DETECTION OF BLACKHOLE ATTACK IN DISTRIBUTED WIRELESS SENSOR NETWORKS

Dr. Sharvani G.S  
Associate professor, Dept of CSE  
RVCE, Bangalore

Rakesh R  
PG student, Dept of CSE  
RVCE, Bangalore

Abstract: Wireless sensor network is one of the emerging technologies where it provides various kinds of applications for military and societal purpose. The sensing methodology which is a combination of wireless communication and processing power makes it as one of the powerful technology. Incorporating security into wireless sensor network is one of difficult task due to their limitations. Wireless sensors networks are prone to various kinds of threats. One of the security attacks to wireless sensor network is a black hole attack. In black hole attack, the malicious node will advertise itself stating that it has the shortest route to the destination by exploiting routing protocol. The black hole attack is a kind of denial of service attack. This paper deals with the architecture of sensor network with access point, vulnerabilities of adhoc on distance vector routing protocol associated with black hole attack and detection mechanism. To detect black hole attack in the network, authentication mechanism and sensor network with mobile access point using Adhoc On Distance Vector Routing protocol is used. To detect the number of black hole nodes present in the network, fusion rule is used. The fusion rule used in this paper is q-out-of-m rule, which provides good tradeoff between false alarm rate and miss detection rate.

Keywords: sensor network with access point, authentication, black hole, adhoc on distance vector routing, q-out-of-m rule

I. INTRODUCTION

Wireless sensor Networks is a spatially distributed sensors which can monitor physical or environmental conditions. Basically the idea of wireless sensor network is to distribute small sensing nodes, which have the ability to discover the incidents that occur in its range and they can communicate with surrounding devices. The sensors are capable of tracking the target, environmental monitoring and surveillance. The sensors can detect temperature, humidity, pressure, vehicular movement, lighting conditions, noise levels, soil makeup and other properties. The communication with the sensors is performed using wireless transceivers. Wireless sensor network development was motivated by the community of research people since there was an extensive use of military and civilian applications[1],[2],[3],[4]. Incorporating security into wireless sensor networks is a challenging task since they are limited by power supply, type of tasks and processing speed. Wireless sensor networks are prone to various kinds of attacks. One of the dangerous attacks to the network is the black hole attack, where an adversary would advertise itself stating that it has the shortest path to the destination.

The technique used to detect blackhole attack in the network is a wireless sensor network with mobile access points(SENMA)[5] and authentication mechanism[6]. The Mobile Access point(MA) present in SENMA traverses entire network to collect the information from all the sensor present in the network. SENMA architecture provides direct line of sight to the sensors which are present with its range so that information can be conveyed without routing. This makes the architecture to be energy efficient. To minimize bandwidth and energy used during the sensing, the obtained results are transferred in the form of single bit[7],[8],[9],[10]. The MA receives the sensing reports from all the sensors present in the network and then it implements fusion rule to make final conclusion. The fusion rule used for detecting number of black hole nodes present in the network is a simplified q-out-of-m rule[9],[10],[11], in which MA polls reports from m sensors and in that if q sensors reports 1 then the target is present. This rule provides good tradeoff between false alarm rate and miss detection rate.

The paper can be summarized as follows, section 1 deals with introduction, section 2 deals with background work of sensor network with mobile access point and adhoc on distance routing protocol, section 3 deals with problems associated with black hole attack, section 4 deals with detection mechanism for black hole attack, section 5 deals with conclusion.

II. LITERATURE SURVEY

A. SENMA:

Consider SENMA architecture as shown in fig 1 which consists of n ‘sensor nodes which are distributed randomly and it contains powerful access point. The mobile access point traverses entire network according to a trajectory and collects information. If the network is large, then the area is divided into smaller region and then fusion rule is applied over the sensors which are in the same region. This ensures that the sensors which are in the same region have the same chances of finding the target. The SENMA architecture performs distributed detection.

Whenever target enters the sensing region of sensors, each sensor would detect the target by applying
energy detection algorithm[12] and sends the 1-bit decision report to mobile access point. If sensors report ‘1’, then this means that target is present.

![Diagram of sensor network with mobile access](image)

**Fig 1 Sensor network with mobile access.**

### B. AODV:

AODV(Adhoc On Demand Distance Vector)[13] is one of the routing protocol which is used to route packets. The discovery of route process is not started until they are required by source node. The AODV protocol performs two operations they are route maintenance and route discover. The route discovery process gets initiated when there is no route from source to destination. The route discovery process starts from source node by sending Route Request packet (RREQ) to its neighbouring nodes. The node that receives RREQ packet would check for the route to destination in its Routing Table(RT), if the details regarding the destination route is found then it sends acknowledgement to the source node else the RREQ packet is forwarded to its neighbouring nodes. Before forwarding RREQ packet, the node would store all the details regarding the reverse path to source node in its RT. The RT maintains details of next hop, distance and sequence number. When the RREQ reaches destination node then the destination node responds with RREP (Route Reply Packet) to source. The source node chooses the path from which it gets the first reply to transfer data packets.

**AOVD Weakness:**

Some of the weaknesses that can be exploited from AOVD to disturb the communication process are:

- False message propagation with RREQ: It reroutes all the traffic through malicious nodes and finally it would drop the packets.
- False message propagation with RREP: In this kind of attack malicious node reroutes the traffic with false RREP packets. The aim is to discard the data and create Blackhole node.
- False reply with RREP:It intercepts request with a solution before it reaches final destination.
- Rush Attack with RREQ: This attack suppresses valid RREQ sent by genuine node.

### III. PROBLEM STATEMENT:

**A. BlackHole attack [14]:**

In this kind of attack malicious node makes use of routing protocol to advertise itself stating that it has the shortest path to the destination. The attacker hears about the request for the routes from AOVD protocol. When attacker obtains the requests for route to the destination node, the attacker responds to the request by stating that it has the shortest route. If the attacker reply successfully reaches the source node before the reply from the genuine sensor node reaches, then the fake route gets created. The malicious node will be able to drop the packets successfully to perform denial of service attack once they get placed between the communicating nodes. This can result in congestion and can increase energy consumption of the sensors involved in the process.

The process of black hole attack can be shown in fig 2, initially node 1 broadcast RREQ packets to neighbouring nodes for finding the route to the destination node 5. If the black hole node receives the RREP packet then it responds with fake RREP packet by adding highest sequence number. As the fake RREP packet reaches the node 1,node 1 assumes that this packet is from intended destination or from the node which has fresh route with shortest route to the destination. Then the node 1 starts to transmit the data packets. The black hole node receives the packets and drops it instead of forwarding.

![Diagram of blackhole attack](image)

**Fig 2: Blackhole attack**

### IV. Malicious Node Detection Scheme:

To detect malicious node which is present in the network, end to end authentication mechanism using AOVD protocol is used. The source node starts to transmit the data after route becomes secure.

**Methodology:**

The source node performs the following Process after receiving RREP from the destination node.
Step 1: Secret key[6] is generated

Step 2: Time Stamp is generated.

Step 3: Message Authentication Code(MAC) is generated by taking attributes like time stamp, secret key, RREP.

Step 4: Symmetric cryptosystem is used to generate an encrypted packet by taking the attributes such as Time Stamp, RREP, and MAC.

Step 5: Transmits the encrypted packet to all the nodes which are present in the route to the destination. Encrypted packet value and MAC value is stored in mobile access point.

When the encrypted packet reaches the destination node then the following process occurs.

Step 1: Checks the value of encrypted packet with the mobile access point.

Step 2: Decrypts the Encrypted packet to obtain Time Stamp, RREP and MAC.

Step 3: Checks the MAC value with mobile access point.

Step 4: Decrypts the MAC packet to obtain Time Stamp, Secret key, and RREP.

Step 5: checks if the value of time stamp is in reasonable range.

Step 6: Checks if the Time Stamp value is same as that of Time stamp value present in the node.

If all the process in the destination goes proper then the destination node would sent an acknowledgement to the source node via mobile access point stating that the route is secure then the source node would start to transmit the data packets. If the source gets an acknowledgement stating that there is a malicious node in the path then the source node does the following operations:

Step 1: Discard the RREP packet and there might be chances that MAC might be duplicated. MAC with invalid value is dropped.

Step 2: Starts another route discovery process.

Step 3: The source node generates an alarm in the network stating that there are malicious nodes present in the network.

To obtain the total number of malicious nodes present in the path from source to destination then q-out-of-m fusion rule is used, where the mobile access point scans 'm' sensors and obtains the encrypted packet value from the nodes present in the route and compares with the value present in its database. After comparing the value if the mobile access point reports ‘1’ then ‘q’ number of black holes are present in the network.

The fig 3 represents the flowchart of whole process to detect the black hole attack in wireless sensor network and the flow of RREQ and RREP packets.
V. CONCLUSION

This paper deals with the detection of blackhole attack in wireless sensor network. To detect the blackhole nodes present in the network authentication mechanism and architecture of SENMA are used. The mobiles access point helps the destination node in validating the encrypted packet and also in transmission of acknowledgement from destination to source. Fusion rule helps in finding the number of black hole nodes present in the path between source and destination. The position of malicious node can be obtained through SENMA since it provides direct line of sight. The authentication mechanism helps in obtaining the secure route from source to destination.

REFERENCES


