International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-1 Issue-8 March-2013

Research on Qualitative Analysis of LEACH with Wormhole attack in Wireless Sensor Network

Priya Maidamwar[1] and Nekita Chavhan[2]
Wireless Communication & Computing, Department of Computer Science & Engineering,
G H. Raisoni College of Engineering, Nagpur, India

Abstract

Wireless Sensor Networks are real time distributed systems often deployed in adhoc fashion with self-configuring capability along with ability to connect wirelessly at extremely low cost, makes WSN a promising technology for wide range of applications. Routing is a major issue in development of Wireless sensor network. Due to resource constrained nature, sensor networks are vulnerable to harmful attacks including Sink hole, Wormhole, Sybil attacks which affects the performance of various routing protocols. In this paper, primary focus has been made to analyze the network performance of LEACH with wormhole attack. Emphasis is made to propose and develop a scheme for detection of wormhole attack from intermediate and surrounding threats.

Keywords

LEACH protocol, Security, Wireless Sensor Network, Wormhole attack.

1. Introduction

Sensor networks refers to a heterogeneous system consisting of multiple detection stations called sensor nodes with a communications infrastructure intended to monitor and record conditions at diverse locations. Sensor nodes are small, lightweight and portable devices equipped with a transducer, microcomputer, transceiver, and power source. The transducer produces electrical signals based on the sensed physical phenomena. The microcomputer processes and stores the sensed information. The transceiver receives instructions from the base station/central computing system and sends data to it. Each sensor nodes derives its energy usually from a battery or any other embedded form of energy harvesting [1].
Essential features of Wireless Sensor Networks are as follows:

- Limited power supply.
- Fault tolerant nature.
- Heterogeneity of nodes.
- Large scale deployment.
- Mobility of nodes.
- Communication failures.
- Dynamic network topology.
- Deployment in hostile environment.

Size and cost constraints result in corresponding constraints on energy, memory, computational speed and communications bandwidth. Also sensor networks are responsible for sensing and transmission of data. Since large amount of data is to be processed with limited number of sensor nodes, data transmission is critical and challenging task. Hence routing protocols for such kind of networks should be designed by considering these limitations in mind. Due to inherent resource constraint nature of Wireless sensor network, these networks are vulnerable to various kinds of attacks [2].

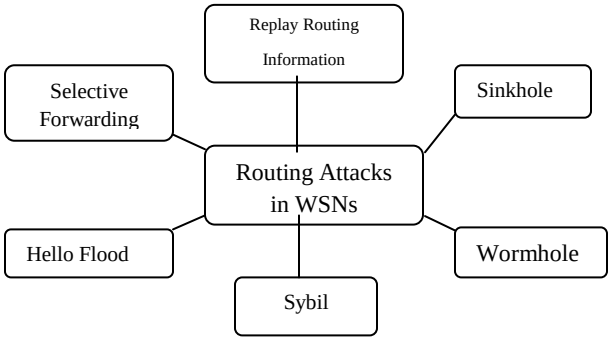

Figure 1: Classification of Routing Attacks

Wormhole attack is a specific attack on sensor routing protocols where two or more malicious nodes receive packets at one point of the network and transmit them to another location by a wired or wireless tunnel. Depending upon the how protocol selects next hop for packet forwarding, routing in wireless sensor networks can be classified as flat-based routing, hierarchical-based routing, and location-based routing.

- In flat-based routing, same functionality or role is exhibited by all the nodes in the topology.

- In hierarchical-based routing, virtual tree is formed by nodes. Nodes are assigned different roles or functionalities according to the hierarchy. Sensor nodes forwards the data to node placed in higher hierarchy than sender. This node is an aggregator which further forwards data to base station.
- In location-based routing, path to route the data from source to destination is decided according to the sensor nodes position in the field.

In our study, we analyze performance of wormhole attack on LEACH protocol. Low Energy Adaptive Clustering Hierarchy (LEACH) is an energy efficient hierarchical-based routing protocol.

Here primary attempt is made on the analysis of LEACH based upon certain parameters like throughput, delay, packet delivery ratio and also the effect of Wormhole attack on LEACH protocol.

Thus, the proposed paper is organized into 6 sections. Section 2 introduces the background of sensor networks; section 3 describes significance of wormhole attacks in sensor networks; section 4 presents proposed scheme. Section 5 describes the scope of study and section 6 followed by conclusion.

2. Background

Security is a major issue in all forms of communication networks, but wireless sensor networks face the greatest challenge due to their inherent nature and multihop routing. As a result they are susceptible to wide range of malicious attacks. In this section we give brief overview of LEACH (Low Energy Adaptive Clustering Hierarchy) routing protocol.

Description of routing protocol: Leach

Heinzelman introduced a hierarchical clustering algorithm for sensor networks, called Low Energy Adaptive Clustering Hierarchy (LEACH). LEACH divides the network into small clusters and determines one of them as the cluster-head. A primary goal for WSN is to use energy efficiently. Clustering algorithm ensures optimal energy utilization as compared with non-clustering routing algorithms. Node first senses its destination and then transmits the relevant information to its cluster-head. Later the cluster head performs data aggregation and compresses the information received from all the nodes and sends it to the base station. Low Energy Adaptive Clustering Hierarchy (LEACH) is the first adaptive cluster-based routing protocol for wireless sensor network whose implementation process includes many rounds. Remaining nodes are cluster members of this protocol. The operation of LEACH is divided into rounds; each round consists of two phases: the set-up phase and the steady state phase.

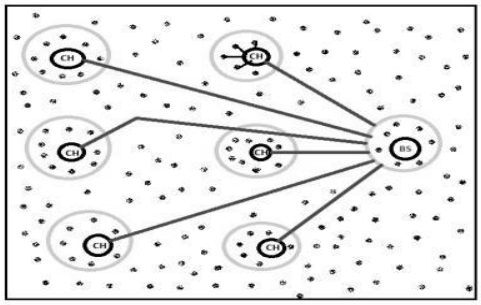

Figure 2: Cluster formation by sensor nodes [3]

In the set-up phase, the clusters are organized and cluster-heads are elected. In the steady state phase, the transmission and reception of data to the BS takes place in reality. The length of time taken by steady state phase is longer than the time taken by the set-up phase in order to reduce overhead. During the set-up phase, a fraction of predetermined nodes, *p* elects themselves as cluster-heads as described follows.

A sensor node selects a random number, *r*, between 0 and 1. According to this, node becomes a cluster-head for the current round, if this random number is less than a threshold value T(n). The threshold value is measured based on an equation that incorporates the desired percentage to become a cluster-head denoted as p, the current round denoted as r, and the set of nodes denoted as *G* that have not been selected as a cluster-head in the last (1/P) rounds. It is calculated as:

$$T(n) = \frac{p}{1 - p\left(r \bmod \left(\frac{1}{p}\right)\right)} \quad \text{if } n \in G$$

All elected cluster-heads broadcast its identity to the rest of the nodes in the network that they are the new cluster-heads. After receiving this advertisement, all the non-cluster-head nodes decide on the cluster to which they want to join depending on the signal strength of the advertisement.

The non-cluster-head nodes sends join-REQ message to cluster-heads that they will be a member of the

cluster. Upon receiving all the join-REQ information, it creates a TDMA schedule, and informs all the member nodes in the cluster. After a member node receives the schedule, it transmits data in its own time slots, and goes to sleep state in other slots.

During the steady-state phase, cluster-head, upon receiving entire data, aggregates it and sends it to the base station. Hence in this phase sensor nodes can begin actual transmission of data to the cluster-heads.

After an interval of time, the network goes back into the set-up phase again and enters another round of selecting new cluster-heads. Each cluster, in order to reduce interference from nodes belonging to other clusters communicates using different CDMA codes [3].

3. Significance of Wormhole Attack

Scarcity of various resources makes wireless sensor network vulnerable to several kinds of security attacks. Adversary possessing sufficiently huge amount of memory space, power supply, processing abilities and capacity for high power radio transmission, results in generation of several malicious attacks in the network [4].

Wormhole attack is a type of Denial of Service attack that misleads routing operations even without the knowledge of the encryptions methods unlike other passive and active attacks. This vulnerability enables it to identify and to defend against it.

Wormhole attack is a specific attack on Wireless sensor network routing where two or more attackers are connected by high speed off-channel link called wormhole link.

Wormhole attacks can be distinguished in two different modes, namely 'hidden' and 'exposed' mode, depending on whether attackers put their identity into packet headers when tunneling and replaying packets.

In wormhole attack, a pair of attackers forms 'tunnel' to transfer the data packets and replays them within the network. This attack has a powerful effect on wireless security systems, network routing and clustering protocols. Routing mechanisms can be disrupted and confused when routing control messages are tunneled. The tunnel formed between the two colluding attackers is referred as wormhole [5].

Figure 1 shows the wormhole attack. Packets received by node X is replayed through node Y and vice versa.
Normally it take several hops for a packet to traverse from a location near X to a location near Y, packets transmitted near X travelling through the wormhole will arrive at Y before packets travelling through multiple hops in the network.
The attacker can imitate A and B that they are neighbors' by forwarding data packets, and then selectively drops the packets to disrupt communication between A and B.

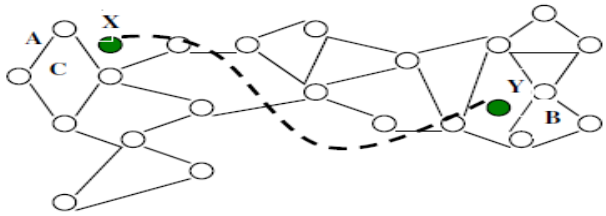

Figure 3: Wormhole tunnel formation [5]

Several Researchers have worked on detection and prevention of wormhole attacks in Wireless Sensor Networks. In this section important wormhole attack detection mechanisms are described.

Table 1: Summary of Wormhole Attacks Detection Mechanism

Methods	**Requirements**	**Comments**
Temporal Packet Leashes by Hu, Perrig and Johnson[6]	Tightly synchronized clocks	Required time synchronization level and currently not achievable in sensor networks
Geographical Packet Leashes[7]	GPS coordinates of every node; Loosely synchronized clocks (ms)	Robust, straightforward solution; inherits general limitations of GPS technology
Statistical Analysis by Song et al[8]	Requires statistical routing information from each sensor node.	Works only with multi-path on-demand protocols; Easy integration with intrusion detection system

Directional Antennas by Hu and vans[7]	Nodes use specific 'sectors' of their antennas to communicate with each other; Directional antennas on all nodes.	It cannot be directly applied to other networks. Provides good solutions for networks employing directional antennas,
Network Visualization(MDS-VOW) by Wang and Bhargava[6]	Requires central coordination	Works best on dense networks; Mobility is not studied
Graph theoretic model by Lazos and Poovendran[8]	Requires a combination of location information and cryptography	Uses location aware guard nodes equipped with GPS receivers
Travelling time mechanism by Tran et al.[9]	Does not require any special supporting hardware	Measures Round Trip Time of a message and its acknowledgement
Multipath Hop-count Analysis by Shang, Laih and Kuo[9]	No hardware requirement	Scheme has high efficiency and very good performance with low overhead
Trust Based Model by Jain and Jain[10]	No hardware requirements	Effectively locate dependable routes through the network

4. Proposed Scheme

LEACH protocol is difficult to attack as compared to the other conventional multi-hop protocols. In the conventional multi-hop protocols, the nodes around the base station are more attractive to compromise. Whereas in LEACH, the CHs are the only node that directly communicate with the base station. However, clusters in LEACH are formed dynamically (at random) and periodically, which changes interactions among the nodes and requires that any node needs to be ready to join any CH at any time. The location of these CHs can be anywhere in the network irrespective of the base station. And more over the CHs are varying periodically. So determining the position of these CHs is extremely difficult for the adversary. However, since it is a cluster-based hierarchical routing protocol, relying primarily on the CHs for data aggregation and data transmission, attacks involving CHs severely affects the network performance. If any adversary nodes become a CH, then it can facilitate attacks like Wormhole attack, Sybil attack, selective forwarding and HELLO flood attack. The adversary can thereby send powerful advertisement to all the nodes in the network and hence because of strong signal strength, every node is likely to choose the adversary as the cluster-head. Thereafter adversary can selectively forward information to the base-station or modify or dump it.

In order to overcome these loopholes the proposed scheme focuses on the work to analyze and simulate all possibilities of wormhole attacks behaviors in respect of recent scenario that further needs to design an algorithm and protocol architecture for wormhole attack prevention.

One way to prevent wormhole attack, as used by Tran et al., Jane Zhen and Sampalli [6], is to measure RTT of a message and its acknowledgement. Round trip time (RTT) measurement is also referred to as Message travelling time information. The RTT is the time that extends from the Route Request (RREQ) message sending time of a source node to Route Reply (RREP) message receiving time from a destination node.

Consider Node A as source and Node B as destination RTT between A and all its neighbors is measured by Node A. Since the RTT between two fake neighbors is higher than between two real neighbors, both the fake and real neighbors can be identified easily by node A. In this mechanism, each node computes the RTT between itself and all its neighbors.

Wireless Sensor Networks (WSN) is an active research area in today's computer science and telecommunication. The development of clustered sensor networks has recently been shown to decrease system delay, save energy while performing data aggregation and increase system throughput. These are strong motivational points behind selecting LEACH as the baseline protocol for the analytical study. LEACH protocol uses limited energy thus increases the network lifetime.

The objective of selecting this work is to have very vast opportunities to detect and prevent a wormhole attack and to predict all possible simulations. So, an effective technique for indentifying an end to end connection among various nodes of sensor networks is to be proposed to eliminate possible hazards.

The following figure elaborates the work process of proposed scheme. The operation of LEACH protocol starts with collection of network parameters (number of packets, packet size, link layer type, Mac type ,

queue length, packet type) as an input. Further the threshold is computed for selection of cluster-heads which changes for every round. CH broadcasts advertisements, other nodes joins to CHs depending on signal strength. To detect wormhole RTT is calculated between all nodes.

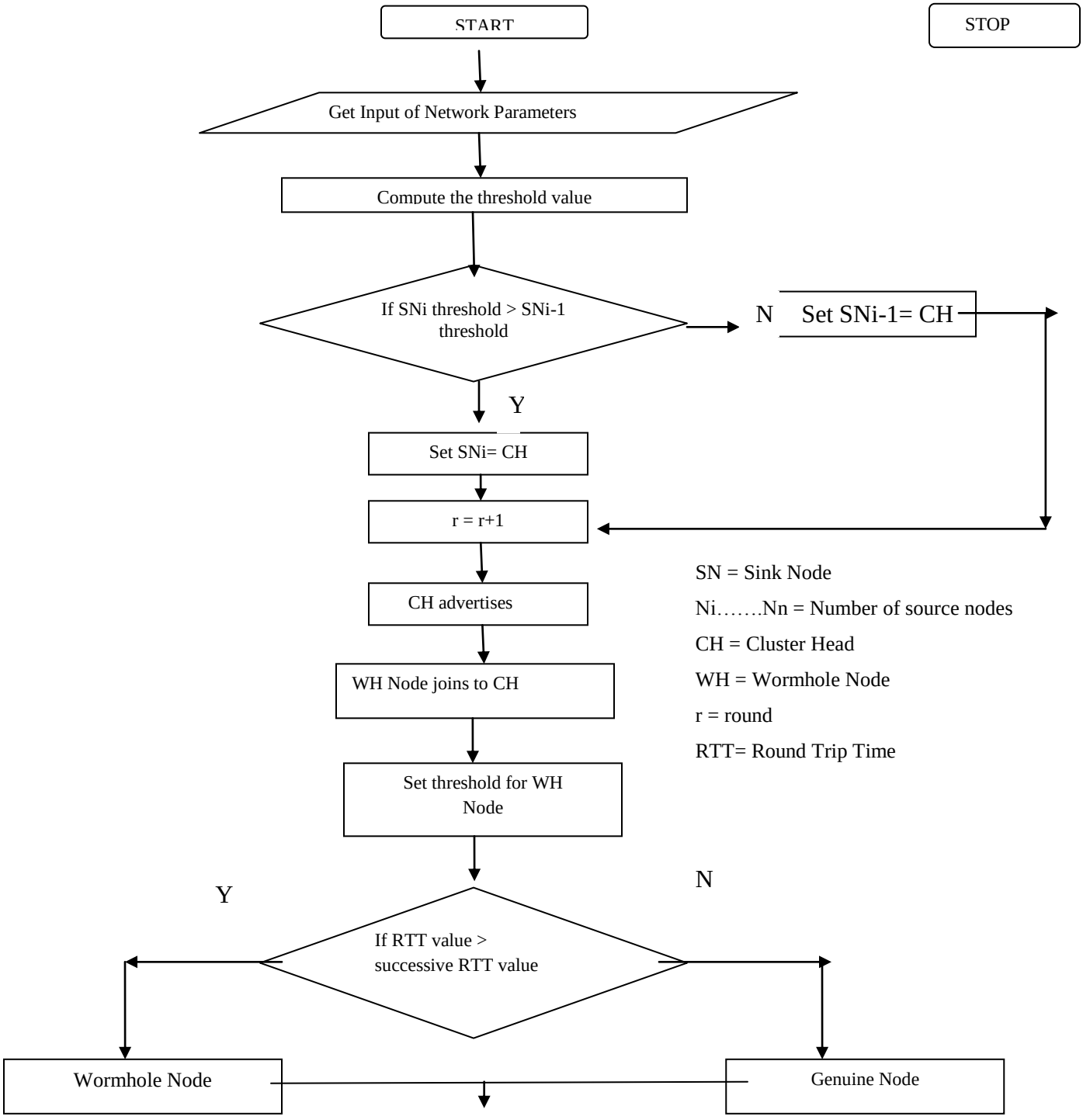

Figure 4: - Work Flow

5. Scope of Work

The scope of this work is intended to reduce the possibilities of wormhole attacks in wireless sensor network. The proposed scheme may assist to design new paradigm for sensor routing protocols in better and faster way. The proposed work after simulations will give various results to actuate the problem of wormhole attacks and clear cut analysis of its occurrence and to motivate the existing protocols to update.

6. Conclusion

In this work the technique of end to end detection of wormhole attacks is emphasized. This proposal may change their evolutionary direction in hierarchical routing protocols in wireless sensor networks. This challenging opportunity of studying and simulating wormhole attacks may give relevant outcomes and this simulation based on the wormhole detection and identification of the source node that may select a shortest route from a set of legitimate routes. This may eliminate the existence of wormhole and their occurrence in WSNs.

References

[1] Ali Modirkhazeni, Norafida Ithnin, Mohammadjavad Abbasi, "Secure Hierarchal Routing Protocols in Wireless Sensor Networks: Security Survey Analysis", IJCCN International Journal of Computer Communications and Networks, Volume 2, Issue 1, February 2012.

[2] Sushma, Deepak Nandal, Vikas Nandal, "Security Threats in Wireless Sensor Networks", IJCSMS International Journal of Computer Science & Management Studies, Vol. 11, Issue 01, May 2011.

[3] M.Shankar, Dr.M.Sridar, Dr.M.Rajan, "Performance Evaluation of LEACH Protocol in Wireless Network", International Journal of Scientific & Engineering Research, Volume 3, Issue 1, January-2012.

[4] G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security Vol. 4, No. 1 & 2, 2009.

[5] Rama Krishna Challa ,Mani Arora, Divya Bansal, "Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", IEEE Second International Conference on Computer and Network Technology, pp 102-104, 2010.

[6] 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.

[7] Khin Sandar Win, "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology 24, 2008.

[8] Dhara Buch, Devesh Jinwala, "Prevention of wormhole attack in Wireless sensor network", International Journal of Network Security & Its Applications (IJNSA), pp 85-98, Vol.3, No.5, Sep 2011.

[9] 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.

[10] Prasannajit B, Venkatesh, Anupama S, Vindhykumari, "An Approach towards Detection of Wormhole Attack in Sensor Networks", IEEE First International Conference on Integrated Intelligent Computing, pp 283-289, 2010.

Priya Maidamwar received the B.E. degree from K.D.K College of Engineering, Nagpur, and State-Maharashtra, India. She is pursuing Master of Engineering (M.E.) in Wireless Communication and Computing from G. H. Raisoni College of Engineering, Nagpur. Maharashtra, India. Her research area includes Wireless network security, Wireless sensor network.

Nekita Chavhan received the Master of Engineering (M.E.) in Wireless Communication and Computing from G. H. Raisoni College of Engineering, Nagpur, and State Maharashtra, India. She is working as Assistant Professor in G. H. Raisoni College of Engineering, Nagpur. Her research area includes Ad-hoc Wireless networks, Wireless sensor networks and Mobile Technology.