A REVIEW PAPER ON DETECTION AND PREVENTION OF WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK

Parmar Amish[1], V.B. Vaghela[2]

[1]PG Scholar, Department of E&C, SPCE, Visnagar, Gujarat, (India)
[2]Head of Department of E&C, SPCE, Visnagar, Gujarat, (India)

ABSTRACT

Wireless sensor network (WSN) is vulnerable to many kinds of attacks since they have unique characteristics like limited bandwidth, limited battery power and no specific network topology. Therefore interest in research of security in WSN has been increasing since last several years. Security is a very challenging issue in WSN as it is without infrastructure and self-governing. Wormhole attack is one of the severe attack in wireless sensor network. In this paper, the techniques dealing with wormhole attack in WSN are surveyed and an approach for wormhole detection and prevention is proposed. Our approach is based on timing measurement mechanism and other characteristics of Wormhole attack and will be implemented for AOMDV (Ad hoc on demand Multipath Distance Vector) routing protocol in WSN. Proposed approach looks very promising compared to other solutions proposed in literature. All the simulations will be performed in NS2 simulator.

Keyword- *AOMDV, malicious node, RTT, Wormhole attack, WSN.*

I. INTRODUCTION

The wireless sensor network is an approach to perform the communication using sensor nodes. The technology allows nodes in a network to communicate directly with each other using wireless transceivers without need for a fixed infrastructure. Sensor nodes are deployed in large number to monitor the environment or system by measurement of physical parameters such as temperature, pressure, characteristic of object and their motion or relative humidity. Each node of the sensor network consist of the three subsystems: the sensor subsystem which senses the environment, the processing subsystem which performs local computations on the sensed data and the communication subsystem which is responsible for message exchange with neighbouring sensor nodes. Size and cost on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The application scenarios for WSNs are many, including military surveillance, commercial, environment, medical, manufacturing and home automation to name many but few [1]. WSNs are vulnerable to variety of security attacks due to the broadcast nature of the transmission medium and fact that sensor nodes often operate in hostile environments.

Classification of security attacks in WSNs is done according the layers of the OSI model. The attacks which operate at the network layer are referred to as routing attacks. There are many types of attacks possible in

network layer like spoofed or replayed routing information, selective forwarding, sinkhole attack, Sybil attack, Wormhole attack and Hello flood attack.

Section II describes about wormhole attack in detail. Section III describes related work proposed by various authors. Section IV deliberates our proposed work for detection and prevention of wormhole attack. Section V defines the platform of implementation. In section VI we conclude.

II. WORMHOLE ATTACK

During this attack, a malicious node captures packets from one location in network and "tunnels" them to another malicious node at a distant point which replays them locally. The tunnel can be established in many ways e.g. in-band and out-of-band channel. This makes the tunnelled packet arrive either sooner or with a lesser number of the hopes compared to the packets transmitted over normal multi hop routes. This creates the illusion that the two end points of the tunnel are very close to each other. However, it is used by malicious nodes to disrupt the correct operation of WSNs routing protocols [2]. They can then launch a variety of attacks against the data traffic flow such as selective dropping, replay attack, eavesdropping etc. Wormhole can be formed using, first, in-band channel packet to another malicious node m_2 using encapsulation even though there is one or more nodes between two malicious nodes, the nodes following m_2 nodes believe that there is no node between m_1 and m_2 employ an physical channel between them by either dedicated wired link or long range wireless link shown in Fig. 1

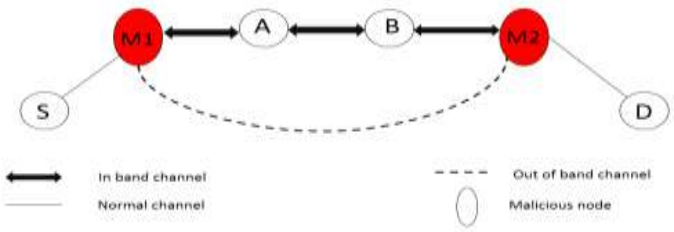

Figure 1. Wormhole Attack

When malicious nodes from a wormhole they can reveal themselves or hide themselves in a routing path. The former is an exposed or open wormhole attack, while the latter is a hidden or close one. In Fig 1, the destination D notice that the packet from the source S is transferred through the node A and B under hidden wormhole attack, while it believes that the packet is delivered via node m_1 and m_2 under exposed wormhole attack.

III. RELATED WORK

In this section we discuss some of the existing solutions to the wormhole attacks in wireless ad hoc networks and mobile ad hoc networks. Few of the solutions are as below:

S.Gupta et al [2] proposed a Wormhole Attack Detection Protocol using Hound packet called WHOP for detecting wormhole attacks without using any special hardware or monitoring system. In this method after route

discovery process source node uses a hound packet to detect wormhole attacks which counts hop difference between the neighbours of the one hop away nodes in the route. After the process the destination node detects the wormhole based on the hop, difference between neighbours of nodes exceeds the acceptance level.

The technique called 'packet leashes' [3] prevents packets from traveling farther than radio transmission range. The wormhole attack can be detected by an unalterable and independent physical metric, such as time delay or geographical location. It overcomes wormhole attack by restricting the maximum distance of transmission, using either tight time synchronization or local information. Temporal leash is to ensure that the packet has an upper bound on its lifetime. The drawback of this is that they need highly synchronized clocks. Geographical leash is to ensure that the recipient of the packet is within a certain distance from the sender. The drawback of this scheme is that, each node must know its own location and all nodes must have loosely synchronized clocks. Because clock synchronization is resource demanding, and thus, packet leashes have limited applicability in wireless sensor networks.

Chiu et al. [4] introduce a delay analysis approach called DELPHI. It calculates mean delay per hop of every possible route. DELPHI applied a multi-path approach, and recorded the delay and hope counts in transmitting RREQ and RREP through the paths. After collecting all response, the sender computes mean delay per hop of each route. The path with the wormhole attacks, the delay would be obviously longer than the normal path with the same hop count. Hence, the path with longer delays would not be selected to transmit data packet and wormhole nodes could be avoided.

Khalil et al. [5] introduces LITEWORP in which they used notion of guard node. The guard node can detect the wormhole if one of its neighbour is behaving maliciously. The guard node is a common neighbour of two nodes to detect a legitimate link between them. In a sparse network, however it is not always possible to find a guard node for a particular link.

Varsha et al. [6] presented efficient method to detect a wormhole attack called modified wormhole detection AODV protocol (MAODV). Detection of wormhole attack is performed using number of hops in different paths from source to destination and delay of each node in different paths from source to destination. It compares the delay per hop of every node in the normal path and a path that is under wormhole attack, finds that delay per hop of a path that is wormhole attack is larger in comparison of normal path. Drawback is that this method does not work well when all the paths are wormhole affected.

IV. PROPOSED MECHANISM TO DETECT AND PREVENT WORMHOLE ATTACK

Ad-hoc on-demand Multipath Distance Vector routing protocol is an extension to the AODV protocol to discover multiple paths between the source and the destination in every route discovery. In AOMDV routing protocol for communication of any two nodes the sender node checks in the route table whether a route is present or not, if the route is not present then it broadcasts the RREQ packet to its neighbours which in turn checks whether a route is present to the required destination or not, if present it gives the routing information else it broadcasts the packet. Whenever the destination receives the RREQ packet it sends RREP packet to the source along the same path through which the RREQ packet has arrived. For all RREQ packets arrived through other routes the RREP packets are sent along the same path. All the paths are stored in the routing table at

source node. In this way the routes are established [7]. The main idea in AOMDV is to compute multiple paths during route discovery procedure for contending link failure. When AOMDV builds multiple paths, it will select the main path for data transmission which is based on the time of routing establishment. The earliest one will be regarded the best one, and only when the main path is down other paths can be effective.

This paper proposed a technique to detect and prevent the wormhole attack in the network efficiently using AOMDV protocol. Details of the proposed algorithm is as follows. Note time t_1 when the source node broadcasts a RREQ packet and when the corresponding RREP packet is received by the source, again note the received time of the packet. If there are multiple RREP packets received, that means there are more than one route available to the destination node then note the corresponding times t_{2_i} of each RREP packet. By using the above two values one can calculate the round trip time t_{3_i} of the established route or routes. Take Round Trip Time of each route t_{3_i} and divide it by respective hop count. With the help of this value say t_{s_i} calculate the average round trip time of all the routes. The value obtained is threshold Round Trip Time t_{th}. Compare the threshold value with each Round Trip Time t_{s_i}. If the total Round Trip Time t_{s_i} is less than threshold Round Trip Time t_{th} and hop count of that particular i^{th} route is equal to two than wormhole link is present in that route else no wormhole link present in that route. Since wormhole link detected in that route, sender detects first neighbour node m_1 as wormhole node and sends dummy RREQ packet through that route i and neighbour m_1. At the destination end receiver receives dummy RREQ packet from its neighbour m_2 and detects neighbour m_2 as wormhole node. Routing entries for m_1 and m_2 are removed .from the source node and broadcast to other nodes. Thus wormhole affected link is blocked and is no more used. So, that from the next onwards whenever a source node needs a route to that destination, first it checks in the routing table in the route established phase for a route and it will come to know that, the route is having wormhole link and it will not take that route instead it will take another route from the routing list of the source node which is free from wormhole link if available. Advantage of using AOMDV protocol in our proposed mechanism is that, it has less overhead and end to end delay.

4.1 Algorithm

1. When sender broadcast route request packet it will note the time t_1.
2. For each route reply received by the sender node, sender node notes time t_{2_i}.
3. Sender node calculates the round trip time for all routes using a formula

$$t_{3\_i} = t_{2\_i} - t_1.$$

4. Calculate the threshold round trip time by using this formula

$$\frac{t_{3\_i}}{hop\ count_i} = t_{s\_i}$$

5. Calculate average round trip time for every route, using round trip time of different routes obtained in step 4.
6. Note this time as threshold round trip time t_{th} for each route.
7. **If** (t_{3_i} is less than t_{th} and hop count on route *i* is equals to 2 == true) **then**{

a. Detect route *i* as a wormhole link

b. Sender detects first neighbour node m_1 as wormhole node

c. Sender sends dummy RREQ through route *i* and neighbour m_1

d. Receiver receives dummy RREQ from its neighbour m_2

e. Receiver detects its neighbour m_2 as wormhole node

f. Routing table entries for m_1 and m_2 are removed and also broadcasted to other nodes

}

Else {

There is no threat of wormhole attack and it is not detected

}

End If

4.2 Diagram of Proposed Algorithm

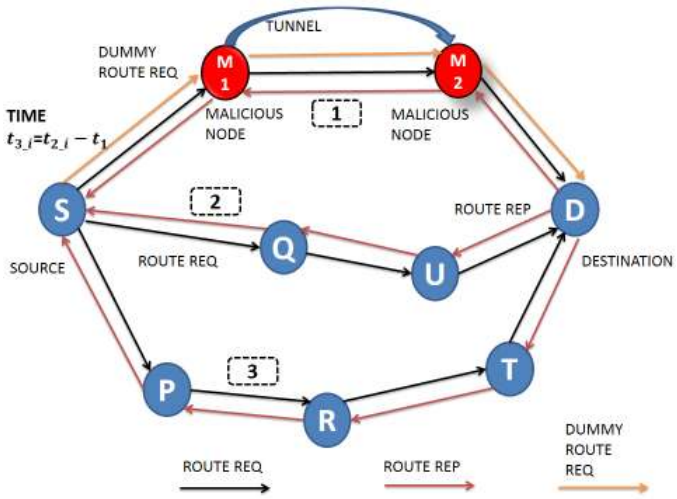

Figure 2 Route Selection of Proposed Method

The process explained in section VI sub section A. is same as presented in the above diagram. Number of the routes (*i)* is equal to 3. Route 1 is wormhole affected path and so dummy route request is sent through this path to detect the malicious nodes, thus avoid the path from being used to send the packets by source node S to destination node D.

V. SIMULATION ENVIRONMENT

The preferred Network Simulator version 2 (NS-2) is discrete event packet level simulator. NS-2 is a package of tools that simulates behavior of networks such as creating network topologies, log events that happen under any

load, analyze the events and understand the network. Network Simulator is based on two languages: C++ and OTcl. OTcl is the object oriented version of Tool Command Language. While the core of NS-2 is written in C++, one uses OTcl to write simulation scripts. Operating system used is Linux or UNIX based. Trace file is obtained at the output used for Network Animator and also for plotting X-Graph [8].

VI. CONCLUSION

In our technique no special hardware is required. All we need to do is calculate the round trip time of established route and average round trip time (RTT) of every route to calculate threshold RTT. In this strategic method not only wormhole nodes in WSNs are prevented but also detected. Future plan is to implement a new mechanism to defend against wormhole attack which could be easily integrated with AOMDV routing protocol. Effort will be done to improve the parameters like Packet delivery ratio, throughput and end to end delay. Lastly compare its result with standard methods.

REFERENCES

[1] C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks-Architecture and Protocols," Prentice Hall PTR, Theodore S. Rappaport, Series Editor.

[2] S. Gupta, S. Kar and S. Dharmaraja, "WHOP: wormhole Attack Detection protocol using hound packet". In the international conference on innovations Technology, IEEE 2011.

[3] Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE 2006.

[4] H.S. Chiu and K.S. Lui. DELPHI: wormhole detection mechanism for ad hoc wireless networks. 1st International Symposium on Wireless Pervasive Computing, Pages 6–11, January 2006.

[5] Umesh kumar chaurasia and Mrs. Varsha singh, "MAODV: Modified Wormhole Detection AODV Protocol". IEEE 2013.Pg. 239-243.

[6] Khalil S. Bagchi and N.B. Shroff. LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks. International Conference on Dependable Systems and Networks, Pg. 612–621, 2005.

[7] S. R. Biradar, Koushik Majumder, Subir Kumar Sarkar, Puttamadappa S.R.Biradar, "Performance Evaluation and Comparison of AODV and AOMDV", (IJCSE) International Journal on Computer Science and Engineering , Vol. 02, No. 02, 2010, Pg. 373-377

[8] The Network Simulator. ns-2. http://www.isi.edu/nsnam/ns/.