DETECTION AND MITIGATION OF SELFISH NODE IN WIRELESS MESH NETWORKS(WMN'S)-A REVIEW

[1]Afshan Hassan, [2]Mr.Rajeev Sharma,
[1]M.Tech ,Research Scholar,[2] Assistant Professor
[1]Computer Science & Engineering
[1]Chandigarh Group of Colleges,Landran,Punjab(Mohali)

Abstract -Wireless Mesh networks (WMN's) are prone to a number of attacks & these attacks compromise the security of these networks. Attaining security in these networks is a challenging task.In this paper, our point is that the virus is present in the internet and the authors are coming up with the methodology to fix it. In this paper, the authors will work on the Application layer, which contains a number of protocols.. In this paper the authors have come up with a methodology to first detect the selfish node in the network & later on provided a technique for mitigation of the same.NS2 simulator has been used to simulate & analyze the performance of our proposed methodology for Open Shortest Path First(OSPF) protocol in WMN's.

Keywords - Wireless Mesh Networks(WMN's), Distributed Denial Of Service (DDoS), covert channel, Media Access Control (MAC), Open Shortest Path First(OSPF),Switch port analyzer, Intrusion Detection Systems(IDS), Packet Delivery Ratio(PDR).

I. INTRODUCTION

A. Wireless Mesh Networks

Wireless Mesh Networks (WMN's) consist of Wireless Access points (AP), Mesh routers (MR's) & Mesh clients (MC's)(Figure 1.1).Wireless Mesh networks consist of a large number of these Mesh nodes (usually hundreds or thousands of nodes). These types of networks are highly distributed and deployed in hostile environments [1]. Wireless Mesh networks monitor the system or environment by measuring physical parameters such as humidity, pressure and temperature. WMNs are best suited for applications like military command, intelligent communications, industrial quality control, observation of critical infrastructures, smart buildings, distributed robotics, traffic monitoring etc. [2]. So, Wireless Mesh Network is a collection of small devices which provides:

- The ability to measure physical and environmental conditions such as temperature, pressure and humidity.
- The ability to operate devices such as actuators, motors and switches that control conditions.

Efficient and reliable communications. There are two types of wireless nodes in Wireless Mesh networks, Mesh node and a Base Station node. A large number of Mesh nodes are there in Wireless Mesh Networks which collect or sense the data and transmit it to the Base Station through multiple hops. The Base Station can use that data locally or globally using internet.

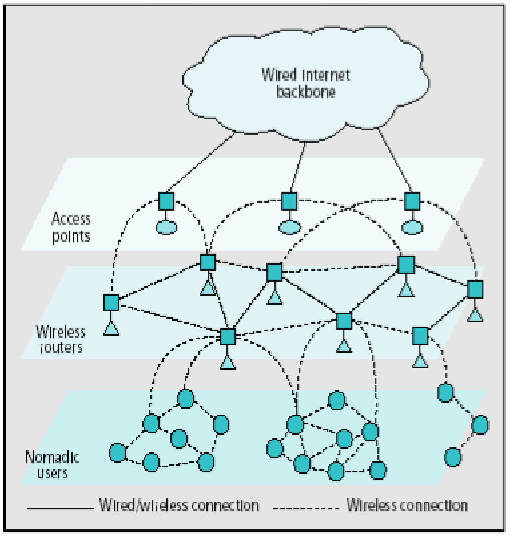

Figure 1.1: Wireless Mesh Network

Mesh nodes use battery power as an energy source. Battery is a limited power resource and as wireless Mesh networks are usually deployed in a hostile environment it is nearly impractical to replace batteries of the Mesh nodes, so power consumption in wireless Mesh networks is always a major concern. Therefore it is often required to have energy efficient techniques which can increase the life of these wireless Mesh networks. An inbuilt trade-off mechanism should be made so that the end-user can opt for prolonging network lifetime at the cost of lower throughput or higher transmission delay. [3].

1)Mesh Architecture: The traffic in Wireless Mesh Network depends on the number of queries generated per Mean time. The Base Station node transmits the information to be sensed by sending a query throughout the Mesh field. The Mesh nodes respond to the query by gathering the data using their Mesh's. Ultimately when the Mesh nodes have the result of the injected query,they will reply to the Base Station node through some routing protocol. A Mesh node also aggregates the replies to a single response which saves the number of packets to be sent back to the Base Station node [4].

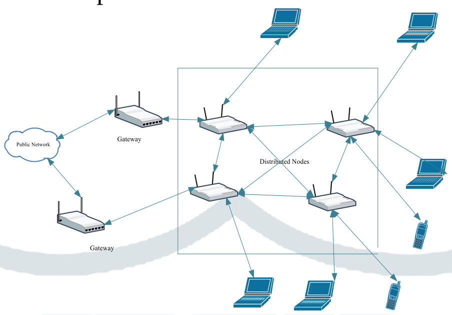

Figure 1.2: Wireless Mesh Architecture

Table 1.1: Major roles of architecture in OSI layer

Major Layer	**Roles**
Network Layer	Mesh router, Gateway
Data Link Layer	Data transfer used in this layer
Physical Layer	Radio (RF) Communication

2) Characteristics:

a) Medium of Communication: Nodes in a Wireless Mesh Network use wireless medium (such as radio waves or infrared waves) for communication. Mesh nodes can revise the transmission power of wireless transmitter according to the distance [6].

b) Hardware Constraints: Wireless Mesh Networks use battery as a source of power. Lifetime of a wireless Mesh network depends on the depletion of the batteries. Wireless Mesh Networks are also restricted in terms of Memory [7].

c) Application Dependent: Wireless Mesh Networks are application dependent as they are designed for real time collection and analysis of data.They are implemented to perform specific task as per requirements of the application [9].

d) Distributed Processing:In Wireless Mesh Networks processing is carried out by every node, so a centralized mechanism should be there to aggregate the data.

e) Prone to attacks: As Wireless Mesh networks are usually deployed in harsh environmental conditions where securing the networking is fairly difficult, so these networks are prone to attacks [11].

f) Multi-hop Routing: Mesh nodes use the direct transmission or multi-hop transmission to communicate with the base station.

g) Paradigm of Communication: There is a predefined paradigm of communication as all the Mesh nodes sense data in different environments as per query of the Base Station node and also they always have to send the data back to the Base Station node.

3) Applications of WMN

Wireless Mesh Networks are able to monitor a variety of conditions in the different environment like temperature, pressure, noise, movements, stress etc. So based on these conditions in which wireless Mesh networks can be used we have a wide variety of applications of these wireless Mesh networks.

h) Military and Public-Protection Applications: Wireless Mesh Networks are used in battlefield surveillance, monitoring and detecting nuclear and biochemical attacks. Such a wireless Mesh network which is installed for military and public protection purposes should itself be protected from intruders, because false alarming of such a network will raise threatening conditions in public.

i) **HealthCare Applications**: Wireless Mesh Networks are used in healthcare sector to monitor the effect of drugs and other related affects in patients by the doctor.

j) **Scientific Applications**: Wireless Mesh Networks are used by researchers to carry out different research projects. For example the behavior of different birds are monitored and detected by Wireless Mesh networks

k) **Engineering Applications:**Many Engineering projects use wireless Mesh networks to monitor the pressure, stress and different environmental conditions like mesh used in robotics projects.

l) **Household Applications**: Wireless mesh networks are used for a wide variety of different household applications like washing machine, microwave etc.

m) **Environmental Applications**: Wireless mesh networks are used to monitor different environmental conditions like flood detection, soil and agricultural conditions and other different atmospheric conditions [12].

B. Security in Wireless Mesh Networks

Wireless Mesh networks are usually installed at unprotected and bitter environments where security is a challenging issue. In such unprotected environments wireless Mesh networks are open to many physical as well as logical attacks. Security of Wireless Mesh network is very important as such types of networks are generally giving alerts which require serious attention. False alerts generated by the wireless Mesh networks may lead to unwanted actions.

1)Security Goals of Wireless Mesh Networks [2]

a) **Confidentiality**: In Wireless Mesh network the data is transmitted from one node to another node and after routing through many nodes, the data or information is passed to the base station. It is important that any message routed through wireless Mesh network is confidential and not accessible to unauthorized user.

b) **Authentication:** It may be possible that unauthorized access by some malicious node may drop some packets from the network or may introduce some false packets into the network. Such unwanted effects can be avoided if we have some means to identify the original Mesh nodes.

c) **Integrity:** The alteration done in data packets by malicious node violates the concept of integrity. Integrity means to ensure the correctness of the data. Receiver node should receive the data in original as sent by the sender node.

d) **Availability**: Failure of a node may lead to failure of a path & failure of a base station may lead to failure of the entire network. Mesh nodes and base station should always be available to provide services of Wireless Mesh networks.

e) **Freshness**: The data of each message should have freshness i.e. data should be recent; no old data should be replayed by the malicious nodes.

f) **Time Synchronization:** Most of the Wireless Mesh networks use time synchronization to calculate the delay between packets within a pair of nodes.

2)Attacks in Wireless Mesh Network:

Security attacks are the main concern in Wireless Mesh networks. These attacks can be categorized as follows:

g) **Worm hole Attack:** In wormhole attack, a malicious node, records packets at a particular location in the network and tunnels them to another location. When the control messages in routing are tunneled it creates disruption. It is a network layer attack. The solution to this problem is monitoring the network and flexible routing schemes.

h) **Black hole Attack**: In Black-hole attack a malicious node captures and re-programs a set of nodes in the network and blocks the packets that it receives instead of forwarding them towards the base station. Any packet that enters into the black hole region is captured by the malicious node and never reaches the destination node. [7, 8]

i) **Denial of Service Attack:** The malicious node in this attack hitsthe accessibility of all the nodes in the network. Aim of this attack is to block the services of the Mesh nodes [7, 8]. The attacker generally uses battery exhaustion method and radio signal jamming. It has further sub categories:

- 1. Smurf Attack
- 2. Distributed denial of services
- 3. SYN flood attack

j) **Byzantine Attack**: In this attack, an intermediate compromised node carries out attacks such as creating collision forwarding packets on non-optimal paths, routing loops, and dropping packets selectively which result in interruption or dreadful conditions of the routing services.

k) **Jamming:** In this attack the radio frequencies used by the Mesh node are inferred. The attacker monitors initially in order to verify frequency at which destination node is getting signal from the sender. The attacker transmits the signal on that frequency which is powerful enough to disrupt the network.

l) **Collision Attack**: In this attack, an attacker attempts to send the data on the same frequency with which other nodes are transmitting the data, so that the packets collide and retransmission is required [11].

m) **Man-in-the-middle attack**: In this attack, an attacker sits in between the sender and receiver node. The information being passed by the sender is captured by the attacker sitting in the middle. In some cases, attacker may masquerade as the sender to communicate with receiver or masquerade as the receiver to reply to the sender.

n) Base Station-hole Attack: In this attack the traffic is attracted by the malicious node. The malicious node draws attention of its neighboring nodes by announcing a fake optimal path using attractive power or bandwidth. Fooled neighboring nodes then route their data to malicious node and this results in dropping of packets by the malicious node. Many attacks like eavesdropping, selective forwarding and black holes, etc can be empowered by Base Station hole attack [1, 2, 7, 8].

o) Node Replication attack: The attacker tries to add a malicious node in the network by assigning the malicious node the same Node ID as that of some existing node in the network.

C. DoS (Denial of Service)

Denial of service (DoS) attacks have become a major threat to current computer networks. The aggregation of the attacking traffic can be tremendous compared to the victim's resource. The attack can force the victim to significantly downgrade its service performance or even stop delivering any service. ConventionalDoS attacks could be addressed by better securing service systems or prohibiting unauthorized remote or local access. The design of the Internet is one of the fundamental reasons for successful DoS attacks. The Internet is designed to run end-to-end applications. Routers are expected to provide the best effort packet forwarding, while the sender and the receiver are responsible for achieving desired service guarantees such as quality of service and security. Accordingly, different amounts of resources are allocated to different roles. Routers are designed to handle large throughput that leads to the design of high bandwidth pathways in the intermediate network. On the contrary, end hosts may be only assigned as much bandwidth as they need for their own applications. Consequently, each end host has less bandwidth than routers. Attackers can misuse the abundant resources in routers for delivery of numerous packets to a target.

D. DoS vs DDoS

Distributing the generation of packets to the target host, thus the name DDoS – distributed denial of service attack. Every packet stream from one of those hosts is aggregated at the target so we have an amplification of traffic. Apart from a greater amplification factor there are other advantages to DDoS attacks, at least from the point a view of an attacker.

Usually a server machine has more processing power, memory and especially bandwidth than a client machine (a workstation). So using server machines the attacker has better chances of saturating a target. Then there is a matter of mitigating the attack. If the attack comes from one single source and it is possible to trace it back, then in most cases it will be possible to stop it only if a source system owner/administrator manually does the action. In order to perform DDoS attack from numerous hosts first we need to gain access to them. As such those compromised hosts are often called the “secondary victims/targets” and the host/system/network under attack itself is called the “primary victim/target”. The use of secondary targets allows attackers to use much larger base of packet generating hosts while providing higher degree of anonymity as real flooding attack is performed by secondary sources so tracking down a real attacker becomes a formidable task.

Another benefit for the attacker, as was mentioned earlier, is that the aggregation of attack traffic is done only at the target so we can restrict our packet generation rates to much lower values and it becomes very hard to distinguish this kind of traffic at the source networks and intermediate nodes on the way to the target. As DDoS attacks are much more disruptive, currently the majority of research on denial of service attacks is done with emphasis on distributed systems. The following comparison is shown in the table 1.2.

Table 1.2: DOS vs. DDos attacks

Parameter’s	**DoS**	**DDoS**
Type	Centralized, local only	Distributed
Target	Only single server	Attack on Thousands of machines
Complexity	Low	High
Identification	Moderate	Hard to detect
Impact	Infects 10 to 20 Machines	Infects the whole network

II.LITERATURE SURVEY

[1] R. Kaur et al introduced the concept of wireless mesh networks, an unusual method of producing, keeping and sharing information ability of mobile objects to show spontaneous and cheap adjusting arrangement itself. There are different types of communication devices in technology by which performance is measured. There are different types of attacks such as black hole attack, wormhole attack, Greyhole attack, and eves dropping attack. Black hole and Greyhole attacks are network layer attacks that degrade the performance by dropping the packets. The black hole and Grey hole attacks are the problems of security that are considered in wireless networks. Black hole and Greyhole attack are two types of interrupting attack which can cause huge damage to the network. Black hole attack is like ad-hoc network. The attacker achieves this attack when all the similar kinds of nodes communicate and make network to each other. It is very important to protect the network layer from these attacks which is also a challenging task in wireless mesh networks. Greyhole attack is very difficult to detect in a wireless mesh network.

[2] R. Upadhyay et al studied the characteristics of DDoS problems and investigates that the corresponding defense mechanisms have significant contributions not only for academia and industry, but also for the social security and emergency management agencies, since they can use such knowledge to enhance their abilities of risk assessments and help the stakeholders to make appropriate decisions when facing DDoS threats. In the existing research work the different types of problems, in terms of detecting DoS attacks is to view the problem as that of a classification problem on network state (and not on individual packets or other units) by modeling normal and attack traffic and classifying the current state of the network as good or bad, thereby detecting attacks when they happen. Also the transmission failures or deadline misses may result in disturbances to the process, degradation of the overall control performance.

[3] S. Biswas et al proposed a solution for detecting and avoiding black hole attacks (both single and cooperative) and ensuring secure packet transmission along with efficient resource utilization of mobile hosts at the same time. According to the proposal, evaluation of trust of every node in the network is based on parameters such as stability of a node defined by its mobility and pause time, remaining battery power etc. This trust of a node forms the basis for the selection of the most reliable route for transmission. The simulation results show that the solution provides good performance in terms of throughput, secure routing, and efficient resource utilization.

[4] A. Gawareet al discussed the Wireless Mesh networks using IEEE 802.11 standard. The authors present an autonomous network reconfiguration system (ARS) that enables a multiradio WMN to autonomously recover from local link failures to preserve network performance. The ARS (autonomously reconfigure system) uses its local network settings channel, radio, and route assignment for real-time recovery from link failures. The accurate link quality information from the monitoring protocol is used to identify network changes that satisfy applications' new QOS demands or that avoid propagation of QoS failures to neighboring links. The authors used WMN test bed and implemented it with the help of NS2 Simulator.

[5] Alan Saied et al combined the detection of known and unknown DDoS attacks followed by a defense mechanism that prevents forged packets from reaching the victim, but allows genuine packets to pass through. This solution is designed to continuously monitor the network for abnormal behaviour by retrieving packets from the network and analysing their header information using the trained ANN. However, retrieving a large number of packets in a busy network requires high processing rates and is expensive. Therefore, individual packet thresholds for each protocol were introduced. If the number of packets in a given network is greater than a specific threshold per protocol, the retrieved packets are subjected to investigation

[7] G. W. Kibirigeet al designed a paper based on the behavior or technique used to launch sinkhole attack. Then these rules are embedded in intrusion detection system which runs on each of the sensor nodes. These rules are then applied to the packet transmitted through the network nodes. If any node violates the rules,it is considered as adversary and isolated from the network. The combination of both anomaly and signature based method is used in this approach. The false positive rate which is produced by the anomaly based method is reduced in this approach due to the use of both the methods in combination. Also the advantage of this approach is the ability to catch any suspicious nodes when their signature is not included in detection database.

[7] C. Lal et al used an OWCA (Optimized Weight-based Clustering Algorithm) to partition the network into different clusters. Each cluster has a Cluster Head (CH) along with sensor nodes which exist in the communication range to CH. Clustering is a method in which sensor nodes do not need to send their data directly to the Base Station (BS) because if all nodes send their data directly to BS, lot of energy of these nodes will get wasted in transmission. Nodes in a cluster send data to their CH. CH collects data packets from all nodes in their cluster and sends these data packets to the BS. Now if a black-hole attacker node exists in the network, this node senses the data from environment but does not send this data to the CH. The area covered by attacker node will be left unattended. If this attacker node becomes CH during simulation time, then all nodes send their data to CH.

[9] K. Abasikeleş et al modeled the sinkhole and the black hole attacks on the LEACH, which is a cluster-based routing algorithm. The LEACH has three basic components called the base station (sink), the cluster head and the sensor nodes. The sink is responsible for evaluating the data, which is gathered from the cluster heads. The sensor nodes transmit their data to the cluster head, while the cluster head node receives data from all the cluster members, performs signal processing functions on the data, i.e. data aggregation, and transmits data to the remote sink.

III.OSPF PROTOCOL[13]

A. OSPF which stands for Open Shortesr Path First is one of the routing protocols which is used for exchange of packets containing best path information. It is a a Link State Routing protocol which uses Shortest Path First algorithm known as Dijkistra algorithm for calculating the best path towards destination networks. It is a type of IGP protocol which operates within a single autonomous system. It was developed by IETF.OSPF was developed keeping in mind the shortcomings of RIP which included better path calculation ,detailed information of the network & faster convergence.

1) Highlighting features of OSPF

a) Being a link state protocol,OSPF uses link speed,cost & path congestion for choosing the shortest path instead of relying on only hop counts.

b) OSPF exchanges routing information only when there is a change in topology or in the network which results in efficient use of bandwidth & less routing overheads.

c) Practically OSPF doesn't have any hop count limitations as was the case with previous routing protocols.

d) OSPF has detailed information of the topology because of which it can take better routing decisions & avoid routing loops.

e) We can control the amount of information that is exchanged between the OSPF routers by grouping the routers in multiple areas.

f) Unlike distance vector protocols,OSPF sends a HELLO packet before the actual exchange of routing information.

g) OSPF uses hierarchial network design instead of flat network design which gives much granular control to network administrators

2) Operation & messages in ospf:

OSPF header is of 24 bytes which is used to validate & process the incoming OSPF packets whereas in OSPF version 3 the header size is 16 bytes.OSPFheader consists of following fields:

a) Version number.

b) Type of OSPF packet.

c) Packet length.

d) Router-id.

e) Area-id.

f) Checksum.

g) Authentication.

OSPF uses five different types of packets during its operation:

a) **HELLO packet**: HELLO packets are exchanged prior to the exchange of routing information. HELLO packets are periodic in nature with a default of 10 seconds for point-to-point links & 30 seconds for non BMA links. HELLO packets are used to form adjacencies between OSPF enabled routers & to confirm the bidirectional flow of packets between the neighboring routers. By default if no HELLO packet is received by the OSPF router within 40 seconds for point-to-point & 120 seconds for NBMA links, the neighbor is considered dead & all the exchanged information is removed from the database.

b) **Database descriptor (DBD) packet:** After adjacency is formed using HELLO packets,OSPF exchanges database descriptor packets which are used to synchronize link state database.

c) **Link State Request(LSR)packet:** If after the exchange of DBD packets ,it is found by the router that the link state database is not up to date or is not in synchronization with other LSDB's,then a link state request packet is sent towards the neighbor, requesting the neighboring router to sent the most recent of missing LSA's.

d) **Link State Update (LSU):** The router multicasts LSU packets to its neighbors which contain one or more link state advertisements. The sending router floods LSA within an LSU packet to its neighboring routers.

e) **Link State Acknowledgement (LSA):**These packets are used to acknowledge whether the link state update packets were received successfully & if not a retransmission request is sent for the same. Multiple update packets can be acknowledged by a single acknowledgement packet.

Iv Conclusion

This paper aims to analyze DDOs attack & propose a framework for mitigating the same. This will help to protect the Internet Applications & API's from malicious traffic targeting network & allow the application layer to maintain availability & performance through proposal of proper mitigation technique

References

[1] R. Kaur and P. Singh, "Black Hole and Greyhole Attack in Wireless Mesh Network," no. 10, pp. 41–47, 2014.

[2] R. Upadhyay, U. R. Bhatt, and H. Tripathi, "DDOS Attack Aware DSR Routing Protocol in WSN," Phys. Procedia, vol. 78, no. December 2015, pp. 68–74, 2016.

[3]S. Biswas T. Nag, and S. Neogy, "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET," 2014 Appl. Innov. Mob. Comput., pp. 157–164, 2014.

[4]A. Gaware and S. B. Dhonde, "A Survey on Security Attacks in Wireless Sensor Networks," pp. 536–539, 2016.

[5]Alan Saied, Richard E.Overill, Tomas z Radzik, "Detection of known and unknown DDoS attacks using Artificial Neural Networks", Neuro computing, 2016, pp.385-393.

[6] G. W. Kibirige and C. Sanga, "A Survey on Detection of Sinkhole Attack in Wireless Sensor Networks," Int. J. Comput. Sci. Inf. Secur., vol. 13, no. 5, pp. 1–9, 2015.

[7] C. Lal, "An Energy Preserving Detection Mechanism for Blackhole Attack in Wireless Sensor Networks," vol. 115, no. 16, pp. 32–37, 2015.

[8] K. Abasikeleş, I Aydin, M N Tohma, "A Realistic Modeling of the Sinkhole and the Black Hole Attacks in Cluster-Based WSNs," vol. 4, no. 1, pp. 74–78, 2016.

[9] S. D, S. V R, A. Begam, and C. G. M, "Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent," Artif. Intell., 2012.

[10] RakshaUpadhyay, Salman Khan, HarendraTripathi, Uma Rathore Bhatt, "Detection Mechanism for Black hole attacks in WSN for AODV and DSR using Battery Drain," vol. 5, no. 4, pp. 98–100, 2016.

[11] A. H. Moon, N. A. Shah, U. I. Khan, and A. Ayub, "Simulating and analysing security attacks in wireless sensor networks using QualNet," Proc. - 2013 Int. Conf. Mach. Intell. Res. Adv. ICMIRA 2013, pp. 68–76, 2014.

[12]TeodorSommestad Fredrik Sandstrom, "An empirical test of the accuracy of an attack graph analysis tool", Information & Computer Security, 2015.

[13]V.Vetriselvan,PravinR.Patil,M.Mahendran "Survey on the RIP,OSPF,EIGRP Routing Protocols"Vol 5 (2),2015,

JETIR