I.J. Information Technology and Computer Science, **2016, 6, 44-51**
Published Online June 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2016.06.06

Deployment of Coordinated Multiple Sensors to Detect Stealth Man-in-the-Middle Attack in WLAN

Ravinder Saini
Research Scholar (PG), Central University of Punjab, Bathinda, India
E-mail: saini.imperative@gmail.com

Surinder S. Khurana
Assistant Professor, Central University of Punjab, Bathinda, India
E-mail: surinder.seeker@gmail.com

***Abstract*—**The use of wireless devices is increasing tremendously in our day-to-day life because of their portability and ease of deployment. The augmented practices of using these technologies have put the user security at risk. The Stealth Man-In-The-Middle (SMITM) is one of the attacks that has arisen out of the flaw in the wireless technology itself. This attack aims at stealing the data of the network users by redirecting the traffic aimed at a legitimate user towards itself. Moreover the access point or any other detection device connected to the wired media fails to detect this attack. The objective of this work is to develop a technique that would be able to detect SMITM attack efficiently. In this work we present a SMITM detection approach. Our approach detects the SIMTM attack by deploying multiple coordinated sensors. The simulation results witnessed that the proposed scheme is capable of detecting SMITM attack even in case of a mobile attacker.

***Index Terms*—**Stealth Man-In-The-Middle attack, wireless local area network, hole 196 vulnerability, group temporal key, ARP cache poisoning, WLAN security.

I. Introduction

With the advent of wireless technology, networking has simplified to a great extent. Sharing of the resources at personal or business level has become easier and uncluttered due to wireless communications. Wireless networking provides the capabilities comparable to the wired network without the overhead of laying and managing wires. Users with wireless devices can roam about anywhere and get access to the service. Because of the ease of use, flexibility, reduced cost and roaming capability, wireless networking has gained a lot of popularity and masses have mostly switched over to this technology.

A. Architecture and Operation of WLAN

Wireless LAN consists of two types of architectural subsets [1]: Basic Service Set and Extended Service Set.

Basic Service Set is made up of stationary or mobile stations including an optional Access Point (AP) which acts as a central station. The BSS with an AP is known as infrastructure-based network and the one that does not include AP is called an ad-hoc architecture. In ad-hoc architecture, the nodes make the network without the use of AP. They discover one another and become the part of BSS. Extended service set consists of two or more BSSs. The Basic Service Sets connect to each other through a distribution system. The distribution system is usually a wired LAN.

B. Encryption and Security

For Wireless Local Area Networks, three encryption standards [2] have been implemented: Wireless Equivalent Privacy (WEP) [3], Wireless Protected Access(WPA)[4] and Wireless Protected Access version 2(WPA2) [5]. Among the above-stated protocols, the one that is considered to be most secure till now is WPA2. WPA2 is based on 802.1x authentication and used Advanced Encryption Standard (AES) [6] Algorithm.

Wired Equivalent Privacy was the part of original 802.11 standard. The protocol was implemented to provide confidentiality and security equivalent to the wired network. WEP uses RC4 stream cipher to provide confidentiality and CRC-32 checksum for providing integrity. The 64-bit key is a combination of 10 hexadecimal numbers (40 bits) and a 24 bit initialization vector. While in 128 bit key, 26 hexadecimal characters along with 24 bit initialization vector is used. Options with152 bit and 256 bit WEP systems are also available using 32 and 58 hexadecimal characters respectively along with 24 bits of the initialization vector. However, WEP was deprecated in 2004 due to its security flaws, and WPA took over it [7].

WPA was implemented as an immediate remedy for WEP flaws. Firmware upgrades were made on wireless NICs implementing WEP, to make them compatible with the newly introduced WPA standard. Temporal Key Integrity Protocol is used in WPA. TKIP generates a 128-bit key for each packet and this helps to prevent the attacks earlier possible on WEP. A message integrity check is also included in WPA and cyclic redundancy check method was removed from it as it could not guarantee integrity. An algorithm called Michael is used in WPA to check the integrity of the packets. The drawback Michael holds is that it retrieves the keystream for short packets and it can be used for reinjection and spoofing.

WPA2 operates in two modes: Pre-shared Key (PSK) mode and Enterprise mode. In PSK mode, the router is configured just with a plain-English passphrase (encrypted or non-encrypted). This passphrase may contain up to 133 characters. Unique encryption keys for each Wi-Fi client are generated by this passphrase using TKIP (Temporal Key Integrity Protocol). The keys are frequently changed. On an attempt, by the client, to connect to the network, a password is used to verify them. The access is provided to the client as long as the passwords match. The WPA2 enterprise (802.1x) mode uses AES encryption. An external server named as Remote Authentication Dial In User Service (RADIUS)[8] or Authentication, Authorization and Accounting (AAA)[9] is used to allow authentication requests from IP addresses of Access Points. The RADIUS server uses the Extensible Authentication Protocol (EAP) [10] to establish a secure channel between the authenticating parties and to communicate with wireless Access Points.

Enterprise mode provides a more secure environment by providing centralized control over the connections. The users log-in through their credentials provided to them by the administrators. The actual encryption keys are never stored with the users. For each session, a new key is generated and assigned after the user provides its log-in credentials. This prevents the key recovery and its misuse.

WPA2 uses two standard types of keys for encryption i.e. Pairwise Transient Key (PTK) and Group Temporal Key (GTK). The AP provides PTK to every client connected to that particular access point. Every client has its own unique key. It is used to secure the unicast communication being carried out between the access point and the clients. In other words, it could be said that PTK is the private key for a two way private communication that can be used by the corresponding client or the access point to encrypt or decrypt the data meant for any one of the two. On the other hand, GTK is shared by all the clients associated with a particular access point. It is used by the access point to send multicast or broadcast data. Only the access point is authorized to use this key for encryption purpose. The clients are allowed to just decrypt the data and retrieve the information from the broadcast or multicast packets. Thus, the GTK is said to be a one way key. T.S. Sobh[11] has compared various security standards used in WLAN and tested these security standard under few attack conditions.

II. Related Work

The Hole 196 [12] vulnerability in WPA 2 was first exposed by M. S. Ahmad [13] in 2010 in Defcon 18. Along with the discussion of the GTK vulnerability, stealth ARP Poisoning attack has been brought to light. For the mitigation of the attack, three strategies have been discussed. The first one being the Client IDS to detect ARP cache poisoning with the limitation that it works only on Windows and Linux based operating systems but nor for smartphones, etc. Second being the PSPF or client isolation[14] to restrict peer to peer communication by blocking traffic between two Wi-Fi clients with the limitation that this PSPF or Client isolation capability is not included in all the controllers or standalone mode APs. The third being the software based solution i.e. by depreciating the use of GTK. For backward compatibility, AP should send randomly generated different GTKs to different clients so that all associated clients have different copies of GTK all the time. Decreased network throughput and frequent AP software upgrade requirements are limitations of this technique.

A. Herzberg and H. Shulman [15] have defined Stealth Man-in-the-Middle adversaries and analyzed the ability of these adversaries to launch denial and degradation of service (DoS) attacks on secure channels. Realistic attacks which disrupt TCP communication over secure VPNs using IPsec have been shown. They have presented an amplifying DoS attack on IPsec, deployed with and without anti-replay window and have analyzed the sufficient window size. A solution to prevent the presented attack has also been illustrated. This solution provides a secure channel that can resist degradation and other such DoS attacks. In addition to their practical importance, their results also challenge formally defining secure channels immune to DoS and degradation attacks, and provide almost secure implementations. The scheme does not include the measures to prevent ARP Poisoning, which is the prime factor in the case of SMITM.

A Wireless Intrusion Detection System [16] is developed to detect the Stealth Man-In-The-Middle attack possible in wireless LAN because of the vulnerability called Hole 196. In this paper, multiple sensors have been deployed to catch the ARP Response packets spoofed by the attacker, which is an authorized user. When an ARP response packet with spoofed content is found, an alarm is generated by the WIDS and the packet with malicious content is dropped. A drawback of this scheme was that it could detect the attack only when the attacker was under the coverage of a single sensor. Moreover, this scheme may also increase the load on the network.

Another wireless network IDS [17] is also designed to detect, record, process, prevent and generate alarms for real-time intrusion behaviors of the system. It has some modules for data packet capturing, analyzing, filtering, storage, maintenance, etc. The data capturing module captures the data and forwards it to the data analysis module. According to the results generated by the module, the packets are labeled suspicious or normal. The suspicious packets are then transferred to the detection module, which then with the help of anomaly detection module detects the packets and response module is instructed to work accordingly. During the process, the rule base and parameter base are automatically loaded into the system according to the requirements. This system also lets the users adopt self-defined rule base and other authorization lists. Firewalls and their rule base are not able to detect SMITM as it is an insider attack, and the packets responsible for launching the attack need not pass any firewall.

M. Kacic & et al. [18] have explained the possibility of malware injection into wireless communication using Hole 196 vulnerability of Group Transient Key. They have created and injected the malware through a crafted frame. In their method, they extracted the GTK from the interface and then wait for the broadcasted frame to exploit it. They have described abusing of the vulnerability of the encryption key used for broadcast communication and consequences of this vulnerability has been shown in malware injection attack. The impact of this kind of attack on the user is found to be major, because with an increasing number of users a risk of abuse of user privileges increase. The result of the security incident was to compromise the target client by an attacker. The proposed attack is an insider type of attack abusing user privileges, and this kind of attack can bypass any traditional network intrusion detection system.

The creation and use of a dataset for intrusion detection system for the wireless system are also proposed [19]. The datasets have been collected from two scenarios, first being the real and controlled typical WPA/WEP network and the other being corporate network WPA2 network. By performing different attacks on both the scenarios the datasets for IDS under attack and in normal conditions were evaluated. Pattern recognition and classification algorithms are used to validate the dataset. These datasets reflect the traffic conditions under normal as well as attack conditions. The drawback of the scheme to detect SMITM is that the altered traffic flow cannot be detected in the case of SMITM as the traffic directed towards attacker seems legit.

III. Stealth Man-In-The-Middle-Attack

A. Hole 196 Vulnerability

When following WPA2 protocols, APs use Group Temporal Key to encrypt broadcast or multicast communications frames. The Same key is used to decrypt those frames at the client side. Only the access point is authorized to encrypt the data through this key but sometimes the clients authorized with the access point may violate the standard rule and may misuse the GTK. The client may encrypt any malicious data using the GTK and may broadcast or multicast it to other clients which, as generally, would take those frames to be coming from the access point. Through these frames, any malformed data can be injected into the legitimate traffic and these frames can be used to exploit the clients in many ways. As GTK is not dependent either on authentication or encryption, it makes both modes (PSK and Enterprise) of WPA2 vulnerable to attacks [20]. Some attacks that are possible through this vulnerability are ARP poisoning [21], DoS attack and DNS manipulation, etc.

B. SMITM Attack Mechanism

Stealth Man in the Middle Attack is one of the most complicated attacks, and detection is not easy because it is an insider attack. This vulnerability arises from the MAC Header in WLAN 802.11. A general frame format of a MAC Header contains four types of MAC addresses: Destination MAC Address, Source MAC Address, Receiver Address, Transmitter address. The format of MAC header and details of its field Frame Control are mentioned in Fig. 1 and Fig. 2 respectively.

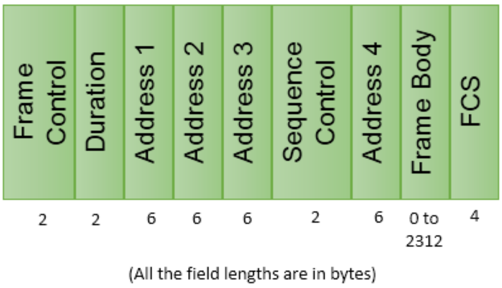


Fig.1. MAC Header

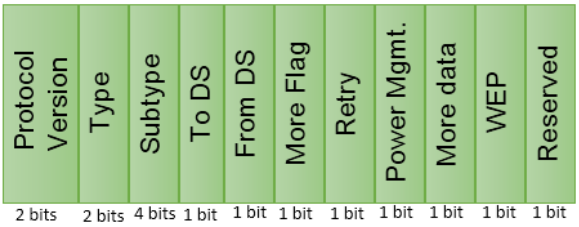


Fig.2. Fields in Frame Control

SMITM attack can be performed as follows:

- The attacker prepares a forged ARP frame.
- Right circular shift operation is performed on FromDS, ToDS and Address-I, Address- 2, Address-3 on the IEEE 802.11 frame header attached to ARP frame. This changes the direction of the frame from uplink to downlink.
- This forged ARP frame is then encrypted with GTK using Hole 196 attack, and the frame is transmitted to the victim.
- After receiving the frame, the victim can never get to know that the frame it received is not from authorized AP but sent by an attacker.
- Victim updates its cache according to the

information gathered through forged frame sent by the attacker and thus its ARP cache gets poisoned.

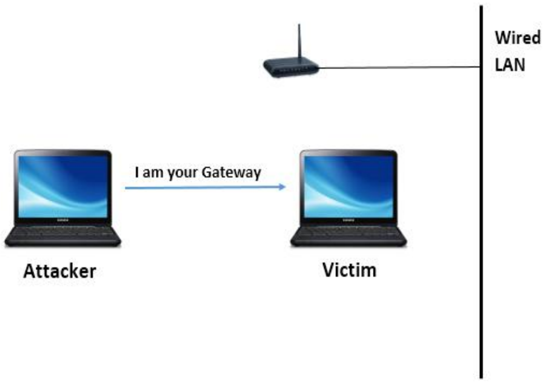


Fig.3. Stealth Man-In-The-Middle attack

IV. Proposed Modelling

The proposed technique to detect Stealth Man-In-The-Middle attack in wireless local area network includes the deployment of sensors that can overhear the transmissions that are going on in the network. The detection system is incorporated into all the sensors. To begin with the detection mechanism, the sensors capture the ARP replies that are being transmitted in the network. After capturing the ARP reply packet, it extracts the values from the source protocol address and the source hardware address.

Further, each sensor maintains two lists. The First list: Restricted_Pair list contains the IP-MAC address pairs that have been blocked and marked as malicious on the basis of records maintained by the respective sensors. The sensor add the IP-MAC into this list in case it detects that this belongs to some attacker. The second list: Genuine_Pair list contains the IP-MAC address pairs that have been marked genuine through verification.

The captured IP-MAC pair is checked for its entry in the Restricted_Pair list. If the pair is present in this list, an alarm for attack is generated. If it is not present in the Restricted_Pair list, the Genuine_Pair list is checked. The presence of the corresponding IP-MAC pair in Genuine_Pair list signifies that it is a genuine pair and thus no further action is taken.

If the captured IP-MAC is present neither in Restricted_Pair list nor in Genuine_Pair list, the intrusion detection system has to take various steps to decide about the authenticity of the captured IP-MAC pair. To begin with the sensor sends a probe request to the access point containing the captured IP-MAC pair. On receiving the probe request, the access point handles the probe by sending the ARP request to the IP address received in the probe request. If the ARP reply has the MAC address same as the one in the probe request, the AP sends a positive probe reply to the sensor. If the MAC address received in the ARP reply corresponding to the ARP request sent by the AP does not match with the one received in the probe request, the AP sends negative probe reply to the sensor.

On receipt of the probe reply, the sensor looks for the IP and MAC address received in the reply packet. If the IP-MAC pair is same as the one it probed for, the values for the IP and MAC address are added to the Genuine_Pair list otherwise if the MAC address is different from the one the sensor probed for, the values are inserted into the Restricted_Pair list.

As soon as a sensor updates any of its lists, it prepares a packet and sends it to all the other sensors in the network. On receiving this packet, the sensors check their corresponding list for the existence of the IP-MAC pair received in the packet. If the corresponding pair is not found in the list, the IP-MAC pair is added to the list. Now all the sensors have the information about the malicious MAC address. This would help to detect the attack even if the attacker moves from the range of one sensor to another and launches the attack on other victims, the attack will be detected in its first attempt itself.

A. Pseudo code depicting the working of sensor node on capturing the ARP Request

Input: ARP Reply Packet
Output: Alarm in case of attack

```
Capture ARP reply packets except those induced by AP during verification
if $ARP\_IP_s$ = $GenList\_IP_i$ and $ARP\_MAC_s$ = $GenList\_MAC_i$
    Do nothing
end if
if $ARP\_IP_s$ = $RstList\_IP_i$ and $ARP\_MAC_s$ = $RstList\_MAC_i$
    Generate alarm for attack
    else if $ARP\_IP_s \neq RstList\_IP_i$ and $ARP\_MAC_s$ = $RstList\_MAC_i$
        Alarm for attack on multiple nodes
    end if
end if
if $ARP\_IP_s \neq RstList\_IP_i$ and $ARP\_MAC_s \neq RstList\_MAC_i$
    sendProbeReq($ARP\_IP_s$, $ARP\_MAC_s$)
end if
```

B. Pseudo code for detection scheme working at AP

Input: Probe packet from sensor
Output: Probe Reply

```
Receive probe request from the sensor
if $P_{rq}\_IP$ = AP_IP and $P_{rq}\_MAC$ = AP_MAC
    sendProbeReply($P_{rq}\_IP$, $P_{rq}\_MAC$, true)
end if
if $P_{rq}\_IP$ = AP_IP and $P_{rq}\_MAC \neq$ AP_MAC
    sendProbeRep($P_{rq}\_IP$, $P_{rq}\_MAC$, false)
end if
if $P_{rq}\_IP \neq$ AP_IP and $P_{rq}\_MAC \neq$ AP_MAC
    sendARPReq($P_{rq}\_IP$)
end if
recvARPRep()
if $IP_{ARP}$ = $P_{rq}\_IP$ and $MAC_{ARP}$ = $P_{rq}\_MAC$
```

```
    sendProbeRep($P_{rq}$_IP, $P_{rq}$_MAC, true)
end if
if IP$_{ARP}$ = P$_{rq}$_IP and MAC$_{ARP}$ $\neq$ P$_{rq}$_MAC
    sendProbeRep($P_{rq}$_IP, $P_{rq}$_MAC, false)
end if
```

C. Pseudo Code for Simulation of Detection Scheme on Sensor after Receiving Probe Reply

Input: Probe Response Packet
Output: Updated Lists

```
for each probe response packet
if reply = true
    update GenList
    sendWIDSBeacon(ARP_IP$_s$, ARP_MAC$_s$, true)
end if
if reply = false
    update RstList
    sendWIDSBeacon(ARP_IP$_s$, ARP_MAC$_s$, false )
end if
end for
```

Table 1. Symbols Used in Pseudo Code

SYMBOL USED	MEANING
GenList	Genuine_Pair List
RstList	Restricted_Pair List
ARP_IP$_s$	Source IP Address in captured ARP Reply
ARP_MAC$_s$	Source MAC Address in captured ARP Reply
GenList_IP$_i$	IP Address at i^{th} level of GenList
GenList_MAC$_i$	MAC Address at i^{th} level of GenList
RstList_IP$_i$	IP Address at i^{th} level of RstList
RstList_MAC$_i$	MAC Address at i^{th} level of RstList
P$_{rq}$_IP	IP Address received in probe request
P$_{rq}$_MAC	MAC Address received in probe request
AP_IP	IP address belonging to AP
AP_MAC	MAC address belonging to AP
IP$_{ARP}$	IP address received in ARP reply induced by AP
MAC$_{ARP}$	MAC address received in ARP reply induced by AP

V. Results and Discussions

A. Simulation Environment

To implement the proposed detection technique, NS-2.35 has been used. The simulated network consists of 24 nodes for which four sensor nodes have been deployed to cover the whole network collectively. All the nodes along with the sensors and an access point collectively form a BSS. Out of all the authenticated nodes, a nodes acts as at attacker. The attack is launched over two victims with node IDs 3 and 5 respectively. The attacker, as well as the victims, are under the range of the same sensor. After launching the attack under the range of one sensor, the attacker moves to another sensor, and there it launches attack on another victim.

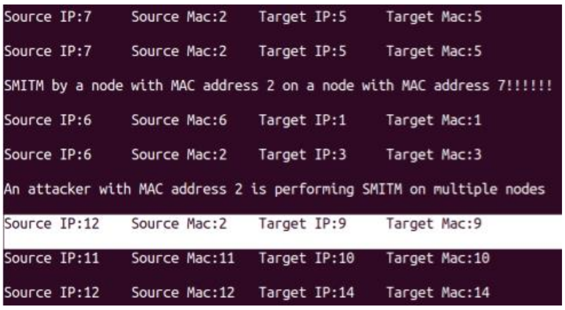
The network is simulated under the normal as well as attack scenario. In the attack scenario as well, there are two cases, the first in which the sensors implement the detection scheme on their own and the other being the scenario where the sensors coordinate among each other and share their data. Without coordination each sensor has its own lists prepared through the data collected by it during detection but when the sensors work in coordination, as soon as a sensor updates its lists, it shares that data with other sensors in the network. It helps in detection of attack in the following cases:

- The attacker attacks the victims when both of them are under the range of the same sensor.
- Attacker attacks the victim under the range of a sensor and then moves to the range of another sensor and attacks the victims that are under the same or different sensors as the victim.

The detection scheme is capable of detecting the attack in both scenarios.

B. Results

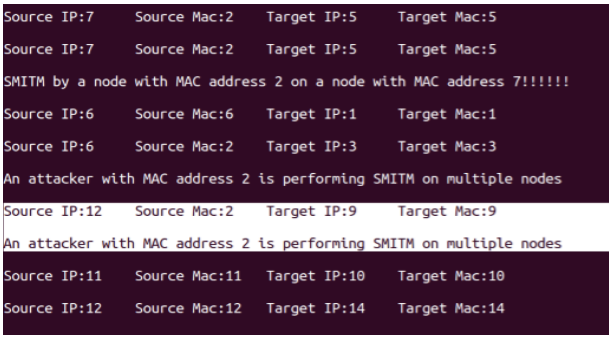
In fig. 4., the values from the ARP Reply packets as well as the alerts (if any) corresponding to them have been printed. We can see here that the node with IP address 5 has been victimized by the attacker with MAC address 2. The simulator has used the flat addressing, therefore, the IP and MAC addresses appear in the form of simple numerals rather than the conventional formats prescribed for each of them. The attack goes undetected for the first time because the lists are being populated during this course. But when the attacker attacks for the second time, an alert for the attack is generated. Now the attacker moves to sensor number 2 and attacks the node with IP address 9. This time, sensor number 2 is not able to detect the attack, and thus no alarm has been generated.



```
Source IP:7     Source Mac:2    Target IP:5     Target Mac:5

Source IP:7     Source Mac:2    Target IP:5     Target Mac:5

SMITM by a node with MAC address 2 on a node with MAC address 7!!!!!!

Source IP:6     Source Mac:6    Target IP:1     Target Mac:1

Source IP:6     Source Mac:2    Target IP:3     Target Mac:3

An attacker with MAC address 2 is performing SMITM on multiple nodes

Source IP:12    Source Mac:2    Target IP:9     Target Mac:9

Source IP:11    Source Mac:11   Target IP:10    Target Mac:10

Source IP:12    Source Mac:12   Target IP:14    Target Mac:14
```

Fig.4. Detection scenario without coordination among sensors

Fig. 5. shows the generation of alarm when the sensors have implemented the coordination scheme among themselves. Here the attacker moves from sensor number 1 to sensor number 2 during the course of the attack. Unlike the scenario without coordination of the sensors, sensor number 2 was immediately able to detect the attack in its first attempt only because the sensors have already shared their lists and detection can be made on the basis of these shared lists.



```
Source IP:7     Source Mac:2    Target IP:5     Target Mac:5
Source IP:7     Source Mac:2    Target IP:5     Target Mac:5
SMITM by a node with MAC address 2 on a node with MAC address 7!!!!!!
Source IP:6     Source Mac:6    Target IP:1     Target Mac:1
Source IP:6     Source Mac:2    Target IP:3     Target Mac:3
An attacker with MAC address 2 is performing SMITM on multiple nodes
Source IP:12    Source Mac:2    Target IP:9     Target Mac:9
An attacker with MAC address 2 is performing SMITM on multiple nodes
Source IP:11    Source Mac:11   Target IP:10    Target Mac:10
Source IP:12    Source Mac:12   Target IP:14    Target Mac:14
```

Fig.5. Detection scenario with coordination among sensors

C. Effect on Network Performance

The network performance in this detection scheme can be calculated from the load that is imposed on the system. To determine the network load we analyzed the number of packets being transmitted during the simulation of detection scenario with respect to the transmissions carried out in the normal scenario.

To simulate of the detection scheme, a few packets other than those help in network management, network control, and data transfer are also made to flow in the network. Let’s assume that x number of packet transmissions take place in the network under the normal conditions. After the simulation of the detection scheme, there are two scenarios.

One is when the detection technique is working, and there is no attack on the network. During this time, for each captured ARP reply a probe request packet, a probe reply packet, an ARP request packet and an ARP reply packet is transmitted into the network. Along with that, the WIDS packet is transmitted only to share verified pairs. So the network load, considering these packets, will be

$$x + (1+1+1+1+1)y = x+5y,$$

where y is the number of ARP replies captured by the sensor.

The second scenario is the attack scenario. This scenario leads to the transmission of a probe request packet, a probe reply packet, an ARP request packet, an ARP Reply packet and a WIDS Beacon packet to share the blocked and verified pairs of the addresses. But the total number of packets remain the same in both the cases. So the network load for this scenario is also (x+5y) packets.

Thus in any case the same number of packets are transmitted in the number. So the network load due to wireless intrusion detection system will largely depend on the number of ARP reply packets in the network that in turn depend on the number of nodes in the network. Thus, the detection scheme does not pose the undesirable load on the network, and the transmissions are carried out with an approximately equal end to end delay in the normal scenario as well as with detection scheme.

D. Average End to End Delay

End to end delay in packet transmission in the normal scenario as well during the simulation of detection scheme is mentioned in fig. 6. It is evident from the value in the graph that there is insignificant variation in delay during both the scenario. Thus from the graph, we can conclude that the proposed detection scheme does not slow down the network transmissions beyond the acceptable levels.

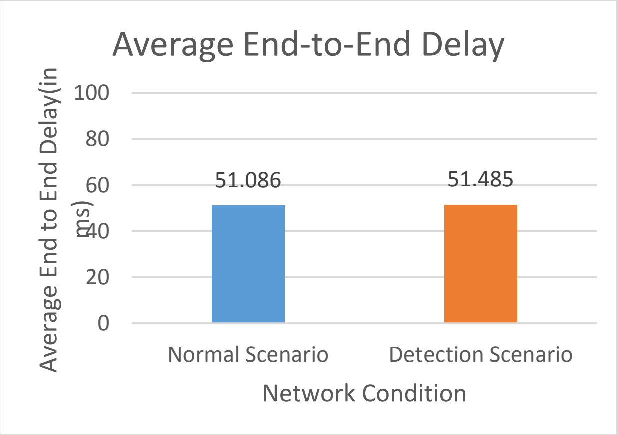


Fig.6. Average End-to-End Delay

VI. Conclusion

The Stealth Man-In-The-Middle attack is proved to be a fatal attack for the security of a network as it is a silent attack. Neither the access point nor the wired intrusion detection systems can detect it because it is carried out by an authenticated node in the network. Moreover, it makes the adulterated packets look like they are coming from the genuine source. These malicious packets never get to reach the wired system as they are made to circulate within the wireless medium by exploiting certain vulnerabilities found in the WPA2 protocol implementation itself.

In this work, a detection scheme to detect the attack in the wireless local area network has been proposed. The scheme proposed by V. Kumar & et al., to detect Stealth Man-In-The-Middle attack in WLAN was unable to detect the attack when the attacker moved from the range of one sensor to another and attacked other victims there. If the attacker attacks a victim being under the range of one sensor, the other sensor would have no information about this session of attack and would have to undergo the detection procedure from the beginning. Thus, the first attempt would go undetected. And if, by chance, the attacker moves to another sensor after a single but successful attack attempt, the sensor would never be able to detect that attack. Therefore, a technique has been proposed in this paper to coordinate the sensors so that they can share their data with one another. The sharing of data would prevent each and every sensor from undergoing the whole detection procedure from the beginning, yet making the detection possible in the case of a mobile attacker in first attempt only. Moreover, this detection scheme does not put much load on the network and thus the transmissions can be carried out easily without considerable delay in the network

The only shortcoming of this detection scheme is a false negative case in the very beginning of the detection procedure and a false positive when the attacker replies for the genuine ARP request frames addressed to it, but the detection scheme considers it to be attack because of the blacklisted MAC address of that node. So in future work the technique can be improved to remove those flaws. Moreover, a prevention scheme could also be designed to prevent the attacker from launching the attack.

References

[1] B. A. Forouzan, "Wireless LANs," in Data Communications and Networking, The McGraw Hills Publications, pp. 421-443.

[2] A. H. Lashkari, M. M. S. Danesh and B. Samadi, "A Survey on Wireless Security Protocols (WEP, WPA and WPA2/802.11i)," Beijing, 2009. URL: http://www2.it.lut.fi/wiki/lib/exe/fetch.php/courses/ct30a2001/opiskelijat/2008/a_survey_on_wireless_security_protocols_wep_wpa_and_wpa2_802.11i_.pdf

[3] S Vibhuti, "IEEE 802.11 WEP wired equivalent privacy concepts and vulnerability." Accessed on August-10-2015. URL: http://www.cs.sjsu.edu/~stamp/CS265/projects/Spr05/papers/WEP.pdf

[4] Wi-Fi Alliance,. "Wi-Fi Protected Access: Strong, standards-based, interoperable security for today’s Wi-Fi networks." White paper, University of Cape Town, 2003. URL: http://www.ans-vb.com/Docs/Whitepaper_Wi-Fi_Security4-29-03.pdf

[5] M. Matthews and R. Hunt , "Evolution of Wireless LAN Security Architecture to IEEE 802.11i (WPA2)," in Proceedings of the Fourth lASTED Asian Conference on Communication Systems and Networks, 2007. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.490.9144&rep=rep1&type=pdf

[6] S. Heron, "Advanced Encryption Standard (AES)." Network Security 2009, pp. 8-12, Vol. no. 12, 2009. URL: http://www.sciencedirect.com/science/article/pii/S1353485810700064

[7] K. Curran, and S. Elaine, "Demonstrating the Wired Equivalent Privacy (WEP) Weaknesses Inherent in Wi-Fi Networks." Information Systems Security 15, 2006, pp. 17-38. URL: http://www.tandfonline.com/doi/abs/10.1201/1086.1065898X/46353.15.4.20060901/95121.3#.VeBL-DmQmuE

[8] P. Congdon, B. Abode, A. Smith, G. Zorn, and J. Roese. "IEEE 802.1 X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines." No. RFC 3580. 2003. URL: https://tools.ietf.org/html/rfc3580

[9] C. Perkins, and P. Calhoun. "Authentication, authorization, and accounting (AAA)." IETF RFC 5637, 2005. URL: https://tools.ietf.org/html/rfc5637

[10] B. Aboba, B. Larry, V. Vollbrecht, C. James, and L. Henrik, "Extensible authentication protocol (EAP)". No. RFC 3748. 2004. URL: https://tools.ietf.org/html/rfc3748

[11] T.S. Sobh, “Wi-Fi Networks Security and Accessing Control”, International Journal of Computer Network and Information Security, vol. 5, no. 7, pp. 9-20, 2013. URL: http://www.mecs-press.org/ijcnis/ijcnis-v5-n7/v5n7-2.html

[12] “IEEE Standard for information technology communications and information exchange between systems local and metropolitan area networks specific requirements," IEEE, 2007. URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6178212

[13] M. S. Ahmad, "WPA Too!," in Defcon, Las Vegas, 2010. URL: https://www.mediafire.com/?sharekey=qelvipkzu054z

[14] Thuc, NGUYEN Dinh, and NGUYEN An Bien. "Hotspot Security." URL: http://dept-info.labri.fr/~dicky/PUF/Internships/Nguyen%20An%20Bien%202011.pdf

[15] A. Herzberg and H. Shulman, "Stealth-MITM DoS Attacks on Secure Channels," vol. 7, no. 1, pp. 1-27, 19 October 2009. URL: http://arxiv.org/abs/0910.3511

[16] V. Kumar, S. Chakraborty, F. A. Bharbhuiya and S. Nandi, "Detection of Stealth Man-In-The-Middle Attack in WLAN," 2nd IEEE International Conference on Parallel, Distributed and Grid Computiong, pp. 290-295, Dec 2012. URL: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6449834&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6449834

[17] W. Jian, F. Zhi-feng and C. Yong, "Design and Implementation of Lightweight Wireless Lan Intrusion Detection System," in Fourth International Conference on Multimedia Information Networking and Security Nanjing, 2012. URL: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6405633&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6405633

[18] M. Kacic, P. Hanacek, M. Henzl and P. Jurnecka, "Malware Injection in Wireless Networks," in The 7th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Berlin, 2013 URL: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6662732&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6662732

[19] D. W. Vilela, E. W. T. Ferreira, A. A. A. S. Shinoda, N. V. de Souza Araújo, R. de Oliveira and V. E. Nascimento, "A Dataset for Evaluating Intrusion Detection Systems in IEEE 802.11 Wireless Networks," in Colombian Conference on Communications and Computing, Bogota, 2014. URL: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6860434&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6860434

[20] V. Kumar, A. Tiwari, P. Tiwari, A. Gupta and S. Shrawne, "Vulnerabilities of Wireless Security Protocols (WEP and WPA2)," International Journal of Advanced Research in Computer Engineering & Technology, vol. 1, no. 2, pp. 91-96, April 2012. URL: http://ijarcet.org/wp-content/uploads/IJARCET-VOL-1-ISSUE-2-34-38.pdf

[21] N. Agrawal, P. K. Bhale and S. Tapaswi, "Preventing ARP Spoofing in WLAN using SHA-512," in IEEE International Conference on Computational Intelligence and Computing Research, Inathi, 2013. URL: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6724145&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6724145

Authors' Profiles

Ravinder Saini is pursuing her Master of Technology in Cyber Security from Central University of Punjab, Bathinda. She has pursued her Bachelor of Technology in Information Technology from I.K. Gujral Punjab Technical University, Jalandhar. Her research interests include information security, network security and network forensics.

Surinder S. Khurana is an Assistant Professor at Centre for Computer Science & Technology, Central University of Punjab, India, He received his Master's degree in computer science & engineering from PEC University of Technology, India in 2009. He has published many papers in refereed journals and conference proceddings. His research interests includes networks security, cyber forensics and algorithm design..

How to cite this paper: Ravinder Saini, Surinder S. Khurana,"Deployment of Coordinated Multiple Sensors to Detect Stealth Man-in-the-Middle Attack in WLAN", International Journal of Information Technology and Computer Science(IJITCS), Vol.8, No.6, pp.44-51, 2016. DOI: 10.5815/ijitcs.2016.06.06