International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 12 | Dec -2016 www.irjet.net p-ISSN: 2395-0072

Security Frame Work against Denial of Service Attacks in Wireless Mesh Networks

Dr.T.Pandikumar[1], Zeleke Wondimu[2]

[1]Ph.D. Department of Computer & IT, College of Engineering, Defence University, Ethiopia
[2]M.Tech. Department of Computer & IT, College of Engineering, Defence University, Ethiopia

---

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 a dangerous, relatively new type of Internet based network attacks, they have caused wireless routers, switches, servers became inaccessible to customers, partners, and users, the results and losses will be disastrous and unimaginable. Therefore, for guarding our network, it is really important to have Security Frame Work against Denial of Service Attacks in Wireless Mesh Networks.*
This research paper attempts a comprehensive scoping of the DoS Attacks in WMNs namely gray hole attacks (a.k.a selective forwarding attacks) and black hole attacks, and security frame work against Attacks. Wireless mesh networks consist of both mesh routers and mesh clients. And confine to mesh routers which are stationary. it 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. With AODV protocol study the delivery ratio of packets and find out how it is affecting the network in the presence of an attack router.

Key words: Wireless Mesh Networks, DoS, Gray Hole, AODV, DSR, Hybrid, QoS.

1. 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 mesh clients. 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. Mesh clients are nodes which are mobile in the network with power constraints. Though mesh clients can also do routing by forwarding packets 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. 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.

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.

Because of the self-configurable architecture of wireless mesh networks and the wide usage of WMNs for accessing internet, mesh routers and clients are prone to different type of security issues. So providing solution to the security challenges is a major research area in recent years in the fields of WMNs. WMNs are facing two broad categories of attacks such as passive attacks and active attacks. In the case of passive attack, the attackers simply analyze and listen to the network traffic with the objective of capturing sensitive information which can be used later to launch an active attack on the network [2]. Active attacks are which will directly damage the network bandwidth either by tampering, modification or just by dropping of packets. Because of the multi hop nature and ad-hoc connectivity, WMNs are prone to both kinds of these attacks. The three important features of a secure network are confidentiality, integrity and service availability. Confidentiality is compromised by passive attacks, integrity by active attacks and availability by the most severe form of active attack on internet namely Denial of Service (DoS) attacks. Since WMNs is mainly used in long distance internet access and other applications which uses internet, DoS attack is treated as the highest security risk for this network, as DoS uses internet as a platform to be launched.

Denial of Service is one of the major issues of all types of wireless mesh networks as it is mainly designed for internet access. When authorized users are not provided a request service within a defined maximum interval of time, it means that a DoS violation has occurred. It is the most harmful and dangerous attack which can be launched any layer of wireless mesh networks. Network layer is highly vulnerable to different DoS attacks due to multi-hop routing, as the number of hop increases the routing overheads increase. DoS attack in network layer can affect the routing mechanism or can degrade the network performance by exhausting the network resources. A DoS attack in network layer can be black hole attack in which a malicious node absorbs all the packets forwarded towards the target node and dropping those packets or dropping all the packets go through the malicious node. Another form of attack is the selective dropping attack or gray hole attack in which the malicious node selectively dropping some packets or randomly dropping some packets. Worm hole attack is another form of attack which will create networking disruptions. Another for DoS attack in network layer called the flooding attack in which the attacker transmits a flood of packets to the target node or to congest the network and degrade its performance [2].

In this research we deal with two types of denial of service attacks in network layer namely black hole attacks and gray hole attacks and propose a defense mechanism for detecting and eliminating the attacks. This seminar concentrates on the mesh routers alone which are the stationary part of WMNs and implemented the two attacks in Ad-hoc On-Demand Distance Vector (AODV) protocol and studied the impact of these attacks in the network. The protocols implemented are considering attacks on the data packets passed and forward the control packets without dropping. After implementing both black hole and gray hole attack as new two protocols we studied the network performance with the presence of attack node and without that. As expected the network performance of the network degrades in the presence of attack node. Afterwards we proposed a solution for eliminating the attack nodes from the network based on a detection algorithm. The algorithm is based on overhearing the neighboring nodes and observing the forwarding behavior of the nodes. For overhearing the neighboring nodes the AODV protocol should be in promiscuous mode in which the router can over hear the data forwarded by the neighboring nodes. The result shows that our solution eliminates the attacker nodes from the network and thereby improving the delivery ratio of the network.

1.1 Wireless Mesh Networks Architecture

The architectures in wireless mesh network can be classified in to three different types.

1.1.1 Infrastructure/Backbone WMNS

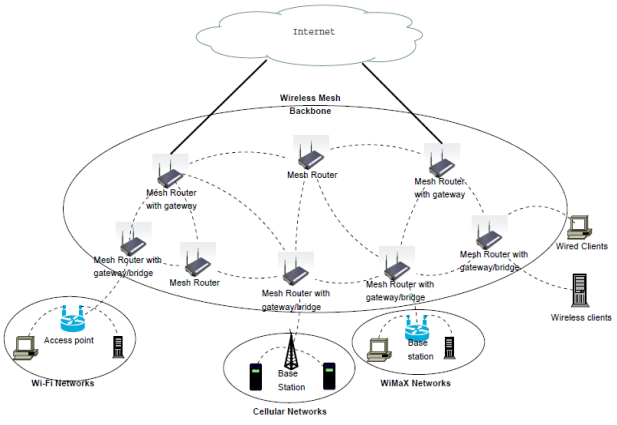

Figure 1: Infrastructure/backbone WMNS

In this architecture the mesh routers in WMNs are connected and form a mesh and will provide an infrastructure for clients, as shown in Fig. 1.1 , where solid lines indicates wired link whereas dashed lines indicate wireless links. The backbone routers can be built using different radio technologies in addition to the mostly used IEEE 802.11 technologies [1]. The mesh routers form a self- configuring and self-healing mesh among themselves. With gateway function few of the mesh routers will be connected to the internet. The conventional clients with an Ethernet interface can connect to any of the mesh routers through the Ethernet interface to communicate with others or to access the internet. These routers form a meshing known as infrastructure meshing which acts as an infrastructure to the client nodes. Clients having the same radio technology as the routers can connect directly to them others have to send packets to their access points or base stations which will be connected to the routers through the gateway for internet access. This approach enables integration of WMNs with existing wireless networks and also provides a backbone for conventional clients.

1.1.2 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 constitute 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 destination 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.

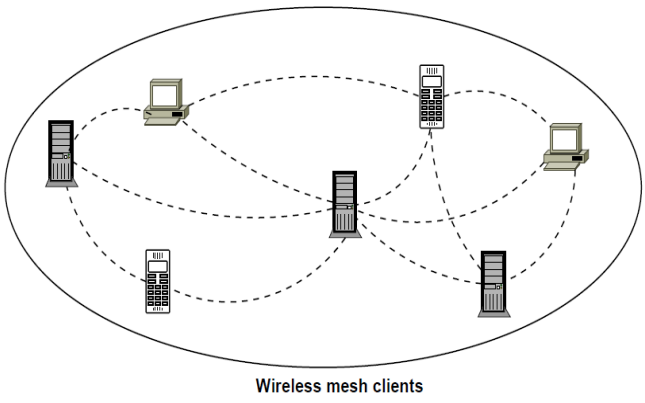

Figure .2: Client WMNS

1.1.3 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. Thus mesh clients can access the network through mesh.

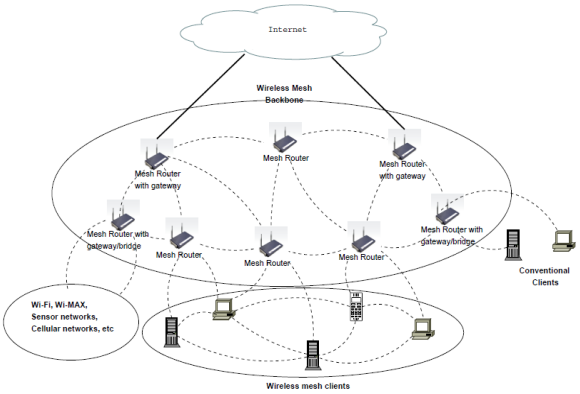

Fig 3: Hybrid WMNS

routers as well as meshing with other mesh clients. While the meshing of routers to form backbone network will provide connectivity to other networks such as internet, Wi-Fi, WiMAX, cellular and sensor networks, the routing capability of mesh clients will provide improved connectivity and coverage inside the WMNs. Since from our study of different architectures we can see that hybrid WMNs has all the advantages of a wireless mesh network.

1.2 Routing Metrics for WMNs

Most of the ad hoc routing protocols use hope count as a routing metric. In the early stages these routing metrics are also used in WMNs. These assume that the link in the path work properly or not work at all and consider all links of equal bandwidth. So in this case minimizing the hop count will reduce the packet delay and also increases the throughput. But in wireless mesh networks links are not of equal bandwidth. A minimum hop count path has higher average distance between nodes present in that path compared to a higher hop count path. This reduces the strength of the signal received by the nodes in that path and thereby increases the loss ratio at each link. Hence, it is always possible that a two-hop path with good link quality provides higher throughput than a one-hop path with a poor/lossy link. The wireless links usually have asymmetric loss rate. Hence, new routing metrics based on the link quality like ETX (Expected Transmission Count), per-hop RTT

(Round-Trip Time), and per-hop packet pair is proposed [4].

1.3 Routing Protocols in WMNs

All the routing protocols available for the prior works in wireless networks especially multi-hop ad hoc networks work well for wireless mesh networks. Thus the protocols designed for ad-hoc networks such as Ad-hoc On-demand Distant Vector Protocol (AODV), Dynamic Source Routing (DSR), and Destination Sequence Distant Vector routing (DSDV) works well with wireless mesh networks too. Since we are using AODV protocol for implementing gray hole attack in WMNs this protocol discussed in detail in Chapter 4. Here some of the protocols which are exclusively designed for wireless mesh networks by taking into consideration of the routing metrics we discussed. Since wireless mesh networks use two antennas for transmitting and receiving packets as compared to one antenna in ad hoc networks and also the link quality between different nodes in the network are not the same and to make advantage of meshing, new routing protocols are designed to improve the routing quality of WMNs. Also the routers in wireless mesh network have minimal mobility and there is no power constraint and the clients are mobile with limited power. Hence the links in wireless mesh networks are long lived compared to the links in ad-hoc networks. Since two types of nodes present in WMNs, that is the mesh routers and mesh clients some protocols even follow different routing techniques for routers and clients.

2. GRAY HOLE AND BLACK HOLE ATTACKS

In this research, 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. Consider these attacks on the less mobile or almost stationary wireless mesh routers. 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. This seminar work mainly concentrated on 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.

2.1 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 [1]

a.Flooding of RREQ
b.RREP from malicious node and other intermediate node

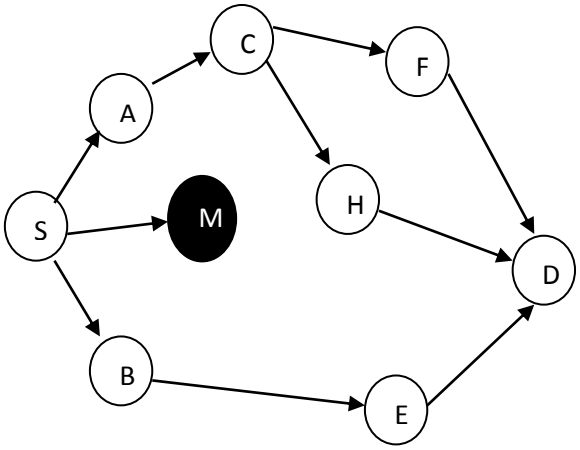

Figure 4: Black hole attack

2.2 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. It can be shown by Simulation of gray hole attack is done on ns-2.34 [18]. In order to simulate gray hole attack on ns2 researches shows that by modifying and implement the existing AODV protocol.

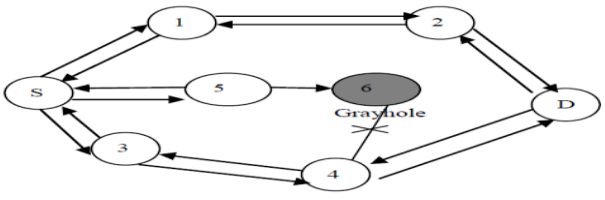

Figure 5: Grey hole attacks

2.3 Channel-Aware Detection of Gray Hole Attacks in WMNs

A gray hole attack forms a serious threat to mesh networks, particularly considering that collaboration among mesh routers is the basic requirement of such networks. An adversary may compromise these mesh routers through physical capture or software bugs, thus gaining full control of them. Once captured, the attacker gains access to all the data residing in victim node and reprogram them to behave in a malicious manner. For a path, v0, v1, v2, . . . , vn, between the source S and destination D, we assume that node v2 is a compromised router that attracts network traffic by advertising itself as having the high quality path to the destination and then performs selective forwarding attacks on the data passing through it. Suppose that source receives data from mesh client to forward to the destination D. On receiving the request for data transmission, it will check if it has an entry for node D in the routing table. If no entry is found, it will broadcasts a ROUTE REQUEST for that destination. Node v2 claims that it has a better path to destination whenever it received ROUTE REQUEST packets and sends the reply back to source. The destination or other intermediate routers may send the reply if it has a fresh route to destination. If node S receives the reply from a *normal behaving* node before it gets the reply from the attacker, everything works well.

2.4 Implementing the new Routing Protocol in NS-2 which show Gray hole behavior

Implementation of the gray hole attack is done in AODV protocol and simulated in NS-2.34. To show the gray hole behavior, one node is selected as attack node and it will drop packets randomly. The attack node should be able to participate in

```
#GAODV patch
Simulator instproc create-gaodv-agent { node } {
        #  Create GAODV routing agent
        set ragent [new Agent/gAODV [$node node-addr]]
        $self at 0.0 "$ragent start"     ;# start BEACON/HELLO Messages
        $node set ragent_ $ragent
        return $ragent
}
```

Figure 6: *ms - lib.tcl* GAODV modification

the AODV messaging. For this the new protocol which exhibits gray hole attack should be able to participate in AODV messaging. Implementation of the new routing protocol which perform gray hole attack is explained below.

All routing protocols in NS2 are installed in the ns-2.34 directory. We start by duplicating the AODV protocol in this directory and named the directory as "GAODV "(all the header files and classes of AODV directory are modified).

All the files in the AODV directory are modified with GAODV such as *gaodv.cc*, *gaodv.h*, *gaodv rqueue.cc*,*gaodv rqueue.h* etc except for *"aodv packet.h*. The new protocol will use the same aodv packets and thus its possible for the new GAODV protocol to send the same AODV packets. So we have changed all the names of classes, structures, functions in all the files except for the struct names that belong to the AODV *packet.h* code. By creating all this we have designed aodv and gaodv protocols to send packets with each other. To integrate the GAODV protocol to the NS2, two common files has to be modified. Since we are using the same packets used in AODV, we don't have to modify the common files related to packet. Thus had to modify two files [18].

The first modified file is the *ms - lib.tcl*. It's in this file the protocol agents are coded in a procedure. So here we had to add the protocol agent for the newly created GAODV protocol. When a node is using GAODV protocol this agent is scheduled at the beginning of the simulation and is assigned to the nodes which use the protocol.

The next file to be modified is the *ms - agemt.tcl*. In this we have to set the port numbers for the new routing protocol. *sport* is the source port and *dport* is the destination port.

```
#GAODV patch
Agent/gAODV instproc init args {
        $self next $args
}
Agent/gAODV set sport_    0
Agent/gAODV set dport_    0
```

Figure 3.4: *ns - agent.tcl* GAODV modification

```
gaodv/gaodv_logs.o gaodv/gaodv.o \
gaodv/gaodv_rtable.o gaodv/gaodv_rqueue.o \
```

Figure 7: *makefile.in* GAODV modification

The third file modified is the *makefile.in* in the root directory of ns-2.34. This file is modified for creating the object files for the cpp coded files. After all the implementations are ready, we have to recompile NS-2 again to create the object files. Till now we have implemented a new routing protocol in NS-2 which is labeled as GAODV. But we still didn't implement the gray hole attack in this protocol. As of now this protocol will act similar to the AODV protocol. To add gray hole behavior in to the new protocol we made we had

to make some changes in the *gaodv.cc* C++ file. By explaining the working mechanism of AODV and GAODV protocol we will describe the changes made to the *gaodv.cc*.

In *aodv.cc* code when a packet is received it is received by a function called the *recv* and the received packets are processed based on the type of the packet. In this code the different control packets in AODV like RREQ, RREP and RERR packets are processed by different functions. The *recv* function checks whether the received packet belongs to any of these control packets. If it so then it will call the *recvAODV* function. If the received packet is a data packet, usually

```
//If destination address is itsself
if ( (u_int32_t)ih->saddr() == index)
   forward((gaodv_rt_entry*) 0, p, NO_DELAY);
else if ((rand()%6)==3 || (rand()%6)==4 || (rand()%6)==1)
// For grayhole attack in the wireless adhoc network, after giving a true route to demanding
// node, misbehaving node drops some packets according to the random function.
   drop(p, DROP_RTR_ROUTE_LOOP);
```

Figure 8: *gaodv.cc* GAODV modification

the AODV protocol will forward the packet to the destination address. But in GAODV protocol the code is modified such that it will drop random packets without forwarding it. This attack is implemented in the *recv* function of GAODV. First the conditions checks whether the packet is destined to itself if it so it will accept the packet, otherwise a condition is checked which is made of random numbers and if the condition becomes true the packet is dropped otherwise it will forward the packet.

3. 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. Some packets will be dropped by attacker node. If the selective dropping attack reduces the delivery ratio drastically an algorithm should be implemented to identify such nodes and prevent them from participating in the data transfer. A RREP from an attacker node can reach the source node earlier than a normal node if it is near to the source node or in other words the shortest path from the source to the destination. In this work we focus on developing an algorithm which focus on single dropping attackers in wireless mesh network and concentrate our study on the stationary routers which are present in hybrid wireless mesh networks.

3.1 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 promiscuous 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 communications do not directly involve A. While promiscuous mode is not appropriate for all wireless mesh network scenarios (particularly some military scenarios) it is useful in other scenarios for improving routing protocol performance. We also assume that the each router is provided with an infinite buffer size so that no packets are dropped because of buffer overflow. In the case of black hole attack we assume that the attack node will drop all the packets that it receives. Finally we also assume that each mesh router is provided with a private/public key pair and also all the public keys of other routers in the network. These keys are used to protect the packets generated while broadcasting the packet reporting the attack generated by the algorithm.

3.2 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 *mt* denotes the number of packets transmitted under a particular threshold to the downstream node. This threshold is denoted as $_{mthreshold.}$ At the same router m_o denotes the number of packets overheard by the router. m_o can be calculated by overhearing the downstream node to which the data is sent. *md* is used to denote the number of packets dropped by the downstream node. P_a is used to denote the probability of attack by the downstream router and also P_g and *Pb* are the threshold values called the probability of gray hole attack and probability of black hole attack respectively. *imterval* is the number of times the probability of attack is checked with the threshold values in a given interval.

3.3 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.

In our algorithm at each mesh router, the router will maintain a packet count history of the number of packets it has forwarded to the downstream node and also the number of packets it has overheard for the forwarded packets. When a router forwards a packet to the downstream node, the number of packet sent (*mt*) is incremented and also buffers the packet for a certain time period. Then it overhears the packet which is forwarded

by the downstream node and compares with the packet in the buffer. When a match is found the number of packets forwarded by downstream node (m_o) is increased. Once the match is found or if the time period is over the packet is deleted from the buffer. If the packet forwarding is not heard within the time period the algorithm assumes that the packet is dropped by the downstream node. After sending out a threshold number of packets ($_{nthreshold}$), the number of packets dropped (nd) is calculated and is the difference of the number of packets transmitted to the number of packets overheard.

$nd = nt - n_o$

According to these observations each router will maintain a probability value called the Probability of attack (P_a), which is obtained by the number of packets dropped by the downstream node(n_d) to the number of packets forwarded by the router to the downstream (n_t).

$P_a = n_d/n_t$

The obtained probability of attack (P_a) is compared with a threshold value of probability called probability of black hole attack (P_b) and if P_a is greater P_b then a possibility of black hole attack is identified.

4. CONCLUSION AND FUTURE WORK

In this research paper, detection and prevention techniques of black & gray hole attack in WMNs is presented. A Black & Gray Hole attack are serious attacks in WMNs. Black hole is an attack where a malicious node do not forward the data packets to the destination and gray hole attack is a special variation of black hole attack which is difficult to detect. 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 performance and security.

In future it is better to make the threshold values dynamic in the presence of normal loses due to wireless channel and MAC layer collisions and to work on the attacks when the attack routers collude together.

REFERENCES

[1] Prasoon P S ,Denial of Service Attacks in Wireless Mesh Networks [2012].

[2] Sonal Singh Inderpreet Kaur: Security against Active Attacks in Wireless Mesh Networks *Magazine*, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013

[3] Anjana Jayant Deen Kanu Geete Piyush Kumar Shukla, A Survey on Grey Hole Attack in Wireless mesh Networks International Journal of Computer Applications (0975 – 8887) Volume 95– No.23, June 2014

[4] Nitesh A. Funde1, P. R. Pardhi2 Detection & Prevention Techniques to Black & Gray Hole Attacks In MANETInternational Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013

[5] Varsha Patidar1, Rakesh Verma,Black Hole Attack and its Counter Measures in AODV Routing Protocol International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5

[6] Shafiullah Khan, Kok-Keong Loo, Tahir Naeem, and Mohammad Abrar Khan. Denial of service attacks and challenges in broadband wireless networks.

[7] S. Ghannay, S.M. Gammar, F. Filali, and F. Kamoun. Multi-radio multichannel 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.

[8] 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.

[9] 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.

[10] S. Seth and A. Gankotiya. Denial of service attacks and detection methods in wireless mesh networks. In *Recent Trends in Information, Telecommunicatioand Computing (ITC), 2010 International Conference on*, pages 238240, march 2010.