Survey of Wormhole Attack Detection Techniques in Wireless SensorNetwork

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

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

dimpy.patel30@gmail.com

mmpatel.comp@srpec.org

***Abstract*: WSN (wireless sensor network) is a network that is establish in hostile environment and this network is remotely managed that increases their vulnerable to attack. There is many attacks but wormhole attack is easy to deployed and hard to detect in a network. In wormhole attack malicious nodes create low latency link in the network. It receive packet from one end tunnel that packet to another end. In this paper we have surveyed many existing methods for wormhole attack detection with merits and demerits.**

Key word - WSN, Wormhole attack, Security, Sensor node.

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

Ii Various Attack in WSN

1. **Active Attack**

Active attack in which hacker interrupt network normal functionality means information interruption and modification.

a) Blackhole Attack – In this attack malicious node receive packets from network and drop all packet. It does not forward Packet in a network.

b) Grayhole Attack – This is a variant ofblackhole attack. Here malicious node drop some packet and some packet forward in a network that's way it is also called selective forward attack.

c) Denial of Service Attack – In this attack aim of malicious node to jam the network. It create traffic in a network by sending unnecessary fake packets. It is also called jamming attack.

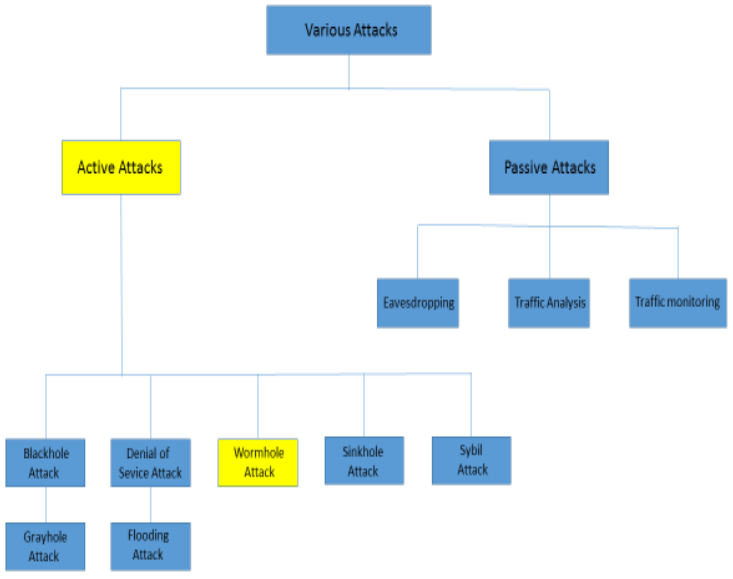


Fig. 1Various attacks in WSN

d) **Flooding Attack –** This is type of denial of service attack. In this malicious node send fake RREQ packet to create a traffic in a network.

e) **Sinkhole Attack –** The goal of attacker to lure all the traffic from particular area for this malicious node advertise that it has better quality line to the base station and attract all traffic.

f) **Sybil Attack –** Here malicious node pretend to be more than one node using different identities of other genuine node.

2. **Passive Attack**

Passive Attacks in which attacker does not interrupt a network just only read the information.

a) **Eavesdropping –** In this attacker gain confidential data from a network which should be secret during all communication in a network. This is any secret key of a node.

b) **Traffic Analysis –** Inthis attacker only observe which node will communicate with which node in network.

III Introduction of Wormhole Attack

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 2 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.

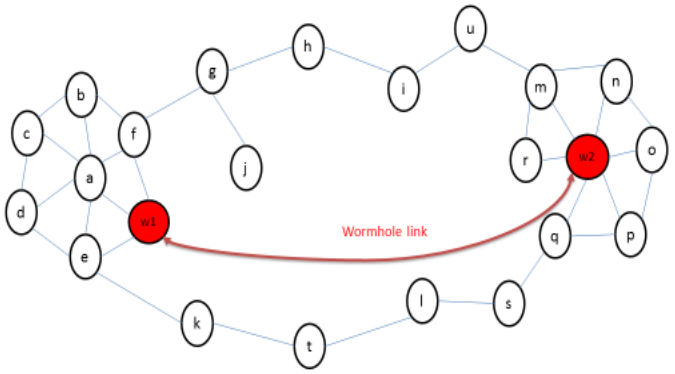


Fig.2 Wormhole attack

IVExisting Methods to Detect Wormhole Attack

1. Packet Leaches Based Technique*[1]*

In this method author introduce two leaches: geographical leaches and temporal leaches.

Geographical leaches required node know its own location for this sensor node required a GPS device. It maintain loosely clock synchronization. It bound a distance between nodes. When any node receive a packet it compute an upper bound on the distance between sender and itself and discard a packet if it has higher distance then threshold.

Temporal leaches bound lifetime of a node for this node have to maintain tightly synchronized clock so it has special device to synchronic a clock. In this method node add time stamp into packet header. When other node receive packet it compere time stamp to its own time and based on this it calculate a travel distance.

2. Using Direction Antenna*[2]*

In this method every sensor node has a special device directional antenna to examine direction of received packet. Antenna has higher transmission range then omni direction antenna it reduce hop count and connect node that is originally not connected.

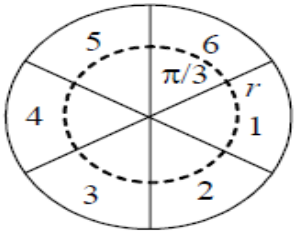
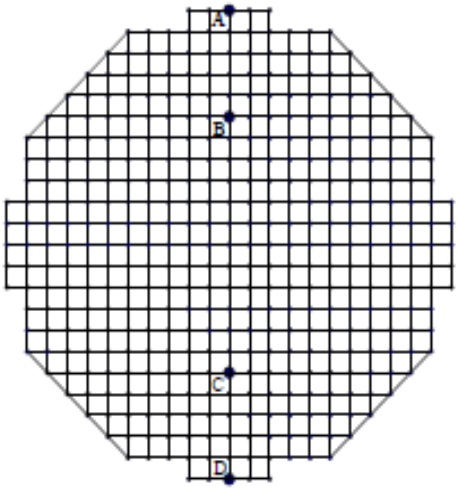


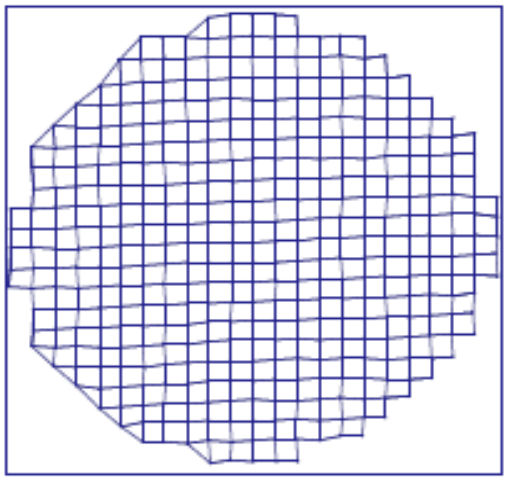
Fig. 3 Directional antenna with 6 zones*[2]*

A node accept each other as neighbor if they are in opposite zone. When node receive a packet it find direction of signal and if this signal does not received by opposite zone it discard a packet.

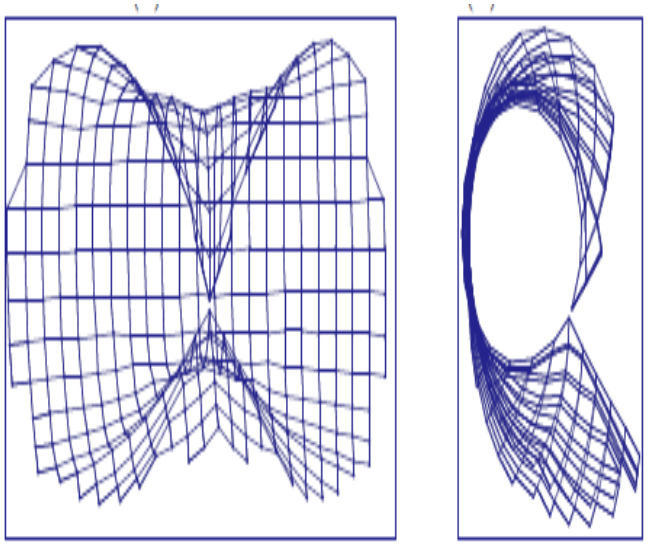
3. Graph Theory Based Approach: Network Visualization *[3]*



(a)



(b)



(c)

Figure 4. (a) Shows the original sensor network (b) Shows the reconstructed network using MDS when no wormhole exists. (c) The wormhole will pull the sensors at the two ends to each other through the fake connection, and results in a bent surface*[3]*

In this method author use MDS technique to determine network layout. Figure 4 [a] is original sensor network here no wormhole present in a network. Figure 4 [b] is network that is reconstructed by MDS algorithm that is same as original network that means there is no wormhole present in a network. If there is wormhole present in a network a network is not a flat as shown in figure 4 [c]. This techniques show network distortion that are generated by wormhole in a network.

4. The SA-TC algorithm [4].

This algorithm consists of tree step.

a) Statistics analysis on routing information

In this step it create set R contain all routes that is used in network. Set R contain number of links. A link appear several time in R. using set R it find average usage of links in a network.

b) Determination of the suspicious link set

It create a set of links that are appear more than average usage of link and called that link to suspicious link.

c) Time constraints for wormhole link validation

Here it send probe message to calculate time. When reply message come it compere it to average time and find wormhole link.

d) Based on RTT techniques [5]

Here four step is used to detect wormhole link.

a) Route Finding

Send a route request R_{req}message and save time T_{req} when it reach to destination node, it reply route reply R_{rep} message and save time T_{rep}. Intermediate node do same procedure. From this all node calculate RTT.

b) Construction of neighbor list

It send neighbor request message $N_{req.}$ A node receive this message reply with N_{rep}message and from this it construct neighbor list**.**

c) Wormhole Attack Detection

It calculates the RTT of successive nodes and compares the value. If there is no attack, the values of them are nearly the same. If any successive nodes has RTT value is higher than other successive nodes, it can be detected as wormhole attack between this link.

d) Calculation of RTT

In this step RTT of all successive node is calculated and compere this all with each other.

5. Pworm scheme [6].

a) Packet marking

In this step it add mark field in packet header. This mark field contain mark ID preceding node ID and MAC.

b) Mark parsing

When packet is mark a parsing module check whether MAC is correct or not. If MAC is wrong than it create attacking report.

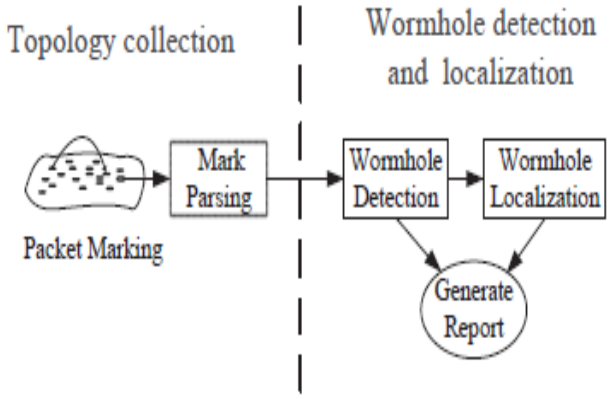


Fig. 5Pworm architecture *[6]*

c) Wormhole detection and localization

After mark parsing it reconstruct all path in a network and variation of path show wormhole attack. Wormhole link has several properties like it attract nearly all traffic and many path are change according that traffic. Pworm also consider that wormhole link decrees path length.

6.* Labeled based approach *[7]

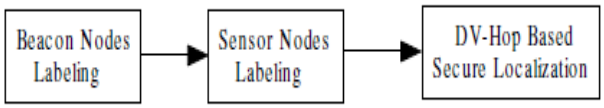


Fig. 6 Flowchart of labeled based DV-hop localization scheme [7]

Author introduce three definition for node labeling.

1) **Duplex Wormhole Attack –** If node lies in common transmission area of two attacker area than it called that node is under a duplex wormhole attack.
2) **Simplex Wormhole Attack –** If node is lie in only one transmission area of attacker than it called node is under simplex wormhole attack.
3) **Pseudo Neighbor –** A node is communicated with wormhole link than it called pseudo neighbor.

Three network property.

1) **Self-exclusion property** – A node cannot here a message from itself.
2) **Packet uniqueness property** – A node cannot receive more than one copy of packet from its neighbor.
3) **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.

Table 1. Compassion of method

Method name	Advantages	Disadvantages
Packet Leaches Based Technique	Temporal leashes is highly efficient.	Requires GPS device and tight clock synchronization .
Using Direction Antenna	It is simpler than using location information.	Requires a special device directional antennas in sensor node.
Graph Theory Based Approach: Network Visualization	Not requires any special hardware.	It is considerably susceptible to distance estimation errors especially for sparsely located network nodes.
The SA-TC algorithm	Not required any special hardware.	Every node should have ainformation about neighboring node.
Based on RTT techniques	Not required any special hardware.	Delay has many reason not only wormhole link.
Pworm scheme	Reduce network overhead.	The wormholes may not be detected if they attract little traffic.
Labeled based approach	Not requires any special hardware.	Assume that the network has no packet loss.

V Conclusion

In this paper we reviewed one of the most routing attack wormhole attack that can degreed network performance. Detection of wormhole attack in network is quite complicated. This attack is easy to deployed and hard to detect. There are many techniques that are used to detect wormhole in a network some of them are discussed here with advantages and disadvantages.

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, UGowriSankar, " Message Authentication And Wormhole Detection Mechanism In Wireless Sensor Network" 9th International Conference on Intelligent Systems and Control (ISCO), 2015 IEEE
6. Guoxing Luo, Zhigang Han, Li Lu, Muhammad Jawad Hussain "Real-time and Passive Wormhole Detection for Wireless Sensor Networks", 2014 IEEE.
7. 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.
8. Yan-Xiao Li, Lian-Qin, Qian-Liang "Research On Wireless Sensor Network Security" 2010 International Conference on Computational Intelligence and Security.
9. Yong Wang, GarhanAttebury, and Byrav Ramamurthy "A SURVEY OF SECURITY ISSUES

IN WIRELESS SENSOR NETWORKS" Communications Surveys & Tutorials, IEEE 2006.

10. Thanassis, Giannetsos, TassosDimitriou, Neeli R. Prasad "State of the Art on Defenses against WormholeAttacks in Wireless Sensor Networks" IEEE 2009.