# Detecting Wormhole attack in Wireless Sensor Network using Localization

Ajay Jangra
Astt. Prof, CSE department
University Institute of Engineering & Technology,
Kurukshetra University Kurukshetra, INDIA
ajay.jangra@uietkuk.org

Bhavana
M.Tech. Scholar, CSE department
University Institute of Engineering & Technology,
Kurukshetra University Kurukshetra, INDIA
er.bhavanachoudhary@gmail.com

***Abstract*-Wireless Sensor Network is an emerging technology that shows great promise for various futuristic applications both for mass public and military. The sensing technology combined with wireless communication and processing power makes it lucrative for being exploited in abundance in future. Sensors used for real time response capability also make it difficult to devise the resource intensive security protocols because of their limited battery capacity, power, memory and processing capabilities. Use of wireless medium and inherent collaborative nature of the network protocols make such network vulnerable to various forms of attacks. Out of these various types of attacks, one of the most severe attacks to detect and defend in wireless sensor network is wormhole attack, in which an attacker records packets at one location in the network and tunnels them to another location, retransmitting them into the WSN and it either drops or selectively forwards the packets. In this paper, propose wormhole detection procedure for WSN, based on range-free localization methods; this approach performs the wormhole detection after the conclusion of the localization discovery protocol.**

***Keywords- WSN, wormhole attack, Affects, techniques***

## I. INTRODUCTION

Sensor networks are distributed networks that consist of small, lightweight wireless nodes, deployed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, sound, humidity. Sensor node collects the information from the scene of event and sends the data to a sink node or base station. Each node of sensor network consists of three subsystems: Sensor Subsystem which senses the environment (physical and environmental data). Processing Subsystem performs the local computation on the sensed data. Communication Subsystems is responsible for message exchange with neighboring sensor nodes. Wireless sensor network has restricted resources in terms of battery power, energy, bandwidth and capabilities of processing and storing data. Due to these resource constraint, some wireless network application work without security which decrease the quality of service.

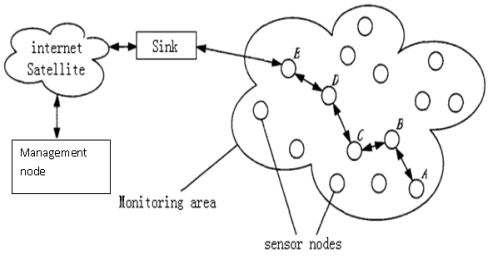


Fig 1. Wireless Sensor network

Wireless Sensor Network are deployed in hostile environments like military battle field, habitat monitoring, nuclear power plants, target tracking, fire and flood detection, security becomes more important because wireless networks are prone to different kinds of attacks and wireless communication links can be eavesdropped and communication protocols on all layers are vulnerable to specific attacks. Wormhole attack is one of the most severe security threats in sensor networks. An adversary connects two distant points in the network using a direct low-latency link called the wormhole link. Once the wormhole link between malicious nodes is established, the adversary captures transmissions at one end, sends them through the wormhole link and replays them at the other end in the network. The tunnelling or retransmitting of bits could be done selectively. This attack can confuse routing, data aggregation and sensor querying protocols.

## II. WORMHOLE ATTACK

In wireless sensor network, a malicious node can join the network discretely and compromise network security from the inside as in the wormhole attack. A wormhole is a direct communication link between two malicious nodes; an attacker receives packets at one point in the network, tunnels them through their private link and replays them at another location in the network. Wormhole attack is a network layer attack that can affect the network even without the knowledge of cryptographic techniques and this attack does not inject abnormal volumes of traffic

into the network. That's why it is very difficult to detect.

This kind of attack does not need to decrypt any code in the network or infect any node in the network to achieve its harmful objective; therefore detecting wormhole attack is a way to improve network security beyond cryptographic protection techniques.

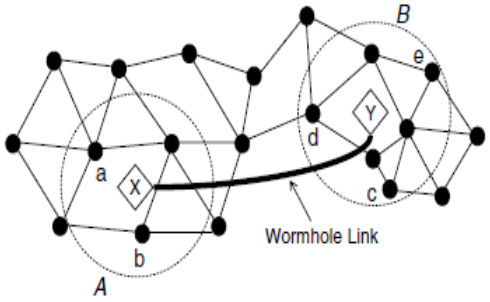


Fig 2. Wormhole attack

Ritesh Maheshwari et. Al [2] explains the wormhole attack using an example. Here *X* and *Y* are the two end-points of the wormhole link. As the signals received on one end of the wormhole link are repeated at the other end, any transmission generated by a node in the neighbourhood of *X* will also be heard by any node in the neighbourhood of *Y* and vice versa. The net effect is that all the nodes in region *A* assume that nodes in region *B* are their neighbours and vice versa. For example, traffic between nodes like *a* and *e* can now take a one-hop path via the wormhole instead of a multi-hop path.

## III. AFFECTS OF WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK

The wormhole will attract a large amount of traffic between various source and destination nodes in the network. Once traffic is routed through the wormhole, the attacker can selectively drop data packets or cause intermittent disconnections that will lead to denial-of-service. Cryptographic techniques (encryption/authentication) do not detect the wormhole attack as the transceivers simply relay the encrypted or authenticated packets.

Problems created by the wormhole attacker in WSN:

*Independent of MAC layer protocols*

A wormhole attack is considered dangerous as it is independent of MAC layer protocols and immune to cryptographic techniques. The attacker does not need to understand the MAC protocol or be able to decode encrypted packets to be able to replay them.

*Selectively dropped the packets*

Attackers can discard the packets rather than forwarding all the packets. This creates a permanent denial of service attack, where Base station can't receive any information from the target area.

*Modifying Data packets*

Attackers can modify the packets or deletes some information and forward to other nodes in the network.

*Generate unnecessary routing activities*

Attackers can generate unnecessary routing activities in the network.

## IV. WORMHOLE DETECTION AND REMOVAL TECHNIQUES

Various techniques have been developed used to defense against the wormhole attack in wireless sensor network. Some techniques used special hardware such as the directional antenna and the precise synchronized clock to defend the network against wormhole attacks and some are based on the location information

### *A. Location and Time Based Solutions*

Y. C. Hu et. al. 2003[3], defined the wormhole attacks. They proposed a mechanism, "packet leashes", for detecting and defending against the wormhole attacks. The geographical leash ensures that the recipient of the packet is within a certain distance from the sender. The temporal leash ensures that the packet has an upper bound on its lifetime, which restricts its maximum travel distance. This mechanism requires either location information or tight clock synchronization.

S. Capkun et. al. 2003 [4] gives an authenticated distance bounding technique called MAD is used. The approach works similar to packet leashes at a high level, but it does not require location information or clock synchronization. In the Echo protocol ultrasound is used to bound the distance for a secure location verification.

L. Hu, D. Evans, 2004[5] Explains the method that Uses Directional Antennas in which mobile nodes are equipped with directional antennas to defend against wormholes. In this approach to preventing wormhole attacks is for nodes to maintain accurate information about their neighbors (nodes within one hop communication distance). The goal of this method is to design a neighborhood discovery protocol that is not vulnerable to wormhole attacks. Their assumption is that if there is no wormhole attack and if one node sends packets in a given direction, then its neighbor will get that packet from the opposite direction. The neighboring nodes examine the directions of the received signals from each other with a shared witness. O When the directions of both pairs match, the neighboring relation is confirmed. This approach prevents wormhole attacks when the adversary has only two end points. Disadvantages of using directional antenna are each node is to be equipped with the special hardware called directional antenna. This method does not prevent multiple endpoint attacks. Directional errors are possible. Directional

antennas have been shown to improve efficiency and capacity of wireless networks.

*B. Statistics Based Solution*
*Using Beacon Nodes*
He Ronghui et. al. 2009[6], proposed a method in which Beacon nodes are used to find wormhole in network. Beacon nodes are known about its location. Each beacon node acts as a detector, each sensor node participates in hop counting, while the base station controls the start and end of the detecting process, and estimate the locations of wormhole ends based on alarm messages sent from beacon nodes. A hop counting technique is employed to make every beacon node know its hop distance to the other beacon nodes as well as the coordinates of them. When a straight line distance is larger than a hop distance by a threshold value, then there exists a wormhole attack. The wormhole has been detected by compare with threshold value. Disadvantages of this method is, to know location of each beacon nodes, they have to connect by GPS. The communication cost is relatively high.

*C. Using Local Neighbor Information*
Jin Guo et. al. 2011[7] presented a kind of wormhole attack defense strategy of WSN based on neighbor nodes verification. In the early period of network deployment, each normal node broadcasts HELLO message. After each node received HELO from neighbor nodes, it will establish neighbor node table. Each item record related information of this neighbor node, such as MAC and build routing table. It also record other routing information as Sequence Number, hop count and others. In the routing query phase, when each node send or forward control packets as RREQ, RREP, RREP ACK and RERR as well as DATA, it needs to add information into packet that can characterize its identity, such as MAC or node number node. After each node received control packets and data packets from normal nodes or malicious nodes, it firstly extracts characterization information carried in the packet to determine where these packets come from. At the same time, it compares the characterization information with record information in the neighbor nodes table to determine whether these packets come from its neighbor node. If so, conduct appropriate processing, otherwise discard these packets.

Sebastian Terence. J 2011[8] present a Secure Routing protocol against a Wormhole Attack for sensor networks (SeRWA) for discover secure route in sensor network, but it has a disadvantage of false positive. SeRWA protocol consists of four steps: One-hop neighbor discovery, Initial route discovery, Data dissemination and wormhole detection and secure route discovery against a wormhole attack [9]. Due to false positive the close neighbor nodes are treated as remote node. It makes, SeRWA cannot select close neighbors for routing. We use mobile agents to avoid false positive in route discovery. A mobile agent is a program, which is capable of migrating autonomously from node to node, and performs computation on behalf of the user. The mobile agent can process its task by autonomously migrating to an appropriate location, even if the mobile agent cannot get communications with its user as well as other agents.

## V. PROBLEM FORMATION ON THE BASIS OF SURVIVES TECHINQUES

Wormhole attack and its survived solutions are classified into location based, time based, statistics, and graph based solutions. But most of the existing techniques have some disadvantages which are described as follows.

*A. Hardware dependent*
Most of the techniques require some special hardware to detect wormhole attacks, and some of techniques cause high overhead in each sensor nodes. So we have to developed techniques that does not requires any special hardware or provide security at less cost by consuming less energy or power which are limited resources in WSN.

*B. Location information*
Techniques based on location information ensure that the recipient of the packet is within a certain distance from the sender and also ensures that the packet has an upper bound on its lifetime, which restricts its maximum travel distance.

*C. High overhead*
Some of the techniques cause high overhead on each sensor node because all nodes contain information about itself and its neighbors also.

*D. GPS based solution*
Some techniques based on GPS system for their location information, which is very costly in wireless sensor network.

*E. False Positive*
When a node moves from an old position to a new position, and performs a new round of neighbor discovery, a false positive occurs when the distance between the newly obtained value and the statistic from the training window is larger than Threshold. A false positive is some nodes are mistakenly detected to be connected by the wormhole since they are actually close nodes.

*F. Range-Based Localization Schemes*
Time of Arrival (TOA) technology is commonly used as a means of obtaining range information via signal propagation time. The most basic localization system that uses TOA techniques is GPS. GPS systems consists expensive and energy-consuming electronics to precisely synchronize with a satellite's clock. Due to hardware limitations and the inherent energy constraints of sensor

network devices, GPS and other Time of arrival technology present a costly solution for localization in wireless sensor networks. Range-based localization schemes, need transceivers, have more device constraints and have disadvantages in cost and energy consumes [10].

## VI. PROPOSED WORK

In this paper, propose wormhole detection procedure for WSN, based on concepts employed in a kind of range-free localization methods; this approach performs the wormhole detection after the conclusion of the location discovery protocol.
GPS is the most extended technology for localization. However, GPS is unsuitable for localization in WSN due to its high cost, high energy consumption and the impossibility of operating indoors. A much more flexible approach to location discovery is obtained if we assume that only a small number of network nodes are assumed to know their own locations, while the other nodes are only able to measure their relative distances to other neighbor nodes and use these data to position themselves. Once the position of node is localized, apply the wormhole detection procedure for finding out whether there is any wormhole attack in the network. This can be done as follows:
When a given node has completed the localization procedure and it has obtained a position within the local network deployment area. Then the idea is to use the anchor nodes to test the validity of the node location.

*Detection after localization*

1. The tested node broadcasts packets that
Contain its estimated position.
2. The anchor nodes (and other well-located nodes) collect the packets sent by the tested node and obtain position values for them.
3. The anchor nodes send their positions and the position they have measured for the packets transmitted by the tested node to a centralized decision node.
4. The decision node computes the distances between the locations of the anchor nodes and the position reported by the tested node.
5. For each anchor node, the decision node determines if the distance of the tested node to the anchor node is consistent; if another anchor node that is supposed to be farther to the tested node reports a lower distance or a nearer anchor node reports a higher distance, a "discrepancy" is annotated.
6. The decision node counts the number of discrepancies for all the anchor nodes and, if it is below a given threshold, the location provided by the node is labelled as "trustworthy"; otherwise, the localization processes of the tested node is considered failed and this fact is reported by the decision node to the rest of the nodes.

## VII. CONCLUSION

Wireless networks are more vulnerable to various types of attacks than wired networks, due to the broadcast behavior of the transmission medium. Wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. So Security in WSN becomes more important, because they are subject to various types of malicious attacks. Malicious nodes can join the network discretely and compromise network security from the inside as in the wormhole attack. This kind of attack does not need to decrypt any code in the network or infect any node in the network to achieve its harmful objective; therefore detecting wormhole attack is a way to improve network security beyond cryptographic protection techniques. In this paper, propose a technique that detects the wormhole attack using range free localization.

## VIII. ACKNOWLEDGEMENT

This paper covers the affects of wormhole attack in wireless sensor network and author has found a technique to detect the wormhole attack in wireless sensor network. This work would not have been possible without the support of her Guide and the author wishes to express her gratitude to her supervisor, Dr. Ajay Jangra who was abundantly helpful and offered invaluable assistance, support and guidance. I consider it as a great opportunity to do my work under his guidance and to learn from his research expertise.

## REFERENCES

[1] Prasannajit B, Venkatesh, Anupama S "An Approach towards Detection of Wormhole Attack in Sensor Networks" 2010 First International Conference on Integrated Intelligent Computing,2010.

[2] Ritesh Maheshwari, JieGao and Samir R Das "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information" IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2007 proceedings, 2007.

[3] Y. C. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), IEEE ,2003.

[4] S. Capkun, L. Buttyn, and J. P. Hubaux, "SECTOR: Secure tracking of node encounters in multi-hop wireless networks," 2003.

[5] L. Hu, D. Evans, "Using directional antennas to prevent wormhole attacks", in Proceedings of the IEEE

Symposium on Network and Distributed System Security (NDSS),2004.

[6] He Ronghui, Ma Guoqing, Wang Chunlei, and Fang Lan "Detecting and Locating Wormhole Attacks in Wireless Sensor Networks Using Beacon Nodes", World Academy of Science, Engineering and technology, 2009.

[7] Jin Guo, Zhi-yong Lei "A Kind of Wormhole Attack Defense Strategy of WSN Based on Neighbor Nodes Verification", IEEE 2011.

[8] Sebastian Terence.J "Secure Route Discovery against Wormhole Attacks in Sensor Networks using Mobile Agents", IEEE 2011.

[9] Rakesh Kumar, Dr.Mayank Dave, "Mobile Agent as an Approach to Improve QOS in Vehicular Ad hoc Network", IEEE 2010.

[10] LI Nian-qiang, LI Ping,"A Range-Free Localization Scheme in Wireless Sensor Networks", IEEE 2008.