© 2018 IJSRST | Volume 4 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

# Wormhole Attack Detection in Wireless Senor Networks

**Harkesh Sehrawat, Yudhvir Singh**
Department of CSE, UIET, MDU, Rohtak, Haryana, India

## ABSTRACT

wireless sensor network is one of the recent trends in the field of networking. They have the capacity to work where it otherwise impossible for human beings. Wireless sensor network has extended the limits of human being with its usage in varied areas like military surveillance, medical etc. These networks consist of small nodes which can be placed anywhere in any type of environment. However these networks are vulnerable to certain attacks like black hole, wormhole and selective forwarding. Many authors have tried to tackle this attack by proposing various kinds of methods. In this paper wormhole attack, its impact on wireless sensor network is analyzed. A comprehensive study of various approach and their impact on the network is presented here.

**Keywords:** WSN, Wormhole Attack, AODV

## I. INTRODUCTION

In Wireless Sensor Networks [1](WSNs), sensor nodes are used to sense the network by detecting events in the surrounding environment. It has two components i.e. aggregation points and base stations. Aggregation points collect information from nearby sensors, integrate them and then forward it to base stations to process the gathered data. Base station is also termed as gateway or access point. Various functions of WSNs are broadcast and multicast, routing, forwarding and route maintenance. The sensor's components are: sensor unit, processing unit, storage/memory unit, power supply unit and wireless radio transceiver; these units are communicating to each other. WSNs are vulnerable to many types of attacks and due to unsafe and unprotected nature of communication channel, un-trusted and broadcast transmission media, deployment in hostile environments, automated nature and limited resources, most of security techniques of traditional networks are impossible in WSNs; therefore, security is an important and complex requirement for these networks.

WSNs has inherent limitations, a sensor network is vulnerable to all external or internal attacks. To manage these kinds of situations, the infrastructure and protocols of the network must be prepared appropriately. The nodes in sensor networks have always constraints such memory and energy, unreliable communication, collisions of packets, latency, physical limitations like unattended nodes after deployment and remotely managed networks

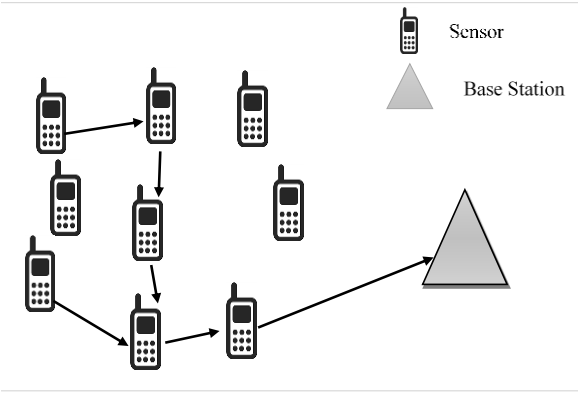


**Figure 1**. Architecture of WSN

**Characteristics of WSN:**[2]

Various characteristics are as following.

- Small in size and low power consumption
- Concurrency-intensive operation
- Diversity in design and usage
- Security issues and constraints

- Sensor nodes are limited in power, computational capacities, and memory.

**Applications of WSN's** [3]

Wireless sensor networks have recently emerged as a technology that has resulted in a variety of applications. Some applications are:

- Health care monitoring
- Monitoring environments
- Medical diagnostics
- Disaster management
- Military surveillance and tracking
- Industrial automation
- Civil structural monitoring
- Traffic control
- Rapid Emergency Response

**Threat Models in WSNs**[4]

As discussed in Security threat in a WSN can be divided into various categories according to their behavior or operation etc. These are:

- External threats versus internal threats
- Mote-class attacker versus laptop-class attacker:
- Passive attacker versus active attacker

**Attacks in Wireless Sensor network**[5]

- **Hello flood attacks:**[6] In this attack the attacker impersonates that he is the neighbor in the sensor network by sending high transmission power signals and replay hello packets. It disrupt routing protocols and instantiated other types of attack.
- **Wormhole attack:**[7]Intruders here are tactically placed at ends of the network. They receive information and sends back information in different nodes via a tunnel. Wormhole attack is difficult to prevent and detect.
- **Sybil attack:** [8]Intruder can make use of identities of others nodes in order to capture necessary information. Topology maintenance, fault tolerance are attacked by Sybil attack.
- **Sinkhole attack:** [9]It is an insider attack. The goal of attacker is to attract whole network traffic so that the BS cannot acquire complete information of the data packet. It then purposely changes data content or completely destroys it.
- **Selective forwarding:**[10] In this attack, compromised nodes may refuse to pass on some messages and straightforwardly drop them.
- **Black hole attack:** [11] Its only goal is to pass nothing and then making a black hole in the network.

## II. WORMHOLE ATTACK

In a wormhole attack, an attacker archives data packets at one node in the network, forwards these through tunnels to another area, and retransmits them into the network. A wormhole attack can undoubtedly be propelled by the attacker without knowing about the network or trading off any authentic nodes or cryptographic components. Fig 2 and 3 shows data transmission in a normal wireless sensor network and a network with a wormhole attack respectively. Fig 2 shows how the node E is tunneling the packets to node D bypassing the intermediate nodes that will be used in the absence of the wormhole attack.

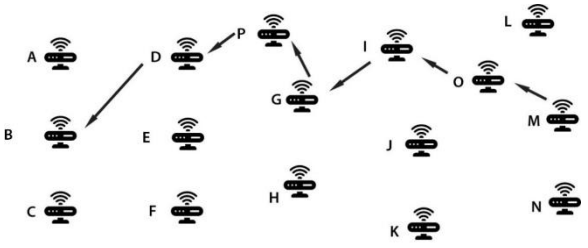


**Figure 2.** A normal WSN scenario

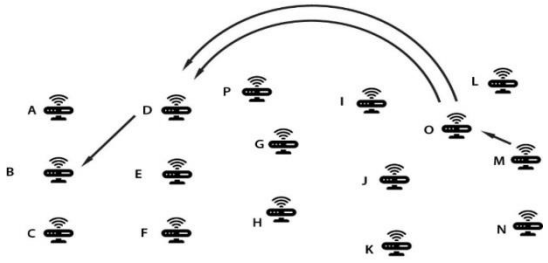


**Figure 3.** A Wormhole Attack

## III. RELATED WORK

Asif Habib [12] described various vulnerabilities in wireless sensor network at network layer and provides us some defensive measures that can be taken against these threats. The paper mainly focuses is on various attacks and their defense measure. The authors discuss various kinds of attacks in network layer- sinkhole attacks, sybil attack, wormhole, selective forwarding and others. In the defense techniques against these attacks the author gives references to various techniques. He also discusses that some encryption technique be applied to prevent these attacks in network layer. The author concludes the paper by arguing the need to develop a unique and light weight protocol to counter these attacks together instead of handling these attacks separately.

Kavitha and Sridharan [13] discussed how security is becoming a major concern for designers of WSN's protocol. The authors discussed protocol stack for WSNs as well as node's constraints in terms of energy, memory and transmission range. The authors provide performance metrics for WSNs as well as for the individual nodes, the need of security and the complication in implementing security are also discussed in detail. This paper provides some guiding principles for implementing security in WSNs. Various classes of attacks like active and passive attacks, mote class and laptop class attacks, host based and network based attacks are defined. The paper provides taxonomy of attacks at each layer in wireless sensor networks.

Dezun Dong *et al.* [14]explore the impact of wormhole attacks on network connectivity topologies, and develop a simple distributed method to detect wormholes, called wormcircle. Wormcircle relies solely on local connectivity information without any requirements on special hardware devices or making any rigorous assumptions on network properties. Authors establish the correctness of this design in continuous geometric domains and extend it into discrete networks. This paper presents two algorithms for wormhole detection the basic and localized wormcircle. They rely solely on local connectivity information without any additional requirements on special hardware devices or making strong assumptions on network properties. Wormcircle makes successful attempt to detect wormholes merely using local connectivity without any rigorous requirements and assumptions. The effectiveness of algorithms is evaluated in randomly deployed sensor networks through extensive simulations.

Lukman Sharif and Munir Ahmed [15] examine some of the most common routing attacks in wireless sensor networks. In particular, they focus on the wormhole routing attack. The examination of the wormhole routing attack and some of the proposed countermeasures makes it evident that it is extremely difficult to retrofit existing protocols with defenses against routing attacks. The authors suggest some methods to countermeasure the wormhole attack in wireless sensor networks. One method is to provide tight time synchronization between the nodes during the route discovery stage, but this is not feasible in case of large networks. Another method includes the use of geographical routing and using modified Ad hoc on demand distance vector routing protocol.

Tiwari and Chaudhary [16] move their research in direction to recognize the malicious wormhole attacker that are available in remote sensor systems. The extent of this work is to contemplate different approaches to apply Worm-Hole assault and infer a need to distinguish and keep WSNs from Worm-Hole Attack in light of Ad-hoc on demand distance vector protocol (AODV).

Anwar et al. [17] present their work to safeguard the wireless sensor network from routing attacks in the presence of malicious nodes, a trust aware distance vector routing protocol (T-AODV) discuss to shield

wireless sensor network from wormhole. Through trial comes that this approach in system effectiveness regarding enhanced packet conveyance proportion, end-to-end defer and number of node to the targeted attacks.

Kaissi et al. [18] presented DAWWSEN as a protection routing protocol for guarding against "wormhole attack" in WSN. They proposed a routing tree protocol and demonstrated its powerfulness through NS-2 simulations. This protocol is based on the hierarchical representation where root node represents the base station and leaf nodes represent the sensor nodes. The base station finds its children nodes by broadcasting a request packet containing the node ID and hop count.

Pirzada and McDonald [19] provide "trust based" scheme for finding and removing sinkhole nodes in WSNs. From human behavior model a trust based scheme is extracted. On the basis of operational mode, trust details are used by every source node in order to obtain best route for base station and leaving behind compromised nodes. The research is deviated from cryptography to trust based scenario to detect attack.

Trust levels are obtained in side by nodes, depending on their trustworthiness in implementation of routing protocol. Number of hops can be more but the nodes in this route are having a greater trust value. This scheme is more satisfactory, can BE deployed easily in the network.

**Table 1.** Qualitative analysis of Wormhole Detection Techniques

| **Technique** | **Proposed Solution** | **Pros** | **Cons** |
|---|---|---|---|
| Song et al. [20] | The proposed scheme make use of the "Statistical analysis" mechanism for detecting any abnormality during routing the packets in multi route environment. During detecting wormhole attacks using SAM scheme no additional architecture or systems is used by the authors in research. | 1.Multi-path routing<br>2. No security architecture, systems or services is used<br>3. Successful in locating malicious nodes.<br>4. Very limited overhead.<br>5. Work well under different topologies and transmission range. | 1. If a malicious node behaves normally during routing, SAM cannot detect it.<br>2. If any real neighbor connection is wrongly labeled as wormhole false positive alarm will be caused |
| Maheshwari et al. | The authors proposed a localized algorithm to detect worm hole attack that is totally dependent on connectivity information. A connected graph is built of the entire multi-hop wireless sensor network. So, by using the information of this forbidden structures of the legal connective graph compromised node is detected. | 1. Does not require any local information or special hardware, making it a universal technique.<br>2. Work effectively in low density networks where disconnection rate is high.<br>3. No timing analysis<br>4. It can also detect attacks launched before the network is set-up. | 1. Network is assumed disconnected if two nodes do not have a path between them. |
| Hu et al. | Packet leashes scheme is used by the | 1. Prevents packets from | 1. Need highly |

| | | | |
|---|---|---|---|
| [21] | authors to detect wormhole attacks in WSN. Packet Leashes may be of two kind: geographical leashes and other one is temporal leashes. Also, in the proposed work TIK protocol used to implement temporal leashes. TIK provides authentication and better performance to the proposed mechanism. | travelling farther than radio transmission range.<br>2. TIK protocol can be easily implemented on current technologies.<br>Less computation and storage is required by TIK. | synchronized clocks.<br>2. Each node must know its own location.<br>3. All nodes must have loosely synchronized clocks. |
| DELPHI (Delay Per Hop Indication) [4] | In this proposed scheme "delay per hop indication" (DELPHI) techniques is used to detect wormhole attack. Delays between the sender and the receiver sensor nodes is calculated and based on this calculation wormhole attack is detected. | 1. Collects information at sender, therefore, no need of synchronized clocks.<br>2. Does not need position information.<br>3. High power efficiency as no requirement of mobile devices to equip with hardware.<br>4. Performance: 95% to detect normal paths and 90% to detect wormhole attack.<br>5. It can detect both hidden and exposed attacks. | 1. False alarm is not detected.<br>2. Rescheduling of packet propagating is very high. |
| Poovendran and Lazos [22] | For detecting worm hole attacks the authors construct a communication graph of the sensor nodes in the network. Based on this graph they proposed a mechanism based on local- broadcast keys to avoid wormhole attack. | Requirement: Combination of location information and cryptography<br>Uses location aware guard nodes equipped with GPS receivers.<br>Based on Local broadcast keys. | |
| MDS-VOW [6] | The proposed scheme detect the wormhole attack in WSN by using MDS-VOW protocol. MDS-VOW rebuild the network frame-wok using the multidimensional scaling technique to balance the deformation occurs due to distance measurement faults. After that MDS-VOW visualize the abnormalities caused by fake nodes, it rebuilds the network by bringing the far nodes together and removing the compromised nodes. | 1. Does not require sensors to be equipped with special hardware<br>2. Works effectively in dense networks | It is assumed that sensors are not self-movable. |

| | | | |
|---|---|---|---|
| Buch and Jinwala [23] | The proposed method used a two-hop neighbor node technique to detect and prevent the worm hole attack in the wireless sensor network. In this scheme while sending the data packets validity of the two- hop neighbor node is checked, if it is illegal then a wormhole attack is detected in the network. | 1. No special hardware or time synchronization is required.<br>2. Only self-geographical location is required. | Only focuses on the type of wormhole with out-of-band channel. |
| Tun and Maw [24] | In this proposed system RTT (Round Trip Time) and "neighbor number" of nodes is used to detect wormhole attack in WSN. The compromised node can increase the "neighbor number" of other nodes in the network due to which detection of wormhole is possible .This scheme is mainly designed for Ad-hoc On Demand Routing Protocol(AODV) and can be extended to other protocols also. | 1. No special hardware.<br>2. Less overhead<br>3. Good performance | Depends on successful transmission of packets. |

## IV. CONCLUSION

This paper shows a qualitative analysis of various approach to detect and prevent wormhole attack in wireless sensor networks. The advantages and disadvantages of various schemes is presented. It is found that that various schemes are effective in various situations. In future we will devise an algorithm for the detection of these attacks.

## V. REFERENCES


[1]. A. Tayebi, S. Berber, and A. Swain, "Wireless Sensor Network Attacks:An Overview and Critical Analysis," in Seventh International Conference on Sensing Technology Wireless, 2013, pp. 97-102.

[2]. A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Secure Localization Algorithms for Wireless Sensor Networks," IEEE Commun. Mag., no. April, pp. 96-101, 2008.

[3]. S. Zhang and H. Zhang, "A review of wireless sensor networks and its applications," 2012 IEEE Int. Conf. Autom. Logist., no. August, pp. 386-389, 2012.

[4]. M. Islam and S. AshiqurRahman, "Anomaly intrusion detection system in wireless sensor networks: security threats and existing approaches," Int. J. Adv. Sci. Technol., vol. 36, pp. 1-8, 2011.

[5]. K. Xing, R. S. S. Srinivasan, M. Rivera, J. Li, and X. Cheng, "Attacks and Countermeasures in Sensor Networks : A Survey," in Network Security, S. C.-H. Huang, D. MacCallum, and D.-Z. Du, Eds. Boston, MA: Springer US, 2005, pp. 251-272.

[6]. V. P. Singh, S. Jain, and J. Singhai, "Hello Flood Attack and its Countermeasures in Wireless

Sensor Networks," Int. J. Comput. Sci. Issues, vol. 7, no. 3, pp. 23-27, 2010.

[7]. A. Gupta and A. K. Gupta, "A Survey: Detection and Prevention of Wormhole Attack in Wireless Sensor Networks," vol. 14, no. 1, 2014.

[8]. M. Studies, R. Gill, B. Road, and B. Road, "Sybil Attack Detection and Prevention Using AODV in," vol. 13, no. 7, 2013.

[9]. S. Sharmila and G. Umamaheswari, "Detection of sinkhole attack in wireless sensor networks using message digest algorithms," in Proceedings of 2011 International Conference on Process Automation, Control and Computing, 2011, pp. 1-6.

[10]. J. Brown and X. Du, "Detection of selective forwarding attacks in heterogeneous sensor networks," in IEEE International Conference on Communications, 2008, pp. 1583-1587.

[11]. E. Fazeldehkordi, I. S. Amiri, and O. A. Akanbi, A Study of Black Hole Attack Solutions: On AODV Routing Protocol in MANET. 2015.

[12]. A. Habib, "Sensor Network Security Issues at Network Layer," in 2nd International Conference on Advance in Space Technologiees (ICAST 2008), 2008, pp. 58-63.

[13]. T. Kavitha and D. Sridharan, "Security Vulnerabilities In Wireless Sensor Networks : A Survey," J. Inf. Assur. Secur., vol. 5, pp. 31-44, 2010.

[14]. D. Dong, M. Li, Y. Liu, and X. Liao, "WormCircle: Connectivity-Based Wormhole Detection in Wireless Ad Hoc and Sensor Networks," in Proceedings of 2009 15th International Conference onParallel and Distributed Systems (ICPADS), 2009, pp. 72-79.

[15]. L. Sharif and M. Ahmed, "The Wormhole Routing Attack in Wireless Sensor Networks (WSN)," J. Inf. Process. Syst., vol. 6, no. 2, pp. 177-184, 2010.

[16]. M. Tiwari and J. Choudhary, "Study of Wormhole Attack in Wireless Sensor Networks," Int. J. Comput. Appl., vol. 5, no. 4, pp. 1-7, 2015.

[17]. R. W. Anwar, M. Bakhtiari, H. Abdullah, and K. N. Qureshi, "Enhanced Trust Aware Routing against Wormhole Attacks in Wireless Sensor Networks," in International Conference on Smart Sensors and Application, 2015, pp. 56-59.

[18]. R. El Kaissi, A. Kayssi, A. Chehab, and Z. Dawy, "DAWWSEN : A Defense Mechanism against Wormhole Attacks in Wireless Sensor Networks," in Second International Conference on Innovations in Information Technology, 2005.

[19]. A. A. Pirzada and C. Mcdonald, "Circumventing Sinkholes and Wormholes in Wireless Sensor Networks," in Proceedings of International Workshop on Wireless Ad-hoc Networks (IWWAN'05), 2005, vol. 71, no. May.

[20]. N. Song, L. Qian, S. Ning, Q. Lijun, and L. Xiangfang, "Wormhole attacks detection in wireless ad hoc networks: a statistical analysis approach," Parallel Distrib. Process. Symp. 2005. Proceedings. 19th IEEE Int., p. 8 pp., 2005.

[21]. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," IEEE INFOCOM 2003. Twenty-second Annu. Jt. Conf. IEEE Comput. Commun. Soc. (IEEE Cat. No.03CH37428), vol. 3, no. C, pp. 1976-1986, 2003.

[22]. L. Lazos, R. Poovendran, C. Meadows, P. Syverson, and L. W. Chang, "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach," IEEE Wirel. Commun. Netw. Conf. 2005, vol. 2, pp. 1193-1199, 2005.

[23]. D. Buch and D. Jinwala, "Prevention of Wormhole Attacks in Wireless Sensor Network," Ijnsa, vol. 3, no. 5, pp. 85-98, 2011.

[24]. Z. T. and A. H. Maw., "Wormhole attack detection in wireless sensor networks," Proc. World Acad. Sci. Eng. Technol. Technol., vol. 46, no. 3, pp. 545-50, 2008.