ISSN (Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

A Secure Data Transmission for Cluster based Wireless Sensor Network Using LEACH Protocol

Vinoda B Dibbad[1], C M Parameshwarappa[2]

[1]PG Student, Dept of CS&E, STJIT, Ranebennur, Karnataka, India

[2]Professor, Dept of CS&E, STJIT, Ranebennur, Karnataka, India

ABSTRACT- Secure data transmission is a critical issue for Wireless Sensor Networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. In recent years, wireless communication due to rapid hardware cost reduction and providing its devices with portability has become one of the most important communication methods in our everyday life. Many people communicate with others through wireless environment almost every day. However, from privacy viewpoint, wireless security is a crucial challenge since messages are delivered to their destinations through the air so hackers can maliciously intercept the messages and decrypt the messages. A Clustering sensor node is an efficient topology and a crucial issue in Wireless Sensor Network (WSN). Clustering is a technique in which small light weight, low cost , low power sensor nodes are grouped in to some clusters. In this paper, propose a security solution for LEACH (Low-Energy Adaptive Clustering Hierarchy), a protocol where clusters are formed dynamically and periodically. A LEACH protocol effective one to reduce and balance the total energy consumption for CWSNs.

KEY WORDS*:* Clustering, Wireless Sensor Network, LEACH

I. INTRODUCTION

The wireless sensor network consists of small sized, light weighted, low power, inexpensive wireless nodes called sensor nodes, deployed in physical or environmental condition. And it is measured physical parameters such as sound, temperature, pressure, humidity and light. In WSNs the individual Sensor node are capable of data sensing their environments, processing the data locally, sending data to one or more collection points and aggregates the data and sends the data to the base station in a WSN [1] as shown in fig 1.The cost of data transmission is much more expensive than that of data processing. The sensor nodes have the ability to communicate either among each other or directly to a base station. Data in sensor network are bound either downstream to nodes from a sink node or upstream to a sink node from nodes. Wireless sensor network are a kind of application specified network.

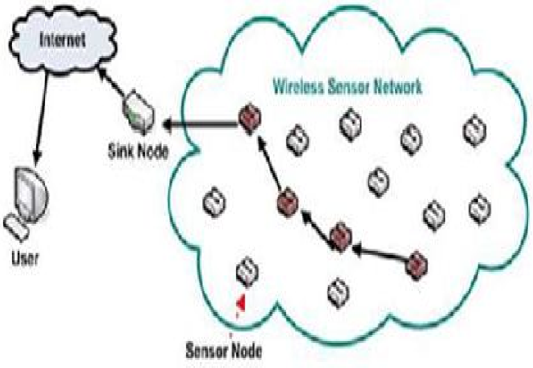

Fig 1: Wireless Sensor Network Architecture

II. RELATED WORK

In [2] authors proposed a networking together hundreds or thousands of cheap microsensor nodes allows users to accurately monitor a remote environment by intelligently combining the data from the individual nodes. These networks require robust wireless communication protocols that are energy efficient and provide low latency. They develop and analyze low-energy adaptive clustering hierarchy (LEACH), a protocol architecture for microsensor networks that combines the ideas of energy-efficient cluster-based routing and media access together with application-specific data aggregation to achieve good performance in terms of system lifetime, latency, and application-perceived quality. LEACH includes a new, distributed cluster formation technique that enables self-organization of large numbers of nodes, algorithms for adapting clusters and rotating cluster head positions to evenly distribute the energy load among all the nodes, and techniques to enable distributed signal processing to save communication resources. The results show that LEACH can improve system lifetime by an order of magnitude compared with general-purpose multihop approaches. In [3], authors have shown to increase system throughput, decrease system delay, and save energy while performing data aggregation. Whereas those with rotating cluster heads, such as LEACH have also advantages in terms of security, the dynamic nature of their communication makes most existing security solutions inadequate for them. In this paper, they investigate the problem of adding security to hierarchical (cluster-based) sensor networks where clusters are formed dynamically and periodically, such as LEACH. For this purpose, we show how random key predistribution, widely studied in the context of flat networks. In [4], authors increased interest in the potential use of wireless sensor networks (WSNs) in applications such as disaster management, combat field reconnaissance, border protection and security surveillance. Sensors in these applications are expected to be remotely deployed in large numbers and to operate autonomously in unattended environments. To support scalability, nodes are often grouped into disjoint and mostly non-overlapping clusters. In this they presented a taxonomy and general classification of published clustering schemes. They survey different clustering algorithms for WSNs; highlighting their objectives, features, complexity, etc. We also compare of these clustering algorithms based on metrics such as convergence rate, cluster stability, cluster overlapping, location awareness and support for node mobility.

III. CLUSTER NETWORK MODEL

Fig 2 shows the simple cluster Network Architecture, In Cluster Network, consist of large number of Sensor Nodes(SN) are grouped into different clusters. Each Cluster is composed of one Cluster Head(CH) sensor node which is elected autonomously and cluster member nodes or leaf(non CH). Leaf (non CH),join a cluster depending on the receiving signal strength. The Cluster Head(CH) gets the sensed data from the leaf(non CH),aggregates the sensed information and then sends it to the base station[4].

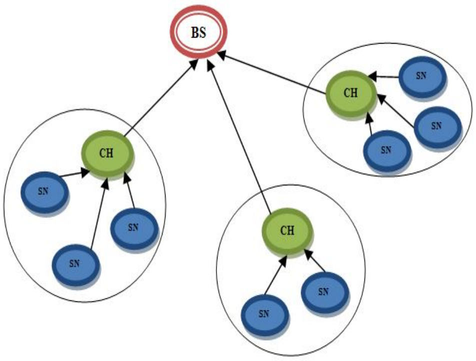

Fig 2: Simple Cluster Network Architecture

In Cluster wireless sensor networks have the following characteristics:

1. It includes two kinds of nodes:

- *Sensor nodes* with limited energy can sense their own residual energy and have the same architecture.
- *Base Station (BS)* without energy restriction is far away from the area of sensor nodes.

2. All sensor nodes use the direct transmission or multi-hop transmission to communicate with the BS.
3. Sensor nodes sense environment at a fixed rate and always have data to send to the BS.
4. Cluster head perform data aggregation and Base Station(BS) receives compressed data.
5. The lifespan of WSN is the total amount of time before the first sensor node runs out of power.
6. Some very big clusters and very small clusters may exist in the network at the same time.

IV. ADVANTAGES AND DISADVANTAGES OF DATA AGGREGATION IN WIRELESS SENSOR NETWORK

Advantages:

- Data aggregation process we can enhance the secure, robustness and accuracy of information which is obtained by entire network, certain redundancy exists in the data collected from sensor nodes thus data fusion processing is needed to reduce the redundant information.
- Another advantage is those reduces the traffic load and conserve energy of the sensor.

Disadvantages:

- The Cluster Head(CH)send fuse these data to the base station .This Cluster Head(CH) may be attacked by malicious attacker. If a cluster head is compromised, then the base station (sink) cannot be ensure the correctness of the aggregate data that has been send to it.
- In existing systems are several copies of the aggregate result may be sent to the base station (sink) by uncompromised nodes .It increase the power consumed at these nodes.

- Sensor nodes are having normal battery life and Cluster Head(CH) having high battery life time as compared with sensor nodes.

V. LEACH PROTOCOL OPERATION

Clustered WSNs were first proposed for various reasons including scalability and energy efficiency. The LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol presented by Heinzelman *et al.* [2] is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. In order to prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensor nodes in the network, in rounds. LEACH achieves improvements in terms of network lifetime. Adding security to LEACH-like protocols is challenging, because they dynamically, randomly and periodically rearrange the network's clusters and data links [3]. Therefore, providing steady long-lasting node-to-node trust relationships and common key distributions are inadequate for LEACH-like protocols. In this paper, we focus on providing efficient security to pairwise node-to-CH communications in LEACH-like protocol. Our main contribution is to have provided an efficient solution for securing pairwise communications in LEACH. We introduce the original LEACH protocol, and discuss its vulnerabilities. LEACH (Low Energy Adaptive Clustering Hierarchy) [3] was proposed to balance energy among nodes. It assumes that every node can directly reach a BS by transmitting with high enough power. However, to save energy, sensor nodes(SN) send their messages to their CHs, which then aggregate the messages, and send the aggregate to the BS. To prevent energy drainage of a restricted set of CHs, LEACH randomly rotates CHs among all nodes in the network, from time to time, thus distributing aggregation- and routing-related energy consumption among all nodes in the network. LEACH thus works in rounds. In each round, it uses a distributed algorithm to elect CHs automatically and dynamically cluster the remaining nodes around the CHs. The resulting clustering structure is used by all sensor-BS communications for the remaining of the round.

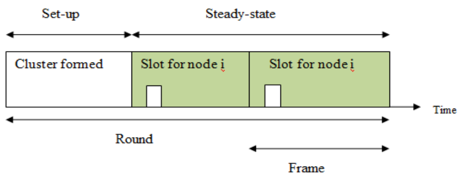

Fig 3: LEACH Protocol Operation

LEACH Protocol operates in rounds during communication Rounds and have predetermined duration as shown in fig 3, LEACH Protocol operation consist of two phases:
1. Set-up phase
2. Steady-state phase.

1. **Set-up phase**: The setup consists of three steps.

Step 1: Sensor nodes decide probabilistically whether or not to become a CH for the current round (based on its remaining energy and a globally known desired percentage of CHs). The Cluster head(CH) broadcast the message to the set of all sensor nodes in the network.

During the setup phase, a predetermined fraction of nodes p, elect themselves as CHs as follows.

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

- It is given by

$$T(n) = \frac{p}{(1-p(mod(1/p)))}$$

if n € G, where G is the set of nodes that are involved in the CH election.

Step 2 (cluster joining step): All elected CHs broadcast an advertisement message to the rest of the sensor nodes in the network that they are the new CHs. All the non-CH nodes, after receiving this advertisement, decide on the cluster to which they want to belong. This decision is based on the signal strength of the advertisement and communicate their intention to join by sending a join req(join request) message. The non-CH nodes inform the appropriate CHs that they will be a member of the cluster. After receiving all the messages from the sensor nodes that would like to be included in the cluster and based on the number of nodes in the cluster, the CH node creates a TDMA(Time Division Multiple Access) schedule and assigns each sensor node a time slot when it can transmit. This schedule is broadcast to all the nodes in the cluster. During the steady-state phase, the sensor nodes can begin sensing and transmitting data to the CHs. The CH node, after receiving all the data, aggregates it before sending it to the Base station(BS). After a certain time, which is determined a priori, the network goes back into the set-up phase again and enters another round of selecting new CHs.

Step 3 (confirmation step): It starts with the CHs broadcasting a confirmation message that includes a time slot schedule to be used by their cluster members (Sensor nodes) for communication during the steady-state phase.

2. Steady-State Phase

Once the clusters are set up, the network moves on to the steady-state phase, where actual communication between sensor nodes and the Base Station(BS) takes place.

Step 4: Each Sensor node(SN) knows when it is its turn to transmit the data to the cluster head(CH)according to the time slot schedule.

Step 5: The CHs collect messages from all their Sensor nodes (SN) or cluster members, aggregate these data, and send the result to the BS. The steady-state phase consists on multiple reporting cycles, and lasts much longer compared to the set up phase.

Table 1: LEACH Protocol Operation

Set-up Phase			
1.	CH ⇒ G_s	:	id_{CH} , adv
2.	SN → CH	:	id_{SN}, id_{CH}, join_req
3.	CH ⇒ G_s	:	id_{CH}, (... <id_{SNi} ,t_{SNi} >,…),sched)
Steady-State Phase			
4.	SN_i → CH	:	id_{SNi} , id_{CH}, d_{SNi}
5.	CH → BS	:	id_{CH}, id_{BS}, F(.. d_{SNi} ..)

Notations:

⇒ , →	: Broadcast and Unicast
SN_i, CH, BS	: A sensor node, cluster head, base station.
G_s	: The set of all nodes in the network.
Id_i	: Node i's id.
d_i	: Sensing report from node i.
$<id_i, t_i,>$	: Node i's id and time slot t_i.
Adv,join_req,sched	: Message string types which denote advertisement, join_request and schedule message
F	: Data aggregation function

VI. CONCLUSION

In this paper, we presented LEACH, a protocol for securing node-to-node communication in LEACH-based networks. LEACH bootstraps its security from random key predistribution, and can yield different performance numbers on efficiency and security depending on its various parameter values. Our estimates show that the overhead incurred by LEACH is manageable; and memory usage, energy efficiency, and security level can be each traded off for another, depending on what is most critical in a system.

VII. FUTURE WORK

Our current analysis are based on a simple three cluster model, further systematic studies of more generalized multi-cluster networks are needed. Thus far we have concentrated on the homogeneous sensor networks with a single powerful processing center (sink). In our future work, we would rather focus on the heterogeneous wireless sensor networks with multiple resource-rich actors for carrying out energy consuming tasks.

REFERENCES

[1]. T. Hara, V. I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Stud. Comput.Intell. Springer-Verlag, 2010, vol. 278.

[2]. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670,2002.

[3]. L. B. Oliveira, A. Ferreira, M. A. Vilaca *et al.*,"SecLEACH-On the security of clustered sensor networks," *Signal Process.*, vol. 87, pp. 2882–2895, 2007.

[4]. A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Comput. Commun.*, vol. 30, no. 14-15, pp. 2826–2841, 2007.

[5]. Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks Huang Lu, Student Member, IEEE, Jie Li, Senior Member, IEEE, Mohsen Guizani, Fellow, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEM YEAR, 2013.