Volume 5, Issue 2, February 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Impact of ARP Spoofing attack on MAC layer over IEEE 802.3 and IEEE 802.11 Hybrid Network

[1]Bharti Chopra, [2]Dr. Parminder Singh
[1]Student, [2]Assistant Professor
Department of Information Technology
CGC, Landran, Chandigarh, India

Abstract*—There are numerous attacks taking place at MAC layer in both wired and wireless networks at exuberant rate because this layer is very sensitive and most compromised layer in connectivity. So as a result of that many Intrusion Detection Systems have also come in existence from a long time till now for the detection of number of vulnerable attacks. Intrusion Detection Systems (IDS) are the tools and techniques which analyze and detect the abnormal data patterns coming from the unauthorized network. These abnormal patterns are known as attacks which are send through the intruder to harm as well as gain the confidential information. In this paper we are discussing the ARP Spoofing attack taking place at MAC layer which is affecting the propagation of data the most and soiling the resources at surplus level. In addition to that our proposed work illustrates the scenarioof hybrid network. In the process of intrusion detection we mean that whenever attack is occurred, in a network, it should be detected. Basically detection process is done by the Authenticated Token. In the current paper we have presented the Authenticated Token field used with ARP. We have presented that attack has been cancelled if the node has no information for Authenticated Token Field.

Keywords- IDS, intrusion, MANETs, MAC layer, AODV, ARP spoofing.

I. INTRODUCTION

Computer Networks are the telecommunication networks providing data exchange and accessibility of connection between numbers of nodes varying from local to large scale area. With the passage of time these networks are becoming very much dense and complex. There are two main type of networks according which complexity varies, that are, wired and wireless. IEEE 802.3(wired) are the connected nodes which are reliable but gets complex with increase of network size whereas IEEE 802.11 (wireless) are the mobile ad hoc networks(MANETs) which are flexible but not reliable [11].

As the revolution took place in the connectivity the attacks are also prevailing and exceeding to a very advance level. Previously, in wired networks the attackers had only center access point like modem for getting into the network by generating the automated hacking scripts of numbers. As the MANET technology came to real working the attack levels also get a hike as attack can be done through any node because every node works as a router too. Therefore, small scale as well as broadband connectivity both is of equal concern for security and authentication.

The intrusions are happing at all the levels of the connectivity modal but the security is weakest at MAC layer [19]. If MAC layer gets hacked then all the above layers will suffer too. Therefore, implementation of security controls over MAC layer is the foremost task to be done. Here we are taking the ARP spoofing attack at MAC layer to analyze and implement the better IDS for detecting it in a hybrid wired and wireless scenario.

II. ARP SPOOFING

ARP stands for Address Resolution Protocol which helps in communication by providing required addresses. Hence as application, ARP protocol is an independent protocol that connects to physical layer and network layer directly to provide the mapping between IP and MAC addresses [3]. An ARP Request is a message requesting to resolve a given IP address into its associated MAC address [12]. Accordingly the response will come back through the server as if the requested IP is available in the network. It thus also gave the existence to the most critical and dangerous intrusion known as ARP spoofing.

ARP Spoofing is a hacking technique to send fake ARP request or ARP reply, ARP spoofing problem comes from the way the ARP protocol works [1]. Since the ARP protocol is a stateless protocol that receives and processes ARP replies without issuing ARP request, the ARP cache can be infected with records that contain wrong mappings of IP-MAC addresses [1].

Thus ARP spoofing manipulates data in the ARP table and all this intrusion can be done in two ways:

(i) *MITM:* In Man in the Middle(MITM), the intruder fetches the location in between the communication path of client and host. By doing so, intruder poisons the ARP table by behaving as a authenticated client.

(ii) *DoS:* Here in Denial of Service(Dos), all the data will be forwarded to intruder as the intruder provides the wrong IP-MAC pairing.

III. RELATED WORK

NavidBehboodian and ShukorAbdRazak[12] proposed a scheme where entries are look after through the web browser but this is also the main drawback of this scheme that it would not work if web browser is not working.The technique specified in [6] is about creating a data table in the cache memory of the server for maintaining the record of the nodes. Therefore, this in result overloading the server with large amount of data.The proposed method [20] uses the alarm notification during filtration. The alarm buzzes if the ARP attack occurs in the subnet area. The main problem with this scheme is that it not scalable and thus cannot work in the dense network.

IV. PREVIOUS APPROACHES

For information security, many intrusion detection and prevention techniques are persisting and varying from host level to network level. For the perfection purpose, improvements take place time to time till now. In the previous methods the major area to be improved is to reduce the huge table storage data because it utilizes lot of sever memory which in result slow down network or it can even totally breakdown the network. The solution of creating cache storage is overloading the server which in result is slowing down the whole network. There is no practical way to identify the spoof attack. Even the single network is used instead of hybrid due to which the results vary and complete problem area could not be determined. So these things strongly need to be readdressed.

V. TOKEN BASED APPROACH

To overcome the existing problems we can use a wired and wireless hybrid network in which we can add encrypted information in the packet header which we have named as Authenticated Token Field (ATF).This token is generated by a generator function and stores the information of verification instead of using large capacity buffer table. This will not only reduce the overhead but also makes applicable the authenticity of the packet in the network. Thus if packet enters the network area without token field will be easily captured and reported as spoof attack.

VI. CLIENT-SERVER MECHANISM

In ARP connectivity, the two sided functioning is required where firstly the client node sends the request to the server and then in response to that the server takes required action. We have used the active mechanism for verification of the nodes which manages the scalability of network. For such scenario, thus, two main algorithms are proposed to obtain the better results and verify major to minor details of the connecting node. In addition, there will be two main functions i.e. RequestTokenGenerator() which will provide tokens to the every authenticated node and ReplyTokenVerification() which will work at host side to check whether the node is valid or malicious. The algorithms are explained as follows:

(i) *Client-to-Server Request Algorithm:* The algorithm performs the initial phase where the entering node sends the request to the server for authentication. At this point, the token request is performed which is cryptographic key to provide authentication to the node.

Algorithm 1: ARP Client Request

```
Start
ARP Request Packet is checked
if(Changes occurred in Packet == True)
then
    Status= Malicious Packet
else if (Packet Request is Unicast)
then
    Status=Unicast
    The Request IP addresses are then matched between Client and Server
else if (Source IP == Destination IP)
then
    Status = Normal packet
    Then IP-MAC pairing is verified through verification table
    if (IP-MAC pair == matched)
    then
        Status=Authenticated Node
        Request Token from the server
        get = RequestTokenGenerator()
    else
        Status= Corrupted Node
end if
```

(ii) *Server-to-Client Response Algorithm:* In this algorithm, the response from the server is performed corresponding to the request. The node is further verified and according to that the action will be taken. If the node is genuine then only token will be provided and at last the entry of node is done through the valid token.

Algorithm 2:ARP Server Reply

```
Start
ARP response Packet is checked
```

```
if (Changes occurred in Packet == True)
then
    Status= Malicious Packet
    The Response IP addresses are then matched between Server and Client
else if (Source IP == Destination IP)
    if(Wrong Request Trials are then set value)
    then
        Status = Normal packet
    end if
else if(IP-MAC pair == matched)
then
    Obtain Token as per requested node
    set = Generated Token
end if
```

After getting the token, the verification can be done at any access point through the implemented IDS. Then if the cryptographic token is matched the requesting node can enter the network. There is further algorithm for IDS that is working at every access point for the entry of the node in the network and is mentioned as follows:

Algorithm 3: IDS Protection

Let $RQP_{reqIP}$is a request packets send to ARP and let T be the token that has been attached with $RQP_{reqIP.}$

```
Start
Obtained $RQP_{reqIP} = T \{RQP_{reqIP}\}$
Send(Obtained $RQP_{reqIP}$)to ReplyTokenVerification()
if (ReplyTokenVerification() == Genuine)
then
    Allow the node to enter to network
else
    Report: Intrusion or attack has been occurred
end if
```

VII. SIMULATION

The experimental work is done in virtual environment with the simulator known as NS-2. In NS2, we can analyze the ongoing as well as discrete events performed by the nodes in both wired and wireless networks. It can, therefore, give the clear picture of experimental progress.

A. Simulation Parameters

In proposed work we have created a dense network as compared to the earlier one [21]. The network is consisting of count of wired and wireless nodes which in result are creating a hybrid network. Hence, the access points are also more than one from where the foreign node can request for the connectivity. There are thus following parameters used to create a new proposed network:

Table 1: Resources for Proposed Network

S.No.	Parameters	Details
1.	Simulator	NS2
2.	Simulation Time	50 seconds
3.	Protocol	AODV
4.	Number of Nodes	50
5.	OSI layer	MAC
6.	Traffic Model	BR, TCP, FTP

B. ExperimentalResults

Here in the following graphs the red line shows earlier technique and the green line shows the proposed technique in different scenarios:

(i) *End to End Delay:* It is lucid from the delay analysis, as shown in Fig-1 that the earlier technique shows the greater delay with attack and traffic whereas on the other hand there is a consistent delay in the proposed work which is far less than the earlier one.

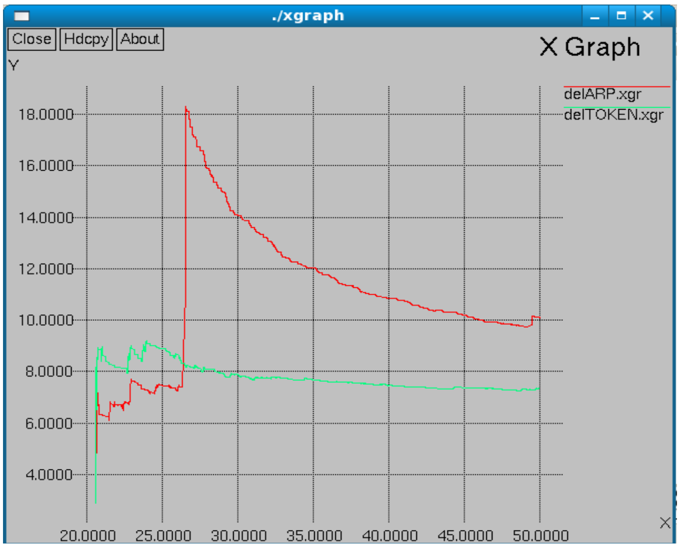

Fig-1: End to End Delay

(ii) *Packet Data Fraction(PDF):*In data rate, after 30sec of simulation we operate heavy congestion i.e. dense traffic which includes CBR, TCP and FTP which in resultant gives downfall of PDF value. In comparison to both techniques, token based approach still has better results than previous ARP spoofing solution.

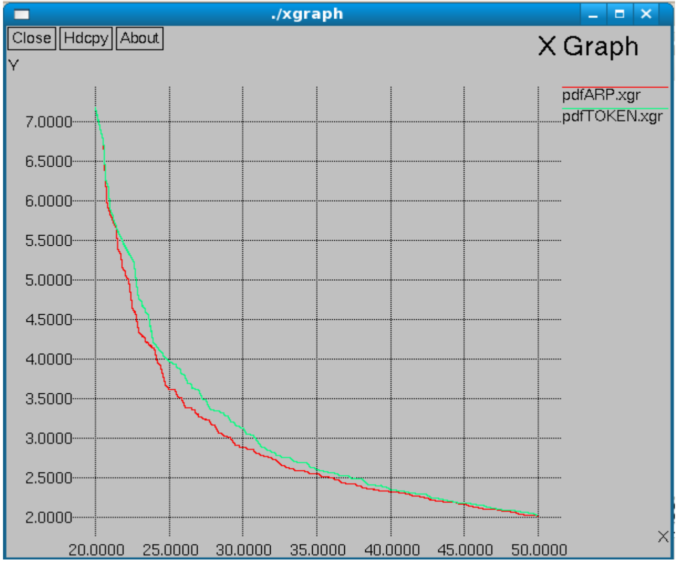

Fig-2: Packet Data Fraction

(iii) *Throughput:* At initial stage, the value of proposed work surged to 800kbps which later on decreased after 30sec of simulation time. It is because the multiple traffic has been added at that time.

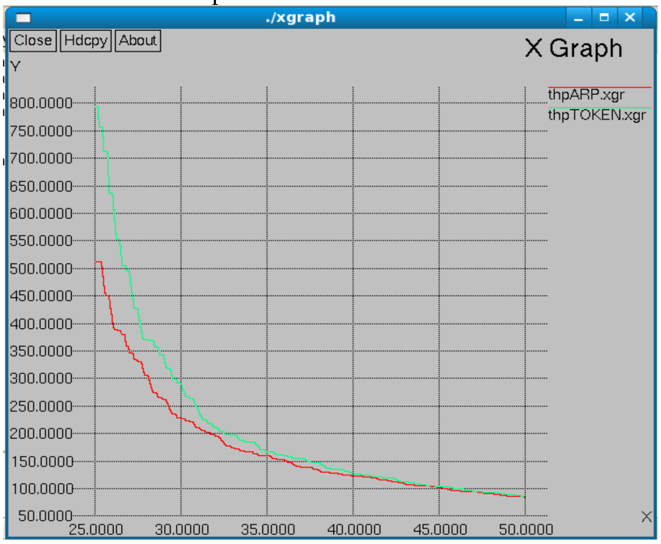

Fig-3: Throughput

VIII. CONCLUSION AND FUTURE WORK

In the current work we have seen that, the attacks can be occurred from any layer. But it is also observed that security at MAC is very weakest and can be easily attacked. Henceif any intrusion takes place at the MAC layer then the whole network will suffer. Thus security at MAC layer is addressed and the concept of Token Based ARP is introduced, which not only controls the intrusions but also reduces the complexity that has been occurred with earlier techniques such as memory table overhead. The previous solutions were also observed and the overheads were determined where network performance was hampering. Since in previous works we observed two complexities one is memory storage table, and second one is Mapping of IP to MAC address. In future we will present the modified version of IP to MAC address in the network.

REFERENCES

[1] Ahmed M.Abdel Salam, Wail S.Elkilani and Khalid M.Amin, “An Automated approach for Preventing ARP Spoofing Attack using Static ARP Entries”, *International Journal of Advanced Computer Science and Applications,* Volume 5, Number 1, 2014

[2] Alberto Lopez Toledo, “Robust Detection of MAC Layer Denial-of-Service Attacks in CSMA/CA Wireless Networks*”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,* Volume 3, Number 3, September 2008

[3] Amit Kumar Tyagi, Surendra Kumar Tyagi, Prafull Kumar Singh, “A Novel Approach to Detect and DefenceagainstAddress Resolution Protocol (ARP) Spoofing Attack*”, International Journal of Advanced Research in Computer Science and Software Engineering,* Volume 4, Issue 2, February 2014

[4] Chundong Wang, Quancai Deng, Qing Chang,Hua Zhang and Huaibin Wang “ A New Intrusion Detection System Based on Protocol Acknowledgement”, *IEEE*, 2010

[5] FatemehBarani and Mahdi Abadi*,”* An ABC-AIS Hybrid Approach to Dynamic Anomaly Detection in AODV-based MANETs*”,*in *International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11*, 2011

[6] Ferdous A Barbhuiya, Santosh Biswas and Sukumar Nandi, “AN ACTIVE HOST-BASED INTRUSION DETECTION SYSTEM FOR ARP-RELATED ATTACKS AND ITS VERIFICATION”, *International Journal of Network Security & Its Applications (IJNSA),* Volume 3, Number 3, May 2011

[7] Jatinder Singh, “A MAC Layer Based Defense Architecture for Reduction-of-Quality(RoQ) Attacks in Wireless LAN*”, (IJCSIS) International Journal of Computer Science and Information Security*, Volume 7, Number 1, 2010

[8] Jyh-How Huang, Jason Buckingham, and Richard Han,” A Level Key Infrastructure for Secure and EfficientGroup Communication in Wireless Sensor Networks”in*Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*,0-7695-2369-2/05,*IEEE*,2005

[9] Khalil El-Khatib,”Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems*”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, Volume-21, Number-8,* August 2010

[10] KiranDhangar, Prof. Deepak Kulhare, Arif Khan, “Intrusion Detection System (A Layered Based Approach for Finding Attacks)”, *International Journal of Advanced Research in Computer Science and Software Engineering,* Volume-3, Issue-5, pp. 277-283, May 2013

[11] M. Thangavel and P. Thangaraj, “Efficient Hybrid Network (Wired and Wireless) Intrusion Detection using Statistical Data Streams and Detection of Clustered Alerts”, *Journal of Computer Science7 (9): 1318-1324,* 2011

[12] NavidBehboodian and ShukorAbdRazak, “ARP Poisoning Attack Detection and Protection in WLAN via Client Web Browser”, *International Conference on Emerging Trends in Computer and Image Processing (ICETCIP'2011,* Dec. 2011

[13] Rafsanjani K, Movaghar A, and KoroupiF,“Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes,” *in Proceedings of WorldAcademy of Science, Engineering andTechnology,* Canada, pp. 123-128, 2008.

[14] Rui Xu, Zemao Zhao, Fei He, “DDoS Attacks at MAC Layer in Tactical Mobile Ad hoc Networks”, in *International Conference on Communications and Intelligence Information Security, IEEE,* 2010

[15] *SafaaZaman and FakhriKarray,”*TCP/IP Model and Intrusion Detection Systems*”,* in *International Conference on Advanced Information Networking and Applications Workshops, IEEE*, 978-0-7695-3639-2/09, 2009

[16] SeungYeob Nam, SirojiddinJurayev, Seung-Sik Kim, Kwonhue Choi and Gyu Sang Choi, “Mitigating ARP poisoning-based man-in-themiddleattacks in wired or wireless LAN*”, Nam et al. EURASIP Journal on Wireless Communications and Networking,* 2012

[17] Shafiullah Khan, Kok-Keong Loo, and Zia UdDin, “Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks”, *The International Arab Journal of Information Technology,* Volume-7, Number-4, October 2010

[18] Mrs. Sneha Kumari, Dr. Maneesh Shrivastava,"A Study Paper on IDS Attack Classification Using Various Data Mining Techniques" *International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970),*Volume-2, Number-3, Issue-5, September-2012

[19] S.Venkatramulu, Dr.C.V Guru Rao, "Various Solutions forAddress Resolution Protocol Spoofing Attacks*", International Journal of Scientific and Research Publications,ISSN 2250-3153,* Volume 3, Issue 7, July 2013

[20] S.Vidya and R.Bhaskaran,"A Subnet Based Intrusion Detection Scheme for Tracking down the Origin of Man-In-The-Middle Attack", *International Journal of Computer Science Issues,* Volume 8, Issue 5, Number 1, September 2011

[21] TapanP.Gondaliya, Maninder Singh, "Intrusion Detection System on MAC Layer for Attack Prevention in MANET*", IEEE – 31661, 4th ICCCNT,July 4-6,* 2013