Analysis of Denial of Service Attacks in IEEE 802.11s Wireless Mesh Networks

Divya* and Sanjeev Kumar**

Computer Science & Enginee
Punjab Engineering College,
Chandigarh. India
{divya,sanjeevsofat}@pec.edu.in

Abstract. Unlike wired networks, wireless networks do not have well-defined physical boundaries, which makes them prone to several security threats. As various wireless networks evolve into the next generation to provide better services, a key technology in the form of wireless mesh networks (WMNs) has emerged recently. Wireless Mesh Networks hold the promise of facilitating large-scale community networks in complex environments. There are number of issues in deploying WMNs, amongst others, security is a very serious issue. In these and other vital or security-sensitive deployments, keeping the network available for its intended use is essential. Without proper security mechanisms, networks will be confined to limited, controlled environments, negating much of the promise they hold. One of the major loop-holes in the security of WMNs is that management frames are not authenticated, and hence can be easily spoofed to cause DoS or Denial of Service attacks. We analyze the existing schemes and the proposed protocols to authenticate Disassociation and Deauthentication management frames. In this paper an original scheme is proposed that can be used to prevent DoS attacks over 802.11i security standard.

Keywords: Advanced Encryption Standard (AES), Wired Equivalent Privacy (WEP), 802.11i, WMNs, Denial of Service, 802.11w.

1 Introduction

Denial of Service (DoS) refers to a form of attack in computer systems over a network. DoS is normally a malicious attempt to render a networked system unusable (though often without permanently damaging it). Denial of Service (DoS) attacks prevents legitimate users from the use or management of a network asset. A denial of service attack may target a user, to prevent him from making outgoing connections on the network. A denial of service may also target an entire organization, to either prevent outgoing traffic or to prevent incoming traffic to certain network services, such as the organizations web page.

* Lecturer and Associate Coordinator, Cyber Security Research Centre.
** Professor and Coordinator, Cyber Security Research Centre.

D. Weerasinghe (Ed.): ISDF 2009, LNICST 41, pp. 1–10, 2010.

DoS attacks usually consist of frequency jamming whereby the attacker interferes with the whole of frequency band used in transmission of data by sending signals with more power at the same frequency. Also DoS attacks can be launched exploiting the manner in which channels are allocated to WLAN nodes wishing to transmit data. The attacker can cause the client device to think the channel is busy and defer sending data waiting for the channel to be idle. Furthermore, DoS attacks against a network can be launched by saturating a network devise with requests such that it cannot respond to legitimate traffic and therefore making the particular device unavailable to legitimate users. Denial of service attacks are much easier to accomplish than remotely gaining administrative access to a target system. Because of this, Denial of Service attacks have become very common on the Internet. Several security protocols have been proposed to prevent DoS attacks, most of which include modification of management frames in order for them to be authenticated.

1.1 Types of Dos Attacks

Probe Request Flood
Probe request frames are used by stations to actively scan an area in order to discover existing wireless networks. Any AP receiving a probe request frame must respond with a proper probe response frame that contains information about the network, to allow the station to associate. By sending a burst of probe request frames very quickly, each with a different MAC address (MAC spoofing) to simulate the presence of a large number of scanning stations in the area, the attacker can induce a heavy workload on the AP, resulting in a wastage of computing and memory resources which cannot be used for normal operations.

Denial of Service (DoS) Attack
In this attack, the intruder sends continually stream of different kinds of management frames to the WLAN. An attacker can spoof MAC address of a client and flood the WLAN with different kinds of forgery de-authentication, disassociation, association, or beacon management frames by using both directions of the communication. In this case, the WLAN overloads and will be unusable for even legitimate users.

Power Saving Attacks
The power conservation functions of 802.11 also prevent several identity-based vulnerabilities. To conserve energy, clients are allowed to enter a sleep state during which they are unable to transmit or receive. Before entering the sleep state, the client announces its intention so the access point can start buffering any inbound traffic for the node. Occasionally, the client awakens and polls the access point for any pending traffic. If there is any buffered data at this time, the access point delivers it and subsequently discards the contents of its buffer. By spoofing the polling message on behalf of the client, an attacker may cause the access point to discard the client's packets while it is asleep. Along the same vein, it is potentially possible to trick the client node in to thinking that there are no buffered packets as indicated in a periodically broadcast packet called the traffic indication map, or TIM. If the TIM message itself is spoofed, an attacker may convince a client that there is no pending data for it, and the client will immediately revert back to the sleep state. Finally, the power conservation mechanisms

rely on time synchronization between the access point and its clients so clients know when to awake. Key synchronization information, such as the period of TIM packets and a time-stamp broadcast by the access point, are sent unauthenticated and in the clear. By forging these management packets, an attacker can cause a client node to fall out of synch with the access point and fail to wake up at the appropriate times.

De-authentication attack

After an 802.11 client has selected an access point to use for communication, it must first authenticate itself to the AP before further communication may commence. Moreover, part of the authentication framework is a message that allows clients and access points to explicitly request de-authentication from one another. Unfortunately, this message itself is not authenticated using any keying material. Consequently, the attacker may spoof this message, either pretending to be the client or AP as shown in fig 1. In response, the AP or client will attempt to re-authenticate and any higher level time-outs or back-offs that may suppress the demand for communication. By repeating the attack persistently, a client may be kept from transmitting or receiving data indefinitely. One of the strengths of this attack is its great flexibility: an attacker may elect to deny access to individual clients, or even rate limit their access, in addition to simply denying service to the entire channel. However, accomplishing these goals efficiently requires the attacker to promiscuously monitor the channel and send deauthentication messages only when a new authentication has successfully taken place (indicated by the client's attempt to associate with the access point).

Disassociation Attack

A very similar vulnerability may be found in the association protocol that follows authentication. Since a client may be authenticated with multiple access points at

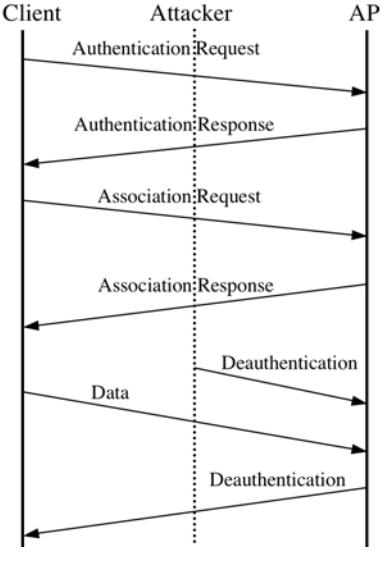

Fig. 1. De-authentication attack

once, the 802.11 standard provides a special association message to allow the client and access point to agree which access point shall have responsibility for forwarding packets to and from the wired network on the client's behalf. As with authentication, association frames are unauthenticated, and 802.11 provides a disassociation message similar to the deauthentication message described earlier. Exploiting this vulnerability is functionally identical to the deauthentication attack. However, it is worth noting that the disassociation attack is slightly less efficient than the deauthentication attack. This is because deauthentication forces the victim node to do more work to return to the associated state than disassociation, ultimately requiring less work on the part of the attacker. Association frames are unauthenticated and 802.11 provide a disassociation message similar to the de-authentication message [8, 9].

1.2 DoS Attacks in WMNs

One of the most severe threats on wireless mesh networks will be Denial of Service (DoS) attacks. The attack slows down the system and ceases the network from working properly. Unfortunately, there is no possible way to completely avoid this attack. This phenomenon takes place at link layer, as an attacker or invader can inject the frames with high network allocation vectors. The result of such an attack is that the nodes receiving the frames will stay idle till the duration indicated by network allocation vector (NAV). DoS can be avoided to some degree using some cryptographic mechanisms and surplus paths. Unauthorized access to the mesh nodes is yet another security concern in WMNs. The key concern is that at which level can the nodes participating in the communication be trusted? Generally, mesh nodes are protected with some secure text like password. There are many way to find out or retrieve passwords. What may happen if an attacker gains access to a mesh node by retrieving the secure text or password? The possibilities to make use of the network are multiple like, get access to the network or obtain the rights of a mesh node or Perform DoS by refusing to forward data or spreading false routing information or conducting Man in the Middle (MITM) attacks or applying message deletion and modification. An attack like Node spoofing also has the same penalty. A malicious node can pretend to be a regular member of the network. If an attacker succeeds in injecting such a node into the network, he may also gain access to other mesh nodes and can redirect the traffic over the corrupt node to obtain sensitive information about the network.

2 Analysis of Existing Security Models

2.1 Addition of IEs Inside Frame Body Fields

To authenticate Deauthentication and Disassociation frames, [11] proposes addition of two IEs – a crypto IE and a timestamp IE. The crypto IE is of 128 bits and filled with octets generated using MD5 hashing, RC4 or AES Cipher, while the timestamp IE is of 40 bits and prevents replay attacks. However, the limitations of this proposal are increased length, requirement for more computational resources and compatibility with only 802.11w networks.

2.2 Addition of 11 Bit Code by Replacing Bits of Frame Control and Sequence Control

This scheme, proposed in [10], consists of addition of 11 bits, randomly generated by using a key as a seed for a random number generator algorithm. The 11-bit code is split into 7 bits and 4 bits. The 7-bit code is inserted into the Frame Control field and the 4-bit code is inserted into the Sequence Control field. The bits of the Frame control field used are (i) To DS (ii) From DS (iii)More fragmentation (iv) Power Management (v)More data (vi)Protected frame (vii)Order.

The part of the Sequence control field used is the fragment number. This scheme is implemented by adding new functions to the NS-2 simulator. First, the standard 802.11 De-authentication and Disassociation procedures are added and after that the proposed scheme is implemented.

The proposed scheme can work since the problem is that of authentication of management frames and by deciding a code through which the access point and the station can authenticate each other, the problem is solved to some extent.

However, the drawbacks or weaknesses of the scheme are:

(i) Since a limited number of random numbers exist, i.e. 2^{11}, spoofing is possible.

(ii) The fields that have been deemed as unused may actually be of much use. In the frame control field, the To DS and from DS fields tell whether the station and the access point belong to the same BSS or different ones. The retry field instructs retransmission, the power management field indicates the power management mode and so on. Similarly, in the Sequence control field, the fragment number is important.

(iii) Since there is no private key exchange using a cryptographic algorithm, there is nothing to guarantee that the frame indeed has been sent by the station in question and has not been spoofed.

2.3 Proposed Draft as IEEE 802.11w

This scheme works for management frames in a way similar to the 802.11i standard for data frames. 802.11w will define the management frame protection scheme. Thus, the aim is to utilize existing security mechanisms rather than creating new ones or new Management frame format.

Protection-capable Management Frames are protected by the same cipher suite as an ordinary Data MPDU

- MPDU payload is TKIP or CCMP encrypted
- MPDU payload and header are TKIP or CCMP integrity protected

The MIC Key, the sender's MAC address, the receiver's MAC address and the frame are used to generate the Message Integrity Code (MIC), which is appended to the management frame. To prevent replay attacks, the IV (Initialization Vector) is used as part of the 802.11i header. The headers and the management frame body are authenticated by MIC, while the frame body and MIC are in encrypted format as shown in Fig 2.

As in the case of 802.11i, the cryptographic algorithm used is AES, which is a significant improvement over RC4 which is used in WEP. The use of TKIP ensures that the same encryption key is not used again. [12].

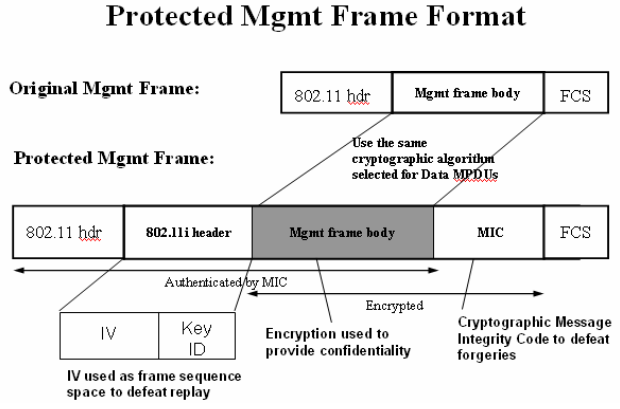

Fig. 2. Protected Management frame format in 802.11w

Since the scheme works for the authentication of normal data frames, and the same mechanism is applied to management frames, it is bound to work. MIC provides security against forgery attacks. The IV and the sequence counter prevent replay attacks.

However, just like in data frames, the problems for the implementation in case of management frames is the replacement of existing access points which are WEP compatible in order to be able to implement the more complex AES algorithm.

2.4 Other Related Work

Investigation of access point invulnerabilities to DoS attacks in 802.11 networks has been carried out in [16]. It describes possible denial of service attacks to infrastructure wireless 802.11 networks. To carry out such attacks only commodity hardware and software components are required. It identified some simple attack schemes that might lead to a **DoS** effect and observes the reactions of various types of infrastructure networks to these attacks. It identifies the message sequences that could lead to an attack towards an AP. The paper discusses probe request flood (PRF) , Authentication Request Flood (ARF), Association request flood (ASRF) and response by the AP to each of these attacks and how each of these attacks may bring the AP down to a level where all resources of AP are consumed to saturation level. It discussed the mechanism how to forge arbitrary 802.11 management frames and injecting them in the medium, regardless of protocol rules and constraints using Netgear MA401 PCMCIA card and Host AP driver and presented various attack statistics for different network configurations. The paper explains why the DoS effect does not appear when MAC spoofing is disabled. In the end it concluded that PRF, ARF and ASRF flooding attacks can be executed by any malicious station in the area of a wireless infrastructure network, without being neither associated nor authenticated to the access point and **AP's** main vulnerability to these flooding attacks seems to reside in unacknowledged frame retransmission, which causes memory buffers exhaustion and freezes AP functionalities

An analysis and cryptographic solution to two Denial of Service (DoS) attacks: Deauthentication flooding (DeauthF) and disassociation flooding (DisassF) attacks has been presented in [11].To authenticate deauthentication and disassociation

frames; it adds two IEs inside their frame body fields. One is the crypto IE, and the other is the timestamp IE. The crypto IE is used to hold crypto information for authenticating deauthentication and disassociation frames. Timestamp is used to prevent the replay attack. The crypto field has a fixed length of 128 bits, which is filled with octets generated by MD5 hashing, RC4 or AES cipher. The timestamp field has a length of 40 bits. It Implements 802.11w cryptographic mechanisms to protect deauthentication and disassociation frames using NS-2.But the limitation is that this proposed solution is only compatible with 802.11w networks. Other limitations of the protocol are increased length and requirement of more computation resources.

A three bit random bit authentication mechanism to protect 802.11 networks from DoS attacks has been proposed in [13]. Random bits are placed into unused fields of the management frames. AP and STA can then authenticate each other according to these authentication bits. The experimental results are shown are using Prism/2/2.5/3 802.11b PCMCIA cards and Host AP driver.

A model for Management Frames with Authentication and Integrity (MFIA) has been proposed in [15]. 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. However, issues with the protocol are increased size of frame and additional computation time.

Based on hash chains technique, a new authentication and key management scheme for WLAN has been proposed in [14], which achieves authenticating the main entity STA in the foremost time and negotiating and refreshing session keys efficiently. A hash chain is generated by multiple iterations of a secure hash function upon a secret seed and tip of the chain is used as a key. The scheme named fast WLAN authentication infrastructure (FWAI) includes five protocol flows or conversation messages between two stations.

Some implementation changes to mitigate the underlying vulnerabilities have been proposed in [17].The paper provides an experimental analysis of 802.11-specific attacks – their practicality, their efficacy. It discusses deauthentication, disassociation and power saving attacks and evaluates the practicality of implementing them and how well they perform in practice. The paper proposes a queuing mechanism to deal with deauthentication attacks, where it delays the effects of deauthentication or disassociation requests (e.g., by queuing such requests for 5-10 seconds) an AP has the opportunity to observe subsequent packets from the client. If a data packet arrives after a deauthentication or disassociation request is queued, that request is discarded – since a legitimate client would never generate packets in that order. However, our proposed solution is has certain drawbacks. It may lead to more severe DoS attacks. In particular; it opens up a new vulnerability at the moment in which mobile clients roam between access points. The association message is used to determine which AP should receive packets destined for the mobile client. In certain circumstances leaving the old association established for an additional period of time may prevent the

routing updates necessary to deliver packets through the new access point. Or, in the case of an adversary, the association could be kept open indefinitely by spoofing packets from the mobile client to the spoofed AP by keeping the association current.

A central Manager Solution to prevent Dissociation attacks has been proposed in [18].But the drawbacks of the solution is that it requires a single dedicated node to counter the attacks.

3 Proposed Scheme

The scheme that we have thought of is a modification of the *Scheme C* proposed. The *Scheme B* was ruled out for modifications because it used fields that may be of use, and adding an extra 11-bit code to the existing frame is a considerable over-head and would not provide much security.

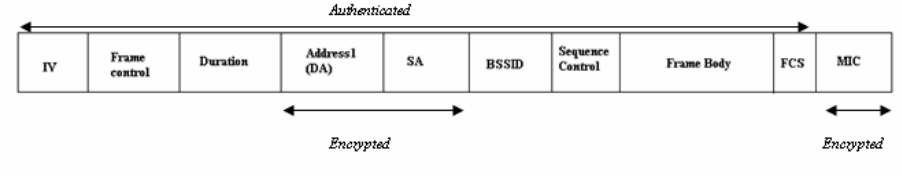

Fig. 3. Modified frame under proposed scheme

We propose that the de-authentication be performed in a way similar to the authentication in the case of 802.1X, i.e. Key in a pass phrase (master key) is used at both the client end and AP end. The pass phrases should match in case the key is correct. In addition to that, we propose that a MIC (Message Integrity Code) be added to the frame, but in order to simplify process involved, entire management frame body need not be encrypted (unlike 802.11i in which the entire data frame body is encrypted). The encryption is to be carried out using AES algorithm. We propose that management frames need not be completely protected unlike as proposed in the draft standard 802.11w as encrypting the entire header adds to overheads reducing the capacity of the mesh network.

3.1 Advantage over the Proposed Draft

To establish a connection with a legitimate station concerned only the MAC addresses needs to be secured. It is therefore sufficient to encrypt only the source and destination address fields in the frame. This makes the process less time-consuming and more efficient. We propose that management frames need not be completely protected unlike as proposed in the draft standard 802.11w. For the disassociation and de-authentication frames to be authenticated, the fields that need to be protected are the MAC addresses. The MAC addresses carry the information about the source and the destination. By spoofing the MAC address of a different station to send information can lead to de-authentication and disassociation attacks.

3.2 Shortfalls of 802.11w

As soon as IEEE 802.11w gets ratified it will become widely accepted and will offer better security to the users. However the standard will still not be able to mitigate the DoS attacks. DoS attacks can be mitigated through strong systems practices but DoS attacks against wireless networks can still not be stopped. The following attacks will still be prevalent on Wireless Mesh Networks:

- Net Allocation Vector(NAV) DoS:
  802.11w does not provide protection against attacks based on control frames. An attacker can manipulate the Network Allocation Vector (NAV) using RTS/CTS frames to force other stations to back-off, preventing them from transmitting on the network.
- Exposed Node Problem:
  Using RTS/CTS problem does provide solution in case of hidden node problem. However there is no solution for exposed node problem.
- Beacon invalid channel DoS:
  Many wireless cards will follow whatever channel is specified in spoofed beacon frames, allowing an attacker to manipulate the station into switching to channel "0", for example.
- EAPOL Start DoS & Logoff DoS:
  In an EAPOL Start DoS, an attacker rapidly hides the AP and RADIUS server with EAP Start requests. This can cause an AP to exhaust all memory and reboot, and it can cause severe performance degradation on the RADIUS server. In EAPOL logoff attack, the adversary sends EAP Logoff messages to a target station, impersonating the RADIUS server/AP. The station disconnects, and the user loses connectivity.
- PEAP Account Lockout:
  Since PEAP networks transmit the username information in plaintext, an attacker can capture valid PEAP usernames and attempt to login as that user with randomly selected passwords. This will often trigger account lockout policies from multiple failed authentication attempts, resulting in DoS for the end-user.

4 Conclusion

The draft standard 802.11w solves the problem of unprotected management frames to quite some extent with the use of MIC and IV along with sequence counter. However, protecting the entire header adds to considerable overheads. In this paper we have proposed a modified scheme which utilizes the advantages offered by the draft standard 802.11w and also makes the process less time-consuming and hence more efficient. It is evident from this study that many of the DoS attacks can still not be prevented by the new standards and the impact of such an attack is significant as it can be achieved using only commodity based hardware and software. Further such attacks can be executed with minimal chance of detection and localization. These concerns are most pronounced in network environments that rely on the correct behavior of participating nodes for continued operation. There is a dire need to develop adequate

strategies to mitigate the significant threat of denial of service in current IEEE 802.11s WMN technology, the application of this technology should be precluded from use in safety-critical environments which may typically have stringent availability requirements.

References

1. IEEE 802.11 Architecture, http://www.tutorial-reports.com/wireless/wlanwifi/wifi_architecture.php
2. Fogie, S.: Maximum Wireless Security by Cyrus PeiKari. Sams Publishing, ISBN:0-672-32488-1
3. Wang, Y.: A Tutorial of 802.11 Implementation in NS-2
4. Zhang, H., Zhu, Y.: A New Authentication and Key Managemtn Scheme of WLAN
5. Ergen, M.: University of California Berkley, IEEE 802.11 Tutorial (June 2002)
6. Gast, M.: 802.11 Wireless Networks. O'Reilly & Associates, Inc., Sebastopol (2002)
7. Miller, S.S.: Wi-Fi Security. Tata McGraw Hill Publication, New York
8. Liu, C., Yu, J.T.: An Analysis of DoS Attacks on Wireless LAN. In: IASTED International Conferences on Wireless Networks and Emerging Technologies (WNET 2006), Banff Canada (2006)
9. Liu, C., Yu, J.T.: A Solution to Wireless LAN Authentication and Association DoS Attacks. In: Second International Conference on Computer Science and Engineering (JIC-CSE 2006) (December 2006)
10. A Protocol to defend Against Deauthentication and Disassociation Attacks, A Dissertation submitted to PEC (Deemed University) for Masters of Engineering in Computer Science and Engineering (2008)
11. Liu, C., Yu, J.: Rogue Access Point Based DoS Attacks against 802.11 WLANs. In: Fourth Advanced International Conference on Telecommunications
12. Qi, E.H., Walker, J.: Management frame protection. Intel Corporation (2005)
13. Lee, Y.-S., Chien, H.-T., Tsai, W.-N.: Using Random Bit Authentication to Defend IEEE 802.11 DoS Attacks
14. Zhang, H., Zhu, Y.: A New Authentication and Key Management Scheme of WLAN
15. Malekzadeh, M., Ghani, A.A.A., Zulkarnain, Z.A., Muda, Z.: Security Improvement for Management Frames in IEEE 802.11 Wireless Networks. IJCSNS International Journal of Computer Science and Network Security 7(6) (June 2007)
16. Ferreri, F., Bernaschi, M., Valcamonici, L.: Access points vulnerabilities to DoS attacks in 802.11 networks. In: WCNC 2004. IEEE Communications Society, Los Alamitos (2004)
17. Bellardo, J., Savage, S.: 802.11 Denial-of-Service Attacks. Real Vulnerabilities and Practical Solutions. In: Proceedings of the 12th USENIX Security Symposium, Washington, D.C, August 4-8 (2003)
18. Ding, P., Holliday, J., Celik, A.: Improving the Security of Wireless LANs by Managing 802.1X Disassociation. In: Proceedings of the IEEE Consumer Communications and Networking Conference, Las Vegas, NV, January 2004, pp. 53–58 (2004)