A Dynamic Grid Based Route-Driven ECDH Scheme for Heterogeneous Sensor Networks

S. Pradheepkumar, R. Fareedha, M. Jenieferkavetha,
A. Geanremona, and R. Juliajoyce

Christ College of Engineering and Technology, Pondicherry, India-605014
{spradheepkumar,fareedha1990,jeniferkavetha}@gmail.com
{geanremona,juliajoyce.b.tech}@gmail.com

Abstract. Ongoing research work shows that homogeneous sensor networks have poor security, connectivity, performance and scalability. Heterogeneous sensor network (HSN) consists of physically different types of sensor nodes. The feasibility of implementing Elliptic Curve Diffe-Helmen (ECC) in HSN is simulated in this approach. Under dynamic condition of sensor node, implementation of grid-based coordinate route driven scheme has been proposed. This route driven scheme is highly adaptable for public key management scheme for HSN. It also compares the energy and throughput efficiency for dynamic position of sensor nodes. The proposed method is compared with the existing routing techniques like AODV and DSR. The proposed method dramatically increases network lifetime based on the elected coordinator nodes and the size of the grid area.

Keywords: Heterogeneous Sensor Network (HSN), Key Management, Elliptic Curve Cryptography (ECC), Elliptic Curve Diffie-Hellman (ECDH).

1 Introduction

Wireless Sensor Networks (WSN) has recently focused a lot of interest in the research community due to their wide range of attractive applications and its important position is promoted rapidly. Each sensor node contains a battery-powered embedded processor and a radio, which enables the nodes to self-organize into a network, communicate with each other and exchange data through wireless network links. HSN are a result of the combination of advances made in the field of analog and digital circuitry, wireless communications and sensor technology.

HSN deployments increasingly employ in-network processing to achieve scalability, integrity, energy-efficiency and timeliness. HSN are commonly used in ubiquitous and pervasive applications such as military, homeland security, health-care, and industry automation [1]. An important area of research interest is a general architecture for wide area wireless sensor networks that seamlessly integrates homogeneous sensor network and HSN. HSN have different types of sensors, with a large number of ordinary sensors in addition to a few potent sensors. The main goal of key management in HSN is the establishment of secure links between neighbour

N. Meghanathan et al. (Eds.): NeCoM, WiMoN, and WeST 2010, CCIS 90, pp. 98–106, 2010.

sensors at network formation phase. In order to provide secret communication in a sensor network, shared secret keys are used between communicating nodes to encrypt data. Key establishment protocols are used to set up the shared secrets, but the problem is complicated by the sensor nodes' limited computational capabilities, battery energy, and available memory. The proposed key management scheme is resilient against collusion attack. The rest of the whole paper is designed as follows. In Section II and III discuss about the proposed scheme in detail. Section IV discusses the matrices, simulation results and outputs. Finally Section V concludes the proposed method.

2 The ECDH Based Key Management Scheme

One possible key management scheme is to permit every LN-sensor (lower end sensor node) set up shared keys with each of its neighbours by using the ECDH key exchange scheme. In many existing reliable sensor networks, nodes are obtusely deployed in the field. One sensor node could have as many as 40 or more neighbours in the network. Although ECC public-key cryptography is executable for small sensor nodes, a 160-bit [2] ECC point multiplication still takes about less than one second. It would need too much computational time and energy for LN-sensor to run ECC with each of its 30 neighbours. In this section, an efficient key distribution management scheme requires only a small number of ECC computations in each LN-sensor. A server node [3] is used to generate pairs of ECC public and private keys, one pair for each LN-sensor and HN-sensor (Higher end sensor node). The server node selects a new elliptic curve *EC* over a large Prime field *F* and a point *P* on that curve. Each LN-sensor (say *x*) is pre-loaded with the private key (say $SK^{y}_{x} = I_x$). A HN-sensor has large storage space and is pre-loaded with public keys of all the LN-sensor (ex: $SK^{x}_{x} = I_x P$, etc).Each HN-sensor also stores the association between each LN-sensor and its private key. Each HN-sensor is pre-loaded with a pair of ECC public key and private key. The public keys[4] of HN-sensor are also loaded in each LN-sensor and the keys are used to authenticate broadcasts from HN-sensor.

The ECDH algorithm is used for authenticating broadcasts from HN-sensor. Each LN-sensor can verify the digital signature by using HN's public key and thus authenticate the broadcast. In addition, each HN-sensor is pre-loaded with a special key SK_H, which is used by a symmetric cryptography algorithm for verifying newly deployed sensors and for secure communications among HN-sensors. Even if an adversary captures a HN-sensor, she could not obtain the key materials. Given the protection from the tamper-resistant hardware, the same pair of ECC public/private keys may be used by all HN-sensor and this can reduce the storage overheads. Assume [5] each LN-sensor can determine its location by using some secure location services, such as the scheme. After selecting a cluster head HN, each LN-sensor *x* sends to HN a clear *key-request* message, which includes the LN-sensor ID_i and *i*'s location. A proposed scheme may be used to forward the *Key-request* message to HN [6]. Fig.1 shows the basic example of ECDH secret key exchange.

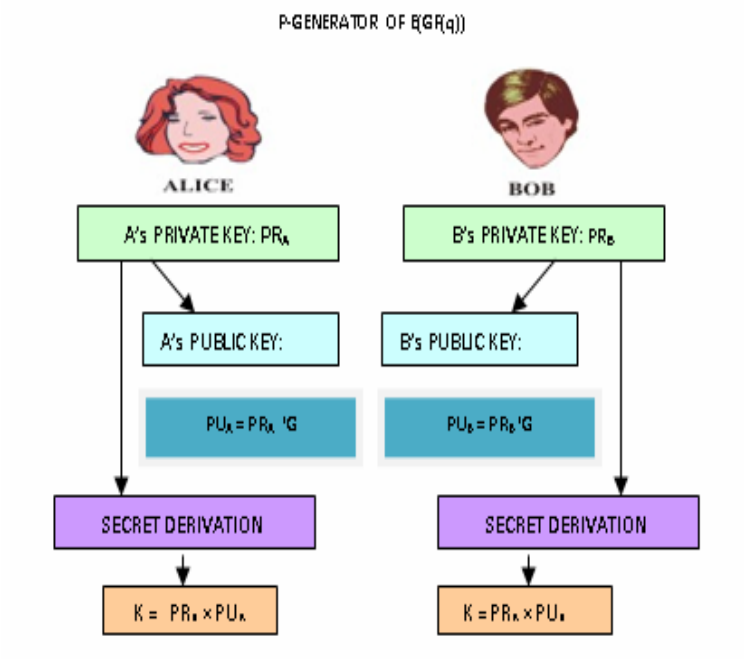

Fig. 1. ECDH secret key exchange

3 Dynamic Grid Based Coordinate Route Driven Scheme

Here, the key management scheme [7] is highly depend on mobility of sensor node (i.e.) dynamic grid-based coordinate route driven scheme [8], which assume the deployment knowledge for HSN. In dynamic grid-based coordinate route driven scheme, the sensor nodes are assumed as dynamic after deployment. The distribution of nodes can be predicted from deployment model in fig. 2 and fig. 3 that shows how sensor nodes are deployed. The main focus of dynamic grid-based coordinate route driven scheme is on dividing the network into square shaped grids to extend network lifetime. The entire network is partition into equally shaped grids, and in each grid a non-stationary nodes, the coordinator is elected, like in the span algorithm. The implicit routing algorithm used in dynamic grid-based coordinate route driven scheme is similar to level flooding. In dynamic grid-based coordinate route driven scheme, messages reaches only selected nodes in the field instead of all the nodes in the network.

The main idea of partitioning the network into grids is to make only one node dynamic-alive for each grid, while the rest of the nodes in that grid are sleep mode so as to conserve their battery-energy life. In each square grid, the coordinator participates in routing as long as the amount of energy level in that coordinator is above a certain threshold value. When the energy level drops below the threshold, a new coordinator is elected for that grid. The source node transmits information to the sink node through the active coordinators node, and the sink node traces a route back

to the source. The process of flooding algorithm continues till the nodes participating in the routing run out of energy level, when new coordinators are elected and a new route back to the source node from the sink node is calculated. The source node starts flooding algorithm by sending a query information message to all the neighbour coordinators nodes, which flood other coordinators node in the network till the query information message reaches the sink node. For example, each square grid of side of a fixed length, 200 m. Connectivity level in the network depends on the square grid size, coverage transmission range and the sensitivity of all the nodes. When square grid coordinators are elected, care should be taken such that the coordinators node must still be able to connect to neighbouring grid coordinators node. Therefore, square grid size is very important to maintain connectivity level throughout the network as too large a grid size will result in loss of connectivity level of the nodes in the network.

In [9], dynamic grid-based coordinate route driven scheme places an upper bound on the square grid size and determines the conditions to maintain connectivity level throughout the network depending on the grid size and the transmission range of the nodes. It also maintains load balancing as does Geographic Adaptive Fidelity (GAF). The function of the coordinator node is distributed amongst the nodes in the network based on the ranking of the nodes in each grid. It observes the effects of transmit power, receiver sensitivity and grid size on network lifetime, and determines that decreasing the transmit power increases network lifetime. The idea of a virtual square grid over the network field was proposed in the GAF algorithm. Dividing the entire network into equal sized grids, and electing nodes in each grid to participate in routing while other nodes were put to sleep was introduced in dynamic grid based coordinate route driven scheme. Two types of grid based coordinate route driven scheme have been seen in proposed system. They are; uniform grid-based coordinate route driven scheme for dynamic sensor nodes and non-uniform grid-based coordinate route driven scheme for dynamic sensor nodes. Uniform grid-based coordinate route driven scheme is more efficient when the distribution of the sensor nodes in the sensor field is uniform. Varying the square grid sizes in the network extends the lifetime of the network.

In [10], the relation between optimal radio range and traffic is used to define in both uniform and non-uniform grid for the GAF protocol. In this proposed scheme, the non-uniform grid size for the dynamic grid-based coordinate route driven scheme is implemented and the results were analyzed. The underlying route algorithm of non-uniform grid-based coordinate route driven scheme is the same as the grid-based coordinate route driven scheme. The entire sensor surveillance field is divided into non-uniform sized grids. For adopting these route driven techniques, partition the network into small grid size. And calculate the best suite grid structure with the help of collision rate in the network with respect to grid structure and result the life time of the network. When considering the grid size of 50 units, the number of sensor node deployed in the 50 unit grid size will be very less. So obviously wastage of resource will be highly seen in HSN. But the collision rate will be less. When considering the grid size of 100 units, an average number of sensor nodes can be adopted by the 100 unit grid size, so that the collision will be at normal rate. When considering the grid size of 200, and an average-limit numbers of sensor nodes were adopted by the 200

unit grid size, so the collision rate will be slightly above the normal rate. Collision rate for 200 unit grid size will be more than 100 unit grid size.

So, by keep on increasing the unit of grid size, more number of sensors will be adopted according to the respective grid size, so the collision rate is highly seen. Hence by the simulation result, the grid size for 100 units and 200 units is suited for the network partition. To maintain the life time of the HSN, energy level is maintained at very low threshold level and throughput is highly maintained. By using the metrics like energy efficiency and throughput, the life time of the sensor network can be calculated. And by comparing the network life time of the proposed technique with respect to Ad Hoc On-Demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR) in terms of energy spent by the sensor node in the sensor network and by throughput efficiency of the sensor node in the HSN. All the simulation results are done using GLOMOSIM simulator and shown in fig.4-8.

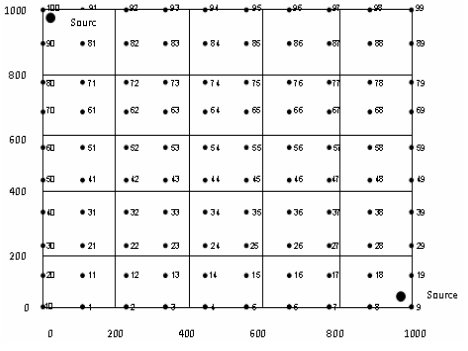

Fig. 2. Uniform grid based coordinate route driven scheme for dynamic nodes

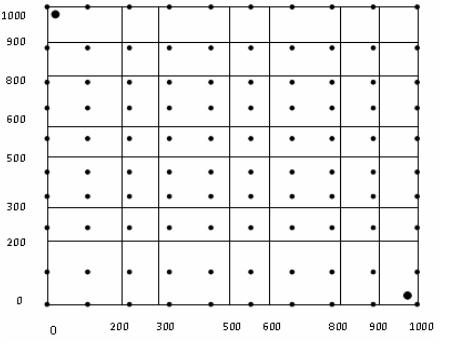

Fig. 3. Non-uniform grid based coordinate route driven scheme for dynamic nodes

4 Performance Metrics

4.1 Energy Comparison of Uniform Grid-Based Coordinate Route Driven Scheme for Dynamic Sensor Nodes

Fig. 4 shows the simulation results of energy comparison for different routing technique like uniform grid-based coordinate route driven scheme, AODV and DSR. Under dynamic condition of sensor nodes, uniform grid based coordinate route driven scheme consumed less energy when compare to AODV and DSR.

4.2 Energy Comparison of Non-uniform Grid-Based Coordinate Route Driven Scheme for Dynamic Sensor Nodes

Here the non-uniform grid-based coordinate route driven scheme had consumed less energy when compare to AODV and DSR with respect to dynamic condition of sensor nodes. Fig. 5 shows the simulation result of energy comparison for different

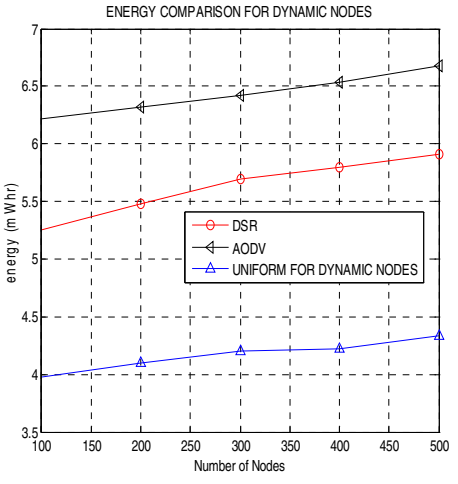

Fig. 4. Energy comparison for Uniform grid-based coordinate route driven scheme for dynamic nodes

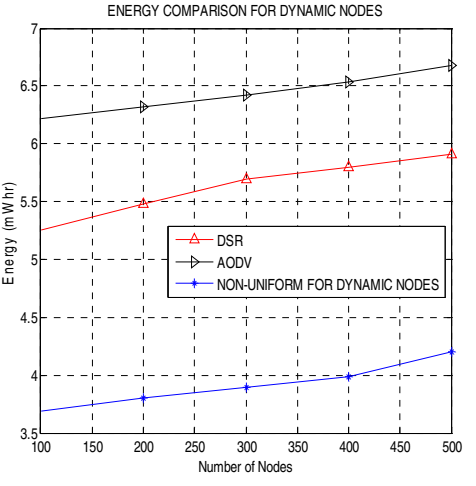

Fig. 5. Energy comparison for Non-uniform grid-based coordinate route driven scheme for dynamic nodes

routing techniques like non-uniform grid-based coordinate route driven scheme, AODV and DSR. When comparing with uniform grid-based coordinate route driven scheme, the energy consumption is very less in non-uniform grid-based coordinate route driven scheme.

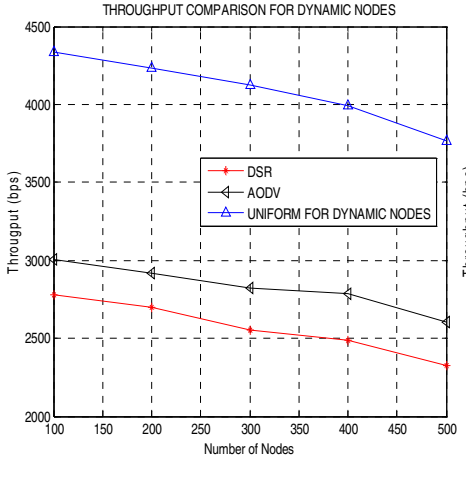

Fig. 6. Throughput comparison for Uniform grid-based coordinate route driven scheme for dyanmic nodes

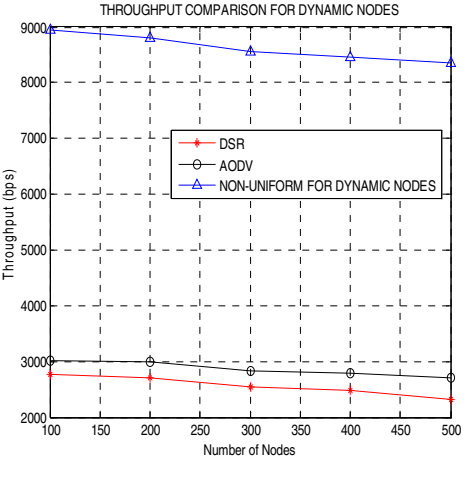

Fig. 7. Throughput comparison for Non-uniform grid-based coordinate route driven scheme for dyanmic nodes

4.3 Throughput Comparison Uniform Grid-Based Coordinate Route Driven Scheme for Dynamic Sensor Nodes

Fig. 6 shows the comparison of throughput between DSR, AODV and uniform grid-based coordinate route driven scheme. Here the uniform grid-based coordinate route driven scheme has higher throughput when compare to AODV and DSR.

4.4 Throughput Comparison for Non-uniform Grid-Based Coordinate Route Driven Scheme for Dynamic Sensor Nodes

For Dynamic condition of sensor nodes, the non-uniform grid-based coordinate route driven scheme has higher throughput when compare to AODV and DSR. Fig. 7 shows the simulation result of throughput comparison for different routing. When comparing with previous results (i.e.) fig.6, the throughput is very high in non-uniform grid-based coordinate route driven scheme when compare to uniform grid-based coordinate route driven scheme.

4.5 Network Life Time for Different Routing Techniques

Fig.8 shows the simulation result of network life time for different routing techniques for mobile sensor nodes. Here, it compare the network life time for non-uniform based coordinate route driven scheme, uniform based coordinate route driven scheme, DSR and AODV. Network life time is referred as the total number of days survived by sensor node in the network. Here the comparison demonstrates that non-uniform grid-based coordinate route driven scheme has more number of days count to live. Here the life time is calculated for the sensor node by the mean of energy consumed by the sensor nodes in the portioned network.

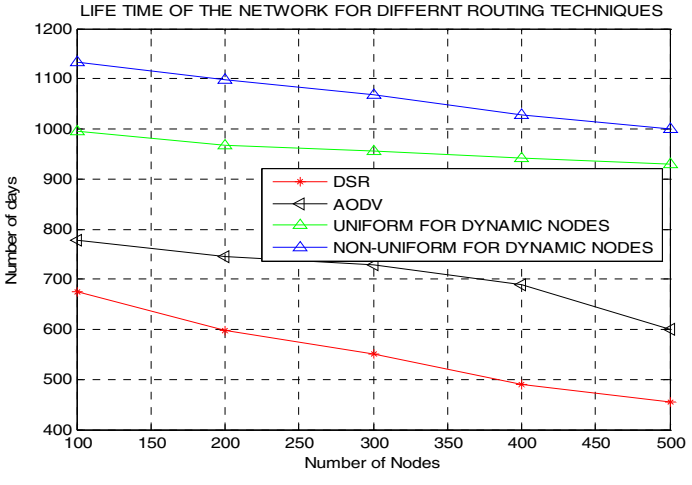

Fig. 8. Network life time for different routing techniques

When comparing network life time with different routing techniques, non-uniform grid-based coordinate route driven scheme has more number of days to live.

5 Conclusion

The proposed key distribution scheme describes a dynamic grid based route driven ECDH scheme for HSN. This proposed scheme utilizes the fact that a sensor only communicates with a small portion of its neighbours and thus greatly reduces communication and computation overheads of key setup. Simulation results show various attributes for densely random and uniform deployed sensor networks. The proposed route driven scheme is tested for scalability by varying the node density from 100 nodes in the network to 1000 nodes in the network. The performance shows that the lifetime network of the sensor network increases by using the non-uniform grid-based coordinate route driven scheme. The results are compared and contrasted to non-uniform grid-based coordinate route driven scheme, uniform grid-based coordinate route driven scheme and the existing routing techniques. By using the non-uniform grid-based coordinate route driven scheme, the sensor network can achieves goals for their survival. Hence non-uniform grid-based coordinate route driven scheme plays a major role in routing the information from source to destination. And they can be easily applicable and adaptable for any type of real time application for HSN.

References

1. Brown, J., Dug, X., Nygard, K.: An efficient public - key base heterogeneous sensor network key distribution scheme. In: Proceedings of IEEE Telecommunication conference, Washington, DC, pp. 991–995 (2007)
2. Duarte-Melo, E., Liu, M.: Analysis of energy consumption and lifetime of heterogeneous sensor network. In: Proceedings of Global Telecommunications Conference, GLOBECOM, pp. 23–35 (2002)
3. Chan, H., Perrig, A., Son, D.: Random – key pre-distribution scheme for Sensor network. In: Proceedings of IEEE Symposium on the Security and Privacy, USA, pp. 197–213 (2003)
4. Du, X., Yang, X., Song, C., Guizani, M., Chen, H.: A routing-key management scheme for heterogeneous sensor network. In: Proceedings of IEEE Global Conference, Scotland, pp. 3407–3412 (2007)
5. Mhatre, V.P., Rosenberg, C., Kofman, D., Mazumdar, R., Shroff, N.: A minimum cost heterogeneous sensor network with a lifetime constraint. IEEE Transactions on Mobile Computing, USA, 4–15 (2005)
6. Du, X., Yang, X., Guizani, M., Chen, H.: A Pseudo - random function based key Management scheme for heterogeneous sensor network. In: Proceedings of Global IEEE Telecommunication Conference, Washington, DC, pp. 5138–5142 (2007)
7. Kim, J.M., Cho, J.S., Jung, S.M., Chung, T.M.: An Energy-Efficient Dynamic Key Management in Wireless Sensor Networks. In: 9th International Conference on Advanced Communication Technology, Gangwon-Do, pp. 2148–2153 (2007)

8. Wen, Y., Shiang, C.: Integrated design of grid - based routing in heterogeneous sensor network. In: IEEE International Conference on Advanced Information Networking and Applications, Niagara Falls, ON, pp. 625–631 (2007)
9. Baoxian, Z., Mouftah, H.T.: Efficient grid – based routing in heterogeneous multihop networks. In: Proceedings of 10th IEEE Symposium on the Computers and Communications, Spain, pp. 367–372 (2005)
10. Akl, R., Kadiyala, P., Haidar, M.: Non-uniform grid - based coordinated routing in wireless sensor network. Journal of Sensors (2009)