International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 4, August 2019, pp. 2695~2702
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i4.pp2695-2702

Integrated framework for secure and energy efficient communication system in heterogeneous sensory application

Yogeesh A.C.[1], Shantakumar B. Patil[2], Premjyoti Patil[3], Roopashree H.R.[4]
[1]Department of Computer Science and Engineering, Nagarjuna College of Engineering and Technology, India
[2]Department of Computer Science and Engineering, Nagarjuna College of Engineering and Technology, India
[3]Department of Electronics and Communication, Nagarjuna College of Engineering and Technology, India
[4]Department of Computer Science and Engineering, GSSS Institute of Engineering and Technology for Women, India

Article Info

Article history:

Received Aug 24, 2018
Revised Dec 17, 2018
Accepted Mar 11, 2019

Keywords:

Cost effectiveness
Energy Consumption
Optimization
Security
Wireless Sensor Network

ABSTRACT

Irrespective of different forms and strategies implementing for securing Wireless Sensor Network (WSN), there are very less strategies that offers cost effective security over heterogeneous network. Therefore, this paper presents an integrated set of different processes that emphasize over secure routing, intellectual and delay-compensated routing, and optimization principle with a sole intention of securing the communication to and from the sensor nodes during data aggregation. The processed system advocates the non-usage of complex cryptography and encourages the usage of probability their and analytical modelling in order to render more practical implementation. The simulated outcome of study shows that proposed system offers reduced delay, more throughputs, and reduced energy consumption in contrast to existing system.

Corresponding Author:

Yogeesh AC
Research Scholar, Department of Computer Science and Engineering,
Nagarjuna College of Engineering and Technology,
VTU, Belagavi, Karnataka, India
Email: yogeesh13@gmail.com

1. INTRODUCTION

The upgrading in the micro-electro-mechanical systems with digital electronics and network communication technologies have made possible to employ low cost, automated and intelligent device for different qualities of purposes in both indoor application and outdoor application [1]. This device is capable with sensing task and performs communication through a wireless channel, and it is popularly known as WSN (wireless sensor network). Therefore, WSN is a collection of several sensors latched with tiny nodes that perform together various operations such as environmental sensing, data collection and processing, and performs communication among other sensor nodes through radio link transmission frequency [2].

The nodes in WSN are miniature and also called as motes which consist of a micro-control device, transistors and equipped with the fixed battery source. The objectives of sensors are to sense the event (temperature, humidity, air, soil quality and object) occurred in the region of interest and therefore nodes perform further data processing and communication processes as per application requirement [3]. Furthermore, the sensor nodes are resource constraints (limited energy, limited processing capacity, fixed storage and limited sensing range) in nature due to its low cost and small size structure. Nowadays, WSNs are highly taken in remote applications that employed by several industries and organisation such as forest, healthcare organisation for patient monitoring and elderly care, government and military application for surveillance, security, and target tracking, home automation, weather forecasting, home, school, office for monitoring purposes and also it utilizes in industrial application for automation and control processes [4]. Although, the WSN application is mostly based on the real-time data information and due to its resource

constraints nature, its open numbers of security challenges towards itself. Usually, WSNs are highly deployed in a hostile environment and left to be alone which makes it vulnerable to several attacks.

Various researchers have discussed the issues related with WSN security [5-7] and proposed several different security solutions to preserve its privacy and to provide robust protection with considering its resource limitations [8-10]. Hence, providing an energy efficient security mechanism in WSN is not a simple job. Therefore, there is a need of optimal security approach that keeps WSN secure, reliable, long life functioning, and preserve from the various attacks. This paper presents a discussion of novel solution that is meant for balancing the security demands as well as energy related demands of wsn. Algorithm is briefd in Section 2 while result is discussed in Section 3 and summary in Section 4.

This section presents state of the art in the domain of WSN security for realizing the current status of progress in WSN applications. The work taken in the study of Illiano et al. [11] have considered the problem of malevolent data insertion in the WSN and presented an optimization algorithm to improve the event detection operation and to enhance the efficiency of anomaly detection in WSN. The work carried out by Mohindru, and Singh [12] came out with the energy efficient node validation algorithm based on the cryptographic concept to detect the node replication attacks and prevent WSN from other node compromised attacks. By considering resource constraint property of sensor nodes the work of Poriye and Upadhyaya [13] have offered a new security scheme based on the DNA cryptography technique and secures socket layer protocol to increase the level of sensor node security in WSN.

Venkatraman and Kumar et al. [14] have presented a smart control system based on a distributed system of automation concept to secure the whole network from malicious attacks, to improve data reliability and to enhance the overall performance of sensor network. Movassaghi et al. [15] presents a spectrum allocation dependent novel interference mitigation approach for wireless body area network in order to improve its QoS. Li et al. [16] have analyses some existing authentication techniques that carried for real-time WSN application. The findings of the presented investigation show that the current techniques are still in a critical phase that suffers from data loss attack and less user anonymity and friendliness. The work of Chen et al. [17] have invented an advanced, intelligent and reliable routing protocol based on opportunistic routing technique to achieve higher accuracy data transmission within a fixed interval of time for Cyber-physical system WSN.

Singh et al. [18] have utilized the concepts of Fuzzy system and neural network and developed an enhanced hybrid interference detection system to identify the different types of attacks and to become aware of compromised nodes in the WSN. Zhang et al. [19] uses Elliptic Curves Cryptography technique for key exchange protocol anonymously in the WSN. The experimental outcomes show that the presented technique achieves better security mechanism, but it has a disadvantage that it consumes higher energy. Tian et al. [20] have introduced a modified version of mixed integer and nonlinear programming and gave a joint approach of full duplex and security by considering cross-layer optimization to improve the energy utilization, spectrum efficiency and to enhance the security level. Alves et al. [21] have argued that SDN (Software defined network) have the capability to provide better flexibility in WSN. The authors have presented an SDN based model to handle node deployment and efficient distribution of a symmetric key.

Zhang et al. [22] constructed an Intrusion detection system based on self-adaptive and active trust threshold mechanism to detect malicious behavior and to control overhead problem in WSN. Zhu et al. [23] have presented an overview of physical layer security in IWSNs to point out some challenges and essential requirements to improve both security and IWSN overall performance. Rana [24] has presented a distributed estimation technique for controlling cyber attacks and stabilization technique for controlling packet loss in the electric vehicles. Kumar et al. [25] focused on the issue related with secure localization of sensor nodes and presented a secure localization algorithm to protect the sensor nodes from the outsider attack and as well as it also monitors the insider node to detect compromised node in the network. Faisal et al. [26] have created a novel scheme based on receive signal strength mechanism to counter the identity replication attack on the IEEE 802.11 based wireless ad-hoc network.

The work carried out by the Liu et al. [27] have presented an improved distributed estimation technique based on least mean square algorithm to tackle the problem of secure estimation over WSN under the presence of attacks. Nurellari et al. [28] presents, a reliable scheme to investigate the compromised nodes and to control their behaviors toward the data fusion process. Tayebi et al. [29] have given an improved chaotic based direct sequence spread spectrum (DSSS) technique in order to enhance the security of chaotic-DSSS dependent WSN. The work carried out by Shen et al. [30] uses Id-based aggregation signature technique for improving the security level of data integrity in WSN. The experimental effects display that the presented method achieves provides excellent protection as well as it minimizes storage cost and reduces bandwidth. Naik and Nayak [31] have presented its involvement by demonstrating classifications of predictable cost-estimation methods and after that investigates the investigation trends towards commonly addressed issues in it. Kulkarni et al. [32] have illustrated a real-time design of effective examining and

control of grid power technique by using the remote cloud server. This study also focused to use the remote cloud server to fetch, examine as well as control the real-time energy method data to enhance the worldwide control and reply time. Benslimane and BenAhmed [33] have introduced a novel lightweight key management procedure which permits the inhibited node into the 6loWPAN network to transmit captured data to internet host in the secure channel. The next section discusses about the problems associated with the strategies introduced in the existing system.

The significant research problems are as follows:

1. Existing studies considers security implementation without considering various energy-related factors that doesn't offer energy efficiency.
2. Existing solutions for security are more inclined towards specific forms of attack in WSN and hence the solution has very less scope of implementation towards other attacks.
3. Existing solutions are incapable of identifying the form of the malicious intention incorporated within the routing request that fails to identify the degree of vulnerability.
4. There is no much discussion of the optimization technique within the sensor network that could offer a good retention of energy and more resistivity against the routing principle.

   Therefore, the problem statement of the proposed study can be stated as "Developing a secure, intellectual, and optimizated routing principle in WSN is one of the most computationally challenging task". The next section briefs of the solution against such problems

This part of the proposed study is a continuation of prior work [34]. The proposed system targets to offer higher degree of secure communication system with equal emphasis on energy efficiency. The complete proposed system is classified into three processes that emphasize on incorporating secure routing, intellectual routing, and optimization process. Figure 1 highlights the proposed implementation plan.

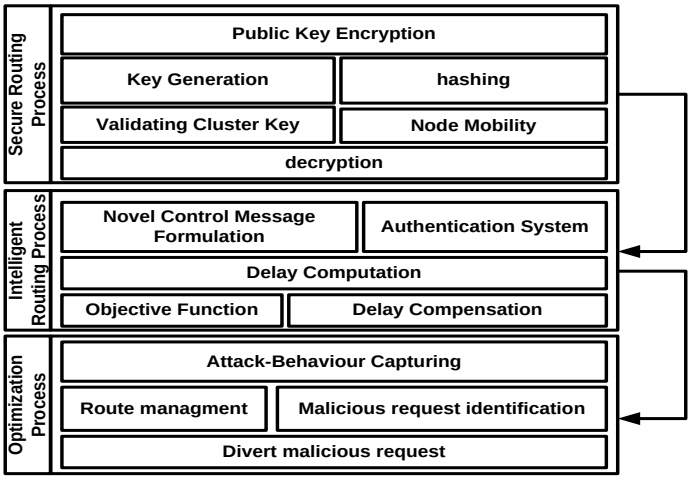

Figure 1. Effects of selecting different switching under dynamic condition

Referring Figure 1, the first process refers to addressing non-usage of conventional cryptographic scheme in order to introduce a simple hashing-based encryption along with dynamic key management. The second process refers to address the problems associated with symptomatic solutions towards similar attacks in WSN. It ensures that irrespective of any forms of attack, the proposed system offers to identify and compensate delay factor that generates intrusion. The final process of optimization is carried out using a very simple approach of identifying the malicious request and barring them from joining the network. The prominent contribution of the proposed system is its usage of simple and cost-effective approach to offer security and energy efficiency. The next section discusses about the system design elaborating more about the design principles.

2. SYSTEM DESIGN

Incorporating a security scheme in WSN is not a simple task as can be seen from various existing research approaches till date. The prominent problem of existing security approaches are that they are less practical and highly theoretical while the route cause of this problem is one i.e. design doesn't consider various essential and comprehensive factors that are directly linked to security performance.The development

of the proposed logic is carried out on the basis of the multiple integrated processes in order to retain maximum level of security over the communication process in WSN. The discussions of the different processes are as follows:

2.1. Secure routing process

This process implements a graph theory where probability logic is incorporated for ensuring robust authentication scheme along with energy efficiency considering the case of heterogeneous WSN. This is the first process module that emphasizes on an effective generation of key, dynamic mobility of the sensor, and authenticates the cluster key. The mechanism for key generation is responsible for generating a secret key in such a way that even of this secret key is stolen it will be of no use for the attacker. Referring to Figure 1, this module introduces a communication model considering cluster head, member node, and base station. The security aspects of this process use simple public key encryption that uses simple pseudorandom number generation method to generate a secret key of public type while private key is obtained by splitting. This operation has a significant advantage to incorporate both forward and backward secrecy. Another important part of this design principle is that it offers increasing layer of encryption using very lightweight mechanis of hashing. The mechanism of the mobility is associated with randomly positions within the simulation area. This phenomenon will mean that there is never a defined pattern of movement. This mechanism is constructed using simple hashing and usage of pseudorandom numbers.

The next process is all about authencating cluster key that is essentially meant for validating a cluster head. According to this mechanism, any information associated with the victim sensor (i.e. cluster head) is forwarded to the neighboring sensors as an update that is further spread until and unless it reaches the last node present in the network. In this process, the forwarding sensor transmits a beacon bearing the information of compromised node (that could be either cluster head or member node or both). This message is subjected to decryption by the clusterhead and the information associated with this decryption is updated by both cluster head as well as its member node. The authentication is carried out by checking the presence of decrypted key within the neighboring sensors that confirms that there is a presence of used (or malicious) key and hence that specific key is discarded or else it is considered. An interesting fact to observe is that proposed process doesn't include any form of complex cryptographic mechanism other than usage of hashing and pseudorandom operation, which is very much lightweight and doesn't include more memory or processing capability within the sensor to execute them for invoking the security features. Shows in Figure 2 design principle of secure routing process.

2.2. Intelligent routing process

The first process is responsible for carrying out initial operation of authentication for ensuring secure routes; however; it needs more behavioural information for boosting up its security features. Hence, this second process implements a novel mechanism of inter-arrival time to investigate its necessary impact over the security feature. The backbone of the proposed system is controlled using a novel form of control message that uses three forms of message i.e. i) first message for generating beacons, ii) second message for broadcasting beacons, and iii) third message for authenticating beacons. The next action considered in this process is linked with the computation of the delay which is meant indirectly to control any form of network as well as computational overhead owing to the authentication mechanism dicussed in the first process. This process also introduces a novel and simple objective function that is responsible for minimizing the energy consumption, which will mean that amount of energy allocated will be checked for single and double hops as well as size of packets. If an allocated energy is found to be surplus as compared to the genuine energy required than surplus energy will be minimized. However, this process doesn't occur frequently. Hence, if the energy is found devoid of having surplus amount that the proposed system looks for an alternative secured link with lesser inter-arrival time. This operation not only assists in positively leading all the packets in safer routes but also minimizes any form of possible delays. Hence, the delay factor is compensated at the end at any cost in this model. Therefore, this process acts as complementary to the first process of secure routing scheme. Shows in Figure 3 design principle of intelligent routing process.

2.3. Optimization process

The prime problem to be addressed in this phase of the work is to identify and resist the type of attack that tampers the programmes embedded in the commercial sensor application. Usually, commercial sensor applications are highly prone to various forms of unknown and anonymous service request from the adversarial node. Such adversarial nodes are quite hard to be identified and thereby it is difficult to capture/ encapsulate the adversary. The complete basis of this part of the study is a new adversarial module which has the potential to access and control the programming object of the sensor node that finally leads to physical node capture. However, the scope will be only limited towards capturing programming object by the

malicious node and how the proposed system resists it. The study will use similar communication model used in prior section but will introduce a novel adversarial model. The study will apply analytical modelling approach with formulation of a programming object. An authentication module will be developed which will be responsible for authenticating the challenge generated by the node. After the authentication is carried out by the node, the next step will be to apply probabilistic data structure in order to securely store the programming object of a sensor node. This phenomenon is a type of novel sandboxing mechanism that any sensor node will be using in order to secure checks the legitimacy of the incoming route request. In case of legitimate request, a secure route will be established; however, in case of illegitimate request, the sensor node is still safe as any change the programming object invokes to sandbox renders instantly the forced damage of the data structure and a new probabilistic data structure is developed. Before, forwarding the secured routing information, the mechanism also checks for the probability of the true positive or negative in the notification generated from the sandboxing mechanism. This will be carried out in order to perform a second check on the validity of the notification about the malicious node. A novel optimization policy will be then constructed which will use an extremely lightweight cryptographic module without an extensive recursive operation in order to have better suitability with the real time sensor operation. Finally, the system will perform filtration for the legitimate and illegitimate task from the requestor node. Shows in Figure 4 design primciple of optimization process.

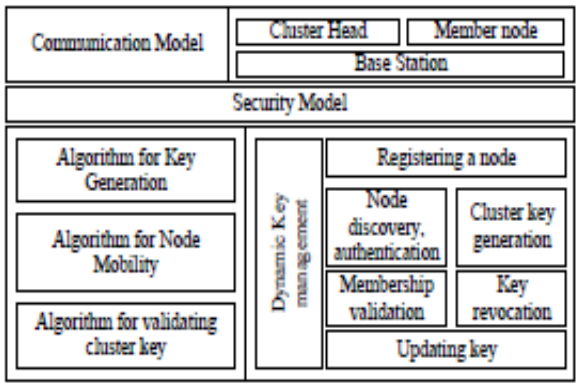

Figure 2. Design principle of secure routing process

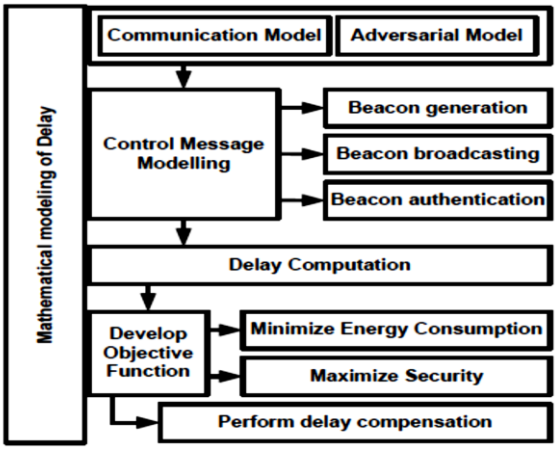

Figure 3 Design principle of intelligent routing process

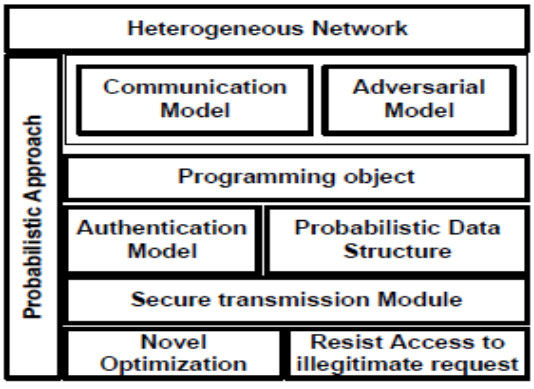

Figure 4. Design principle of optimization process

3. RESULTS ANALYSIS

The implementation of the proposed system is carried out using MATLAB over normal system configuration using 1000 x1200 m2 simulation area with 100 sensors. The complete analysis is carried out with respect to outcome of each phase to exhibit its potential capability of offering security and reducing energy dissipation.

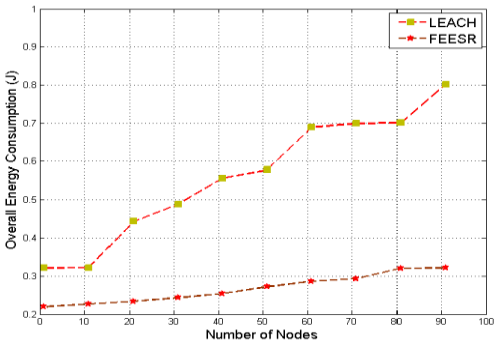

Figure 5. Analysis of overall energy consumption

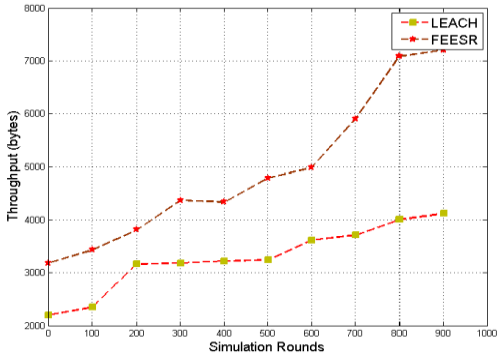

Figure 6. Analysis of overall energy consumption

Figure.5 and Figure.6 is a comparative analysis of secured routing process where the proposed system is shown to be compared with the existing energy efficient LEACH algorithm. The study outcome shows that proposed system over quite low rate of energy consumption as well as higher throughput with increasing number of simulation rounds. The outcome shows that the proposed system also offers a significant scalability in its performance while offering security of higher. The prime reason behind this outcome is that proposed system discussed in secured routing process doesn't use any form of potential encryption or any other form of iterative principle that makes the operation quite faster resulting in lesser energy consumption and higher throughput. LEACH algorithm fails to do so as they offer good energy efficiency but their clustering operation is based on centrality principle which is non-practical.

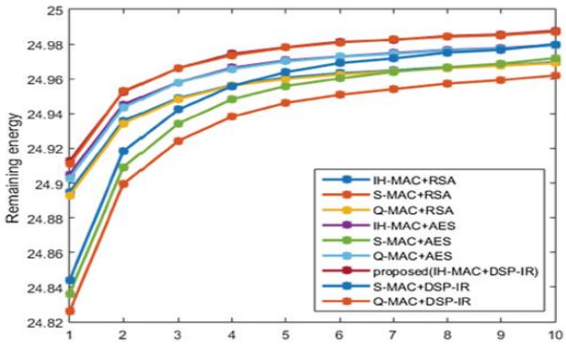

Figure 7. Analysis of residual energy

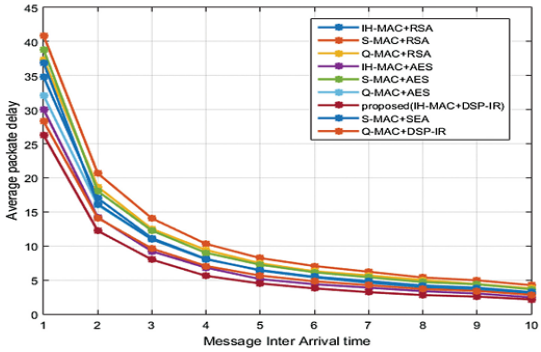

Figure 8. Analysis of delay

Figure.7 and Figure.8 is a comparative analysis of proposed system with secured-LEACH [35]. It is because of the reason that this algorithm is the only standard conventional algorithm that claims of incoporrating key management for security and hierarchical clustering for energy efficiency. All the activity carried out by proposed system is mainly related to checking the control messages for searching the nodes and controlling topology. Based on this, every routing and accessibility decision is undertaken by the sensors. With increasing simulation, the network gains more information owing to presence of auxiliary nodes which is responsible for lowering the network overhead. Moreover, usage of probability parameter further assists in faster computation and lower iterative operation that results in very slower pace of energy consumption for proposed system. However, SecLeach is not found to offer much resistivity against energy drainage and hence it shows faster degradation of energy thereby reducing the network lifetime in WSN. It was also seen the complete processing time of proposed system is 85% faster as compared to the existing approach. Hence, proposed system offers better energy efficiency over increased period of time. The complete implementation techniques show that proposed system offers enhanced security operation and is resistive against all major forms of threats irrespective of their specific adversarial behaviour.

4. CONCLUSION

The paper presents a discussion of a solution that is meant for offering practical security features within resource constraint sensors. The significant contribution of the proposed system are as follows: i) The proposed system offers approximately45% increased throughput as compared to existing secured and hierarchical energy efficiency protocols, ii) the applicability of proposed system is more on heterogeneous network while majorty of the existing security solutions are only directed towards homogeneous WSN, iii) the proposed system can successfully reduce the energy consumption and increase the network lifetime to more than 67% in contrast with existing system, and iv) proposed system offers capability to identify and resist malicious request and hence they are capable of resisting majority of attacks and hence the solution is not attack specific.

REFERENCES

[1] Zhang W, Dong Y, Tan Y, Zhang M, Qian X, Wang X. "Electric Power Self-Supply Module for WSN Sensor Node Based on MEMS Vibration Energy Harvester," *Micromachines*. Apr 1;9(4):161 2018.

[2] Le, Dac-Nhuong, Raghvenda Kumar, and Jyotir Moy Chetterjee. "Introductory Concepts of Wireless Sensor Network. Theory and Applications," 2018.

[3] R. T. Tse and Yubin Xiao, "A portable Wireless Sensor Network system for real-time environmental monitoring," *IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Coimbra, pp. 1-6 2016.

[4] Murphy, R.R., Lisetti, C.L., Tardif, R., Irish, L. and Gage, A., "Emotion-based control of cooperating heterogeneous mobile robots," *IEEE Transactions on Robotics and Automation*, 18(5), pp.744-757. 2002.

[5] Chawla, Heena, Hardeep Kaur, and Charanvir Kaur. "Review on Security Issues in Wireless Sensor Networks," 2016.

[6] Tomić and J. A. McCann, "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols," in *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1910-1923, Dec 2017.

[7] J. Xu, G. Yang, Z. Chen and Q. Wang, "A survey on the privacy-preserving data aggregation in wireless sensor networks," in *China Communications*, vol. 12, no. 5, pp. 162-180, May 2015.

[8] Yu, F., Chang, C. C., Shu, J., Ahmad, I., Zhang, J., & De Fuentes, J. M. "Recent Advances in Security and Privacy for Wireless Sensor Networks 2016," *Journal of Sensors*, 2017.

[9] A. Karakaya and S. Akleylek, "A survey on security threats and authentication approaches in wireless sensor networks," *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, Antalya, , pp. 1-4 2018.

[10] K. Shim, "A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 577-601, Firstquarter 2016.

[11] Illiano, Vittorio P., et al. "Determining Resilience Gains From Anomaly Detection for Event Integrity in Wireless Sensor Networks," *ACM Transactions on Sensor Networks (TOSN)* 14.1: 5 2018.

[12] Mohindru, Vandana, and Yashwant Singh. "Node authentication algorithm for securing static wireless sensor networks from node clone attack," *International Journal of Information and Computer Security* 10.2-3: 129-148 2018.

[13] Poriye, Monika, and Shuchita Upadhyaya. "DNA-Based Cryptography for Security in Wireless Sensor Networks." *Cyber Security: Proceedings of CSI 2015*, Springer Singapore, 2018.

[14] Venkatraman, S., and P. Arun Raj Kumar, "Improving Adhoc wireless sensor networks security using distributed automaton," Cluster Computing: 1-7.

[15] Movassaghi S, Smith DB, Abolhasan M, Jamalipour A. "Opportunistic Spectrum Allocation for Interference Mitigation Amongst Coexisting Wireless Body Area Networks," *ACM Transactions on Sensor Networks (TOSN)*. Jul 21;14(2):7 2018.

[16] Li W, Li B, Zhao Y, Wang P, Wei F. "Cryptanalysis and Security Enhancement of Three Authentication Schemes in Wireless Sensor Networks," *Wireless Communications and Mobile Computing*. 2018; 2018.

[17] Chen, Aiguo, et al. "RTGOR: Reliability and Timeliness Guaranteed Opportunistic Routing in wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking* 2018 : 1-8 2018.

[18] Singh, Rupinder, Jatinder Singh, and Ravinder Singh. "Fuzzy Based Advanced Hybrid Intrusion Detection System to Detect Malicious Nodes in Wireless Sensor Networks," *Wireless Communications and Mobile Computing* 2017. 2017.

[19] Zhang K, Xu K, Wei F. "A Provably Secure Anonymous Authenticated Key Exchange Protocol Based on ECC for Wireless Sensor Networks," *Wireless Communications and Mobile Computing*. 2018 ; 2018.

[20] Tian F, Chen X, Liu S, Yuan X, Li D, Zhang X, Yang Z. "Secrecy Rate Optimization in Wireless Multi-Hop Full Duplex Networks," *IEEE Access*, 6:5695-704 2018.

[21] Alves, R. C., Oliveira, D. A., Pereira, G. C., Albertini, B. C., & Margi, C. B. "WS3N: Wireless Secure SDN-Based Communication for Sensor Networks," Security and Communication Networks, 2018. 2018.

[22] Z. Zhang, H. Zhu, S. Luo, Y. Xin and X. Liu, "Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Networks," in *IEEE Access*, vol. 5, pp. 12088-12102, 2017.

[23] J. Zhu, Y. Zou and B. Zheng, "Physical-Layer Security and Reliability Challenges for Industrial Wireless Sensor Networks," in *IEEE Access*, vol. 5, pp. 5313-5320, 2017.

[24] M. M. Rana, "Attack Resilient Wireless Sensor Networks for Smart Electric Vehicles," in *IEEE Sensors Letters*, vol. 1, no. 2, pp. 1-4, April, Art no. 5500204. 2017.

[25] Kumar, Gulshan, et al. "A Secure Localization Approach Using Mutual Authentication and Insider Node Validation in Wireless Sensor Networks," Mobile Information Systems 2017. 2017.
[26] Faisal, Mohammad, Sohail Abbas, and Haseeb Ur Rahman. "Identity attack detection system for 802.11-based ad hoc networks," *EURASIP Journal on Wireless Communications and Networking 2018*.1 : 128 2018.
[27] Y. Liu and C. Li, "Secure Distributed Estimation Over Wireless Sensor Networks Under Attacks," in *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 4, pp. 1815-1831, Aug. 2018.
[28] Nurellari, Edmond, Des McLernon, and Mounir Ghogho. "A secure optimum distributed detection scheme in under-attack wireless sensor networks," *IEEE Transactions on Signal and Information Processing over Networks* 4.2 (2018): 325-337. 2018.
[29] Tayebi, Arash, Stevan Berber, and Akshya Swain. "Security Enhancement of Fix Chaotic-DSSS in WSNs," *IEEE Communications Letters* 22.4 : 816-819. 2018.
[30] Shen, L., Ma, J., Liu, X., Wei, F., & Miao, M . "A secure and efficient id-based aggregate signature scheme for wireless sensor networks," *IEEE Internet of Things Journal*, 4(2), 546-554. 2017.
[31] Naik, Praveen, and Shantaram Nayak. "Insights on Research Techniques towards Cost Estimation in Software Design," *International Journal of Electrical and Computer Engineering (IJECE)*, Vol.7, No. 5, pp. 2883-2894, 2017.
[32] Nachiket Kulkarni, S.V.N.L Lalitha, Sanjay A. Deokar, "Real time control and monitoring of grid power systems using cloud computing," *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 9, No. 2, 2017.
[33] Benslimane, Yamina, and Khelifa BenAhmed. "Efficient End-to-End Secure Key Management Protocol for Internet of Things," *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 7, No. 6, pp.3622-3631, 2017.
[34] A. C. Yogeesh, S. B. Patil and P. Patil, "A Survey on Energy Efficient, Secure Routing Protocols for Wireless Sensor Networks," *International Journal of Engineering and Computer Science*, Vol.5, No.8, 2016.
[35] L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab and A. A. F. Loureiro, "SecLEACH - A Random Key Distribution Solution for Securing Clustered Sensor Networks," *Fifth IEEE International Symposium on Network Computing and Applications (NCA'06)*, Cambridge, MA, pp. 145-154. 2006.

BIOGRAPHIES OF AUTHORS

Yogessh A.C. has completed B.E (CS&E) in 2006 from VTU, Belagavi, Karnataka, India. I have done M.Tech (CS&E) in 2008 from VTU, Belagavi, Karnataka, India. Presently He is pursuing his PhD from Nagarjuna College of Engineering & Technology, Karanataka, India, VTU, Belagavi, Karnataka, India. He has around 7 years of teaching and 4 years of industrial experience. His areas of interest are Wireless Sensor Network, Adhoc Network.

Shantakumar B. Patil has completed B.E in 1993 from karanataka University, Dharwad and M.Tech from VTU, Belagavi, Karnataka, India. He has completed his PhD from Dr. MJR Eductioanl & Research Institute University, Chennai, India in 2011.Presently He is workingas as a professor in Department of CSE at Nagarjuna College of Engineering & Technology, Karanataka, India.

Premjyoti Patil has completed B.E in 1994 from Gulbarga University, Gulbarga and M.E from Gulbarga University, Gulbarga, India. She has completed his PhD from Dr. MJR Eductioanl & Research Institute University, Chennai, India in 2012.Presently She is workingas as a professor in Department of Electronics & Communication at Nagarjuna College of Engineering & Technology, Karanataka, India.

Roopashree H.R. has completed B.E (E&C) in 2006 from VTU, Belagavi, Karnataka, India. She has done M.Tech (CS&E) in 2012 from VTU, Belagavi, Karnataka, India. Presently She has complted her PhD from CHRIST (Deemed to be University) Bengaluru, Karanataka, India. She has around 12 years of industrial experience. Presently working as a Senior Associate TRM at Publicis.Sapient at Bengaluru, Karnataka, India.