International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Wormhole Detection Mechanism in Wireless Sensor Networks

Gandham Swetha, Y.Vijay Bhaskar Reddy, S.Sai Satya Narayana Reddy

Abstract: ***A Wireless Sensor Network (WSN) is a component with sensor nodes that continuously observes environmental circumstances. Sensor nodes accomplish different key operations like sensing temperature and distance. It has been used in many applications like computing, signal processing, and network self-configuration to expand network coverage and build up its scalability. The Unit of all these sensors that exhibit sensing and transmitting information will offer more information than those offered by autonomously operating sensors. Usually, the transmitting task is somewhat critical as there is a huge amount of data and sensors devices are restricted. Being the limited number of sensor devices the network is exposed to different types of attacks. The Traditional security mechanisms are not suitable for WSN as they are generally heavy and having limited number of nodes and also these mechanisms will not eliminate the risk of other attacks. WSN are most useful in different crucial domains such as health care, environment, industry, and security, military. For example, in a military operation, a wireless sensor network monitors various activities. If an event is detected, these sensor nodes sense that and report the data to the primary (base) station (called sink) by making communication with other nodes. To collect data from WSN base Stations are commonly used. Base stations have more resources (e.g. computation power and energy) compared to normal sensor nodes which include more or less such limitations. Aggregation points will gather the data from neighboring sensor nodes to combine the data and forward to master (base) stations, where the data will be further forwarded or processed to a processing center. In this manner, the energy can be preserved in WSN and the lifetime of network is expanded.***

Keywords: WSN, sink, sensor nodes.

I. INTRODUCTION

The principle of wormhole attack depends on malicious nodes. The person who wants to attack creates two or more malicious nodes at different places. Initially they were connected with low latency. As a process, they creates virtual tunnel. It is used for packet transformation. Attacker used to record transmitted packets in one location, and transfer to other location using tunnel.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
Gandham Swetha*, Asst. Professor**,** Vardhaman College of Engg, Hyderabad, India. E-mail: gandhamswetha47@gmail.com
Y.Vijay Bhaskar Reddy, Assoc. Professor, Vardhaman College of Engg, Hyderabad, India. E-mail: yaramala.vijay@gmail.com
S.Sai Satya Narayana Reddy, Principal, Vardhaman College of Engg, Hyderabad, India. E-mail: saisn90@gmail.com

This kind of attack is serious in WSN, because of it is possible even without hosting nodes[1].
Let us use the following example to understand wormhole attack. Let us assume A and B are two networks. Among them one of them is initiated as malicious node, and are considered as malicious nodes. These wormhole nodes are connected through a link. Because of this link, neighbor nodes X and Y considered as neighbors. The attacker can suspend communication between A and B. Network can reschedule transmission when it is found that attack occurs. In protocol discovery, it is also observed that packets will be received in fast A to B. it can happened in link when number of hops are small. This disrupts the routing protocol[2] and causes severe damage to the network.
This kind of attack is complex than other kind of attacks in WSNs. If the attackers are connected to the wormhole link, then such can cause forming tunnel. If the attackers are connected in link, then attacker has a flexible environment such that they can make wrong direction. Due to the above scenario, routing get confused and disrupted in tunnels. The tunnel formed between the two colluding attackers is referred to as wormhole link.
Figure 1 represents the working principles of the wormhole attack. It uses the same line for sending and receiving packets during the transmission of X and Y. Usually, to access a packet a lot of hops needs to be travelled. If the packets are near to X and Y, they will be reaching X and Y before visiting multiple hops. Due to this, it allows others to believe that A and B are neighbors.

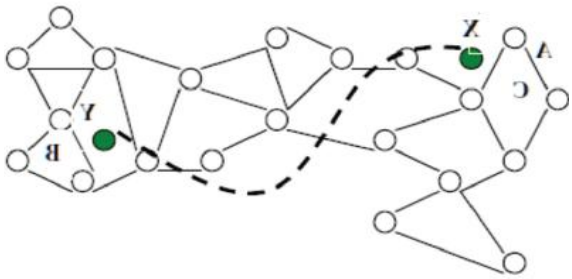

Figure1: Wormhole Attack

II. LITERATURE SURVEY

Firstly, Hu et al [1] presented the report on ad-hoc networks that focus on wormhole attacks. The same authors have presented another approach packet leashes to avoid packets that are roaming outside transmission range. The proposed methodology consider Geographical and Temporal leashes. In the first one, each node is aware of its location and associated with synchronized clocks to establish relation with neighbors. In packet transmission, each node is associated with transmission and position. At receiving end, it determines the distance from the sender and transmission time.

This kind of distance calculation helps receiver to verify the packet gone through the wormhole or other path. In other method that is temporal leashes, each node is associated with clock that is tightly synchronized [2]. These two uses hash chains that compute lightweight operations for validating nodes [3]. Because of these additions the computation overhead is low.

Song proposed a new approach based on the analysis of routing that is named as wormhole mechanism. A tunnel is created for high frequency transmission. These kind of tunnels will be requested based on the analysis of routing. This kind of mechanism helps in handling abnormal frequency in routing. This kind of mechanism gives more challenging and informative when it is integrated into intrusion detection systems. But it is suitable for on-demand routing protocols that are multipath [1].

Hu et al [4] have proposed hardware kind of mechanism using directional antennas. This method is under the assumption that there is no wormhole link. Here, sender has to send packets in some direction, then the receiver which is located in the opposite direction receive packets. It is observed that the neighbors are get paired when directions are matched. Unfortunately, it is required to have special hardware.

General measure for calculating message travelling time is known as Round Trip Time is also popular as RTT. Tran et al[2] and Sampoli et al [1] used RTT and acknowledgement. It is calculated from route request from sender to replay received from receiver. Node A calculates Round Trip Time between sender and its neighbors. This measure helps in finding actual and dummy neighbors. Sender node can easily find the dummy whose distance usually higher than between two actual neighbors. It does not need any hardware to transmit packets.

Jain et al. [1] proposed Trust-Based method for separating nodes that are malicious in the wormhole. Here, they determine how much it is suitable based on their genuine participation in routing rules. This conviction helps in avoiding participation in wormholes. Because trust level should be minimum as per the requirement. The dropping rate[6] It has been reduced to 20% and increased throughput to 8-9%.

III. PROPOSED WORK

Usually attacks in Wormhole happen at network-layer protocols. For new routing protocols, it is essential to study the limitations of the existing routing protocols. This kind of study allows to propose new protocol. The study on the limitations of the proposed method gives more prominent rules for network protocols. It happens by examining the measured performance w.r.t to the possible attacks [6]. The proposed method effectiveness is determined from the comparison of the wormhole detection existing techniques. It is observed that there is a lot to do in measuring the performance of existing wormhole detection techniques on proposed routing protocols. It can be extended in incorporating security enhancements along with routing protocols in WSN.

Dynamic WSN is an intensive area that offers many challenges. The detection of wormhole is not straight forward method. One instance is, Let say X and Y are two sensors that were identified as far away from each other. Because of dynamic, they may be 1 hop away from each other. The result of such instances gives direction towards conformation that attack has happened. Hence it is challenging task to determine what genuine attacks are, and differentiate from malicious nodes [7].

I would like to develop a new approach which detects wormhole attack as the research work in the field related to Wireless Sensor Networks (WSN).This proposed approach will handle wormholes in effective manner.

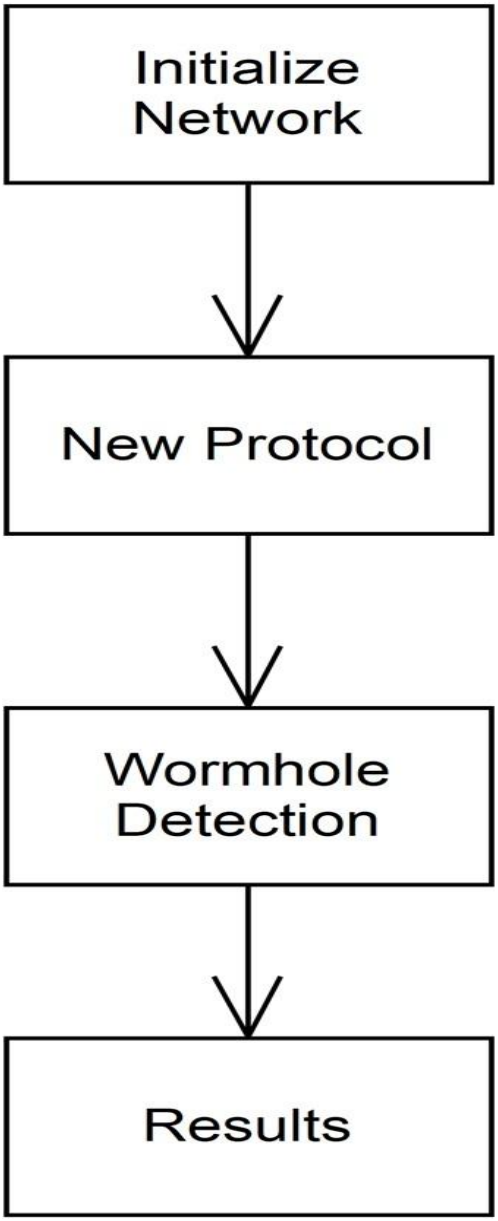

Figure: 2 Proposed Wormhole detection

IV. RESULTS AND DISCUSSIONS

To implement the new routing protocol various researches has been done to show the better results. By using simulation in java and netbeans 8.0.2 as the programming the results are shown based on the performance of the proposed system. Totally there are 100 nodes are initialized and among those the malicious nodes are detected with more accuracy by using the proposed system. Table 1 shows the performance of proposed system with accuracy.

Total number of Normal Nodes	Total number of malicious Nodes	Accuracy
100	8	92%

Table: 1 show the performance of the proposed system

V. CONCLUSION

In this paper, a new routing protocols, it is essential to experiment the limitations of the existing routing protocols. This kind of research allows proposing new protocol. WSN are mainly unpredictable in nature and have various issues regarding the wormhole attack. In this system, the detection of malicious nodes plays the major role. Based on the behavior of the nodes the malicious nodes are detected. Thus the proposed system performs well compare with the existing systems.

REFERENCES

1. Preeti Nagrath, Bhawna Gupta, "Wormhole Attacks in Wireless Adhoc Networks and their Counter Measurements: A survey", pp 245-250, IEEE 2011.
2. 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-Apr 2011.
3. Dhara Buch, Devesh Jinwala, "Detection of Wormhole Attacks in Wireless Sensor Networks", IEEE Conference on Advances in Recent Technologies in Communication and Computing, pp 7-14, 2011.
4. Zhibin Zhao, Bo Wei, Xiaomei Dong, Lan Yao, Fuxiang Gao, "Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis", IEEE International Conference on Information Engineering, pp 251-254, 2010.
5. Zaw Tun et al., "Wormhole Attack Detection in Wireless Sensor Network" World Academy of Science, Engineering and Technology 46 2008.
6. Guowei Wu, Xiaojie Chen, Lin Yao, Youngjun Lee, and Kangbin Yim. An efficient wormhole attack detection method in wireless sensor networks. Computer Science and Information Systems, 11(3):1127 – 1141, 2014.
7. Yurong Xu et al., "Detecting Wormhole Attacks In Wireless Sensor Networks" Critical Infrastructure Protection, Chapter 14.