International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-5 Issue-9, February 2016

ROMCOB - Reduced Overhead and Memory Consumption on Base Station with Improved LEACH Protocol for Clustered Wireless Sensor Networks

Parminder Kaur

Abstract: ***Wireless Sensor Networks (WSNs) are gaining popularity with each passing day because of their wide range of applications [1]. WSNs consist of sensor nodes, which are small in size and have wireless communication capability [2]. To increase the efficiency of the network, the sensor nodes are grouped in the form of Cluster, such a network of clusters is known as Clustered Wireless Sensor Network. In Clustered WSN, the base station keeps and maintains the record of all the sensor nodes in the network hence the load on the base station is more than any other sensor node in the network. This paper attempts to reduce the workload of base station, reduce memory consumption and maintains secure connectivity by using the concept of Exclusion Basis System (EBS) matrix. The paper is organized in five sections. Section I & II gives the overview of background and literature review. Section III explains the system architecture which gives the description of proposed scheme. Section IV describes the performance evaluation. Section V explains the future scope.***

Index Terms: ***WSN, Exclusion basis system, Key management, secure group communication.***

I. INTRODUCTION

Background Terminology

- **Sensor nodes:** The sensor node is an important component of Wireless Sensor Network (WSN). The sensor nodes are responsible for performing following functions: data gathering, sensing, routing, data processing, etc.
- **Clusters:** To improve performance and life of the network, the large sensor networks are divided into small groups. Each group is called a cluster and behaves as hierarchical unit for WSN.
- **Cluster Head (CH):** Each cluster has a leader or head of the cluster. CHs are responsible to control and organize the activities of the cluster. It performs data aggregation, organizes and maintains the communication schedule of the cluster.
- **Base Station (BS):** The Base Station (BS), also known as sink or command node, provides the link for communication between the sensor network and the end user.
- **End User:** End user is responsible for generating queries. It performs a wide range of applications based on the data received from the sensor network.

Manuscript published on 28 February 2016.
*Correspondence Author(s)
Parminder Kaur, Department of Computer Science and Engineering, Chandigarh University, Gharuan, Mohali, Punjab. India.

Clustered Wireless Sensor Network:

The system architecture for clustered WSNs is shown in Fig. 1.1. The network includes the Base Station (BS), gateways, and sensor nodes. Sensor nodes can communicate with each other if they are within certain range.

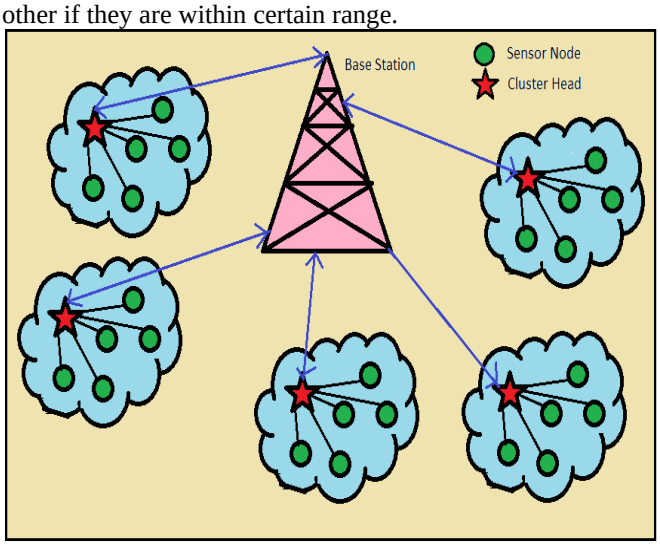


Fig. 1.1 Architecture of Clustered WSN

In clustered sensor networks, some sensors are elected as cluster heads (CHs) for each cluster created. Sensor nodes collects data in each cluster and transmit their data to the respective CH and the CH aggregates data and forwards to a sink node i.e. base station. Clustering provides the efficient utilization of limited energy of sensor nodes and hence extends life time of network. Clustering is proposed because of its network scalability, energy saving and network topology stability. Clustering schemes reduce the communication overheads among the sensor nodes [6]. Base Station is assumed to be secure and trusted by all the nodes in the network. Moreover, it is assumed that sensor and gateway nodes are stationary and all nodes are assumed to be aware of their position information.

II. LITERATURE REVIEW

A. Key Management in WSN

Key management is the set of techniques and procedures which support the establishment and maintenance of keying relationships between authorized parties, and covers the following:

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

- initialization of system users within a domain
- generation, distribution, and installation of keying material
- control over the use of keying material
- updating, revocation, and destruction of keying material
- Store, backup/ recovery and archival of keying material.

The fundamental function of key management schemes is the establishment of keying material, which in turn can be subdivided into agreement on a key and transport of this key.

A WSN key management scheme consists of three main components:

1) Key establishment
2) Key refreshment
3) Key revocation

Key establishment is about creating a session key between the parties that need to communicate securely with each other. Key refreshment prolongs the effective lifetime of a cryptographic key, whereas Key revocation ensures that an evicted node is no longer to able to decipher the sensitive messages that are transmitted in the network.

III. IMPROVED KEY MANAGEMENT SCHEME

A. *System Architecture*

This section explains the architecture for clustered WSN and proposed ROMCOB scheme. The system architecture represents the research work which includes the methodology adopted to reduce memory consumption as well as reduce overhead on base station while maintaining desired security.

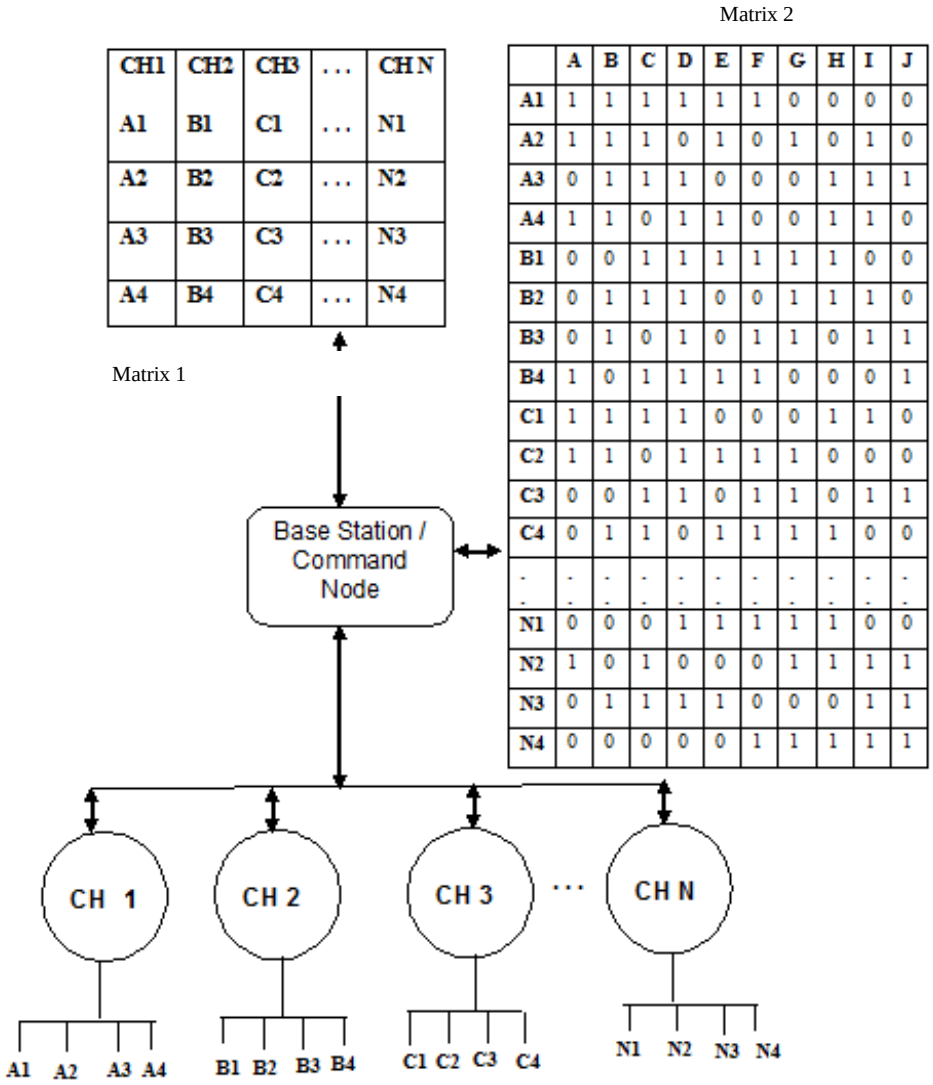


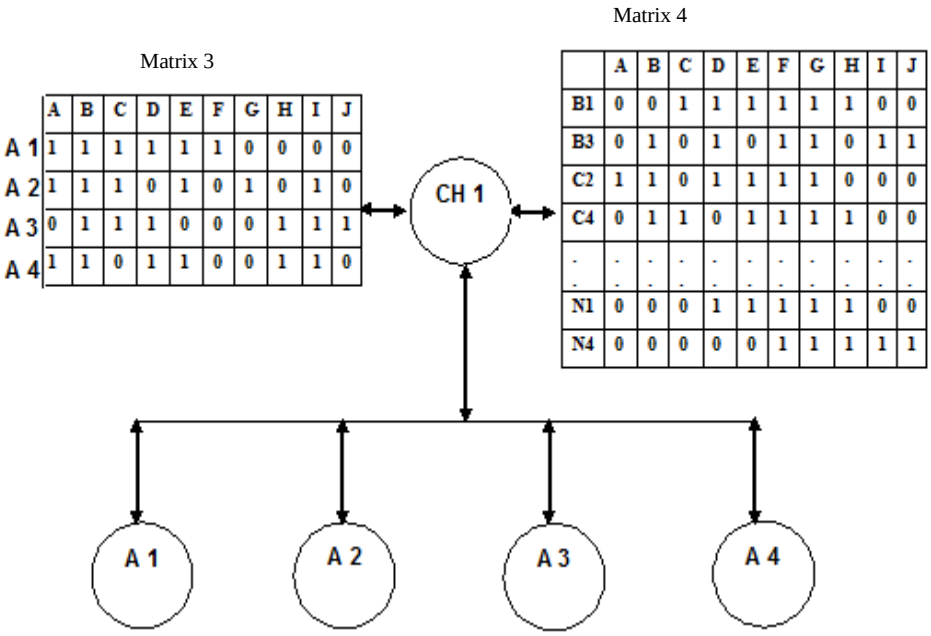
Fig. 1.2 Memory Status of Base Station

In Fig. 1.2, Base station (also known as Command node) is connected to the clusters, these clusters consists of tiny sensor nodes. Each cluster has a head of the cluster known as Cluster Head (CH). CHs are responsible to control and organize the activities of the cluster. The base station can reach each of the sensor nodes via cluster heads (gateway node). BS maintains two matrices:

(i) Matrix 1: store the ids of cluster heads (CH 1 to CH N) and sensor nodes (A1, A2, B1, etc.) within each cluster.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

(ii) Matrix 2: store the keys assigned to each sensor node in the network using Exclusion Basis System (EBS(10,6,4)). Keys are A,B,C,.....,J.



	A	B	C	D	E	F	G	H	I	J
A 1	1	1	1	1	1	1	0	0	0	0
A 2	1	1	1	0	1	0	1	0	1	0
A 3	0	1	1	1	0	0	0	1	1	1
A 4	1	1	0	1	1	0	0	1	1	0

	A	B	C	D	E	F	G	H	I	J
B1	0	0	1	1	1	1	1	1	0	0
B3	0	1	0	1	0	1	1	0	1	1
C2	1	1	0	1	1	1	1	0	0	0
C4	0	1	1	0	1	1	1	1	0	0
. .	. .	. .	. .	. .	. .	. .	. .	. .	. .	. .
N1	0	0	0	1	1	1	1	1	0	0
N4	0	0	0	0	0	1	1	1	1	1

Fig. 1.3 Memory Status of Cluster Head

As shown in Fig. 1.3 the cluster head is assumed to consist of four sensor nodes (this range can be much larger in actual). The cluster head stores two matrices:

(i) Matrix 3: to store the ids and assigned keys of sensor nodes within that cluster.

(ii) Matrix 4: to store the ids and assigned keys of few most recently communicated nodes of other clusters.(Hence the memory consumption is reduced as the CH has to store only few most communicated nodes instead of all the nodes)

All matrices are interconnected to tha tables stored at Base Station. After fixed time intervel when the keys are reshuffled (for security reasons) at the matrix 2 (Base Station), the corresponding matrices will be updated accordingly.

Cluster head keeps the details of ids and assigned keys of its sensor nodes. It also maintains the ids and key details of most recently communicated nodes of other clusters. Whenever a sensor node wants to communicate with another sensor node it sends the request message to its CH for connection establishment. The format for request message is REQ(source id, destination id, message). The CH receives the REQ message, it checks the source id and destination id, if the source node and destination node share the same cluster then there is no need of matching the keys for intra-cluster communication. If the destination id is inter-cluster then CH check the Matrix-4, if the destination id exists in the most recently and regularly communiacted nodes then retrieves the keys from the matrix 4, if the destination id does not exist in the matrix 4, only then CH refers to the BS. After retrieving keys from the BS, key details of destination id are stored in matrix-4 by replacing the key details of least recently communicated node. The keys of destination id and source id are matched at the CH of destination cluster, hence reducing the overhead at BS. In previous key management schemes the keys are matched at BS but in proposed scheme the BS doest not participate in key matching.

If the keys are matched then CH sends the 'Key_Matched_ACK' acknowledgement to the source node and establishes the connection between the source and destination nodes. If the keys do not match the CH will send a negative acknowledgement, NACK, to the source node and discards the request message.

In previous key management schemes CH keeps the details of all the sensor nodes of each cluster, hence the memory consumption at each CH is very large. The proposed scheme reduces the cost of memory consumption by minimizing the size of table by only keeping the details of recently communicated nodes of other clusters. The idea is taken from the mobile phones and chat messangers, as the mobile phones and chat messangers consists the most recently communicated name/number/id in recent conversations. The phonebook and address list is refered only if the required name/number/id doesnot exist in the recent conversations. Hence the cost of memory consumption at CH is reduced by maintaing the details of few sensor nodes (most recently communicated). The same procedure is done at other CHs

IV. PERFORMANCE MATRICES

This is the performance diagram of improving the memory consumption. The observation includes:

- The keys are assigned according to EBS matrix.
- Node receive unique combination of keys.
- The node sends request to the CH for communication with the destination node.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

- CH checks the keys and as the authorized nodes can communicate if they have at least two shared keys. If the keys are not matched then the authentication of communication is discarded.

The graph shows the comparison of proposed scheme with previous key management schemes in terms of memory consumption and reduced overhead on base station.

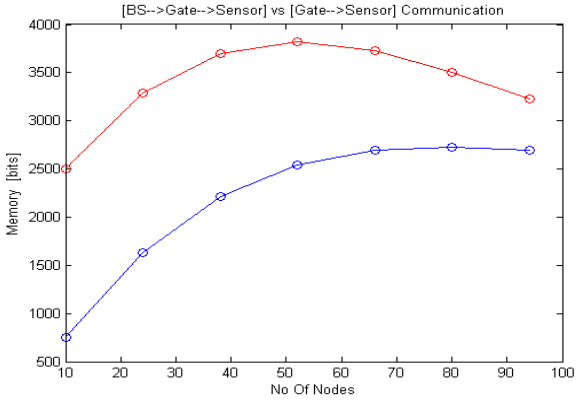


Fig.1.4. Proposed scheme (in terms Cost of memory consumption)

As shown above the blue line shows the result of proposed scheme with reduced memory consumption. Following is the comparison of Previous key Management schemes and the proposed improved key management scheme.

ROMCOB	LEACH Schemes
Reduced Memory consumption: The memory consumption is reduced in this scheme as there is only one main table at the base station which includes the key assignment details and node details in the network. The tables at cluster head include only the recently used communication details instead of complete details of all the nodes.	**More Memory consumption:** The memory consumption is more as each cluster head stores the details of all the nodes of the network, whether they are needed for the communication or not.
Reduced overhead on Base Station: In this scheme the matching of keys is done at Cluster head of respective cluster, therefore, for key matching the reference of Base station is reduced and hence the overhead too.	**More overhead on Base Station:** The matching of keys is done at Base Station and hence every time if there is a request (by sensor nodes) of connection establishment the cluster head refers to the base station for matching of keys.

Proposed scheme Vs Previous key management scheme

V. FUTURE WORK

The future work includes the Self-healing of lost keys, recover data, and detection of compromised keys in clustered wireless sensor network. The main property of self-healing key distribution is that the sensors are capable of recovering lost session keys by itself, without requesting additional transmissions from the cluster head or Base station. The objective is to determine the key which may be lost during transmission. The data can be recovered which was lost during the sleep mode of node or during the session when key was lost. In case any of the nodes is found to be compromised, the keys of the compromised node needs to be detected and regenerated. Hence the future scheme can provide a hybrid of secure communication, and self-healing of lost keys.

REFERENCES

1. Reza Azarderakhsh, Arash Reyhani-Masoleh, and Zine-Eddine Abid. “A key management scheme for Clustered wireless sensor networks”, IEEE/IFIP, International Conference on Embedded and Ubiquitous Computing, 2008.
2. Mohamed F. Younis, Senior Member, IEEE, Kajaldeep Ghumman, and Mohamed Eltoweissy, Senior Member, IEEE, “Location-Aware Combinatorial Key Management Scheme for Cluster Sensor Networks”, IEEE Trans. on Parallel and Distributed Systems, Vol.17, No.8, August 2006.
3. Li Zheng, Wei Guoheng, and Waang Ya. “Key-management scheme based on identity and cluster layer in wireless sensor network”, IEEE workshop on Advanced reaearch and Technology in Industry Applications (WARTIA), 2014.
4. Rong Jiang, Jun Luo, Fang Tu, and Jin Zhong, “LEP: A Lightweight Key Management Scheme based on EBS and Polynomial for Wireless Sensor Networks”, International Conference on Signal Processing, Communications and Computing (ICSPCC), 2011.
5. Ian Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. “A survey on sensor networks” IEEE Communications Magazine, vol. 40.
6. Rabia Riaz, Arshad Ali, Ki Hyung Kim, H. Farooq Ahmad, and Hiroki Suguri, “Secure dynamic key management for sensor networks” IEEE 2006.
7. Kamal Kumar, A.K. Verma, and R.B. Patel, “Framework for key management scheme in heterogeneous wireless sensor networks”, Journal of emerging technologies in web intelligence, vol. 3, no. 4, November 2011.
8. Olutayo Boyinbode, Hanh Le, Audrey Mbogho, Makoto Takizawa, and Ravi Poliah, “A survey on clustering algorithms for wireless sensor network”, 13th International Conference on Network-Based Information Systems, 2008.
9. I.F. Akyildiz et.al., “Wireless Sensor Networks: a survey, computer networks”, vol. 38, pp. 393-422.
10. S. Tanenbaum, Computer Networks, 4th ed. NJ: Prentice Hall.
11. W. Stallings, Cryptography and Network Security-Principles and Practices, 3rd -ed. Upper Saddle River, NJ: Prentice Hall.
12. Minghui Shi and Xuemin Shen, Yixin Jiang and Chuang Lin, “Self-healing group-Wise Key Distribution Schemes with Time-Limited Node Revocation for WSN”, IEEE Wireless Communications, October 2007.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

13. D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," IEEE Commun. Surveys Tutorials, vol. 7, pp. 2–28, 2005.
14. Ossama Younis, Marwan Krunz, and Srinivasan Ramasubramanian, "Node clustering in wireless sensor networks: Recent developments and deployment challenges", IEEE Network, May/June 2006.
15. Johnson C. Lee, Victor C. M. Leung, Kirk H. Wong, Jiannong Cao, and C. B. Chan, "Key management issues in wireless sensor networks: current proposals and future developments", IEEE wireless communications, pp. 76-83, October 2007,
16. R.C. Johnson. Sandia enlists MEMS for anti-terror systems. EE Times, March 2002. URL http://www.eet.com/at/news/OEG20020514S0033.
17. G. Boone. Reality mining: Browsing reality with sensor networks. Sensors, vol. 21, no. 9, September 2004. URL http://sensorsmag.com/articles/0904/14/main.shtml.
18. J. Kloeppel. Smart bricks could monitor buildings, save lives. News Bureau, University of Illinois at Urbana-Champaign.
19. Intel Corporation. Intel Research–Exploratory Research–Deep Networking. http://www.intel.com/research/exploratory/heterogeneous.htm
20. B.J. Feder. Wireless Sensor Networks Spread to New Territory. The New York Times, July 2004. URL http://www.nytimes.com/2004/07/26/business/26sensor.html.
21. K. Mayer. Instrumenting cattle – real time health monitoring of cattle using wireless technologies. Poster for Sir Mark Oliphant Conference 2004 "Converging Technologies for Agriculture and Environment", August 2004. URL http: //mobile.act.cmis.csiro.au/kevin/smartsensors2004.pdf
22. Alan Mainwaring, David Culler, Joseph Polastre, Robert Szewczyk, and John Anderson. Wireless sensor networks for habitat monitoring. In Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, pages 88–97. ACM Press, 2002. ISBN 1-58113-589-0.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)