Energy Efficient Secure Key Management Scheme for Hierarchical Cluster Based WSN

B.S. Venkatesh Prasad[1*] and H.R. Roopashree[2]

[1*]Assistant Professor, Department of CSE, Government Engineering College, K R Pet, India.
venkyp25@gmail.com, Orcid: https://orcid.org/0009-0009-2068-4167

[2]Associate Professor, Department of CSE, GSSSIETW, Mysuru, India.
roopashreehr@gsss.edu.in, Orcid: https://orcid.org/0000-0003-2287-9389

Received: February 27, 2023; Accepted: April 06, 2023; Published: May 30, 2023

Abstract

Advance development in wireless sensor network (WSN) has offered tremendous applications in various fields. WSN consists of tiny sensors with unique features, capable of processing the sensed data and are resource constrained. WSN provides robust connection between objects to share information via wireless medium. Despite the significance, WSN face several issues such as more energy consumption, bandwidth constrain and security. Due to open environment and wireless medium secure data transmission within WSN is a critical issue, thus to cope with WSN applications a robust security development is required. Cluster based hierarchical network guarantees energy efficient over flat network. However existing security scheme employs high computational cryptographic functions which consumes more energy and has higher computational overhead. In this work we propose energy efficient hybrid secure key management scheme (EEHSKM) for secure communication from cluster head to base station. This scheme aims to optimize public key cryptographic steps and utilizes symmetric key cryptographic operations which extensively reduce energy consumption and ensures secure communication. The simulation results are evaluated to achieve QoS metrics.

Keywords: Energy Efficient, Clusters, Key Management, Security and WSN.

1 Introduction

Communication has been revolutionized in the field of data gathering and remote sensing. Low-powered and inexpensive tiny micro-sensor devices are widely designed and used in WSN (Akyildiz et al., 2002; Tubaishat et al., 2003; Al-Karaki et al., 2004). Sensor nodes are distributed in a sensing area, nodes cooperate to detect, process and transmit information via wireless medium (Cai et al., 2018; Zhou et al., 2003). WSN is responsible for two important tasks: target tracking and event monitoring. WSN tracking applications include tracking of multiple things such as forest monitoring, object tracking or human activity tracking. Tiny nodes are uniformly or randomly distributed without the need for human intervention. WSNs is been utilized in various application fields such as military, intelligent infrastructure monitoring, hospitals, environment monitoring and mission critical networks due to its low cost, fault tolerance and self-organizing characteristics (Akyildiz et al.,2002). Sensor nodes are

Journal of Interner Services and Information Security (JISIS), volume: 13, number: 2 (May), pp. 146-156
DOI: *10.58346/JISIS.2023.I2.009*

*Corresponding author: Assistant Professor, Department of CSE, Government Engineering College, K R Pet, India.

battery operated and are constrained to bandwidth, storage, computation and energy. Due to continuous sensing, the nodes energy gets depleted faster which may lead to death of node and results in network degradation. Therefore, it is required to optimize nodes energy consumption in order to prolong network lifetime (Pantazis et al., 2006). Hierarchical cluster-based routing algorithms have proven energy efficient and offers better solution to extend network lifetime compared to flat routing. Cluster based algorithms organize WSN into group of clusters each group contains cluster head (CH) and cluster members (CM). CH is responsible to gather information from CM, aggregate the collected data and forwards towards data collection node known as base station (BS) or sink node through single or multihop transmission (Younis O et al, 2006, Afsar et al, 2014, Jan et al, 2017, Elshrkawey et al, 2018). Since nodes communicate through wireless medium and deployed in open environments, nodes are more often exposed to various kinds of attacks wherein an adversary node can eavesdrop the packets and alter the data. An adversary node aims to attack cluster head or misbehaves on the path towards BS by eavesdrop the packets. Therefore, CH is quite exposed to several types of attacks than cluster members. Communication between CH and BS can be made secured by integrating cryptographic techniques using symmetric or asymmetric keys which provide stronger security (Bose and Kumar, 2016). Cryptographic techniques have more computational function and overhead which is a significant issue for resource constrained nodes. Several key management schemes (KMS) using symmetric and asymmetric have been proposed to benefit scalability and has better security advantages (Lee et al., 2007). However, such key management schemes cannot be applied for hierarchical cluster-based network due to their shortcomings of not providing complete security. This paper proposes an energy efficient hybrid secure key management key scheme which integrates the combination of symmetric and asymmetric cryptographic methods for hierarchical cluster to provide secure communication between CH and BS. This scheme optimizes cryptographic steps and utilizes symmetric key operation can easily be adopted across different frameworks. Main contributions of proposed scheme are: Light weighted secret key generation mechanism using XOR function, for secure routing through CH to BS. Combining symmetric and asymmetric key cryptographic based hybrid scheme is employed. EEHSKM scheme has more robustness over node capture attack and consumes less amount of energy. Key establishment steps have been minimized to reduce computational overhead and are light weighted. EEHSKM scheme guarantees extended network lifetime and provides adequate security.

2 Problem Definition and Motivation

Light weighted sensor nodes are resource constrained and deployed in a sensing area to monitor the activities, senor nodes are battery operated and continuously sense the information. However, it is challenging issue to achieve energy efficiency for resource constrained nodes. Energy consumption and extending network lifetime remains performance limitation factors, as nodes battery cannot be replaced once it is been deployed. Cluster based routing protocols offers reliable solution for low energy consumption, load balancing and energy efficient WSN. The data information sensed from sensor nodes are gathered by cluster head and forwarded to base station. CH and BS are connected through wireless links through shortest path. Securing these wireless links are very essential to prevent from hacker nodes which can degrade and disrupt the network performance. Due to open environment nodes in the network are vulnerable to several kinds of attacks. Various cryptographic techniques have been proposed to provide strong security from information being hacked by attacker nodes. However, these cryptographic functions have more computational overhead, more storage space and energy consumption which are major drawbacks for resource constrained nodes. This motivates us to propose a light weighted energy efficient security scheme to defend attacker nodes and provide robust security between two communicating nodes.

3 Related Works

The research work on light weighted mutual authentication protocol for real time industry applications has been presented (Gope et al., 2019). In this authentication scheme, they are providing security at a physical layer of sensor nodes. This scheme utilizes the lightweight cryptographic one-way hash function to ensure strong security from an adversary node. Secret credentials and sensitive information are not stored and uses physically unclonable function, real or random model to generate session key and bitwise exclusive (XOR) operations to strengthen the security of sensor nodes. This scheme has an advantage of lower computation overhead but fails to achieve higher WSN scalability. In 2016 (Sun X et al., 2016) have proposed self-healing modified polynomial key management scheme to resist collusion and provide strong security for revocation and addition of node. Two self-defending schemes is presented. In SCH-I the pairwise key across member and cluster group are dynamically updated and shared, which reduces the vulnerability of polynomial access. Forward security is provided by one-way hashing function and modified polynomial access provides security for backward. In SCH-II the hash chain is removed by ensuring strong security. This scheme has an advantage of providing robust security, self-adaptive capabilities that supports infinite session key issues. However, this scheme cannot reach to some nodes and has lower accessibility. In 2019 (Hamsha et al., 2019) have proposed light weighted threshold key cryptographic scheme for secure communication between cluster head and BS. This scheme uses Shamir's polynomial secret key sharing technique. The base station distributes shares of generated secret keys to cluster head, upon receiving the secret key the CH aggregates data and forward to BS. The key reconstruction takes place at BS through threshold management from different CH. This key management has an advantage of providing strong authentication between CH and BS, however this scheme has more cryptographic computational overhead in generating polynomial function. In 2020 (S. Ali et al., 2020) authors have proposed modified Diffie Hellman cryptographic scheme for secure communication in WSN. This scheme uses asymmetric key generation function to prevent man-in-the-middle attacks. This scheme provides strong authentication for hierarchical cluster-based network and provides efficient results in terms of key generation, security operations. However, this scheme has higher computation time and high data response time. In 2019 (Haseeb et al., 2019) have proposed secret sharing for IoT devices to defend against malicious attacks and to improve network lifetime. This scheme has three aspects. Network is divided into inner and outer zones depending on node positions initially, each zone contains various clusters depending on nodes transmission range. Second the secure data communication across cluster head to base station is secured through XOR function. And lastly the quantitative analysis for data routing without disturbance is considered. This scheme provides extended lifetime since it uses light weighted key sharing scheme, however this scheme suffers for large scale WSN. Many of the related works provides strong authentication which utilizes more computation overhead in executing cryptographic function. However, it is necessary to consider energy efficiency and extend network lifetime along with secure data communication. Most of the related work mainly focus on providing secure communication by employing complex Cryptographic functions that requires more computational functions to generate and authenticate nodes. Complex operations consume more energy and will incur more overhead. Light weighted key management techniques have an advantage of generating key and optimize the cryptographic functions to provide robust security.

4 Proposed Energy Efficient Hybrid Secure Key Management Scheme (EEHSKM)

Network Model

Network consists of randomly deployed sensor nodes in an area. Nodes are organized in hierarchical cluster-based model, network is segmented into group of clusters (Y. Cheng and Agrawal, 2007). Each cluster consist cluster head (CH) which gathers data from sensor (cluster members). CH aggregates data from members and forward towards base station (BS) through multi hop transmission. Figure 1 shows the cluster communication

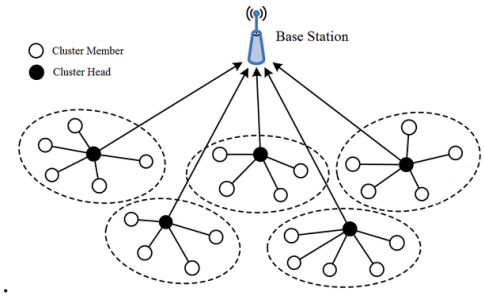

Figure 1: Network Architecture

Assumptions

1. Nodes are deployed randomly in a sensing area and all nodes are assigned with unique identifier (ID) and same initial energy (Darabkh et al., 2018, Darabkh et al., 2019)
2. Nodes are stationary, base station (BS) is placed far from WSN.
3. Neighbour nodes are computed using Euclidean distance.

$$D = \sqrt{\left(y_i - y_j\right)^2 + \left(x_i - x_j\right)^2} \qquad (1)$$

The optimal cluster formation is done according (Venkatesh Prasad and Roopashree 2021), CH collects data from CM and transmits to base station. Base station is aware of locations of all nodes and nodes utilize contention window-based transmissions. Notations and Abbreviations used is shown in table 1.

Table 1: Notations

Notations	Descriptions
Q_p	Large prime numbers $q \geq$2512
b	Complex number $b \geq$ 2512
s_n	Sensor nodes ($s_n \ldots \ldots s_1, s_2, s_3$)
s_k	Session key
ps_k	Pre-session key
h	hashing
d_{BS}	Base station private key
p_{BS}	Base station public key
CH_n	Cluster head
rni	Random number generation
E_k	Encryption with key
D_k	Decryption with key
r_{BS}	Random number of BS
r_{CH}	Random number of CH
$ps_{k'}$	New pre-session key

Energy Consumption

Proposed scheme adopts free space and multipath fading channel model for data transmission between CH to BS. Energy consumption of node depends on the distance between the transmitter node and receiver node. The radio energy consumed by node to transmit message of l bits through distance d, either using free space (d^2) or multipath fading (d^4) is computed as:

$$E_{t_x}(l,d) = \begin{cases} l * E_{elec} + l * \epsilon_{fs} * d^2 & d \leq d_0, \\ l * E_{elec} + l * \epsilon_{amp} * d^4 & d > d_0, \end{cases} \quad (2)$$

E_{elec} is the energy consumed by electronic circuit by transmitter or receiver which depends on the modulation, digital coding and propagation factors? ϵ_{fs} , represents the energy coefficient per bit for free space model when $d < d_0$ otherwise multipath fading ϵ_{amp} is used when $d > d_0$ where d_0 is the threshold value. Energy required at receiver to receive data of l bits is given as:

$$E_{r_x} = l * E_{elec} \quad (3)$$

Proposed Key Generation and Distribution Scheme

Proposed energy efficient hybrid secure key management scheme consists of four phases:

Key Preloading Phase: In this phase each sensor node is preloaded with public and private key. Base station is loaded with public key of each sensor node present in network also base station is loaded with its public and private keys.

Selection of Cluster Head-Phase: The selection of cluster head and optimal cluster formation is adopted from the work of (Venkatesh Prasad and Roopashree 2021). CH manages key management of cluster members within the cluster. Rotation of CH is done after it reaches its threshold energy value and updated in network. CH gathers information from cluster members and transmits to BS, thus CH plays major role in communicating with BS.

Session Key Establishment Phase: In this phase the session keys are established between communicating nodes such as cluster member (CM) to cluster head (CH) and cluster head (CH) to base station (BS) for secure data communication

Rekeying Phase

In rekeying phase, the cluster head generates new random number r_{ch} , BS does not consider previously generated random number therefore the new pre-session key is $ps_{k'}$ and the operation is similar to session key establishment phase.

Table 2: Pseudo Code for Session Key Establishment

Start
CH to BS
Gate way d_{BS} $(ps_k \parallel h\,(ps_k))$
BS to CH
BS to CH_n $E_{ps_k}(s_k \parallel h(s_k))$ such that $s_k = ps_k = ps_k\ XOR\ r_{BS}$
$CH_n D_{ps_k}$ $(s_k \parallel h(s_k))$
$CH_n \rightarrow s_n E_{pv}(s_k \parallel h(s_k))$
$s_n D_{pv}(s_k \parallel h(s_k))$

Table 3: Algorithm of EEHKMS

- Pre-session ps_k key is generated by CH using unique random number rni
- CH along with its hash value encrypts ps_k through BS public key p_{BS}
- BS upon receiving data, BS decrypts with d_{BS} i,e ($ps_k \parallel h\ (ps_k)$)
- Session key generated by BS is given as $s_k = ps_k = ps_k\ XOR\ r_{BS}$
- Using ps_k BS encrypts session key s_k and hash of session key $h(s_k)$ and transmits to all CH present in network.
- CH_n decrypts received information from BS and checks for the integrity of pre-session key ps_k
- CH_n encrypts the received session key combined with hash of session key $h(s_k)$ and transmits to all nodes s_n

Table 4: Pseudo Code for Re-Keying Phase

Start
CH to BS
$CH\ to\ BS \rightarrow\ E_{p_{BS}}\ (ps_{k'}\ \parallel h\ (ps_{k'}))$ ie, $ps_{k'} =\ r'_{CH}$
BS $D_{d_{BS}}(ps_{k'}\ \parallel ps_{k'})$
BS to CH
$BS \rightarrow CH_n\ E_{ps_{k'}}\ (s'_k \parallel h(s'_k))$ i,e $s_k = ps_{k'}\ XOR\ r_{BS}$
CH $D_{ps_{k'}}(s'_k \parallel h(s'_k))$
$CH_n \rightarrow\ s_n E_{pv}(s'_k \parallel h(s'_k))$
$s_n D_{ps_{k'}}(s'_k \parallel h(s'_k))$

5 Simulation and Performance Analysis

Performance of proposed EEHSKM scheme is evaluated using network simulator tool NS2 and crypto ++ libraries are used for key generation. NS2 simulator is based on C++ and TCL script which support sufficient WSN protocol, functionalities and libraries. For simulations setup we deploy 100 nodes randomly in an area of 100 x100 mts, the nodes are assigned with same initial energy and are homogeneous (Khedr, A.M., 2020). Base station is place far from sensor nodes and has infinite energy and resources. The optimal clusters are formed and CH is selected based on the high residual energy, the complete simulation parameters used is shown in table. The proposed EEHSKM scheme is compared with existing LWKMS (Hamsha and Nagaraja 2019) key management scheme and performance metrics such as energy consumption, delay, communication overhead and delivery ratio are analyzed.

Table 5: Simulation Parameters

Parameters	Values
Simulation Area	100 x 100m
Node Numbers	100
Traffic Type	CBR
Transmission Range	10 mts
Initial Energy	20 Joules
Propagation Model	Two Ray Ground
MAC Type	802.11
Protocol	Improved LEACH
No of rounds	25
No of Base Station	1

Power Consumption

Low power consumption is the fundamental goal of proposed system to extend network lifetime and performance is evaluated on sensor energy consumption. Figure 2 shows the energy consumption versus number of rounds. It is observed that as the number of rounds increases the energy consumption of nodes increases. In proposed scheme the optimal cluster formation takes place by considering energy parameters of nodes and network, however existing scheme considers only residual energy. In proposed scheme nodes consume less energy for key generation and for light weighted operation compared to existing scheme. It is observed that the existing scheme generates more number of keys since it does not concentrate on forming optimal clusters which consumes more energy.

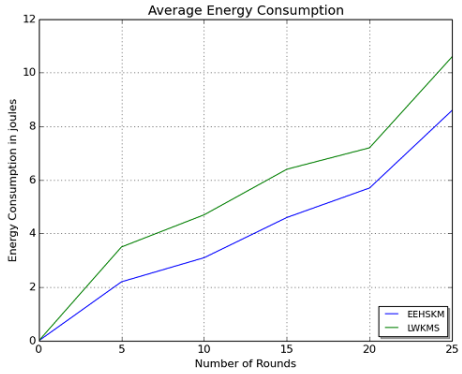

Figure 2: Energy Consumption vs Number of Rounds

Packet Delivery Ratio

Is the ratio of the packets received at BS to the number of packets sent by cluster head, the data freshness is computed as:

$$PDR\ (\%) = \frac{P_{BS}}{P_{CH}}\ X\ 100 \qquad (4)$$

Figure 3 illustrates the packet delivery ratio of proposed scheme, it is seen from the graph the packets are sent to BS through secure route by authentic nodes, however existing scheme delivers lower packets as the authentication process involves inter and intra cluster cooperative communication. Due to light weighted operation in proposed scheme helps to secure inter cluster communication such that base station has control on the entire network.

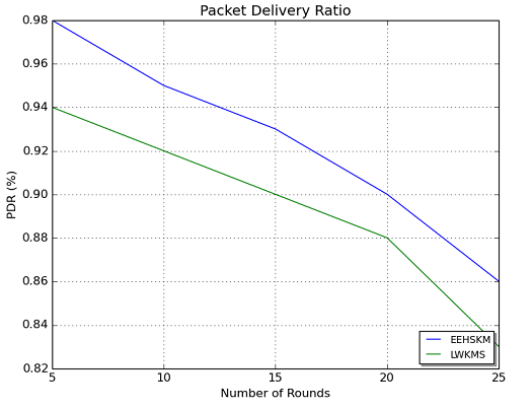

Figure 3: Packet Delivery Ratio vs Number of Rounds

Key Establishment Delay

The delay versus number of rounds is depicted in the figure 4. Proposed scheme reduces the key generation time due to reduced operation for session key establishment. The minor operation is involved between CH and CM which are based on symmetric operations and communication between CH to BS is based on asymmetric operation. Therefore, the key establishment delay is reduced compared to threshold key generation which is based on polynomial numbers.

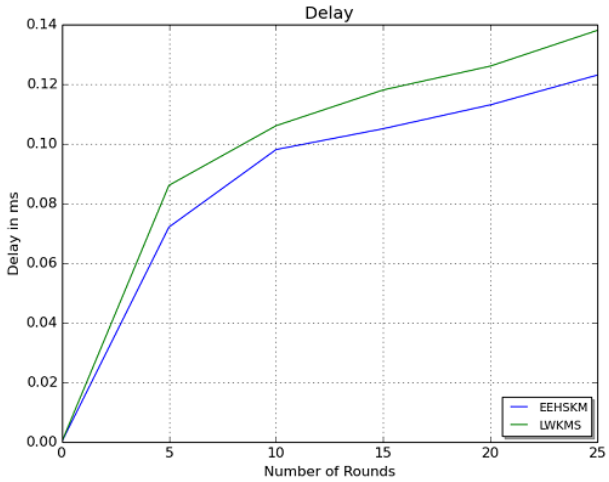

Figure 4: Delay vs Number of Rounds

Communication Overhead

Figure 5 illustrates the communication overhead of proposed scheme. It is observed from the figure that the unnecessary communication reduces which in turn reflects the low energy consumption, formation of optimal clusters and light weighted operations. Further, it also indicates the communication which reduces significantly compared to existing scheme. The transmission of fewer packets during key establishment phase between CH and BS helps to reduce amount of overhead in the network.

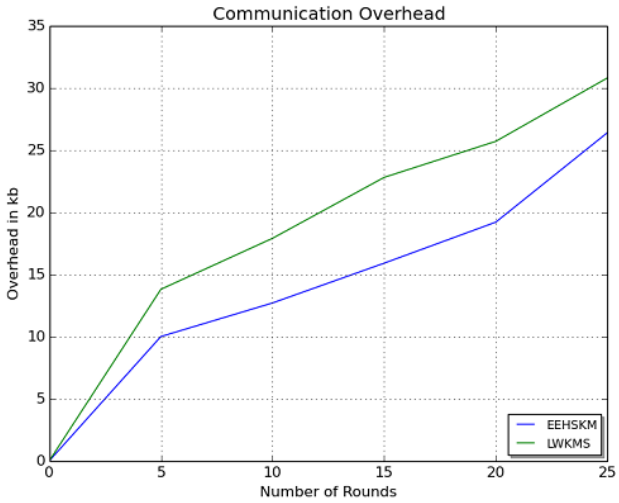

Figure 5: Comparison of EEHSKM and LWKMS for Communication Overhead

Table 6: Number of Bits Exchanged (Kbytes/Sec)

Node Numbers	LWKMS	EEHSKM
30	8.6	5.8
70	17.6	12.2
100	39.4	27.3

6 Conclusion

Due to open environment WSN is exposed to various kinds of attacks, providing data security is primary requisite for secure communication between nodes in the network. Several security schemes are proposed to provide security solutions but, these schemes cannot be configured to WSN platform due to its high computational functions. To ensure proper security and energy efficient for resource constrained WSN it is required to optimize computation functions and operations. In this paper we propose a light weighted energy efficient hybrid secure key management (EEHSKM) scheme for hierarchical WSN. This scheme combines symmetric and asymmetric cryptographic techniques to provide secure session key and reduces the computation overhead. Communication between CH and BS utilizes asymmetric operations and between sensor and CH utilizes symmetric operation. Majority of process between sensor and CH are symmetric based which consumes less energy.

The proposed scheme is scalable and can adapt to dynamic situations, the simulation results shows the better performance in terms of energy consumption, PDR, delay and communication overhead. In future, light weighted dynamic threshold key management scheme can be modeled for mobile IoT devices for secure and robust authentication for smart cities applications.

References

[1] Afsar, M.M., & Tayarani-N, M.H. (2014). Clustering in sensor networks: A literature survey. *Journal of Network and Computer applications*, *46*, 198-226.

[2] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. *IEEE Communications magazine*, *40*(8), 102-114.

[3] Ali, S., Humaria, A., Ramzan, M.S., Khan, I., Saqlain, S.M., Ghani, A., & Alzahrani, B.A. (2020). An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks. *International journal of distributed sensor networks*, *16*(6), 1-24.

[4] Al-Karaki, J.N., & Kamal, A.E. (2004). Routing techniques in wireless sensor networks: a survey. *IEEE wireless communications*, *11*(6), 6-28.

[5] Bose, S., & Vijaykumar, P. (2016). *Cryptography and network security*. Pearson Education India.

[6] Cai, S., & Lau, V.K. (2017). Modulation-free M2M communications for mission-critical applications. *IEEE Transactions on Signal and Information Processing over Networks*, *4*(2), 248-263.

[7] Cheng, Y., & Agrawal, D.P. (2007). An improved key distribution mechanism for large-scale hierarchical wireless sensor networks. *Ad Hoc Networks*, *5*(1), 35-48.

[8] Darabkh, K.A., Al-Maaitah, N.J., Jafar, I.F., & Khalifeh, A.F. (2018). EA-CRP: A novel energy-aware clustering and routing protocol in wireless sensor networks. *Computers & Electrical Engineering*, 72, 702-718.

[9] Darabkh, K.A., El-Yabroudi, M.Z., & El-Mousa, A.H. (2019). BPA-CRP: A balanced power-aware clustering and routing protocol for wireless sensor networks. *Ad Hoc Networks*, 82, 155-171.

[10] Elshrkawey, M., Elsherif, S.M., & Wahed, M.E. (2018). An enhancement approach for reducing the energy consumption in wireless sensor networks. *Journal of King Saud University-Computer and Information Sciences*, *30*(2), 259-267.

[11] Gope, P., Das, A.K., Kumar, N., & Cheng, Y. (2019). Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks. *IEEE transactions on industrial informatics*, *15*(9), 4957-4968.

[12] Hamsha, K., & Nagaraja, G.S. (2019). Threshold cryptography based light weight key management technique for hierarchical WSNs. In *Ubiquitous Communications and Network Computing: Second EAI International Conference, Bangalore, India, Proceedings 2*, 188-197. Springer International Publishing.

[13] Haseeb, K., Islam, N., Almogren, A., Din, I.U., Almajed, H.N., & Guizani, N. (2019). Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs. *IEEE Access*, *7*, 79980-79988.

[14] Hasheminejad, E., & Barati, H. (2021). A reliable tree-based data aggregation method in wireless sensor networks. *Peer-to-Peer Networking and Applications*, *14*(2), 873-887.

[15] Heinzelman, W.B., Murphy, A.L., Carvalho, H.S., & Perillo, M.A. (2004). Middleware to support sensor network applications. *IEEE network*, *18*(1), 6-14.

[16] Jan, B., Farman, H., Javed, H., Montrucchio, B., Khan, M., & Ali, S. (2017). Energy efficient hierarchical clustering approaches in wireless sensor networks: A survey. *Wireless Communications and Mobile Computing*, *2017*.

[17] Khedr, A.M., Raj, P.P., & Al Ali, A. (2020). An Energy-Efficient Data Acquisition Technique for Hierarchical Cluster-Based Wireless Sensor Networks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *11*(3), 70-86.

[18] Lee, J.C., Leung, V.C., Wong, K.H., Cao, J., & Chan, H.C. (2007). Key management issues in wireless sensor networks: current proposals and future developments. *IEEE Wireless Communications*, *14*(5), 76-84.

[19] Pantazis, N.A., Nikolidakis, S.A., & Vergados, D.D. (2012). Energy-efficient routing protocols in wireless sensor networks: A survey. *IEEE Communications surveys & tutorials*, *15*(2), 551-591.

[20] Saidi, A., Benahmed, K., & Seddiki, N. (2020). Secure cluster head election algorithm and misbehavior detection approach based on trust management technique for clustered wireless sensor networks. *Ad Hoc Networks*, *106*.

[21] Sun, X., Wu, X., Huang, C., Xu, Z., & Zhong, J. (2016). Modified access polynomial based self-healing key management schemes with broadcast authentication and enhanced collusion resistance in wireless sensor networks. *Ad Hoc Networks*, *37*, 324-336.

[22] Tubaishat, M., & Madria, S. (2003). Sensor networks: an overview. *IEEE potentials*, *22*(2), 20-23.

[23] Venkatesh Prasad, B.S. (2021). Improved energy efficient hierarchical cluster tree-based routing to prolong network lifetime. *Information Technology in Industry*, *9*(2), 694-706.

[24] Younis, O., Krunz, M., & Ramasubramanian, S. (2006). Node clustering in wireless sensor networks: Recent developments and deployment challenges. *IEEE network*, *20*(3), 20-25.

[25] Yousefpoor, M.S., Yousefpoor, E., Barati, H., Barati, A., Movaghar, A., & Hosseinzadeh, M. (2021). Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review. *Journal of Network and Computer Applications*, *190*, 1-42.

[26] Zhou, Y., Fang, Y., & Zhang, Y. (2008). Securing wireless sensor networks: a survey. *IEEE Communications Surveys & Tutorials*, *10*(3), 6-28.

Authors Biography

Venkatesh Prasad B S received the B.E degree in Computer Science and Master Degree in Information Technology from Bangalore University, Karnataka, India He is presently working as Assistant professor in the Department of Computer Science and Engineering at Government Engineering College, K, R. Pet. His main research interests include computer networks, wireless sensor networks and Machine Learning.

Dr. Roopashree H.R. has completed B. E (E&C) and M. Tech (CS&E) from VTU, Belagavi, Karnataka, India and PhD from CHRIST (Deemed to be University) Bengaluru, Karnataka, India. She has around 13 years of Industrial experience and 2 years of teaching experience. She is presently working as Associate professor in Department of CSE at GSSSIETW, Mysuru, India and supervising 6 PhD research scholars in VTU.