Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 5 (2017) pp. 1129-1138

http://www.ripublication.com

An Efficient and Reliable Methodology for Wormhole Attack Detection in Wireless Sensor Network

Jitendra Kurmi[1], Ram Singar Verma[2] and Sarita Soni[3]

[1,2,3] Department of Computer Science
[1,2,3] BBA University (A Central University), Lucknow, India.

Abstract

Now a days, wireless sensor network is affected with an attack, called as wormhole attack. To deal with wormhole attack one of the widely used requirement either they use specialized hardware or in order to capture a specific pattern extra overhead over the network. The paper presents an efficient and reliable wormhole detection and localization based scheme on the basis of key observation that a huge amount of network traffic will be attracted by the wormholes. Our aim is to minimize the cost of detection of wormhole attack.

Keywords: Wireless Sensor Network, Security, Attacks, Communication Overhead, Energy of Node, Message Passing Nodes.

1. INTRODUCTION

Wireless sensor networks are consists of various attacks, especially destructive wormhole attack, which completely destroyed the network topology. In a wireless sensor network, scenario there is a base station and sensor nodes. Some of sensor nodes try to transmit the data information to the base station. Due to wormhole attack in the scenario sensor nodes are misguided that base station is available to few hops ahead. Hence the shortest path is elected to transmit the data, in other words the data is transmitted through the attacker node due to wormhole attack. Finally all the traffic path passes through the attackers which leads to unauthorized access to the important data.

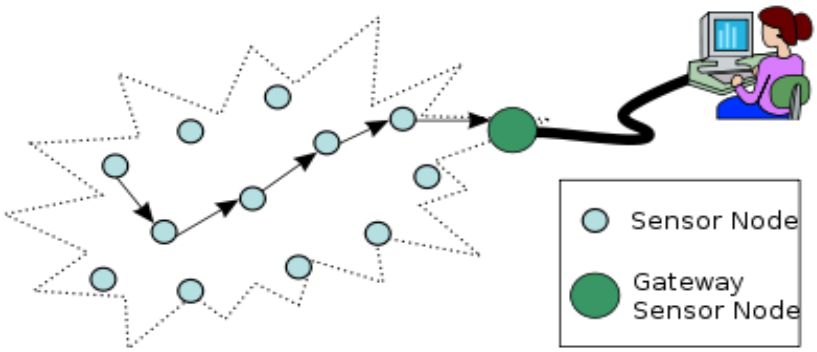


Fig 1. Wireless sensor network

- **Wormhole Attacks in WSN**

For secure communication there are some privacy primitives defined like sensor node identification privacy, sensor node location privacy, route privacy and data packet privacy. These privacy primitives help sensors to secure the data they have. But attacker can easily capture the packet and get this security information and hence can get access to sensor network.

Also sensor nodes have limited resources these nodes need to replace after some time. These sensor nodes are also generally deployed in unattended environment. So in order to steal this sensitive information, attacker compromises any node in the network or he introduces his own node in the network without getting noticed. This node is then called as malicious node which is totally controlled by attacker. A typical wormhole attack needs two or more such malicious nodes to perform wormhole attack successfully needed that these nodes have larger resources than other nodes.

2 SECURITY IN WIRELESS SENSOR NETWORK

2.1 Security Requirements

Computer security deals with prevention, detection and survivability of attacks. As sensor networks are commonly deployed in unattended environments, it is common to focus on the survivability of attacks, that is, coping with some attack and still function normally. Several properties could be demanded to a secure protocol, according to the specific application. The major security requirements ones are listed below.

- **Confidentiality or privacy** is defined as the prevention of unauthorized access to information. A violation of the confidentiality results in information disclosure.
- **Integrity** is defined as the prevention of unauthorized, either accidental or malicious, modification or destruction of information. Data modification or

deletion would result in deceiving the authorized entity by providing him with false information.

- **Authentication** – Entity authentication is defined as the process of verifying an entity's claimed identity, while data origin authentication is defined as the process of verifying the originator of the data, which implies data integrity.
- **Availability** – Availability refers to the percentage of time a system is working and available to the user. In the context of a sensor network it refers to the ability to collect data from the sensors. It is not directly security requirement, nevertheless as an adversary can mount different attacks to interfere with the normal functionality of the sensor network, we consider it as part of the security requirements.
- **Data freshness** – An adversary should not be able to reuse old authentic messages

3 REVIEW OF WORK

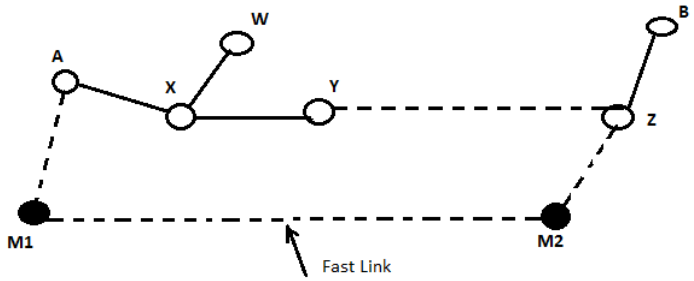
There exist a number of solution for the detection of wormhole attacks and the misbehaving node in the network. Some of the solutions uses either a specified hardware or minor changes in the protocol and provides smart method of detection of wormhole attack. Due to use of a specified hardware in the network which results in required extra processing of data, additional cost and a battery life of a sensor node. In this section we deals with some of the solutions available for wormhole attack detection. Hu et al. [3] proposed a method to detect the wormhole attack using geographical and temporal packet leaches. The disadvantage of this methodology do not support global positioning system and time synchronization. Lazos et al. [4] describe the scenario where few of the sensor nodes are reserved by the global positioning locators and some of them uses directional antennas. The proposed scheme supports locally broadcasting of keys to transmit the data to the other node. Krawczyk et al. [17] proposed a transmission based route setup to identify the attacks by observing the transmission time among the sensor node. Which helps to reduce the cost of the detection of wormhole attack. Poovendran et al. [6] describe 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. Some of the methodology deals with traffic flow analysis using statistical analysis and anomaly based detection scheme. Wenliang Du, et al. describe an anomaly detection scheme named LAD [11] which helps in the deployment of the sensor nodes by estimates the location from its observation. In [11] Awerbuch *et. al.*, a acknowledgement is required form all of the data packets by its receiving nodes. Due do the limited number of missed data packet which leads to poor quality in an investigation. By limiting the number of missed data packets, the route with poor quality will result in an investigation. The existence of wormhole attack could be justify only after the degradation has been detected and the process will repeated further to go over from beginning. L. Buttyan et al [9] have describe a wormhole attack discovery

mechanism which is based on statistical analysis method for finding multipath routing. By observing the link which is created by wormhole attack and helps in routing and it is selected and requested with its frequency. That's help to integrate this method with intrusion detection system. The disadvantage of this protocol is that it will be only works with on-demand protocol.

4 PROPOSED METHODOLOGY

4.1 Outline of Proposed Approach

Definition of Wormhole Attack: Node A wants to traverse towards node B. The node B broadcast the RREQ message which is firstly received by the node x and M1. In this scenario the attacker node may be in hidden to the network and X replies with RREQ to its nearest neighbor node as W and A. Now the malicious node M1 and M2 creates a fast link with the help of node A and Y, Z. Hence the node Z broadcast the RREQ message to the node B. In this scenario the node A wants to transmit the data from A to node B, but due to the fast link created between M1 and M2 it pretends to be the shortest path and the malicious route is selected which is A->M1->M2->Z->B. Which results in terms of the delay and packet drop in the network. And node M1 and M2 now modify the packets which violets the properties of CIA trade.



Proposed System: The system is used to detect the wormhole attack and to secure the wireless sensor network from packet drop, delay, modifying packets, adversaries misdirecting the multi-hop routing, we designed a trust based energy efficient framework for detection of wormhole attack in wireless sensor network.

Advantages of Proposed System:

- Relies on routing not on the specialized hardware.
- Proposed methodology provides detection of wormhole attack in less time.
- Easily identify the suspected node or attacker node.
- Calculate the energy level of each node in real time using energy watcher module.
- Also calculate the trustworthiness of each node.
- Message Passing nodes and reply message nodes are identified with the help of trust manager.
- Which improves the overall performance of the wireless sensor network.

5 DESIGN AND ARCHITECTURE

In this chapter we will discuss the architecture of proposed system, to detect the wormhole attack in wireless sensor network to secure the network from packet drop, delay, modifying packets, adversaries misdirecting the multi-hop routing. Wireless Sensor Networks offers protection against identify the deception through replaying routing information. An Adversary can exploit this defect to lunch the harmful or even devastating attacks against the routing protocols including wormhole attack. The key feature of this proposed methodology is based on observation of the behaviour of each node in a network. The routing agent module is responsible for route calculation. The route calculation is done on the basis of shortest path to the sink node. The energy watcher module monitor the energy level of each and every node by which packet is transmitted. The routing table and energy level of nodes, data is forwarded to trust agent module. The trust agent module calculate the trust level of each node on the basis of information provided by the routing agent and energy watcher module. If the calculated trust level or value of a particular node is less than appropriate value i.e 0.9 to 0.99. Then the suspected node is identifies as replying the messages and wormhole attack is detected.

5.1 Flow Chart of Simulation

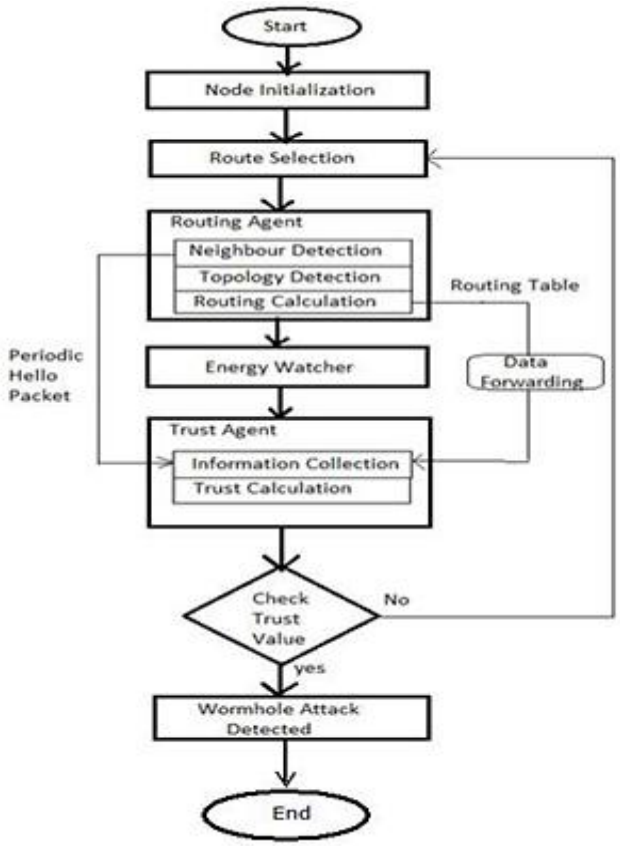


Fig. 5.1. Simulation of Flow Chart

5.2 The proposed methodology consist of different modules as describe below

- **Node Initialization:** Node initialization process is used to deploy the sensor nodes by deploying the sensor nodes and base stations.

- **Route Selection:** For a Trust based energy Efficient Framework node N transmit the data packet form a base station to other nodes. By using the localization method the node N observe the neighboring node position and forwards the data packets by considering the trust level and the energy level of node.

- **Routing Agent:** Routing agent module is consist of three modules which are as follows neighbour detection, topology detection and routing calculation. The neighbour detection sub module uses neighbour selection algorithm for forwarding the data packets to the next-hop. And from next-hop i.e. node N will forward the data packet to the base station. The Topology detection module is used to identify, which topology is used for data packet transfer from one node to next-hop. The routing calculation module is responsible for the finding the shortest path between a node N and next-hop.

- **Energy Watcher:** We uses an energy watcher module to monitor the energy level of each node in network. By monitoring the energy level of nodes we further calculate that node has enough capability to forward a data packet from one node to the other nodes.

- **Trust Manager:** We adopted a trust manager module that is responsible for calculating the trust of each node on the basis of routing information, neighbour behaviour and energy level of nodes. The trust module computes the trust of each entity and assign to another entity. Hence more trust level is identifies as more trustworthiness. The trust to the neighbouring node N by the node x, and it is given by the following.

$$T_x(y) = \sum_{i=1}^{n} [W_x(i) * T_x(i)]$$

Where $W_x(i)$ is the weight of the ith trust category to x and $T_x(i)$ is the situational trust of x in the ith trust category.

From the above equation, we can get the following equations:

$$C_h = \frac{Hs - Hf}{Hs + Hf} \text{ for } Hs + Hf \neq 0 \text{ else } C_h = 0$$

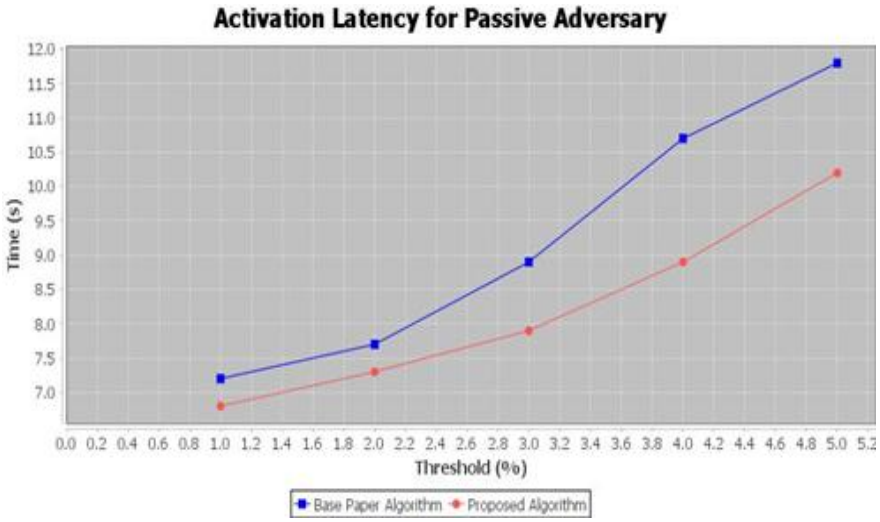
$$C_d = \frac{Ds - Df}{Ds + Df} \text{ for } Ds + Df \neq 0 \text{ else } C_d = 0$$

Hence a value of -1 represents complete distrust, a value of 0 implies non-contributing event and a value of +1 means absolute trust in a particular event. Especially the trust level of the neighbour is N's estimation of the probability that this neighbour correctly delivers data received to the base station.

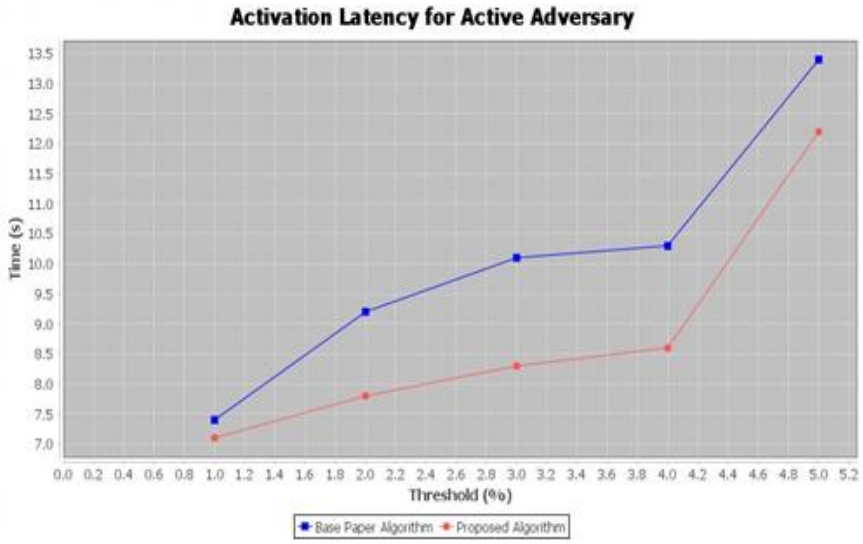
6 RESULT AND DISCUSSION

The paper presents an efficient methodology for wormhole attack detection in wireless sensor network. The proposed methodology uses energy watcher and trust manager to calculate the performance

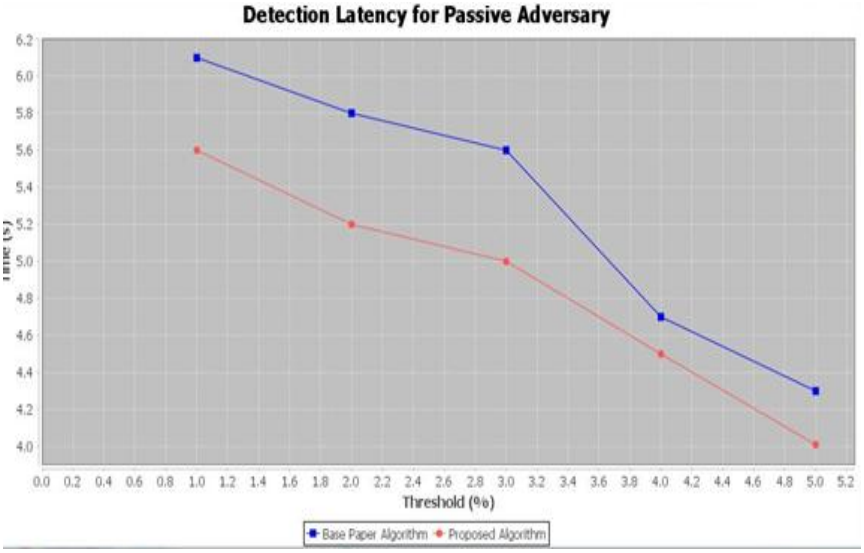
- **Activation Latency for Passive Adversary:** The performance of efficient wormhole attack detection is calculated by plotting the graph between threshold value and time to estimate the activation latency for passive adversary.



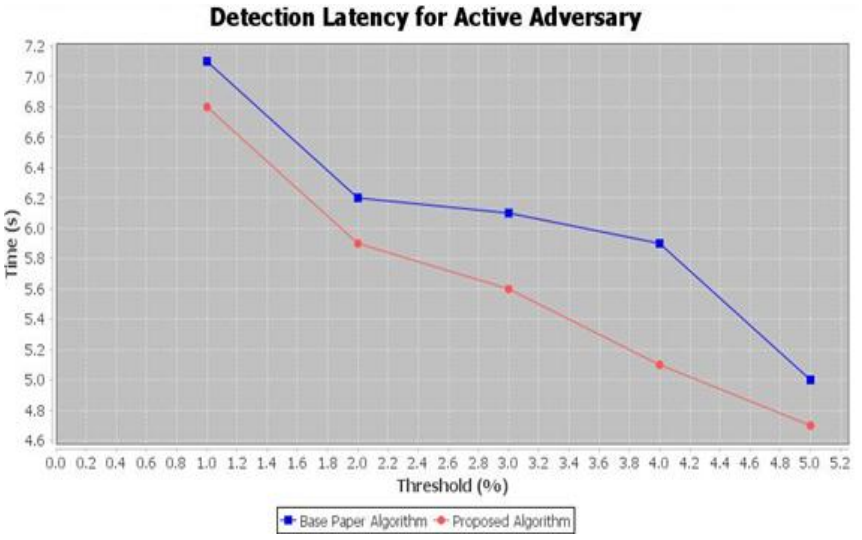
- **Activation Latency for Active Adversary:** The performance of efficient wormhole attack detection is calculated by plotting the graph between threshold value and time to estimate the activation latency for active adversary.
-



- **Detection Latency for Passive Adversary:** The performance of efficient wormhole attack detection is calculated by plotting the graph between threshold value and time to estimate the detection latency for passive adversary.



- **Detection Latency for Active Adversary:** The performance of efficient wormhole attack detection is calculated by plotting the graph between threshold value and time to estimate the detection latency for passive adversary.
-



7 CONCLUSION AND FUTURE WORK

WSN carry maximum number of misbehaving nodes which transfer the data from one system to another system without making use of any wires., The Lifetime of the network

is Limited because All these depends on energy of particular node in the network. The detection of wormhole attack is much faster which is proposed in this paper because of uses of energy watcher and trust manager. The energy watcher module keep the record of energy level of each node and trust manager keeps the behavior of each node in the network.

Future work, several improvements can be allowed and could start to a further minimize in power consumption and taking the more time of simulation. It also include exploration of other matrices and mobility of the nodes.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankara subramaniam, and E. Cayirci. "Wireless sensor networks: a survey". Computer Networks, 38(4):393–422, 2002.

[2] Y.-C. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in *Proc. IEEE INFOCOM*, 2003, vol. 3, pp. 1976–1986.

[3] Bhaskar Krishnamachari, Deborah Estrin, and Stephen B. Wicker. "The impact of data aggregation in wireless sensor networks". In Proc. of IEEE ICDCSW, pages 575–578, Washington, DC, USA, 2002. IEEE Computer Society.

[4] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," presented at the NDSS, 2004.

[5] J. Eriksson, S. V. Krishnamurthy, and M. Faloutsos, "Truelink: A practical countermeasure to the wormhole attack in wireless networks," in *Proc. IEEE ICNP*, 2006, pp. 75–84.

[6] R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," *Wireless Netw.*, vol. 13, pp. 27–59, 2007

[7] S. Capkun, L. Buttyan, and J.-P. Hubaux, "Sector: Secure tracking of node encounters in multihop wireless networks," in *Proc. ACM SASN*, 2003, pp. 21–32.

[8] I. Khalil, S. Bagchi, and N. B. Shroff, "Mobiworp: Mitigation of the wormhole attack in mobile multihop wireless networks," in *Proc. IEEE SecureComm*, 2006, pp. 1–12

[9] L. Buttyan, L. Dora, and I. Vajda, "Statistical wormhole detection in sensor networks," in *Proc. IEEE ESAS*, 2005, pp. 128–141

[10] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromisetolerant security mechanisms for wireless sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 247–260, Feb. 2006.

[11] W. Du, L. Fang and P. Ning, "LAD: Localization anomaly detection for wireless sensor networks," Journal of Parallel and Distributed Computing, vol. 66(7), 2006, pp. 874~886.

[12] Khin Sandar Win, Pathein Gyi, "Analysis of Detecting Wormhole Attack in Wireless Networks," Proceedings Of World Academy Of Science Engineering And Technology Volume 36 December 2008.

[13] H. Chan, A. Perrig, and D. Song, "Random key pre-distribution schemes for sensor networks," in IEEE Symposium on Research in Security and Privacy, 2003, pp. 197–213.

[14] S.Marti,T.J.Giuli,K.Lai and M.Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. the Sixth annual ACM/IEEE International Conference on Mobile Computing and Networking, 2000, pp. 255-265.

[15] Y. Hu, A. Perrig and D. B. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks," Technical Report TR01-384, Rice University Department of Computer Science, Dec. 2001.

[16] V. Loscri, G. Morabito, and S. Marano, "A Two-Level Hierarchy for Low Energy Adaptive Clustering Hierarchy", DEIS Department, University of Calabria.

[17] H. Krawczyk, R. Canetti, and M. Bellare, "HMAC: keyed hashing for message authentication," Tech. Rep. RFC 2104, Internet Society, Reston, Va, USA, 1997.

[18] X. Long and Z. Jian, "Improved leach cluster head multi-hops algorithm in wireless sensor networks," in International Symposium on Distributed Computing and Applications to Business Engineering and Science, Aug. 2010, pp. 263–267.

[19] Lee, H.S., K.T. Kim, and H.Y. Youn, "A New Cluster Head Selection Scheme for Long Lifetime of Wireless Sensor Networks," ICCSA, 2006. 3983