International Journal of Engineering & Technology, 7 (2.23) (2018) 59-62

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Security Techniques for Wormhole Attack in Wireless Sensor Networks

Surinder Singh[1] andHardeep Singh Saini [2]

[1]Research Scholar, IKG PTU, Kapurthala, Punjab, India
[1]Assistant Professor,Chandigarh Engineering College,Landran,Punjab,India, email: sunny16387@gmail.com
[2]Indo Global College of Engineering, Abhipur, Punjab, India
Email: hardeep_saini17@yahoo.co.in

Abstract

The wireless sensor network has group of sensors which can sense the data and route this data to base station. As there is no physical connection between sensor and base station the important data can be routed without wires. The broadcast nature of wireless sensor network makes it prone to security threat to the valuable data. The attacker node can detect the data by creating their own data aggregation and routing mechanism .The number of attacks can be possible on the network layer. Out of these attacks wormhole is one of the major attack which can change the routing method of the whole wireless sensor network. In this attack,the attacker node can control the packet transmission of whole network and route it to the tunnel of nodes. The major drawback of this attack is to increase the packet drop and disturbing the routing mechanism. A number of security techniques are developed by the researcher to reduce the packet drop ratio and secure the routing mechanism of the network. Out of all thesetechniquesfew related to packet drop ratio are discussed in this paper. TheLightweight countermeasure for the wormhole attack (LITEWORP) based on Dynamic Source routing (DSR) protocol security technique,Delay Per Hop Indication (Delphi) based on AODV(Avoidance Routing Protocol) Protocol security technique and MOBIWORP based on DSRprotocol security technique reduce the packet loss percentage 40%,43% and 35% respectively.

Keywords:*Attacker node, Detection techniques, Security,Wormhole attack, Wireless Sensor Networks*

1. Introduction

The nonstop improvement in Wireless Sensor Networks (WSNs) has added to their broad application in various businesses, incorporating into scratch zones, for example, the electrical, social insurance, and military ventures. Every one of these zones keeps up strict security necessities as a result of its extraordinary requests. Subsequently, the security of WSNs is pivotal. WSNs confront both malicious outside and malignant inner hub assaults that are arranged in view of the assault source. Outside hub assaults can be averted with confirmation and encryption innovations; be that as it may, interior hub assaults are hard to kill with these methodologies[1][2]. In this manner, interruption identification is viewed as a moment line of safeguard for ensuring the security of a WSN. Figure 1 shows the impact of wormhole attack on wireless sensor network. The red nodes are affected nodes and the series of black circles nodes are the attacker node which itself make a tunnel. This tunnel is known as wormhole tunnel. The white circles are the non-affected nodes. The wormhole tunnel destroys the routing and data aggregation of wireless sensor network. The green circle is the base station which can collect the data from all the sensor nodes within the network. The tunnel also creates an artificial path for data transmission and reply locally to the sensor nodes[3][4]. The wormhole attack can increase the packet drop ratio as all important information from the sensor nodes are directly communicated with attacker node. This wormhole tunnel can be detected by the detection techniques which further reduce the packet drop ratio discussed later in this paper. The current drive in the data innovation industry toward new remote specialized gadgets and frameworks and their use in tending to a wide assortment of true issues has brought about a few new territories of dynamic research, remote sensor systems being one such interesting issue.

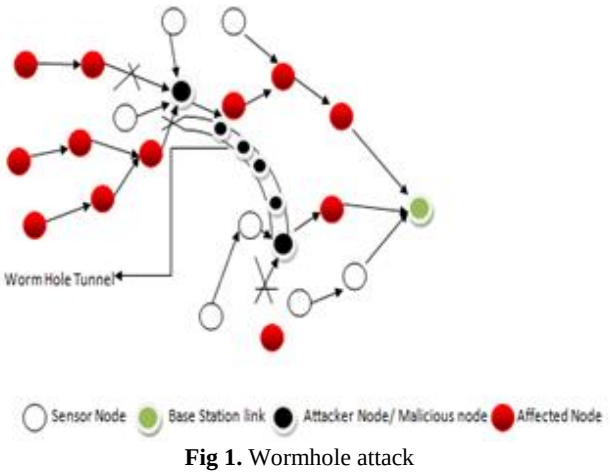

Fig 1. Wormhole attack

A number of researchers made many routing protocols which can reduce the packet drop ratio. The packet drop rate is basically the rate at which the packets are dropped by the attacker nodes[5][6]. Sensor hubs have to be a great degree constrained assets, for example, battery life, memory space and handling capacity. Directing conventionsand calculations are wanted to accomplish longer sensor life. WSNs are self arranging and self sorting out

Copyright © 2016Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

remote systems. The topology of sensor arranges changes quickly and arbitrarily. Sensor hubs are consistently included and erased from the system. WSNs have brought together the approach as far as system control is concerned. The base stations could communicate inquiry/control data to sensor hubs.Among the plans of WSNs, security is one of the critical perspectives that merits the extraordinary. As we know, the Internet has possessed the capacity to furnish countless with the capacity to move different types of data speedy and consequently reformed business, resistance, training, industry, research, and science. Sensor systems administration may, over the long haul, be similarly critical by giving estimation of the physical marvels around us, prompting their comprehension and eventually the usage of this data for an extensive variety of down to earth applications. Potential utilization of sensor organizing incorporate resistance, ecological and living space observing, medicinal services checking, transportation, assembling, and pursuit and protect.

An average WSN comprises of a base station and a few hubs dispersed or situated in the earth of intrigue. Every hub is relied upon to distinguish occasions of intrigue and gauge parameters that portray these occasions. The subsequent data at a hub should be transmitted to the base station either specifically or in "multi-jump" mold including programmed steering through a few different hubs in the system. Usage of such a system requires equipment segments and comparing programming modules to program these parts in an agreeable manner.A business equipment stage that is being examined comprises of processor cum radio sheets normally alluded to as "bits". Every bit, a battery-controlled gadget, comprises of a sensor unit, a power unit, a two-way ISM band radio handset unit (incorporates a RF reception apparatus), an ADC unit, a processor that runs tinyOS-based code, and lumberjack memory fit for stockpiling to 100,000 estimations. A base station comprises of a bit joined to a bit interface-board that is interfaced to a PC by means of the parallel port. A stationary system is characterized as a system of sensor hubs, in which, every sensor hub's position is settled with respect to the base station and different hubs in the system. An exhibited application toward this path is stickiness checking in a vineyard. Information procured by a bit is transmitted to the base station which at that point forms the data and triggers essential activities, for example, limited watering. There are two conceivable cases to transmit information. At the point when a hub is in coordinate remote contact i.e. in the scope of the base station, coordinate correspondence is conceivable. At the point when a hub isn't in the range, it transmits information in a specially appointed condition likewise alluded to as multi-bounce. Execution of a productive multi-jump framework requires ideal directing to encourage most limited course, lessened power utilization and enhanced transmission.An case in this classification is a group of creatures on a broad homestead, where every creature is furnished with a sensor hub. The creatures are in consistent movement with respect to each different and in addition the base station. Such a confounded versatility administration requires a much more complex usage of steering calculations. Keeping in mind the end goal to maximally profit by remote sensor systems of this compose, we predict extra equipment prerequisites as GPS gadgets and different types of bit location.A remote sensor orchestrate (WSN) has basic applications, for instance, remote common checking and target following. This has been enabled by the availability, particularly starting late, of sensors that are more diminutive, more affordable, and adroit. These sensors are equipped with remote interfaces with which they can talk with each other to shape a framework. The layout of a WSN depends basically on the application, and it must think about variables, for instance, the earth, the application's arrangement targets, cost, gear, and structure prerequisites. Sensor center points are low power contraptions arranged with no less than one sensors, a processor, memory, a power supply, a radio, and an actuator. An arrangement of mechanical, warm, regular, compound, optical, and alluring sensors may be added to the sensor center point to evaluate properties of the earth. Since the sensor centers have compelled memory and are normally passed on in difficult to-get to zones, a radio is executed for remote correspondence to trade the data to a base station (e.g., PC, individual handheld contraption, or a passageway point to a settled establishment). Battery is the basic power source in a sensor center point. Discretionary power supply that harvests control from the earth, for instance, sun controlled sheets may be added to the center depending upon the appropriateness of nature where the sensor will be passed on. Dependent upon the application what's more, the kind of sensors used, actuators may be participated in the sensors.

2. Types of Wormhole Attack

The wormhole attack can be classified into four categories.In this segment, we characterize the wormhole assault in light of the methods utilized for propelling it. Number of hubs associated with building up wormhole and the best approach to set up it orders wormhole into the accompanying kinds [1][7].

2.1 Wormhole using Packet Encapsulation

Here a few hubs exist between two noxious hubs and information bundles are exemplified between the vindictive hubs. Henceforth it keeps hubs on path from increase bounce tallies. The bundle is changed over into unique frame by the second end point. This method of wormhole assault isn't hard to dispatch since the two closures of wormhole don't need any cryptographic data, or exceptional prerequisite, for example, high-control source or high transmission capacity channel.

2.2 Wormhole using Out-of-Band Channel

This sort of wormhole approach has just a single malignant hub with much high transmission capacity in the system that draws in the bundles to take after way going from it. The odds of malevolent hubs exhibit in the courses built up amongst sender and collector increments for this situation.

2.3 Wormhole using Packet Relay

At least one noxious hub can dispatch packet transfer based wormhole assaults. In this sort of assault pernicious hub replays information bundles between two far hubs and thusly counterfeit neighbors are made. This sort of assault is additionally called as "replay-based assault" in the writing.

2.4 Wormhole using Protocol Distortion

In this method of wormhole assault, single malignant hub tries to pull in arrange movement by misshaping the directing convention. This mode does not influence the system directing much and henceforth is safe. Likewise it is known as "surging assault" in the writing.

Table 1: Summary of Wormhole Attack

Type of attack	Minimum no. of Attacker node	Hardware Requirement
Packet Encapsulation	Two	None
Out-of-Band Channel	Two	High speed wireless link
Packet Relay	One	None
Protocol Distortion	One	None

Table 1 summarizes the type of wormhole attack with respect to minimum no. of attacker node requirement and hardware requirement. For first type of wormhole attack that is packet Encapsulation the minimum no. of attacker node requirement are

two and hardware requirement is none. Similarly the Out of Band channel, Packet Relay and protocol Distortion the requirements are mentioned in Table 1.

3. Security Techniques against wormhole attack

In this section few detection schemes wormhole attack are discussed. Based on previous work the detection schemes are classified in this part. All these schemes work on packet drop ratio against wormhole attack. These security schemes are

- LITEWORP (Lightweight countermeasure for the wormhole attack) based on Dynamic Source routing (DSR) protocol security technique [8]
- Delay Per Hop Indication (DelPHI)based on Avoidance [10] Routing Protocol (AODV) Protocol security technique
- MOBIWORP based on DSRprotocol security technique [11]

These techniques are discussed in detail in the coming section.

3.1 LITEWORP based on Dynamic Source routing (DSR) protocol security technique

LITEWORP (Lightweight countermeasure for the wormhole attack) in wirelesssensor systemsuses DSR routing protocol for transmission of data within the network. This permits identification of the wormhole, trailed by disconnection of the noxious hub. Each wormhole is recognized and secluded inside a brief timeframe over a substantial scope of situations. The outcomes additionally demonstrate that the division of packets lost because of the wormhole attack.LITEWORP, to recognize and moderate wormhole assaults in static specially appointed and sensor remote systems. It utilizes secure twohop neighbor revelation and nearby observing of control movement to identify hubs engaged within the wormhole assault. It uses dynamic source routing protocol. [8]. It gives a countermeasure procedure that confines the malevolent hubs from the system. They give a novel scientific categorization of the distinctive manners by which wormhole assaults can be propelled and demonstrated. LITEWORP can be utilized to deal with every type of wormhole attacks. It has a few highlights that make it particularly appropriate for asset obliged remote conditions, for example: sensor systems. It does not require specific equipment, for example, directional radio wires etc. It doesn't require time synchronization between the hubs in the system. It doesn't expand the extent of the system movement, and causes immaterial data transfer capacity overhead.The lightweight element of LITEWORP is as opposed to different countermeasures for wormhole assaults[9]. It reduces the packet loss rate upto 40%.

3.2 Delay Per Hop Indication (DelPHI) based on Avoidance Routing Protocol (AODV) security technique

In DelPHI technique, wormhole location is introduced to gather both leapcount and delay data of disjoint ways. The explanation for this is that under typical circumstance, they refer a bundle encounters in proliferate one hop data to be comparative along each count. Under a wormhole assault, the deferral for engendering crosswise over false detection ought to be nonsensically high since there are in reality numerous increase between them [10].To stay away from the need of synchronized time sequence, situating gadget and other unique durable sequence, it gathers data and performs discovery at the sender. It gets postponement and skip data path like the AODV course setup component [10].It uses delay per hop indication routing protocol At the point when the identification is started, the sender communicates a demand message to the recipient, and the beneficiary answers all the demand messages got. Along these lines, the sender can get the data of some other ways to the beneficiary. It reduces the packet loss rate up to 43%.

3.3 MOBIWORP based on Dynamic Source routing(DSR) protocol security technique.

A convention called MOBIWORP for relieving the wormhole assault in versatile multi-hop specially used, sensor systems with two conventions viz. Self-centered Move Convention and Connectivity Aided Protocol with constant velocity for contrasting degrees of usefulness to a portable hub. The neighborhood and worldwide detachment conventions that will destroy the capacity of the malignant hubs from propelling further assaults after discovery, whether at the current area or at another area. They showed the impact of MOBIWORP under various system conditions and portability designs utilizing a reproduction model [11].The discovery in MOBIWORP is of two kinds'neighborhood identification and worldwide location. In the former, the used hub is recognized by its present neighborhood in a circulated mold [11]. In the last mentioned, the adversary is identified on a worldwide system scale by the important aspect which protects at numerous areas. The principal convention proposed under MOBIWORP is known as the Selfish Move convention[12]. In this, the versatile hub can create, send, and get its own movement . This method emerges a hub that can just dispatch a wormhole assault in the event that it can forward packets. It may make the system to detache if an extensive portion of the hubs are versatile in the meantime[13][14]. MOBIWORP gives a strategy that confines the malignant hubs from the system in this manner evacuating their capacity to cause future harm. The disconnection is accomplished in two stages – locally, whereby the malevolent hub is expelled from the present neighborhood and internationally utilizing worldwide data at the focal expert with the goal that a peripatetic versatile hub can't cause unbounded harm in the system[15][16]. The identification procedures are done wisely to limit the likelihood of defrauding pure hubs due to false detection caused by characteristic crashes in the remote medium[17]. It reduces the packet loss rate upto 35%.Table 2 gives theSummary of Wormhole security techniques with respect to packet loss rate.

Table 2: Summary of Wormhole security techniques with respect to packet loss rate%

Wormhole Security Technique	Packet loss rate %
LITEWORP based on DSR(Dynamic Source routing) protocol security technique	40%
DelPHI (Delay Per Hop Indication) based on AODV(Avoidance Routing Protocol) Protocol security technique	43%
MOBIWORP based on DSR(Dynamic Source routing) protocol security technique	35%

4. Conclusion and Future scope

The requirement of wireless sensor network in many applications changed the focus of researcher to work on wireless sensor network parameters. The security becomes a very important challenge when attacks like wormhole attacks reduce the performance of wireless sensor network. In this paper three techniques Lightweight Countermeasure for the Wormhole Attack (LITEWORP) based on Dynamic Source Routing Protocol Security Technique,Delay Per Hop Indication (Delphi) based on AODV(Avoidance Routing Protocol) Protocol Security Technique and MOBIWORP based on Dynamic Source Routing Protocol Security Techniqueto overcome this attack are discussed in detail. These schemes are capable of reducing the packet loss rate to minimum level. The hybrid approach for any of two schemes further reduces the packet loss to minimum level. These techniques can also be used for other network layer attacks in future.

5. References

[1] P. Maidamwar and N. Chavhan, "A Survey on Security Issues to Detect Wormhole Attack in Wireless Sensor Network," *Int. J. Ad hoc Netw. Syst.*, vol. 2, no. 4, pp. 37–50, 2012.

[2] J. H. Zheng, H. Y. Qian, and L. Wang, "Defense technology of wormhole attacks based on node connectivity," *Proc. - 2015 IEEE Int. Conf. Smart City, SmartCity 2015, Held Jointly with 8th IEEE Int. Conf. Soc. Comput. Networking, Soc. 2015, 5th IEEE Int. Conf. Sustain. Comput. Communic*, pp. 421–425, 2015.

[3] M. Seth, "Detection of Wormhole Attacks in Wireless Sensor Networks Detection of WormHole Attacks in Wireless Sensor Networks by," vol. 3, pp. 21–25, 2012.

[4] C. Paper, W. Znaidi, and S. Appliqu, "Detecting wormhole attacks in wireless networks using local neighborhood information Detecting Wormhole Attacks in Wireless Networks Using Local Neighborhood Information," no. December 2015, 2008.

[5] Z. Rui and Z. Yanchao, "Wormhole-Resilient Secure Neighbor Discovery in Underwater Acoustic Networks BT - INFOCOM, 2010 Proceedings IEEE," pp. 1–9, 2010.

[6] J. Harbin, P. Mitchell, and D. Pearce, "Wireless sensor network wormhole avoidance using disturbance-based routing schemes," *Proc. 2009 6th Int. Symp. Wirel. Commun. Syst. ISWCS'09*, pp. 76–80, 2009.

[7] X. Lu and Z. Yonghua, "Modeling the wormhole attack in underwater sensor network," *2012 Int. Conf. Wirel. Commun. Netw. Mob. Comput. WiCOM 2012*, pp. 5–8, 2012.

[8] I. Khalil, S. Bagchi, and N. B. Shroff, "LiteWorp: Detection and isolation of the wormhole attack in static multihop wireless networks," *Comput. Networks*, vol. 51, no. 13, pp. 3750–3772, 2007.

[9] M. Y. Su, "WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks," *Comput. Secur.*, vol. 29, no. 2, pp. 208–224, 2010.

[10] Hon Sun Chiu and King-Shan Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks," *2006 1st Int. Symp. Wirel. Pervasive Comput.*, pp. 1–6, 2006.

[11] I. Khalil, S. Bagchi, N. B. Shroff, C. Engineering, N. Avenue, and W. Lafayette, "MOBI W ORP : Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks," pp. 1–12.

[12] J. Wu, H. Chen, W. Lou, Z. Wang, and Z. Wang, "Label-Based DV-Hop Localization Against Wormhole Attacks in Wireless Sensor Networks," *2010 IEEE Fifth Int. Conf. Networking, Archit. Storage*, pp. 79–88, 2010.

[13] Q. Li and Q. Zeng, "Efficiently detecting wormhole attacks in sensor networks by information potential," *3rd Int. Conf. Commun. Netw. China, ChinaCom 2008*, pp. 692–698, 2008.

[14] T. N. D. Pham and C. K. Yeo, "Statistical wormhole detection and localization in delay tolerant networks," *2014 IEEE 11th Consum. Commun. Netw. Conf. CCNC 2014*, pp. 380–385, 2014.

[15] B. Yu and T. Li, "Study of wormhole attack detecting based on local connectivity information in wireless sensor networks," *2011 Int. Conf. Comput. Sci. Serv. Syst. CSSS 2011 - Proc.*, pp. 3585–3588, 2011.

[16] I. Khalil, S. Bagchi, and N. B. Shroff, "LITE WORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks," *Proc. Int. Conf. Dependable Syst. Networks*, pp. 612–621, 2005.

[17] M. Čagalj, S. Čapkun, and J. P. Hubaux, "Wormhole-based antijamming techniques in sensor networks," *IEEE Trans. Mob. Comput.*, vol. 6, no. 1, pp. 100–114, 2007.