Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.643 – 648

RESEARCH ARTICLE

Protected Data Transfer in Wireless Sensor Network Using Promiscuous Mode

K.Rashidha Begam[1], M.Savitha Devi[2]

[1]Research Scholar, Don Bosco College, Dharmapuri, TamilNadu, India

[2]Assistant Professor, PG & Research Department of Computer Science, Don Bosco College, Dharmapuri, TamilNadu, India

[1] rasfiraz@gmail.com; [2] savithasanma@gmail.com

Abstract*— Wireless Sensor Networks consist of large number of sensor nodes computing the sense, and communications capabilities. Wireless sensor networks are widely used in many applications like battlefield monitoring, environment monitoring and so forth. These applications have the cooperation among various sensor nodes which is needed to forward the data packets to the base station. In this paper we are explaining about Wormhole attacks. A wormhole attack is a severe attack in wsn. It is a severe threat to the network layer. In Wormhole attack two or more malicious nodes makes a covert channel which attracts the traffic towards itself by depicting a low latency link and then start dropping and replaying packets in the multiple path route. In this paper we are suggesting about promiscuous mode with the help of two extensions called Watchdog and Path rater in AODV protocol. This method is used detect and isolate the malicious node during wormhole attack and it observes the nodes which are not participating in multi-path routing generates an alarm message during delay and then detects to isolate the malicious node from the network.

***Keywords*— Wireless Sensor Networks, Security Attacks, Wormhole Attacks, AODV, Promiscuous mode**

I. INTRODUCTION

A Wireless Sensor Network is a self-configuring network of small sensor nodes communicating through radio signals and deployed in quantity to sense, for monitoring to understand the physical world. Wireless Sensor nodes are called motes. Wireless sensor network requires a detailed understanding of the both capabilities and limitations of each of the underlying hardware components, as well as modern networking technologies and distributed systems theory. Each individual node must be designed to provide the set of primitives which is necessary to synthesize the interconnected web that will emerge as they are deployed, while meeting strict requirements of size, cost and power consumption. In WSN each node act as a routing path for another nodes in the network, follows multi hop multi path routing. Improper use of information or using forged information may cause unwanted information leakage and provide inaccurate results. Due to its dynamic topology, lack of reliability and wireless infrastructure WSN are prone to various attacks which leads to the tampering of wireless networks by attackers.

II. RELATED WORK

A. Attacks in Wireless Sensor Networks

Wireless sensor networks are vulnerable to various types of attacks. These attacks are of three types which are attack on network availability, attack on secrecy and authentication, stealthy attack against service integrity. In attack on network availability which can be referred as Dos attacks. In attacks on secrecy and authentication, which standards cryptographic techniques can protect the secrecy and authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks and also spoofing of packets? In a stealthy attack the goal of the attacker is to make the network accept a false data value. In these attacks, keeping sensor network available for its intended use is essential. In wireless sensor networks can be broadly classified into two different levels of views. The first is the attack against the security mechanisms and the second is the routing mechanism which is very basic in nature. Here we are analyzing the attacks in the routing mechanisms which are more susceptible in Wireless sensor attacks.

b. Routing attacks

In WSN, the attacks which acts on the network layer are called routing attack. We are discussing some of the attacks that happen while routing the messages. Spoofed, altered and replayed routing information When a malicious node miss-present his identity, so this way it can alter the vision of sender and sender change the topology. It will create routing loops, extend or shorten service routes, and generate false error messages. And also increase end-to-end latency. In Selective forwarding the sensor networks which is assumed that nodes faithfully forward received messages. But some compromised node might refuse to forward packets, however neighbors might start using another route. Sinkhole Attack typically works by making a compromised node look especially attractive to surrounding nodes. In this attack, the adversary's goal is to attract nearly all the traffic from a particular area through a compromised node. Sybil Attack refers to the multiple copies of malicious nodes. It can be happen, if the malicious node shares its secret key with other malicious nodes. This way the number of malicious node is increased in the network and the probability of the attack is also increased. If we use the multipath routing, then the possibility of choosing a path in the network, those contain the malicious node will be increased. HELLO flood attacks are an attacker sends or replays a routing protocol's HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes that are isolated in a large area within a WSN.

c. Wormhole attacks

Wormhole attack is also called as tunneling attack. An attacker receives a packet at one point and tunnels it to another malicious node in the network. This way beginner assumes that the user found the shortest path in the network. This tunnel between two colluding attackers is called the wormhole. In a wormhole attack, the malicious nodes will tunnel the eavesdropped packets to a remote position in the network and retransmit them to generate fake neighbor connections, thus spoiling the routing protocols and weakening some security enhancements. Route discovery mechanism used in many routing protocols. The tunnel can be established in many different ways, such as through an out-of band hidden channel (e.g., a wired link), packet encapsulation, or high powered transmission. The tunnel creates the illusion that the two end points are very close to each other, by making tunneled packets arrive either sooner or with lesser number of hops compared to the packets sent over normal routes.

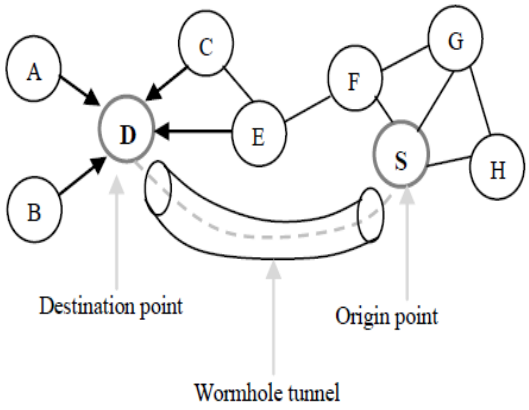

Fig. 1 Wormhole attack in a network

1. Types of Wormhole attack Modes

In this Wormhole attacks, we are classifying this attacks based on the techniques which we are used for launching it. Number of nodes involved in establishing wormhole and the way it is used for launching using several modes, among these modes. Some of these are discussed in this paper.

a. Wormhole using Encapsulation: In this mode a malicious node at one part of the network and hears the RREQ packet. It tunnels it to a second colluding party at a distant location near the destination. The second party then rebroadcasts the RREQ. The neighbors of the second colluding party receive the RREQ and drop any further legitimate requests that may arrive later on legitimate multi-hop paths. The result is that the routes between the source and the destination go through the two colluding nodes that will be said to have formed a wormhole between them. This prevents nodes from discovering legitimate paths that are more than two hops away.

b. Wormhole using Out-of-Band Channel: The second mode for this attack is the use of an out of band channel. This channel can be achieved, for example, by using a long range directional wireless link or a direct wired link. This mode of attack is more difficult to launch than the previous one since it needs specialized hardware capability.

c. Wormhole with High Power Transmission: Another method is the use of high power transmission. In this mode, when a single malicious node gets a RREQ, it broadcasts the request at a high power level, a capability which is not available to other nodes in the network. Any node that hears the high-power broadcast rebroadcasts it towards the destination. By this method, the malicious node increases its chance to be in the routes established between the source and the destination even without the participation of a colluding node.

d. Wormhole using Packet Relay: Wormhole using Packet Relay is another mode of the wormhole attack in which a malicious node relays packets between two distant nodes to convince them that they are neighbors. It can be launched by even one malicious node. Cooperation by a greater number of malicious nodes serves to expand the neighbor list of a victim node to several hops.

e. Wormhole using Protocol Deviations: A wormhole attack can also be done through protocol deviations. During the RREQ forwarding, the nodes typically back off for a random amount of time before forwarding reduce MAC layer collisions. A malicious node can create a wormhole by simply not complying with the protocol and broadcasting without backing off. The purpose is to let the request packet it forwards arrive first at the destination.

2. Models of Wormhole attacks

The classification of wormhole attack facilitates the design of prevention and detection methods. According to that the attackers are visible on the route in which the wormhole attack can be classified in three types: Open wormhole, half open wormhole and closed wormhole.

a. Open Wormhole attack: In this type of attack, the attackers include themselves in the RREQ packet header following the route discovery procedure. Other nodes are aware that the malicious nodes lie on the path but they would think that the malicious nodes are direct neighbors.

b. Closed Wormhole Attack: In this attack, the attacker does not modify the content of the packets, even though the packet is in a route discovery packet. Besides that they simply tunnel the packet from one side of wormhole to another side and it rebroadcasts the packet.

c. Half open wormhole attack: In this attack, one side of wormhole does not modify the packet and only another side modifies the packet, following the route discovery procedure.

III. AODV ROUTING PROTOCOL

AODV (Ad-hoc on Demand Distance Vector) is a reactive protocol. The reactive routing protocols do not periodically update the routing table like table driven proactive protocols periodically. It is the modification of DSDV (Destination Sequence Distance Vector). It provides unicast, multicast and broadcast. It works on, on demand algorithm. It searches for route between nodes only which is decided by the source nodes. These routes are maintained as long as they are needed by source. AODV builds route using route request and route reply query cycle. It is the loop free, self-starting scale to large number of nodes. AODV is a well-known distance vector routing protocol and it works as follows. Whenever a node wants to communicate with another node, it looks for an available path to the destination node, in its local routing table. If there is no path exists, then it broadcasts a route request (RREQ) message to its neighborhood nodes. Any node that receives this message for route discovery looks for a path leading to the respective destination node. The important feature of AODV is the maintenance of time based states. This means that routing entry which is not used recently is expired. The intermediate nodes store the route information in the form of route table.

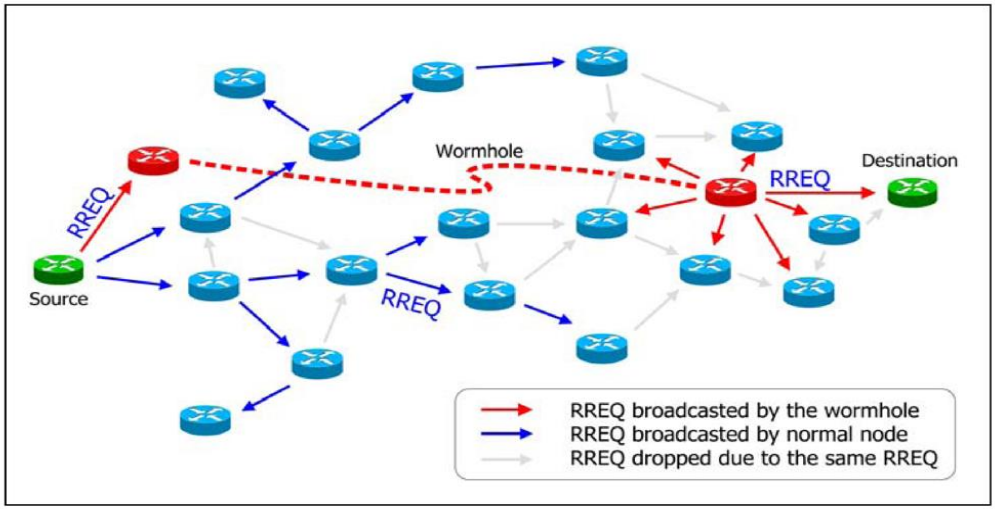

Fig. 2 Wormhole attack route request

Control messages used for the discovery and breakage of route are Route Request Message (RREQ), Route Reply Message (RREP), Route Error Message (RERR).The main advantages of AODV protocol are that routes are established on demand and destination sequence numbers are used to find the latest route to the destination. The connection setup delay is less. The HELLO messages supporting the routes maintenance are range-limited, so they do not cause unnecessary overhead in the network. One of the disadvantages of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries.

IV. PROMISCUOUS MODE

To protect the WSN from wormhole attack, it has been proposed the method of categorizing nodes based upon their dynamically measured behavior, named as Promiscuous mode. In this paper two extensions to Ad Hoc on Demand Routing protocol (AODV) are implemented in order to mitigate the effect of routing misbehavior during wormhole attack. The two extensions namely Watchdog and Path rater are implemented. Watchdog technique is used for identifying the misbehaving nodes and path rater helps the routing protocol (AODV) to avoid these nodes from forwarding the packets. When the node is forwarding the packet, the watchdog verifies the nodes that the next node in the path also forwards the packet. Watchdog does this by listening promiscuously to next nodes transmissions. If next node does not forwards the packet, then it is misbehaving node. Path rater uses this knowledge of misbehaving nodes to choose the network path that is most reliable to deliver the packets. In this paper during simulations the multi-hop route is established between the source and destination by the source node then the delay parameters are observed when the delay proceeds from the implied time then the watchdog became active and generate the promiscuous mode. In which all the other sensor nodes except the path nodes enters into the promiscuous mode after getting alarm message from source node. The watchdog then detects the malicious node and isolates it from the network and path rater then finds the other most reliable and suitable route to forward the packets from source to destination.

The software developed is to detect the attack in the wireless sensor networks. The basic modules to be implemented are Discover Neighbor node Module, Verify Neighbor node Module, and Finding adversial node Module.

V. SIMULATION RESULTS

Ns-2.3 Network Simulator tool is used to evaluate the performance of different routing protocols in Wireless sensor networks. In this simulation, we have tested AODV routing protocol with scalability of nodes. To prevent the WSN from wormhole attack, it has been proposed the method of categorizing nodes based upon their dynamically measured behavior, named as Promiscuous mode. The performance of AODV routing protocols is analyzed on behalf of metrics like Throughput, delay and Packet Delivery ratio. Parameters used in simulations are summarized as follows:

(1) Queue length = 50
(2) Routing protocol=AODV
(3) Packet Size = 1000 bytes
(4) Traffic generator= CBR

(5) Antenna = Omnidirectional
(6) Propagation Ground = 2-way ground
(7) X = 300
(8) Y = 300
(9) Number of nodes = 50 802.11 standard wireless channel

After simulations the results are shown that the throughput before implementing promiscuous mode was very low during wormhole attack and after the methodology implementation the throughput became very high even in the presence of wormhole attack. The effect of delay on wireless sensor network during wormhole attacks before and after implementing promiscuous mode. There is sharp rise in delay when wormhole attack was done before promiscuous mode implementation. The number of packets is delivered more after implementing this promiscuous mode.

a) Network Throughput

In this performance is measured in terms of throughput as the number of packets received at the destination over a period of time and is measured in kbps. Network throughput decreases drastically when the number of wormhole peers are increased from 0 to 10 (wormhole links increased from 0 to 5).With Watchdog launched, it is observed from the below table that the throughput improves by 49.4% compared to wormhole attacked AODV.

b) Average End-to-end delay

It is the total time taken for a packet to reach from source to destination and it is measured in seconds. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

$$\text{End to end delay} = \frac{\Sigma\ (\text{arrive time} - \text{send time})}{\Sigma\ \text{Number of connections}}$$

The lower value of end to end delay means the better performance of the protocol. Average end to end delay increases drastically when number of wormhole links are increased as the link latency is high for wormhole tunnels leading to more time consumption. With all 5 wormhole links activated, delay is 4.6723 sec in AODV in which the Watchdog and path rater in launch, it is reduced to 0.989sec.

C) In Packet delivery ratio

PDR is the ratio of number of packets received at destination node with that of number of packets sent by the source node. Again PDR decreases drastically with increase in wormhole links as more wormhole peers perform selective packet dropping. PDR improves by 24% with Watchdog in place compared to wormhole infected AODV. In this, the improvement made in PDR with watchdog in action in network. This illustrates the level of delivered data to the destination.

$$\text{Packet delivery ratio} = \frac{\Sigma\ \text{Number of packet receiveed}}{\Sigma\ \text{Number of packet send}}$$

VI. CONCLUSIONS

In this paper, we briefly introduced wireless sensor network, its application and most wildly used elements in WSN which is sensor device. Then we discussed the modes of wormhole attacks which are already existed with their models and the functional modules. The performance of wireless network with AODV provided extensions with promiscuous mode mechanism is better than wireless network with simple AODV routing protocol in terms of throughput, packet delivery ratio and end to end delay. To overcome from the detected data and the route distract we have proposed this work for perfect delivery of data without any intruders by their attacks. In Future, work on this topic will include developing any protocol that will prove much better security than existing against the wormhole attack with the help of other techniques. The parameters which we have discussed in this are packet delivery ratio, throughput and End-to-end delay. Further we can use the other parameters to simulate it in the future work.

ACKNOWLEDGEMENT

Rashidha Begam.K is a Research Scholar in Don Bosco College, Dharmapuri, TamilNadu, India and I thank my college for giving me the opportunity to present this article under Network Security. I acknowledge our Management for their moral support and cheer to present the article to enrich the values of Research. The present work is benefited from the input of, my Research Guide Mrs.M.Savitha Devi, Assistant Professor, PG & Research Department of Computer Science, Don Bosco College, Dharmapuri, TamilNadu, India. I would like to thank her, for her valuable support to the undertaking of the training shot concise here.

REFERENCES

[1] Dahill.B , Levine B. N., Royer E., and Shields C., "A secure routing protocol for ad-hoc networks," Electrical Engineering and Computer Science, University of Michigan, Tech. Rep. UM-CS-2001-037, August 2001.

[2] Mohammad Matin e-book edited "Wireless Sensor Networks - Technology and Applications", ISBN 978-953-51-0676-0, Published: July 18, 2012.

[3] Dhara Buch and Devesh, "Prevention of wormhole attack in wireless sensor network" on International Journal of Network Security and its Applications (IJBSA) , vol.3, Sep 2011.

[4] Teerawat Issariyakul, Ekram Hossain edited the e-book, "Introduction to Network Simulator NS2", 2010.

[5] Hu L. and D. Evans, "Using directional antennas to prevent wormhole attacks," Network and Distributed System Security Symposium (NDSS), 2004.

[6] Rashidha Begam.K and Savitha Devi. M, "A Complete Survey on Facts and Attacks in Wireless Sensor Networks", Volume 3 Issue 3, page 5, March 2014 in International Journal of Science and Research.

[7] Dhara Buch, Devesh Jinwala, "Detection of Wormhole Attacks in Wireless Sensor Networks", IEEE Conference on Advances in Recent Technologies in Communication and Computing, pp 7-14, 2011.

[8] Preeti Nagrath,Bhawna Gupta, "Wormhole Attacks in Wireless Ad-hoc Networks and their Counter Measurements: A survey", pp 245-250, IEEE 2011.

[9] Khin Sandar Win. "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology, 48, pp. 422-428, 2008.

[10] Vandana C.P, A. Francis Saviour Devaraj, "Evaluation of impact of wormhole attack on AODV", International Journal of Advanced Networking and Applications, ISSN 0975-0290 Volume: 04 Issue: 04 pp. 1652-1656, 2013.

