ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

Comparison of LEACH protocol with Wormhole Attack and without Wormhole Attack in Wireless Sensor Networks

Dr.M.Pushpavalli[1], P.Mahalakshmi[2]

Assistant Professor (Sr.G), Dept. of ECE, Bannari Amman Institute of Technology, Sathy, Tamilnadu, India [1]

PG Student, Dept. of ECE, Bannari Amman Institute of Technology, Sathy, Tamilnadu, India [2]

ABSTRACT: In Wireless Sensor Networks, routing is the major concern. It comprises of small sensor nodes with limited resources. It is necessary to introduce a routing protocol to extend network life time and to reduce the power consumption in sensor nodes. LEACH is one of the most interested techniques that offer an efficient way to minimize the power consumption in sensor networks. It uses self organizing and dynamic cluster formation which makes it attractive to various routing attacks, such as Denial of Service (DoS), Black hole, Wormhole and Sybil attacks. Wormhole attack is a Denial of Service attack launched by malicious nodes. It records packets at one location and tunnels them into another location. To check the reliable operation of LEACH, implement wormhole attack and evaluated the LEACH protocol in terms of metrics like throughput, average end-to-end delay, Packet Delivery Ratio (PDR). The evaluation of LEACH with wormhole attack has been done with the help of NS2 simulator. Watchdog is a monitoring technique which detects the misbehaving nodes in the network. It can be implemented in LEACH. In Watchdog-LEACH, some nodes are considered as watchdogs and some changes are applied on LEACH protocol for intrusion detection. Watchdog-LEACH is able to protect against a wide range of attacks and it provides security, energy efficiency and memory efficiency. Comparison made on LEACH with wormhole attack and LEACH with watchdog shows that LEACH with watchdog achieves high throughput, Packet Delivery Ratio and low End to End Delay.

KEYWORDS: LEACH Protocol, NS2, Watchdog, Wireless Sensor Network (WSN), Wormhole Attack.

I. INTRODUCTION

Wireless sensor network (WSN) is composed of large number of small sized, inexpensive and computable sensors, which are limited in power, memory, and computation. Normally, large numbers of tiny sensors are deployed randomly to monitor one or more phenomena, to collect and process the sensed data and to send the data back to the sink. The important applications of WSN include environmental monitoring, personal healthcare, military applications, etc. Sometime the sensitive data is communicated to the destination node through an insecure medium. Thus, WSN can be easily attacked by Denial-of-Service (DoS) attacks, which cause information loss along with large energy expenditure.
Cluster-based communication protocols have been proposed for Adhoc networks in general and sensor networks in particular for various reasons including scalability and energy efficiency. In cluster-based networks, nodes are organized into clusters; with cluster heads (CHs) that they relay messages from ordinary nodes in the cluster to the Base Stations (BS). LEACH is a clustering-based protocol that minimizes energy dissipation in sensor networks. The purpose of LEACH is to select sensor nodes randomly as cluster heads. The operation of LEACH is separated into two phases: the set-up phase and the steady phase. The duration of the steady phase is longer than the duration of the set-up phase in order to minimize the overhead. During the set-up phase, a sensor node n chooses a random number between 0 and 1. If this random number is less than a predetermined threshold, t, the sensor node becomes a cluster head. After a node is self-selected as a cluster head, it advertises this to all its neighbors. The sensor nodes inform their cluster head that they will be a member of the cluster, and then the cluster head assigns a time slot for every sensor node in which they can send data to the cluster head. During the steady phase, the sensor nodes can begin sensing and transmitting data to the cluster heads. The cluster heads also aggregate data from the nodes in their cluster before sending them to the base station.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

Wormhole tunnel is created by any two malicious nodes (generally at distant location) which collude together to create an illusion that they are just one hop away and thereby routing the packets to them as neighbor nodes. As soon as wormhole entities create the tunnel successfully, they can drop the packets, replay, tampers the packets or selectively forward them. The organization of paper is as follows: (i) introduce the LEACH routing protocol, (ii) wormhole attack is launched in LEACH, (iii) simulation of wormhole attack in LEACH, (iv) simulation of watchdog in LEACH and (v) its result analysis.

II. LITERATURE SURVEY

A. Routing protocols in WSN : Wireless Sensor network protocols can be classified into four categories. They are Location-based Protocols, Data-centric Protocols, Hierarchical Protocols and QoS-based protocols. MECN (Minimum Energy Communication Network), SMECN (Small Minimum Energy Communication Network), GAF (Geographic Adaptive Fidelity), GEAR (Geographic Energy Aware Routing) are the protocols comes under Location based protocols. SPIN, Directed Diffusion, Energy-aware Routing, Information-Directed Routing are the protocols comes under Data Centric protocols. LEACH (Low Energy Adaptive Clustering Hierarchy), PEGASIS (Power Efficient Gathering System Information System), HEED are comes under Hierarchical protocols. SAR (Sequential Assignment Routing), SPEED, Energy-aware routing comes under QoS based protocols.

B.Routing protocols for different Applications : Wireless sensor network protocols can be categorized for different applications. SPAN, GAF are the protocols used for Habitat Monitoring. LEACH, GBR, SAR, SPEED are the protocols used for Health applications. GAF can be used for Military applications. APTEEN, GEAR used for Home/Office applications.

C. Different Types of Attacks in Different Layers: In Application layer, Repudiation and Data corruption attacks will occur. Session hijacking, flooding are the attacks comes under Transport layer. Worm hole, Black hole, Byzantine, flooding, resource consumption are the attacks comes under Network layer. Traffic analysis comes under Data link layer. Jamming, interceptions, eavesdropping comes under Physical layer.

III. NETWORK MODEL OF LEACH

LEACH: Low Energy Adaptive Clustering Hierarchy.
All the nodes in the network have the same initial energy and have ability to communicate with the base station.

- The position of the base station is far away from the wireless sensor network area
- The nodes within the network are changing their position and hence movable
- All sensor nodes are able to control their transmit power to change the communication range

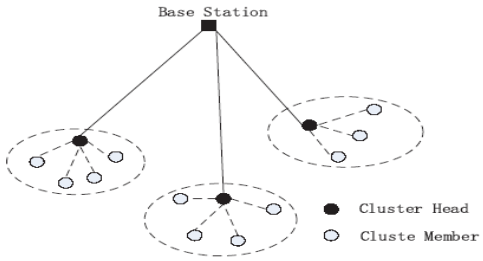

Fig. 1 Network Model of LEACH

IV. WORMHOLE ATTACK IN LEACH ROUTING PROTOCOL

Wormhole attack is a network layer attack launched by malicious nodes by creating a high speed tunnel through which packets are replayed to malicious nodes disrupting the communication channel and corrupting the routing process.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

Wormhole attack is launched in LEACH routing protocol. The malicious nodes create a high speed tunnel, thereby causing RREQ to reach the destination at a faster rate compared to usual path. According to LEACH protocol, destination discards all the later RREP packets received, even though they are from authenticated node. The destination then chooses the false wormhole tunnel infected path to send the RREP causing the inclusion of wormhole tunnel in the data flow route. The tunnel can be created in one of the four ways: packet encapsulation, creation of out of band link using specialized hardware channel, packet relay approach and usage of high power transmission.

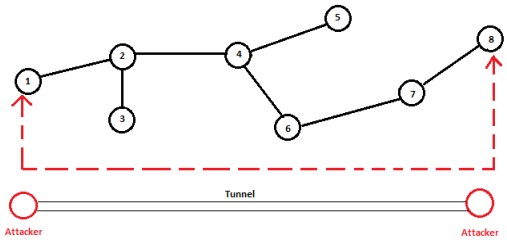

Fig. 2 Wormhole Tunnel

V. WATCHDOG IN LEACH

Watchdog is one of the techniques in Intrusion Detection System (IDS). It monitors misbehavior node. Once anomalies are detected it sends an alert message to Base Station, before the intruder starts to attack. It first recognizes the normal behavior of nodes and compared it with detected behavior and it can report what type of attack it is.
In Watchdog-LEACH, Spontaneous Watchdog approach is added before steady phase. Intrusion Detection method is added in setup and steady phase for Intrusion Detection.

A. Watchdog-LEACH Phases

Setup Phase

It's like LEACH setup phase as it is described in Introduction section.

Selecting Watchdog nodes

For selecting watchdog nodes Spontaneous Watchdogs approach is used. Each node has a monitoring module that is activated upon selecting as a watchdog node. This monitoring module must be in charge of analyzing packets that their neighbors in a cluster send and receive. Maybe they receive some packets from other clusters but they ignore signals from other clusters. Other sensors also can generate some alerts depends on the situation so their monitoring module can be started to work in some situations like attacks against the physical or logical safety of sensor but they don't check other nodes communications.

Due to the broadcast nature of communications, every watchdog node will receive all packets sent inside its cluster. A single node will select itself as a watchdog for a cluster with a probability of 1/n.
If a node has been selected as a CH in previous phase, it's not selected as a watchdog in a cluster. There isn't any extra energy consumption overhead for the decision of being a watchdog node as we assume that the result has been calculated before and has been embedded to the sensors.

Watchdog nodes are independent from CHs so they also monitor CHs behavior. During Steady phase, watchdog nodes listen to communications and when they detect an attack they send alarm to BS directly. In Watchdog-Leach Decentralized Intrusion Detection approach is used for detecting attacks and sending report to BS. After each round, Black listed nodes are reported to all nodes so after that, other nodes will ignore messages from black listed nodes and they will not be selected as CH in next rounds.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

VI. RESULTS AND DISCUSSIONS

Software used	:	NS2
Operating system	:	Fedora
Protocol	:	LEACH
Number of sensor nodes	:	37
Network Area	:	500x500
Number of Cluster Heads	:	4
Initial Energy of a node	:	200 J
Simulation time	:	30s

Objective: To verify the operation of LEACH protocol, Wormhole attack can be implemented. After implementing Wormhole attack, LEACH protocol without Wormhole attack and with Wormhole attack is compared in terms of throughput, PDR and delay.

To monitor the misbehaving node in a network, watchdog mechanism can be implemented. After implementing watchdog, LEACH with wormhole attack and LEACH with watchdog will be compared.

A. Scenario of Sensor nodes

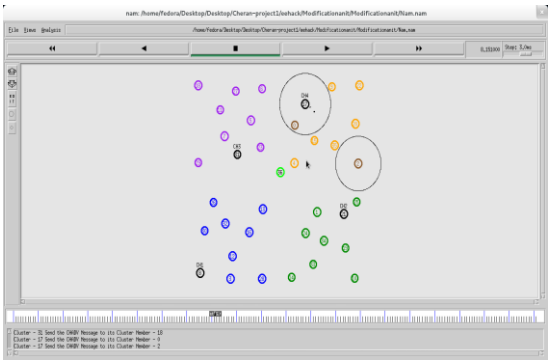

Fig. 3 Cluster formation in LEACH

In Fig.3 cluster head can be formed randomly in LEACH protocol. Cluster head can be selected by considering maximum energy level of node.

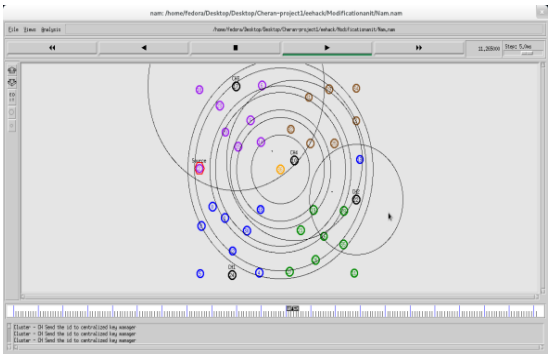

Fig. 4 Packet flow between sensor nodes
(LEACH without wormhole)

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

In Fig.4 packets or data can be flow between sensor nodes. Node in one cluster can communicate with node in another cluster by cluster heads only.

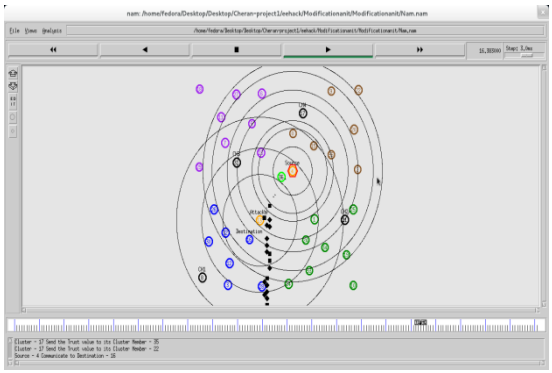

Fig. 5 Wormhole Attack in a network
(LEACH with wormhole)

In Fig.5 wormhole attack is implemented in the network. Packet lost occur in the network due to the attacker.

B. Throughput

It is the number of bits successfully received through a network in a second. It is measured in bits per second. It measures how fast data can pass through.

Fig. 6 LEACH Throughput with and without Wormhole

In Fig 6 LEACH protocol without wormhole attack achieves high throughput when compared to LEACH protocol with wormhole attack.

C. End to End Delay

It indicates difference between the time at which the sender generated the packet and the time at which receiver received the packet.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

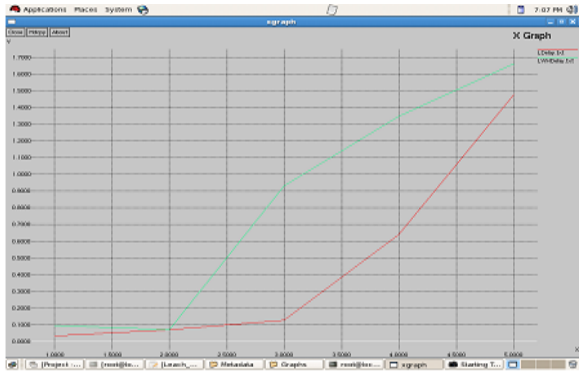

Fig. 7 LEACH Delay with and without Wormhole

In Fig 7 LEACH protocol without wormhole attack achieves low end to end delay when compared to LEACH protocol with wormhole attack.

D. Packet Delivery Ratio

It is the rate of successfully delivering the data packets to the sink. It is denoted as PDR = (D/S)*100, Where D is the number of packets received by the destination and S the number of packets sent by the source node.

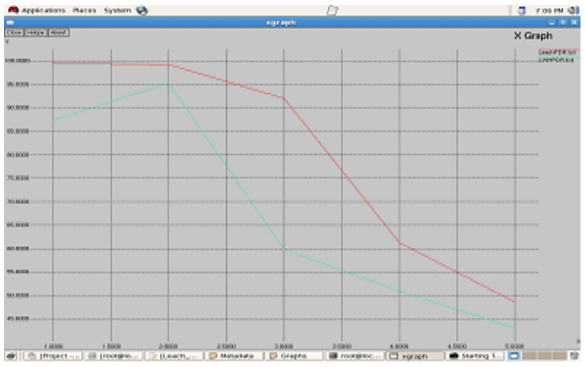

Fig. 8 Leach Packet Delivery Ratio with and Without Wormhole

In Fig 8 Packet Delivery Ratio in LEACH protocol without wormhole attack is high when compared to LEACH protocol with wormhole attack.

VII. FUTURE WORK

The extension of this project is to implement Watchdog mechanism in the network to monitor misbehaving nodes. After monitoring misbehaving nodes, the route between source and destination will be changed. Attacker node will be discarded. So, throughput and PDR will be achieved high and low end to end delay will be achieved. Then, LEACH with wormhole and LEACH with watchdog will be compared.

VIII. CONCLUSION

LEACH protocol can be used for health applications in the Wireless Sensor Network. This project considers Wormhole attack under network layer attack. By implementing wormhole attack in the sensor network - LEACH protocol,

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

throughput and Packet Delivery Ratio (PDR) will be low and end to end delay increases. So, watchdog mechanism can be included to monitor the attacker in the network and to eliminate them. The route between source and destination can be changed to achieve high throughput and PDR. Also, this project aims to reduce the delay while watchdog mechanism will be implemented in the network. Finally, compare the LEACH protocol with Wormhole attack and LEACH protocol with Watchdog mechanism. The result shows that LEACH protocol with Watchdog achieves high throughput and PDR, low end to end delay.

REFERENCES

[1]Bishan Ying, "CUSUM-Based Intrusion Detection Mechanism for Wireless Sensor Networks", Journal of Electrical and Computer Engineering, Volume 2014, Article ID 245938.
[2] Priya Maidamwar & Nekita Chavhan, "Impact of wormhole attack on performance of LEACH in wireless sensor networks", International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC) ISSN 2250-1568 Vol. 3, Issue 3, Aug 2013, 21-32 © TJPRC Pvt. Ltd.
[3] Dr. A. Francis Saviour Devaraj, Vandana C.P, "Evaluation of Impact of Wormhole Attack on AODV", International Journal of Advanced Networking and Applications, Volume: 04 Issue: 04 pp: 1652-1656, 2013.
[4] Soojin Lee, Yunho Lee and Sang-Guun Yoo, "A Specification based Intrusion Detection Mechanism for LEACH Protocol", Information Technology Journal 11(1): 40-48, 2012.
[5] Mohammad Reza Rohbanian, Mohammad Rafi Khan, Alireza Keshavarz-Haddad and Manije Keshtgary, "Watchdog-LEACH: A new method based on LEACH protocol to Secure Clustered Wireless Sensor Networks".
[6]LiTian,HuaichangDu,YanweiHuang, "The Simulation and Analysis of LEACH Protocol for Wireless Sensor Network Based on NS2", IEEE International Conference on System Science and Engineering, pp 530-533 June 30-July 2, 2012.
[7] Lu Jianyin, "Simulation of Improved Routing Protocols LEACH of Wireless Sensor Network", IEEE 7th International Conference on Computer Science & Education (ICCSE), pp 662-666, July 14-17, 2012.
[8] Shio Kumar Singh, M P Singh and D K Singh, "Routing Protocols in Wireless Sensor Networks –A Survey", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010.
[9] TEODOR-GRIGORE LUPU, "Main Types of Attacks in Wireless Sensor Networks", Recent Advances in Signals and Systems.