A Reliable and Efficient Design for Detection of Wormhole Attack in Wireless Sensor Networks

P. Balamurugan, K. Marimuthu and M. Shyamala Devi

1Vel Tech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Chennai.
drpbalamurugan@veltech.edu.in
2Vellore Institute of Technology, Vellore.
3Vel Tech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Chennai.

Abstract

Wireless sensor network which, now a days, is affected with several attack. The attack which is happening in WSN, called as wormhole attack. To deal with wormhole attack this paper uses some requirement which is either it uses specialized hardware or in order to capture a specific pattern extra overhead over the network. This paper explains a reliable and efficient design to detection of wormhole attack and localization based method on the basis of key study. The wormholes attack a large number of network traffic so the goal of this paper is to, detect the wormhole which is attacked the flow of networks, reduce the cost of detection of wormhole attack.

Key Words: Wireless sensor networks, attacks, overhead, energy, security, detection and latency.
1. Introduction

WSN, collection of small devices called nodes, is attacked by various attackers, especially destructive wormhole attack, which completely destroyed the network topology. WSN has a base station and sensor devices called nodes. In sensor network field, each node can try to transmit the collected information to the base station. The definition of WSN is clearly shown in figure 1. Sometime due to wormhole attack, sensor nodes are misdirected to base station which is available to few hops ahead. In this case, the data is transmitted through the attacker node. Due to wormhole attack false data will be passed to base station instead of important data. Each node communicates false statements, which is sent by attacker node. The attacker node which leads to unauthorized access to the important data.

![Wireless Sensor Network](image)

Fig. 1: Wireless Sensor Network

**Wormhole attack in WSN:** Sensor node identification privacy, sensor node location privacy, route privacy and data packet privacy are used as some privacy primitives in wsn for secure communication. These primitives which has to secure the data they have. Attacker can collect the security information which is

**Security Requirements in WSN**

Computer security involves in some factors to secure data such as prevention, detection and survivability of attacks. Commonly wsn nodes are deployed in unattended environments to focus on the survivability of attacks. Several properties may be considered to a secure protocol, depending the specific application. In this paper some of security requirements are defined here.

1. Confidentiality which prevents unauthorized access in process of communication.
2. Integrity which is defined as the prevention of unauthorized, either accidental or malicious, modification or destruction of information
would result in deceiving the authorized entity by providing with false information.

3. Authentication is the process of verifying an object’s or entity’s claimed identity in Communication process.

4. Availability: in sensor network, it refers how much time a system is functioning to the user, which means that collecting data from the sensors. It is not directly considered as security requirements but may be considered as an adversary can mount different attacks to interfere with the normal functioning of the sensor network.

5. Data freshness: while message exchange between nodes, they should obey in a message ordinary or have not be reused the old authentic message.

2. Related Work

There are many existing solution in WSN for detection of wormhole attacks and the misbehaving node. In these solutions, many existing protocol uses a specified hardware to provide selection for detection of wormhole attack. Due to use of this specified hardware, it requires extra processing of data, additional cost and based on this nodes consume more energy.

In this part, this paper discuss with some of the solutions available for detecting of wormhole attack. The proposed methods in [1] are to detect the wormhole attack using geographical and temporal packet leaches. GPS and time synchronization are not supported in this work. The paper [2], which reserves a some of the sensor nodes for global positioning locators and directional antennas. This paper also uses broadcasting of keys to transmit the data to the other node. The paper [3] has developed a transmission based route setup which uses to identify the attacks by observing the transmission time among the sensor nodes. The method, developed by Krawczyk, which helps to reduce the cost of the detection of wormhole attack in WSN.

The paper [4] has developed a graph based mechanism for the identification and detection of wormhole attacks, which supports proactive protocols but it fails when UDG model is not supported by the connectivity graphs. A few of methods have discussed with traffic flow analysis using statistical analysis and anomaly based detection scheme. L. Buttyan et.[5], who has developed a mechanism, which is based on statistical analysis method to find multipath routing. It helps to integrate this method with intrusion detection system. The drawback of the protocol is it will be working with on-demand protocol.

3. Problem Formulation

This paper clearly finds the wormhole attack problems in figure 2. In figure1, Node P wants to send data to node Q so it sends request message to node Q through nodes r, s and t. now node Q broadcast the reply request to node P but node r receives the reply request sent by node Q and node r replies reply request
to its neighbor node u and P. in this case, the malicious nodes may be hidden in the network. These nodes can form new link called fast link with help of nodes s, t and P. Hence the node t broadcasts the reply request message to the node Q. in this case, node P wants to transmit the data to node Q but it chooses the alternative path instead of original path which is P→r→s→t→Q, so it can choose shortest path, which is created by malicious nodes, which is P→m1→m2→Q.

The malicious route results in term of delay and packet drop in the networks. So malicious nodes can modify the packet while communicate the information between source to destination.

Fig. 2: Definition of Walmhole Attack

**Objective of the work:** The new method is used to detect the wormhole attack and secure the data in WSN. It can also monitor the forward packets from packet drop, delay, modifying packets and adversaries misdirecting the multi hop routing. Based on these, this paper creates a new framework which is for detection of wormhole attack in WSN.

**Benefits of Proposed Work**

This work is not used a specified hardware. The proposed methodology, which provides detection of wormhole attack in less time, identify the suspected node or attacker node, which also calculates energy level of each node in real time using monitor module. The trustworthiness of each node is also calculated. The proposed method also identifies Message passing node and reply message nodes with help of trust manager. Overall, it improves the performance of WSN.
4. Design and Architecture

In this part, the proposed method is discussed, which is used to detect the wormhole attack in WSN. The Packet drop, delay, modifying packets and adversary misdirecting the multi hop routing are used to secure and analyses the performance of the proposed system against the wormhole attack. WSN which gives protection against identify the deception through replaying routing information. An adversary can exploit this detect to lunch the harmful or even devastating attacks against the routing protocols including wormhole attack. The proposed method, which observes the behaviors of each node in the network, also gives the good performance in the network based routing calculation done in the work, is done on the basis of shortest path to the sink node. The energy watcher module which monitors the energy level of each node, by which packet is transmitted. The routing table, node’s energy level and data will be forwarded to trust agent module which calculates the trust level of each node on the basis of information provided by the routing agent and energy watcher module. If the calculated value is less than between 0.9 and 0.99, then the suspected node is identified as replaying the messages and wormhole attack is detected.

Algorithm of Simulation

Step 1: Start
Step 2: Node initialization (No of nodes used in network)
Step 3: Route selection
Step 4: Routing Agent
   i. Neighbor detection  go to step 6 with periodic “hello packet”
   ii. Topology detection  [Maintaining Routing Table]
   iii. Routing calculation  go to step 6 with data
Step 5: Energy watcher
Step 6: Trust manager
   i. Information collection
   ii. Trust calculation
Step 7: Check Trust Value
   i. If yes, go to step 8
   ii. else,  go to step 3
Step 8: Wormhole attack detected
Step 9: Stop

5. Components of Proposed Methodology

1. Node initialization: it is the process of deploying the sensor nodes to form a network to perform a particular task.

2. Route selection: if node A waits to transmit the data from a base station to other nodes, node A observes the neighboring node position and forwards the data by considering the trust level and the energy level of node.
3. Routing agent: in routing agent, there are the three modules, namely neighbor detection, topology detection and routing calculation, considered for forwarding data to other hops. Neighbor detection which uses neighbor selection algorithm to forward the base station. Topology detection, which is used to identify and for data packet transfer from one node to next node. The routing calculation module which is used to find the shortest path between a node A and next hop.

4. Energy watcher: the energy level of each node is monitored and node’s energy can be calculated. It also checks whether nodes are have energy enough to forward a packet from one node to another.

5. Trust manager: trust manager which is one of the module used in this for calculating the trust of each node based on routing information, neighbor behavior and energy level of nodes, computes the trust of each node and assign to another. The node is identified by having more trust level as trustworthiness.

The trust to the neighboring node X by the node n, and it is given by the following.

$$T_n(t) = \sum_{i=0}^{\infty} [Z_n(i) \times T_n(i)]$$

(1)

Where $Z_n(i)$ is the weight of the $i^{th}$ trust category to n and $T_n(i)$ is the situational trust of n in the $i^{th}$ trust category.

Form equation (1), there is the two equations are derived.

$$A_c = \frac{E_s - E_f}{E_s + E_f} \text{ for } E_s + E_f \neq 0 \text{ else } A_c = 0$$

(2)

$$A_d = \frac{F_s - F_f}{F_s + F_f} \text{ for } F_s + F_f \neq 0 \text{ else } A_d = 0$$

(3)

Hence a value of -1 represents complete distrust, a values of 0 implies non-contributing event and a value of +1 represents the absolute trust in a particular event. Based on The probability of trust level of neighbor estimation, this neighbor correctly delivers the received data to the base station.

6. Result and Discussion

The proposed work in this paper presents an efficient methodology to detect wormhole attack in wireless sensor network. Energy watcher and trust manager are used to calculate the performance of proposed work.

**Activation Latency for Passive Adversary**

The fig.3 shows that the performance of efficient wormhole attack detection which is calculated by plotting the graph between threshold value and time to estimate the activation latency for passive adversary.
Activation Latency for Active Adversary

The fig.4 shows that the performance of efficient wormhole attack detection which is calculated by plotting the graph between threshold value and time to estimate the activation latency for active adversary.

Detection Latency for Passive Adversary

The fig.5 shows that the performance of efficient wormhole attack detection which is calculated by plotting the graph between threshold value and time to estimate the detection latency for passive adversary.
Fig. 5: Detection Latency for Passive Adversary

Detection Latency for Active Adversary

The fig.6 shows that the performance of efficient wormhole attack detection which is calculated by plotting the graph between threshold value and time to estimate the detection latency for active adversary.

7. Conclusion

WSN can be used a number of nodes which can transfer the data from one network to another network without making use of cables and communicate each other nodes through base station. The lifetime of networks is limited because all the nodes are depending upon the residual energy of nodes in the
network. The detection of wormhole attack, which, is proposed in the paper, is effective method because it uses the energy watcher and trust manager. The energy watcher module which maintains the energy of each nodes and trust manager which holds the characters of each node in the network.

References
