International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 141-144
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

A NOVEL APPROACH FOR DETECTION AND PREVENTION OF DOS ATTACK IN WIRELESS MESH NETWORK

Devi Prasad Mishra
Department of CSE
Guru Nanak Institute of Technology,
Hyderabad, Telangana, India

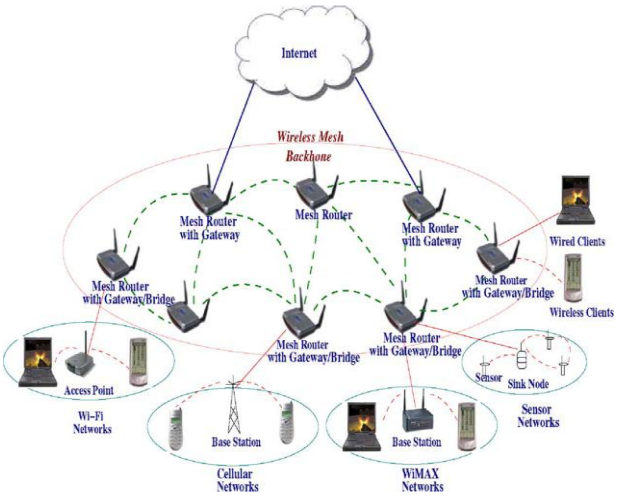
Nusrath Khan
Department of CSE
Guru Nanak Institute of Technology
Hyderabad, Telangana, India

***Abstract*— In Present era communication is the most prominent factor for any person. Wireless Sensor Network is one of the advanced key technology through which we can communicate without any pre-existing communication infrastructure. It is very popular due to low cost, simplicity, good performance and more area coverage. But with all these advantages security issues is the disadvantage in WMN. Due to its open nature and distributed nature attacker can easily interrupt the service by using many kind of attacks. Out of all the attacks Denial of service attack is a great threat because it will interrupt the service and is very difficult for prevention. In this paper we are focusing on how to detect the DOS attack and an approach to prevent the attack by using Co-operation mechanism.**

Keywords— **Wireless Sensor Network, DOS attack, Co-operation mechanism**

I. INTRODUCTION

The wireless mesh network [WMN] is a new broadband Internet access technology. WMN offer the high bandwidth Internet access for mobile users by using the multi-radio technology. WMN comprised of two types of nodes: Mesh Routers and Mesh Clients. Mesh routers is equipped with multiple radios to perform routing and access functionalities.
Mesh Clients can be user devices with wireless network card, like PCs laptop, PDAs and mobile phones. They have limited energy, computing power and radio range.



Security is a vital problem in the design of WMN. The client should have end-point to end-point security assurance. However, being different from wired and traditional wireless network, WMN could easily be comprised by various types of attack. Even the WMN infrastructure like MR could be relatively more easily reached and modified by attackers. Therefore, appreciate security measures should be taken.
The WMN is vulnerable to Denial- of Service [DoS] attacks due to the vast coverage area and dense deployment of wireless mesh routers. DoS is the most server security threat. As DoS can compromise the availability & integrity of the service. DoS attack prevent the legitimate user to access the service. In DoS attack the attacker target is MRs as it form the backbone of WMN. One of the best example of this loss is the attacks of Yahoo, CNN, and Amazon in Monday February 7th of 2000 which had an estimated loss of several million to over a billion dollars [3].

II. SECURITY

Security is a vital problem in the design of a WMN. The client should have end-point-to-end-point security assurance. However, being different from a wired and traditional wireless network, a WMN could easily comprise various types of attacks. Even the WMN infrastructure like MR could be relatively more easily reached and modified by attackers. Common security threats in a WMN are listed below:

II.I-Physical Threat: Generally, routers in wired networks are properly protected. Therefore, the attack toward the routers in a wired network is difficult. However, the routers of a WMN are usually deployed outdoors like on roofs of buildings or on street lamps. Therefore, physical protection to the routers of a WMN is very weak. This could cause the attacks to the routers like tempering the information in the router, stealing the private key for authentication stored in the router, or even replacing the router with a malicious one and hence the attacker will be able to connect to network as a legal node and send incorrect routing information. Therefore, secure

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 141-144
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

routing protocols are essential to fight against this kind of attack.

II.II-System Threat:

II.II.I- Wormhole Attacks: Two distant points in the network are connected by a malicious connection using a direct low-latency link called the wormhole link. The wormhole link can be established by a variety of means, e.g., by using an Ethernet cable, long-range wireless transmission, or an optical link. Once the wormhole link is established, the attacker captures wireless transmissions on one end, sends them through the wormhole link, and replays them at the other end.
It is a simple illustration of a wormhole attack. From node A to node D, the normal route should be A-B- C-D. However, if an attacker connects nodes M1 and M2 using a wormhole link, the route becomes S-M1- M2-D; the malicious nodes, i.e., M1 and M2, could then start dropping packets and cause network disruption. The attacker can also spy on the packets going through and use the large amount of information gained to launch other types of attacks and comprise the security.

II.II.II- Black hole Attack: While receiving the routing request, the attacker claims to have a link to the destination node even if there is not any and then forces the source to send the packet through it without forwarding the data packet to the next hop.

II.II.III- Rushing Attack: In on-demand routing protocols, the attacker sends a lot of routing request packets across the network in a short interval of time keeping other nodes busy from processing legal routing request packets.

II.II.IV-DoS Attack: Attackers could send a large amount of useless packets like a routing request packet or a data packet, depleting the resource of network and nodes, such as bandwidth, memory, CPU, or battery.

III. EXISTING MECHANISM

The main aim of research community is to protect wireless mesh network from security attacks, mainly from DoS attacks against the APs, because they are the back bone of the network as they are working in the middle level. If we can protect the APs there are a less chances of DoS attacks and interruption in the network. Gateways are serving many APs and are directly connected with the wired internet infrastructure. So if the attacker successfully attacks the gateways, its impact is very high and it may leads to the zero service of the network. So to make our service without any disturbance and to avoid the zero-service situation, we have to make necessary arrangement to protect our Wireless Mesh Network. For that APs are using mutual Cooperation Mechanism.
Mechanism:
When a new AP will join the WMN, it is going to send one packet to all its neighoubor APs. When the neighoubor existing AP get the packet from new AP it will perform the following steps.
1st step-Neighbour database is going to store the new AP information which contains Service Set Identifier(SSID), IP and MAC address.
2nd Step-Gateway will recive one report containing the SSID, MAC and IP address of the newly joined AP.Then the information is checked with the help of APs database containg SSIDs, IP address,MAC address and the neighbours of the IP. If getway found the same information is already exiting then it treated it as cloned AP, otherwise normal. Once the gateway makes the decision that the new AP is normal, an acknowledgement message is send to all its neighbours that they can route the traffic, if the newly added AP is cloned, then the gateway informs all its neighbours not to route the traffic through it.
Limitation: If one attacker is successful in adding one new APs with the gateway it can interrupt the network by using DoS attack which may leads to the zero-service situation. It's very difficult to identify the attacker node once it is added in the network.

IV. PROPOSED SYSTEM

All the APs in WMNs network are categorized as well known, known, or unknown based on their relationships with their neighboring APs. During network initiation all APs will be unknown to each other. A trust estimator is used in each node to evaluate the trust level of its neighboring APs. The trust level is a function of parameter like length among APs within their transmission range. Accordingly, the neighbors are categorized into well known, known, or unknown.
the relationship of a AP to its neighbor AP can be any of the following types
(i) AP i is a Un Known (U) to neighbor AP j:AP i have never sent/received messages to/from node j. Their trust levels between each other will be very low.
(ii) AP i is an Known (K) to neighbor AP j:AP i have sent/received few messages from node j. Their mutual trust level is neither too low nor too high to be reliable. The chances of malicious behavior will have to be observed.
(iii) AP i is a well known (W) to neighbor AP j:AP i have sent/ received many meaages from AP j. Their mutual trust level is very high.
The above relationships are computed by each AP and a friendship table is maintained for the neighbors
Algorithm:
Begin
Set Xrw, Xrk and Xru = The threshold values for well-known, known, un- known depending upon the range of neibouring AP.
If an intermediate AP receives RREQ flooding packet from AP 'i'then

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 141-144
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

If AP 'i' is a well known
If X[i] > Xrw
Drop the RREQ packet
else
Forward the RREQ packet
If AP 'i' is an known
If X[i] > Xrk
Drop the RREQ packet
else
Forward the RREQ packet
If AP 'i' is an unknown then
If X[i] > Xru
Drop the RREQ packet
else
forward the RREQ packet
End

Let X[i] denotes the number of packets delivered from neighboring AP i, where $1 \leq i \leq n$. Xrw, Xrk and Xru are the threshold values set for well-known, known, un- known. The algorithm for preventing RREQ flooding is as given above. The algorithm to prevent DATA flooding is similar to the algorithm discussed above. The threshold values for DATA flooding can be set as per the requirements of the application software

V. RESULT

Simulations are carried out to test the performance of the flooding attack prevention algorithm over AODV protocol in matlab. Compromised APs are introduced into the network which involve in RREQ flooding. The simulation setup is carried out taking 20 number of APs in WMNs is shown in Fig 1.

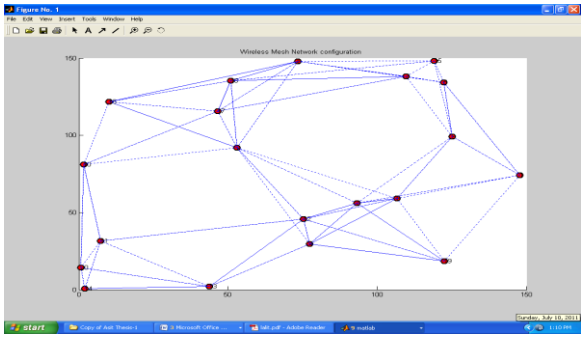


Figure 1: Screenshot of WMN setup

The source APs are AP1, AP2, AP3 . The destination APs are AP16 AP17 AP18. The trust levels for neighbors are determined by the APs. Fig. 2: shows the routing traffic sent by a malicious AP in a compromised network. The volume of routing information received by the victim AP will deprive it of its resources. Most of the victim AP energy will be exhausted by listening to the routing traffic sent by the malicious neighbor.

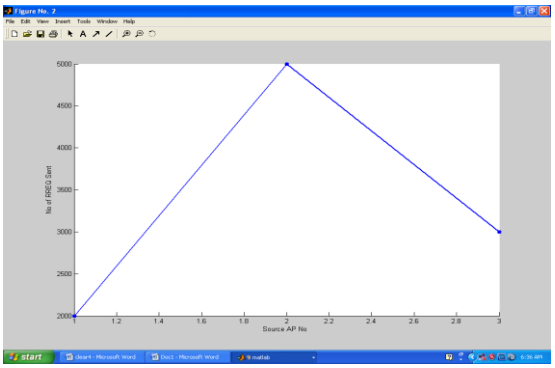


Figure 2: Flooding of RREQ packets by neibouring APs

Figure 3 shows Flooding of RREQ packets dropped by neibouring source APs by using our proposed algorithm.

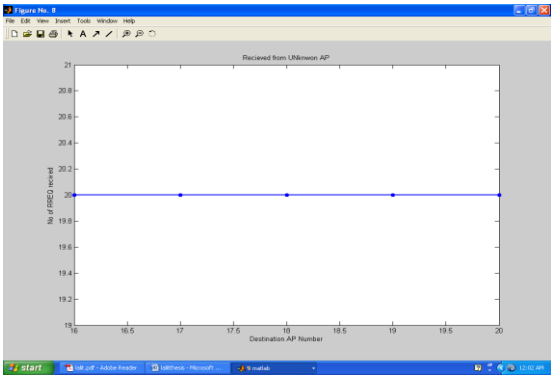


Figure 3: Flooding of RREQ packets dropped by neibouring source APs

In the default setup shown with blue line in Fig 4: the APs communicate using the AODV protocol which shows the degradation in throughput of the network and increased delay in the presence of malicious nodes. With the implementation of flooding attack prevention algorithm over AODV, the flooding attacks are constrained and this results in increased throughput and reduced delay shown in red line.
Fig. 4 shows the increase in the throughput of the network improvised with the prevention algorithm. All the nodes in the network monitor the threshold values of their respective neighbors. If the neighbors exceed their limit in sending the RREQ packet, they are immediately droped,as shown in Fig 3. Hence the neighboring nodes do not waste their energy, involving in superfluous traffic information. Their resources are conserved. This results in the overall improvement in the throughput of the network. Additionally, The decrease in the delay of packet traffic in the network due to reduction in the volume of routing traffic by malicious APs. By using this the unnecessary traffic in the network is reduced and hence the

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 141-144
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

APs are able to process the data traffic and send to the destination in less time.

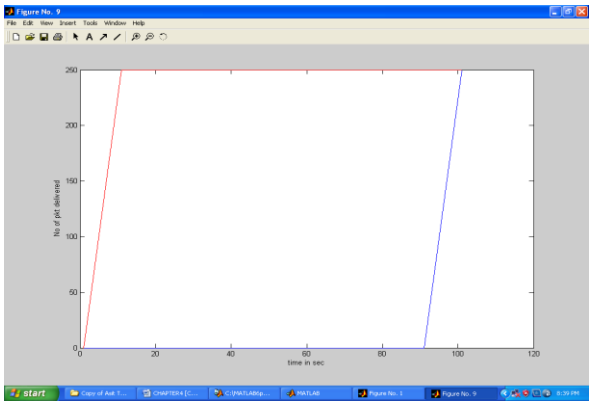


Figure 4: Comparison of RREQ delivered with flooding and droping packets

VI. CONCLUSION

WMNs networks exhibit new vulnerabilities to malicious attacks or denial of cooperation. We work on security issues and trust establishment schemes. A proposal to effectively prevent flooding attack using AODV Protocol is discussed and also implemented. A better understanding and modeling of the security attacks is needed in WMNs if efficient secure routing algorithms are to be built in the network. Our future work will include simulation and performance analysis of our proposed flooding attack prevention and to develop comprehensive models for security attacks and a trustworthy security framework against all possible security attacks in WMNs.

VII. REFERENCE

[1] I.F. Akyildiz and Xudong Wang. A survey on wireless mesh networks. Communications Magazine, IEEE, 43(9):S23 – S30, sept. 2005.

[2] Shafiullah Khan, Kok-Keong Loo, Tahir Naeem, and Mohammad Abrar Khan. Denial of service attacks and challenges in broadband wireless networks," International Journal of Computer Science and Network Security, Vol. 8, No. 7, pp.1-6, July 2008.

[3] Amitabh Mishra, "Security and Quality of Service in Ad hoc Wireless Networks,"pp. 42-57, Cambridge University Press, 2008.

[4] C.Siva Ram Moorthy, B.S. Manoj: Ad hoc Wireless Networks Architectures and Protocols, Prentice Hall, 2004.

[5] Shafiullah Khan1,2, Noor Mast1,2 and Kok Keong Loo1, Ayesha Salahuddin Cloned Access Point Detection and Prevention Mechanism in IEEE 802.11 Wireless Mesh Networks Journal of Information Assurance and Security 3 (2008) 257-262.

[6] R. Venkatesha Prasad, P. Pawtczak, J. A. Hoffmeyer, and H. S. Berger, "Cognitive functionality in next generation wireless networks: Standardization efforts," IEEE communication Magazine, Vol. 46, Issue 4, pp.72-78, April 2008.