Detection of Wormhole Attack Based on RTT in Wireless Sensor Network

Dimpy Patel[1], prof. Manish Patel[2]

[1]*computer engineering, s.r patel engineering college, dabhi,* [2] *computer engineering, s.r patel engineering college, dabhi*

dimpy.patel30@gmail.com

mmpatel.comp@srpec.org

ABSTACT: The wireless sensor network is a network that is used for hostile environments that make it unsecure many attacks disturb a network and one of this is wormhole attack. In wormhole attack malicious node create high power tunnel between two node. Malicious node receive packet from network tunnel that packet to another malicious node and between this it can modify or delete a packet. Wormhole attack is very hard to detect and it affect a network very much. In this thesis we proposed a method that is used to detect a wormhole link. In first step node count neighbor number and second step node count RTT to its neighbor to detect a wormhole attack in a network.

KEYWORDS: WSN, security, confidentiality, integrity, authentication.

I INTRODUCTION

Wireless sensor network consists of thousands of sensor node this sensor node has very limited resources in terms of energy and power. WSN used in many application such as Military Applications, Medical Application, Environmental Monitoring, Industrial Applications, etc. The sensor network has many limitation such as

- Lack of a-priori knowledge of post-deployment position.
- Limited bandwidth and transmission power
- Unreliable Communication
- Collisions and latency
- Unattended after deployment
- Remotely managed

Because of above limitation sensor network are open for many security threats. Generally WSN is deployed in hostile environment, and operated on an unattended mode, network will be exposed for many security threats. Security goal are as follow

- Confidentiality
- Integrity
- Availability
- Non-repudiation
- Authentication
- Authorization
- Anonymity

Wormhole attack create a low latency link (high bandwidth link) between two malicious node. One malicious node receive packet from a network and tunnel this packet to another malicious node in between this tunnel malicious node can drop a packet modify a packet and can only read the packet. Here two malicious node are hidden in a network. Creation of wormhole attack is simple but to detection of wormhole attack is crucial task. There is many method to detect a wormhole attack in a network some of them is explained in this paper.

Figure 1 shows a wormhole attack in a network w1 and w2 is a malicious node w1 receive packet from a network and tunnel that packet to second malicious node w2.

A malicious node used for wormhole attack has higher communication range then normal sensor node. Wormhole link between malicious node is wired or wireless link.it shorter a path from node to base station so as per AODV scenario it forward packet to this link.

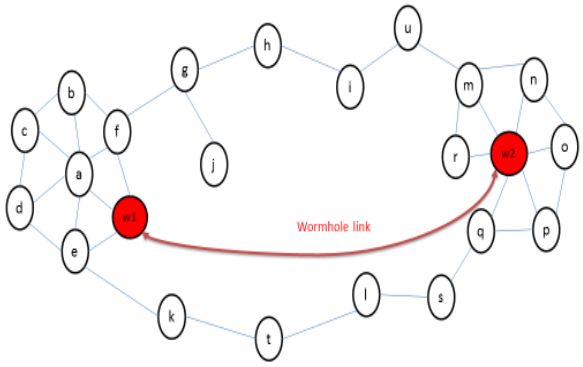

Fig. 1 Wormhole attack

II RELATED WORKS

In [1] author introduce two leaches: temporal leaches and geographical leaches. Temporal leaches bound life time of a packet and geographical leaches bound distance between sender and receiver. In [2] each node occupied with special device direction antenna. When node send a packet its neighbor node receive that packet in opposite zone. This techniques is efficient but node have a special device that is direction antenna. A graph theory based approach is used in [3]. Using MDS it find a network layout and if layout is flat that means there is no wormhole and if layout is band that means there is wormhole present in a network and then it locate that link. In [4] using statistical analysis it find a suspicious link and after that using RTT it verify a wormhole link in a network. In [5] it calculate RTT between all successive node if there is no wormhole present in a network the RTT between all successive node is nearly a same and if wormhole link present in two successive node than RTT of that two successive node is higher than other. In [6] author introduce three network property: **Self-exclusion property –** A node cannot here a message from itself. **Packet uniqueness property –** A node cannot receive more than one copy of packet from its neighbor. **Transmission constraint property –** A node cannot communicate with node outside its transmission range. If network violate any of above property that means there is wormhole link present in a network.

III PROPOSED WORK

Phase 1: Count Neighbor Number (NN)

Each node broadcast a HELLO packet. The node that receive a HELLO packet respond to REPLY packet. The node construct a neighbor list according to REPLY packet and count neighbor number (NN). If suddenly neighbor number is increases and it is higher than average neighbor number (ANN) it go to phase 2.

Phase 2: Calculate RTT for Each Neighbor

It count a RTT from each neighbor from following equation. RTT = $Trep$ - $Treq$ The RTT time is higher than average RTT that means node is not a genuine neighbor and RTT time is not higher that means it is a genuine neighbor.

Proposed Algorithm

Step1: Count Neighbor Number (NN)

If (NN>ANN) then

Go to step 2.

Step2: Calculate RTT from all neighbor

RTT = $Trep$ - $Trep$

If (RTT>ARTT) then

The node connected through tunnel

else

It is genuine node

Flowchart of Proposed Method

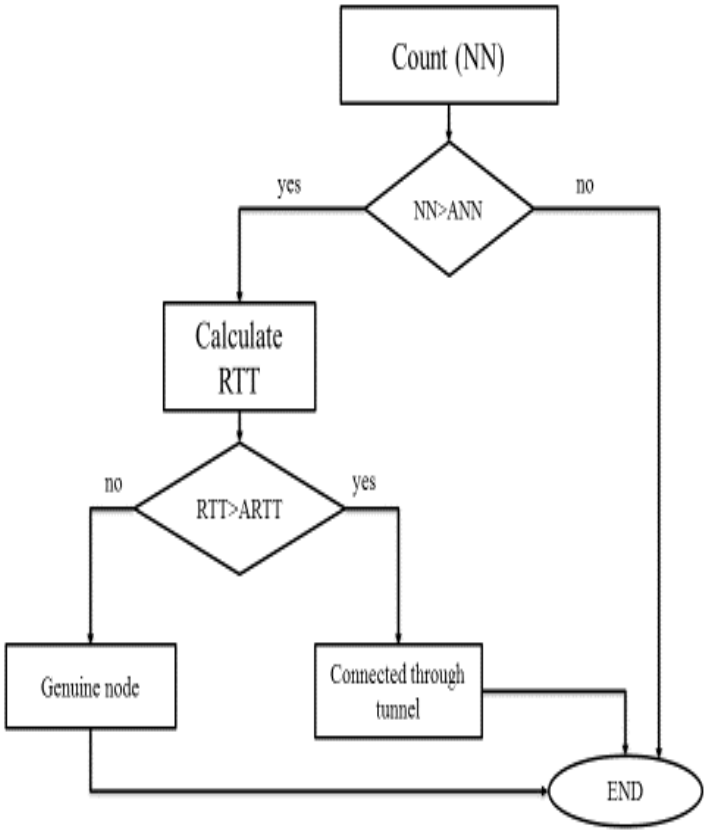

Fig. 2 flowchart of proposed method

IV SIMULATION AND RESULT

Simulation Parameter

Parameter	Value
Area	500 × 500 m
Number of Nodes	10,20,30
Routing Protocol	AODV
Packet Size	512 bytes
Simulation Time	200 s
Traffic	CBR

Table. 1 simulation parameter

Simulation on Different Node Distribution Techniques

We use two different node distribution techniques for wireless sensor network (WSN) one is random node distribution and second is grid distribution.

Random node distribution - In random distribution node is distributed randomly in area.

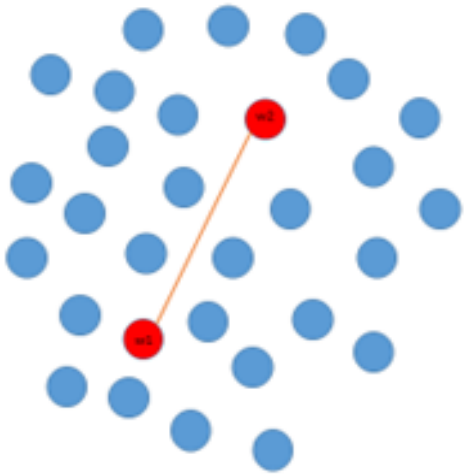

Fig. 3 random node distribution in WSN

As shown in figure 5.1 node are distributed randomly and one wormhole link present in this network and that link cover almost whole network. We take result of this situation and graph shows result.

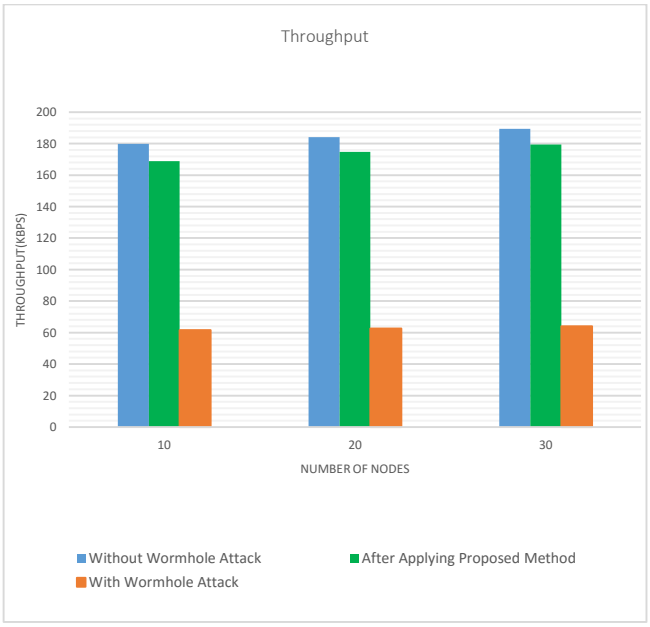

Fig. 4 Throughput in Random distribution

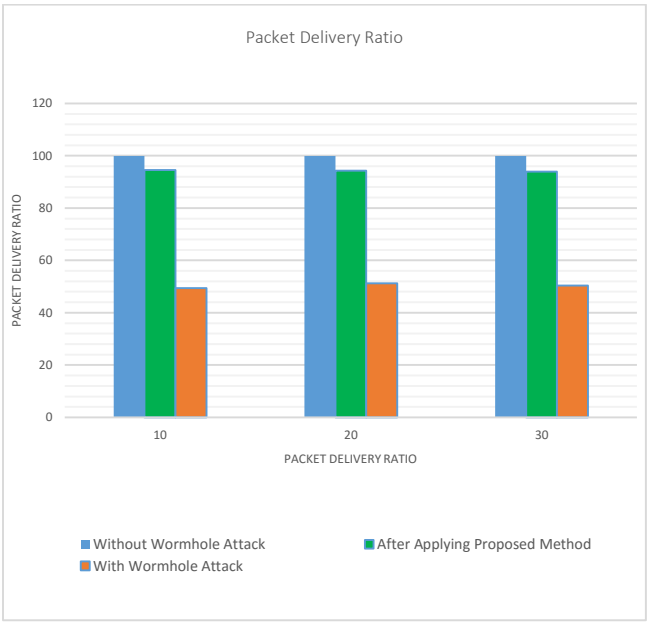

Fig. 5 Packet delivery ratio in random distribution

Grid distribution - In grid distribution node are distributed flat and linear in an area.

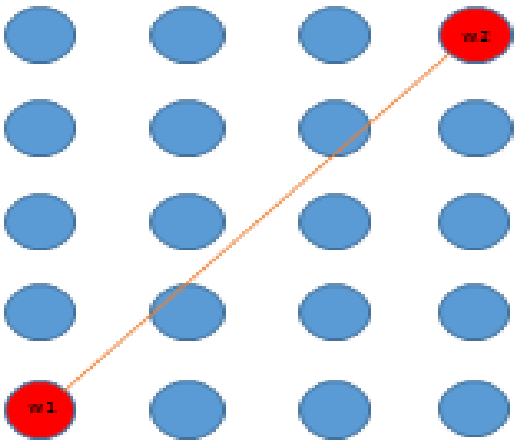

Fig. 6 grid distribution in WSN

As shown in figure 5.4 all node are distributed linearly in a network here one wormhole link is present in network that is in diagonal node.

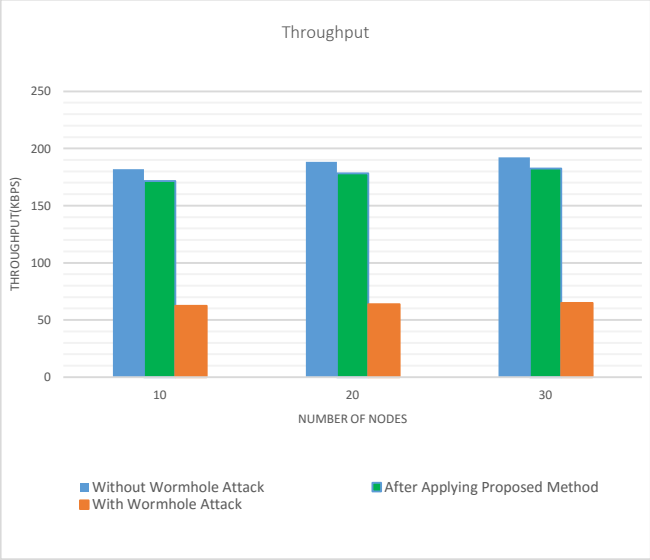

Fig. 7 Throughput in grid distribution

Fig. 8 Packet delivery ratio in grid distribution

V CONCLUSION

Security comes from attacks. Detection of wormhole attack is very crucial in wireless sensor network because it harm a network very badly. Our proposed method use neighbor number to find wormhole link and then use RTT for verification.

REFERENCES

1. Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," Proc. IEEE Conf.Infocom, April 2003.
2. L. X. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," Proc. IEEE Symp. Network and Distributed System, Security (NDSS 04), San Diego; February 2004.
3. B. B. W Wang, "Visualization of wormholes in sensor networks," 2004, in Proceedings of ACM Workshop on Wireless Security (WiSe), in conjunction with MobiCom.
4. Zhibin Zhao, Bo Wei, Xiaomei Dong, Lan Yao, Fuxiang Gao" Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis" WASE International Conference on Information Engineering, 2010 IEEE.
5. S.Subha, UGowri Sankar, " Message Authentication And Wormhole Detection Mechanism In Wireless Sensor Network" 9th International Conference on Intelligent Systems and Control (ISCO), 2015 IEEE
6. Junfeng Wu, Honglong Chen, Wei Lou, Zhibo Wang, and Zhi Wang "Label-Based DV-Hop Localization Against Wormhole Attacks in Wireless Sensor Networks" Fifth IEEE International Conference on Networking, 2010 IEEE.
7. Yan-Xiao Li, Lian-Qin, Qian-Liang "Research On Wireless Sensor Network Security" 2010 International Conference on Computational Intelligence and Security.
8. Yong Wang, Garhan Attebury, and Byrav Ramamurthy "A SURVEY OF SECURITY ISSUES IN WIRELESS SENSOR NETWORKS" Communications Surveys & Tutorials, IEEE 2006.
9. Thanassis, Giannetsos, Tassos Dimitriou, Neeli R. Prasad "State of the Art on Defenses against Wormhole Attacks in Wireless Sensor Networks" IEEE 2009.