International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 2, April 2020, pp. 1641~1647
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i2.pp1641-1647

An efficient approach for secured communication in wireless sensor networks

Jyothi R, Nagaraj G Cholli
Department of Computer Science & Engineering, Global Academy of Technology, Bengaluru, Karnataka, India

Article Info

Article history:

Received Jul 18, 2019
Revised Oct 12, 2019
Accepted Oct 20, 2019

Keywords:

Authentication
Cryptography
Key management
security
Wireless sensor network

ABSTRACT

Wireless sensor network (WSN) have limited bandwidth, low computational functions, energy constraints. Inspite of these constraints, WSN is useful where communication happens without infrastructure support. The main concern of WSN is the security as the sensor nodes may be attacked and information may be hacked. Security of WSN should have the capability to ensure that the message received was sent by the particular sent node and not modified during transmission. WSN applications require lightweight and strong authentication mechanisms for obtaining data from unprivileged users. In wireless sensor networks, authentication is the effective method to stop unauthorized and undisrupted communication service. In order to strengthen the authenticated communication, several researchers have developed mechanisms. Some of the techniques work with identifying the attacked node or detecting injected bogus message in the network. Encryption and decryption are the popular methods of providing the security. These are based on either public-key or symmetric-key cryptosystems.Many of the existing solutions have limitations in communication and computational expertise. Also, the existing mechanisms lack in providing strength and scalability of the network. In order address these issues; a polynomial based method was introduced in recent days. Key distribution is a significant aspect in key management in WSNs. The simplest method of distribution of key is by hand which was used in the days of couriers. Now a day, most distribution of keys is done automatically. The automatic distribution of keys is essential and convenient in networks that require two parties to transmit their security keys in the same communication medium. In this work, a new type of key exchange mechanism is proposed. The proposed method for authentication among sensor nodes proves to be promising as per the simulation results. The nodes which are unknown to each other setup a private however arbitrary key for the symmetric key cryptosystem.

Corresponding Author:

Jyothi R.,
Department of Computer Science and Engineering,
Global Academy of Technology,
Bengaluru, Karnataka, India.
Email: jyothir.gat@gmail.com

1. INTRODUCTION

By using the concept of authentication, the corrupted and unofficial message can be avoided I wireless sensor network. Authentication means provisioning a message with authenticity and integrity assurances. In the literature, it can be found that there exist various authentication methods to provide genuineness of message and verification of integrity in WSNs. The basic strategies are public-key system and symmetric-key crypto systems.Several hash based authentication methods were proposed for WSNs. In these methods, each of the symmetric authentication key is shared among sensor nodes. By capturing a one sensor node, an attacker can compromise the key [1]. Hence, these methods are not resilient to compromise attacks

on node. These mechanisms require initial time synchronization which is very difficult to implement in large scale wireless sensor networks. The security mechanism introduces overhead like delay in message authentication which increases as the scalability of the network increases.

As wireless sensor networks have constraints in terms of bandwidth and energy, reducing the communication between base station and sensors plays vital role on power consumption and utilization of bandwidth. Aggregated wireless sensor network serve this purpose. The process of collecting, processing and forwarding the result of the raw sensed data from sensor nodes by intermediary nodes called 'aggregators' is called Data Aggregation. This concept reduces the data transmitted in the network and as a result leads to prolonged life time of network [2]. Without proper security mechanism, it is not possible to perform this operation. Due to the deployment environment of WSNs, the physical compromise of sensor nodes and aggregators is possible. It may also lead to false aggregation results [3]. To address these issues, the first option is cryptographic mechanisms using which confidentiality and integrity mechanisms can be achieved [3].

Because of high deployment cost and communication cost, the sensor nodes cannot practically make use of third party trusted servers. The public key protocols involve very high cost for computation. Hence, in WSNs, the better method for cryptography is the one which involves symmetric key cryptography. There exist lot of difficulty in key management in WSNs because of their dynamic structure, self-organization property and easy node compromise. There are large number of approaches which are focused on this area of key management because of its difficulty and importance. Based on the existing techniques, the current approaches can be classified as one way hash schemes, hybrid cryptography schemes and key pre-distribution schemes, key infection schemes etc. Some of the techniques are combination of more than one of these approaches. [4]. Figure 1 shows the apparoaches of key management in WSNs. These security challenges in WSN opens up a broad research issues in this area. In this work, an attempt has been made for design and development of new key management mechanism among WSN components.

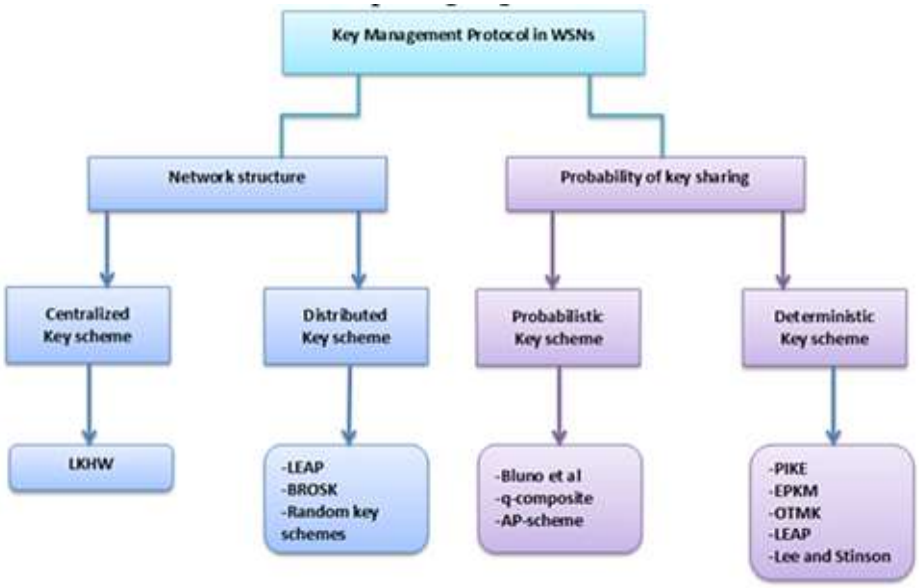

Figure 1. Key management approaches in WSNs Source [5]

2. RELATEDWORK

Bin Tian *et al* [6] state that in any secure communication, key management is one of the issues. It is the need of the hour to introduce reliable and secure key management schemes into the wireless sensor networks. In this work, the author has proposed a hierarchical method for key management to ensure network services security and WSN applications. Using this model, transmission and computing energy saving can be achieved. The researcher proposed an improvement of one-way hash function tree (OFT) by Chinese Remainder Theorem (CRT) for usage in large-scale WSNs. The experimentation has been done for evaluation of the security and performance. The results of the experimentation indicated that the results are satisfactory. C. Chen *et al* [7] opine that the key management is one of the significant research topics in secure communications in WSNs. Considering the mobility, large scale deployment, node failures, dynamic

network topology, communication failures etc, several dynamic key management methods like LOCK and SHELL have been proposed for guaranteed security. But the problem of collusion in key management is still not completely addressed. In this research work, the authors have tried to provide the solution. The new method has been proposed for secured communications in WSNs. The proposed method employs the three layered LOCK architecture. The method uses the encryption based on ciphertext-policy attribute for refreshing the group key in the upper layer and usage of EBS in the lower layer. The proposed method performed better than the existing related methods and also can avoid collusion attacks. In addition, considering the overhead of the communication, the number of messages used for rekeying is greatly reduced.

Guohua Ou *et al* [8] state that in wireless sensor network, key management is one of the considerable concerns. In the existing techniques, key management methods share the key for neighbour pairs of sensors in homogeneous sensor networks. Recently, some of the researchers have proved that compared to homogeneous networks, heterogeneous networks can achieve better performance in security. In this research work, key management scheme based on key-chain is proposed for heterogeneous networks. In the proposed scheme, various events like pair-wise key establishment, cluster key distribution and renovation are efficiently handled. Considering performance and security, it is demonstrated that the proposed scheme reduces the node storage requirements andsupport for dynamic sensor networks. It also achieves better security than the existing sensor key management techniques. R. Kuchipudi *et al* [9] state that Wireless Sensor Networks are installed in hostile areas necessitating the need for security. Establishing the secure links between nodes is a challenging issue in WSNs. Compared to wired wireless sensor networks are more vulnerable. Security between sensor nodes can be achieved using secret keys for encryption of the messages exchanged. Key management is the necessity for secured services such as authentication and confidentiality. The asymmetric and symmetric key cryptography or trusted server methods are used to provide solution to this problem. Asymmetric key cryptography enhances the security of the network security but also increases overhead in terms of memory, computation and energy. Symmetric key cryptography provides is efficient but it provides less security. Some of the techniques use trusted server for key management. It is not suitable for WSNs as there is trusted server usually. In this research work, Mobile agent based key distribution (MAKBD) in which mobile agents disseminate public keys and shared keys are updated. Different symmetric keys are constructed by each of the sensor node with its neighbour. Security of the communication is achieved by mutual authentication and data encryption with these keys. The results of the simulation indicate that the proposed method (MAKD) is scalable with less memory overhead.

S. B. Kamble *et al* [10] opine that as a sensor node is vulnerable to attacks by intruder, the security key management method has lot of options for coverage. Security and necessities of operational network activities are presented in various ways in the present techniques. The usage of WSN is in several types of applications like military surveillance, monitoring of healthcare devices, process monitoring etc. Encryption algorithms are used in WSNs for securing the data. In this work, security method has been proposed that used protocol certificate. A CL-EKM helps efficient key updation when a new node gets connected to a cluster. It also provides the key secrecy. The mitigation of wide effect of node customization on security happens by a withdrawal of compromised node. The security issues and solution for some of the issues have been discussed in our previous works [11-15]. From the literature, it can be observed that there are continuous efforts for improvement in security techniques [16-27].

3. THE PROPOSED METHOD

A public key cryptography called Elliptic Curve Cryptography (ECC) can be used for key generation and exchange between nodes and CH.In this method, each device that takes place in the communication has a pair of keys. The pair of keys is private key and a public key which are associated with a set of operations for cryptographic operation. The private key is known to a particular user whereas the all users have similar public key. Secure communications can be established by Public-Key cryptography (PKC) systems without sharing a secret key. RSA and ECC are the most used cryptography systems in recent days. This method was proposed by Victor Miller and Neal Koblitz in 1985.

The elliptic curve $y2 = x\ 3 + ax + b$ is defined by the mathematical operations of ECC where $4a3 + 27b2 \neq 0$. Different elliptic curve can be obtained by varying the value of a and b. The points (x,y) that satisfy the equation plus a point at infinity lies on the elliptic curve. The private key is the random number and public key is a point in the curve. The multiplication of the private key and the generator G in the curve results in the Public key. The domain parameter of ECC consists of the generator point G and the curve parameters a and b, together with few more constants.The proposed method uses enhanced ECC algorithm for secure transmission of messages as well as key.

3.1. ECC in wireless sensor network

WSNs are rapidly growing and hence, relevant to research and public at large. Two types of communication that happen in wireless sensor networks are between nodes and between base station and nodes. Table 1 shows the comparison of RSA algorithm and ECC. Following is the comparison of the ECC and RSA algorithms for key generation and exchange for WSN.

Table 1. Comparison of keys in ECC and RSA

ECC Key Sizes	RSA Key Size	Comment
160	1024	Short period security
256	3072	Medium period security
384	7680	Long term security

3.2. ECC algorithm

The ECC is based on the concepts of algebra related with elliptic curves over finite fields Fp and F2m. Elliptic Curve encryption and decryption system requires appoint G and an elliptic group $E_q(a, b)$ as a parameters. For encryption and sending a message Pm to B, A selects a random positive integer k. The cipher text Cm is produced as given by the (1).

$$Cm = [k*G, Pm + k*P_B] \quad (1)$$

In this scenario, A has used P_B, the public key of B.
The cipher text is decrypted using ECC. Here, B multiplies the first point in the pair by B's private key n_B and subtracts the result from the second point as shown by equation.

$$Pm + k*P_B - n_B(k*G) = Pm + k(n_B*G) - n_B(k*G) = Pm \quad (2)$$

The following steps indicate the key exchange between users A and B.

Step 1 A select an integer $n_A < n$ as A's private key.
Step 2 A generates a public key $P_A = n_A*G$ which is a point in $E_q(a, b)$.
Step 3 B select an integer $n_B < n$ as B's private key.
Step 4 B generates a public key $P_B = n_B*G$ which is a point in $E_q(a, b)$.
Step 5 Public keys are exchanged between A and B.
Step 6 A generates the secret key $K = n_A* P_B$ and B generates the secret key $K = n_B* P_A$

3.3. Enhanced ECC method

The existing ECC algorithm has been modified. The proposed algorithm uses Arnold map which is also known as cat map. Arnold map that is generalized is presented with two parameters a and b as given below.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\text{mod } 1) \quad (3)$$

a and b are control parameters which are real numbers. It can be concluded that the largest Lyapunov exponent in map (1) is greater when a >1 and b>1. This means that map (1) can perform better in data shuffling.
The proposed algorithm is given below.

Step 1 Generate key pairs (Public and private key)
Step 2 Convert both keys to binary representation
Step 3 Using Arnold map keys shuffling is done
Step 4 Share the shuffled key with the participating nodes
Step 5 Using Arnold map reshuffle the key , use these keys to encrypt the message using ECC algorithm
Step 6 After encrypting the message, again encrypt the cipher text using Arnold method for data shuffling
Step 7 Send the encrypted message to the CH, then CH uses Arnold method for reshuffle. Using private key original message is recovered.

The implementation has been tested using MATLAB tool. It is a tool developed by Math Works for multi-paradigm computing environment. The tool can be used to implement algorithms, user interface creation, plotting functions and data etc. MATLAB has a wide variety of functions useful to the genetic algorithm and also has provision to experiment with the genetic algorithm. MATLAB essentially supports only one data type, a rectangular matrix of real or complex numeric elements. The following figures show the screen shots of simulation of the proposed work. The screenshot of data encryption between nodes and cluaster head is shown in Figure 2. Figure 3 depicts the encryption process using public key cryptography. Cluster head based architecture of wireless sensor network is shown in the Figure 4.

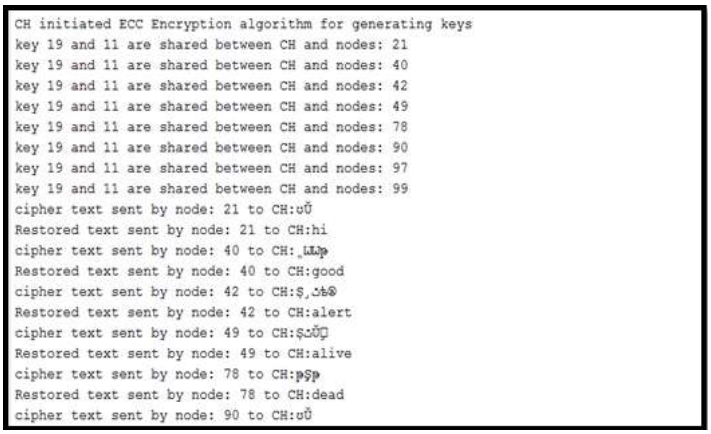

Figure 2. Data encryption between nodes and CH

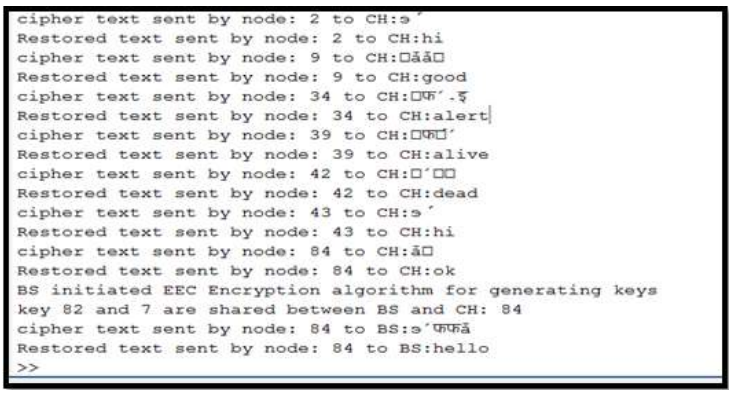

Figure 3. Encryption using public key cryptography

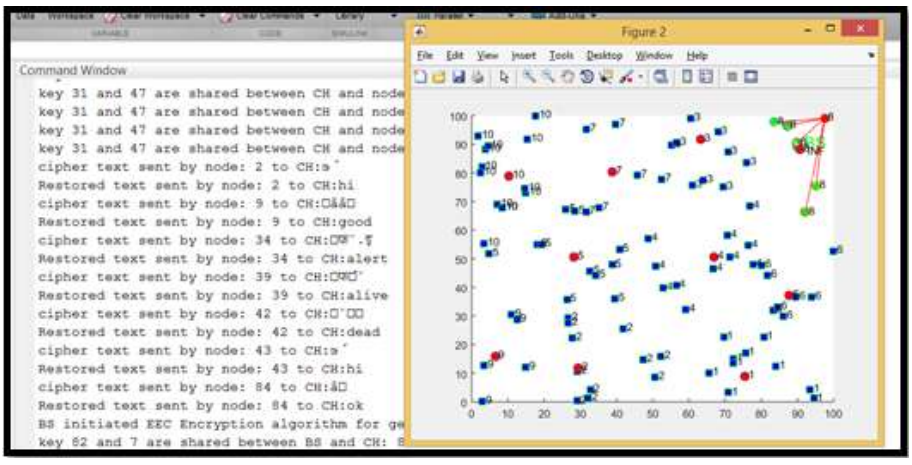

Figure 4. CH based architecture of WSN

4. RESULTS AND CONCLUSIONS

ECC is a suitable choice to achieve wireless sensor network security. The proposed enhanced version of ECC uses Arnold map for reshuffling the keys as well as messages. In portable devices, ECC provides a good choice for asymmetric cryptography. The RSA key with 1024 bit key provides the secured environment as that of 160 bit elliptic curve key. By using speed, storage, power and bandwidth several advantages can be achieved by smaller key sizes. The shorter key means less storage space and reduced arithmetic operations. In total, enhanced ECC based algorithm can be easily included into currently used protocols to achieve security with smaller resources.

REFERENCES

[1] K. HimaBindu, Ch. LavanyaAishani, M.Kamalakar, "A Secure Key Exchange Scheme in Wireless Sensor Networks Using Diffie Hellman," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 4, no 9, pp. 16338-16343, Sept 2016.

[2] D. Djenouri And L. Khelladi, A. NadjibBadache, "A Survey Of Security Issues In Mobile Ad Hoc And Sensor Networks," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 4, pp.2-28, Fourth Quarter 2005.

[3] MohitSaxena, "Security In Wireless Sensor Networks - A Layer Based Classification," Cerias Tech Report 2007-04.

[4] Ms. T P Rani and Dr. C Jaya Kumar, "Establishment of secure Communication in wireless sensor Networks," *Science & Engineering*, vol. 2, no. 2, pp. 35-39, April 2012.

[5] Salah-ddine, Krit, "Review on the Attacks and Security Protocols for Wireless Sensor Networks," ICEMIS 2016 CFP The International Conference on Engineering & MIS 2016vol. 101, no. 265-283, pp. 1-5, (2013).

[6] Bin Tian *et al*., "A Novel Key Management Method for Wireless Sensor Networks," *2010 3rd IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT)*, Beijing, pp. 1106-1110, 2010.

[7] C. Chen, Z. Huang, Q. Wen and Y. Fan, "A Novel Dynamic Key Management Scheme for Wireless Sensor Networks," *2011 4th IEEE International Conference on Broadband Network and Multimedia Technology*, Shenzhen, pp. 549-552, 2011.

[8] GuohuaOu, Jie Huang and Juan Li, "A Key-chain based Key Management Scheme for Heterogeneous Sensor Network," *2010 IEEE International Conference on Information Theory and Information Security*, Beijing, pp. 358-361, 2010.

[9] R. Kuchipudi, A. A. M. Qyser and V. V. S. S. S. Balaram, "An Efficient Hybrid Dynamic Key Distribution in Wireless Sensor Networks with Reduced Memory Overhead," *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Chennai, pp. 3027-3030, 2016.

[10] S. B. Kamble and V. V. Jog, "Efficient Key Management for Dynamic Wireless Sensor Network," *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, pp. 583-586, 2017.

[11] Jyothi R, Nagaraj G Cholli, "New Approach to Secure Cluster Heads in Wireless Sensor Networks", *In the Proc of 5th International Conference on Advanced Computing & Communication Systems*, pp. 1097-1101, 2019.

[12] Jyothi R, Nagaraj G Cholli, "A Secure Data Aggregation Technique for Wireless Sensor Networks using Iterative Filtering", *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 11, no. 1, pp. 284-293, July 2018.

[13] Jyothi R, Nagaraj G Cholli, " Secure Data Aggregation using RSA Algorithm", *International Journal of Scientific Development and Research*, vol 2, no 7, pp 189-197, July 2017.

[14] Asha R N, Jyothi R, Kiran Kumar K, "Detection of Malicious Nodes in WSN-A survey," *International Conference, SSCE –IFERP*, Bangalore, pp. 36-40, June 7th 2016.

[15] Sunanda V K, Jyothi R, "Survey on Dynamic Clustering for Energy Efficient Data Aggregation Technique using Secure Data Encoding Scheme for WSN," *International Journal of Engineering Research &* Technology, vol 3, no 2, pp. 1954-1956, Feb 2014.

[16] S. Wen, R. Du and H. Zhang, "A Segment Transmission Secure Routing Protocol for Wireless Sensor Networks," *International Conference on Computational Intelligence and Security*, Guangzhou, pp. 579-1582, 2006.

[17] Y. Nishikawa et al., "Design of stable wireless sensor network for slope monitoring," *IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet)*, Anaheim, CA, pp. 8-11, 2018.

[18] W. A. Hussein, B. M. Ali, M. F. A. Rasid and F. Hashim, "Design and performance analysis of high reliability-optimal routing protocol for mobile wireless multimedia sensor networks," *IEEE 13th Malaysia International Conference on Communications (MICC*), Johor Bahru, pp. 136-140, 2017.

[19] K. Fukuda et al., "Transmit control and data separation in physical wireless parameter conversion sensor networks with event driven sensors", *IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet)*, Anaheim, CA, pp. 12-14, 2018.

[20] Ping Wang, Chang Zhang, Heng Wang and XiaoYuan Xu, "A TR069 WAN management protocol for WIA-PA Wireless sensor Networks," *25th Wireless and Optical Communication Conference (WOCC)*, Chengdu, pp. 1-4, 2016.

[21] S. M. H. Aejaz, T. Zemen and A. Springer, "Performance of a partner selection algorithm in IEEE 802.15.4 based wireless sensor networks," *IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet)*, Austin, TX, pp. 4-6, 2016.

[22] T. Nowak, A. Koelpin, F. Dressler, M. Hartmann, L. Patino and J. Thielecke, "Combined localization and data transmission in energy-constrained wireless sensor networks," *2015 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet)*, San Diego, CA, pp. 4-6, 2015.
[23] A. Mateen, M. Sehar, K. Abbas and M. A. Akbar, "Comparative analysis of wireless sensor networks with wireless multimedia sensor networks," *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, Chennai, pp. 80-83, 2017.
[24] J. P. Singh, M. K. Mishra and M. A. Khan, "Energy-efficient approach towards video-based sensor networks (wireless) beneath barrier coverage," *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Delhi, pp. 1-5, 2017.
[25] J. Jose, S. M. Kumar and J. Jose, "Energy efficient recoverable concealed data aggregation in wireless sensor networks," *IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN)*, Tirunelveli, pp. 322-329, 2013.
[26] G. Ma, Y. Yang, X. Qiu, Z. Gao and H. Li, "Fault-tolerant topology control for heterogeneous wireless sensor networks using Multi-Routing Tree," *IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon*, pp. 620-623, 2017.
[27] A. Aseeri and R. Zhang, "Secure Data Aggregation in Wireless Sensor Networks: Enumeration Attack and Countermeasure," *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, Shanghai, China, pp. 1-7, 2019.

BIOGRAPHIES OF AUTHORS

Jyothi R is a Computer Science and Engineering graduate. She is graduated in the year 2004 and later obtained M Tech degree in Computer Science & Engineering in the year 2009. Currently she is pursuing PhD from VTU in the area of *Wireless Sensor Network*.Currently she is working as an Assistant Professor in the department of Computer Science & Engineering, Global Academy of Technology, Bengaluru, Karnataka, India. She has 15 years of teaching Experience. She has guided several UG and PG projects. She is active in research and published 12 papers in various national & international conferences/Journals. She is also Life time member in ISTE and CSI society.

Dr. Nagaraj G Cholli is a Computer Science and Engineering graduate. He also holds the M Tech degree in Computer Science & Engineering from IIT-Roorkee. He obtained PhD from VTU in the year 2016 in the area of Software aging and rejuvenation. He presently works as Associate Professor at Department of Information Science and Engineering, R.V College of Engineering, Bengaluru, Karnataka, India. He has a total of 13 years of experience in teaching, research and industry. He has pushed several research articles in International journals and presented papers at Conferences. He is active in research, has filed patents and guiding several PhD scholars. He is also a life member of ISTE and CSI society.