Transmission Time based Detection of Wormhole Attack in Wireless Sensor Networks

S.Sharmila
Research Scholar, Department of ECE,
PSG College of Technology, Coimbatore

G.Umamaheswari
Associate Professor, Department of ECE,
PSG College of Technology, Coimbatore

ABSTRACT

The open nature of wireless communication channels, lack of infrastructure and fast deployment practices make vulnerable to wide range of routing attacks. One of the most popular attacks is wormhole attack. The transmission time based detection of wormhole attack is proposed and is simulated in Network simulator (ns-2). The detection accuracy of the network is analyzed. The proposed method does not require any specific hardware.

Keywords

Routing attacks , Time, Wireless Sensor Networks, Wormhole attack.

1. INTRODUCTION

A Wireless Sensor Network (WSN) is an aggregation of sensor nodes, distributed in an environment, to sense and collect information. A typical WSN consists of low-cost, low-power, and energy-constrained sensors responsible for monitoring a physical phenomenon and reporting to access points where the end-user can access the data. Wireless Sensor networks are widely used in tracking, security, area monitoring, industrial and health monitoring. Sensor Nodes have insecure wireless communication, limited node capabilities and easily prone to threats. The adversaries can use high energy and long range communication to attack the network. Most network layer attacks such as Spoofed, Altered, or Replayed Routing information, Selective Forwarding, Sinkhole Attacks, and Sybil Attacks, Wormhole Attacks, Hello Flood Attacks and Acknowledgement Spoofing degrades the performance of the network. Among these attacks wormhole attack is investigated [1].

This paper proposed a detection scheme is based on tranmission time time. This scheme detects the wormhole link by calculating the time between the route request and reply of successive nodes in the routing path and time of CACK between the suspected nodes.The delay in time indicates the presence of wormhole link in the network. The proposed system does not require any specific hardware.

The remaining sections of the paper are structured as follows: In section 2, wormhole attack is described in detail. Section 3 explored the existing methods of detection. Section 4 discusses the proposed detection mechanism. In section 5, Simulation results are presented and compared with the existing system. Finally, a conclusion is drawn in section.

2. WORMHOLE ATTACK

An attacker receives packets at one point in the network, tunnels them to another point in the network and then replays them in to the network from that point. For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for an attacker to make the tunneled packet arrive with better metric than a normal multihop route. For example (Figure 1) a single node situated between the two other nodes forwarding messages between two of them. Since it suggests better in QoS than the other routes, it absorbs most of the transmission volume in the network. Wormhole and sinkhole attacks are particularly difficult to defend against, especially when the two are combined and. It is difficult to detect the wormhole attack in WSNs when using routing protocols in which routes are decided based on advertised information.

A wormhole attack could be launched in two different modes: hidden-mode and participation mode. In hidden mode the attackers do not use their identities so they remain hidden from the legitimate nodes. In fact, the attackers act as two simple transceivers which capture messages at one end of the wormhole and replicate them at the other end. In this way, they can make a virtual link between two far-off nodes by for example "tunneling" the HELLO messages. Clearly, the attackers require no cryptographic keys to launch the wormhole attack in the hidden mode.

In participation mode attackers possess valid cryptographic keys that can be used to launch a more powerful attack. In this mode, the attackers make no virtual links between the legitimate nodes. In fact, they participate in the routing as legitimate nodes and use the wormhole to deliver the packets sooner or with smaller number of hops. In this mode it is extremely difficult to detect since the malicious nodes can simply ignore the security mechanisms of the routing protocol. As in the hidden mode, the attackers can drop data packets after being included in the route between the source and the destination. Detection is potentially difficult when used in conjunction with the Sybil attack and in ad hoc network routing protocols.

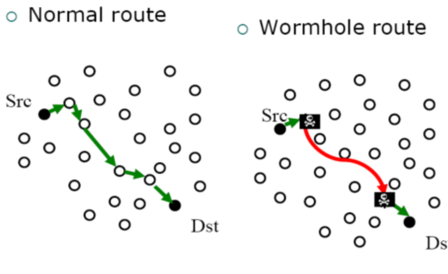

Figure 1: Example of Wormhole attack

3. REVIEW

Y.Hu, A. Perring and D.B Johnson [2] proposed a technique called packet leashed prevents packets from travelling 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. The drawback of this scheme is that each node must know its own location and all nodes must have loosely synchronized clocks. Because synchronization is resource demanding and thus packet leashes have limited applicability in wireless sensor networks. W.Wang and B.Bhargava[3] proposed multidimensional scaling – visualization of wormholes. It reconstructs the network and analyzes the abnormalities of the networks then identifies the fake connection and prevent malicious node from transmitting message. The experiment detects almost fake connection and error rate is the higher detection accuracy. This method requires a central controller and thus not readily suitable for decentralized networks.

L. Lazos, R Poovendran, C Meadows [4] describes scheme to prevent the wormhole attack on wireless ad hoc networks on the use of Location –Aware 'Guard' Nodes(LAGNs).They inherit the guard node to detect the message flow between nodes. The drawback of the scheme is that the guard nodes are required to know their location and it is suitable for dense stationary sensor networks. Cagalj, M. Capkun, S. Hubaux, J.-P.[5] presented a wormhole based ant jamming techniques in sensor networks. In this method senor nodes can exploit channel diversity in order to create wormholes that lead out of the jammed region, through which an alarm can be transmitted to the network operator..The solutions are based on wired pairs of sensors, frequency hopping, and uncoordinated channel hopping.

Zaw Tun and Aung Hteing[6] Maw proposed round trip time and neighbor numbers based wormhole detection. Detection rate depends up on the wormhole length .Bandwidth overhead and memory overhead incurred after the deployment. Majid Khabbazian, Hugues Mercier and Vijay K Bhargava [7] discuss the effect of wormhole attack on shortest path routing protocols for wireless ad hoc networks and proposed timing based to detect the wormhole attack. Zhibin Zhao, Bo Wei Dong and Gao [8] proposed a statistical Analysis and Time Constraint Algorithm for Split Multi-path Routing Protocol (SMR). The algorithm identifies the Wormhole attack when there is a dramatic change in statistics of routing information stored in the Sink Node. It consists of Statistic analysis of routing information, determination of suspected link and validation of wormhole with time constraint. It lacks to detect multiple wormhole attack in the network. Dezun Dong [9] proposed a distributed detection method which relies solely on network connectivity information. It detects the wormhole based on topology. It is suitable for continuous geometric surface where each node locally communicates with neighboring ones and homogenous nodes. In this paper, time and hop based approach is proposed.

4. PROPOSED METHOD

In this section, the detection scheme of wormhole attack is proposed. It is based on time and hop based.

4.1 Assumptions

It is assume that there are three types of nodes in a WSN: Nodes, Attackers and Base stations. The base stations are located in fixed positions and nodes are mobile nodes. All network nodes contain the same hardware and software configuration. Nodes are symmetric, node A can only communicate with node B if and only if B can communicate with A. It is assume that the sensors send their neighborhood information to the closet base station regularly in a secure way. It is assume that the node density is high enough so that the network is always connected. Routing is done using Ad hoc On Demand Distance Vector routing protocol.

Attackers exist in a pair and collude with each other to launch a wormhole link. It is characterized by the distance between the two locations that it connects and the radio ranges of its transceivers. The proposed mechanism consists of three phases. The first phase is the grid formation. The second phase is neighbor list construction. Third phase is the route construction and the wormhole detection phase.

4.2 Phase 1: Grid Formation phase.

At first with the specific terrain range, sensor nodes are divided in to virtual girds. Since nodes are scattered and also mobile. Control packets are required to identify the adjacent nodes and to identify the forward routing path. Nodes which are located far away from the base station consumes large amount of energy. Communication consumes a large amount of energy and thus reducing the node life time. In order to increase the node life time virtual grids are framed. The total terrain range which is in square of size d X d is divided equally in order to form the grids. The grid is identified with the help of x and y coordinates. Each grid contains the base station that helps in route discovery.

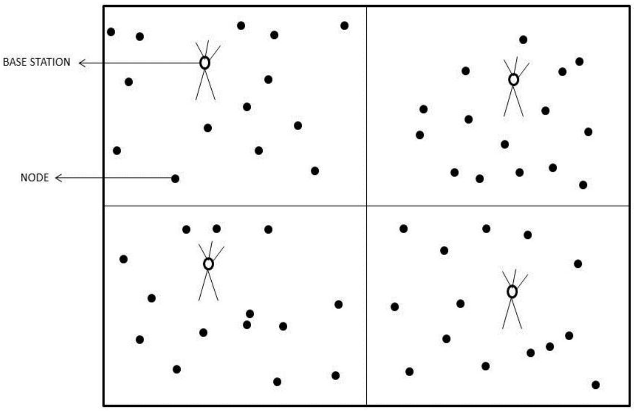

Figure 2: Grid Formation

Equation -1 is used to identify the location of the node.

$$LX = \frac{x}{d} \; and \; LY = \frac{y}{d} \qquad (1)$$

4.3 Phase 2: Construction of Neighbor list

Each node broadcast the neighbor request (REQ) message. The NREQ receiving node responds to the neighbor reply (REP) message. The requesting node constructs the neighbor list based on the received of REP messages and counts its neighbor number. The time (T) is calculated between the REQ and REP of the neighbor nodes in the routing path is calculated using Equation -2 and stores it.

$$T = Trep\text{-}Treq \qquad (2)$$

4.4 Phase 3: Detection

A routing path is identified based on the AODV routing protocol and a routing table is constructed. The data is transmitted from source to destination. The successive nodes in the routing path send an acknowledgment to its sender stating that there is no link exists between them and calculates its time. For example (Figure 3.2), the route from source(S) to destination (D) pass through node A, B, and D so which routing includes S-A-B-D . Its time is calculated based on the equation (2) and further to ensure that there is no wormhole between the successive nodes.

$$Ta = Tsa(REP) - Tsa(REQ)$$
$$Tb = Tab(REP) - Tab(REQ)$$
$$Td = Tbd(REP) - Tbd(REQ)$$

And the total time (TT) is calculated as follows

$$TT = Ta+Tb+Td \qquad (3)$$

The Route acknowledgement (Rack) between the successive nodes indicates the successful transmission of packet up to that node. After that it forwards the packet to the next neighbor node that exits in the forward routing path. In the actual routing protocol RACK is sent to the source as similar to the data packet. Wormhole attack exits in between the nodes involved in the routing path can be detected by examining the time. Under normal circumstances time ranges are similar value in range (i.e Ta=Tb=Td). If the time value may considerably higher than other successive nodes and it is suspected that wormhole link exists between the two nodes which lie in the routing path.

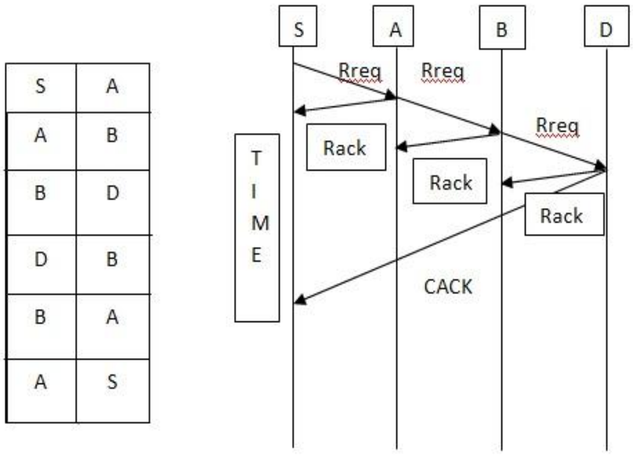

Figure 3: Transmission of Control Packets.

The CACK (Similar to the REP packet) is tranmistted through suspected nodes. Its time is calculated based on the equation -2 and is compared with the time value of succesive nodes . If it is higher than the time value of successivee nodes then the suspected nodes are wormhole nodes.

$$Tsd = Tbd(Cack) - Tbd(REQ) \qquad (4)$$

The time of Ta, Tb, Td and Tsd depends up on the distance the transmission time (RT) is calculated using the formula

$$RT = (TH^* TT) + (1-TH) * Tsd \qquad (5)$$

TH= Threshold Value lies within the limit $(0<TH<1)$

If it lies in the range nearer to 1 then RT is equal to the value of T(Ta, Tb, Td) and it denotes wormhole link does not exists in that routing path otherwise RT lies in the range nearer to 0 and it denotes the delay in time and indications that the link is utilized more. It further confirms the suspected nodes are wormhole nodes. The threshold value can be determined based on the simulation with appropriate parameters.

5. PERFORMANCE EVALUATION

In this section, the performance of the proposed scheme is evaluated using network simulator (ns2). In this experiment the network includes 50 nodes deployed randomly in a 1000 meters x 1000 meters field. The nodes are mobile nodes. The transmission range is defined 250 meters and CBR connection with 4 packets per second are created and the size of the packet is 512 bytes. Wormhole nodes are created randomly into the network and establish a tunnel between. Table –I shows the environment settings of the simulation.

Table :1 Experimental setup

No of Nodes	28 nodes
No of Grids	4
No of base station	4
Transmitting power (dBm)	15.0
Receiving power (sensitivity dBm)	-91.0
Terrain	1000 meters,1000 meters
Mobility Minimum speed Maximum speed	Random way point 0s 10s
Propagation	Radio Propagation
Simulation time(minutes)	5
Packet size(bits)	512
Detection time(ms)	590
Routing Protocol	AODV

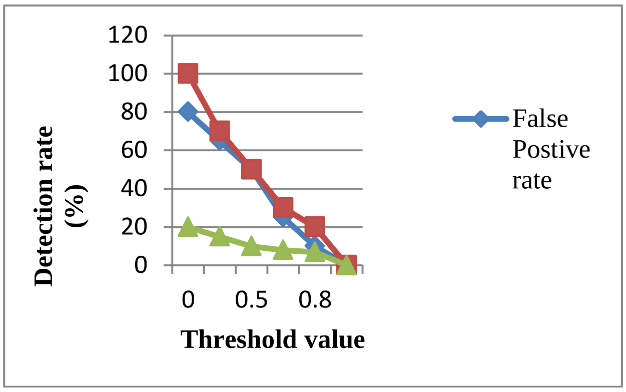

Figure 4: Detection rate

Accuracy of the detection: It is determined by the detection rate, false positive rate and false negative rate.

Detection rate: The rate at which the detection scheme detects the malicious node successfully. The rate of detection depends up on the threshold value and if it is zero, then response time will be more. This shows that the transmission time between the two malicious nodes is longer and it is easy to detect. If the threshold value lies between 0.1 to 1 there will be false detection of the malicious node. This is due that network traffic and network throughput. The false positive rate is the rate at which the detection scheme identifies the malicious nodes falsely. The false negative rate is the rate at which the detection scheme missed to detect the malicious node and is shown in the figure 5.1. From the simulation results it is observed that up to transmission speed of 12 kbps of data the proposed scheme achieves 100% detection. It is observed that the maximum throughput of network is achieved after 45ms and it depends up on network traffic.

Memory Overhead: Each node use to store the neighbor list and also to calculate time in order to detect the wormhole attack. Each node needs n*(4+ 4 + 4) bytes of memory. Where n is the maximum number of requests come to that node. The value of n depends on the traffic and the topology of the network. In our simulation n is set to 4 and each node needs 48 bytes of memory to run the mechanism.

Bandwidth: Bandwidth overhead is incurred after the detection scheme. It is calculated as (size of the REQ * number of node) + (size of the REP * length of established route)+(size of CACK * length of suspected link).In the simulation for 50 nodes and 1000x1000 space is used so the average established route path is 4.57438 and the overhead before the detection scheme is 1783.176 and after the detection scheme is 2103.168.

Energy Consumption: The energy metric is taken as the average energy consumption per node. Initially all the nodes are configured with 100 J. It is observed that the energy consumed the node after the detection scheme is 9J. This overhead happens of transmitting the CACK packet and when a new route is requested. This overhead is acceptable in exchange for higher security. From the figure 5.2 it is observed that energy value is reduced after the detection and thus improves the node life time. It also infers that for the threshold value zero, the node consumes more energy this shows that node is involved in communication for a longer time.

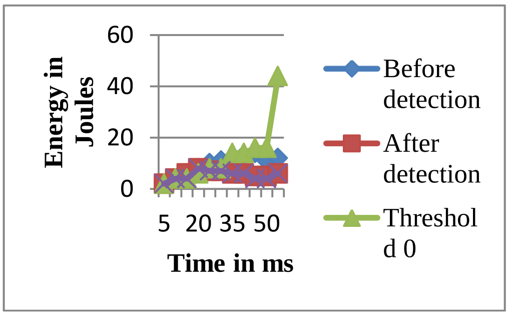

Figure 5: Energy consumption

The table 2- shows the performance of the existing system and the proposed system .Though the overheads of the proposed detection scheme are slightly higher than the existing method but the detection rate is improved. This is due to that the nodes are mobile nodes. The proposed scheme detects the wormhole link within 590ms.The scheme is able to detect the both the hidden attack and exposed attack.

Table: 2 Performance Comparison with the existing system

S.No	Parameters	Existing method[6]	Proposed Method
1	Detection Method	Round trip time and neighbor numbers	Transmission time
2	Simulation environment	NS-2	NS-2
3	Number of Nodes	50	50
4	Detection rate Based on wormhole length	100% When the length of the wormhole is greater or equal to 5	100% When the threshold value is zero
5	False Positive rate	70%	80%
6	False Negative rate	30%	20%
7	Average route established path	4.57438	4.57438
8	Bandwidth	83.6	319.992
9	Energy consumption	Not analyzed	9J
10	Memory overhead	32 bytes	48 bytes
11	Detection time	Not analyzed	590ms
12	Transmission Volume	Not analyzed	12kbps
13	Examined routing Protocol	AODV	AODV

6. CONCLUSION

In this paper, the transmission time based scheme is proposed to detect the wormhole attack using AODV routing protocol. The scheme calculates the transmission time of the route request and reply between every successive node in the routing path. The additional control packet is transmitted between the suspected wormholes for further confirmation. It is able to detect the both the hidden attack and exposed attack. The significant feature of the proposed is that it does not need any specific hardware to detect the wormhole attacks.

7. REFERENCES

[1] Chris Karlof and David Wagner, “Securing routing in Wireless Sensor Networks: Attacks and countermeasures”, Elsevier’s Ad hoc Networks J., vol.2-3, pp.293-315, Sep. 2003.

[2] Y. Hu, A. Perring, and D. B. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks,” in Proc. 22nd Annu. Conf. IEEE Computer and Communication Society, 2003, pp.1976-198.

[3] W.Wang and B.Bhargava,”Visualization of wormholes in sensor networks,” in Proc. ACM Workshop on Wireless Security (WiSe), 2004, pp.51-60.

[4] L. Laos, R. Poovendran, C. Meadows, P. Syverson and W. Chang, “Preventing Wormhole attacks on Wireless Ad Hoc Networks: A graph Theoretic Approach,” in IEEE. Conf. Wireless Communications and networking, vol 2, pp.1193-1199, 2005.

[5] Cagalj, M. Capkun, S. Hubaux, J.-P, “Wormhole based Antijamming Techniques in Sensor Networks,” IEEE Trans. Mobile Computing , vol. 6 , pp.100-114,2007

[6] Zaw Tun and Aung Htein Maw,”Wormhole attack detection in Wireless sensor networks”, World Academy of Science, Engineering and Technology, vol.46, pp 545-550, 2008.

[7] Majid Khabbazian , Hugues Mercier and Vijay K Bhargava, “Severity analysis and counter measures for the Wormhole attack in Wireless Ad hoc networks,” IEEE Trans. Wireless Communications, vol. 8, pp.736-745, Feb.2009.

[8] Zhibin Zhao, Bo Wei, Xiaomei Dong , Lan Yao , Fuxiang Gao , “Detecting Wormhole attacks in Wireless Sensor Networks with Statistical Analysis”, WASE Int. Conf. Information Engineering, pp. 251-254.

[9] Dezun Dong, Mo Li, Yunhao Liu, Xiang-Yang Li and Xiangke Liao, **“**Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks,” IEEE/ACM Trans. Networking, vol. 19, pp. 1787-1796, 2011.