MOBILE ELEMENTS DATA INTEGRATION AND ENHANCING SECURITY WITH LEACH PROTOCOL USING WSN

Pooja Mehta[1]

Abstract

A wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions. It Provide a bridge between the real physical and virtual worlds. wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. To enhance the security of sensor nodes, the data transmitted must be encrypted among sensor nodes In this paper we applied Data Encryption Standard scheme to add security to LEACH protocol. The objective of this paper is to add secret encryption scheme to the LEACH protocol.

Keywords— Wireless Sensor Network, LEACH, DES, BS, Applications

Introduction

Wireless sensor networks are a group of specialized devices or sensors which are used to monitor different environmental conditions and to collect and organize that data at some certain central location. It detects and measures a number of physical conditions such as humidity, temperature, sound, pressure, speed and direction, chemical concentrations, vibrations, pollutant levels and many other such conditions. It has many applications of WSNs are available in number of directions which includes environmental applications, medical monitoring, security for homes, surveillance, inventory management industrial and manufacturing automation, process control, distributed robotics, etc.

There are a number of nodes in a sensor network, these nodes are the detection stations and they are very small and portable. There is a sensor/transducer, microcontroller, transceiver and power source in every sensor node. The transducer senses the physical condition and if there is any change then it generates electrical signals. These signals go to the microcomputer for processing. A central computer sends commands to the transceiver and data is then transmitted to that computer. In recent years, wireless sensor network (WSN) has achieved a great attention of the researchers. The network comprises of number of sensor nodes which are deployed according to required application.

[1] Asst. Professor , MCA Department, Y.M.T College of Management, Kharghar, pooja@ymtcollegeofmanagement.org

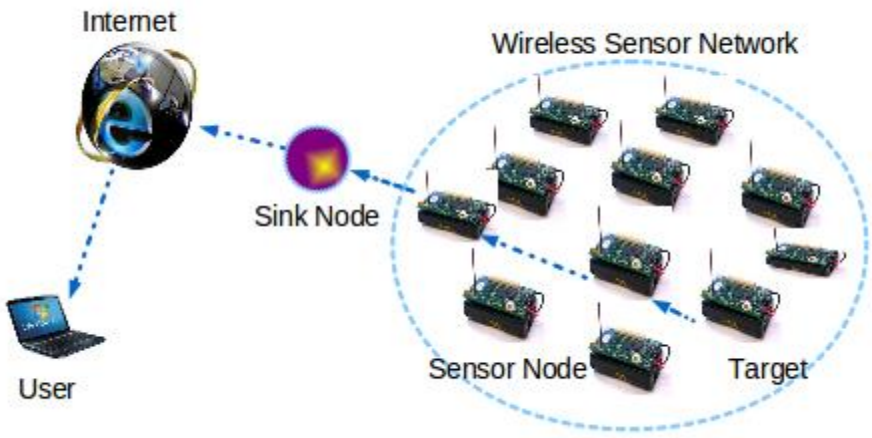

Figure 1: Structure of WSN

Characteristics of WSN:

The main characteristics of a WSN are

- Scalability to large scale of deployment
- Power consumption constrains for nodes using batteries or energy harvesting
- Mobility of nodes
- Dynamic network topology Communication failures
- Ability to withstand harsh environmental conditions

Wireless Sensor Networks With Mobile Elements

To better understand the specific features of Wireless Sensor Networks with Mobile Elements (WSN-MEs), let us first introduce the reference network architecture, which is detailed according to the role of the MEs.

The main components of WSN-MEs are the following.

- **Regular sensor nodes** are the sources of information. Such nodes perform sensing as their main task. They may also forward or relay messages in the network, depending on the adopted communication paradigm.
- **Sinks** are the destinations of information. They collect data sensed by sensor nodes either directly or indirectly. They can use data coming from sensors autonomously or make them available to interested users through an Internet connection.
- **Special support nodes** perform a specific task, such as acting as intermediate data collectors or mobile gateways. They are neither sources nor destinations of messages, but exploit mobility to support network operation or data collection.

Depending on the specific scenario, the support nodes might be present or not. When there are only regular nodes, the resulting WSN-ME architecture is homogeneous or flat. On the other hand,

when support nodes are present the resulting WSN-ME architecture is non-homogeneous or tiered. Different from traditional WSNs, which are usually limited to be dense, WSN-MEs can also be sparse.

Types of Mobile Elements (MEs):

Mobile Elements are categorized according to increase in mobility level.

1. **Relocatable Nodes:** These are mobile nodes which change their location to better characterize the sensing area, or to forward data from the source nodes to the sink. Relocatable nodes provide a mobility-assisted approach to WSNs, in the sense that MEs are not actively exploited for data collection.

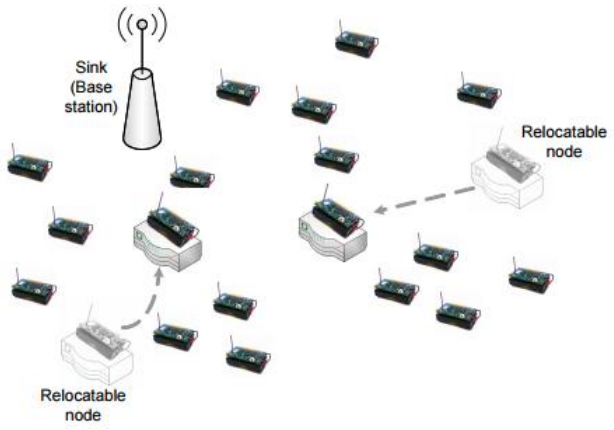

Figure 2: Architecture of a WSN-ME with relocatable nodes

2. **Mobile Data Collectors (MDCs):** These are mobile elements which visit the network to collect data generated from source nodes. Depending on the way they manage the collected data, MDCs can be either mobile sinks or mobile relays.

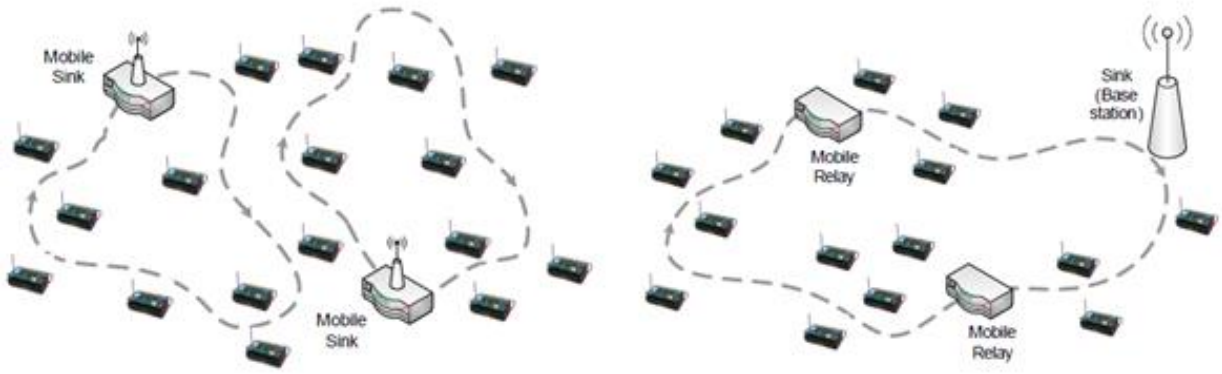

Figure 3: Architecture of a WSN-ME with MDCs: (1)Mobile sinks (2) Mobile relays

3. **Mobile peers:** Unlike MDCs, which are either sinks or special relay nodes, mobile peers are ordinary mobile sensor nodes in WSN-MEs. Since they can be both originator and relays of messages in the network, their interactions are symmetrical because the sink itself might also be mobile. When a peer is in the communication range of the base station, it transfers its own data as well as those gathered from other peers while moving in the sensing area.

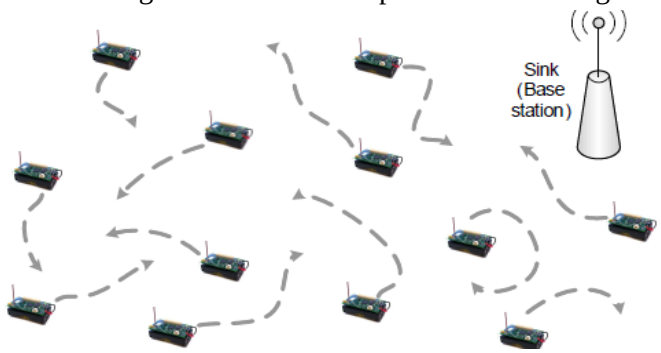

Figure 4: Architecture of a WSN-ME with mobile peers

Why Leach?

Security is one of the challenging aspects in wireless networks because it has effect on the sensors resource due to the very limited resources in the wireless sensors [6]. Mobile and ad-hoc networks employ conventional security. Due to wireless sensor limitations it is hard to employ conventional security measures on wireless sensors networks. For example, it is inefficient to employ SSL protocol. SSL protocol requires a high amount of energy which is inefficient in wireless sensor networks [7].

In wireless sensor networks, there are many applications that require a high security level. For instance, military and health care applications. Such applications require maximum security. Increasing security consumes more resources. When more resources are consumed it can negatively impact the lifespan of the network. Wireless sensors should have the maximum security with minimal power consumption to assure secure communication [8].

Security challenges in WSN:

- Wireless channels are open to everyone so anybody can monitor in communication in a wireless channel.
- Most protocols for WSN did not consider necessary security mechanism.
- implementing stronger security on sensor platform due to their complexity.
- Strong protocol costs more resources in sensor nodes which can lead to performance degradation of applications.
- Deployed in hostile environment without any fixed infrastructure.

Therefore it may face various attacks.

Issue of security in WSN Network [7]:

- Data Integrity: Data integrity in sensor networks is needed to ensure the reliability of the data. It ensures that data packets received by destination is exactly the same with transferred by the sender and any one in the middle cannot alter that packet. It is achieved by means of authentication the data content.
- Data Authentication: Data Authentication of a sensor node ensures the receiver that the data has not been modified during the transmission]. It is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys.
- Data Confidentiality: Data confidentiality of the network means that data transfer between sender and receiver will be totally secure and no third person can access it (neither read nor write). It can be achieved by using cryptography: symmetric or asymmetric key can be used to protect the data
- Data Availability: Data Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate. It should be ensured that security mechanisms imposed for data confidentiality and authentication are allowing the authorized nodes to participate in the processing of data.

Security Attacks in WSN:

Any actions that compromises the security of information owned by an organization or person is called security attack. Different types of attack are:

1. Passive attacks are the attacks in which an attacker does not actively participate in bringing the network down. A passive attacker attempts to learn or make use of information from the network. The attacker can then forward this information to an accomplice who in turn can use it to launch attacks to bring down the network.

2. Active attacks are the attacks in which an attacker actively participates in disrupting the normal operation of the network services. The attacker drops packets, modifies packets, fabricates messages or pretends to be as some other nodes.

3. Denial of Service Attacks are specific attacks that attempt to prevent legitimate users from accessing networks, servers, services or other resources. There are various kinds of DOS attacks which can cause in and decrease network life time in different ways. Some of DOS attacks are Jamming attack, Sybil attack, Sinkhole/Black hole attack, Wormhole attack, Flooding attack , Selective forwarding attack, Spoofing attack, Replay attacks.

Leach Mechanism:

When wireless sensor networks gradually go into our lives, it is of great significance to research on LEACH protocol. LEACH is the first and most popular energy efficient hierarchical clustering algorithm for WSNs that was proposed for reducing power consumption and also to increase the lifetime of the network. LEACH minimizes energy dissipation by dividing WSNs into clusters to reduce the number of messages and restrict direct communication between micro-sensor nodes and the Base Station (BS). The data aggregation can exclude a lot of redundant data to decrease the communication load on the CH node. The CH node's energy is rapidly exhausted because it has to process more work

than other nodes. In order to overcome this problem, after being the cluster head for a certain time, the CH node passes this role to another node to balance energy consumption between all nodes in the WSN. The member nodes in a cluster communicate with their CH node by single-hop, and only the CH can forward aggregative data to the BS directly. In order to avoid internal communication collisions, CH nodes use a time division multiple access (TDMA) schedule for members, and the BS categorizes the CHs with a code division multiple access (CDMA) schedule [5]. The operation of LEACH is divided into rounds; each round consists of two phases: the setup phase and the steady-state phase.

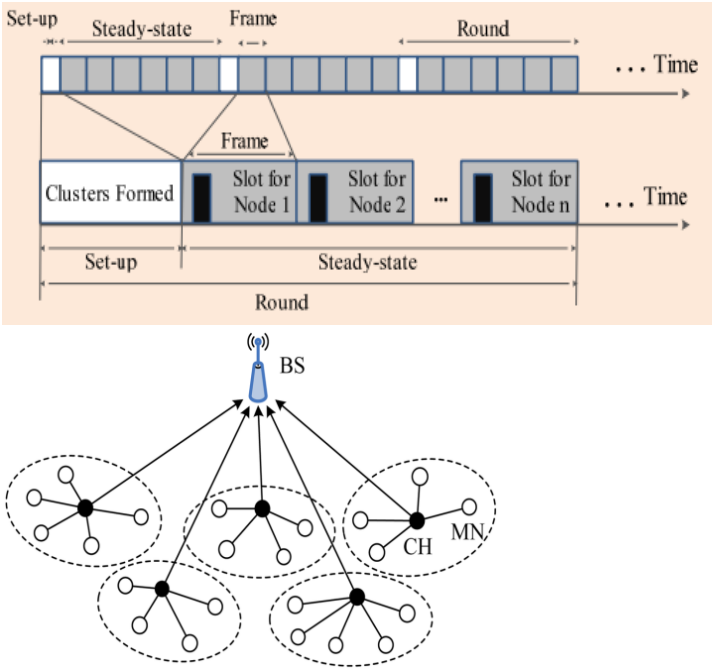

Figure 5: Two phases (set-up and Steady-state) operation in a round of LEACH

Methodology of LEACH Protocol:

Phase 1: The Setup Phase

Step 1: Cluster-head selection

During this step, each candidate node selects a random number between 0 and 1 and compares it with a calculation threshold value $P_t(n)$. If the random number is lower than the the threshold value $P_t(n)$, then that candidate node will become the CH in the current round.

$$P_t(n) = \begin{cases} \dfrac{k}{1 - k(r \bmod \frac{1}{k})} & , if\ n \in G_t(n) \\ 0 & otherwise \end{cases}$$

where k =Probability value of the candidate node that wants to become the CH

r= current round in the network

$G_t(n)$ =set of nodes

$P_t(n)$= threshold probability value for candidate node n to become a CH at round r in time t.

Step 2: Cluster formation

The non-CH nodes receive the HEAD_Adv_Msg broadcast from the CH and send join-cluster message (JOIN_Clu_Msg) to the CH for which it has the received signal strength, among other factors. The JOIN_Clu_Msg transmission contains the node's ID and the CH's ID.

Step 3: Schedule TDMA and CDMA

After the network is organized into clusters, each CH creates TDMA time slots and distributes them to each member in its cluster. Each CH also selects a CDMA code that it will use to forward sensed data to the BS.

Phase 2: The Steady-state Phase

The sensor nodes begin sensing in their areas and send data to their CH within the TDMA time slot allocated in Step 3. The CH node will receive sensed data from all members in its group, then compress or aggregate them by data fusion and transmit to the BS. The state of the network will return to Step 1 of the setup phase and a new round is started.

Advantages of LEACH:

- The selection of path and routing information is easy in LEACH so the sensor nodes don't have to keep large routing information and there is no need of complex functions.
- The CH is selected randomly so each node has an equal opportunity for being selected as CH, thus balancing the network load.
- Due to data fusion mechanism in LEACH protocol the energy consumption of data transmission is reduced by the CH, and thus the network life cycle can be extended.

Disadvantages of LEACH:

- LEACH does not take into account the residual energy of each node.
- The distribution of cluster head depends on random number, so there is a possibility that at some regions the CH are large whereas at other regions the CH may be small.

Leach Against Attacks:

Alshowkan, Elleithy, Al Hassan, proposed new Secure LEACH protocol named as LS-LEACH. It provides security measures to LEACH protocol after including the source and limitation of nodes. They provide two encryption key for security. They include Group Key between Cluster Head and Local Cluster nodes and Private Key between Cluster Head and Base Station. They also provide securing LEACH protocol against denial of services while maintaining its high performance. They also include that only the authenticated nodes are allowed to join and communicated in the network. So LS-LEACH protocol is better than other protocol in terms of system throughput, network life time and

the total energy consumption. This LS-LEACH protocol provided a secure authentication protocol for the network [1].

Simulation result:

The performance of the system was measured using the system throughput, network life time and the total energy consumption.

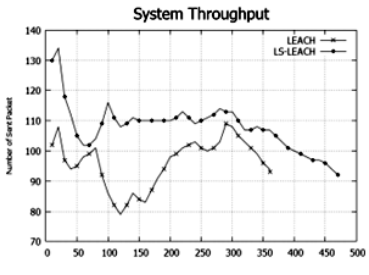

Figure 6: System Throughput

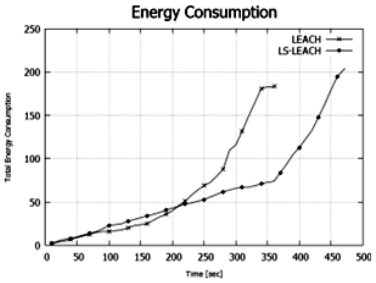

Figure 7: Energy Consumption

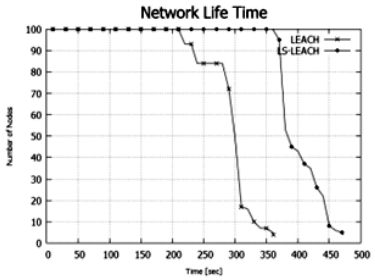

Figure 8: Network Life Time

Conclusion

LEACH has found one of the most energy efficient protocols used in WSN. LEACH protocol has been discussed with its drawbacks and how these drawbacks are overcome by its descendants. A brief study of various improved versions of LEACH protocol has been done in order to compare performance. It is concluded that for prolonging network lifetime of WSN, there is need to explore more robust, reliable and efficient protocols in future. LS-LEACH which is an improvement of LEACH protocol. After improving LEACH protocol power consumption and adding the security measures, the protocol performed better in terms of the system throughput, network life time and the total energy consumption. The proposed protocol provided a secure authentication protocol for the network from different types of attacks.

References

[1] Hemali M. Bhalodiya ,Sunera Kargathara "A Survey on Secure Hierarchical LEACH Protocol over Wireless Sensor Network"

[2] L. Jun, H. Qi, L. Yan, "A Modified LEACH algorithm in wireless sensor network based on ns2," in Proc. of International Conference on Computer Science and Information Processing, pp. 604-606, 2012

[3] J. F. Yan, Y. L. Liu, "Improved LEACH routing protocol for large scale wireless sensor networks routing," in Proc. of International Conference on Electronics, Communications and Control, pp. 3754-3757, 2011

[4] A. Somasundara, A. Ramamoorthy, and M. Srivastava, "MobileElement Scheduling for Efficient Data Collection in WirelessSensor Networks with Dynamic Deadlines," Proc. IEEE 25th Int'lReal-Time Systems Symp. (RTSS '04), 2004.

[5] S. D. Muruganthan, D. C. F. Ma, B. Rollyi, A. Fapojuwo, "A centralized energy-efficient routing protocol for wireless sensor networks," IEEE Radio Communications, vol. 43, no. 3, pp. 8-13, 2005

[6] Mayur S, Ranjith H.D,"Security Enhancment on LEACH Protocol From HELLO Flood Attack in WSN Using LDK Scheme"

[7] Muneer Alshowkan, Khaled Elleithy, Hussain AlHassan “LS-LEACH: A New Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks”

[8] H. Modares, R. Salleh, and A. Moravejosharieh, "Overview of Security Issues in Wireless Sensor Networks,"