Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks

Rupinder Cheema
Department of Computer Science and Engineering,
PEC University of Technology
Chandigarh, India

Divya Bansal
Department of Computer Science and Engineering,
PEC University of Technology
Chandigarh, India

Dr. Sanjeev Sofat
Department of Computer Science and Engineering,
PEC University of Technology
Chandigarh, India

ABSTRACT
Wireless Mesh Networks have emerged as a widely deployed, new paradigm with improved performance and reliability. Mesh Networks offer ubiquitous network connectivity along with better flexibility and adaptability features. Despite of these benefits, Wireless Mesh Networks are vulnerable to attacks due to the absence of trusted central authority and the unprotected nature of the management frames. This security breach leads to the spoofing of legitimate client's information. Thus facilitating the launch of dos attacks on the behalf of the legitimate identity holders .The influence of DOS attacks is highly intense, because complete network resources have been consumed by the attacker after launch of the attack. Consequently, it leads to deterioration of network performance thus halting the communication. Therefore, security is a major concern that needs to be dealt with to alleviate the effect of these attacks . So that the deterioration and disruption caused by these attacks to the network performance has been thwarted. In this paper we have implemented the dos attacks on the real wireless mesh test bed and analyzed their impact on the network performance and proposed a security algorithm for the detection of these attacks.

General Terms
Wireless mesh networks, DOS attacks, Deauthentication flooding attack, Disassociation flooding attack Spoofing, Security.

Keywords
Management frames, MAC address, Threshold value, Detection of dos attacks.

1. INTRODUCTION
The use of Wireless Networks have been increased at the tremendous rate because of the various functionalities offered by the wireless networks irrespective of their wired counterparts [22]. Wireless networks owe the following features such as scalability, low cost, mobility, low data error rates etc [25]. They are not bound by the perimeter and do not require any physical connection. Moreover reconfiguration according to the needs of the enterprise is easy in case of wireless networks. But along with all these benefits come the threats and weaknesses that makes them easy to be compromised [1]. As in case of Wireless Networks the communication is over radio waves so signals are transmitted over air. These signals can be received by the sender and the receiver in the vicinity of the sender by the use of antennas. So these signals may be heard by the attackers too. Thus attacker may spoofs the data and masquerades it leading to the launch of different attacks to which the wireless networks are vulnerable [2]. In case of Wired Networks as the communication requires the establishment of the physical connection between the sender and the receiver so authenticity is ensured [22]. But in case of Wireless Networks this authenticity has been checked explicitly by using the authentication mechanisms such as open system authentication or shared key authentication. Moreover only Access point has got the flexibility to authenticate client, thus validating client's identity. But there is no provision for the client to validate the genuineness of the Access point. This has opened the doors for the launch of the fake AP or rouge AP attacks [4]. A Wireless Mesh Network is a communication network made up of radio nodes organized in a mesh topology. Wireless Mesh Networks often consists of mesh clients, mesh routers and gateways [18]. Fig 1 shows the basic architecture of the Wireless Mesh Networks. Mesh stations can collocate with MAPs for getting access over the network resources. The MAC layer of IEEE 802.11s draft standard (Wireless mesh networks) is consistent with the already existing IEEE 802.11 networks along with some added functionalities such as multihop, forwarding property. WMNs are distributive by nature as there is no need for each MAP to connect to the external network. Only one MAP referred to as Mesh Portal has been connected to the external network and the other Mesh points and MAPs can communicate with that via that Portal only [24]. Mesh points possess forwarding property and by virtue of this, each MP and MAP can forward data to and fro between these nodes. Stations do not retain this property and can get the network access via the MAPs [3]. Moreover Mesh Networks offer better network performance as compared to their already existing counterparts. As in case of 802.11s networks the MPs and MAPs can communicate by the virtue of IEEE802.11a and the communication between the MAPs and stations is via IEEE 802.11b so these two actions will not intervene and may takes place simultaneously [24]. Because of its architecture IEEE 802.11s draft standard has been providing end users with better experiences, more achievable bandwidth, fewer cost, and more fairness than 802.11 standards do [17].

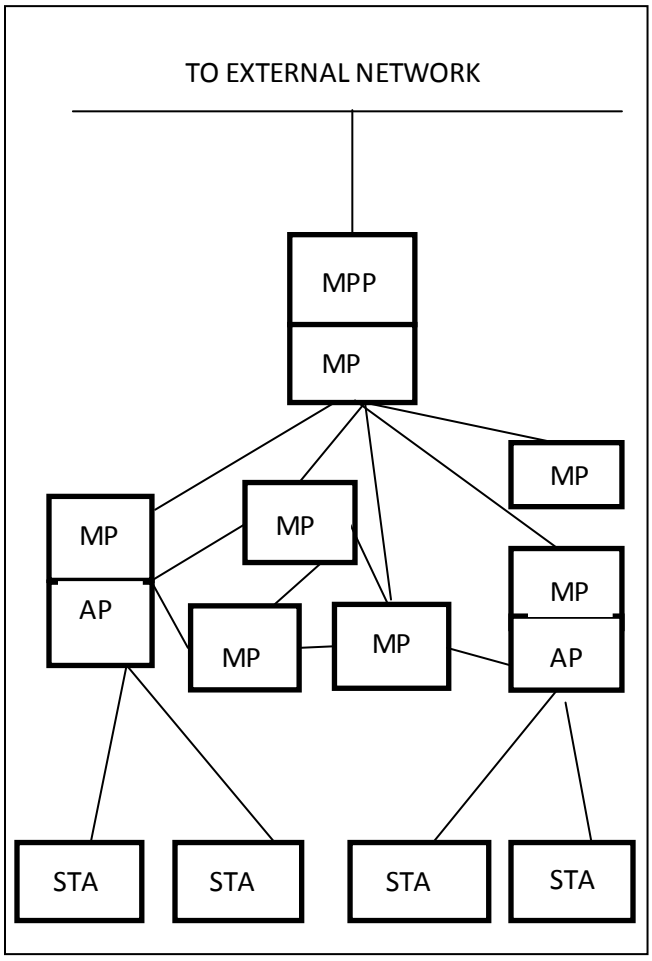

Fig 1: Network Architecture of WMN

2. LOOPHOLES IN SECURITY

In Wireless LANs the vulnerabilities are of two types, they are due to poor configuration methods and due to poor encryption methods. The reason behind most of the vulnerabilities is the use of poor configuration methods such as the easy deployment of WLANs with inadequate configuration security [5]. A default configuration for WLANs make an attacker to penetrate into the network easily. Access to the network can be gained easily by configuring the WLAN adapters [2]. The second class of vulnerabilities occur due to poor encryption methods used like WEP, that basically consists of the master key to be concatenated with 24 bit IV. This leads to the generation of 2^{24} unique keys that can be compromised in few minutes and may facilitate many attacks like FMS attack [15]. Then new standard 802.11i have been introduced which relies upon 802.1X server for authentication. This requires only firmware upgradation and works with same hardware as the IEEE 802.11 standard. Key generation process has been complicated by the introduction of key mixing function and various levels for the generation of keys such aas PMK, PTK etc. This has reduced the exposure of the master key but still it can be compromised [21]. Then comes the more secure solution referred to as RSN (robust security network) proposed by the task group 802.11i which is the most secured one and very difficult to be compromised. In this RC4 algorithm which was used earlier for encryption has been replaced by the AES counter mode algorithm. This speeds up the key generation process because keys have been generated prior to the arrival of message. In this case the generated key stream is independent of the message . WMNs derive security from IEEE 802.11i standard proposed by the task group also referred to as RSN (robust security network). They rely on WPA2 the most advanced protocol based on AES algorithm for providing security. In this standard the security and authenticity between the clients and MAPs has been established by the authentication server i.e. RADIUS server by several protocols like PEAP, EAP, LEAP. But still all these security mechanisms are viable for securing the data frames only .[16] The management frames are still sent in clear and are unencrypted. So this facilitates the launch of several dos attacks [4]. The attacker has been obfuscating his presence by setting legitimate client's address as source address. Thus leading to the flooding of the network with these attacking frames. Hence, causing deterioration of the network resources and thus halting the communication [17].

3. DENIAL OF SERVICE ATTACKS

Denial of Service attacks aim at overwhelming the network with huge amount of illegitimate data thus depriving legitimate clients of using the resources. Although the means to carry out, motives for, and targets of a DOS attack may vary, it generally consists of the concerted efforts of a person or people to prevent a service from functioning efficiently or at all, temporarily or indefinitely [23]. In the context of Wireless Networks, whole bandwidth has been consumed by the illegitimate traffic produced by the attacker, as an impact of the launch of dos attacks, thus prohibiting the legitimate clients to be served [26]. Denial-of-service attacks have an impressive history for instance blocked out websites like Amazon, CNN, Yahoo and eBay. The attack has been initiated by sending excessive demands to the victim's computer(s),exceeding the limit that the victim's server can support and making the server crash [2]. Sometimes, many computers has been entrenched in this process by installing a Trojan on them; taking control of them and then making them send numerous demands to the targeted computer. On the other side, the victim of such an attack may see many such demands (sometimes even numbering tens of thousands) coming from computers from around the world[1] Wireless communications that use shared RF waves as a medium of communication are vulnerable to DOS attacks. DOS attacks may be launched at all the layers of the TCP/IP reference model. These attacks may be triggered intentionally by an attacker or unintentionally by other devices causing interference because they too are based on radio communication [19]. Fig.2 shows classification of DOS attacks at different layers [16]. At the first layer known as the Physical layer, Jamming attack may be launched which reduces the throughput of the network to unacceptable levels. Interference caused by other radio transmitters in the radio range too thrashes the network performance [23]. At the second level attacks occur at the data link layer or the MAC layer due to the security breaches in this layer that may be exploited very easily. As the communication is via shared medium, so once the attacker gains the access to this medium, threats have been posed to all the users [26]. At the next layer comes the layer 3 and layer 4 levels and at these levels several attacks such as Ping of Death, Smurf

Attack, SYN Flooding attack may be launched. Thus flooding the network and leading to the disruption of the network performance. At the last level the attacker exploits the weakness at the application layer protocol thereby facilitating the launch of DNS Poisoning attack. Viruses or worms have been sent by the attacker posing detrimental effects to the network [16].

Application level DOS attacks
DOS at internetwork level
Protocol/media access level DOS
Physical layer attacks

Fig 2: DOS attacks classification

4. MAC LAYER ATTACKS

In IEEE 802.11 or IEEE 802.11s standard based networks, an attacker can transmit packets using a spoofed source MAC address of an Access point or Mesh access point [4]. The recipient of these spoofed frames has no way of telling if they are legitimate or illegitimate requests and has to respond instantly. The ability to transmit spoofed management frames allows the launch of MAC layer DOS attacks [13]. These attacks can be launched easily by the readily available tools such as AirJack [9], Airsnarf [10], KisMAC [11]. The vulnerabilities at the MAC layer can be categorized in two different types, they are:-

- Identity Vulnerabilities.
- Media Access Vulnerabilities.

4.1 Identity Vulnerabilities

The rise of identity vulnerabilities is due to the MAC address of the network. As MAC address consists of 12 byte address, the field of the MAC frame stores both the sender's and the receiver's address [4]. In WLAN, for class one frames no mechanism has been developed for the verification. Thus the attacker has been spoofing the MAC address which leads to several distinct vulnerabilities[2].

4.2 Media Access Vulnerabilities

Media access vulnerabilities can be performed by the attacker blocking the access to the medium [13]. It can be blocked by using the combination of collision domains like physical carrier sense and virtual carrier sense mechanisms. The attacks which can be launched by this blocking, includes time window attack and virtual carrier sense attack [2].

Identity vulnerabilities causes three types of attacks, they are as follows:-

- Deauthentication Attack.
- Disassociation Attack.
- Beacon Spoofing Attack.

4.1.1 Deauthentication Attack

The connection between the Mesh clients and Mesh APs has been be established by the exchange of various frames as shown in Fig 3. The communication between the mesh client and the mesh AP has been established after probing the available wireless APs. After that the exchange of the series of management frames like authentication and association request frame takes place [2] . Then the mesh AP responds by sending authentication response and association response via the authentication server (Radius server) [17].

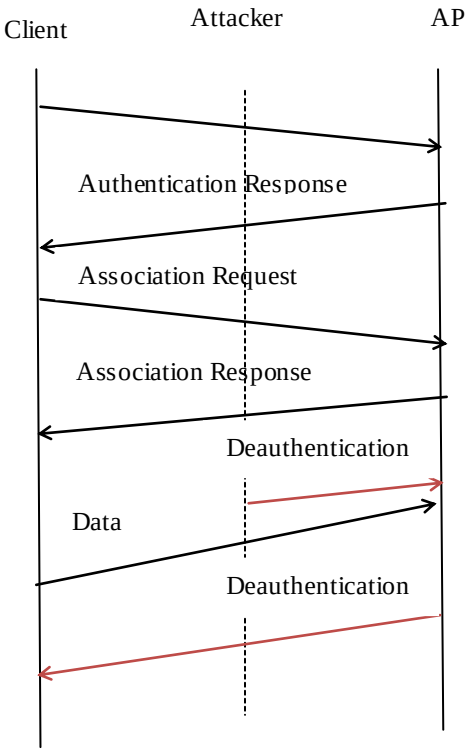

Fig. 3 Deauthentication Attack

As these frames are unprotected and sent in clear. So these frames has been spoofed by the attacker [4]. The attacker then sends deauthentication requests with the client's address set as the source. Then the mesh AP responds by sending the deauthentication response to the client. Thus the communication between the client and the AP has been halted [13]. As deauthentication requests are notifications, so cannot be ignored and the AP responds instantly to these requests [2]. The attacker can periodically scan all the channels and send these spoofed messages to valid clients thus terminating their connection [19].

4.1.2 Disassociation Attack

A client can be authenticated to more than one Mesh APs, but has been associated to only one AP at once [6]. Fig 4 shows the frames exchanged between the client and the AP for the launch of the disassociation attack. The client sends association request to the selected AP and this communication too may be spoofed by the attacker. Then the client sends disassociation request to the AP with source address set to client's address, as these too are notifications and cannot be ignored . So the Mesh AP instantly responds by sending the disassociation response frame.

Thus halting the communication between the Mesh AP and the client, but the client has been still authenticated to the previously associated network. The client may reassociate after the attack by sending solely the reassociation request. As reconnection requires less time in this case, so this attack is less severe than the deauthentication attack [2].

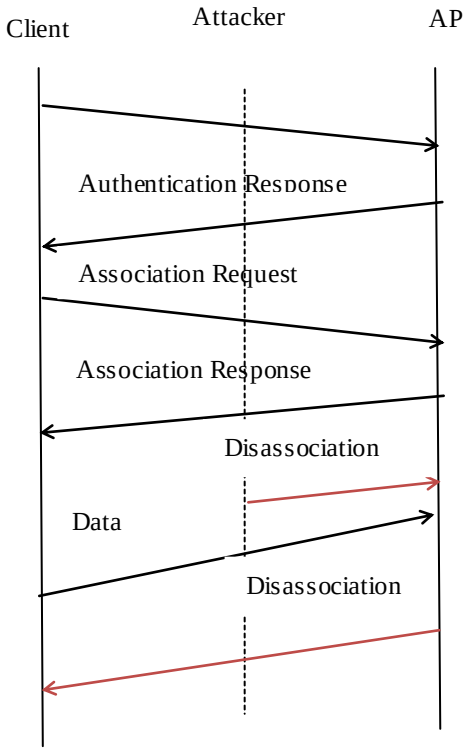

Fig. 4 Disassociation Attack

4.3 Beacon Spoofing Attack

Beacons are the notifications sent at regular intervals by the AP for synchronization [5]. These beacons frames are too a category of management frames and thus not protected and sent in clear. So they too may be spoofed and masqueraded by the attacker machine, thereby leading to the launch of Rouge AP attack and flooding attack. This too may flood the network with a large number of illegitimate beacons along with the limited number of legitimate beacons. Consequently, leading to congestion in the network and deterioration of performance of the network [7].

5. RELATED WORK

Dos attacks such as Deauthentication and Disassociation have been implemented in the Wireless networks using the tools viz KISMET and AIRCRACK. The contribution of various authors in this area is illustrated here. John and Stefan [2]"802.11 Denial of service attacks: real vulnerabilities and practical solutions", 2003, provided a description of the vulnerabilities in the 802.11 management and media access services that were vulnerable to attacks. It was focused that all such attacks were possible by circumventing the normal operation of firmware in commodity 802.11 devices. Moreover two important classes of DOS attacks were implemented and the range of their practical effectiveness was investigated. It focused on various tools implemented in firmware for injecting raw 802.11 frames into the channel. In this paper the focus was mainly on attacks on 802.11 MAC protocol rather than pure resource consumption. The main functionalities associated with MAC layer which resulted in the vulnerabilities includes the ability to discover networks , join networks and leave networks , and coordinate access to the radio medium [22]. The problem that leads to the identity vulnerabilities was, the non-verifiability of the source and destination address contained in the MAC management frames, which could be easily spoofed by the attacker. Then attacker could have intervened the communication and acted as client so that the AP responded to the requests sent by the attacker as if they were sent by the client itself thus dos attacks were have been facilitated [13]. When AP was selected by the client after the probe request and probe response, then the next step was for the client to authenticate it with that AP. For that an authentication request message was sent by the AP to the client and client responded based on the mechanism used for authentication OSA (open system authentication) or SKA (shared key authentication) [1]. The part of that message exchanged between the client and the AP was not authenticated by any of the keyed mechanisms, so that can be spoofed and redirected by the attacker. As deauthentication /disassociation frames are notifications and thus cannot be ignored so the client has been deauthenticated/disassociated on receiving these frames as the network has been flooded with large number of these frames. As a consequence connection has been reset or terminated depending on the number of frames [6]. These attacks were implemented in 802.11 networks and their impact on network performance was analyzed. Security is a major concern in case of the Wireless mesh networks that needs to be dealt with. Although several authors have given their contributions in this area for implanting security in Wireless networks they will not work for Wireless mesh networks because of the distributive nature of these networks.Sans Institute have proposed scripts for the detection of the deauthentication/disassociation attack [20]. In this they have used the idea that, the deauthentication/disassociation frames may be sent by the client too if the client wishes to deauthenticate or disassociate from the AP , The reason may be decrease in the signal strength associated with the already associated AP. If it falls below some specified value then the client may start probing other networks over same channel or different channels. And after selecting the appropriate AP the client may associate with the new AP. For this client needs to disassociate from the already associated network, as the client may associate with only one AP at a time. So in the scripts proposed by them they have firstly identified the frame type .Then they have specified a threshold value for the number of deauthentication or disassociation frames which they considered as normal. If the intensity that is the number of frames received at a particular instant falls beyond this threshold then it have been identified as the attack. And it was launched to flood the network thus leading to congestion. Then in the final step MAC address of the source of the attack was harvested [4]. This MAC address could be of the legitimate client, as all the attacks have been launched after spoofing the MAC address of the legitimate clients. So spoofing detection has been identified as the inevitable area for the detection and prevention of dos attacks [8]. Fanglu – guo and Tzi-cker Chiueh proposed sequence number based spoof detection algorithm for the detection of

MAC address spoofing in case of 802.11 networks [8]. As sequence number is a field in the 802.11 frames, every frame has associated with it a unique sequence number, that grows incrementally with frames sent out. So the author considered this specification to check if the frame is spoofed one. Wright [4] also proposed sequence numbers to detect spoofing. The approach specified by him was simple and relied upon SN gap i.e. the difference between two successive frames SN and it was compared with a threshold value and if the gap falls beyond this alert was raised but this generated too many false positives. Instead of a threshold-based approach, Dasgupta [12] used a fuzzy decision system to detect MAC address spoofing. They first collected the sequence number traces in which spoofing attacks were active to train the fuzzy system. After training, they validated the effectiveness of their system by applying it to detect new spoofing attacks. This approach aims to detect sequence number anomaly. By using fuzzy logic the false positives generated by the duplicate frames and lost frames were reduced. Rather than a sequence number-based approach, Bellardo [2] used the heuristic that if a STA sends additional frames after deauthentication/disassociation frame was observed, the deauthentication/disassociation frame must be spoofed one. However, this heuristic was able to detect only spoofed deauthentication/disassociation frames, but not other types of spoofed frames such as power-saving, data, etc. Cardenas [13] suggested RARP based approach in which suspected MAC addresses were analyzed and if multiple IPs were generated in correspond to a particular MAC then it could be detected as the spoofed one. But as multiple IPs may be assigned to a single NIC so this scheme won't prove successful. And moreover the attacker must firstly spoof the IP address before launching the attack. So the IP harvested corresponding to the MAC could be of legitimate client. Finally, Hall [14] proposed a hardware based approach for spoofing detection and for that a Trans receiver switch needs to be embedded in hardware that won't allow for the attacker to forge the characteristics viz MAC. Though the success rate achieved with this was 94-100% but the deployment of this hardware circuitry with all the NICs was practically infeasible. Wi-Fi Protected Access (WPA) [15] With the introduction of WPA the Wireless LAN security was improved. WPA that is TKIP based and enhanced the security by introducing the key mixing functions that added up to the security provided by the earlier secure protocol WEP. Then next came the most secured one WPA2 based on the AES algorithm and used in case of Wireless Mesh Networks for maintaining security. These protocols proved to be useful for securing data frames only and the management frames have not been benefitted. So management frames are susceptible to various attacks. In this paper we have launched the attacks on the real Wireless mesh test bed and analyzed their impact on the network performance. Moreover we have proposed a novel security algorithm for the detection of these dos attacks to alleviate their adverse effects.

6. IMPLEMENTATION OF DISASSOCIATION/ DEAUTHENTICATION ATTACK

Disassociation and deauthentication attack has been launched by sending the deauthentication packets only to the AP or the client depending upon the initiator for sending the frames. Fig. 5 shows that initially the client is neither associated nor authenticated to any network. And then via the exchange of management frames, authentication request frame and on the reception of the response frame the client's identity has been validated with the network. It may be feasible that at a particular instance of time a client has been authenticated to more than one networks but it can be associated to only one network at a time. In the third step the client has been associated after the exchange of association request and response frames.

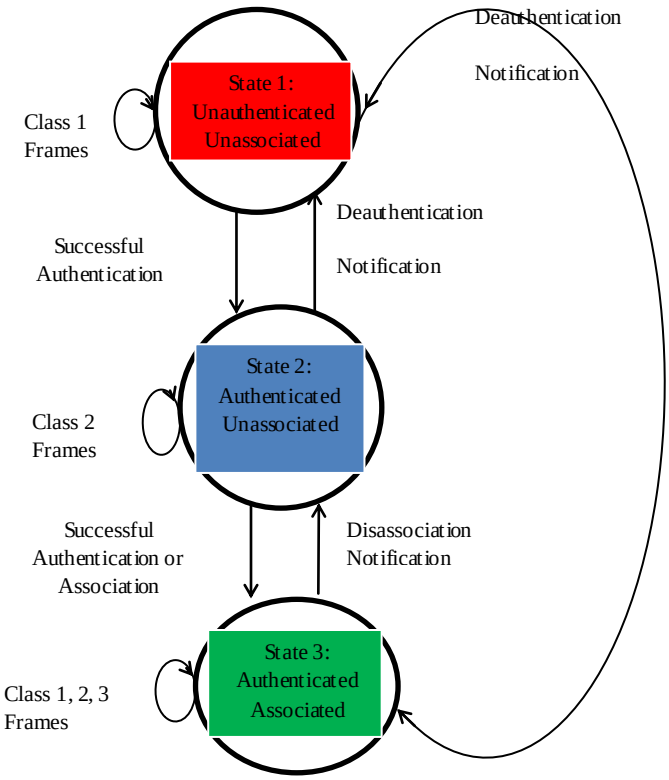

Fig 5 State Diagram of Management Frames

Deauthentication is a two-step process:-

1. Firstly the client or AP has been disassociated from the other party but still remains authenticated to it with limited or no connectivity as a consequence of the attack.

2. In the second step it has been deauthenticated and after that Mesh client's identity is not validated to the mesh AP.

And for reassociation whole process such as authentication followed by the association needs to be repeated again after the attack in case of the deauthentication attack. In case of disassociation attack, for reassociation the client needs to reassociate only to reestablish the connection over the wireless channel. Thus disassociation attack is less severe and may be launched by fewer packets and deauthentication can be launched by increasing the number of packets. As a consequence there has been degradation in the throughput and bandwidth corresponding to the launch of the attack.

7. NETWORK SCENARIO USED

The test bed comprised of one server station, one client station connected to Wireless mesh network AP, the AP connected to same wired network as the server system and an attacker machine capable of running attacking tools. The attack has been launched via the attacker machine after spoofing the details of the available networks and thus launching the attack on the behalf of the legitimate AP, hence masquerading the details. As these requests are the notifications, so cannot be ignored. Thus client has been disassociated/deauthenticated from the network to which it has been already connected. Thus leading to the congestion in the network by flooding and hence deterioration of the resources like throughput, bandwidth etc. Network performance can be measured by using the parameters like throughput, bandwidth, jitter, bandwidth. We have considered two parameters throughput and bandwidth for analyzing the performance of our Wireless mesh test bed before and after the launch of the attack.

Throughput

Throughput is defined as the number of data packets sent by a sender and received by a receiver in a grant time . It is the average rate at which data is successfully delivered over the wireless channel. Thus the performance of a network depends on throughput, as we need each data packet to be transmitted successfully. A high throughput is the most important goal of a WMN. There are two ways to improve the throughput performance. One is to use less time when transmitting every unit data between source node and destination node. The other one is to transfer more data bits within a unit transmission time. Owing to the noisy nature of the Wireless channel, errors are introduced into the received packets which means that corrupted packets have to be re-transmitted. Re-transmitting the packet increases the time required to deliver the data and hence reduces the throughput.

Bandwidth

It refers to the data rate supported by the network connection or interface. Bandwidth is defined as the capacity of the network connection. The greater the capacity, the more likely that better performance will follow.

7.1 Dissassociation attack launch

Fig 6 shows the outcome of the attack launch over the network performance measurement parameter throughput and Fig 7 shows its influence over the bandwidth. The network performance of our test bed has been measured in terms of throughput and bandwidth. It seems to be normal before the attack. But after the launch of the attack till the time the attack lasts, the network parameters such as throughput as well as bandwidth starts decreasing and then reaches zero. As in case of disassociation attack, the client has been authenticated to the same network but with limited or no network connectivity, as a consequence of the attack launch. It may reassociate afterwards by sending the reassociation request explicitly.

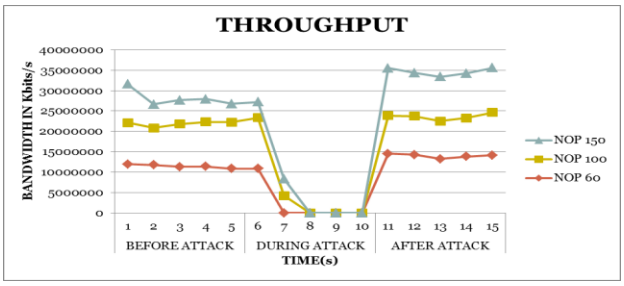

Fig. 6 Impact of the disassociation attack over bandwidth

During the attack, client has not been able to reassociate as the network is congested by the disassociation messages. Thus network has not been left with the flexibility to serve any one. After the lapse of this interval the Mesh client may again reassociate by sending solely the reasssociation request. The network performance again started improving as throughput as well as bandwidth has been increasing . This attack is less severe as it has been launched with lesser number of packets, so its span is also less . Thus its easy for the network to recover network parameters after this attack.

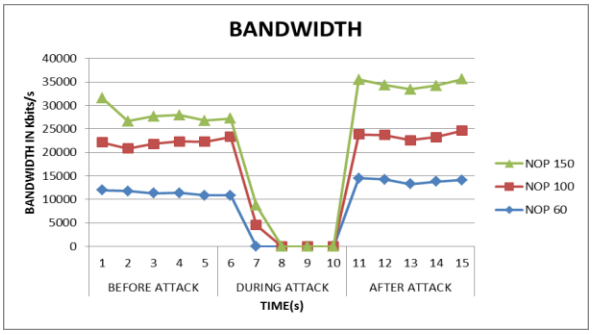

Fig 7 Impact of the disassociation attack over bandwidth

7.2 Deauthentication attack launch

Fig 8 shows the impact of the deauthentication attack launch over the network performance which has been measured in terms of throughput. Fig 9 shows its impact over the bandwidth. The deauthentication attack has been launched by increasing the number of packets. This is due to the reason that the impact of this attack over network performance is worst. As after the launch of this attack, the mesh client has no longer been authenticated to the mesh AP with which it has been associated. During the attack the client, has been deauthenticated and thus may probe other networks and connect to any other mesh AP available in the range with good signal strength. Moreover, the tenure of this attack is very high, as it's a two-step process. Thus the client may rejoin by sending authentication request followed by the association request explicitly, but the network performance for that mesh AP has been deteriorated considerably. So it takes time for the network to recover from the loss in its performance even after the attack.

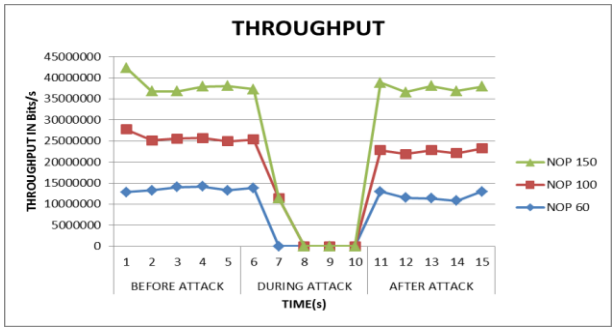

Fig. 8 Impact of the deauthentication attack over throughput

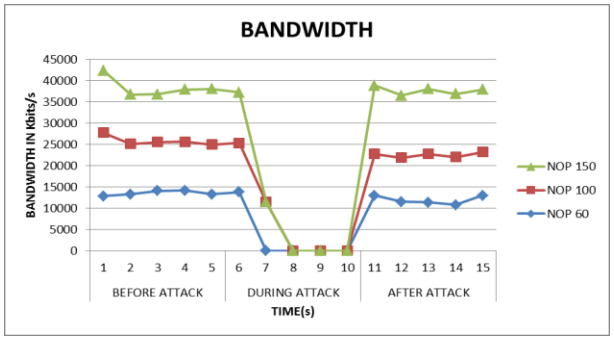

Fig. 9 Impact of the deauthentication attack over bandwidth

7.3 NEW DETECTION ALGORITHMS

In the earlier proposed algorithm based on scripts, the authors have compared the number of deauth/disas frames at any instance recorded in the time variable with the threshold value. And if the number of received frame falls beyond the specified threshold it have been notified as attack. But there were, the chances of generation of too many false positives in this case. As in case of congestion, there may be slight delay in the reception of the frames. Moreover, it might be possible that frames supposed to be delivered at a particular instant, suppose time t1 has been delivered at time t2 and at that instant we have received the frames for this instant t2 along with those of previous instant t1. So it added up to the number of total frames received at a particular time interval. And may falls beyond threshold, so has been notified as an attack when it was actually not.

Moreover in case, if the attack has actually been occurred, the MAC address harvested was of the legitimate AP. As the attack have been launched by the attacker after spoofing the identity of the legitimate client. Moreover, no provision have been available with the AP to discriminate whether the frames are legitimate or spoofed ones. So we have proposed the new algorithm for the detection of deauthentication/disassociation flooding attack. This algorithm overcome the short comings of the previous algorithm, so it has reduced the generation of false positives. Moreover we have imbibed the spoofing detection function too in our algorithm. So in case of deauthentication flooding attack it has helped us to find out whether the attack has been launched by the legitimate client or by the attacker after spoofing legitimate client's MAC address.

7.3.1 Algorithm For Detection of Deauth / Disass Attack

1. Start monitoring the interface.

2. Initialize the variables such as the $\mathbf{C_{deauth}}$ counters for recording deauth flood and $\mathbf{C_{attack\ ocuurences}}$ counter for recording the number of attack occurrences and set these to zero value.

3. Record the value of the starting time say $\mathbf{time_{cur}}$ in a variable named Start.

4. Start sniffing the interface for monitoring packets.

5. Initialize the variables for specifying the values of thresholds specified for deauth flooding as $\mathbf{Thresh_{flood}}$= 25/5 which is computed by dividing the value by the time span for which we have analyzed the frames .The value of the analyzed time interval is stored in $\mathbf{Value_{init}}$ = 5 and the value of threshold for notifying attack is stored in variable $\mathbf{Thresh_{attack}}$= 3 6. Check frame type and subtype and if the value of type is 0 and sub type comes out to be 12 then the frame would be identified as the deauthentication frame.

7. Calculate Δ that is the difference between the current time $\mathbf{time_{cur}}$ and the value of timer stored earlier in variable Start.

a) If delta is greater than the value of reporting interval $\mathbf{Value_{init}}$ and the value of dividing the count of deauthentication frames received by difference time $\mathbf{(C_{deauth}/\Delta)}$ comes out to be greater than the threshold specified for the deauthentication flooding detection $\mathbf{Thresh_{flood.}}$

8 b) increment the value of the counter for recording the number of attack occurrences $\mathbf{C_{attack\ ocuurences}}$.If the value of counter for attack occurrences $\mathbf{C_{attack\ ocuurences}}$ is greater than the threshold specified for the attack$\mathbf{Thresh_{attack}}$ then it has been notified as the detection of the deauthentication attack.

9. Harvest MAC address and this comes out to be of legitimate client as the attack has been launched after spoofing MAC. So call the spoof detection function.

7.3.2 Algorithm for Spoofing Detection

1. Check if a STA sends additional frames after deauthentication/disassociation frame is observed, the deauthentication/disassociation frame must be spoofed one.

2. Check whether the first three bytes of the harvested MAC address matches with the OUI if it does not match then the MAC address is the anomalous one else it may be the spoofed one so for that we have to analyze using Sequence number analysis.

3. Initialize variables $\mathbf{Sequence_{cur}}$,$\mathbf{Sequence_{last}}$, ,$\mathbf{Sequence_{next}}$ as the sequence numbers of the current , last and next frame

4. Assign values for threshold and sequence number counter as $\mathbf{Thresh_{SN}}$, $\mathbf{Count_{SN}}$

5. Repeat till the value of count is less than threshold

a. Apply the verification process to check spoofing.

b. Send ARP request to current frame source station and that will put the station in verification state.

c. When the station is in verification state , then the monitor node checks

   - If the value of next sequence number is greater than the last sequence number and less than the current sequence number then it has been identified as the spoofed frame.

   - If next sequence number is greater than or equal to current sequence number then the frame has been identified as the retransmitted frame that was lost earlier because of congestion.

8. CONCLUSION AND FUTURE WORK

Wireless technologies ranging from IEEE 802.11 to draft standard IEEE 802.11s are susceptible to DOS attacks. We have implemented the deauthentication and disassociation DOS attacks over the actual Wireless mesh testbed.Although Wireless Mesh Networks derive their security from the IEEE 802.11i standard based protocol WPA2. This protocol can provide security to only the data frames. The management frames and the control frames are unencrypted and have been sent in clear. Thus DOS attacks have been launched by the attacker after spoofing and masquerading these frames. We have analyzed the impact of these attacks over the real Wireless Mesh Networks testbed. It has been noticed from the graphs that the network performance measured in terms of bandwidth and throughput appeared to be normal before the attack. But after the launch of the attack network performance starts decreasing and may reaches zero. So in lieu of this we have proposed a security algorithm for the detection of these deauthentication/ disassociation DOS attacks. This algorithm has reduced the generation of false positives. In this we have increased the number of metrics and based on all of these we have identified whether the attack has occured or not. Although Airdefense have proposed several hardware equipments that may raise alert in case of the attacks. Although these tools have been succeeded in ensuring secure communication in organizations where security is the primary concern, but cost is an issue associated with this solution. Thus there is the need to devise a globally viable cost effective solution. Moreover the security mechanisms that have been proposed so far can only detect the occurrence of these DOS attacks. So there is an imperative need to develop the security solutions for the prevention of DOS attacks.

9. REFERENCES

[1] Stuart Compton, Charles Hornat. May 17th 2007 802.11 Denial Of Service Attacks and Mitigation. SANS Institute InfoSec Reading Room.

[2] John Bellardo and Stefan Savage. Aug 4 -8, 2003 Denial of Service Attacks: Real Vulnerabilities and Practical Solutions. In the Proceedings of the 12TH USENIX Security Symposium. Washington, D.C., U.S.A.

[3] N. Bisnik and A. Abouzeid Jun 2006 Delay and Throughput in Random Access Wireless Mesh Networks. In the Proceedings Of IEEE International Conference on Communications (ICC 2006). vol.1, pp. 403 -408.

[4] Joshua Wright Jan 21, 2003 Detecting wireless LAN MAC Address spoofing. GCIH, CCNA, pp 1-5.

[5] Asier Martinez, Urko Zurutuza, Roberto Uribeetxeberria, Miguel Fernandez, Jesus lizarraga, Ainhoa Serna and Inaki Velez 4-7th March 2008 Beacon frame Spoofing Attack Detection in IEEE 802.11 Networks. In the proceedings of the third international conference on Availability, Reliability and Security (ARES08). pp 520-522, Barcelona.

[6] Thuc D. Nguyen, Duc H. M. Nguyen. Aug 3 -7, 2008 A light weight solution for defending against deauthentication / disassociation attacks on 802.11 networks. In the proceedings of 17th International Conference on Computer Communications and Networks. St. Thomas, U.S. Virgin Islands , USA.

[7] Baber Aslam, M Hasan Islam and Shoab A.Khan Sep 17-20, 2006 802.11 Disassociation Dos Attack and its Solutions: A Survey. In the proceedings of the First International Conference on Mobile Computing and Wireless Communication. pp 221-222, Amman.

[8] Fanglu Guo and Tzi-cker Chiueh. Sequence Number Based MAC Address Spoof Detection. In the book named Lecture Notes In Computer Science. pp 315-325, Volume 3858/2006, Springer Link.

[9] AirJack. http://sourceforge.net/projects/airjack/

[10] Airsnarf. http://airsnarf.shampoo.com/

[11] KisMAC//binaervarianz.de/projekte/programmieren/kismac

[12] D. Dasgupta, F. Gonzalez, K. Yallapu and M. Kaniganti June 22-27, 2003 Multilevel Monitoring and Detection Systems (MMDS). In the proceedings of the 15th Annual Computer Security Incident Handling Conference (FIRST). Ottawa, Canada.

[13] E. D Cardenas. MAC Spoofing {An Introduction. http://www.giac.org/practical/GSEC/Edgar Cardenas GSEC.pdf.

[14] J. Hall, M. Barbeau and E. Kranakis November 22-24, 2004. Using Transceiver Prints for Anomaly Based Intrusion Detection. In Proceedings of 3rd IASTED, CIIT 2004. St. Thomas, US Virgin Islands, USA.

[15] F. Robinson 2004 802.11i and WPA up Close. Network Computing.

[16] Peter Egli, Product Manager Wireless & Networking Technologies," Susceptibility of wireless devices to denial of service attacks"/http://www.netmodule.com.

[17] A. Gerkis and J. Purcell. Sep 2006 A Survey of Wireless Mesh Networking Security Technology and Threats. Sans Infosec Reading Room.

[18] Wireless Mesh Networks /http://www.wikkipedia

[19] White papers "Can Wireless LAN Denial of Service Attacks Be Prevented? "Understanding WLAN Vulnerabilities and their Countermeasures.

[20] TJ O Connor. Oct 13 , 2010. Detecting and Responding to Data Link Layer Attack. Sans Institute Infosec Reading Room.

[21] Jon Edney, William A. Arbaugh. 2003. Real 802.11 Security: Wi-Fi Protected Access and 802.11i, 480 pages, Addison Wesley, ISBN: 0-321-13620-9.

[22] Matthew S. Gast. April 2002. 802.11 Wireless Networks: The Definitive Guide, 464 pages, O'Reilly & Associates, ISBN: 0596001835.

[23] Vikram Gupta, Srikanth Krishnamurthy, Michalis Faloutsos. October 2002. "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks", Proceedings of 2002 MILCOM Conference, Anaheim, CA.

[24] S. Asherson, A. Hutchison. "Secure Routing in Wireless Mesh Networks". University of Cape Town.

[25] S. Kapp. Jan./Feb. 2002. 802.11: Leaving the Wire Behind. IEEE Internet Computing, vol. 6, no. 1, , pp. 82-85.

[26] CERT/CC. 2001. Denial of Service Attacks. Available Online: http://www.cert.org/tech tips/denial of service.html.