Journal of Computer Applications ISSN: 0974 – 1925,
Volume-5, Issue EICA 2012-2, February 10, 2012

Secure Encrypted-Data Routing Protocol for Wireless Sensor Networks

Lakshmi S
M.E. Computer Science and Engineering
Kamban College of Engineering
Tiruvannamalai-606603, Tamilnadu
E-Mail:lakshmisubash04@gmail.com
Mobile: 9500757054

Ramesh P S
M.E. Computer Science and Engineering
Kamban College of Engineering
Tiruvannamalai-606603, Tamilnadu

Abstract - In sensor networks, it is crucial to design and employ energy-efficient communication protocols, since nodes are battery-powered and thus their lifetimes are limited. Such constraints combined with a typical deployment of large number of sensor nodes have posed many challenges to the design and management of sensor networks. These challenges necessitate energy-awareness at all layers of networking protocol stack. At the network layer, the main aim is to find ways for energy efficient route setup and reliable relaying of data from the sensor nodes to the sink so that the lifetime of the network is maximized. This paper presents a secure energy-efficient data routing protocol which provides both security and energy efficiency together in cluster-based wireless sensor networks.

Keywords: *communication protocols , energy efficient protocol, cluster-based network.*

I. INTRODUCTION

Advances in embedded system technologies motivate the deployment of sensor networks which consist of a large number of sensor nodes scattered over a spacious area. Each sensor node has a processor, memory, and a short range radio communication facility. These distributed sensing systems enable remote monitoring and event detection in a geographically large region or an inhospitable area. For example, in an explosion area rescuers equipped with handheld devices can be notified of the nearest survivor's location detected by sensor nodes thrown over the area.

Sensor nodes are scattered in a physically spacious are and accordingly powered by batteries instead of being tethered to durable power sources. Generally nodes are assumed to be revoked rather than replenished when they exhaust all the battery power. Previous empirical studies show that the larger portion of power is consumed by communication between nodes [2, 8, 10]. Therefore, in order to expand overall system lifetime, it is crucial to design energy efficient communication protocols for sensor networks.

We describe a three-level system model in the wireless sensor network comprising the Sensor nodes (SN), Gateway nodes (GN) and Sink as shown in Figure 1 We divide the whole network into certain clusters and each cluster comprises one GN that controls several SNs. The GNs of different cluster communicate with each other to exchange the collected data. The GNs forward the collected data to the nearby Sink and finally to the user or the controlling authority, which is located somewhere, far away from the monitoring region that accesses the sensed data and monitors the network via the Sinks. The three different level of the WSNs may be planned as given below.

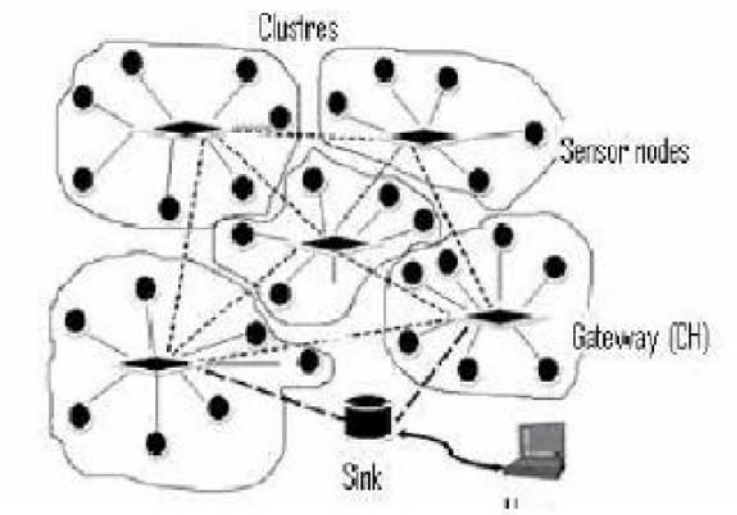

Figure 1. Three Level WSNGs Architecture

Level-1: These are the set of generic sensor nodes(SN) like Mica Motes [10] and are deployed hundreds of thousands in a specific monitoring area. The whole monitoring area is divided into certain clusters which can be formed based on cluster selection algorithms and based on the number and type of sensors for different applications Their functions are simple, specific and are usually operated independently. They sense the medium, collect the raw data and forward it to the second level.

Level-2: These are some special-purpose sensor nodes like Spec 2003 [10], limited number of which is deployed in the monitoring region. In each cluster, there exists only one cluster head and is termed as the Gateway node (GN), which can collect raw data from the SNs of its cluster. Each GN of the network has unique ID and its assignment is based on the cluster number. GNs can track events or targets using the sensors of its own cluster and prepare the nal report using data fusion and aggregation techniques and forwards the fuseddata to the third level.

Level-3: The high-bandwidth sensing and communication nodes like RSC Wins-Hidra Nodes [10] form the third level of the network and are known as the Sink of the WSGNs.

II. BACKGROUND AND MOTIVATION

Wireless Sensor Networks represent a new generation of real-time embedded systems with significantly different communication constraints. As these devices are deployed in large numbers, they will need the ability to assist each other to communicate data back to a centralized collection point. The integration of the sensor, coupled with unceasing electronic miniaturization, will make it possible to produce extremely inexpensive sensing device. Sensor nodes are tiny devices which are composed of a sensing unit, a radio, a processor and a limited battery power. These devices will be able to monitor a wide variety of ambient condition: Temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, so on. In sensor network, the energy is mainly consumed for three purposes: data transmission, signal processing, and hardware operation. It is said in [4] that 70 percent of energy consumption is due to data transmission. So for maximizing the network lifetime, the process of data transmission should be optimized. The data

transmission can be optimized by using efficient routing protocols and effective ways of data aggregation.

Routing protocols providing an optimal data transmission route from sensor nodes to sink to save energy of nodes in the network. Data aggregation plays an important role in energy conservation of sensor network. Data aggregation methods are used not only for finding an optimal path from source to destination but also to eliminate the redundancy of data, since transmitting huge volume of raw data is an energy intensive operation, and thus minimizing the number of data transmission. Also multiple sensors may sense the same phenomenon, although from different view and if this data canbe reconciled into a more meaningful form as it passes through the network, it becomes more useful to an application. Moreover when data aggregation is performing data is compress as it is passed through the network, thus occupying less bandwidth. This also reduces the amount of transmission power expended by nodes. Hence secure data aggregation can be considered as a very challenging problem in wireless sensor network.

Data routing protocols aims at eliminating redundant data transmission and thus improve the lifetime of energy constrained wireless sensor network. In wireless sensor network, data transmission took place in multi-hop fashion where each node forwards its data to the neighbor node which is nearer to sink. That neighbor node performs aggregation function and again forwards it on. But performing data forwarding and aggregation in this fashion from various sources to sink causes significant energy waste as each node in the network is involved in operation .so above approach cannot be considered as energy efficient. An improvement over the above approach would be clustering where each nodes ends data to cluster-head (CH) and then cluster-head perform routing on the received raw data and then send it to sink. Incase of homogeneous sensor network cluster-head will so on die out and again re-clustering has to be done which again cause energy consumption.

III. SYSTEM MODEL

This section describes the system model comprising the modules as cluster-based approach, selection of the cluster head for controlling the sensor nodes . It also speaks about the data routing from the sensor nodes to the sinks through the gateways using a single hop communication. In addition it touches the data redundancy elimination model.

A. Cluster Based Approach

In cluster-based approach, whole network is divided in to several clusters. Each cluster has a cluster-head which is selected among cluster members. Cluster-heads do the role of aggregator which aggregate data received from cluster members locally and then transmit the result to sink. The algorithm employs cluster heads, namely gateways, which are less energy constrained than sensors and assumed to know the location of sensor nodes.

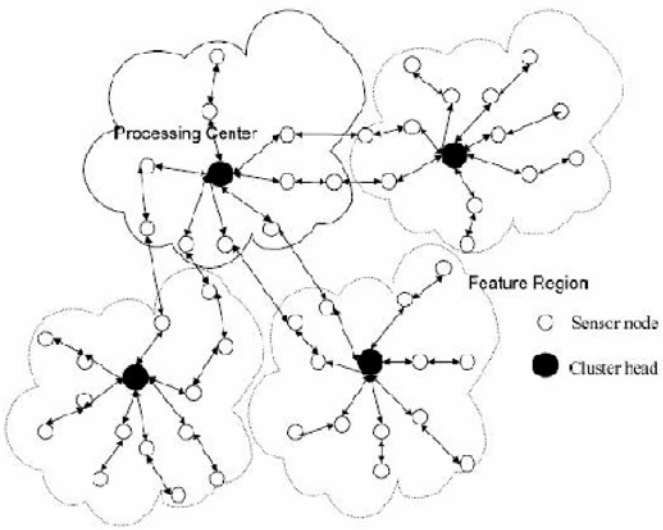

Figure 2. Cluster Based Wireless Network

Gateways maintain the states of the sensors and sets up multi-hop routes for collecting sensors 'data. A TDMA based MAC is used for nodes to send data tothe gateway. The gateway informs each node about slots in which it should listen to other nodes' transmission and slots, which the node can use for its own transmission. The command node (sink) communicates only with the gateways.

B. Data Routing

Our design based on hierarchical structure where data is routed from sensor nodes to the Sink through Gateways. Sinks are assumed to have sufficient power and memory to communicate securely with all the sensor nodes and gateways. Sensor nodes are deployed randomly over an area to be monitored and organize themselves into clusters after the initial deployment. A cluster-head *(*gateway) is chosen from each cluster to handle the communication between the clusters nodes and the Sink. Cluster-heads (gateways) are resource rich like as they have more computational and communication power comparatively other sensors nodes. Here we are assuming static gateway (CH) concept. That means gateways(CH) choose once at the time of network deployment using energy-efficient cluster head selection algorithm, based on its

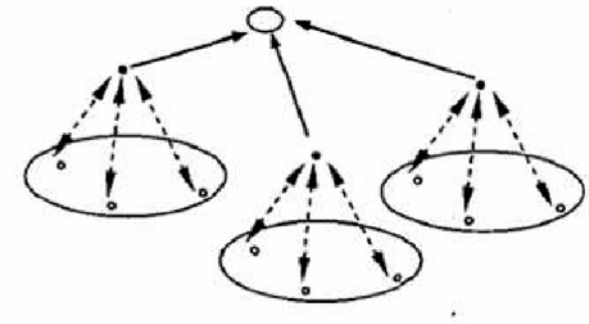

Figure 3. Data Routing in Cluster-Based Wireless Sensor Network

resource rich characteristic of the gateway, in order to saved power consumption among all sensor nodes, unlike other conventional algorithms the cluster head has change dynamically, due to this communication overhead will be more, so these algorithms consume more energy. Since data transmission is a major cause of energy consumption, ESDRP first reduces transmission of data from sensor nodes to cluster heads with the help of static cluster-head concept. Then, data aggregation is used to eliminate redundancy and to minimize the number of transmissions for saving energy. In our data aggregation methods, gateway receives all the data from sensor nodes and then eliminates the redundancy by checking the contents of the sensor data.

C. Data Redundancy Elimination Model

When all sensor nodes select the gateway to which it can forward the data packet .The cluster selection procedure i*s* based on our propose energy efficient cluster selection algorithm. After selecting the gateway node, each sensor node now forwards its data to its gateway. When a gateway node receives multiple data packets from its cluster's nodes, it performs aggregation operation by eliminating redundancy in the data. the gateway node perform aggregation by applying any aggregation functions like MIN, MAX, and AVG on the values of data packet and send only one packet while discarding other packets. But if this equation do not satisfies the gateway performs aggregation by simply concatenating two data packet in to one keeping value of both packets intact. The selection of value for redundancy factor (K) has a tradeoff between precision and energy consumption. If the application wants more precision, it should select a low value for redundancy factor otherwise a high value. Selecting high value for K means sending only one value thus less number of bits needs to be transmitted and hence low energy consumption.

D. Single Hop Communication

SEDR significantly reduces the energy consumption of all nodes in the cluster by reducing the transmission power of all nodes. The important beneficial issue in our designed protocol is that after the formation of cluster and selection of cluster head, all sensor nodes have to reduce their transmission power in such a way that they could only reach their single-hop distance neighbors. This operation requires some kind of synchronization among all nodes. The nodes have to calculate AMRP before to perform the single-hop communication. AMRP is the average of all the minimum power levels required for each sensor node within a cluster range(r) to communicate effectively with the CH .Sensor nodes calculate average minimum reach ability power based on strength of the CH selection message which is broadcast by the gateways, and based on the AMRP each sensor node self choose its cluster-head. Each sensor node looks in to the weight of all its possible gateways. Now when cluster-head received all data packets and aggregated them, it has to now increase its transmission power so that it can transmit the final aggregated data up in the cluster-head hierarchy towards the sink.

IV. SECURE ENCRYPTED - DATA ROUTING PROTOCOL(SEDRP)

1.Sensor to Gateway:- A Sensor node S*i* encrypt the packet P*i* using current session key SK, which is built-in at the time of sensors deployments and send to it's a local gateway G*i*.
Si ->GiE*SK* (P*i*)
2. Gateway to Gateway:-Following action are performed at the gateway:

(i) Gateway concatenates the encrypted packets it received from the sensors in its own cluster and from the other gateways on the path to the sink,

(ii) Increment the value of logical time stamps T*GS* by one and appends it to the concatenated packets,

(iii) Concatenate its own ID and send it to the next Gateway on the path to the Sink.
Gh ->Gk
{{ESK(Pl)}||{ESK(Pm)}||. . . ||{ESK(Pn)}||TGS ||Gh }

3. Gateway to Sink: Sink has received concatenated Encrypted packets from the gateway
Gk ->Sink
{{ESK(Pl)}||{ESK(Pm)}||. . . ||{ESK(Pn)}||TGS||Gh }
{{ES1K1(Pd) }||TGS||Gm}||. . . .||{{(ES2K2(PX)}||TGS||Gn)}

4. The following actions are performed by the sink on receiving packet from the gateway:
(i)For a credible time stamp sink decrypts the encrypted packets using the current session key,

DSK {ESK (Pl)} ||{ESK(Pm)}||. . . ||{ESK(Pn)}||TGS||Gh }
{{(ES1K1 (Pd)} ||TGS ||Gm)}||. . . .||{{(ES2K2(PX)}||TGS ||Gn)}
if (TGS >= TSG),the time stamp is credible and data is authentic DSK ESK (PX) ->PX,
if (TGS <= TSG),then the sink either discard the packet or send a retransmission request to the gateway.

(ii) Checks the timestamp credibility by first, sink extracts gateway ID from packet. For a valid gateway ID, it checks the timestamp credibility comparing the sequence number TGS appended by thegateway with the latest value of its logical time stamp TSG,

(iii) Verify gateways IDs in the packets.

5. On expiry of current session, sink increments the value of TSG by1, and generate the new session key using the pseudo random function (f) and current session key. The new session key is a function of current session and x.

V. CONCLUSION

This chapter, a new framework for secure energy efficient data aggregation is proposed. The proposed framework uses anew approach of encryption and aggregation on the based on secure energy efficient algorithms for large-scale and low energy wireless sensor and gateway networks (WSGN).The entire framework is based on the a three level architecture for energy constrained sensor node at lower level, a size able numbers of energy rich gateways at the middle level, and a sink which monitored the activity of sensor field at the upper level. The proposed scheme conserve the sensor node's energy as they are not involved in routing, unlike in WSNs. Sink used pseudorandom function for generating the new session key. As the number is random, key generation algorithm produces a different session key for the each and every session in order to ensure the freshness of the session key. Gateways append the logical time stamp and its id with the encrypted packets. When packet reached to the sink ,then sink check the logical time stamp and match this time stamp with the own time stamp, if it is match that means packet is fresh in order to ensure that message

is not altered . Sink also check the gateway id which is attached to the packet by help this id, sink to know the origination of the packet for further action. Communication between sensor nodes and the sink is secured as the sensor data is encrypted using symmetric key cryptography. The communication is secure because the message is encrypted by the session key, which will be different for each session. Therefore attacker cannot access the message. Thus session key dynamically changes after each and every session so it is very difficult to carryout eaves drop attack on the network for an intruder.

REFERENCES

1. Shriram Sharma "Energy-effcient Secure Routing in Wireless Sensor Networks" National Institute of Technology Rourkela , 2009.
2. S. Capkun and J. Habuax,"Secure positioning of wireless devices with application to sensor networks",inProc.IEEE INFOCOM,2005, vol.3,pp.1917-1928.
3. L. Escheaneur and V. Gligor, "A key-management scheme for distributed sensor networks" in Proc of ACM CSS,2007, pp. 41-47.
4. C.Karlof and D. Wagner, " Secure routing inwireless sensor networks: Attacks and countermeasures," in Proc. 1st IEEE Int.Workshop Sensor Network Protocols applications.,2003,pp.113-127.
5. Kumar.S.P. Chee-Yee Chong. Sensor networks: Evolution, opportunities, and challenges. Proc IEEE, August 2003.
6. W. Su Y. Sankarasubramaniam E. CayirciAkyildiz, I.F. A survey on sensor-networks. IEEE Communications Magazine, pages 102{114, 2002.
7. D. Agrawal N. Shrivastava, C. Buragohain and S. Suri. Medians and beyond: new aggregation techniques for sensor networks. Proceedings of the 2nd inter-national conference on Embedded networked sensor systems, pages 239-249,2004. ACM Press.
8. Z. Yu and Y. Guan," A dynamic enroute scheme for filtering false data injection in sensor networks," in Proc.IEEE INFOCOM,2006,pp .1-12.
9. P.NairH.Cam, S.Ozdemir and D. Muthuavinashiappan. Espda: Energy-efficient and secure pattern based data aggregation for wireless sensor networks. Computer Communications IEEE Sensors, 29:446{455, 2006.
10. J. Stankovic A. Perrig and D. Wagner. Security in wireless sensor networks.
11. Wei Ding and et.al. Energy equivalence routing in wireless sensor networks.
12. Jonathan Jen-Rong Chen Prasan Kumar Sahoo and Ping-Tai Sun. Efficient security mechanisms for the distributed wireless sensor networks. Proceedingsof the IEEE Third International Conference on Information Technology and Applications (ICITA'05), pages 0{7695{2316{1, 2005.
13. P.NairH.Cam, S.Ozdemir and D. Muthuavinashiappan. Espda: Energy-efficient and secure pattern based data aggregation for wireless sensor networks. Computer Communications IEEE Sensors, 29:446{455, 2006.
14. W. Su Y. Sankarasubramaniam E. CayirciAkyildiz, I.F. A survey on sensor-networks. IEEE Communications Magazine, pages 102,114, 2002.