Volume: 10 Issue: 02 Pages: 3794- 3799 (2018) ISSN: 0975-0290

Secured Dynamic Clustering using Light Weighted Key Authentication for Target Tracking in WSN

RAMESH. D
Research Scholar, VTU-RC, Dept. of ECE, PDACEG, Gulbarga, India
E-mail: ramesh.dhavalegar29@gmail.com
G. S. BIRADAR
Professor, Dept. of ECE, PDACEG, Gulbarga, India
E-mail: gsbiradar@yahoo.com

ABSTRACT

Many significant development in communicating with WSN has been developed, to secure the communication among the cooperative sensor nodes, a strong security concepts have been implemented, concerned to the object tracking in WSN, since the object is freely moving in and around the network so as the topology changes as the movement of object. Senor nodes are limited to energy usage and it is battery operated, energy and security is one of the major constrains in object tracking. In this paper, we propose a Light weighted key management technique for object tracking (LWKMOT) to secure the object moving in the network; dynamic clustering method is used to minimize the overhead of the network. In this system dynamic key generation system is adopted, the advantage of this method is to provide security protection, by generating different keys thus attacker cannot use the previous key to cheat.

Keywords **- Dynamic clustering, Key management scheme, Target Tracking, Wireless sensor networks.**

Date of Submission: July 30, 2018 Date of Acceptance: Aug 21, 2018

I. INTRODUCTION

Wireless Sensor Network (WSN) with distributed nodes collaboratively sense physical phenomena of surroundings and send sense information to the sink node through single-hop or multi-hop paths. Communication and data transfer between the devices should be more secured and efficient. Authenticating multiple devices is challenging to provide secure communication. Application area of WSN [1] are wide, these sensors has a capability to sense the intruder or moving object and update tracking report to BS or sink[2].

Optimizing usage of power in wsn is a key factor in designing of sensor node. Many techniques have been proposed to optimize the energy consumption and load balancing of the node.[3][4]. The object tracking method in WSN is considered as an important, such that the data are passed to the sink as the object moves. The monitoring of moving object has to be tracked to get the updated information of the moving objects [5] [6].

Since the WSN are deployed in open environment, the attacks and malicious activities have been increased. Securing the data and communication between the trusted authorities in a secured manner is a challenging issue in the WSN [7]. A security is a major issue in WSN as it is open to nature and unsecured [8]. Several approaches have been proposed for secure communication to achieve security goals for providing data confidential and integrity. Sensor nodes which collects data periodically, transmits the collected information to BS in a single or multihop transmission. For different applications of WSN the data aggregation is done to reduce the communication overhead and sends the aggregated data like pressure counts and average sum, this aggregation information are monitored and computed by the BS [9][10][11]. Secure and reliable transmission can be achieved by using an encryption and decryption techniques, which have been proposed by several authors. To secure communication the network has a key management setup where encryption keys are distributed to nodes, this involves in generation of keys, distribution and revocation of keys [12]. In this paper, a light weighted key management system is used to authenticate the moving object and to provide secure communication with BS. This key management system applies to dynamic wsn, where the moving object keeps changing its position. Light weighted key management scheme supports object tracking, whenever the object joins and leaves the cluster, thus providing a secure communication between cluster and BS. Summarization of the paper is given below

Weakness of the existing system is shown

Propose secure object tracking for WSN, using light weighted key management system. Which reduces the communication overhead of the nodes.

Proposed LWKMOT scheme is simulated in an event driven simulation tool, and network parameters throughput, energy consumption and overhead is evaluated.

The rest of the paper is organised as follows, section II describes the related works.

II. RELATED WORKS

Lee et al [13], proposed scheme to reduce energy consumption using prediction results in dynamic clustering for moving objects which avoids redundant

Volume: 10 Issue: 02 Pages: 3794- 3799 (2018) ISSN: 0975-0290

data. The scheme is evaluated using simulation tool and the efficiency is justified by the author.

In another tracking based, author Deldar et al [14], presented a scheme for tracking nodes based on localization algorithms, which takes node distance and energy. This scheme showed decrease in energy consumption and efficiency in extending network life time. The simulation results have been verified using OPNET simulator

Many Security schemes have been proposed by authors, the past scheme have been focused for static network. Few approaches are concentrated on dynamic sensors. Authors Chuang et al [15] and Agrawal et al [16] presented key management scheme for dynamic WSN using PKC. This scheme is based on Diffie-Hellman, to update key dynamically. However the disadvantage of this scheme was unable to compute of large key sizes and was consuming more communication overhead. Zhang et al. [17] proposed security management system for dynamic WSN using ECC. This approach uses symmetric key pairwise key exchange for existing node and asymmetric approach for new node joining the network, but this approach had a disadvantage of key resilience. Abdoulaye et al [18] proposed an Efficient and Secure Key Management Scheme (ESKMS) for Hierarchical Wireless Sensor Networks (HWSNs) to distribute the keys within a cluster and update the keys at regular interval to avoid node capturing problem. ESKMS use one way hash function, data encryption and message authentication code to authenticates the communicating nodes and update the pre-deployed network keys. In fact, if an intruder manages to capture a node, then an encryption mechanism should be present to restrict the access of intruder to the message history of node. This procedure ensures that intruders cannot acquire the keys easily, and also avoid a different type of attacks from malicious nodes. Du et al. [19] use a ECDSA scheme to verify the identity of a cluster head and a static EC-Diffie-Hellman key agreement scheme to share the pairwise key between the cluster heads. Therefore, the scheme by Du et al. is not secure against known-key attacks, because the pairwise key between the cluster heads is static.

III. NETWORK MODEL

In this approach, a dynamic cluster formation is done; the formation of the cluster takes place by sending beacon signals periodically to the neighbour nodes. After the cluster formation, the cluster head (CH) is elected based on the residual energy. CH is responsible for monitoring the cluster members (CM) and transmitted the aggregate data to the Base Station (BS). Consider WSNs with a base station BS and H no of cluster heads and n number of sensor nodes in the network. The sensor node sends data to the CH and CH aggregates these data and communicate the same to BS. BS is considered with unlimited network resources. Sensor nodes, CHs, and BS are stationary in nature.

Formation of the cluster takes place by broadcasting Hello message to its neighbour within communication range. The Beacon signals are sent to the neighbours once the cluster is formed. Cluster Head is elected based on the high residual energy and each cluster is coordinated by CH, CH aggregates cluster members data before sending to BS. The gateway to connect to other network is BS, which has efficient data processing and controls the network. The key components of our proposed LWKMOT are CH (Cluster Head), BS (Base Station), and Key Management unit. However in wireless sensor network, the node mobility plays crucial roles for different applications. Moving node may join and leave the cluster at any point of time. For application like object tracking, dynamic clustering is necessary to track the moving object and report it to BS. In our proposed method the dynamic clustering is used and the formation of the cluster is as follows

a) Network Division Phase

Node are randomly deployed, overall network is divided into unequal size of rectangular grids. This grid forms a cluster with its unique cluster ID. Base station is deployed at the top of the grid area. X-axis of the rectangular area varies with the width (w) levels varying from 1 – n. This lane width varies linear distance to Base station.

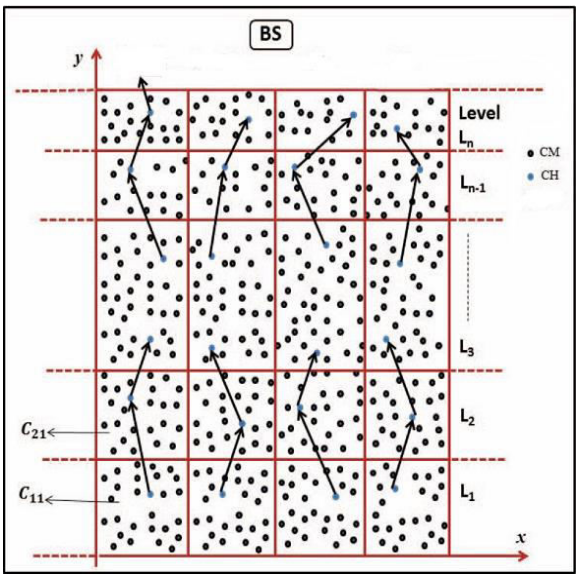

Fig 1: Grid Layout

The cluster head i is elected based on the high residual energy, with time probability Pb (t). If there are N number of nodes in network

$$E\ (CH) = \sum_{i=1}^{N} P\ b(t) * 1$$

Volume: 10 Issue: 02 Pages: 3794- 3799 (2018) ISSN: 0975-0290

Algorithm for dividing network to cluster grids

Initialising parameters: sensing axis (X, Y), Tx range x_0

Step 1: Sensing areas are divided into width varying from low level to high and assigning IDS. Initializing parameters are
y=0, n =1, W = $x_0/\sqrt{5}$

Step 2: while (y < Y)

Step 3: Compute width level, w = W – m* y

Step 4 : Generate horizontal level ids L_n from y and (y + w)

Step 5: Divide levels to form cluster grids and initialize x =0, i =1

Step 6 : if (x < X)

Step 7: Generate cluster id to rectangular grid

Step 8 : x = x + W

Step 9 : Increment i

Step 10 : end while

Step 11: y = y + w

Step 12 : Increment n

Step 13 : end while

Step 14: Decrement n and i

Step 15 : clusters formed (grid) , q = n * i

Allowing each node to become cluster head in a time period $\frac{N}{K}$, to balance the load and energy of the nodes. $Ci\ (t)$ indicates whether node i is CH in recent time rounds (r mod $\frac{N}{K}$) giving chance to become CH for other nodes with time probability

$$P\ b\ (t) = \begin{cases} \frac{k}{N - k*(r\ mod\ \frac{N}{k})} & :\ Ci\ (t) = 1 \\ 0 & :\ Ci\ (t) = 1 \end{cases}$$

This gives the result of nodes that are not being cluster head recent, and their residual energy is high and can become next cluster head. Cluster head selection is based on the probability on assuming all the nodes are given same initial energy and node has a data to transmit. This can be achieved by using

$$Pb\ (t) = \min \left\{ \frac{Ei(t)}{Etotal(t)} k, 1 \right.$$

b) Proposed LWKMOT scheme

Light weighted key management process starts with three phase, first key distribution, second initialization of network and third authentication process

c) Key distribution phase: this phase is mainly concentrated on dynamic moving nodes. This phase starts with generating and storing of symmetric key after the nodes being deployed and has to update to BS about their locations. Nodes broadcast Hello packet for authentication process, thus it uses the initial key

$B_j \rightarrow$ broadcast: E (K_{init}, Hello)

Initial authenticator is installed in each node ∇_i used to identify another node, this include random hashed key and tuples. In the first authentication process, the master key is generated when the initial node deployment is done

$K^0_{auth} = k_M$

$\nabla^0 = \{(r_i, [r_i]k_m)\}$, i=0,.....n-1

d) Network Initialization Phase: In this phase, the nodes calculates its neighbour distance to find within the communication range, this involves

- The node encryption key is generated by using unique ECC symmetric key, k^i_{enc} for all the nodes i using random number $k^i_{enc} = [\ k_M, r_i]$.
- Node broadcast random value, upon receiving random value, neighbour node generates a store list and calculates common master key used and paired keys of neighbour nodes. Node uses hashing scheme to hash the master key for authentication $k^1_{auth} = k_M$.
- The set encryption key k^i_{enc} of neighbour node and the next cycle of authentication key k^1_{auth} is stored in each node.
- Using encryption paring key the node starts to communicate with another node.

On cluster formation, the CH is elected based on high residual energy and the dynamic CH is formed from the above equations. Upon receiving the message and key, the node intend to join cluster replies with its response ID and ACK

CH assigns, CM ids to all nodes that intend to join cluster and sends the updated information to the base station. The base station initializes the light weighted key management set up to authenticate all the nodes and cluster from BS. CH collects the data from the moving object and updates its information to BS.

Dynamic cluster head formation takes place, when the object leaves and joins the other cluster; in this process the formation of new cluster head takes place by sending request packet to BS by suing the encryption key to authenticate itself as node. BS broadcast the reply message to all nodes to guarantee the data integrity of nodes to track malicious activity.

Volume: 10 Issue: 02 Pages: 3794- 3799 (2018) ISSN: 0975-0290

e) Authentication Phase: This phase authenticates each node for communication and enables secure communication to BS. This process verifies the new cluster head for object tracking method.

The authentication cycle j starts from constructed keys of previous cycle j-1. The master key is verified in this way.

New cluster head authentication with random number is applied using k^{j}_{auth}

$$\nabla^{j+1} = \{(r_i, [r_i]k^{j}_{auth})\} \text{ , i=0,.....n-1.}$$

Hashed updated key is

$$k^{j+1}_{auth} = [k^{j}_{auth}]$$

The new key generated is

$$[k^{j+1}_{auth}, \nabla^{j+1} = \{(r_i, [r_i]k^{j}_{auth})\}] \text{ , i=0,.....,n-1}$$

When the moving object moves from one region to another region, the dynamic cluster formation takes place, when the objects enters into new cluster region, the new cluster head authenticates itself to BS by the following steps:

- Cluster head produces random number r_A, then sends message to base station

$$M_1 = r_A$$

- Base station upon receiving will perform the cluster head key function k^{j-1}_{auth} to obtain

$$[r_A]\, k^{j-1}_{auth}$$

- Recovers it encryption key k^{B}_{enc} to obtain $\{k^{B}_{enc}\}$ k^{j}_{auth}

- To synchronization with cluster head, CH sends the following message

$$M_2 = \{r_B, [r_A]\, k^{j-1}_{auth}, \{k^{B}_{enc}\}k^{j}_{auth}, j\}$$

- After receiving M2 from BS the cluster head performs j-1 hash k_M to obtain $k^{j}_{auth} = [k_M]^{j-1}$ to synchronize with BS, and checks for correctness by comparing received key values.

- Own Encryption key is generated using k^{A}_{enc} to obtain $\{k^{A}_{enc}\}k^{j}_{auth}$

$$M_3 = \{[r_B]\, k^{j}_{auth}, \{k^{A}_{enc}\}k^{j}_{auth}\}$$

- Finally, the new cluster head is authenticated by sending M3 from CH to BS and allowed to communicate with BS and update the object location to BS

f) Performance Evaluation

The evaluation of the proposed scheme is discussed in this section; our scheme is to solve the security issues in dynamic clustering based object tracking. We compare the performance of the proposed light weighted key generation scheme with Localized Combinatorial Keying (LOCK) further more we compare the energy consumption of the nodes. The simulation is carried on Network simulator tool (NS2) an event driven simulator tool. The configuration of the simulation is shown in the below table.

Table 1: Simulation Parameters

Parameters	Values
Deployment Layout	Grid
Deployment Area	500 x 500
No of nodes	80
Bandwidth	2Mb
Mobility Model	Random Mobility Model
Traffic Type	CBR
Transmission Range	250 mts
Attacker Nodes	2-10
Initial Energy	30 Joules
Propagation Model	Two Ray Ground
MAC Type	802.11

The simulation has been carried on different scenarios and network parameter has been evaluated. The sensor nodes are deployed in a grid position. Random way point model is used for tracking object which moves randomly in a grid area. As the object moves randomly, the formation of dynamic clustering takes place. CH is elected based on high residual energy and the dynamic CH is formed on the rotation basis. CH is responsible to authenticate moving object and forward the tracking information to BS. Proposed light weighted authentication scheme detects the misbehaving activities efficiently, consumes less energy and reduces the overhead of the overall network communication. The proposed LWKMOT is compared with the LOCK (Localized Combinatorial Keying) method and parameters are evaluated. In the below Figure 2 shows the packet delivery rate, where the packet drop ratio increases with the malicious activity, the proposed method will send only authenticated packets to destination, which reduces the error rate.

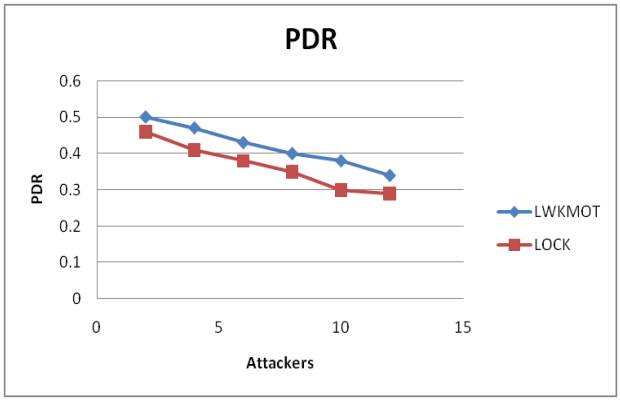

Fig 2: Packet Delivery Ratio

Volume: 10 Issue: 02 Pages: 3794- 3799 (2018) ISSN: 0975-0290

Figure shows the relationship in forming dynamic cluster by ratio of transmission range (t_x) to the sensing range (r_x). If the transmission range is extended means the increases in static clustering. Dynamic clusters are formed when the $^{t_x}/_{r_x}$ falls to lower ratio.

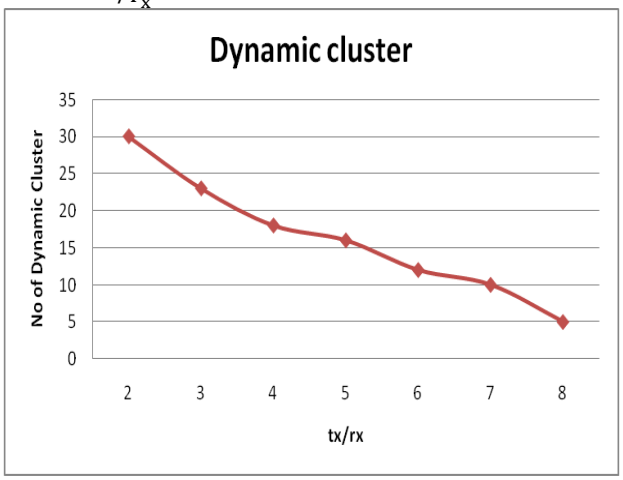

Fig 3: Dynamic Clustering

Periodically the energy levels of the nodes are updated, each node knows the adjacent nodes energy levels, updating energy levels helps in electing CH based on the high residual energy. Based on the energy usage, each node detects the actual energy level for transmission. In case of compromised node, energy level of the node should not be greater than the predicted energy level, predicted level is calculated based on actual detected usage. In the below graph, the node's transmission energy is measured, comparison of LOCK and proposed light weighted method is shown. The energy consumption of node increases when more number of malicious nodes is present in the network, this results in error in packets. Cluster head authenticates malicious node and filters error packets from spreading into the network, thus reducing the energy. In LOCK the CH must generate the key and update the key to the BS when the object is detected in the cluster region and distributes the key to its members by using key generation node technique, which consumes more energy and more network overhead.

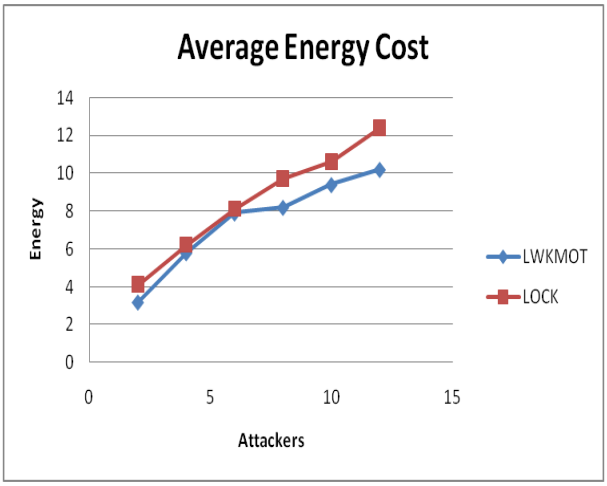

Fig 4: Energy Consumption

In Figure 5, shows the resilience of the network percentage. The proposed LWKMOT scheme avoids malicious activity in the network and increases network rate in presence of attackers. Proposed system can capture hidden keys from the nodes before distribution and updates keys to detect compromise node. In LOCK the key is reused to introduce more malicious nodes into the network, which degrades the network.

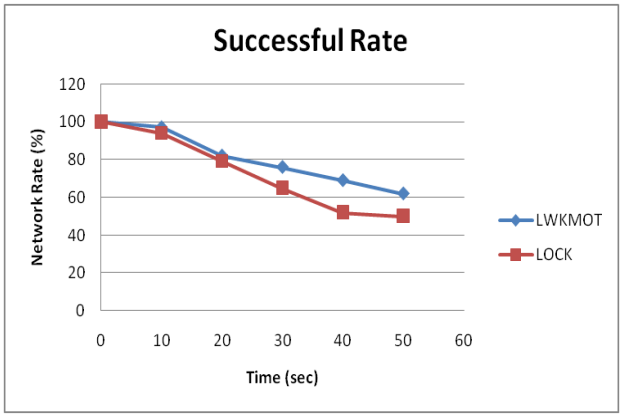

Fig 5: Network Rate

IV. CONCLUSION

Malicious activity in the network causes nodes to become compromise and tries to drain the energy, which is the main constrain of WSN. Authenticating and securing the network from malicious activities increases efficiency of the overall network. In this work a Light Weighted Key Management Scheme for Object Tracking (LWKMOT) for WSN is proposed, the network is first divided into grids to form cluster and CH is elected based on the high residual energy. The moving object is been tracked, as the moving object moves randomly, the dynamic cluster formation takes place and CH formed. The CH authenticates from the BS using light weighted key management and sends the object tracking information to BS. The proposed scheme reduces the overhead of the nodes and delivers the packets efficiently by detecting and avoiding the malicious activity.

REFERENCES

[1] Bhatti, S and Jie Xu, "Survey of Target Tracking Protocols using Wireless Sensor Network," The Fifth International Conference on Wireless and Mobile Communications, pp. 110-115, Cannes/La Bocca, French Riviera, France, August 23-29, 2009.

[2] Hua-Wen Tsai, Chih-Ping Chu and Tzung-Shi Chen, "Mobile Object Tracking In Wireless Sensor Networks," Computer Communications, Volume 30, Issue 8, pp. 1811–1825, 2007.

[3] Sung-Min Lee, Hojung Cha and Rhan Ha, "Energy-aware location error handling for object tracking applications," Computer Communication, volume 30, issue 7, pp. 1443-1450, 2007.

Volume: 10 Issue: 02 Pages: 3794- 3799 (2018) ISSN: 0975-0290

[4] Yingqi Xu and Wang-Chien Lee, "On localized prediction for power efficient object tracking in sensor networks," In Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops, pp. 434–439, Province RI, USA, 29-29 May, 2003.
[5] G. Hoblos, M. Staroswiecki, A. Aitouche, "Optimal design of fault tolerant sensor networks," In proceeding of: Control Applications, 2000. Proceedings of the 2000 IEEE International, pp. 467- 472, Anchorage, Alaska, USA September 25-27, 2000.
[6] Ian Akyildiz and Mehmet Can Vuran, Wireless Sensor Networks. John Wiley and Sons, 2010.
[7] E. E. Papalexakis, A. Beutel, and P. Steenkiste, "Network anomaly detection using co-clustering," in *Proc. 2012 Int. Conf. Advances in Social Networks Anal. and Mining (ASONAM 2012),* 2012, pp. 403-410.
[8] Lidong Zhou and Zygmunt J. Haas, ''Securing Ad Hoc Networks'', IEEE Network, November 1999.
[9] Z. Cai, S. Ji, J.S. He, and A.G. Bourgeois, "Optimal Distributed Data Collection for Asynchronous Cognitive Radio Networks," Proc. IEEE 32nd Int'l Conf. Distributed Computing Systems (ICDCS), pp. 245-254, 2012.
[10] S. Ji and Z. Cai, "Distributed Data Collection and Its Capacity in Asynchronous Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 2113-2121, Mar. 2012.
[11] S. Ji, R. Beyah, and Z. Cai, "Snapshot/Continuous Data Collection Capacity for Large-Scale Probabilistic Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 1035-1043, Mar. 2012.
[12] Johnson C. Lee, Victor C. M. Leung, Kirk H. Wong, Jiannong Cao and Henry C. B. Chan, "Key Management Issues In Wireless Sensor Networks: Current Proposals and Future Developments", IEEE Wireless Communications • October 2007.
[13] In-Sook Lee, Zhen Fu, WenCheng Yang and Myong-Soon Park, "An Efficient Dynamic Clustering Algorithm for Object Tracking in Wireless Sensor Networks," DCDIS series B ,Vol.14(S2),Complex system and application-Modeling Coontrol and Simulation, pp. 1484-1488, 2007.
[14] Fatemeh Deldar and Mohammad Hossien Yaghmaee, "Energy Efficient Prediction-based Clustering Algorithm for Target Tracking in Wireless Sensor Networks," International Conference on Intelligent Networking and Collaborative Systems, Thessaloniki, Greece, pp. 315-318, 24-26 Nov. 2010
[15] I.-H. Chuang, W.-T. Su, C.-Y. Wu, J.-P. Hsu, and Y.-H. Kuo, "Twolayered dynamic key management in mobile and long-lived clusterbased wireless sensor networks," in *Proc. IEEE WCNC*, Mar. 2007, pp. 4145–4150.
[16] S. Agrawal, R. Roman, M. L. Das, A. Mathuria, and J. Lopez, "A novel key update protocol in mobile sensor networks," in *Proc. 8th Int. Conf. ICISS*, vol. 7671. 2012, pp. 194–207.
[17] X. Zhang, J. He, and Q. Wei, "EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2011, pp. 1–11, Jan. 2011.
[18] Abdoulaye Diop "An Efficient and Secure Key Management Scheme for Hierarchical Wireless Sensor Networks" International Journal of Computer and Communication Engineering, Vol. 1, No. 4, November 2012.
[19] D. Du, H. Xiong, and H. Wang, "An efficient key management scheme for wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 2012, Sep. 2012, Art. ID 406254.

Authors' Profiles

Ramesh. D received B. E. Degree from P.D.A.College of Engineering Gulbarga, Gulbarga University, Karnataka, India in 1994 and received M.Tech from the Indian Institute of Technology Kharagpur India, in 2001 , He is a research scholar registered in Visvesvaraya Technological University (VTU), Belagavi, Karnataka, India and is presently working as an Associate Professor in Department of ECE , BKIT Bhalki Karnataka, India. He has 21 years of experience in teaching. His research field is Wireless Sensor Networks. And life member of ISTE and IETE

Dr. G.S. Biradar received the B. E. degree in Electronics and Communication Engineering from Gulbarga University, Karnataka, India, in 1990, M.Tech. degree in Telecommunication Systems Engineering from the Indian Institute of Technology Kharagpur India, in 2002 and Ph.D degree from Indian Institute of Technology Mumbai, India, in 2010. Presently he is working as a professor in ,department of P.D.A. College of Engineering Gulbarga, Karnataka (An autonomous institute affiliated to VTU, Belagavi, Karnataka) . He has more than 24 years of experience in teaching and research. His broad area of research interest is in wireless communication, wireless sensor networks, multiuser detectors, ultra wide band communication and signal processing and has published extensively in these areas.

He is a reviewer for many leading international and national journals and conferences. He has published five international journal papers and twenty-seven international conference papers. He is a recipient of best technical paper award of Shri Hari vallabhdas Chunnilal Shah Research endowment award for the year 2010 from Sardar Patel university Anand, Gujrat.

Dr. Biradar is a life member of ISTE and IEI.