Volume No: 1(2014), Issue No: 10 (October) ISSN No: 2348-4845

Security Framework against Denial of Service Attacks In Wireless Mesh Networks

Marpu Devadas
Student(M.Tech) , CSC,
Gokul Group Of Institutions
Visakhapatnam, India.

K.R.Koteeswa Rao
Asst. Prof, CSC,
Gokul Group Of Institutions
Visakhapatnam, India.

Abstract:

Wireless mesh networks (WMNs) are emerging as a solution for large scale high speed internet access through their scalability, self configuring and low cost. But as compared to wired networks, WMNs are largely prone to different security attacks due to its open medium nature, distributed architecture and dynamic topology. Denial of service (DoS) attacks is one of the most common types of attack which is possible in WMNs. DoS attacks are most common in networks which connect to internet and since WMNs are mainly designed for fast and long distance internet access this type of attacks are common in the network. In our work we mainly concentrate our study on two denial of service attacks namely gray hole attacks (a.k.a selective forwarding attacks) and black hole attacks. Wireless mesh networks consist of both mesh routers and mesh clients.

We confine our studies to mesh routers which are stationary. We implement both gray hole attack and black hole attack in mesh routers and study the delivery ratio of the network with and without the presence of attack routers. By simulating the scenario with AODV protocol we studied the delivery ratio of packets and find out how it is affecting the network in the presence of an attack router. After studying the results we propose a new detection algorithm based on overhearing the neighboring node to which the packet is forwarded. By keeping the history of number packets forwarded and the number of packets overheard the algorithm determines the number of packets dropped and determines the probability of attack. This probability is checked with the threshold value of probability and determines whether a router is misbehaving or not. We also considered the possibility of false positives and took necessary measures in the algorithm to reduce it. If a router is found misbehaving it is removed from the network and excluded from further forwarding of packets. We analyze our algorithm in the presence of an attack router and detect the attack router and study the improvement in the delivery ratio. Through simulation we evaluate the performance of our algorithm depending on the packet delivery ratio achieved and time.

Keyword:

Wireless mesh network, Gray hole attack, Black hole attack .

I. INTRODUCTION:

Wireless mesh networks (WMNs) are a multi-hop wireless communication among different nodes are dynamically self-organized and self-configured, with the nodes in the network automatically establishing an ad-hoc network and maintaining the mesh connectivity. WMNS are emerged as a promising concept to meet the challenges in wireless networks such as flexibility, adaptability, reconfigurable architecture etc [1]. WMNs consist of two kinds of nodes: mesh routers and meshclients. Mesh routers are routers which forms the stationary or least mobile part of the mesh network with less power constraint and forms the backbone of the mesh network.

Meshclients are nodes which are mobile in the network with power constraints. Though mesh clients can also do routing by forwarding pack- ets to the next node in mesh networking the hardware and software platform for them are much simpler compared to mesh routers. Mesh routers can do all the gateway/ bridge functions as in conventional wireless router, in addition to that it contains additional functions to support mesh routing.

They can support multiple wireless interfaces built on either the same or different wireless access technologies. Thus mesh routers are dedicated and stationary nodes for routing functions with less power constraint. Mesh clients are nodes with no gateway/ bridge functions and only one wireless interface is needed in mesh clients. Wireless mesh networks can be integrated with other networks because of the bridge/gateway functions provided by the mesh router. The presence of mesh routers and hop by hop forwarding in WMNs bring many advantages compared to conventional ad-hoc network such as low up-front cost, higher scalability, easy network maintenance, robustness, reliable and need less transmission power.

A wireless mesh network enables ad-hoc mode peer to peer interconnection among mesh clients are is called client meshing [1]. With client meshing, mesh routers that stay outside the radio coverage of a mesh router can rely on other intermediate clients to relay packets to them to get WMN access network connections. Thus packets from a mesh client which lies far away from the mesh router has to travel multi hop client-to-client and client-to-router wireless link before reaching its destination.

The number of hops is determined by the geographical location of the client and also the organization structure of the access network. The architecture of wireless mesh networks can be classified in to three main groups based on the functionalities of the nodes namely infrastructure/backbone WMNs, client WMNs and Hybrid WMNs.

In infrastructure WMNs wireless mesh routers will form a mesh of self-configuring, self healing links among themselves. With gateway functionality these routers can be connected to the internet. This approach provides backbone for conventional clients and enables integration of WMNs with existing wireless networks, through gateway/bridge functionalities in mesh routers.

In client meshing the client devices will form a mesh to perform routing and configuration functionalities as well as providing end-user applications to users. In this architecture no mesh routers are present and thus are same as the conventional ad-hoc network. Hybrid WMNs is the combination of infrastructure and client meshing and a mesh network is formed between the clients and as well as the routers. Mesh clients can access the network through mesh routers as well as directly meshing with each other.

II. WIRELESS MESH NETWORKS:

2.1 Introduction:

Wireless Mesh Network is a promising wireless technology for several emerging and commercially interesting applications, e.g., broadband home networking, com- munity and neighborhood networks, coordinated network management, intelligent transportation systems. It is gaining possible attention as a possible way for Inter- net service providers and other end-users to establish robust and reliable wireless broadband service access at a reasonable cost. Different from traditional wireless networks, nodes in WMN automatically establish and maintain network connec- tivity. This feature brings many advantages for the end-users, such as low up-front cost, easy network maintenance, robustness, and reliable service coverage [3]. The gateway and bridge functionalities in mesh routers enable the integration of wire- less mesh networks with various existing wireless networks, such as wireless sensor networks, wireless-Fidelity (Wi-Fi), and WiMAX [1].

2.2 Network Architecture:

As mentioned in chapter 1, the architectures in wireless mesh network can be classified in to three different types.

2.2.1 Infrastructure/Backbone WMNS:

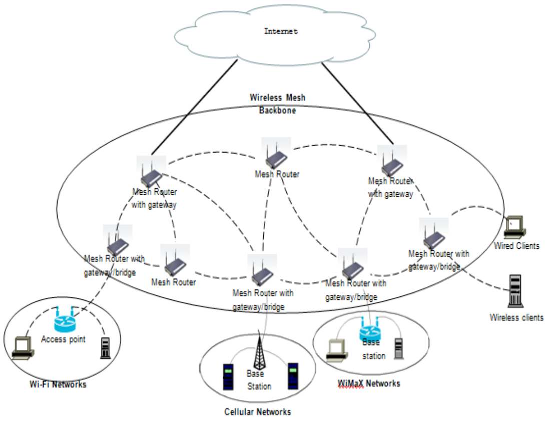


Figure 2.1: Infrastructure/backbone WMNS

2.2.2 Client WMNS:

In this architecture clients form a mesh network among themselves and no routers exist. The clients will establish peer-to-peer networks among them and consti- tute the actual network performing routing and configuration functions as well as providing end-user applications to costumers. The clients will communicate using a single radio interface among the devices and a packet is forwarded to des- tination by hopping through the device. Thus, a Client WMNs is same as the conventional ad-hoc network. By comparing with the Infrastructure WMNs the requirements on the clients increased in Client WMNs because the end-users must perform additional functions such as routing and self-configuration.

2.2.3 Hybrid WMNS:

Hybrid WMN is a combination of both Infrastructure and Client WMN in the sense that both the routers and clients will form mesh networking [1].

Routers will form the backbone by meshing each other and the clients can form mesh network among themselves for communicating hop-by-hop each other and to connect to the backbone router.

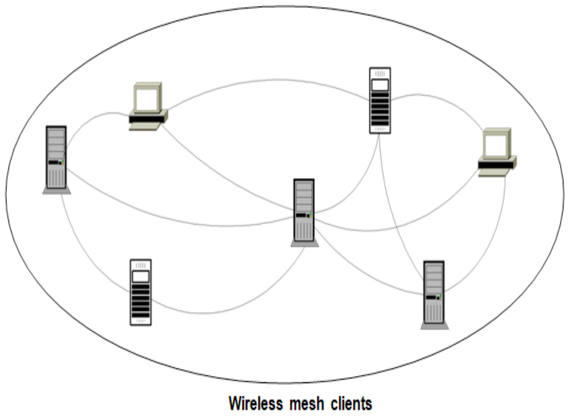


Figure 2.2: Client WMNS.

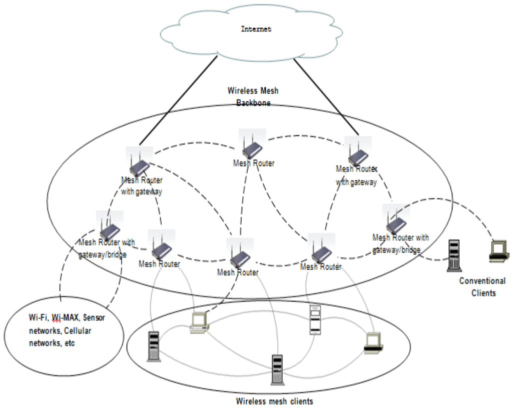


Figure 2.3: Hybrid WMNS.

III. GRAY HOLE AND BLACK HOLE ATTACKS:

In this work we focus our attention to two special type of Denial of Service (DoS) attacks called gray hole attack or selective dropping attack and black hole attack or sink hole attack. We consider these attacks on the less mobile or almost stationary wireless mesh routers. Gray hole attack is a type of attack in which the attack router accepts the packets and refuses to forward certain packets by just dropping the packets. In black hole attack the attack router will advertise in the network that it has a fresh route to the destination and after that may drop all the packets that it receives. Cryptographic techniques are used to protect the physically unprotected mesh routers from various DoS attacks including gray hole and black hole attacks. But if the router is compromised the attacker will gain access to the private/public key pair of the router and can break through the cryptographic systems. Thus non-cryptographic methods will provide a second line of defense [14], [15]. In this work we try to develop a non cryptographic type of defense by checking the forwarding of the upstream routers by overhearing their transmission.

We consider AODV routing protocol to implement these attacks.

3.1 Ad-hoc On-Demand Distant Vector (AODV) routing protocol:

AODV protocol is one of the commonly used in wireless mesh networks and is proposed as one of the protocol in the IEEE 802.11s standard [16]. AODV is a re- active distance vector routing protocol which will establish the path only when the router has some data to send. AODV borrows the basic route establishment and maintenance mechanisms from the Dynamic Source Routing protocol (DSR) and the hop-to-hop routing vectors from the Destination-Sequenced Distance-Vector protocol (DSDV). To avoid routing loops AODV makes use of the sequence number in the control packets.

3.2 Black hole attacks:

In a black hole attack the malicious node will always advertise in the network that it has a fresher route to the destination by setting the sequence number to a large value and will reply to the RREQ before other routers send a reply. Thus the attacker router will attract all the traffic in its transmission range towards itself and then may drop the packets [17].

3.3 Gray hole attacks:

In a wireless mesh network that uses AODV protocol one attacker node can drop some selected packets according to some criteria or randomly. This is called gray hole attack or selective drop attack. This type of attack is very difficult to detect, especially in the wireless scenario, because packets can be dropped because of line congestion, channel capacity, etc. In the simulation we used random dropping of packets using the random function. While the packets are sending to destination, packets are dropped randomly by the malicious node. Simulation of gray hole attack is done on ns-2.34 [18]. In order to simulate gray hole attack on ns2 we had to modify and implement the existing AODV protocol.

IV. PROPOSED ALGORITHM:

When a node wants to send a packet it will send the RREQ packet and if it receives a route reply first from a normal behaving node, then everything will work fine. But if it gets reply from an attacker node in which implements selective dropping all the packets will not reach the destination.

4.1 Related Work:

Most of the prior works related to gray hole attacks were studied in the area of ad hoc and sensor networks. These works can be used in the area of wireless mesh networks too. But since wireless mesh networks are mainly targeting the broadband usage these type of attacks will be more common in wireless mesh networks compared to other two networks. So more research work is needed in the field of security in WMNs.Karlof.et.al [19] proposed selective forwarding attack for the first time in wireless sensor networks and suggested that multi path forwarding can used to counter the attack.

4.2 Assumptions:

We assume that all the routers that are in the network are stationary and have no energy constraints. We also assume that the wireless interfaces support promis- cuous mode operation. Promiscuous mode means that if a node A is within range of a node B, it can overhear communications to and from B even if those commu- nications do not directly involve A.

4.3 Parameters and Thresholds:

Before going in to details about the algorithm, we introduce the parameters and threshold values used in the algorithm. At each router nt denotes the number of packets transmitted under a particular threshold to the downstream node. This threshold is denoted as nthreshold . At the same router no denotes the number of packets overheard by the router.

4.4 Attack Detection Algorithm:

We present an algorithm for finding the intentional selective dropping attack by a node and if all the packets are dropped will identify the attack as a black hole attack by checking the forwarding of packets by the immediate neighbor downstream node to which the data is sent. For this we have to overhear the traffic by the neighboring nodes.

4.5 Result of Simulation:

First we simulated the network with no attack node and checked the delivery ratio of the data sent.Delivery ratio is the performance metric used and is the ratio of the data received by destination to the data sent which is expressed in percentage. In the absence of attack the delivery ratio obtained is 100.Then we introduced a malicious node in the network which will implement gray hole attack and drop packets in a random fashion as explained earlier. Router 6 is selected as the attack router which is in the path of the transmission. Since the node 2 and node 5 is sending UDP packets no acknowledgement is sent back by the destination node 7. The delivery ratio is calculated using the data received by node 7 to the data sent by node 2 and node 5. As expected node 6 drops some packets randomly and the delivery is decreased from 100 to a range of 45-60 as shown in Figure 4.1.

Similarly we implemented the black hole attack to router 6 and checked the delivery ratio and the ratio was coming down from 100 percentage to zero.

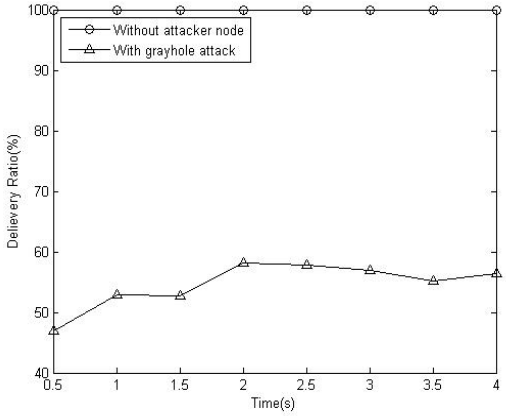


Figure 4.1: Comparison between delivery ratio of network with and without gray hole attack

4.6 Simulation of the Proposed Algorithm:

Previously we implemented both gray hole and black hole attack in ns-2.34 and obtained the results. Since we were not able to implement the promiscous mode of operation in ns-2.34 it become impossible to overhear the transmission of the neighbouring router. So we have written our algorithm in Perl language [21] and using the trace files obtained during the previous simulation.

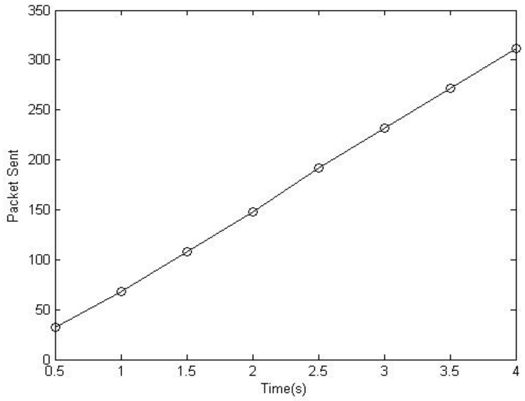


Figure 4.2: Packet sent

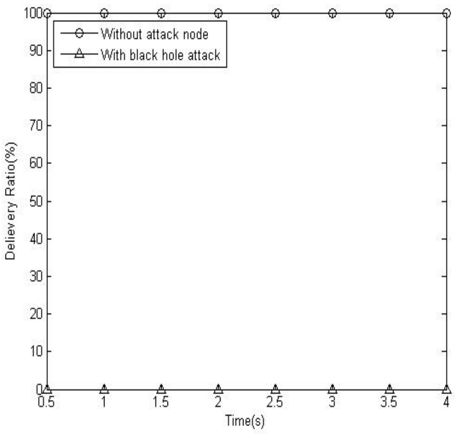
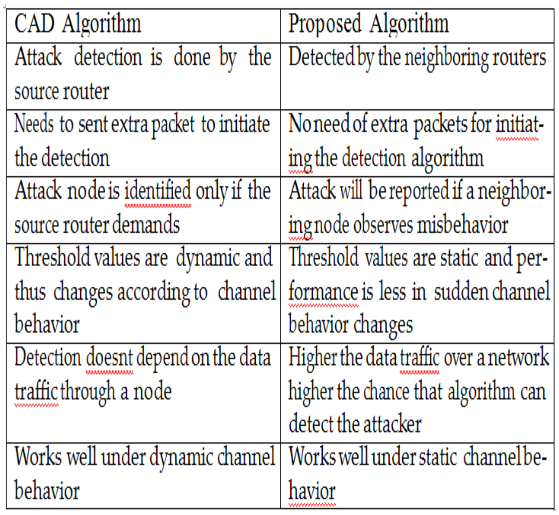


Figure 4.3: Comparison between delivery ratio of network with and without black hole attack

4.7 Comparison of Proposed Scheme with CAD Algorithm

Table 4.1: Comparison of proposed algorithm with CAD



CAD Algorithm	Proposed Algorithm
Attack detection is done by the source router	Detected by the neighboring routers
Needs to sent extra packet to initiate the detection	No need of extra packets for initiating the detection algorithm
Attack node is identified only if the source router demands	Attack will be reported if a neighboring node observes misbehavior
Threshold values are dynamic and thus changes according to channel behavior	Threshold values are static and performance is less in sudden channel behavior changes
Detection doesnt depend on the data traffic through a node	Higher the data traffic over a network higher the chance that algorithm can detect the attacker
Works well under dynamic channel behavior	Works well under static channel behavior

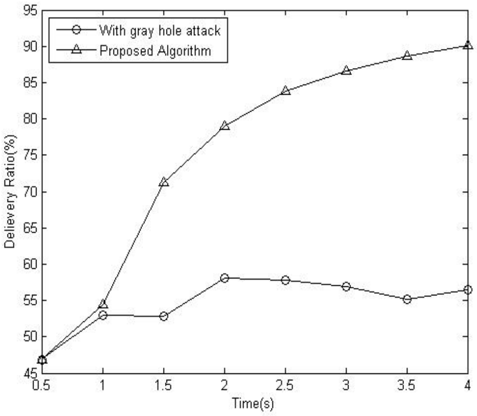


Figure 4.4: Comparison between gray hole attack and proposed algorithm with Pg =.35, nthreshold =10,interval=5

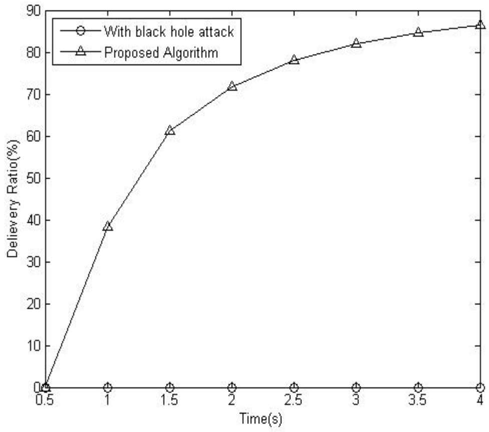


Figure 4.5: Comparison between black hole attack and proposed algorithm with Pb =.35, nthreshold =10,interval=5

CONCLUSION:

Since routers in WMNs work in a fully wireless environment the packet can be lost due to different factors. So finding an appropriate threshold value for detecting the gray hole attack in real environment is really difficult. Wireless mesh networks is having an open architecture and more prone to Denial of Service attacks due to its use in broadband internet access.Thus more research work has to be done to reduce the Denial of Service attacks and improve the network.

REFERENCES:

[1] I.F. Akyildiz and Xudong Wang. A survey on wireless mesh networks. Com- munications 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 net- works.

[3] L. Santhanam, D. Nandiraju, N. Nandiraju, and D.P. Agrawal. Active cache based defense against dos attacks in wireless mesh network.In Wireless Pervasive Computing, 2007. ISWPC '07. 2nd International Symposium on, feb. 2007.

[4] S. Ghannay, S.M. Gammar, F. Filali, and F. Kamoun. Multi-radio multi- channel routing metrics in ieee 802.11s-based wireless mesh networks and the winner is;. In Communications and Networking, 2009. ComNet 2009. First International Conference on, pages 1 –8, nov. 2009.

[5] Choong Seon Hong Muhammad Shoaib Siddiqui. Security issues in wireless mesh networks. In International Conference on Multimedia and Ubiquitos Engineering. IEEE Computer Society, IEEE, 2007.

[6] D. Makaroff, P. Smith, N.J.P. Race, and D. Hutchison. Intrusion detection systems for community wireless mesh networks. In Mobile Ad Hoc and Sensor Systems, 2008. MASS 2008. 5th IEEE International Conference on, pages 610 –616, 29 2008-oct. 2 2008.

[7] S. Seth and A. Gankotiya. Denial of service attacks and detection methods in wireless mesh networks. In Recent Trends in Information, Telecommunicationand Computing (ITC), 2010 International Conference on, pages 238 –240,march 2010.

[8] M. Arora, R.K. Challa, and D. Bansal. Performance evaluation of routing protocols based on wormhole attack in wireless mesh networks. In Computer and Network Technology (ICCNT), 2010 Second International Conference on, pages 102 –104, april 2010.

[9] M. Medadian, M.H. Yektaie, and A.M. Rahmani. Combat with black hole attack in aodv routing protocol in manet. In Internet, 2009. AH-ICI 2009. First Asian Himalayas International Conference on, pages 1 –5, nov. 2009.

[10] A. Patcha and A. Mishra. Collaborative security architecture for black hole attack prevention in mobile ad hoc networks. In Radio and Wireless Confer- ence, 2003. RAWCON '03. Proceedings, pages 75 – 78, aug. 2003.

[11] L. Lazos and M. Krunz. Selective jamming/dropping insider attacks in wire- less mesh networks. Network, IEEE, 25(1):30 –34, january-february 2011.

[12] D.M. Shila and T. Anjali. Defending selective forwarding attacks in wmns. In Electro/Information Technology, 2008. EIT 2008. IEEE International Con- ference on, pages 96 –101, may 2008.

[13] Guorui Li, Xiangdong Liu, and Cuirong Wang. A sequential mesh test based selective forwarding attack detection scheme in wireless sensor networks. In Networking, Sensing and Control (ICNSC), 2010 International Conference on, pages 554 –558, april 2010.

[14] D.M. Shila, Yu Cheng, and T. Anjali. Mitigating selective forwarding attacks with a channel-aware approach in wmns. Wireless Communications, IEEE Transactions on, 9(5):1661 –1675, may 2010.

[15] D.M. Shila, Yu Cheng, and T. Anjali. Channel-aware detection of gray hole attacks in wireless mesh networks. In Global Telecommunications Conference,2009. GLOBECOM 2009. IEEE, pages 1 –6, 30 2009-dec. 4 2009.

[16] Myung J.Lee and Jianliang Zheng. Emerging standards for wireless mesh technology. IEEE Wireless Communications, April 2006.

[17] A. Prathapani, L. Santhanam, and D.P. Agrawal. Intelligent honeypot agent for blackhole attack detection in wireless mesh networks. In Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference on, pages 753 –758, oct. 2009.

[18] K. Fall and K. Varadhan. NS notes and documentation. The VINT Project, UC Berkely, LBL, USC/ISI, and Xerox PARC, 1997.

[19] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Networks, 1(2-3):293 – 315, 2003. Sensor Network Protocols and Applications.

[20] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking, MobiCom '00, pages 255–265, New York, NY, USA, 2000. ACM.

[21] Perl tutorial. www.perltutorial.org.