Role Based Secure Routing in Large Wireless Sensor Networks

Hiren Kumar Deva Sarma, Avijit Kar, and Rajib Mall

***Abstract*—In this paper a Secure Routing Protocol for large Wireless Sensor Networks has been proposed. The protocol can take care of the mobility in the sensor nodes as well as in the base station. The entire sensor field is divided into some logical clusters and each cluster contains three different kinds of nodes namely Gateway Node, Cluster Head Node and Ordinary Sensor Node. The communication from the sensor nodes towards the base station happens in hierarchical manner and also in multi-hop fashion. Different secret keys are used for secure communication and the use of secret keys makes the communications secure. The performance of the proposed protocol in terms of throughput and average energy consumption for communication has been compared with that of LEACH-mobile. Security strengths of the protocol are also analyzed.**

***Index Terms*—Wireless sensor networks, secure routing, hierarchical routing, security threats.**

I. Introduction

Wireless Sensor Networks (WSN) comprise of hundreds to thousands of randomly deployed tiny sensor nodes which communicate through radio. The sensor nodes may be static or even mobile depending on the type of application. They form a distributed system and the sensor nodes forward the sensory data towards the base station through either single hop or multi-hop routes depending on the routing protocol [1]. Such a network suffers from several constraints which include limited battery power in the sensor nodes, limited communication bandwidth, limited onboard memory and also limited computing capability of the sensor nodes. Moreover, radio is an open communication medium and thus suffers from different security threats. As mentioned in [2] a Wireless Sensor Network may have to suffer from several active or passive attacks on its communication protocols. Routing in Wireless Sensor Network is a challenging task and it becomes even more complex while mobility in the sensor nodes as well as in the base station is considered. There are several applications of WSN including defense and military in which security of information becomes of highest priority. Therefore, secure routing in WSN is an extremely important communication task [2]. In [2] different attacks on routing protocols of WSN are summarized. At the same time it is challenging to incorporate security provisions in the routing protocols mainly due to the resource constraints, the WSN suffers from. It is not feasible to implement asymmetric key cryptographic protocols in such networks since they demand high amount of computing power as well as high amount of onboard memory. And symmetric protocols may not be able to provide high level of security to the information floating in the WSN. Thus there has to be a compromise between the required strength of the security protocol and the available computing resources in the system. In this paper, we propose a secure routing protocol intended for a Wireless Sensor Network which covers a large geographic area. Moreover, we consider the mobility of the sensor nodes as well as the base station. The proposed protocol is hierarchical [3] in nature and the sensor field is divided into some clusters after deployment of the sensor nodes. The sensor nodes inside each cluster are given various roles such as Gateway Node (GN), Cluster Head Node (CHN) and Ordinary Sensor Node (OSN). Depending on the respective role of a sensor node, the node uses different security keys for communication. In order to strengthen the security level we use a combination of symmetric and asymmetric cryptographic techniques in our protocol. In the proposed protocol, most of the computing overheads are shifted to the base station. The sensor nodes can save significant amount of energy and thus the proposed protocol is energy efficient. Fig 1 shows a typical clustered Wireless Sensor Network in which the base station and sensor nodes are mobile. The arrows attached to the nodes show the mobility of the nodes. In the Fig. 1, mobility of the nodes is shown only in one cluster just to indicate mobility but all clusters may contain mobile nodes.

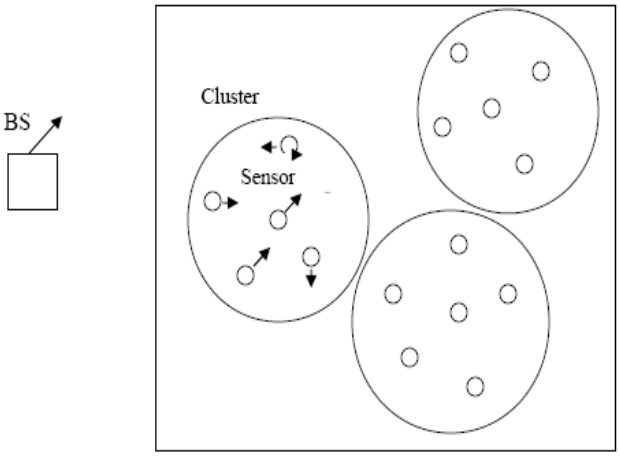

Fig. 1. A typical clustered wireless sensor network.

The rest of the paper is organized as follows: section II

Manuscript received September 26, 2012; revised November 28, 2012.

Hiren Kumar Deva Sarma is with the Department of Information Technology, Sikkim Manipal Institute of Technology, Majitar, East Sikkim, India (e-mail: hirenkdsarma@ gmail.com).

Avijit Kar is with the Department of Computer Science and Engineering, Jadavpur Univesity, Jadavpur, West Bengal, India (e-mail: avijit_kar@gmail.com).

Rajib Mall is with the Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, West Bengal, India (e-mail: rajib@cse.iitkgp.ernet.in).

describes few related works, followed by section III in which the proposed secure routing protocol has been discussed in detail. In Section IV, the experimental results regarding performance evaluation of the protocol are reported and in the Section V, the paper is concluded.

II. Related Work

There are some secure routing protocols proposed for Wireless Sensor Networks available in literature. But most of the secure routing protocols do not consider the mobility in Wireless Sensor Network constituents i.e., in the sensor nodes as well as in the base station. SPINS[4] is a security protocol suite proposed for WSN which consists of two security building blocks namely (SNEP) and μTESLA. Similarly INSENS[5], LEAP[6], TinySec[7] are some representative security protocols for WSN. SIGF (Secure Implicit Geographic Forwarding) [8] is a family of configurable secure routing protocols for Wireless Sensor Networks which can provide resource bound security solution that is good enough and of high performance. FBSR (Feedback based Secure Routing protocol for Wireless Sensor Networks) [9] is another secure routing protocol for WSN which makes use of the feedback of the neighbor nodes for making the forwarding decision in secure and energy efficient manner. SEEM (Secure and Energy-Efficient Multipath routing protocol) [10] uses multi-path alternately as the path for communicating between two specific nodes. SEEM is resistive to some specific routing layer attacks that have the character of pulling all traffic through the malicious nodes (i.e., wormhole, sinkhole, selective forwarding attack). Zhong Su *et al.* [11] proposed an efficient technique for secure communication in large-scale Wireless Sensor Networks which is based on random key pre-distribution scheme. In [13]&[14] authors propose mobile version of LEACH [3] but those protocols do not consider security aspect of routing in WSN. Thus, there is a necessity of secure routing protocol for WSN in which the sensor nodes as well as the base station may have mobility.

III. Proposed Protocol

The entire protocol is discussed in terms of two different sections *Routing* and *Security Provisioning* as mentioned below:

A. Routing

The secure routing protocol we propose here is hierarchical and cluster based in nature. After random deployment of the sensor nodes in the sensor field the entire sensor field is divided into some clusters (the total number of clusters is 5% of the total number of nodes deployed as in [3]). It has been assumed that the base station computes the clusters using efficient algorithm and then it also informs all the participating nodes. After cluster formation the base station distributes different roles such as Gateway Node (GN), Cluster Head Node (CHN) and Ordinary Sensor Node (OSN) to suitable nodes inside each cluster. Ideally each cluster contains one Gateway Node, two Cluster Head Nodes and remaining nodes as Ordinary Sensor Nodes. The Fig. 2 shows the hierarchical organization of the nodes inside each cluster. The Gateway Node is responsible for external communication i.e. inter cluster communication; a Cluster Head Node is responsible for collecting information from the Ordinary Sensor Nodes inside respective cluster and then forwarding the aggregated data to the Gateway Node. Each cluster contains two Cluster Head Nodes because each cluster is expected to be geographically large and moreover, the sensor nodes are mobile. Therefore, each cluster head collects data from only a part of the total number of Ordinary Sensor Nodes belonging to the same cluster. The base station selects the OSN for each CHN inside a cluster based on the proximity of the OSN with respect to the CHN. Thus, two Cluster Head Nodes cover the entire cluster in presence of mobility in the sensor nodes. Therefore, communication in the sensor field happens in a hierarchical manner, for example, from OSN to CHN and then from CHN to GN and finally from GN to base station (BS) either directly or via multi-hop as decided by the BS. All the GNs in the sensor filed and the BS create another network and the BS discovers various alternate routes from one GN to the BS. The BS computes the minimum energy route from one GN to itself by considering the energy expenditures against required number of transmissions and receptions and informs also to the concerned GN. The BS extracts the geographic location information of each sensor node deployed in the sensor field and then computes different routes such as a route from a GN to the BS. Again during the selection of a node as GN or CHN or OSN, the BS uses location information apart from remaining energy level of each sensor node, mobility range i.e., velocity and also neighborhoods. An ideal GN should be of high energy level and the probability of remaining connected to the CHNs should be high. Thus the GN is expected to be relatively of low mobility or near static. Again the two Cluster Head Nodes are selected in such a way that they are of high energy level, near static and also the probability of remaining connected to the respective OSNs is high. In the remaining part we are considering the security aspects of the proposed protocol.

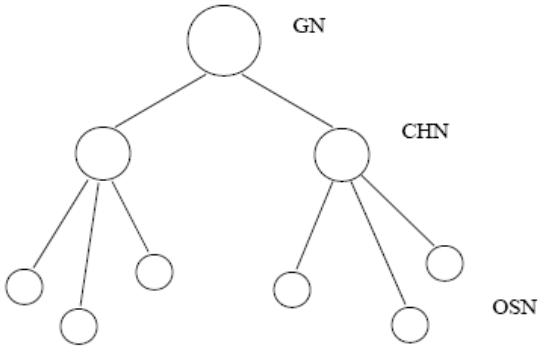

Fig. 2. Hierarchical organization of nodes inside each cluster.

B. Security Provisioning

The security to the routing protocol is provided by using various keys for encryption/decryption. Five major types of secret keys are used in the protocol for ensuring routing layer security in the Wireless Sensor Network system. Those are Initial Key (KINI), Preliminary Key (KPRE), Intra-Cluster Key (KICK), Inter-Cluster Key (KECK), and Common Key

(KCOM). These keys are used for encrypting different messages at various levels depending on the sender-receiver pair in the network system and subsequently also for decrypting the various messages. Some keys are generated though one way hash function and some keys are generated using the principles of Elliptic Curve Cryptography (ECC) [12].

C. Initial Key (KINI) and Preliminary Key (KPRE)

Every sensor node is embedded with an Initial Key before deployment and it is used for initial authentication by the base station. Once the sensor nodes are deployed in the field each node applies to the base station for authentication by encrypting its identification number $(ID)_i$ and the respective initial key $(KINI)_i$ by its Initial Key. After authentication, the base station communicates with the authenticated nodes and sends the respective preliminary key $(KPRE)_i$. $(KPRE)_i$ is the secret key for the node i for any further secret communication to be carried out with the base station.

D. Intra-Cluster Key (KICK)

Different communications inside each cluster happen through this class of key. There are basically two types of communication inside each cluster. Type (a): the ordinary sensor nodes communicate to the respective Cluster Head Nodes and vice-versa. Type (b): similarly, the Cluster Head Node communicates with the Gateway Node and vice-versa. The base station generates an Intra-Cluster Key (KICK) for each cluster k and distributes this key along with cluster ID to the respective nodes. This key distribution can be carried out by using the Preliminary Key (KPRE). Now the key set used for the communication of type (a) is {KICK , KCOM }; here, KICK is the Intra-Cluster Key and KCOM is the common key (KCOM is discussed in the section below). The key set used for the communication of type (b) is {KICK, KHGN} where KHGN is a pair wise key between the $(CH)_i$ and GN inside cluster k and this key is generated through the principles of Elliptic Curve Cryptography (ECC) [12] jointly by the Cluster Head Node and the Gateway Node.

E. Inter-Cluster Key (KECK)

It is necessary to mention that the *Inter-Cluster Key* is used by the Gateway Node of a cluster, for external communication with other Gateway Nodes in order to forward data towards the base station (BS). There are two types of communication possible, for example, (c) communication between two GNs (multi-hop communication towards the BS) and (d) direct communication between a GN and the BS. Inter-Cluster Key is generated by the BS and also distributed by BS encrypting it through the Preliminary Key. For both the communication types (c) and (d) the Inter-Cluster Key is used along with the Common Key (KCOM).

F. Common Key (KCOM)

This Common Key shared by each node is used for secret communication with the base station. As this key is shared by all the authenticated nodes in the network system, this key can always be used for any secret communication between any two authenticated entities irrespective of their roles in the system. This key is generated and distributed by the base station. This is a key which is also refreshed and redistributed by the base station after a regular interval of time. The key is generated by using one way hash function at the base station. The common key is distributed by encrypting it through the preliminary key (KPRE). The refreshed Common Key is again distributed by the BS after a regular time interval, 't_{key}' (t_{key} is also defined by the BS).

Thus, all the above mentioned five secret keys are used for secure routing of data inside a WSN system. It is a symmetric key cryptographic technique. Although KHGN, which is a pair wise key between the CH and GN inside a cluster is generated through the principles of Elliptic Curve Cryptography (ECC) [12] jointly by the Cluster Head Node and the Gateway Node which is an instance of asymmetric key cryptography.

IV. Simulation Results

The performance of the proposed secure routing protocol in terms of energy efficiency and throughput has been evaluated through a homegrown simulator written in C++. The simulator is consisting of several modules namely deployment module, topology construction module, mobility management module, medium access control module, routing module, energy analysis module and data delivery module. In the experiments carried out for evaluating the performance of the proposed protocol, we have considered the following parameters namely *throughput* and *average energy consumption for communication*. The performance of the proposed protocol has been compared with that of LEACH-mobile [14] while increasing the number of sensor nodes deployed in the field. The reason for considering LEACH-mobile for comparisons is being, it is also a hierarchical cluster based routing protocol which considers the mobility of the sensor nodes, although it is not a secure one. The experimental evaluations reported here project a comparative analysis of both the protocols, about the *throughput* and *average energy consumption for communication*. Various simulation parameters are summarized below in the Table I.

TABLE I: Summary of Simulation Parameters

Parameter	Value
Network Size	200 ×200 m
Number of Sensor Nodes Deployed	(20-100)
Percentage of Mobile Sensor Nodes	(10-100)%
Speed of Sensor Nodes	5-10 m/sec
Mobility Model	Random Waypoint Model
Radio Range	50 m
Radio Model	First Order Radio Model
Type of Deployment	Random
Data Rate of each Node	2000 bits/min.
Initial Energy of each Node	12 J

Throughput is the ratio between the total numbers of data packets sent intended for the base station to the actual number of data packets finally arrived at the base station during a specific time interval. *Average Energy Expenditure for Communication* is the parameter which signifies the average value of energy expenditures incurred at various nodes only

due to communication over a specific time interval. We carryout simulation studies in two different situations: (with respect to speed of the nodes and the base station, and the Link Error) *situation 1*: speed of the nodes and the base station: 10 meter/sec, Link Error: (2-5)%; *situation 2*: speed of the nodes and the base station: 15 meter/sec, Link Error: (5-7)%. Fig. 3.1 and Fig 3.4 show the simulation results under *situation 1* and Fig 3.2 and Fig 3.3 depict simulation results under *situation 2*. Fig. 3.1 and Fig. 3.2 show the *Average Energy Expenditure for Communication* under the influence of the proposed protocol and the LEACH-mobile against the *situation 1* and *situation 2*, respectively. For both the *situation 1* and *situation 2*, (and under the proposed protocol and LEACH-mobile) the average communication energy expenditure in the nodes increases along with the increase in the number of nodes. The proposed protocol outperforms LEACH-mobile in all situations.

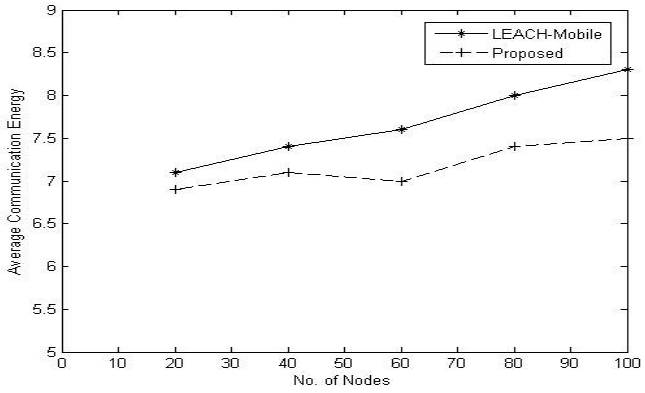

Fig. 3.1. Average communication energy expenditure variation I.

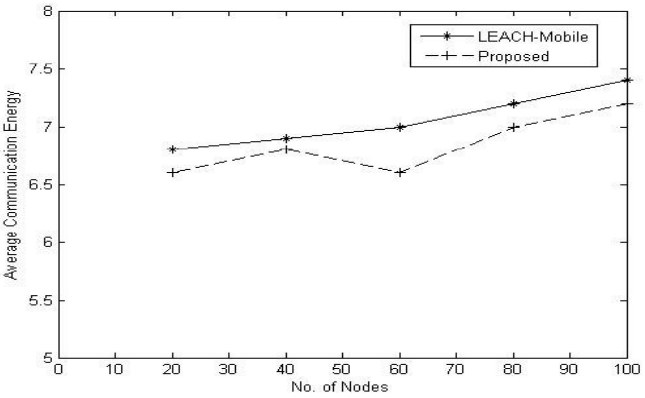

Fig. 3.2. Average communication energy expenditure variation II.

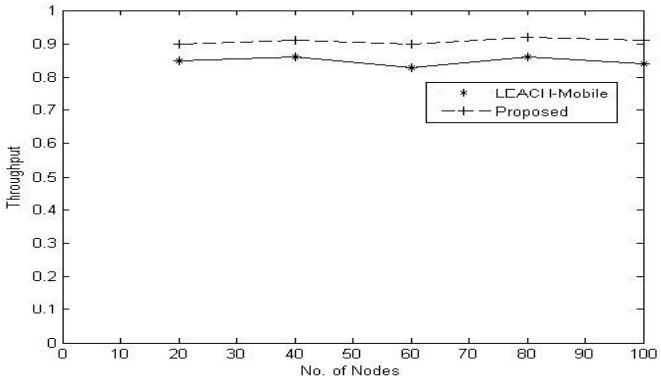

Fig. 3.3. Throughput analysis I.

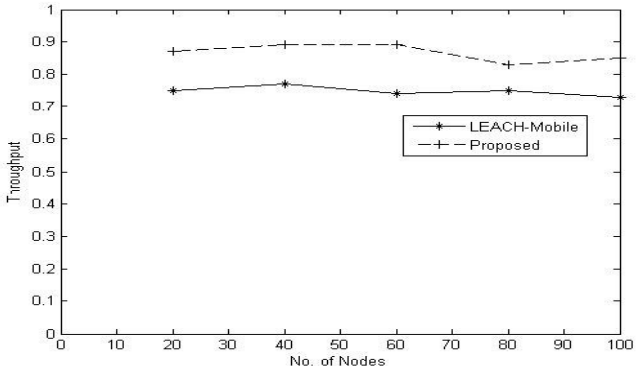

Fig. 3.4. Throughput analysis II.

Fig. 3.3 and Fig. 3.4 depict *throughput analysis* under the influence of the protocols, the proposed and LEACH-mobile for both *situation 1* and *situation 2*. The throughput level of both the protocols slightly degrades while the *mobility* along with the *link error* increases. But under all situations the proposed protocol outperforms LEACH-mobile with respect to throughput level too.

The simulation results show the better performance of the proposed protocol over the LEACH-mobile, while mobility is considered for both the sensor nodes as well as the base station.

Security Strength Analysis

The proposed protocol ensures *confidentiality* of information through encryptions by multiple keys which definitely raise the level of security. Moreover, any node deployed in the network is *authenticated* through initial registration process. Few secret keys e.g., *Common Key* are refreshed after a regular interval of time and thus any outdated message or replayed message can be detected. This also puts restriction against *intrusion* as the intruder node has to achieve the latest key which is not very straightforward. Again the sensor field is logically divided into clusters and thus even if few secret keys are revealed (though it is difficult) by the attackers, the attack shall remain confined to a locality or to the particular cluster and it cannot spread as the key sets for another cluster is different from others.

V. Conclusion

In this paper, we propose a novel secure routing protocol for large mobile Wireless Sensor Networks in which sensor nodes as well as the base station are mobile. The proposed protocol is hierarchical in nature. Most of the computing burden is shifted to the base station and thus the energy constrained sensor nodes save significant amount of energy. The clusters are organized in a unique manner, in the sense that each cluster contains sensor nodes with any one of the three possible roles e.g., Gateway Node, Cluster Head Node, & Ordinary Sensor Node. Moreover, each cluster contains two different Cluster Head Nodes and this provision helps in maintaining overall connectivity inside the clusters and thus throughput level of the proposed secure routing protocol is improved. The security of information is ensured through the use of various Secret Keys and security provision is simple

enough and it does not demand any special hardware in the sensor nodes for its full fledged implementation. Simulation results show an improvement in the routing performance (*average communication energy expenditure*, *throughput*) of the proposed protocol in comparison to the LEACH-mobile. A security strength analysis of the proposed protocol is also presented.

ACKNOWLEDGMENT

Authors of this paper would like to thank the organizers of ICIMT 2010 for proving opportunity to publish this paper in the proceedings of ICIMT 2010 (pp. V3-476-V3-480), ISBN 978-1-4244-8882-7.

REFERENCES

[1] I. F. Akyildiz, W. Su, and Y. Sankarasubramaniam, "A survey on sensor networks," *IEEE Comunications Magazine*, vol. 40, no. 8, pp 102-114, Aug. 2002.

[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, pp. 293-315, 2003.

[3] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. the 33rd Annual Hawaii International Conference on System Sciences (HICSS)*, Jan. 2000.

[4] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, "SPINS: Security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521-534, 2002.

[5] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-tolerant routing in wireless sensor networks," University of Colorado, Department of Computer Science Technical Report CU-CS-939-02.

[6] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in *Proc of CCS'03*, Washington D.C., USA, ACM Press, pp. 62-72, October 27-31, 2003.

[7] C. Karlof, N. Sastry, and D. Wagner, "Tiny sec: A link layer security architecture for wireless sensor networks," in *Proc. of the 2nd Int'l Conf. on Embedded Networked Sensor Systems*, Baltimore, MD, USA, ACM Press, pp 162-175, November 03-05, 2004.

[8] A. D. Wood, L. Fang, J. A. Stankovic, and T. He, "SIGF: A family of configurable, secure routing protocols for wireless sensor networks," in *Proc. of SASN*, Virginia, USA, October 2006.

[9] Z. Cao, J. B. Hu, Z. Chen, M. X. Xu, and X. Zhou, "FBSR: Feedback based secure routing protocol for wireless sensor networks," *J. Pervasive Comput. and Comm.* Troubador Publishing Ltd, vol. 1, no. 1, pp. 1-8.

[10] N. Nasser and Y. Chen, "SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks," *Computer Communications*, vol. 30, pp 2401-2412, 2007.

[11] Z. Su, C. Lin, F. Y. Ren, Y. X. Jiang, and X. Chu, "An efficient scheme for secure communication in large-scale wireless sensor networks," in *Proc. of Int'l Conference on Communications and Mobile Computing*, *IEEE Computer Society*. pp. 333-337, 2009.

[12] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, pp. 203-209, 1987.

[13] S. A. B. Awwad, C. K. Ng, N. K. Noordin, and M. F. A. Rasid, "Cluster based routing protocol for mobile nodes in wireless sensor network," in *Proc. of Int'l Symposium on Collaborative Technologies and Systems 2009, CTS'09*, pp. 18-22, May 2009.

[14] D. S. Kim and Y. Chung, "Self-organization routing protocol supporting mobile nodes for wireless sensor network," in *Proc. of 1st Int'l Multi-Symposium on Computer and Computational Sciences (IMSCCS'06)*, 2006.