International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 2, Issue 4, April 2014)

An Overview on Wormhole Attack in Wireless Sensor Network: Challenges, Impacts, and Detection Approach

Saurabh Ughade[1], R.K. Kapoor[2], Ankur Pandey[3]
[1,3]*P.G. Scholar, NITTTR Bhopal*
[2]*Associate Professor, NITTTR Bhopal*

***Abstract*— The wireless sensor network is an emerging technology in the field of communication. This technology has many advantages but the security issues have been not given much consideration till now. Due to this neglecting, few loopholes in the security have started to occur such as wormhole attack, blackhole attack, etc. In this paper the various aspects have been covered regarding security provisioning in wireless sensor networks. Also some light has been thrown on the various types of attacks and its classification. The special attention has been paid to wormhole attack with the support of some already published works.**

***Keywords*— Attacks, Authentication, Blackhole, Tunnelling, Wormhole, Wireless Sensor Network;**

I. INTRODUCTION

The wireless sensor network is an approach to perform the communication using sensor nodes. These sensor nodes are self-configured. This type of network is used to control and monitor the environment. A wireless sensor network is a network of cheap and simple processing devices (sensor nodes) that are equipped with environmental sensors for sensing temperature, humidity, etc. The wormhole attack is dangerous against the security in WSNs in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of (and thus a neighbor of) that node. It is one of the most powerful attack that are faced by many ad hoc network routing protocols. Since, the wormhole attack does not require exploiting the feature of nodes in the network and it can interfere while executing the routing process.

Attacker uses these attacks to gain unauthorized access to compromise systems or perform denial-of-service (DoS) attacks.

In wormhole, the attacker at one end records the incoming traffic and tunnels packets to another end. If routing control messages like RREQ are tunnelled, this will result in distorted routing tables in the network. If there exist fast transmission path between the two ends of the wormhole that may tunnel the data at higher speed than the normal mode of wireless multi-hop communication. Thus, they will attract more traffic from their neighbours. This will results in rushing attack. In Rushing attack, due to the presence of fast transmission path all the packet will start following that path and this will increase the Average Attack Success Rate. Wormhole attack can also act as the first stage attackers where they can lead to the denial-of-service attacks. In the second stage, this may compromise the security of the global network as that breaks confidentiality and integrity. The wormhole attack is very harmful to the security of network. Due to the placement of the wormhole in the network there will be significant breakdown in communication across a wireless network. A successful wormhole attack may be the reason of disruption and breakdown of a network. Proper balance between these two is necessary to prevent much consumption of resources. The fig. 1 shows the transferring of data within wireless sensor network, which is towards destination node from source node i.e. from sensing node to sink node.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 2, Issue 4, April 2014)

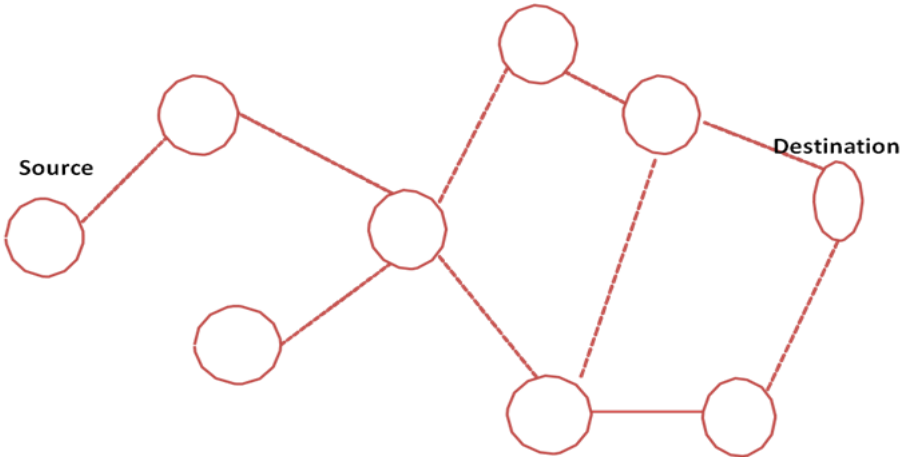

Fig. 1. Connectivity among Sensor Nodes

A wireless infrastructure less network having static or dynamic topology is called the sensor network. The basic entity used here is called the sensor. This type of network meets Combine different types of nodes and gateways. The sensor network can temporal establish instantly. The fig 1 shown is an example of the sensor network. In this scenario there is a source and a destination node available for communication.

A. Applications of WSN

The WSN is very popular because of its properties. It has lots of applications. Some of them are listed below.

- Collaborative Work
- Disaster Management
- Military and intelligence
- Preserving Historical places
- Personal Area Network (PAN)
- Taxi or Cab Network
- Conference or Meeting room

B. Vulnerabilities of WSNs

There exists some vulnerability in wireless sensor technology. Few of them are discussed below.

1) Wireless Connection

The wireless links are very helpful to connect the user with the network. The flexibility of this feature is helps the attacker to join the network.

2) Dynamic Topology

This is a biggest advantage of WSN that nodes can leave and join the network freely. But this approach increase the complexity.

3) Cooperativeness

Most of the routing approaches believe that the nodes which are moving in the network are not the malicious node. Even these nodes are cooperative.

4) Bandwidth

Here the bandwidth is limited due to large number of other activities as compare to wired network.

II. Attacks On Wireless Sensor Network

There are various attacks which are possible in the sensor network. But there are two major classifications in this way. Active and Passive attacks are the most common categories. In active attack the attacker or the malicious node takes the part actively in the network. Here the attacker will modify or alter the data packet and send this packer into the network. In spite of altering the data packet attacker can also inject and drop the data packet so that, such type of attacks becomes very harmful for the end users. Fig. 2 shows the classification of attacks that are common to wireless sensor network. Fig. 2 shows the classification of attacks in wireless sensor network.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 2, Issue 4, April 2014)

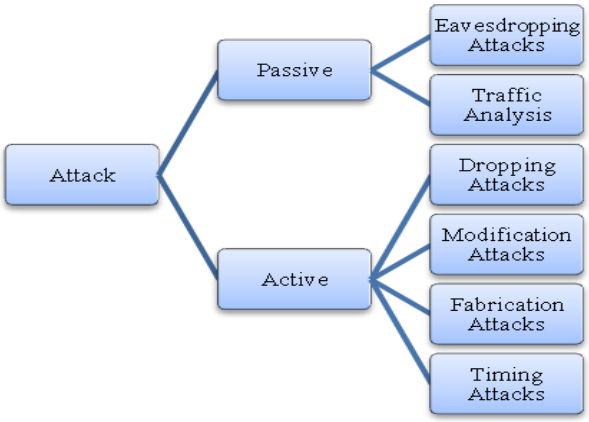

Fig. 2. Classification of Attacks

On the other hand the passive attack can happen without tempering the data packet. In this type of attack the attacker only analyse the data. The main goal of this type of attack is to break the confidentiality. Here the attacker tries to know the activities of the network. It focuses on the pattern to send in the network on the basis of which the attacker will take illegal action. Detection of passive attacks is very difficult since the operation of the network itself does not get affected. The Fig. 2 shows the basic classification of the attacking approaches. It shows that active and passive attack are the first criteria. It is possible to classify this by some other criteria.

A. Types of Attacks on Protocol Stack

The characteristics of WSNs make them susceptible to many new attacks. These attacks can occur in different layers of the network protocol stack. Layer wise attacks are represented in Table-1.

Table I: Layer wise Attacks on WSN

Layer	Attacks
Application Layer	Viruses and Worms
Transport Layer	TCP,UDP
Network Layer	Blackhole, Wormhole
Data Link Layer	Traffic Monitoring,
Physical Layer	Eavesdropping

B. Security Goals of WSN

There are four major security goals of WSN. The Fig. 3 shows the primary security goals in wireless sensor network.

Fig. 3. Security Goals of Wireless Sensor Network

1. Availability

The service should be in the access of user at any time.

2. Authentication

It provides the surety that the sender is an authorized person.

3. Integrity

During Message transmission the message should not be changed or modified.

4. Non-Repudiation

Message should not need to resend it to the network.

C. Attacks on Network Layer

A process in the network for trying to damage or defeat the things using illegal activity in the wireless environment called attack. The person or an object that will do this activity is called the attacker. There are many types of attacks possible in network layer like –

- Blackhole Attack
- Rushing Attack
- Wormhole Attack
- Sinkhole Attack
- Link Withholding & Link Spoofing Attacks
- Replay Attacks
- Resource Consumption Attack
- Sybil Attack

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 2, Issue 4, April 2014)

In all these attacks the wormhole is a common and dangers attack. Wormhole attack is a severe attack in which two attackers placed themselves strategically in the network. The attackers then keep on monitoring the network and record the wireless data.

D. Wormhole Attack

Wormhole is a type of attack in which two attacker nodes creates a link call the wormhole link by which both the nodes can communicate. These nodes give an illusion that the selected path is a shortest path to get the destination. The Fig. 4 shows the general working scenario of wormhole attack on wireless sensor network.

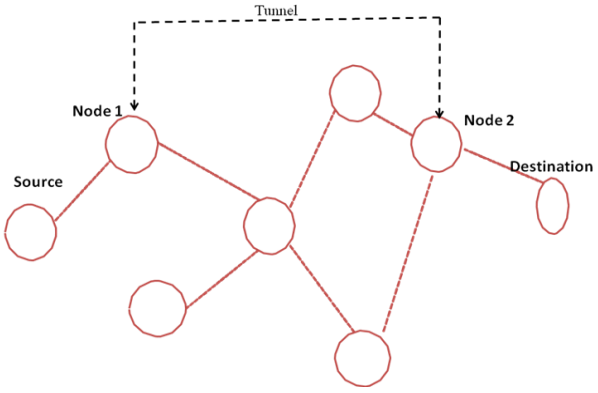

Fig. 4. Wormhole Attack

The wormhole attack can classify in various ways. Here some of classifications are given below

- In bound wormhole attack
- Out of bound wormhole attack
- 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 builds an overlay tunnel over the existing wireless medium so that it is known as the in band wormhole attack. This attack is potentially very much harmful and is the most preferred choice for the attacker. On other hand the out of band uses the different wireless network in order to perform the attack in the network. In open wormhole attack, attacker node keep an eye on the RREQ packets of the network, in the presence of malicious node in the network other node on the network suppose that malicious node are present on path and they are their direct neighbours. It means the both nodes show their identity in the network. The Fig. 5 shows the open wormhole attack of wireless sensor network.

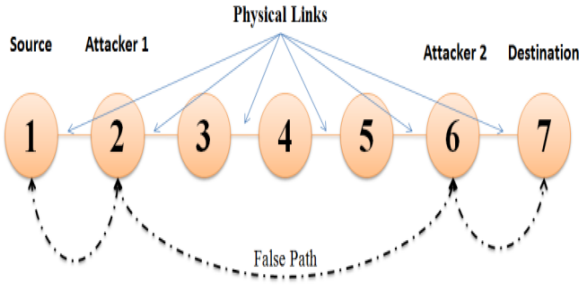

Fig. 5. Open Wormhole Attack

The Half open Wormhole attack is just like the open wormhole but here only one node shows its identity another one hide itself from the network. So the packet modification will do on one side. The Fig. 6 shows the Half Open wormhole attack of wireless sensor network.

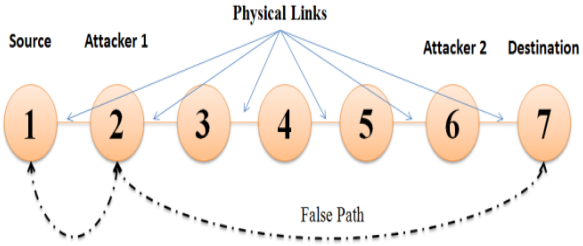

Fig. 6. Half Open Wormhole Attack

This is third types of wormhole where the attacker node doesn't temper the data packet. The both node are hidden from the node. They listen to the network activity and always show the shortest path. When sender finds its path using some algorithm, then hidden node reply and sender trap in this scenario. The Fig. 7 shows the closed wormhole attack on wireless sensor network.

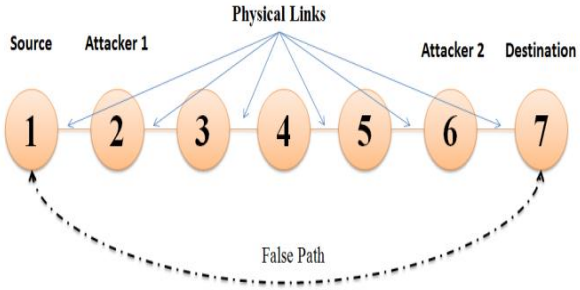

Fig. 7. Closed Wormhole Attack

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 2, Issue 4, April 2014)

III. RELATED WORK

The author of paper [8] proposed solution for digital investigation of wormhole attacks in Wireless sensor Network. The author gives the name observer to those nodes which are the set of investigator nodes. These nodes are responsible for monitoring the network. Observers gather the information of datagram of the network. They generate and securely forward evidences containing information regarding the monitored datagram, the routing paths they followed, and the identity of the nodes whose behaviour is suspicious. The simulation results give the batter results regarding investigation.

In [9] authors presented state-of-the-art research for in order to address the serious problem of wormhole in wireless sensor networks and discuss the relative strengths and shortcomings of the proposed solutions. The author has concluded by highlighting how such a system can be used for defending against wormhole attackers.

Nouri, et al. [10] have introduced first the concept of wormhole attack and five kinds of this attack and clusters in this work. They explained the two IDS approaches for sensor network. These approaches used the efforts of nodes to detect the malicious node. The first technique is designed for detection of malicious nodes in a neighbourhood of nodes in which each pair of nodes in the neighbourhood is within radio range of each other. The other technique is designed for detection of malicious nodes in neighbourhood of nodes, in which each pair of nodes may not be in radio range of each other but where there is a node among them which has all other nodes in its one-hop vicinity. Message passing is used between the nodes in both the techniques. The author has completed these approaches to detect the wormhole attack and isolating them from routing process.

In [11] the author has suggested that the traditional security mechanisms are not feasible for WSNs as they are usually heavy and nodes are limited. One of the most harmful attacks to detect and defend in wireless sensor network is wormhole attack in which data will be forwarded from one part of the network to the other part trough the wormhole tunnel. The author has focused on wormhole attack and proposed distributed network discovery approach to mitigate its effect. The simulation shows that the can mitigated almost 100% of wormhole attack overload in the environment where 54% of nodes are affected with the wormhole.

In [12] the author is give the opinion that still there are many unsolved problems in ad hoc networks. The wormhole attack is one of them. Among all sorts of attack the most threatening and dangerous attacks is wormhole on wireless networks. During this attack, the malicious node captures packets from one location and tunnels them to another distant malicious node in the network, which replays them locally. In this paper, the authors have proposed a scheme for the prevention of wormhole attack. The scheme relies on the concept that generally the wormhole node participates in the routing in an iterative way as it attract most of the traffic. Therefore, each node should be allocated a cost depending on its participation in routing. Besides, preventing the network from wormhole attack, this scheme provides load balancing among nodes to avoid exhaustion of nodes that are always cooperative in routing.

In another paper [13] author explained that the Wormhole is a kind of attack in Wireless Sensor Network (WSN) that needs not to crack encryption key, which has severe harm on the network. Focusing at characteristics of Wormhole attack, the paper proposed a kind of wormhole attack defence strategy of WSN, based on neighbour nodes verification technique. Under this strategy, when each normal node receives control packet, it will monitor these packets to determine whether it comes from its normal neighbour nodes to avoid Wormhole attack effectively. The simulation has done on OMNeT++ shows that the AODV added neighbour nodes verification successfully implements effective defence.

In a study [14], Sejun Song et al. have stated that wormhole attack is a challenging attack in these days. The wormhole has various security issues in mobile wireless sensor networks. The author has proposed the Statistical Wormhole Apprehension by the Neighbours' nodes, called the new approach for getting wormhole in sensor network. As SWAN utilizes the localized statistical neighbourhood information collected by mobile nodes, it intercepts wormholes not only without requiring any special hardware device but also without causing significant communication and coordination overhead. The authors have performed studies on false positive and detection rates via both analyses and simulations. The simulation results show that SWAN can detect wormhole attacks with high probabilities and very low false positive rates.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 2, Issue 4, April 2014)

IV. CONCLUSION

In current scenario, implementing security techniques on wireless sensor network is of ample importance. This paper will help its readers in understanding of the attacks that WSN can be subjected to. The wormhole attack is a major setback of wireless sensor technology. Hence, there is an utmost significance of overcoming this problem. Few techniques have been mentioned which have been proved to be efficient against wormhole attacks. A detailed survey of the previously done study has been carried out in this paper.

REFERENCES

[1] Zunnun Narmawala, Sanjay Srivastava, "Survey of Applications of Network Coding in Wired and Wireless Networks" in Proceedings of the 14th National Conference on Communications, pp. 153-157, February 2008.

[2] Sheikh, R. , Singh Chande, M. and Mishra, D.K., "Security issues in WSN: A review", IEEE 2010, pp 1-4.

[3] Kannhavong, B., Nakayama, H., Nemoto, Y. and Kato, N., "A survey of routing attacks in mobile ad hoc networks" IEEE 2007, pp 85-91.

[4] Verma, M.K. And Joshi, S. ; Doohan, N.V. "A survey on: An analysis of secure routing of volatile nodes in WSN", IEEE 2012, pp 1-3.

[5] P. Papadimitratos and Z. J. Haas, "Secure Routing For Mobile Ad Hoc Networks" in Proc. of CNDS, 2002.

[6] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A Secure Routing Protocol For Ad Hoc Networks" in Proc. of IEEE ICNP, 2002.

[7] C. E. Perkins, and E. M. Royer, "Ad-hoc on-demand distance vector routing," IEEE 1999, pp 25-26.

[8] Bayrem Triki, Slim Rekhis and Noureddine Boudriga, "Digital Investigation of Wormhole Attacks in Wireless Sensor Networks", IEEE 2010, pp 179-186.

[9] Thanassis Giannetsos, Tassos Dimitriou and Neeli R. Prasad, "State of the Art on Defenses against Wormhole Attacks in Wireless Sensor Networks", IEEE 2009, pp 313-318.

[10] Mahdi Nouri, Somayeh Abazari Aghdam and Sajjad Abazari Aghdam, "Collaborative Techniques for Detecting Wormhole Attack in WSNs", IEEE 2011, pp 1-6.

[11] Ali Modirkhazeni, Saeedeh Aghamahmoodi, Arsalan Modirkhazeni and Naghmeh Niknejad, "Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks", IEEE 2011, pp 122-128.

[12] Mariannne. A. Azer, "Wormhole Attacks Mitigation in Ad Hoc Networks", IEEE 2011, pp 561-568.

[13] Jin Guo, Zhi-yong Lei, "A Kind of Wormhole Attack Defense Strategy of WSN Based on Neighbor Nodes Verification", IEEE 2011, pp 564-568.

[14] Sejun Song Haijie Wu and Baek-Young Choi, "Statistical wormhole detection for mobile sensor networks", IEEE 2012, pp. 322 – 327.