Central Manager: A Solution to Avoid Denial of Service Attacks for Wireless LANs

Ping Ding

Computer Engineering Department, Santa Clara University
Santa Clara, CA 95053, USA. (Email: pding@scu.edu)

(Received July 19, 2005; revised and accepted Aug. 30 & Oct. 4, 2005)

Abstract

802.1x is a security protocol based on the frame structure of 802.11. It attempts to provide strong authentication, access control, and WEP key management for Wireless LANs. Unfortunately, 802.1x misses its goals in access control denial of service (DoS) attacks. Currently, there are no IEEE approved ways to solve the security hole. We propose a Central Manager (CM) not only to take the responsibility of an authentication server, but also to add functionality to prevent denial of service attacks. We analyze the performance of WLANs under DoS attacks and demonstrate the correctness of the CM solution through simulations. From the simulations, we conclude the CM solution can efficiently avoid DoS attacks and alleviate the effects from the DoS attacks.

Keywords: Central manager, denial of Service, IEEE 802.1x, wireless Lans

1 Introduction

Because it is convenient to use, wireless networks become more and more popular. However, security is a big issue in wireless communications. The research of security aims to improve the reliability of wireless communications [3] and includes security key management [5, 6, 13], avoiding attacks [9, 15, 16], such as denial of service (DoS) attacks [7], wormhole attacks [9], and jamming attacks [15]. Currently, a lot of studies focus on these areas.

In [3], the authors propose redundancy technology to improve the dependability of wireless lans. In [8], the authors study the MAC layer misbehavior to improve the security of wireless lans. In [4], the authors present a protocol to provide security and authenticated in-network processing in wireless sensor networks. In [9], the authors propose a special protocol, Leashes, to against wormhole attacks in ad-hoc networks. In [15], the authors propose two schemes to detect jamming attacks in wireless networks. In both [5] and [6], the authors propose a key management scheme to improve the security for wireless sensor networks. In [13], the authors propose a group key management scheme to improve security in group communications. Though DoS is a well known security hole in wireless communications, there is no efficient way to prevent it. In [7], the authors analyze DoS attacks and conclude that providing MAC layer fairness can alleviate the effects of such attacks. However, the authors do not give any specific solutions. In [16], the authors propose a new counter measure to prevent two kinds of DoS attacks, a single adversary attack and colluding adversaries attack, in ad-hoc networks. However, it does not cover all kinds of DoS attacks and it only considers non-secured IEEE 802.11 MAC protocol [2]. However, DoS attacks occur in a secured wireless LAN also [12].

There is no published solutions proposed to avoid the DoS attacks in a secured wireless LAN (WLAN), in this paper, we focus on how to avoid DoS attacks in such a WLAN. We will propose a Central Manager (CM) solution to avoid DoS attacks. In addition to take the responsibilities of the authentication server (AS) [12], the CM also traces the activities of the clients to detect and avoid the DoS attacks. We summarize DoS attacks in two categories, login part and logout part. Based on three tables and a timer, the CM manages the Access Points (APs) and clients activities. All the two categories DoS attacks will be detected and avoided. We also demonstrate the correctness of CM through simulations. Simulation results show CM can efficiently avoid DoS attacks and alleviate the effects of the DoS attacks on the performance of the WLANs.

The contribution of the paper is we propose a central manager solution to avoid DoS attacks without making any changes to any IEEE 802.11 frames. The rest of the paper is organized as follows: we analyze the related work in Section 2 and explain IEEE 802.11 and IEEE 802.1x in Section 3. DoS attacks are introduced in Section 4. We propose the central manager solution in Section 5. The analysis of WLANs performance and simulation results are given in Section 6. In Section 7, we conclude the paper.

2 Related Work

Since wireless technologies have been widely used, how to improve the wireless network security become a very active research field. Some research studies on how to efficiently manage secure keys. Du et al. [5] propose a random key pre-distribution scheme to achieve security in sensor networks where the key management is based on deployment knowledge of the sensor nodes. To make the communications between sensor nodes secure and efficient, Du et al. [6] use an one-way hash function to encrypt each packet instead of using Public Key Cryptography. Using a multi-group key management scheme, San et al. [13] build a security infrastructure that ensures multiple levels of access privilege for group members. Dimitriou et al. [4] study a new protocol to provide security in sensor networks, where the protocol relies on aggregator nodes to provide data aggregation and command dissemination.

There is a lot of interesting on access control which includes how to detect and avoid security attacks. Gupta et al. [7] analyze DoS attacks under different traffic patterns in ad-hoc networks and conclude that MAC layer fairness will alleviate the effects of DoS attacks. Hu et al. [9] present a mechanism, packet leashes, to detect and defend against the wormhole attack, a server attack, and, they also propose a protocol to implement the packet leashes. Xu et al. [15] analyze four models of jamming attacks and propose two schemes to detect the attacks where one scheme employs signal strength as a measurement and the other employs location information as a measurement. Zhou et al. [16] propose a timestamp solution to avoid DoS attacks in ad-hoc networks where the timestamp is maintained by each node. However, all previous solutions consider DoS attacks on non-secured IEEE 802.11 MAC protocol. Furthermore, DoS attacks occur in a secured IEEE 802.11 also [12].

All these DoS attacks are done with management frames. Since IEEE has stated that all management frames must be unencrypted in 802.11, management frames should be kept clean in 802.11 or 802.1x. In industry, some companies use keyed integrity check (IC) to prevent rogue disassociation, such as PEAP (Microsoft[10]. Keyed IC uses a key generated from a seed value, source and destination MACs and payload and the key is included to every WEP packet. The method is time consuming and only solves disassociation after the WEP key has been generated. In this paper, we solve DoS attacks in the secured IEEE 802.11, 802.1x.

3 IEEE 802.11 and IEEE 802.1x

IEEE 802.11 is based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) [11]. Carrier sensing is performed using both physical carrier sensing (by air interface) and virtual carrier sensing. The effect of physical carrier sensing is determined by the transmit power of the sender. Virtual carrier sensing is performed by including the duration of the packet transmission in the header of RTS, CTS, and DATA frame which infers how long the transmitting packet will last. When a node wants to transmit, it needs to sense the channel for a DIFS time. If the channel is idle in the DIFS time, then the node sends the data frame. If the node is acknowledged by ACK from the receiver, the transmission is considered successfully. If the channel is busy during the DIFS time or any collisions occur during RTS-CTS-ACK handshake, then the node has to wait another time interval given by the back-off window and retry after the counter of the back-off window reaches zero (the maximum number of retrying limit is 6 or depends on the system setting [11]).

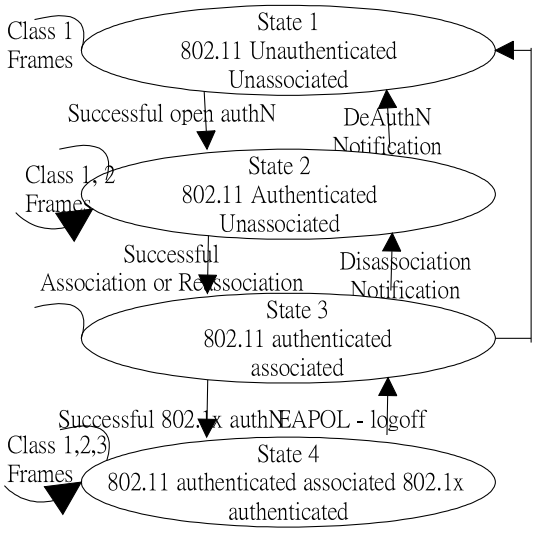

Figure 1: 802.11/802.1x state machine

Since IEEE 802.11 has security holes [2], IEEE has proposed a secure architecture for 802.11 called Robust Security Network (RSN). RSN uses the recently approved IEEE standard for Port-based Network Access Control, 802.1x. 802.1x takes advantage of an existing authentication protocol known as the Extensible Authentication Protocol [11] to provide centralized authentication of wireless clients. EAP messages are encapsulated in 802.1x messages and referred to as EAPOL. 802.1x authentication for wireless LANs has three main components: The supplicant (usually the client software); the authenticator (usually the access point); and the authentication server (AS, usually, it is a Remote Authentication Dial-In User Service server which manages all APs' authentication processes in the WLAN).

Based on RSN, IEEE provides an 802.11/802.1x state machine (Figure 1) to provide strong authentication, access control, and WEP key management for Wireless LANs. Unfortunately, 802.1x does not realize all its security goals since it is still vulnerable to DoS attacks. Mishra and Arbaugh [12] describe these attacks which we will summarize in next section.

Table 1: 802.11/802.1x state transition functions

Management Frame	S1	S2	S3	S4
EAP-Start	NA	NA	S1,4	NA
EAP-Failure	NA	NA	S1	NA
MAC disassociation / EAPOL logoff	S1	S2	S1	S1
802.11 Association	S2	NA	NA	NA

4 Denial of Service (DoS) Attacks

Based on the state machine, we can write a state transition function as in Table 1 (the right four columns show the AP state after receiving corresponding management frame), where NA indicates an AP does not accept the management frame in that state. For example, after an AP receives EAP-Start request in State 3, the AP's state could be State 1 or State 4. After the AP in state 1 receives 802.11 association, the AP's new state is State 2. The AP will not know its next state until the authentication succeeds or fails. However, after an AP receives EAP-Failure, MAC disassociation or EAPOL logoff (State 4), the AP's status goes to State 1. The reason is that the AP can not identify whether the management frame comes from a client or an attacker till authentication is complete. We call these DoS attacks and summarize them as follows:

Large number of association requests: An attacker (an adversary client) continuously uses random MAC addresses to do association with an AP, making the AP busy working with the attacker and preventing any other clients from joining the AP. We call it LASO.

EAPOL Logoff: In this attack, the attacker spoofs the client's MAC address and sends EAPOL logoff request to the AP, making the AP disassociate with its authenticated client, thus denying service to the client.

EAP-Start, EAP- Failure spoofing: In this attack, an attacker continuously sends EAP-Start request, making an AP busy with the authentication dialog and unable to handle legitimate traffic. Or, an attacker continues to send EAP-Failure, then, the AP disassociates with its legitimate client.

MAC disassociation: Attackers continue to send MAC disassociation, making an AP disassociate with an authenticated or authenticating client.

5 Using A Central Manager to Avoid DoS Attacks

We propose to use a Central Manager (CM) to dynamically manage a large number of APs and their clients. The CM is a back-end server that takes the place of the AS defined in 802.1x [11]. It not only takes the responsibilities of the AS, but also tracks clients in the authentication process to avoid the DoS attacks described in Section 4, and helps in load-balancing of the APs. The authentication service of the CM is unchanged from 802.1x. In this section, we explain how the CM avoid DoS attacks.

Table 2: Client authenticated table (T2)

Client MAC	PLO	TLOT	Location
*********	1	0	*******

5.1 Terminology

Priority of login(PLI): 0 indicates the priority of login is low. 1 indicates the priority of login is higher than logout.

Priority of logout(PLO): 0 indicates the priority of logout is low. 1 indicates the priority of logout is higher than login.

Times of login(TLI): It records the number of login requests from some clients to the CM.

Times of logout To CM (TLOT): It records the number of logout requests from some clients to the CM.

Times of logout from CM (TLOF): It records the number of logout request sent by the CM to some clients.

CM will depend on three tables, which are Table for AP (T1), Client authenticated table (T2), and Client unauthenticated table (T3), to avoid DoS attacks. All tables are generated and managed by the CM. T1 records all APs' information. Each AP both has a T2 and a T3 which manages authenticated clients or unauthenticated clients respectively for the AP. T1 and T3 are used to manage all APs in the WLAN to prevent LASO attacks. T2 and T3 are used to prevent all the other DoS attacks. PLI, PLO, TLI, TLOT, and TLOF are either shown in T2 or in T3, which are used to record the activities of each client and identify DoS attacks. Next, we explain the details of T1, T2, and T3.

Table for AP (T1): T1 records all the information of the access points. CM generates and manages the table. It contains the MAC address and location of the AP, and the number of authenticated and unauthenticated clients of the APs (after a client associates with an AP, it becomes the AP's unauthenticated client).

Client authenticated table (T2): It records all the information of authenticated clients of an AP. It includes the MAC addresses of the clients, the time the clients are authenticated (login) and the location of the client. An AP can base on the signal strength and direction to determine the location of its client, then, it sends the client's location information to the CM. The default values of T2 are given in Table 2.

Client unauthenticated table (T3): It records all the information of unauthenticated clients of an AP including its location. Pre-Association Time (PAT) is the time a client starts association. The default values of T3 are

Table 3: Clients unauthenticated table (T3)

CMAC	PLI	TLI	PLO	TLOF	TLOT	AP MAC	PAT	Loc
*****	1	0	0	0	0	********	***	***

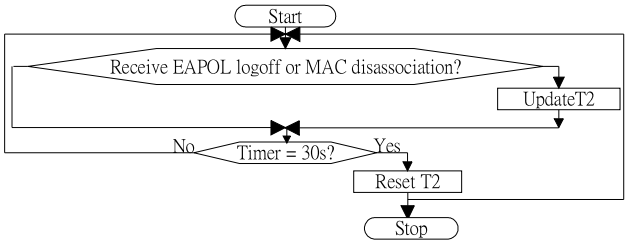

Figure 2: CM manages T2

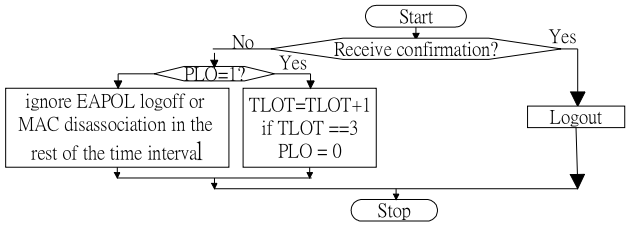

Figure 3: UpdateT2

given in Table 3. CMAC indicates the MAC addresses of clients. Loc indicates the locations of clients.

We also define a timer, a time interval of 30 seconds. The timer is used to limit the client's response time which is no more than 30 seconds. It is suggested in IEEE EAP that a request be resent a minimum of 3 times before terminating the authentication [11]. In our design, a client is allowed to try three times before transforming from one state to another state (recall Figure 1). After that, the CM will ignore the requests from the client. On the other hand, to avoid the busy of the CM caused by the increase of the tables, T1, T2, and T3 will be cleaned or updated at the end of the timer. We will give more details in the next sections.

All vulnerable management frames can be separated into two categories. The first is the login part, such as EAP-Start and 802.11 association. The second is the logout part, such as EAPOL logoff, MAC disassociation or EAP-Failure. In [11], all the management frames are forwarded to the AS by APs excluding all the vulnerable management frames mentioned in Section 4. In our design, all these vulnerable management frames will be forwarded to the CM by the APs. An AP will not respond to the management frames until the CM instructs to it. The CM avoids DoS attacks by using three tables, T1, T2, and T3, and the timer. All management frames are kept clear and unencrypted as defined by the IEEE, however, if the WEP key has already been generated, then the CM will send an encrypted request packet to the client using the WEP key. If the WEP key has not been generated, then the CM will use tables T1 and T3 to decide its next step. In the follow sections, any request received by the CM is forwarded by some AP, and any message sent from the CM to a client is forwarded by some AP.

5.2 Avoiding LASO Attacks

We introduce two processes: Pre-Check and Pre-Association. The two processes work together to avoid LASO attacks. After receiving an 802.11 association request from a client, the CM processes the Pre-Check to decide going to the Pre-Association or not. Pre-Check is the followings. Say the client is associating with an AP, named A. The CM checks the client location information in T3 of A. If the same location information has already been recorded in T3 of A, the CM will ignore the request. Otherwise, the CM goes to the Pre-Association.

During Pre-Association, the CM gets the MAC addresses of both the client and the AP. Based on the network load which is maintained by T1, the CM will decide accepting the request or not. After checking in T1, the CM will send a success or denial packet to the client. If the reply packet is a success packet, it indicates the client can continue the authentication process. The AP will give the client an association id, and the CM will increase the number of unauthenticated clients of A by one in T1 and write down the client in T3 of A. Thus, the Pre-Association is finished with the success of the 802.11 association. If the packet is a denial packet with the location of a suggested AP, it indicates the client needs to connect to the suggested AP. The Pre-Association is finished until either the AP accepts the 802.11 association or denies the request. For example, assume the CM finds that AP-A already has 10 clients, but its neighbor AP-B does not have any clients. When a new client sends an association request to AP-A, the CM will suggest that the client associate with AP-B. After the client associates with AP-B, the CM will increase the number of unauthenticated clients of AP-B by one in T1 and write the client information in T3 of AP-B. The client will be an unauthenticated client of AP-B where the client also gets an association id from AP-B.

We assume some clients are adversary clients, they send 802.11 association requests with random MAC address. From the previous descriptions of Pre-Check and Pre-Association, we know those attackers will not make APs busy and deny service to other clients. Thus, a large number of association (LASO) attacks will be efficiently

avoided. A client is allowed to continue 802.1x authentication only if it gets an association id, e.g., it is in T3 of some AP. Next, we explain how to avoid EAPOL logoff attack.

5.3 Avoid EAPOL Logoff Attack

An attacker sends an EAPOL logoff to an AP using a working (legitimate) client's MAC address, which makes the AP deny the services of the working client. The CM will avoid the attack as the followings. Once the client is authenticated (the WEP key has already been generated), the CM will send an encrypted request packet to the client using the WEP key. In the request packet, the CM will ask the client if it wants to logoff. After the client receives the request packet, it needs to give a confirmation if it is true, or, it can ignore it if it is false. If the CM receives a confirmation message, it will send a logoff-continue message to the AP, then the AP let the client disassociate. If the CM receives a denial message or does not get a response from the client, the CM will send a logoff-ignore message to the AP. The AP will ignore the logoff request and keep the client's current status. Say the corresponding AP is A.

If the CM receives confirmation message from the client, the CM reduces the number of associated clients with A in T1 by one and deletes the client information in T2 of A. If the CM receives a denial message from the client, the CM adds 1 to TLOT in T2 of A. This process will be allowed until TLOT equals 3 in timer time period, at which time the CM will update PLO to be 0. If the PLO is 0, the CM will ignore EAPOL logoff request for the rest of the timer time interval. After the current timer time interval is over, the CM will reset each AP's T2 including A to be its default values. Figure 2 shows how the CM manages EAPOL-logoff request where the detail of the UpdateT2 process is shown in Figure 3. Thus, EAPLO logoff attack can be efficiently avoided.

5.4 Avoiding EAP-Start, EAP-Failure Spoofing and MAC Disassociation Attacks

5.4.1 Avoiding EAP-Start Spoofing Attack

An attacker sends an EAP-Start after it associates with an AP with spoofing a working client's MAC address or not, which makes the AP busy in working with the attacker and makes the attacker start an 802.1x authentication process with the authentication server (AS). The authentication process terminates until the AS can not identify the attacker. Finally, the AS will send an EAP-Failure to the AP and the AP disassociates with the attacker. In this scenario, two things could happen. Before the AS sends EAP-Failure, the attacker sends several EAP-Start; or the AS could identify and send an EAP-Failure to the AP immediately after an EAP-Start request. In addition, there can be a combination of these two cases. With the help of T2 and T3 of the corresponding AP, say it A, the CM can successfully avoid this attack. Next, we show how the CM avoids the attack in three cases.

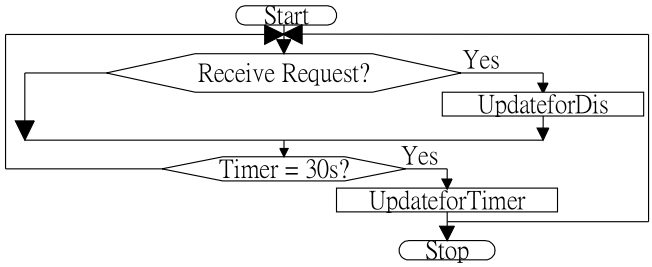

Figure 4: The CM manages T3

Case 1: After receiving the EAP-Start request, the CM checks the client in T2 and T3 of A. If the client's information can be found neither in T2 nor T3, the request will be ignored. Since the request is from an unassociated client, the CM infers that the request is from an attacker.

Case 2: If the client's information is found in T2 of A, the request will be ignored. Since the request is from an authenticated client, the CM infers that the request is from an attacker which spoofs an authenticated client's MAC address.

Case 3: If the client's information is found in T3 of A, then the CM will use T3 to make a decision. After a client finishes Pre-Check and Pre-Association, the CM adds the client information to T3. When the CM receives an EAP-Start request, it will also add one to the TLI. T3 is updated by setting PLI=1, TLI=1, PLO=0, TLOF=0, and TLOT=0. The CM and the client now do mutual authentication based on 802.1x. If 802.1x authentication is successful, then the client information will be deleted from T3 of A and added to T2 of A. And, the number of authenticated and unauthenticated clients of A will be increased and decreased by one respectively by the CM. If the 802.1x authentication failed, the CM just keeps the client's information in T3 of A and let A send an EAP-Failure to the client. Before the CM identifies and sends an EAP-Failure to A, the attacker may continue to send an EAP-Start request. Every time when the CM receives an EAP-Start request message, TLI increases by one. The CM will only allow A responses to the EAP-Start message three times. After the CM finds TLI equals three and TLOT equals zero, the CM will update PLO to one and ignore any EAP-Start request in the current timer time interval. After A receives an EAP-Failure message from the CM, A will disassociate with the client. The algorithm is shown in Figure 4 where the UpdateforDis is shown in Figure 6 and UpdateforTimer is shown in Figure 5. In

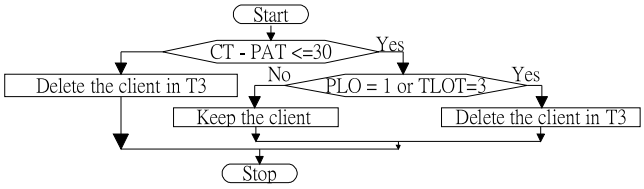

Figure 5: Update for Timer

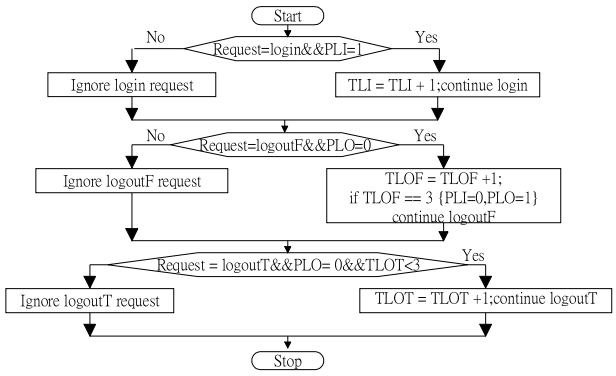

Figure 6: Update for Dis

Figure 6, Request = login indicates the CM receives an EAP-Start request where the client continues to send an EAP-Start request before the CM responds to it.

In another case, the CM sends an EAP-Failure message to A immediately after receiving an EAP-Start request. When the CM sends an EAP-Failure to A, the CM increases TLOF by one. The CM will allow the process to repeat till TLOF to three. At that time, the CM will set PLI to zero and PLO to one. If the CM receives EAP-Start again, the CM will let A ignore EAP-Start request in the rest of the timer time interval. The algorithm is shown in Figure 4 where the UpdateforDis is shown in Figure 6 and UpdateforTimer is shown in Figure 5. In Figure 6, Request = logoutF indicates the CM receives an EAP-Start request where the CM responds to it with an EAP-Failure immediately.

T3 of A is updated regularly in the timer time interval (see UpdateforTimer in Figure 5). If a client's PLO equals one or the client stays in T3 more than 30 seconds (current time (CT) minus Pre-Association time (PAT) longer than 30 seconds), the client's information will be deleted from T3. Otherwise, the client's information is kept in T3. The timer in the CM does not interfere with the time stamps contained in the beacon frames of the APs. Thus, the CM avoids the EAP-Start attack from the attackers.

5.4.2 Avoiding EAP-Failure Spoofing Attack

The EAP-Failure attack occurs when a working client is in the process of authentication. The attacker sends an EAP-Failure message to the AP and the AP disassociates with the working client which is on the authentication process.

The CM uses T3 of the corresponding AP, say it A, to mitigate this attack. When the CM receives an EAP-Failure from the client, The CM will add one to TLOT. The CM lets A disassociate with the client and keeps the client's information in T3 of A. The client will reassociate with A and restart authentication process with the CM. The CM may receive EAP-Failure from the client again. The process can repeat until TLOT equals three. Then, the CM will ignore any EAP-Failure messages for the rest of the timer time interval. The working client gets a chance to continue its authentication process and further attacks are prevented. T3 of A is updated regularly during the timer time interval (see UpdateforTimer in Figure 5). If a client's TLOT equals three or the client stays in T3 more than 30 seconds (current time (CT) minus PAT longer than 30 seconds), the client's information will be deleted from T3 of A. If the TLOT is less than three and CT minus PAT is less than 30 seconds, the client's information is kept in T3. The algorithm is shown in Figure 4 where the UpdateforDis is shown in Figure 6 and UpdateforTimer is shown in Figure 5. In Figure 6, Request = logoutT indicates the CM receives an EAP-Failure message. Thus, the EAP-Failure attacks can be avoided.

5.4.3 Avoiding MAC Disassociation Attack

In this attack, an attacker sends a MAC disassociation to an AP before or after a client is authenticated making an AP disassociate with the working client. With the help of tables T2 and T3 of the corresponding AP, say it A, and the timer, this attack can be avoided.

After the CM receives a MAC disassociation request, the CM checks in T2 and T3 of A. If the CM finds the client is in T2 of A, it indicates the client is currently in state 4. The process will be the same as when the CM receives an EAPOL logoff request. If the CM finds the client is in T3 of A, it infers the client is in state 1, 2 or 3. Then, the process is the same as in case 3 when the CM receives an EAP-Failure message. Figure 4 shows how the CM manages T3 of A where Figure 5 shows the UpdateforTimer process and Figure 6 shows the UpdateforDis process. In Figure 6, Request = logout T indicates the CM receives a MAC disassociation message.

6 Performance Evaluation

In this section, we will show both numerical results and simulation results. To evaluate our algorithms, we define two metrics: **Throughput** (the number of packets that can pass through in a fixed time) and **Delay time** (the interval from the time a user requests a service to the time the service is granted).

6.1 Numerical Results

We calculate the throughput and delay time by considering the valid data frame in each transmission. For example, we only consider the contribution of data frames to the throughput but ignore the contribution of management frames, such as, RTS, CTS, and ACK.

Throughput (S)**:**
Because DCF functionality is based on random techniques and is used by asynchronous traffic, we assume: 1) An event is a packet arrival with Poisson distribution. 2) Arrivals occur at random over a time interval. Let the inter-arrival rate be , so the length of the average idle period is $I = 1/\lambda$. 3) All of the packets have the same propagation delay, τ, and it is much smaller than packet duration L (includes 802.11 Association, EAP-Start, EAP-Failure, EAPOL logoff, 802.11 Disassociation, RTS, CTS, SIFS and ACK period).

The probability of K packet arrivals in $[0, \tau]$ is:

$$P_k = P\{k \text{ arrivals in } (0, \tau]\} = (\lambda\tau)^k e^{-\lambda\tau}/k!$$

The probability of 0 packet arrivals in $[0, \tau]$ is:

$$\begin{aligned} P_0 = P\{0 \text{ arrivals in } (0, \tau]\} &= e^{\lambda\tau} \\ P\{ \text{ one or more arrivals in } (0, \tau]\} &= 1 - P_0 \\ &= 1 - e^{-\lambda\tau} \end{aligned}$$

The probability of successful transmission is $P_s(P_0)$ and the probability of collision is $1 - PS$. MACAW does not guarantee to prevent collisions [1]. The collision duration will be the maximum length of the frames, because of no collision detection. Two mutually exclusive events could happen in a busy period time (B) where if a frame successfully transmits, the transmission time (T_s) is $L+\tau$; or, if a collision occurs, the transmission time T_c is also $L + \tau$. So

$$\begin{aligned} B &= P_s * T_s + (1 - P_s) * T_c \\ &= e^{-\lambda\tau} - *(L + \tau) + (1 - e^{-\lambda\tau}) * (L + \tau) \\ &= L + \tau \end{aligned}$$

The utilization period (U) is the period of successful transmission with no overhead, which is:

$$U = Le^{-\lambda\tau}$$

The Throughput (S) is:

$$\begin{aligned} S &= U/(T_{DIFS} + I + B) \\ &= Le^{-\lambda\tau}/(T_{DIFS} + 1/\lambda + L + \tau). \end{aligned}$$

To analyze the effect of DoS attacks to the throughput, let $G = \lambda L$, which indicates the packet arrival (attempts) per packet time; and let $a = \tau/L$, which indicates the propagation delay (τ) to the percentage of the packet duration (L). Both the increase of G and a could be caused by DoS attacks. Thus:

$$S = Ge^{-aG}/(1 + \lambda T_{DIFS} + G + aG)$$

Table 4: An example of accumulated values of curve codes

Parameters	Simulation 1 & Simulation 2
Packet Rate	448 kbps
Packet Size	112 bytes
Size of the WLAN	15 clients and two APs
# adversary clients	1,2,3,4
Frequency of DoS attacks	Every 3 seconds
Simulation time	100 seconds
Simulation results	average over 50 runs

Figure 7 shows the throughput in a packet time. The x-axis is the G, which indicates the attempts per packet time, and the y-axis is the throughput in a packet time (the maximum is 100% in a packet time). As shown in the figure, S reduces as G or parameter-a grows. It is because the probability of collision grows with the increase of G and a.

Delay Time (T)**:**
When a client wants to access the medium (assume the client has already authorized by the AP), it senses the channel. If the medium is idle, the clients can access the medium immediately after waiting DIFS. The shortest T_{CP} equals $1/\lambda + T_{DIFS}$. If the medium is busy, a client has to wait until it is free. The client waits for a time given by the exponential backoff algorithm, T, which is $\sum_{j=0}^{n} K(i, j)$. $k(i, j)$ is chosen from 0 to $(2^i \times CW_{min}) - 1$ ([11], CW_{min} is the counter of minimum back-off window). Here, j is the number of times the medium is checked and $0 \leq j \leq n; i$ is the stage of the back-off window, where $i = j$ when $0 \leq j \leq 5$ and $i = 5$ when $5 \leq j \leq n$. If DoS attacks occur, then the contentions between the clients is increased. Once collisions occur, a client has to wait in the back-off window and tries next time. So, T is increased.

From the analysis, we can easily conclude that both S and T are mostly determined by collisions where collisions are caused by contentions between the clients. The DoS attacks will increase the contentions between the clients. Therefore, DoS attacks will reduce both S and T. We cannot prevent an attacker from sending DoS attack messages, but we can manage the AP so it does not respond to an attackers request. This reduces the probability of attackers contending with other clients for the medium and alleviates the effects of the DoS attacks on the performance of the WLANs. In the next section, we will show simulation results.

6.2 Simulation Results

To validate that the CM will improve the performance of WLANs, we set up simulations to show how DoS attacks affect the performance and how a CM alleviates the effects. The evaluation is made with respect to the

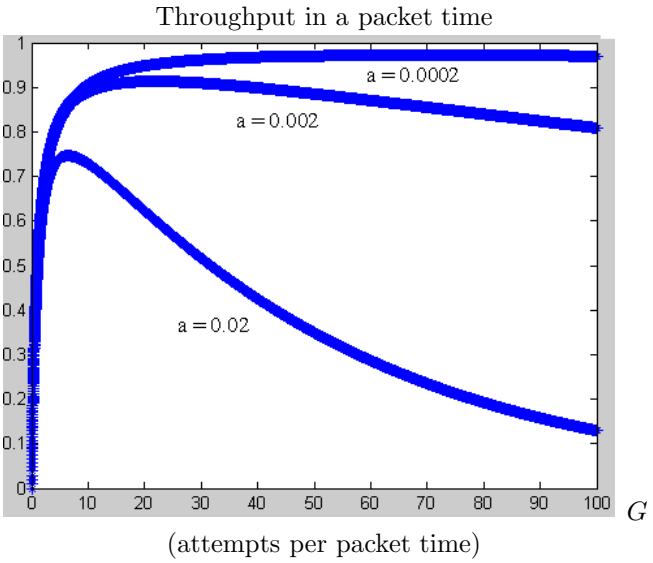

Figure 7: Throughput of S

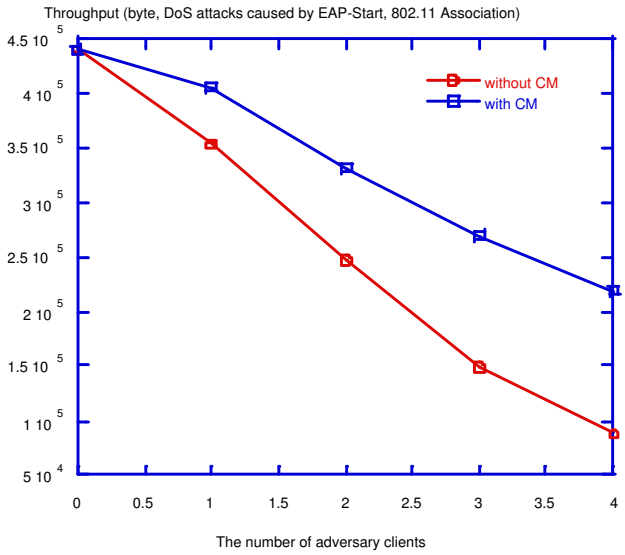

Figure 8: Throughput (login DoS attacks)

two metrics we defined previously, throughput and delay time. We simulate DoS attacks in two parts: those belong to login part which include EAP-Start and 802.11 Association; and those belong to logout part which include EAP-Failure, EAPOL logoff, and MAC disassociation. Our simulations are built on network simulator NS-2 [14]. We use CBR applications as traffic generators. The throughput and delay time are calculated from valid CBR packets that reach their destinations. Table 4 shows the system parameters in the simulations. For example, in all the simulations, the data packet rate is 448kbps and size is 112 bytes; the WLAN consists of 15 clients and two APs where the CM is installed in the backend server which controls the two APs; there are at most four adversary clients in the WLAN, all of which send DoS attacks in every 3 seconds. In the next sections, we will show how the CM avoids login DoS attacks and logout DoS attacks. All simulation results are the average of 50 runs. Each simulation lasts for 100 simulation seconds, which is sufficient for measuring at steady state.

6.2.1 The CM Avoids Login DoS Attacks (EAP-Start and 802.11 Association)

In this simulation, each adversary client randomly sends either an EAP-Start or an 802.11 Association request in every 3 seconds. We will show the CM can reduce the effects from the login DoS attacks (EAP-Start, and 802.11 Association) and improves the performance of WLANs. With the help of tables T1, T2 and T3 (recall Section 5) and the timer, the CM will allow a client to continue login process or block it. Because the CM can not prevent an adversary client from sending either EAP-Start or 802.11 Association, the contentions for the channel caused by the adversary clients can be reduced but can not be avoided. In Figure 8, the x-axis is the number of adversary clients which is from 0 to 4 and the y-axis is the throughput.

As shown in the figure, when the CM works (with CM), the throughput of the WLAN is much better than the throughput in the WLAN without CM (without CM). Compared with the throughput in the WLAN without DoS attacks, the throughput of the WLAN is reduced even with the CM. It is because the contentions for the channel caused by DoS attacks can not be avoided. In Figure 9, the y-axis is the delay time. When the CM works (with CM), the delay time of a packet in the WLAN is much less than the delay time in the WLAN without the CM (without CM). The reason is the same as in the throughput.

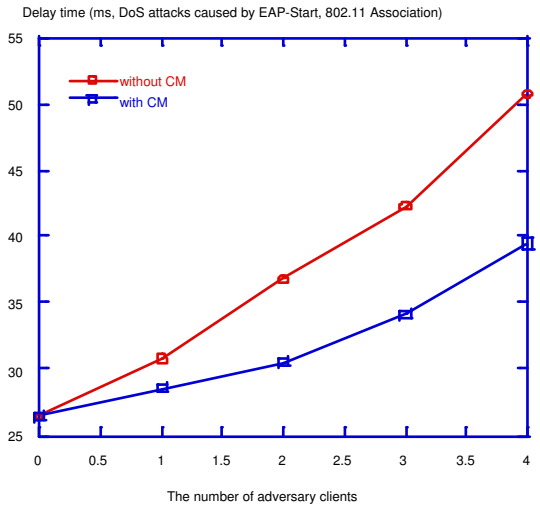

Figure 9: Delay time (login DoS attacks)

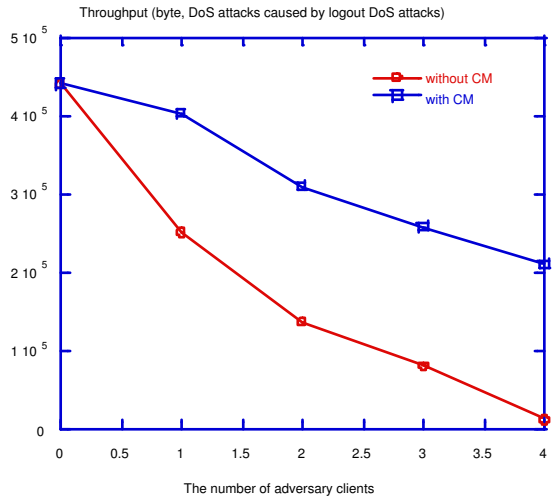

Figure 10: Throughput (logout DoS attacks)

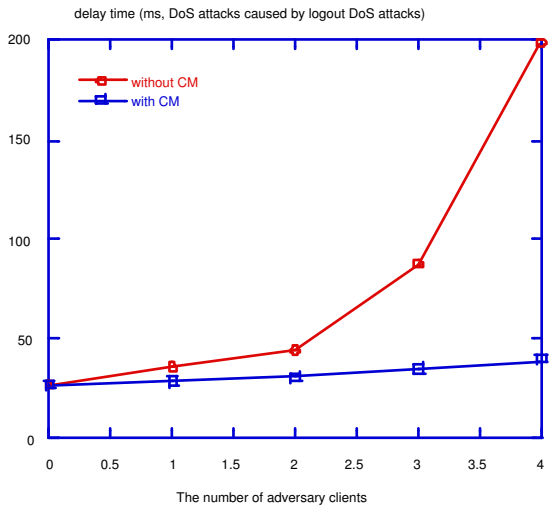

Figure 11: Delay time (logout DoS attacks)

6.2.2 The CM Avoids Logout DoS Attacks (EAP-Failure, EAPOL Logoff, MAC Disassociation)

In this simulation, each adversary client randomly sends an EAP-Failure, an EAPOL logoff, or a MAC Disassociation request in every 3 seconds. We will show the CM can reduce the effects from the logout DoS attacks (EAP-Failure, EAPOL logoff and MAC Disassociation) and improve the performance of WLANs. With the help of tables, T1, T2 and T3 (recall Section 5) and the timer, the CM will allow a client to continue logout process or block it. Thus, an adversary client can not make a working client logout from the WLAN. As the login DoS attacks, the logout DoS attacks cause more contentions betweens the clients. Thus, compared with a WLAN without DoS attacks, the performance of the WLAN will be reduced even with the CM. Figure 10 shows the throughput under logout attacks. As shown in the figure, the throughput is dramatically reduced with the increase of the adversary clients. It is because these adversary clients will prevent a working client from sending a packet. With the help of the CM (with CM), the throughput is much better than the throughput without the CM (without CM). Figure 11 shows the delay time under logout attacks. As shown in the figure, the delay time is dramatically increased with the increase of the adversary clients. With the help of the CM, the delay time can be dramatically reduced. The reason is the same as in the throughput.

6.3 Summary

In this section, we show the DoS attacks will affect the performance of WLANs through both analysises and simulations. From the simulation results, we demonstrate the correctness of the CM solution. We conclude that the CM is a good solution for avoiding DoS attacks and improving the performance of WLANs under DoS attacks.

7 Conclusion

In this paper, we reviewed the denial of service (DoS) attacks in secured IEEE 802.11, IEEE 802.1x. We proposed a Central Manager to dynamically manage APs and clients and avoid denial of service attacks. We analyzed 802.11 MAC protocol to show the effects of DoS attacks on the performance of Wireless LANs. We also demonstrated the correctness of our algorithms through simulations. Our solutions not only improve the security of WLANs, but also improve the performance of WLANs.

References

[1] V. Bharghavan, A. Demers, S. Shenker, and L. Zhang, "MACAW: A media access protocol for wireless LAN's," *ACM SIGCOMM*, pp. 212-225, Sept. 1994.

[2] N. Borisov, L. Goldberg, D. Wagner, "Intercepting mobile communications: The insecurity of 802.11," in *Proceedings, Seventh Annual International Conference on Mobile Computing and Networking*, pp. 180-188, July 2001.

[3] D. Y. Chen, and S. Garg, "Dependability enhancement for IEEE 802.11 wireless LAN with redundancy techniques," in *Proceedings of IEEE The International Conference on Dependable Systems and Networks*, pp. 521-530, San Francisco, CA, USA, June 2003.

[4] T. Dimitriou and D. Foteinakis, "Security and efficient In-Network processing for sensor networks," in *Proceedings of Workshop on Broadband Advanced Sensor Networks*, San Jose, CA, USA, Oct. 2004.

[5] W. L. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *Proceedings of INFOCOM 2004*, pp. 586-597, Hong Kong, China, Mar. 2004.

[6] W. L. Du, R. H. Wang, and P. Ning, "An efficient scheme for authenticating public keys in sensor networks," in *Proceedings of MOBIHOC 2005*, pp. 58-67, Urbana-Champaign, IL, USA, May 2005.

[7] V. Gupta, "Denial of service attacks at the MAC layer in wireless Ad hoc networks," in *Proceedings of MILCOM 2002*, vol. 2, pp. 1118-1123, Oct.7-10, 2002.

[8] P. Kyasanur and N. H. Vaidya, "Detection and handling of MAC layer misbehavior in wireless networks," in *Proceedings of IEEE The International Conference on Dependable Systems and Networks*, pp. 173-182, San Francisco, CA, USA, June 2003.

[9] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A defense against wormhole attacks in wireless networks," in *Proceeding of INFOCOM 2003*, pp. 1976-1986, San Francisco, CA, USA, Mar. 2003.

[10] *Protected EAP Protocol (PEAP)*, Microsoft, Feb. 2002, Internet - draft http://www.globecom.net/ietf/draft/draft-josefsson-pppext-eap-tls-eap-02.html

[11] RFC 2484, Mar. 1998, http://www.armware.dk/RFC/rfc/rfc2484.html

[12] A. Mishra and W. A. Arbaugh, *An Initial Security Analysis of the IEEE 802.1x Standard*, Feb. 2002, http://www.ieee802.org/1/files/public/docs2000 /ieee_plenary.PDF

[13] Y. Sun and K. J. R. Liu, "Scalable hierarchical access control in security group communications," in *Proceedings of INFOCOM 2004*, pp. 1296-1306, Hong Kong, China, Mar. 2004.

[14] The CMU Monarch Project, *The CMU Monarch Project's Wireless and Mobility Extensions to NS*.

[15] W. Y. Xu, W. Trappe, Y. Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of MOBIHOC 2005*, pp. 46-57, Urbana-Champaign, IL, USA, MAY 2005.

[16] Y. H. Zhou, D. P. Wu, and S. M. Nettles, "Analyzing and preventing MAC-layer denial of service attacks for stock 802.11 systems," in *Proceedngs of Workshop on Broadband Wireless Services and Applications 2004*, San Jose, CA, USA, Oct. 2004.

Ping Ding is a Ph.D candidate in computer engineering at Santa Clara University, CA, USA. She received her M.S. from China (P.R.C) in January, 1997. She worked as a research staff in Centre for Wavelets, Approximation & Information Processing (CWAIP) at National University of Singapore from October, 1998 to July, 2000. Before she started her Ph.D study, she worked as a senior software engineer in bay area, CA, USA. Her research interests includes security in WLAN and data dissemination on large-scale Ad-hoc and sensor networks.