11a time to the forgery for MFIA is $t_f = \frac{F}{7663}$.

In IEEE 802.11b time to the forgery for MFIA is $t_f = \frac{F}{3295}$.

(In MFIA F= 3.65×10^{47}, 7.3×10^{47} and 1.10×10^{48} for p=25%, p=50% and p=75% respectively)

In IEEE 802.11a time to the forgery for CRC is $t_f = \frac{F}{7782}$.

In IEEE 802.11b time to the forgery for CRC is $t_f = \frac{F}{3442}$.

(In CRC F=1.07×10^{9}, 2.15×10^{9} and 3.22×10^{9} for p=25%, p=50% and p=75% respectively)

Now by using Table1 to replace the number of F, the results of required time for this attack are shown in Fig.4.

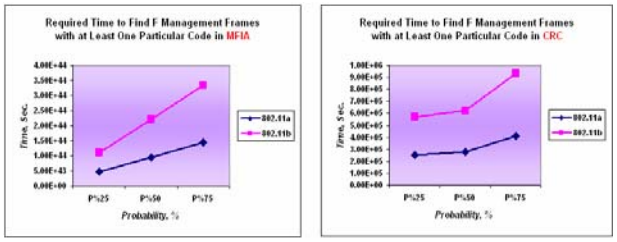

Fig.4 Required Time for Forgery Attack

5) Required Time for Collision Attack

This research as well computes the required time to do collision attack. As it was mentioned in Table 2, the intruder has to send F management frames to do this attack. Since in one second number of transmission management frames is as Table4 therefore to transmit F management frame the required time is computed as follow:

In IEEE 802.11a time to the forgery for MFIA is $t_f = \frac{F}{7663}$.

In IEEE 802.11b time to the forgery for MFIA is $t_f = \frac{F}{3295}$.

(In MFIA F= 8.70×10^{23}, 1.43×10^{24} and 2.02×10^{24} for p=25%, p=50% and p=75% respectively)

In IEEE 802.11a time to the forgery for CRC is $t_f = \frac{F}{7782}$.

In IEEE 802.11b time to the forgery for CRC is $t_f = \frac{F}{3442}$.

(In CRC F= 4.71×10^{4}, 7.73×10^{4} and 1.09×10^{5} for p=25%, p=50% and p=75% respectively)

Now by using Table2 to replace the number of F, the results of required time for this attack are shown in Fig.5.

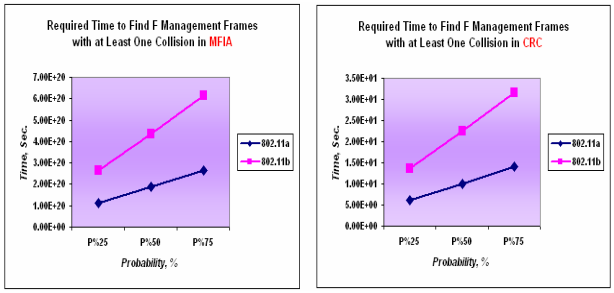

Fig.5 Required Time for Collision Attack

The Fig.4 and Fig.5 show that the intruder needs a shorter time to do a successful attack with CRC in contrast to MFIA. Results show CRC is absolutely susceptible to this attack. From these figures as well is calculated that the required time to do collision attacks is smaller than forgery attack for both MFIA and CRC in both IEEE 802.11a and IEEE 802.11b.

8. Conclusion

In this paper, we introduced the security issues in the WLAN management frames, and proposed an enhancement for their security. Furthermore, we conducted simulation/experiment on comparison of this proposed scheme with the original management frame

scheme. The proposed enhancement provides strong authentication and integrity for management frames which means any management frame that received by receiver first is checked for validation the source and also integrity of the contents to determine whether this received management frame is legal to be accepted or not. Therefore management frame tempering and injection is completely avoided by using the proposed model as the result of forgery and collision attacks probabilities show. This protection by MFIA leads to prevent three other common attacks on management frames it means: man-in-the-middle, session hijacking and MAC address spoofing attack.

From the results of required time to forgery and collision attacks, there does appear to be evidence that the time taken to do attacks is more in the proposed model than CRC. It is concluded that in MFIA, allocation of this time is almost infeasible by intruder because is very cumbersome.

References

[1] Bellardo J. and Savage S. 2003. 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. *Proceedings of the USENIX Security Symposium, Washington D.C.*

[2] Borisov N., Goldberg I., and Wagner D. 2001. Intercepting Mobile Communications: The Insecurity of 802.11. *Seventh Annual International Conference on Mobile Computing and Networking. Mobicom'01,* 180-189.

[3] Ding P. 2005. Central Manager: A Solution to Avoid Denial of Service Attacks for Wireless LANs *International Journal of Network Security,* Vol.4, No.1, 35–44.

[4] Faria D. B. and Cheriton D. R. 2002. DoS and Authentication in Wireless Public Access Networks. In *Proceedings of the First ACM Workshop on Wireless Security (WiSe'02).*

[5] Guo F. and Chiueh T. C. 2005. Sequence Number-Based MAC Address Spoof Detection.*8th International Symposium on Recent Advances in Intrusion Detection.*

[6] Liu C. 2005. 802.11 Disassociation Denial of Service (DoS) attacks. School of CTI DePaul University

[7] IEEE 802.11. 2006. Available online at http://www.answers.com/topic/ieee-802-11.

[8] Proxim Corporation. 2003. Maximizing your 802.11g Investment. Proxim Corporation.

[9] Walker J.R. 2000. Unsafe at Any Key Size: An Analysis of the WEP Encapsulation. Technical Report 03628E, IEEE Standards 802.11Committee.

[10] Welch D., and Lathrop S. 2003. Wireless Security Threat Taxonomy. *Proceedings of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY,* ISBN 0-7803-7808-3/03, 76-83.

[11] Xiao Y., Pan Y., Du X., Bandela C., and Dass K. 2004. Security mechanisms, Attacks, and Security Enhancements for the IEEE 802.11 WLANs. *International journal of wireless and mobile computing.*

[12] Yang H., Ricciato F., Lu S., and Zhang L. 2006. Securing a Wireless World. *Proceedings of the IEEE,* Vol. 94, No. 2, 442 – 454.

[13] He C. 2005. Analysis of Security Protocols for Wireless Networks, PhD. Dissertation, Stanford University.

[14] Wright J. 2003. Detecting Wireless LAN MAC Address Spoofing. White paper. Available online at http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf.

[15] Déziel M. and Lamont L. 2005. Implementation of an IEEE 802.11 Link Available Bandwidth Algorithm to allow Cross- Layering.

[16] Green L., Balmy K. and Embalming M. 2006. Theoretical Throughput Limits, TGT Draft Appendix A.

[17] Jun J., Peddabachagari P. and Sichitiu M. 2005. Theoretical Maximum Throughput of IEEE 802.11 and its Applications.

[18] Pavon J.D.P, Choi S. and Manor B. 2003. Link Adaptation Strategy for IEEE 802.11 WLAN via Received Signal Strength Measurement.

Biography

Mina Malekzadeh obtained her Bachelor in Computer honors degree from S & B University, IRAN in early 1997. After her graduation, she was employed in the biggest copper mine in the Asia National Iranian Copper Industries Company (NICICO) or Sarcheshmeh Copper Complex, IRAN in portion of Quality Control as a computer programmer. She enrolled in the Master of Science (Software Engineering) at University Putra Malaysia in early 2006. The author hopes to continue a doctorate in security in computing in future.

Abdul Azim Abd Ghani received the B.Sc in Mathematics/Computer Science from Indiana State University in 1984 and M.Sc in Computer Science from University of Miami in 1985. He joined Universiti Putra Malaysia in 1985 as a lecturer in Computer Science. He

received the Ph.D in Software Engineering from University of Strathclyde in 1993. He is an Associate Professor and the Dean of Faculty of Computer Science and Information Technology, Universiti Putra Malaysia. His research interests are software engineering, software measurement, software quality, and security in computing.

Zuriati Ahmad Zulkarnain received the B.Sc. Ed. majoring in Physics and M.Sc. in Information Technology from Universiti Putra Malaysia in 1997 and 2000 respectively. She joined Universiti Putra Malaysia in 2000 as a lecturer in Computer Science. She received the Ph.D in Quantum Computation and Information from University of Bradford in 2006. She is the Head of Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia. Her research interests are quantum computation, computer networks, and distributed computing.

Zaiton Muda received the B.Sc and M.Sc. degrees in Computer Science from Universiti Kebangsaan Malaysia in 1984 and 1989 respectively. She is a senior lecturer in Faculty of Computer Science and Information Technology, Universiti Putra Malaysia. Her research interests are computer security and parallel computing.