Detection of Wormhole Attacks in Wireless Sensor Networks

Ms Shweta Dalke
RGPV: Electronics & Communication
,Truba College of Engineering &
Technology,Indore,INDIA

Ms Pallavi Pahadiya
RGPV: Electronics & Communication ,
Truba College of Engineering &
Technology,Indore,INDIA

Abstract— **Wormhole attacks can destabilize or disable wireless sensor networks. In a typical wormhole attack, the attacker receives packets at one point in the network, forwards them through a wired or wireless link with less latency than the network links, and relays them to another point in the network. This paper describes a distributed wormhole detection algorithm for wireless sensor networks, which detects wormholes based on the distortions they create in a network. Wormhole attacks are passive in nature.**

Keywords — Wireless sensor networks, wormhole detection, distributed algorithm.

I. INTRODUCTION

Wireless sensor networks (WSNs) [1, 12] are an emerging technology consisting of small, low-power devices that integrate limited computation, sensing and radio communication capabilities. The technology has the potential to provide flexible infrastructures for numerous applications, including healthcare, industry automation, surveillance and defense. Currently, most WSN applications are designed to operate in trusted environments. However, security issues are a major concern when WSNs are deployed in untrusted environments. An adversary may disable a WSN by interfering with intra-network packet transmission via wormhole attacks, sybil attacks [1], jamming or packet injection attacks [5]. This paper focuses on wormhole attacks .In a typical wormhole attack, the attacker receives packets at one point in the network, forwards them through a wired or wireless link with less latency than the network links, and relays the packets to another point in the network.

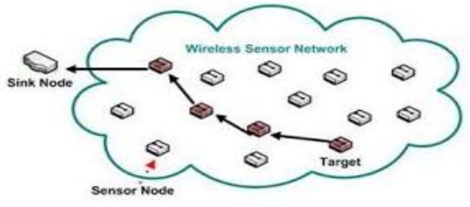


Fig1.1:Simple wireless sensor network

II. WORMHOLE ATTACK

A typical wormhole attack requires two or more attackers (malicious nodes) who have better communication resources than regular sensor nodes. The attacker creates a low-latency link (high-bandwidth tunnel) between two or more attackers in the network. Attackers promote these tunnels as high-quality routes to the base station. Hence, neighbouring sensor nodes adopt these tunnels into their communication paths, rendering their data under the scrutiny of the adversaries Once the tunnel is established, the attackers collect data packets on one end of the tunnel, sends them using the tunnel (wired or wireless link) and replays them at the other end.

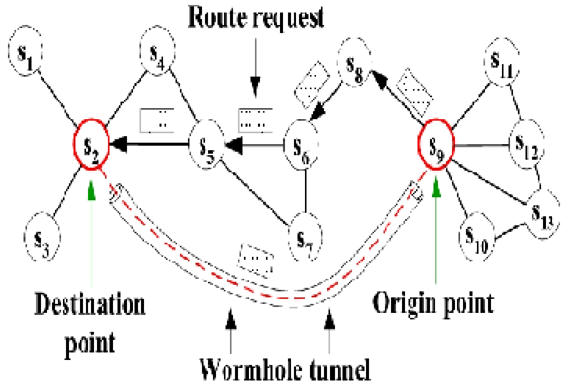


Fig 2.1:Wormhole attack in WSN

2.1 Types of Wormhole Attack
Wormhole attack can be launched by using various techniques in wireless networks. These are as follows [2]:

2.1.1 Wormhole Using Encapsulation:
In encapsulation-based wormhole attacks, several nodes exist between two malicious nodes and the data packets are encapsulated between the malicious nodes. Since encapsulated data packets are sent between the malicious nodes, the actual hop count does not increase during the traversal. Hence, routing protocols that use hop count for path selection are particularly susceptible to encapsulation-based wormhole attacks. For example, ad-hoc on-demand

distance vector (AODV) routing protocol, a source initiated on on-demand routing protocol, is one of the most popular routing protocols in WSNs. In AODV protocol, in order to limit the amount of flooding, each node broadcasts only the first route request (RREQ) message it receives and drops any further copies of the same request. However, AODV protocol fails under encapsulation-based wormhole attacks. When a malicious node at one part of the network hears the RREQ, it transmits this RREQ to the other malicious node at a distant location near the destination. The second malicious node then rebroadcasts the RREQ. The neighbours of the second malicious node receive the RREQ and drop any further legitimate RREQs that are coming from legitimate multi-hop paths. As a result, the route between the source and the destination include the malicious nodes that form the wormhole. This prevents sensor nodes from discovering legitimate paths that are more than two hops away.

2.1.2 Wormhole Using High-quality/Out-of-band Channel: In this mode, the wormhole attack is launched by having a high-quality, single-hop, out-of-band link (called tunnel) between the malicious nodes. This tunnel can be achieved, for example, by using a direct wired link or a long-range directional wireless link. This mode of attack is more difficult to launch than the packet encapsulation method since it needs specialized hardware capability.

*2.1.3 Wormhole using High Power Transmission:*In this type of wormhole attack, only one malicious node with high-power transmission capability exists in the network and this node can communicate with other normal nodes from a long distance. When a malicious node receives an RREQ, it broadcasts the request at a high power level. Any node that hears the high-power broadcast rebroadcasts the RREQ 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 another malicious node. This attack can be mitigated if each sensor node is able to accurately measure the received signal strength.

III. SIMULATION AND PERFORMANCE ANALYSIS

3.1 Simulation of Wireless sensor networks: The simulation of the wireless sensor network consists of three main scenarios. The configuration of scenarios is based on the number of nodes are deployed and the position of the source node and destination node. Initially all sensor nodes in each scenario are normal and no malicious node is present in the scenario. The standard AODV routing algorithm is used at routing protocol on network layer. The scenarios are differentiated on the basis of number of nodes present in the scenario and the nodes are deployed in a manner that they are in the range of other nodes. On the basis of scenarios the result are obtained. Each scenario simulated in two cases.

3.2 Normal scenario: In normal scenario all the nodes have same transmission power. The value of the MY-A integer variable is set before the simulation runs, this value is change at the node in scenarios. If the value of MY-A at the node is 4 than this node become a malicious node in the network. In normal scenario the value of MY-A is equals to 1 at every node in networks deployment phase. There is an assumption in the network deployment phase that in the beginning all the nodes are normal and non malicious. The source node sends the packets to the destination node through intermediate nodes in the routing path.

3.3 Scenario with malicious node: This is a next step after a normal node deployment in the scenario. In these scenarios wormhole attack is implemented. The value of transmission power of two nodes is higher than the other nodes means these two nodes have a high range of propagation distance and they communicate with each other from the long distance. One of these nodes is malicious node means the value of MY-A is 4, so it become a attacker node in the networks and those node which has a value of MY-A=4 dropped the data packets sends by the source node to destination node. Routing path in between the source and the destination is the shortest path within the network and attacker node is a intermediate node in the routing path. Attacker nodes are always trying to drop all the packet comes from the source node.

SCENARIO 1

i. Sensor network with 15 nodes and statically placed.
ii.IEEE 802.15.4 wireless standard for PHY and MAC.

iii.AODV routing protocol for mobile nodes.

iv.All nodes are fully. Functional device (FFD).

v.Network protocol IPv4 is used at nodes.

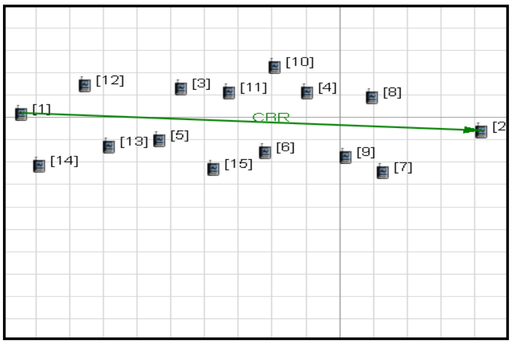


Fig3.1: Scenario-with 15 nodes

Figure 3.1 shows the scenario-2. The CBR traffic generator is from the node-1 to node-2 means node-1 wants to send the data packets to the node-2. Other nodes are the intermediate nodes in between the source node and destination node. Initially the source node finds a route for the destination node so it broadcast the route request packet. The neighbour node received the request packet.

In the figure-3.1, 15 nodes are deployed in the field and make a sensor network of 15 nodes. The source node-1 wants to send a packets or data towards the destination node-2. The distance in between the source and the destination is more as compared to previously described scenarios. All nodes are static they cannot change their position in the sensor networks. The CBR link connects to the source node and destination node. At the network layer the standard routing protocol AODV is used to send the data.

Figure 3.2 indicates route selected for sending the data packets from the source node to destination node. This route has minimum number of hops and it is a shortest path for the destination in the network.

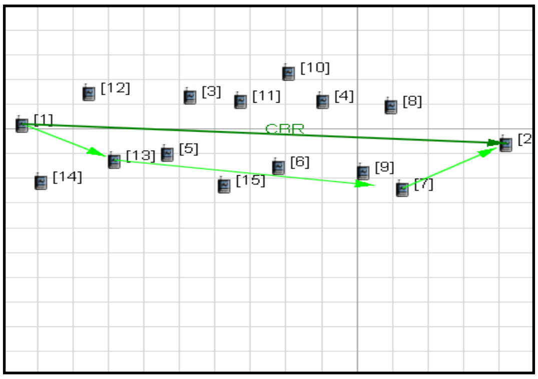
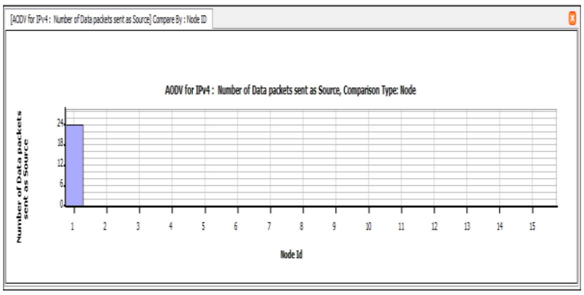


Fig 3.2: Routes Selected

The node-7 and node-13 placed near the source and the destination node. Applied AODV routing protocol finds the shortest path in between the source and destination. The route (1-13-7-2) is the shortest path in the sensor a network, which have a number of hops is 3. Once the route is selected the sender node starts sending packets towards the receiving node. If there is no attacker node is present in the route then the receiver node is received all the packets sent from the sender node

The figure-3.3 shows the number of data packets sends from the source node to the destination node. The graph is generated in analysis of the scenario. In the graph the x-axis indicates the number of data packets sends and the y-axis indicates the node id.

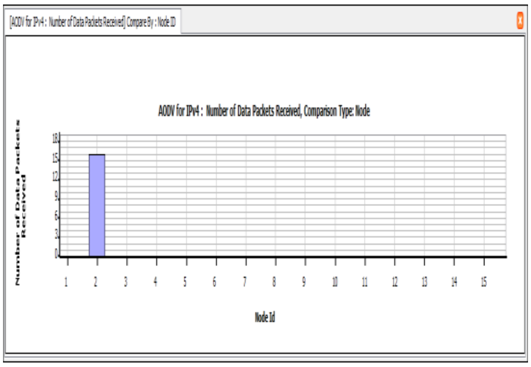

[AODV for IPv4 : Number of Data packets sent as Source] Compare By : Node ID

AODV for IPv4 : Number of Data packets sent as Source, Comparison Type: Node
Number of Data packets sent as Source
0
6
12
18
24
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Node Id

Fig 3.3: Packets Sent.

The sender node-1 sends the data packets to the receiver after selecting the route. In AODV routing protocol data sends through the shortest path in between the source and the destination.

The above figure 3.4 shows the number of data packets received by the destination node. The x-axis indicates number of data packets received and y-axis indicates the node id for received data packets.


[AODV for IPv4 : Number of Data Packets Received] Compare By : Node ID

AODV for IPv4 : Number of Data Packets Received, Comparison Type: Node
Number of Data Packets Received
0
3
6
9
12
15
18
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Node Id

Fig 3.4: Packets Received

The sender sends the data packets to the receiver at the time interval. The scenario is simulated on the Qualnet simulator. The above graph is generated in AODV statistics for IPv4 at the network layer in Qualnet simulator. Figure shows the node-2 which is the destination node in that scenario received the data packets from the source node-1

The figure3.5 shows the wormhole implementation in sensor networks. The node7 is attacker node which dropped all the packets. The destination node does not receive any data packets in the presence of attacker

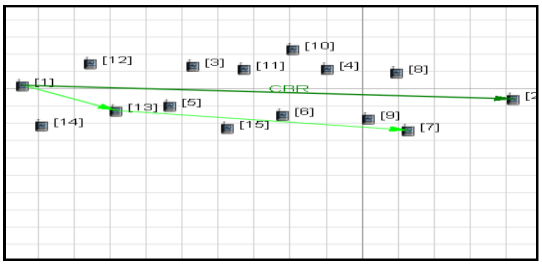


Fig 3.5: Scenario- with Attack

The green arrow line in above figure indicates the data packets sending from the node-1 to node 14 and node-13 to node-7. At the node-7 there is no green arrow line towards the node-2. The node-1 and the node-2 are source and destination respectively. The node-7 is attacker node in a networks, it can drooped all the packets comes from the node-13. Attacker node dropped the data packets not control packets from the source node or from any intermediate node.

In the figure 3.6, the packets dropped by the attacker node is mentioned. The x-axis indicates the number of data packets dropped and y-axis indicates the node id for the nodes in networks.

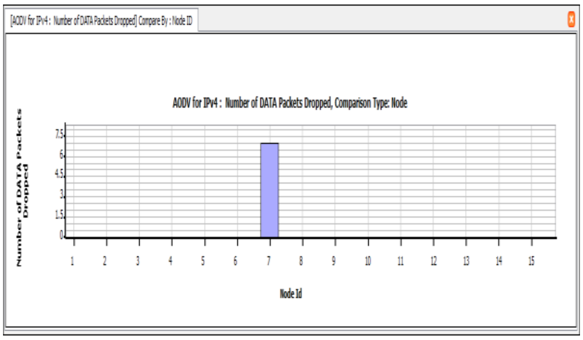

[AODV for IPv4 : Number of DATA Packets Dropped] Compare By : Node ID
AODV for IPv4 : Number of DATA Packets Dropped, Comparison Type: Node
Number of DATA Packets Dropped
7.5
6
4.5
3
1.5
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Node Id

Fig 3.6: Packets Dropped

IV. Results for Comparison for Several Node

4.1 Performance parameters in WSN

The results of this project works is based on the three different scenarios, on the basis of these scenarios this study show that the proposed work is considerable and the results of this study are acceptable.

The scenarios which are simulated in Qualnet simulator have different parameters on the basis of numbers of nodes present in the scenarios, or the number of nodes in the route path. The topologies of the scenarios are different and the attacker node deployed near the destination node each time attacker node dropped the data packets sent from the source node. The number of packets dropped more in case of malicious node and the counter measures for wormhole attacks shows that destination node still received the data packets.

4.1.1Throughput at source

The throughput at the source is calculated as follows:

If the session is complete, i.e., if all packets have been sent before the simulation ends, throughput = (total bytes sent * 8) / (time last packet sent - time first packet sent), where the times are in seconds.

If the session is incomplete, i.e., if all packets have not been sent before the simulation ends, throughput = (total bytes sent * 8) / (simulation time - time first packet sent), where the times are in seconds.

- Throughput at destination

Throughput is the average rate of the successful message delivery over communication channel. The throughput is usually measured in bits per second (bits/sec or bps) or sometimes in data packets per second or data packets per time slot

The throughput at the destination is calculated as follows:

If the session is complete, throughput = (total bytes received * 8) / (time last packet received - time first packet received), where the times are in seconds.

If the session is incomplete, throughput = (total bytes received * 8) / (simulation time - time first packet received), where the times are in seconds.

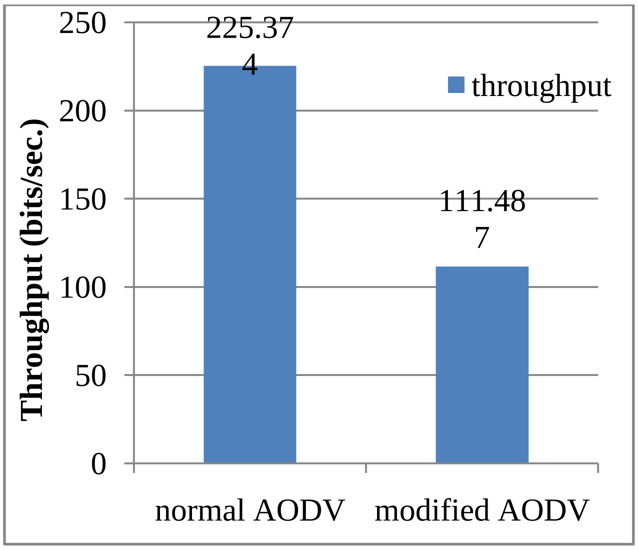


Fig 4.1: Avg. throughput at destination

The above figure 4.1 shows the result for scenario-2. In scenario-2, 15 sensor nodes (FFD) are deployed in the field. A pair of source and destination sent the packets to each other. The above figure analyzed on AODV routing statistics. On x-axis the figure indicates the throughput (bits/sec) and the y-axis indicates the different cases on AODV routing protocol

Compared results

TABLE no 4.1 Avg. throughputs (scenario-2).

	Normal AODV	Modified AODV
Throughput (bits/sec)	225.374	111.487

Percentage reduction in throughput

= 255.374 – 111.487)/255.374*100
=143.887/255.374*100
=56.34%

The average reduction in the throughput at scenario-15 node is 56.34 %.

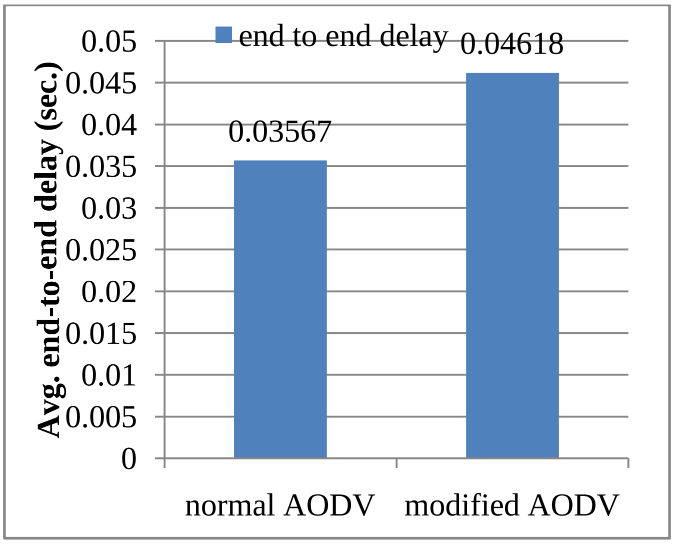


Fig 4.2: Avg. end to end delay (scenario-15 node)

The above figure 4.2 shows the result for scenario-15 node. In scenario-15 node, 15 sensor nodes (FFD) are deployed in the field. A pair of source and destination sent the packets to each other. The above figure analyzed on AODV routing statistics. On x-axis the figure indicates the end-to-end delay (sec.) and the y-axis indicates the different cases on AODV routing protocol.

Compared results

TABLE no 4.2 Avg. end to end delays at destination (scenario-15 node)

	Normal AODV	Modified AODV
End to end delay	0.03567	0.04618

Percentage gain end to end delay

= (0.04618 – 0.03567)/0.03567*100
=0.01051/0.03567*100
=29.46%

The average gain in the end to end delay at scenario-2 is 29.46 %.

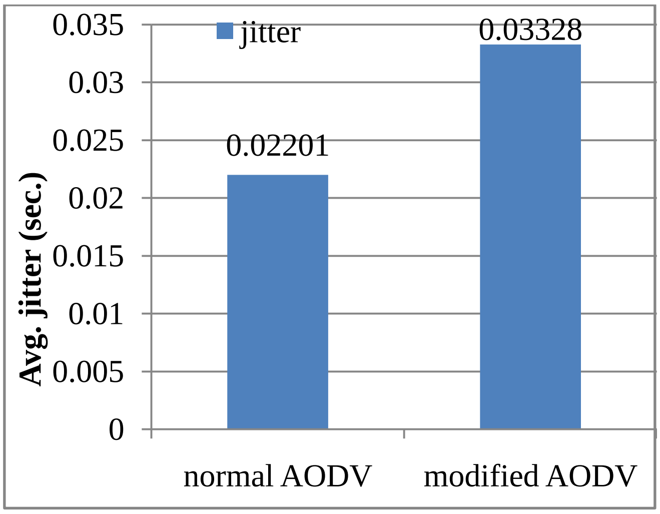


Fig 4.3: Avg. jitter (scenario-15 node)

The above figure 4.3 shows the result for scenario-2. In scenario-15 node, 15 sensor nodes (FFD) are deployed in the field. A pair of source and destination sent the packets to each other. The above figure analyzed on AODV routing statistics. On x-axis the figure indicates the Avg. jitter (sec.) and the y-axis indicates the different cases on AODV routing protocol.

Compared results

TABLE no 4.3 Avg. Jitters at destination (scenario-15node)

	Normal AODV	Modified AODV
Avg. jitter	0.02201	0.03328

Percentage gain in jitter

= (0.03328 – 0.02201)/0.02201*100
= 0.01127/0.02201*100
=51.20

The average gain in the jitter at scenario-2 is 51.20 %.

V. CONCLUSION

This research work carried out the detailed study and analysis of AODV routing protocols and security issues and attacks in WSN theoretically and through simulation. This research work proposed technique namely modified AODV for wormhole attack. To evaluate the performance of proposed techniques, simulation of wormhole attacks along with the simulation of proposed technique had been done.

REFERENCES

1. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", in Elsevier's Adhoc Network Journal Special Issue on Sensor Network Application and Protocols, vol.l, issue.2-3, pp.293-315, September2003
2. Devesh Jinwala, "Ubiquitous Computing: Wireless Sensor Network Deployment, Models, Security, Tbreats and Challenges", in National conference NCIIRP-2006, SRMIST, pp. 1-8, April 2006.
3. Rouba EI Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy, "DA WWSEN: A Defense Mechanism against Wormhole Attacks In Wireless Sensor Networks", in The Second International Conference on Innovations In Information Technology , pp. 1-10, 2005.
4. M. G. Zapata and N. Asokan. Securing ad hoc routing protocols. In WISE, September 2002.
5. AI-Sakib Khan Pathan, Hyung-Woo Lee, and Choong Seon Hong. Security in wireless sensor networks: issues and challenges. In Proc. of the 8th International Conference on Advanced Communication Technology, volume 2, Feb. 2006, pp. 1043-1048.
6. Qualnet Developer Website https://www.scalable-networks.com/products/qualnet/.
7. I. Khalil, S. Bagchi, and N.B. Shroff. "LITEWORP: A lightweight countermeasure for the wormhole attack in multi-hop wireless networks," Proceedings of the International Conference on Dependable Systems and Networks, pp. 612−41, 2005.
8. T. Korkmaz. "Verifying physical presence of neighbors against replay-based attacks in wireless ad-hoc networks," International Conference On Information Technology: Coding and Computing 2005(ITCC 2005), pp. 704−9, 2005.
9. Y.C. Hu, A. Perring, and D. Johnson. "Rushing attacks and defense in wireless ad-hoc network routing protocols," ACM Workshop on Wireless Security, pp. 30−40, 2003.
10. L. Buttyan and J.P. Hubaux. "Security and cooperation in wireless networks," Cambridge University Press Textbook, Draft Ver.1.5.1, 2007.
11. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, A survey of sensor networks, IEEE Communications, vol. 40(8), pp. 102–114, 2002.
12. S. Capkun, ˇ L. Butty´an and J. Hubaux, SECTOR: Secure tracking of node encounters in multi-hop wireless networks, Proceedings of the First ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 21–32, 2003.
13. W. Du, L. Fang and P. Ning, LAD: Localization anomaly detection for wireless sensor networks, Journal of Parallel and Distributed Computing, vol. 66(7), pp. 874–886, 2006.
14. L. Hu and D. Evans, Using directional antennas to prevent wormhole attacks, Proceedings of the Eleventh Network and Distributed System Security Symposium, pp. 131–141, 2004.