ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

Using Cluster Based Approach Wormhole Attack Detection in Wireless Sensor Network: A Survey

Kehkasa Mirza [1], Vaidehi Shah [2]

P.G. Student, Department of Computer Engineering, C.G.P.I.T, Uka Tarsadia University, Bardoli, India[1]

Assistant Professor, Department of Computer Engineering, C.G.P.I.T, Uka Tarsadia University, Bardoli, India[2]

ABSTRACT: Wireless Sensor Network is one type of ad-hoc network; it has limited bandwidth, low energy with small battery. Use of this feature make sensor infeasible to used security solution. It has many applications like military battle field, habitat monitoring, target tracking, seismic monitoring, fire and flood detection. One of the most important attacks in wireless sensor networks is the wormhole attack, in this attack a malicious node receives packets and massage from one side location and tunnels them to another location in the network. To detect this types of attack certain wormhole detection techniques can be used like Cluster Based Approach.

KEYWORDS: Cluster Node, Wireless sensor network, Wormhole attack, Clustering.

I. INTRODUCTION

A wireless sensor network is a collection of sensor nodes with limited bandwidth, low energy with small battery and low power consumption.
In wireless sensor network sensor nodes are self-configured. This type of network is used to control and monitor the environment. Sensor nodes communicate with another node and transmit massage to each other. WSNs are used for various tasks such as surveillance, widespread environmental sampling, security, and health monitoring. In wireless sensor network some time when one node communicate to the other node at that time some attacker attack and change or replace the data or message. For this reason detection techniques are used and remove these problems.
WSN is vulnerable to attack. Different types of attack are wormhole attack, black hole attack, sinkhole attack etc. Wormhole attack cannot be controlled using cryptography, so it is very harmful .wormhole detection is very important. In this review paper cluster based approach for wormhole detection is majorly focused and describes other method also.

II. VARIOUS ATTACKS ON WIRELESS SENSOR NETWORKS

There are various attacks which are possible in the sensor network. In WSNs classify this attack in two types of attack. Active and Passive attacks are the most common categories.

1. **Active Attack[1]:**
   In this type of attack attacker monitors, listens to and modifies the data or massage in the communication channel are known as active attack.

2. **Passive Attack[1]:**
   In this type of attack attacker monitoring and listening of the communication channel are known as passive attack.

The various attacks on sensor node are as follows:
1) Black hole Attack:

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

In this type of attack, an attacker drops all the packets it has received and forwards the packet.

2) Selective Forwarding:
In this type of attack, an attacker forwards some packets while drop the others.

3) Sinkhole Attack:
Attack directly the data which circulated near the sink, at that point attacker catch the maximum data.

4) Sybil Attacks:
A malicious node present multiple identities to the network is called Sybil attack. This attack confused to routing protocols that it is present multiple locations at once.

5) Wormhole Attacks:
In these attacks attacker make fake tunnels and at the time of transmission they replaced data or massages and received another part of tunnel over a low latency link. Wormholes often convince distant nodes that they are neighbours of this node.

6) Hello Flood Attacks:
In this type of attack nodes broadcast hello messages to other nodes in same network and announce their presence to their neighbours. If the attacker also advertises a high quality route it can get every node to forward data to it.

7) Monitor and Eavesdropping:
In this type of attack attacker try to capture some data in the network by listening the network data is sent with no encryption, we can easily read it. I n this attack attacker cannot modify the data so it can difficult to detect.

8) Traffic Analysis:
In this type of attack when some data are transferred at that time sender send continuously data packet, so traffic occurred. And at that time attacker catch the data.

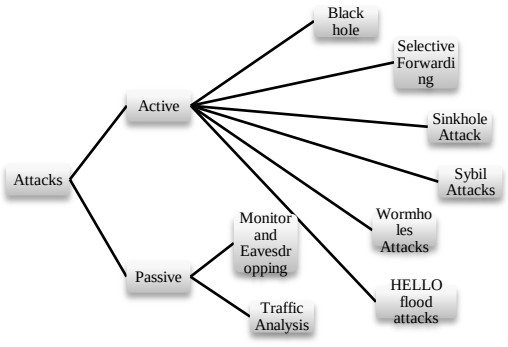

Figure 1.Various Types of Attacks [1]

III. WORMHOLE ATTACK

In all these attacks the wormhole is a very dangers attack because in this attack no crypto graphical breaks. Wormhole attack is a one type of Denial of service attack, one or more attackers are connected by high speed of channel link called wormhole link. Wormhole is a severe attack in which two attackers placed themselves in the network. The attackers monitor the network and record the wireless data.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

In wormhole attack malicious node can receive data packets at a one point and transfer them to another malicious node which is another part of the network, through out of band channel. Second malicious node is replaced this packet or data. This makes all the nodes that can hear the transmissions by the second malicious node believe that the node that sent the packets to the first malicious node is their single-hop neighbour and they are receiving the packets directly from it.

In this figure 2 shows the wormhole attack occurred. In this figure show that X and Y is node using this node packet received by X and replayed by Y.

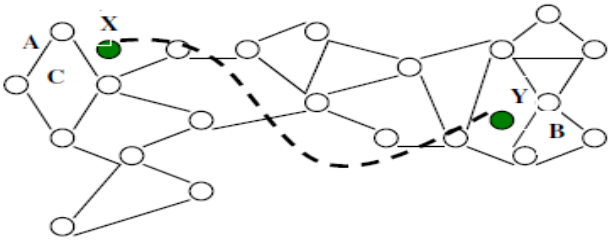

Figure 2.Wormhole Attack [3]

Normally it transmit several hops for a packet from a location near X to a location near Y, packets transmitted near X travelling through the wormhole will arrive at Y before packets travelling through multiple hops in the network. The attacker can make A and B believe that they are neighbours of each other and communication between A and B.
In wormhole attack attacker make the fake tunnel which has shortest path and at the time of transmission they replaced data or massages and received another part of tunnel over a low latency link.

IV. WORMHOLE ATTACK MODEL

There are three types of model of wormhole attack. It can classify in various ways.

- Open Wormhole Attack
- Half open Wormhole Attack
- Closed Wormhole Attack

In band and out of band are two other types of classification of wormhole. In this way the attacker using tunnel and transmit massage to existing wireless medium so that it is known as in band . This attack is very much harmful and is the most preferred choice for the attacker. In out of band uses the different wireless network in order to perform the attacks in network. All three type of wormhole attack show in figure3.

1. **Open wormhole attack[8]**
   In open wormhole attack, attacker node sends the RREQ packets, in the presence of malicious node in the same network other node supposes that malicious node is present on path and consider as they are their direct neighbors. It means the both nodes show their identity in the network.

2. **Half open wormhole attack [8]**
   The Half open Wormhole attack is same as a open wormhole attack, but only one node shows its identity and any other node hide itself from the network. In this type packet modification will modify one side only.

3. **Closed wormhole attack[8]**
   This is third types of wormhole where both the nodes are hidden from the node. They monitor the network and find the shortest path. Using some algorithms sender finds its path, and then hidden node reply and sender confused in this scenario.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

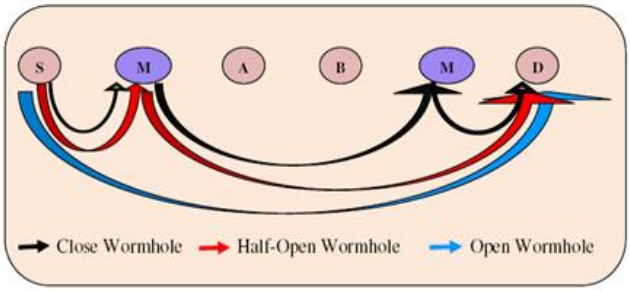

Figure3. Representation of Open, Half-Open and Closed Wormhole [3]

V. WORMHOLE ATTACK TAXONOMY

Wormhole attack can be achieved with the help of several techniques such as packet encapsulation, high transmission power and high quality communication links etc.

1. Wormhole Using Encapsulation[4]

In this type of scenario several nodes exist between two malicious nodes and the data packets are encapsulated between the malicious nodes. Using the malicious node encapsulated data packets are sent, so at the time of transmission hope count does not increase. For path selection routing protocols that use hop count.

2. Wormhole using Out-of-Band Channel [4]

In this scenario wormhole approach has only one malicious node present and it has high transmission capability in the network that attracts the packets to follow path passing from it. Malicious nodes are present in the routes established between sender and receiver increases in network.

3. Wormhole Using High Power Transmission Capability[4]

In this scenario one malicious node present and it has high power transmission capability to exist in the network. This node can communicate with other normal nodes in network from a long distance. When a malicious node receives a RREQ, it broadcasts the request at a high power level. Any nodes that hear the high power broadcast rebroadcasts the RREQ towards the destination.

4. Wormhole using Packet Relay[4]

In this scenario at least one or more malicious nodes are present. In this type of attack malicious node replays data packets between two nodes and this way fake neighbours are created.

5. Wormhole using Protocol Distortion[4]

In this mode of wormhole attack, single malicious node using by routing protocols tries to attract network traffic. This mode does not affect the network routing much and hence is harmless.

VI. WORMHOLE ATTACK DETECTION TECHNIQUES

1) Location and Time based approaches:[3]

In this approach two types of detection techniques is used, one is a space based approach, it is also called as Geographical Leashes each node knows its location and all nodes have loosely synchronized clocks which is to determine the neighbour relation. In this approach node knows its current position and transmission time before sending a packet, on receiving packet, receiving node calculates the distance information about sender and the time required by the packet to traverse the path. Using this distance information receiver check the received packet passed

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

through a wormhole or not [8]. In Temporal Leashes, every node maintains a tightly synchronized clock but does not depend on GPS information. One benefit of packet leashes is the low computation overhead [9]

2) Hardware based Approach:[3]

In this approach directional antenna is used. This type of approach based on ad hoc network with no wormhole link, suppose one node send packet in one direction neighbour will receive that packet from the other direction. Directional antenna is used because neighbours are in same direction, and relation of neighbours is conformed.

3) Statistical Analysis Approach:[3]

Wormhole discovery mechanism based on statistical analysis of multipath routing. Tunnel created by wormhole is attractive in terms of routing, and will be selected and requested with unnaturally high frequency as it only uses routing data already available to a node. This factor enables for easy integration of this method into intrusion detection systems only to routing protocols that are both on-demand and multipath [10].

4) Graph Based Approach:[5]

In this approach using graphical theory solved wormhole attack. Based protocol is using for limited location-aware guard nodes (LAGNs). All nodes known location and origination and can be acquired through GPS receivers. Using local broadcast key that is valid only immediate one hop neighbours. In this method define a massage with a local key, encrypted with the pair-wise key. It cannot be decrypted at another end in network. During the key establishment make hash massage using LAGNs protocols. A node can detect certain in messages from different LAGNs we can say that wormhole is present. If node should not be able to hear two LAGNs that are far from each other so wormhole is absent, and should not be able to hear the same message from one guard twice [10].

5) Cluster Based Approach[6]:

In this approach wormhole is a controlled by the attacker, between two locations in the network. The main purpose of attacker impresses the clustering protocol. Also, malicious node can interfere the communication between cluster heads and be able to attract traffic. Detection is performed based on clustering method to detect wormhole attacks. Using M-Leach protocol performed clustering. Time is divided into parts of equal length called round. Each round consists of four phases: setup phases, member's verification phase, cluster head routing phase and steady state phase. Fig. 4 shows the division of time in this protocol.

The entire network is divided into clusters. Each cluster has its own cluster head and a number of nodes called as member nodes. Member nodes send the information only to the cluster head. The cluster head is reply back the aggregated information to all its members and also send all the information of members node to base station. The cluster head is elected dynamically and maintains the routing information.

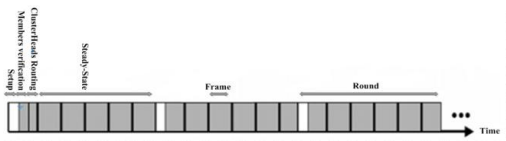

Figure4. The Division of Time [6]

Describe four phases in detail:

1) Setup Phases:

In this phase the nodes are organized in clusters. The cluster heads are determined with respect to the energy and mobility of nodes. Each cluster head selects a number due to the energy and its mobility. The threshold is based on number of times a node has been cluster head, amounts of residual energy in the nodes and the node mobility. Cluster head broadcast the (ADV) advertise massage to show that it is a cluster head. ADV message is a small message that contains the node ID.

The nearest CH has this property for each member node and it is selected as its cluster head node. If there are CH nodes with equal conditions, a node is randomly selected as CH.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

Each cluster member replay sends a join-request message to the intended CH using non-persistent CSMA protocol. This message also is a small message containing the node ID.
After receiving these messages, CHs set a TDMA schedule to coordinate data transfer in the cluster and the impossibility of collision event between nodes data in the cluster as the centre of local control and send this schedule for cluster members.
As a result, it is guaranteed that no collision occurs between the messages in the cluster and also allows turning off radio components of member nodes in all slots except on their own time.
But in this phases one problem is occurred, in the cluster malicious nodes are present and member node of the cluster cannot identify this node and communicate with them.

2) Member Verification Phases:
After the clustering and select the cluster head its member has been identified. Each node broadcast cluster head massage to its one-hop neighbour. Node must receive at least one massage with CH ID, also massage must be received before other massage from neighbour to the requested node.

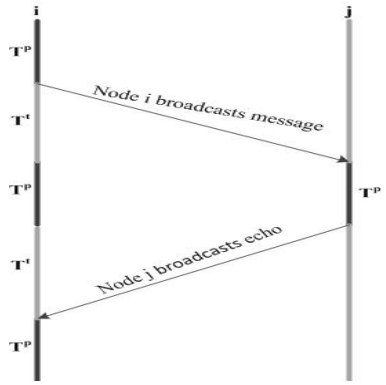

Figure5.The Overhead of the Time without Wormhole Attack [6]

Shown in Fig. 5, if node i and node j are true neighbors, the overhead of the time Tij from node i sends the cluster head packet to receive echo as formula1

$$Tij=T_i^P+T_{ij}^t+T_j^p+T_{ji}^t+T_i^p \text{ [6]} \qquad (1)$$

The notation Tp presents the time which spent processing the message and the notation Tt presents the time which spent transferring the message. In the case of wormhole attack there is the wormhole link between nodes i and j. As Fig. 6 shows, the overhead of the time Tij, is given by formula 2.

$$Tij=T_i^P+T_{im}^t+T_m^p+T_{mn}^t+T_n^p+T_{nj}^t+T_j^p+T_{jn}^t+T_n^p+T_{nm}^t+T_m^p+T_{mi}^t+T_i^p \text{ [6]} \qquad (2)$$

In this case, the requesting node sends a join-request message to another cluster head that has received cluster head response message from its members (and it has been received earlier than the other messages). Then, the node sends a message to the new cluster head to inform it of the existence of the wormhole nodes.

Then, the cluster head sends a message to the BS and informs it from wormhole in the area. In M-leach protocol, each cluster head is responsible for sending data to BS, but in the proposed protocol, in addition to inter cluster communication; cluster heads have intra communication with other cluster heads. In this part, the cluster head routing phase is done.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

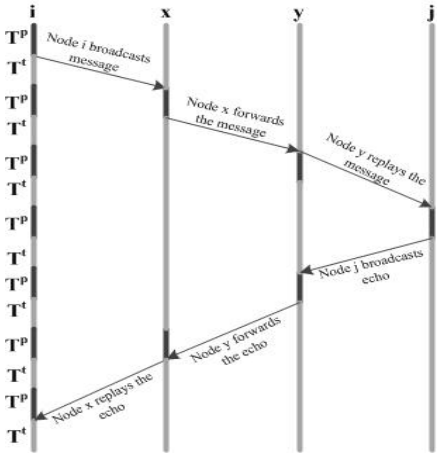

Figure6.The Overhead of the Time with Wormhole Attack [6]

3) Cluster Head Routing Phases:

Cluster heads use tree structures. After CHs have received messages from all nodes, then they fix the cluster boundaries and construct the spanning tree. After certain amount of time the BS will start the tree construction by broadcasting an init_tree message to the CHs. Each CH receiving this message will store the BS information in its neighbors' table after a short period, it will send a t_accept message to the BS which contains node residual energy and its location and it will be chosen as parent for its lower level. After certain amount of time the BS will start the tree construction by broadcasting an init_tree message to the CHs. Each CH receiving this message will store the BS information in its neighbors' table after a short period, it will send a t_accept message to the BS which contains node residual energy and its location and it will be chosen as parent for its lower level.

The parent node sends a short range broadcast message to the other cluster heads. CHs reply with the create_child message. The parent node accepts the CHs as a child if number of children is less than Cmax. Otherwise it forwards the request to one of its child. The network topology which is formed by this algorithm is shown as Fig. 10. Wrong cluster heads become parent for other cluster heads that are farther than others and generally, cluster heads routing tree will not form correctly to communicate together. To prevent this, a confirmation routing is performed by the BS in cluster head routing phase. Each cluster head may receive several parent messages from other cluster heads during the route formation. Each cluster head records nodes ID in a table that receives routing message from them. Each two nodes that are in the range of each other, should receive routing message from each other. Upon completion of this phase, each cluster head directly sends its table to the BS. The BS checks these tables.

4) Steady State Phases

Cluster head nodes collect data from their members and send it to the BS directly or through other cluster heads, after aggregation. If nodes move away from cluster head or cluster head moves away from its member nodes then other cluster head becomes suitable for member nodes and makes inefficient cluster formation to deal with this problem, M-LEACH provides handover mechanism for nodes to current cluster head and also send JOIN-REQ to new cluster head. One of the main advantages of this method is detection and localization of wormhole attacks before sending data. This allows reducing the destroyed, forged, or deleted data by malicious nodes. The use of efficient clustering increases the lifetime of the network and reduces energy consumption.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

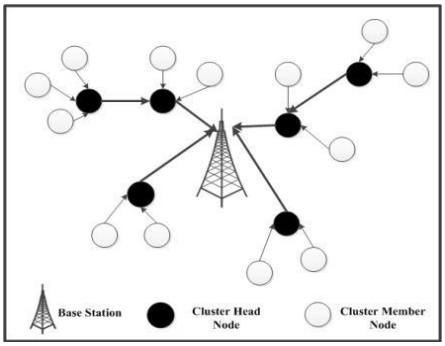

Figure9. Cluster Heads Routing Phase [6]

VII. COMPARATIVE ANALYSIS

Since wormhole attacks are easy to implement but hard to detect, wormhole prevention and detection has been an attractive research problem. Here we have surveyed various wormhole detection techniques and compare some of their features.

Mechanism	**Techniques**	**Advantages[5]**	**Disadvantages[5]**	**Localization Info.[7]**	**Checking Authentication[7]**	**Hop Count Analysis[7]**
Location and time based approach	Temporal Packet leashes,Geographical Packet leashes	Can find Pinpoint location of wormhole	Required special Hardware for location	Yes	RSA, TIK Protocol based on TESLA	N/A
Hardware based approach	Directional Antenna	It only works when the adversary has only two endpoints	Required additional special hardware	N/A	(MAD) protocol	N/A
Statistical based approach	Neighbour Number Test (NNT)	Proposal can only detect the presence of wormhole	Large amount of communication overhead	N/A	Yes	N/A
Cluster based approach[6]	Cluster member and cluster head	Heavy computation and it is independent of network data, Requires no additional hardware	Overhead of cluster formation is high	N/A	Routing table	Yes

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

Graph based approach	Secure neighbour discovery , connectivity graph	Don't required any Hardware Easy to implement, Central Authority	Can't detect Exposed Attacks	N/A	Isolating the malicious nodes globally	N/A

Table1: Comparative Analysis of Different Wormhole Detection Techniques

VIII. CONCLUSION

From the various study of wireless sensor network and its security goals. Discuss about different types of attack. In all attack Wormhole attack is very dangerous attack. This paper describe some detection techniques which are used for detect wormhole in wireless networks. I focus on cluster based approach to detect wormhole and also find malicious node and its location. Then comparison of wormhole detection techniques is provides based on advantages, disadvantages, location information, hop count analysis and check the authentication information.
More analysis from different papers on cluster based approach to detect wormhole can be derived in future. Future work is to explore different wormhole attack detection techniques.

REFERENCES

[1] Mr. Manish M Patel, Dr. Akshai Aggarwal, "Security Attacks in Wireless Sensor Networks: A Survey", IEEE 2010.
[2] David Martins and Hervé Guyennet "Wireless Sensor Network Attacks and Security Mechanisms : A Short Survey", IEEE 2013.
[3] Priya Maidamwar and Nekita Chavhan, "Wormhole Attack In Wireless Sensor Network",IJANS ,Vol. 2, No. 4, October 2012.
[4] Hinal Patel, Jayna Shah Assistant Professor, "Wormhole Attack Detection in Wireless Sensor Networks: A Survey", International Journal of Innovative Research and Devlopment,2014.
[5] Nishant Sharma1, Upinderpal Singh, "Various Approaches to Detect Wormhole Attack in Wireless Sensor Networks", IJCSMC, Vol. 3, Issue. 2, February 2014.
[6] Maliheh Shahryari, Hamid Reza Naji, "A cluster based approach for wormhole attack detection in wireless sensor networks" , JACST 2015.
[7] Yashpalsinh Gohil, Sumegha Sakhreliya, Sumitra Menaria, " A Review On:Detection and Prevention of wormhole Attack in MANET", ISSN, Volume 3, Issue 2, February 2013.
[8] Saurabh Ughade, R.K. Kapoor, Ankur Pandey, "An Overview on Wormhole Attack in Wireless Sensor Network: Challenges, Impacts, and Detection Approach", International Journal of Recent Development in Engineering and Technology,2014.
[9] Y. C. Hu, A. Perrig and D. B. Johnson Apr 2011., "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", IEEE Computer and Communications Societies(INFOCOM), 2003.
[10] Majid Meghdadi, Suat Ozdemir and Inan Guler , "A Survey of Wormhole based Attacks and their Countermeasures in Wireless Sensor Networks", IETE TECHNICAL REVIEW, VOL 28, ISSUE 2, Mar-2013