INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

A Review on Scheme of Leach with Homomorphic Encryption

[1]NEHA CHHABRA,[2]PRIKSHIT SINGLA

Deptt. Of Computer Science & Engineering
DVIET, Karnal
neha11chhabra@gmail.com[1], par7901@gmail.com[2]

Abstract: *Security is always a main task to be performed in any network. Wireless Sensor Network are different from other networks.Hierarchical Routing Protocol are the best energy saving and efficient routing protocol in wireless sensor networks. Our Objective is to Provide End to End Confidentiality in LEACH and Performance measurement of leach protocol for various homomorphic encryptions. Leach is a very secure Protocol as cluster head changes in each round but sometimes data needs to be very confidential of some nodes to Base station. So the best technique used for providing this is Homomorphic Encryption.Our Objective is to apply Multiplicative Homomorphic Encryption in LEACH.So that need of decrypting data at cluster head is removed.*

Keywords: *Leach, Security in leach, Homomorphic encryption*

1. INTRODUCTION

With the furtherance of computer networks extending boundaries and joining distant locations, wireless sensor networks (WSN) emerged as the new frontier in developing opportunities in order to collect and process data from remote locations. A wireless sensor network is a collection of nodes organized in a cooperative manner. Multiple sensor nodes arranged in proximity to sense an event and subsequently transmit sensed and collected information to a remote processing unit or base station. The nodes are able to communicate wirelessly and often self-organize after being deployed in an ad hoc fashion. More than 1000s or even 10,000 nodes are expected. Currently, wireless sensor networks are beginning to be extended at an accelerated pace. It is not unreasonable to expect that in 10-15 years that the world will be covered with wireless sensor networks with access to them via the Internet. This can be considered as the Internet becoming a physical network. This new technology is exciting with unlimited potential for numerous application areas including environmental, medical, military, transportation, entertainment, crisis management, homeland defense, and smart spaces.

Compared with the traditional wireless networks, wireless sensor networks have energy constraints, low-data-rate of high redundant and data flow of high-to-one, and so on. Energy effectiveness is the key performance indicators of wireless sensor networks. Based on the analysis of energy management strategy in the wireless sensor networks, the main factors affecting energy consumption are: perceptual data, data processing and radio communications, the radio communication is the main part of energy consumption.

Wireless sensor networks (WSN) are generally set up for gathering records from insecure environment. Nearly all security protocols for WSN believe that the opponent can achieve entirely control over a sensor node by way of direct physical access. The appearance of sensor networks as one of the main technology in the future has posed various challenges to researchers. Wireless sensor networks are composed of large number of tiny sensor nodes, running separately, and in various cases, with none access to renewable energy resources.

In addition, security being fundamental to the acceptance and employ of sensor networks for numerous applications; also different set of challenges in sensor networks are existed. The security of wireless sensor networks is ever more important nowadays. Most of the proposed security

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

protocols in wireless sensor networks are based on authentication and encryption. But all of them only address part of the problem of security in wireless sensor networks. Recently, the use of reputation and trust systems has become an important secure mechanism in wireless sensor networks

Realization of these and other sensor network applications require wireless ad hoc networking techniques. Although many protocols and algorithms have been proposed for traditional wireless ad hoc networks, they are not well suited for the unique features and application requirements of sensor networks.
To illustrate this point, the differences between sensor networks and ad hoc networks are outlined below:

• Sensor nodes are densely deployed.
• Sensor nodes are prone to failures.
• The topology of a sensor network changes very frequently.
• Sensor nodes mainly use broadcast communication paradigm whereas most ad hoc networks are based on point-to-point communications.
• Sensor nodes are limited in power, computational capacities, and memory.
• Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.

2. LEACH

LEACH stand for Low-Energy Adaptive Clustering Hierarchy and it was one of the first hierarchical protocols. In this the sensor nodes will be unionizing themselves into clusters in which one of the node act as the cluster head. Leach uses rotation of cluster heads to evenly distribute the energy load among the sensors in the network. Here, not only the cluster heads have the responsibility of collecting data from their clusters, but also to aggregate the collected data for reducing the amount of messages to be sent to the BS due to which there is less energy dissipation and network life time is enhanced. The operation of LEACH is done into two phases,

- Setup phase.
- Steady State phase.

During the set-up phase, when clusters are being created, each node determines whether or not to become a cluster head for the current round. This decision is based on a predetermined fraction of nodes and the threshold T (n). The threshold is given by:

$$T(n) = \begin{cases} \frac{P}{1-P*\left(rmod\ \frac{1}{P}\right)} & \text{if } n \in G \\ 0 & \text{Otherwise} \end{cases}$$

where p denotes the predetermined percentage of cluster heads (e.g., p = 0.05), r denotes the current round, and G denotes the set of nodes that have not been cluster heads in the last 1/p rounds. Using this threshold, each node will be a cluster head at some round within 1/p rounds. After 1/p rounds, all nodes are once again eligible to become cluster heads.

In LEACH, the optimal number of cluster heads is estimated to be about 5% of the total number of nodes. Each node that has elected itself a cluster head for the current round broadcasts an advertisement message to the rest of the nodes in the network. After receiving this advertisement message all the non cluster head nodes agree on the cluster to which they will belong for this round. This agreement is based on the received signal strength of the advertisement messages. After cluster head receives all the messages from the nodes that would like to be included in the cluster and based on the number of nodes in the cluster, the cluster head creates a TDMA schedule and assigns each node a time slot when it can transmit.

During the steady-state phase, the sensor nodes can begin sensing and transmitting data to cluster heads. The radio of each non cluster head node can be turned off for the duration of node's allocated transmission time. The cluster heads, after accepting all the data, unify it before sending it to the sink. Each cluster head communicates using different CDMA codes in order to reduce interference from nodes belonging to other clusters.

2.1 DRAWBACKS IN LEACH

- LEACH uses single-hop routing where each node can transmit directly to the cluster-head and the sink. Therefore, it cannot be applied to networks deployed in large regions.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

- The idea of dynamic clustering leads to extra overhead, e.g. head changes, advertisements etc., which may decrease the gain in energy consumption.
- Random election of CH, hence there may be chances that all CHs will be concentrated in same area.
- The protocol assumes that all nodes begin with the same amount of energy capacity in each election round, expecting that being a CH consumes approximately the same amount of energy for each node.

2.2 SECURITY IN LEACH

Like most routing protocols for WSNs, LEACH is vulnerable to a number of security attacks including jamming, spoofing, replay, etc. However being a cluster based protocol; we rely completely on the CHs for the task of data aggregation and routing. Therefore attacks which involve CHs will be detrimental. If an intruder manages to become a CH, it can cause attacks such as sinkhole and selective forwarding, thus disrupting the workings of the network. The intruder may also try to inject bogus data into the network without effecting the routing. A third type of attack is (passive) eavesdropping.

Adding security to LEACH-like protocols is challenging, as its dynamic and periodic rearranging of the network's clustering (and changing links) makes Key distribution solutions that provide long-lasting node-to-node trust relationships (to be sure, provided by most existing solutions) inadequate. There are a number of KD schemes in the security literature, most of which are ill-suited to WSNs: public key based distribution, because of its processing requirements; global keying, because of its security vulnerabilities; complete pair wise keying, because of its memory requirements; and those based on a key distribution centre, because of its inefficiency and energy consumption.

Attacks to WSNs may come from outsiders or insiders. In cryptographically protected networks, outsiders do not possess credentials (e.g., keys or certificates) to show that they are members of the network, whereas insiders do. Insiders may not always be trustworthy, as they may have been compromised. Data authentication (it should be possible for a recipient of a message to authenticate its originator), and data freshness (it should be possible for a recipient of a message to be sure that the message is not a replay of an old message) can be provided by using SPINS, a suite of lightweight security primitives for WSN.

3. HOMOMORPHIC ENCRYPTION

A homomorphic encryption scheme allows arithmetic operations on cipher texts, multiplicatively homomorphic scheme, where the decryption of the efficient manipulation of two cipher texts yields the multiplication of the two corresponding plaintexts. Homomorphic encryption schemes are particularly useful whenever some party not having the decryption key(s) needs to perform arithmetic operations on a set of cipher texts. A more formal description of homomorphic encryptions schemes is as follows.

The encryption function we use is

$$C = X + k \pmod M$$

and the decryption function is

$$X = C - k \pmod M$$

Where X € [o..M---1] is the node's sensor reading, k is a secret key, $M = nb_{nodes} * max_{value,}$ where nb_{nodes} represents the number of nodes in the network and max_{value} is the maximum possible value for the nodes' readings.
In cluster head mode, a node gathers data from the other nodes within its cluster, performs data fusion, and routes the data to the base station through other cluster head nodes.

4. SECURITY CHALLENGES

The aim of security principles in WSNs is to secure the information and resources from attacks and misbehavior. The primary security requirements in WSNs include:

- **A**vailability, which gives assurance that the desired network services are available even in the presence of denial-of-service attacks.
- **C**onfidentiality, provides sureity that a given message cannot be understood by anyone other than the desired recipients.
- **I**ntegrity, which gurantees that a message sent from one node to another is not modified by malicious intermediate nodes.
- **A**uthorization, which ascertain that only authorized sensors can be involved in providing information to network services.

Authentication, which verify that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

- **N**onrepudiation, which controls that a node cannot deny sending a message it has previously sent.

5. CONCLUSION AND FUTURE SCOPE

The security Challenges in WSNs are usually focused on cryptography. However, due to the constraints in WSNs, many already existing secure algorithms are not practical. We discuss this problem in our work and my goal will be to achieve the End to End ***C****onfidentiality* of sensing nodes and Base station.

REFERENCES

[1] "A Survey of security issues in Wireless Sensor Networks" Yong Wang ,Garhan Attebury and Byrav Ramamurthy .IEEE Communication Survey 2006.

[2] "Routing Protocols in Wireless Sensor Networks" Luis Javier García Villalba , Ana Lucila Sandoval Orozco, Alicia Triviño Cabrera and Cláudia Jacy Barenco Abbas,2009.

[3] "A survey on routing protocols for wireless sensor networks" Kemal Akkaya , Mohamed Younis July 2003; accepted 1 September 2003.

[4] "A Review of Power Efficient Hierarchical Routing Protocols in Wireless Sensor Networks" Sanjay Wawarn, Dr. Nisha Sarwade , Pallavi Gangurde ,2012.

[5] "Secure routing in wireless sensor networks: Attacks and countermeasures" C. Karlof and D. Wagner 2003 ,IEEE International Workshop on Sensor Network.

[6] "SecLEACH – A Random Key Distribution Solution for Securing Clustered Sensor Networks" Leonardo B. Oliveira, Hao C. Wong, M. Bern 2006.

[7] "Efficient and Provably Secure Aggregation of Encrypted Data in Wireless Sensor Networks" Claude Castelluccia , Einar Mykletun ,2009.

[8] "On the Security of Cluster-based Communication Protocols for Wireless Sensor Networks" Adrian Carlos Ferreira1, Marcos Aur´elio Vila¸ca1, Leonardo B. 2005.