ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology *Vol 8(S9), 75–81, May 2015* DOI: 10.17485/ijst/2015/v8iS9/65578

Efficient and Secure Hierarchical Key Management Scheme for Wireless Sensor Networks using QR Decomposition Scheme

S. Abinaya*, R. Ezhilarasie and A. Umamakeswari

School of Computing, SASTRA University, Tirumalaisamudram, Thanjavur - 613401, Tamil Nadu, India;
abiselva.21@gmail.com, ezhil@cse.sastra.edu, aum@cse.sastra.edu

Abstract

Wireless Sensor Network (WSN) assures to revolutionize sensing in a spatially dispersed and dedicated manner in various applications. It requires adopting a security mechanism for critical applications. Though many cryptographic algorithms are available it strength depends upon the key used for encrypting and decrypting the collected data. Key Management Scheme (KMS), a technique for establishing and maintaining the key relation, play a vital role in any security mechanism. The proposed work was focused on pairwise key establishment using QR based matrix Decomposition method. Though many metrics are available the prime factor for any WSN is key connectivity. The proposed KMS focuses on 100% key connectivity compared to probabilistic approach. For each communications different symmetric matrices are generated and are decomposed into Q and R matrix. This scheme is implemented in LPC2148 with Xbee to check its feasibility in real time applications. Performance analysis shows that the proposed method achieves 100% key connectivity, better resilience and scalability.

Keywords: Key Connectivity, Key Management Scheme (KMS), Security, Wireless Sensor Network (WSN), QR Decomposition

1. Introduction

Wireless sensor network is a kind of ad hoc network that consists of sensor node commonly referred as motes, with limited power source, communication and computational capabilities. It is appropriate for performing a variety of tasks in ecological monitoring, industrialized automation system, Military application, Health monitoring etc., Sensor nodes are deployed in any (attended/unattended) environment and can establish a wireless connection among them. Since many cases WSN are deployed in hostile and abandoned areas, the collected data has to be secured in an appropriate manner. To ensure secure communication among the sensor nodes, all the data must be encrypted and equally node must also be authenticated[1]. This results in adopting a security mechanism. Though many cryptographic algorithms are available the strength depends upon the key used for encryption and decryption. Thus KMS plays an essential role in WSN to establish a keying relation among the nodes. Many KMS are available but not every method is suitable for WSN because of sensor node constraints.

KMS can be implemented in two ways: Symmetric or Asymmetric technique[2]. As WSN is resource constrained asymmetric key management may not be suitable for WSN because of its keying nature (private and public key). Hence symmetric based key management schemes are preferred for WSN. Security requirements for key management[3] schemes are integrity, confidentiality, authentication and time synchronization. The metrics to be evaluated against KMS are: Key connectivity, Resilience, Scalability, Efficiency (Storage, Communication and computation).

1.1 Key Connectivity

Each node communicates with every node in a region by sharing a key either directly or indirectly.

*Author for correspondence

1.2 Resilience

When a node gets compromised, the remaining node links have to be secured. The need for network resilience increases with the chance of a node being subverted by an adversary.

1.3 Scalability

Capability to support when additional node is added to the network. In WSN thousands of nodes are connected. If the network wants to be expanded KMS should be scalable.

1.4 Efficiency

Network nodes have the limited capabilities like memory, communication and computation. Memory efficiency evaluated against Storage of keys, Computation based processor cycle required to set the key, Communication based on number of messages required to establish a key among the nodes.

2. Related Works

During the deployment stage in WSN, the sensor nodes have to be distributed with keys for implementing key management schemes. Various key managements have been proposed. These key management schemes can be implemented in two ways: Random approach and Deterministic approach.

Various Random Keys Pre-distribution schemes are used. The basic scheme is an E-G scheme[4] in which large pool P of key of size 2^{20} is constructed. Random m keys are chosen from the pool and are stored in sensor nodes. The Key ID's of each node is exchanged with neighboring nodes to obtain a common key. This key is used as secret key in the communication links. The Q-Composite method is an enhancement to the method which uses q keys for communication. The major advantage of this method is higher resilience.

Matrix key distribution scheme[5] uses a cluster structure to reduce the communication and computation overhead. Blom's method is used to improve the connectivity between the clusters. It involves two phases: key agreement and pre distribution phase. A cluster of size m with n cluster heads is formed in the key pre distribution scheme. A common key is shared among the nodes in the cluster with which an inter and intra clustering key mechanism is established. Although this method proves to be efficient, it fails for large number of nodes.

As an improvement to Blom's scheme, a pairwise key distribution method which uses multiple keys is used. A LU composition technique[6] is one of the technique that integrates with Elliptic curve for key path establishment. It is used for group key agreement and management using tree based LU matrix. Elliptic curve Hellman protocol is used for key agreement to share the key in unsecure areas. This method is mainly used for securing communication link between cluster head and nodes in it. The disadvantage of this scheme is that it provides poor scalability and requires high storage.

ID based Pairwise key pre distribution scheme[4] using matrix based hierarchical model is proposed. It uses a pairwise key for matrix method; this scheme provides high resilience compared to the above schemes. On a hierarchical basis, the network is sub-divided into parts. Blom's scheme is used for constructing symmetric matrix. The key is exchanged between the nodes for secured communication.

Deterministic method uses elements with certain characteristics. The Exclusion Basis[7] System is used for group communication. A tree based approach can also be used. The cluster key becomes open on node compromises, whereas in group communication the cluster key changes periodically. However, the energy consumption is high for frequently updating the key.

3. The Proposed Scheme

3.1 The Network model

There are two types of architecture where in sensor nodes are deployed, Hierarchical model and Distributed model. In Distributed model there is no fixed infrastructure which implies that the topology of the network is not prior. In this type of network architecture, keying information loaded will be more this leads to storage inefficiency. In the hierarchical network[8] ordering among the nodes are established i.e., hierarchical levels constitute a network. Many cases the levels will be as three layers with base station, cluster head and sensor nodes. Base stations have many orders of magnitude when compared to cluster head and sensor node. The resources[9] are more for cluster heads when compared to sensor nodes as they involve in long distance transmission. Hierarchical WSN Architecture is shown in Figure 1.

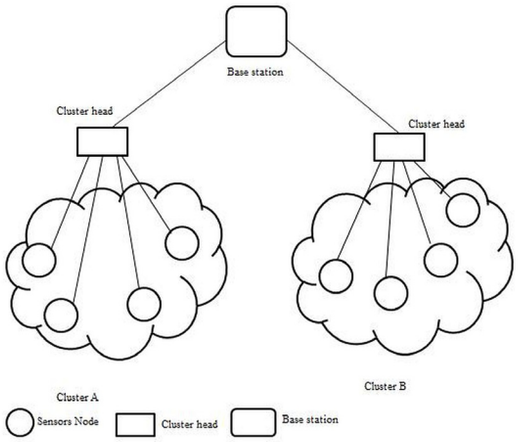

Figure 1. Hierarchical WSN Architecture.

This proposed work mainly focuses on three-level hierarchical modeling. The clusters can be framed in view of different criteria, for example, capacities, area, and signal quality. Every cluster has a cluster head and an arrangement of sensor nodes. Communications are made only with i) sensor nodes within the cluster and ii) Cluster to Base station to reduce the communication overhead and traffic.

3.2 Keying Requirements

The keying requirements are classified as Key Pre distribution and Dynamic keying requirements. In the Key-Pre distribution scheme as it name implies the keys are preloaded into the sensor node. With that keying information, keys are established and nodes in the network will communicate. In dynamic keying, code or some information is loaded into motes to generate the keys. The Computation cost to generate the key will be more and equally code memory size is large. To avoid these complexities, many KMS is based on Key Pre distribution method. The proposed work is based on matrix based Key Pre distribution scheme where symmetric matrix is decomposed using the QR decomposition technique. The symmetric matrix is decomposed using below Figure 2.

3.3 Background of QR Matrix Decomposition

Definition: The symmetric matrix K is decomposed[10] into Q matrix and R matrix using below procedure. Decomposition is performed in base station (High end configuration device).

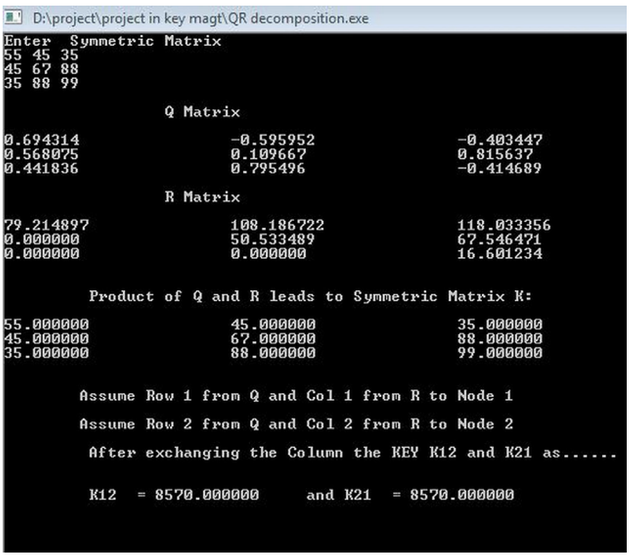

Figure 2. Base station generates Q and R matrix.

$$\begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} = \begin{pmatrix} Q_{11} & Q_{12} & Q_{13} \\ Q_{21} & Q_{22} & Q_{23} \\ Q_{31} & Q_{32} & Q_{33} \end{pmatrix} * \begin{pmatrix} R_{11} & R_{12} & R_{13} \\ 0 & R_{22} & R_{23} \\ 0 & 0 & R_{33} \end{pmatrix} \quad \text{(i)}$$

The Q and R matrix are constructed as,

$$Q = (W_1 | \& W_2 | \quad W_N); R = \begin{pmatrix} V_1W_1 & V_2W_1 & \dots\dots\dots V_NW_1 \\ 0 & \dots\dots\dots & V_NW_2 \\ 0 & 0 & V_NW_N \end{pmatrix}$$

$$W_1 = \begin{pmatrix} Q_{11} \\ Q_{21} \\ Q_{31} \end{pmatrix}; W_2 = \begin{pmatrix} Q_{12} \\ Q_{22} \\ Q_{32} \end{pmatrix}; W_3 = \begin{pmatrix} Q_{13} \\ Q_{23} \\ Q_{33} \end{pmatrix} \quad \text{(ii)}$$

Each column of symmetric matrix K is denoted as V_1, V_2 and V_3.

$$R_{11} = V_1W_1; R_{12} = V_2W_1; R_{13} = V_3W_1;$$
$$R_{22} = V_2W_2; R_{23} = V_2W_2; R_{33} = V_3W_3; \quad \text{(iii)}$$

$$W_1 = \frac{1}{||V1||}V_1; W_2 = \frac{1}{(\square\square| \text{V2} - \text{projV2} |\square\square)}(\text{V}_2 - \text{projV2});$$
$$\text{W}_3 = \frac{1}{(\square\square| \text{V3} - \text{projV3} - \text{projV2} |\square\square)V_3} \quad \text{(iv)}$$

For each cluster different symmetric matrices are generated and then decomposed into Q and R matrix to improve network resilience. Many schemes are based

on threshold[6] say λ, secret sharing scheme i.e., when λ nodes captured the entire network will get revealed. Once matrices are decomposed each cluster's sensor node are preloaded with row of Q matrix and column of R matrix of its symmetric matrix.

3.3.1 Example: QR Matrix Decomposition

In this scheme symmetric matrix is generated from a pool of random numbers. Using Equations (ii), (iii) and (iv) Q and R matrix are constructed. Steps to compute two matrices are as follows:

Step 1: Assume Symmetric matrix K is generated for pool of random numbers.

$$K = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix} \quad \text{(v)}$$

Step 2: The Q matrix can be acquired from the Equation (iii and iv)

$$Q = \begin{pmatrix} \frac{1}{\sqrt{5}} & \frac{6}{\sqrt{70}} & \frac{-2}{\sqrt{14}} \\ \frac{2}{\sqrt{5}} & \frac{-3}{\sqrt{70}} & \frac{1}{\sqrt{14}} \\ 0 & \frac{5}{\sqrt{70}} & \frac{3}{\sqrt{14}} \end{pmatrix} \quad \text{(vi)}$$

Step 3: The R matrix can be acquired from the Equation (iii)

$$R = \begin{pmatrix} \frac{1}{\sqrt{5}} & \frac{6}{\sqrt{70}} & \frac{-2}{\sqrt{14}} \\ \frac{2}{\sqrt{5}} & \frac{-3}{\sqrt{70}} & \frac{1}{\sqrt{14}} \\ 0 & \frac{5}{\sqrt{70}} & \frac{3}{\sqrt{14}} \end{pmatrix} \quad \text{(vii)}$$

Each K element can be calculated by using below equation

$$Q_{11} * R_{11} = K_{11};\ Q_{11} * R_{12} = K_{12};\ Q_{11} * R_{13} = K_{13};$$

$$Q_{21} * R_{11} = K_{21};\ Q_{31} * R_{31} = K_{31};\ Q_{21} * R_{12} + Q_{22} * R_{22} = K_{22}$$

$$Q_{31} * R_{12} + Q_{22} * R_{23} + Q_{31};\ Q_{31} * R_{12} + Q_{32} * R_{22} K_{32};$$

$$Q_{31} * R_{13} + Q_{32} * R_{23} + Q_{32} * R_{32} = K_{32};$$

Since K is symmetric, $K_{ij} = K_{ji}$. So,

$$K_{12} = K_{21};\ K_{13} = K_{31};\ K_{23} = K_{32}\,C;$$

3.3.2 Key Establishment

Two phases to establish pairwise key between sensor nodes:

Phase 1: Key Pre distribution: Row $r_x Q_{i\_j}$ from Q matrix and Column $c_x R_{i\_j}$ from the R matrix are preloaded into sensor nodes of its cluster's symmetric matrix. x-denotes row and column identifiers for example first row and first column.

Phase 2: Key establishment: Each sensor node transmits its column $c_x R_{i\_j}$. The reason to transfer its column is that the R matrix is an upper triangular matrix and some elements are zero, which takes less number of bits message to communicate. While evaluating energy consumption, computation (64 bit ALU operation) performed on a sensor node is equivalent to transmitting a single bit. Concentration should be given for transmission message also. Figure 3 shows the interaction between two nodes to establish the pairwise key.

It is thus possible to use the basic QR matrix based scheme to ensure a pairwise key between any two nodes for communicating in wireless sensor networks[11]. The same procedure is followed for communicating between cluster head and base station by preloading with its Q and R matrix rows and columns. In general different matrices are generated for each clusters and a single matrix between cluster head and base station.

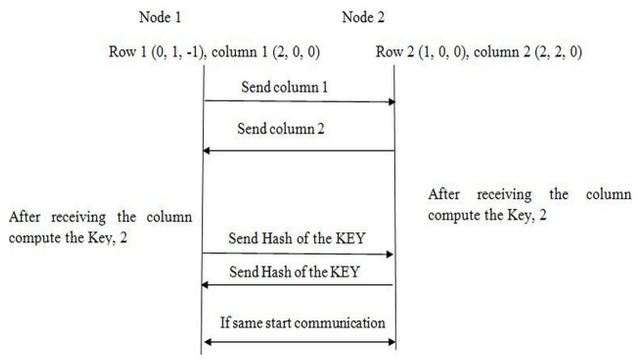

Figure 3. Handshake between two nodes.

4. Hardware Implementation

The proposed key management scheme is implemented in LPC2148 with Xbee to check its feasibility in real time applications. LPC2148 is a 32bit ARM7TDMA with 128 bit memory interface. For communication x bee is used as a transceiver. Experimental setup with coordinator (cluster head) and end device (sensor node) is shown in Figure 4.

Experimental setup shows that each device loaded with its rows and column as shown in Figure 5 and 6.

The pairwise key is established between coordinator and end devices as shown in Figure 7 and 8.

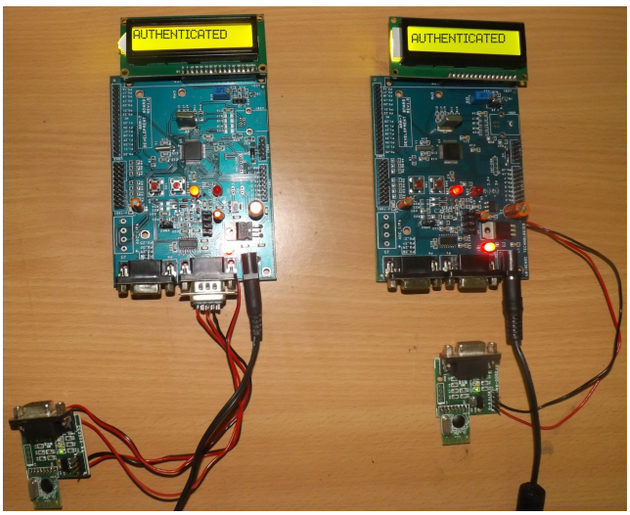

Figure 4. Hardware setup.

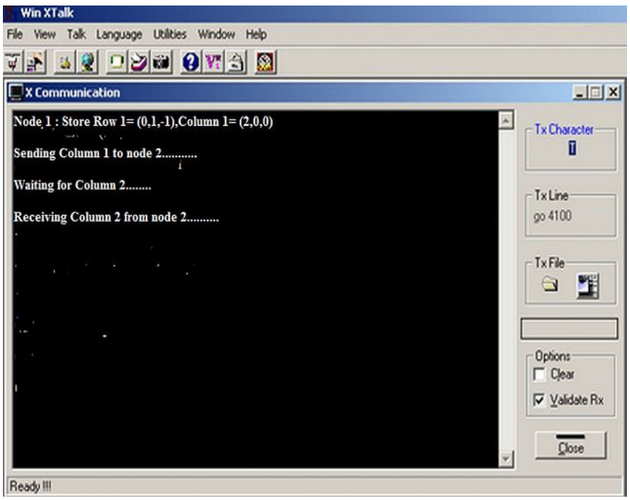

Figure 5. Node 1transmitting to node 2.

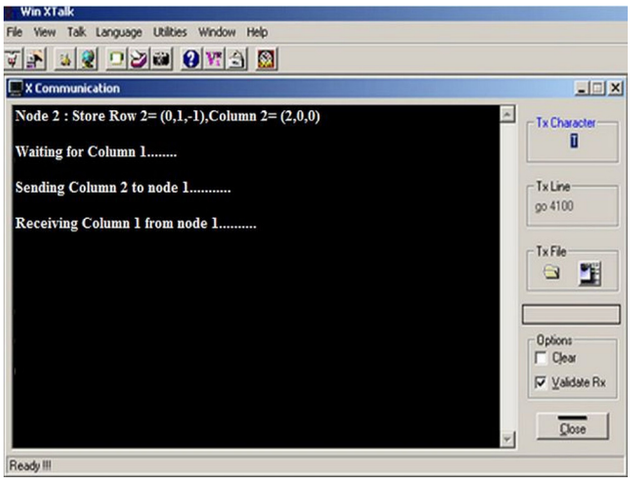

Figure 6. Node 2 transmitting to node 1.

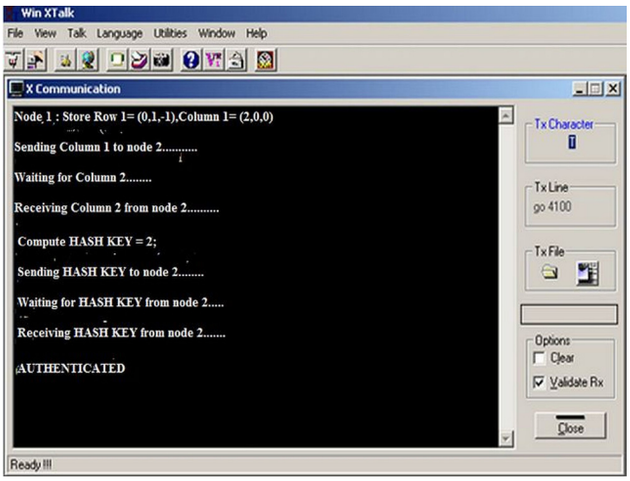

Figure 7. Key computed at node 1.

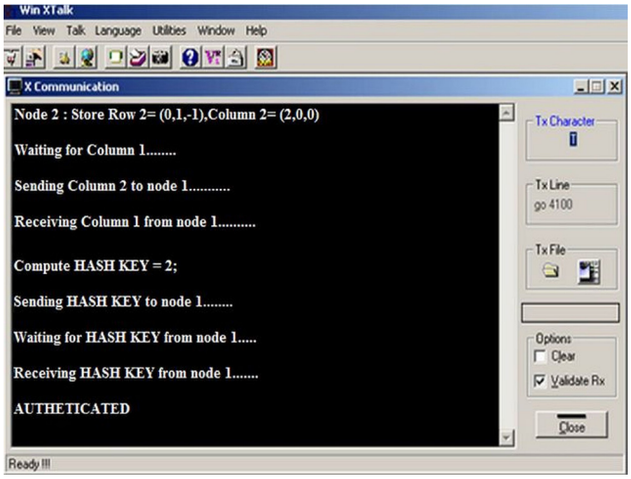

Figure 8. Key computed at node 2.

5. Performance Analysis

The proposed method achieves 100% key connectivity. In probabilistic based approach[12] if the keys loaded into nodes are enormous, probability of key connectivity will be high. By sacrificing memory constraint key connectivity can be obtained. In many cases the keys are directly loaded. So by capturing a minimum number of nodes the entire network will get revealed. But in this proposed work 100% connectivity is obtained without revealing any information as shown in Figure 9.

The proposed method provides good scalability because symmetric matrix decomposition is done at the base station (high end configuration) and there is no restriction on matrix size also. So if any new nodes are added to the sensor field unused row and its corresponding column of R matrix are preloaded.

In terms of resilience the proposed method works better. In most of the matrix based schemes rows and column are randomly selected and preloaded, so there is a chance of selecting the same row and column. But in this scheme none of the row and column is repeated. Rows and columns are preloaded in an orderly fashion. By doing so network resilience will be achieved.

5.1 Storage

Other than Rows and Column no other information related to keying is stored. Moreover, since the R matrix is upper triangular matrix and many elements are zero depending upon the column.

5.2 Computation

Compared to Blom's scheme computation cost is less. Though it is storing the seed alone to regenerate the column, the computation to generate the column will be more. The proposed schemes by single multiplication keys are generated.

Figure 9. Key connectivity.

5.3 Communication

Communication cost is reduced by using data compression technique. And the number of messages to establish a pairwise key is three alone.

6. Conclusion

The key management scheme is very important for WSN, because to secure the information in the network. In this scheme hierarchical network model with QR matrix based key pre distribution scheme is proposed and also analysis shows that the proposed schemes work better in terms of node connectivity, scalability and resilience and efficiency. Several security analysis can be performed on the proposed scheme to test the efficiency of the generated key for wireless sensor networks as a future work.

7. Acknowledgement

This work was supported by FIST Programme, Department of Science and Technology, India, Grant No:SR/FSC/ETI-371/2014 at SASTRA University, Tirumalaisamudram, Thanjavur.

8. References

1. Cui X, Zhang Y. A key management scheme based on cluster radiation matrix in WSN. IEEE International Conference on Computer Science and Electronics Engineering (ICCSEE); 2012.
2. Xu L, Zhang Y. Matrix-based pairwise key establishment for wireless mesh networks. Future Generat Comput Syst. 2014;30:140-5.
3. Data funnelling in wireless sensor networks: A comparative study. In: Ananda Kumar S, Ilango P, editors. Indian Journal of Science and Technology. 2015 Mar; 8(5):470–80.
4. Li-Ping Z, Yi W. An ID-based pairwise key predistribution scheme for wireless sensor networks. 2010 IEEE 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM); 2010.
5. Du W, Deng J, Han YS, Varshney PK, Katz J, Khalili A. A pairwise key predistribution scheme for wireless sensor networks. ACM Trans Inform Syst Secur (TISSEC). 2005; 8(2):228–58.
6. Wang EK, Ye Y. An efficient and secure key establishment scheme for wireless sensor network. IEEE 2010 Third

International Symposium on Intelligent Information Technology and Security Informatics (IITSI); 2010.
7. Eltoweissy M, Heydari MH, Morales L, Sudborough IH. Combinatorial optimization of group key management. J Netw Syst Manag. 2004; 12(1):33–50.
8. Wen M, Zheng Y, Li H, Chen K. A hierarchical composition of LU matrix-based key distribution scheme for sensor networks. Emerging Technologies in Knowledge Discovery and Data Mining: Springer; 2007. p. 608–20.
9. Devika R, Santhi B, Sivasubramanian T. Increase the lifetime of WSN by preventing sink isolation using supercluster formation. Indian Journal of Science and Technology. 2014; 7(4):92–8.
10. Bjorck A. Numerics of gram-schmidt orthogonalization. Lin Algebra Appl. 1994; 197:297–316.
11. Kodali RK. Key management technique for WSNs. IEEE on Region 10 Symposium; 2014. p. 540–5.
12. Doraipandian M, Rajapackiyam E, Neelamegam P, Rai AK. An efficient and hybrid key management scheme for three tier wireless sensor networks using LU matrix. Advances in Computing and Communications: Springer; 2011. p. 111–21.