A Review on Detection and Prevention of Wormhole Attack in Wireless Sensor Network

Swati Bhagat
Department of Computer Science and Engineering
SDBCT, Indore

Trishna Panse
Department of Information Technology
SDBCT, Indore

ABSTRACT
A wireless sensor network (WSNs) is ubiquitous and gets a lot of interest from researchers towards the best applications. Wormhole nodes are false routes that are shorter than the original route in the network it creates problem in routing mechanism, which rely on the facts about distance between nodes. The attacker node captures the packets from the legitimate nodes. In our proposed research work we identify the wormhole node by their high power transmission in the network and also put off the network from the wormhole by achieving confidentiality in our modified AODV.

Keywords
Wireless Sensor Networks, Wormhole Attack, AODV.

1. INTRODUCTION
Sensor network consist of numerous detection stations called sensor nodes, each has small size, light weight and moveable. A WSN is a collection of extraordinary transducers with a communications infrastructure for monitoring and recording conditions at varied locations. Sensors observe such as temperature, humidity, pressure, wind detection, speed, vibrations etc. Major applications of sensor networks consist in the field of Automated and fashionable homes, Video inspection, Traffic control, Industrial computerization etc. Sensor nodes are often deployed into unfriendly environment, where sensors are unlocked and unprotected from physical attacks. Attack can occurs from any direction on any node in a sensor network. This issue causes the requirement of implementation of security policy into a WSN and therefore, security becomes the major cause. [7].

A WSN may consist of few hundreds to thousands of sensor nodes. The sensor node accessory includes a microcontroller, a radio receiver by the side of antenna, an energy source, an electronic circuit, and a battery. The proportion of the sensor nodes can also vary from the dimension of a shoe box to as minute as the dimension of a fragment of dust. As such, their prices also range from a few rupees to hundreds of dollars depending upon the objective of a sensor like energy utilization, bandwidth, memory and computational speed rate.

Vitality usage and asset utilization are significant issues, however security additionally turns into a key essential. In the WSNs, a few irregularities can happen because of their absence of handling and imparting ability, hindered capacity limit, reach, data transmission and vitality. These systems are traditionally sent in remote range and left unattended; they ought to be furnished with security components to forfend against assaults [8].One of the major issues with WSN is to uphold confidentiality. A WSN should not leak out any of its credential even when sensors are read by their neighbor nodes. They use encryption algorithms for privacy conservation. Finally, research concept concludes that there is a necessity to find out different vibrant featured confidentiality approach based on network traffic condition, security level of current event and intermediate node for different applications [7].

1.1 Routing Protocol
To keep up the course of every hub, switch keeps up the steering table. On the bases of table alteration we use receptive steering convention.

In AODV, the source hub shows the route invocation parcel (RREQ) in the system for setting up a course to the favored destination. It may get numerous courses to not at all like destinations from a solitary Route Request. It uses a destination grouping number (DSN) to focus an up to date way to the destination. A hub make change in its way data just if the DSN of the present parcel got is more dominant or equivalent than the last DSN put away at the hub with more minor bounce check [6].

DSN signifies the present course that is winnowed by the source. At the point when a center hub gets a route invocation, it either causes a route response in the event that it has a substantial course to the destination or advances it. The legitimacy of a course at the middle of the road hub is relentless by looking at the grouping number at the moderate hub with the destination arrangement number in the RREQ. Every single halfway hub having ideal courses to the destination or the destination hubs just, are endorsed to send Route response bundles to the source [6].

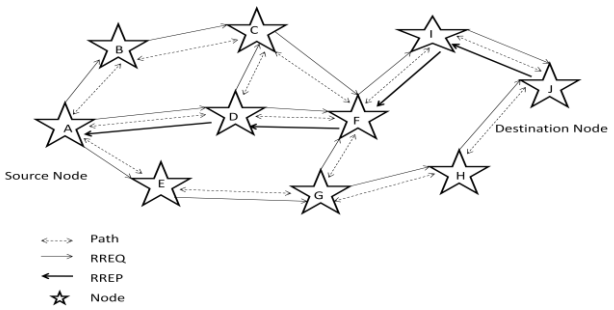

Fig. 1: Ad-hoc on-demand distance vector routing

1.2 Wormhole Attack
This is the attack in which one or more adversary node advertises a route that is two hopes away. Other route is longer, so don't use that. The adversaries are in control of all the traffic in the network.

A wormhole is low inertness connection between two parts of the system over which an attacker replays system messages. This connection may be set up either by a solitary hub sending message between two nearby yet generally non-neighboring hubs or by a dyad of hubs in distinctive piece of system corresponding with one another [8].

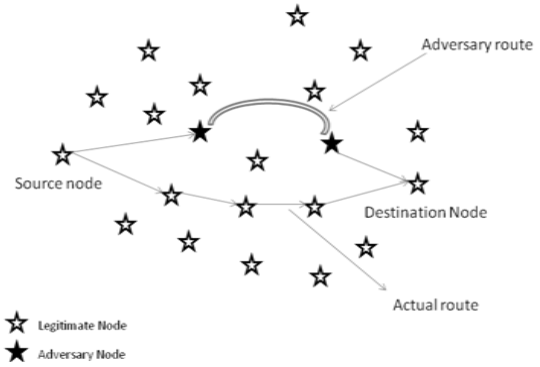

Fig 2: Wormhole Attack

1.3 Modes of Wormhole Attack

1.3.1. Wormhole attack with High Power Transmission

In this sort of wormhole assault, just one pernicious hub by assigns of high-power telecast capacity subsists in the system and this hub can compares with other standard hubs from a stretched space. At the point when a harmful hub gets a RREQ, it sends (shows) the solicitation at a raised force level. Any hub that gets the high-power scatters the RREQ about the destination. By along these lines, the noxious hub expands its opportunity to be in the courses apperceived between the source and the target even select of the involution of a supplemental pernicious hub. This assailment can be diminish if every sensor hub has the capacity exactly measure the got signal energy [9][5].

Fig 3: High Power Transmission

1.3.2. Wormhole attack using Encapsulation

In embodiment based wormhole assaults, various hubs get by in the midst of two malignant hubs and the information parcels are exemplified among the malevolent hubs. Because of typified information bundles are sent alongside the vindictive hubs, the clear jump number need not increase amid the traversal. In this manner, steering conventions which utilize jump mean path choice are essentially powerless against embodiment based wormhole assaults [9][5].

1.3.3 Wormhole attack using out-of- Band Channel

In this mode, the wormhole assailment is propelled by having a top notch, single-jump, out-of-band connection (called passage) between the evil hubs. This passage can be accomplished, for occurrence, by using a straight wired connection. This type of assailment is harder to start on than the bundle exemplification technique since it demands specific equipment potential [2] [1].

1.3.4. Wormhole attack using Packet Relay

Bundle hand-off based wormhole assaults should be possible by one or more foe hubs. In this sort of assailment, a harmful hub transfers information parcels of two inaccessible sensor hubs to persuade them that they are neighbors.

1.3.5. Wormhole attack using Protocol Deviation

In this type of wormhole strikes, a solitary dangerous hub attempts to draw system activity by twisting the steering convention. Directing conventions that rely on upon the 'briefest postponement' rather than the 'littlest bounce check' is at the peril of wormhole assaults by method for convention clasp.

2. LITERATURE REVIEW

U.K. Chaurasia et al [1] proposed a wormhole discovery method which is in view of adjustment in the AODV convention by including another recorded i.e. Timestamp. By this change deferral between two hubs can be measured. It likewise uses number of jump check technique for including the bounces between the source and destination hub. In this approach all the recognition done on the method of In-band channel and out-of-band channel. This system distinguishes the honest to goodness way and wormhole way in the system.

Z. A. Khan et al [2] proposed another discovery system of wormhole assault. In this methodology they utilize DSDV convention for course finding. They additionally alter the including so as directing table new field, for example, way and bounce in the DSDV table for the finding of wormhole way in the system. It chips away at exemplification, In-band channel and out-of-band channel methods of wormhole assault. This system separates the wormhole hubs from the typical ones.

M.G. Otero et al [3] induced wormhole detection in wireless sensor network by using the range-free localization. In this approach geographical routing protocol is used to detect route in the network. It works only on the out-of band channel.

S. Gupta et al [4] induced wormhole assault recognition convention by using hound packet. In it AODV convention is accustomed to distinguishing courses of the system. Dog bundle is utilized to distinguish the wormhole hub in the system. It deals with embodiment, In-band channel and out-of-band channel methods of wormhole assault.

M. Jain et al [5] proposed a full picture of wormhole assault in impromptu systems by presenting complex wormhole assault. In this discovery of wormhole and examine wormhole from assailant perspective is finished. In this AODV convention is utilized for directing. It chips away at exemplification and out-of-band channel methods of wormhole assault.

S. Choi et al [6] proposed a wormhole attack prevention algorithm in MANET. In this approach they used the DSR routing algorithm for finding rout. In this wormhole detection can be done by using geographical leash and temporal leash. It works on out-of band channel modes of wormhole attack.

L. Buttyan et al [7] introduce factual wormhole assault discovery routines in sensor systems. They favored wormhole method of theory and probabilistic testing. They utilize separation bouncing steering convention. They propose two techniques for identifying malignant hubs like neighbor number test and all separation tests.

Jaidip Sen et al [8] proposed a perception on the WSNs security. They have investigated all requirements, Security imperatives in WSNs, security susceptibilities in WSNs and security systems for WSNs. They also demonstrate in which territory explore more requires.

Table 1. Comparative Studies

S. No.	Method Used	Task	Wormhole Mode	Routing Protocol Used	Authenticity & Confidentiality
1	MAODV(Modified AODV)Protocol	Wormhole detection	In-band / Out-of-band channel	AODV	Not Present
2	Modified routing table(path included in table)	Wormhole detection	Encapsulation & In-band /Out-of-band channel	DSDV	Not Present
3	Range free localization	Wormhole detection	Out-of-band channel	Geographical routing Protocol	Not Present
4	WHOP(Wormhole Hound Packet)	Wormhole detection	Encapsulation & In-band /Out- of-band channel	AODV	Not Present
5	WAP(Wormhole Attack Prevention)	Wormhole detection & Prevention	Out-of-band channel	DSR	Not Present
6	1)Neighbor Number test 2)All Distance test	Statistical Wormhole detection	Hypothesis & Probabilistic testing	Distance Bounding Protocol	Not Present
7	Complex wormhole attack	Detection of wormhole & analyze wormhole from attacker Point of view	Encapsulation & Out-of-band channel	AODV	Not Present
8	1)Hop Count based detection 2)Anomaly based detection 3)Neighbor List based detection	Wormhole detection & Removal	Encapsulation & Out-of-band channel	AODV	Not Present

3. PROPOSED WORK

In our proposed work we are going to add to a protected AODV to sense wormhole assaults in remote sensor arrange and infer a system to counteract it. In this we propose another parameter, the powerful transmission of hub in AODV directing table. Utilizing this methodology even a solitary wormhole assault can be identified in the system. As from the relative study we can see that Wormhole assaults in WSNs are recognized by the modes like epitome, In-band channel and out-band divert mode in which wormholes structure burrow i.e. more than one wormhole can be recognized in this mode.

In high power transmission mode we can measure the transmission power of each node in the network, by using the modified AODV protocol. To finding the transmission power of each node we add the new attribute that measure the number of transmission of node in the AODV protocol. In this propose work we also provide the authenticity and confidentiality because legitimate node of the network can also perform the high power transmission. To differentiate the legitimate and wormhole node we provide the authenticity and the transmission should be secure by achieving the confidentiality.

Our Approach. The simulation of the proposed work will carried out in two stages. The simulation of stages will be based on the number of nodes and the position of the initial node and target node. Stage-1 & Stage-2 have 10 nodes and 20 nodes respectively. Both stages will be used to test performance of proposed protocol and wormhole attack in 4 steps.

- Performance analysis of existing AODV protocol.
- Performance analysis of AODV routing protocol with wormhole attack.
- Detection of Wormhole attacks.
- Performance analysis of AODV with proposed preventive technique.

4. CONCLUSION

In our approach detection as well as prevention of wormhole attack takes place by using the high power transmission mode. If a single wormhole is present in the network that can also be detected and prevented by this approach. In this research paper we analyze the traditional AODV routing protocol with wormhole attack and proposed a solution against wormhole detection problem using modified AODV**.** In modified AODV transmission power of each node measure by new field. For the prevention or security point of view we will archive confidentiality and authenticity to the legitimate node of the network.

5. REFERENCES

[1] U.K. Chaurasia and versha singh.. MAODV: Modified wormhole detection AODV protocol, In the six international conference on contemporary computing, IEEE 2013.

[2] Z. A. Khan and M. H. Islam. Wormhole Attack: A new detection technique, In the International Conference on Emerging Technologies (ICET), IEEE 2012.

[3] M.G. Otero and A.P. Hernandez. Detection of Wormhole Attack in wireless Sensor Network Using Range- Free Localization, In the 17th International Workshop on

Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), IEEE 2012

[4] S. Gupta, S. Kar and S. Dharmraja. WHOP: Wormhole Attack Detection Protocol using Hound Packet, In the International Conference on Innovations in Information Technology (IIT), IEEE 2011.

[5] M. Jain and H. kandwal. A survey on complex Wormhole Attack in wireless Ad Hoc Networks, In the International Conference on Advances in computing, control and telecommunication technologies, IEEE 2009.

[6] S. Choi, D.Y. Kim, D.H .Lee and J.I. Jung. WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks, In the International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC '08. IEEE.

[7] L. Buttyan,L. Dora and I. Vajda. Statistical wormhole detection in sensor network, Springer-Verlag Berlin Heidelberg 2005,pp. 128-141.

[8] J. Sen. A survey on wireless sensor network security, In the international journal of communication network and information security, IJCNIS 2009.

[9] M. Azer, S.E. Kassas, M.E. Soudani. A Full image of the wormhole attack International Journal of Computer Science and Information Security, Vol. 1, No. 1, (IJCSIS) May 2009