Secure data transmission towards mitigating potentially unknown threats in wireless sensor network

Chaya Puttaswamy[1], Nandini Prasad Kanakapura Shivaprasad[2]
[1]Department of Information Science and Engineering, GSSS Institute of Engineering and Technology for Women, Mysore, India
[2]Department of Information Science and Engineering, Dayananda Sagar Academy of Technology and Management, Bangalore, India

Article Info

Article history:

Received Sep 4, 2024
Revised Mar 4, 2025
Accepted Mar 26, 2025

Keywords:

Asymmetric
Data transmission
Encryption
Security
Symmetric
Wireless sensor network

ABSTRACT

Wireless sensor network (WSN) is known for its wider range of applications towards sensing physical attributes over human-inaccessible regions. With consistently rising concerns of security threats, WSN is the pivotal topic of network security. A literature review showcases the shortcomings of conventional data transmission schemes in WSN. This manuscript introduces an innovative approach to mitigating the potentially vulnerable and unknown threats. The implemented model promotes a group-based communication followed by a newly introduced threat onlooker node capable of identifying the malicious request of a newly designed adversary module. The scheme also hybridizes symmetric and asymmetric encryption at the end to cipher the aggregated data. The validation of the model is carried out considering standard scores of simulation parameters related to system variables. Further, the scheme has been compared with frequently adopted real-world encryption algorithms. Scripted in MATLAB, the model is assessed to confirm 35% of increased residual energy, 57% of better threat detection, 27% of enhanced throughput, and 68% of reduced processing time in contrast to existing secure data transmission schemes.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Chaya Puttaswamy
Department of Information Science and Engineering
GSSS Institute of Engineering and Technology for Women
Mysore, India
Email: chayaneetha@gmail.com

1. INTRODUCTION

Wireless sensor network (WSN) is characterized by highly connected sensors with each other to capture physical information, followed by processing leading to the generation of aggregated sensory data that is forwarded to the sink node [1]. The aggregated information can be used for various wider range of applications right, from the healthcare sector to tactical defence [2]. Owing to the advantageous features of miniature sensor nodes in WSN, it is considered an integral part of internet-of-things (IoT) [3], edge computing [4], advanced sensing technology [5], and future communication systems [6]. WSN is also known for various ongoing issues related to energy [7], routing [8], traffic management [9], and security [10]. Out of all these, security has been a primary concern to date due to various types of threats, e.g. eavesdropping, data tampering, denial-of-service (DoS), node compromise, Sybil attack, wormhole attack, sinkhole attack, and replay attack [11]. To date, there have been various schemes to solve these security issues. The core solution methodologies are based on integrity checks, secure routing protocols, encryption and authentication, intrusion detection and prevention system [12]-[15]. Irrespective of the presence of various solutions towards secure data transmission in WSN, there are various challenges. The first challenge towards imposing a stronger security protocol is related to resource-constraint sensor nodes, which have limited processing power, energy resources, and memory. Hence, resources will potentially drain when attempting to implement complex cryptographic methods that adversely degrade the network lifetime of sensor nodes. Although various existing research works claim lightweight encryption solutions, they may not be resilient to potential threats in WSNs. The second challenge is associated with the dynamic topology of WSN, where sensors may be moving, leaving, or joining the network randomly. Such dynamic topology will act as an obstruction towards implementing conventional security protocols that demand a more stable and static topology of the network. The third challenge is associated with poor scalability performance as WSN can eventually scale up suddenly where the overall performance degrades with newly joined nodes or when exposed to an increased number of traffic situations. The fourth challenge relates to complex key management while using cryptographic measures, especially in dynamic network systems. Such key management operation not only saturates node resources but also takes up considerable resources from a given network system. Because of all these challenges, WSN is significantly less adaptable to novel and evolving threats. With the evolution of artificial intelligence (AI), it is now feasible to get a deeper insight into all such evolving threats [16]; however, the AI process demands potentially larger scale of resources, which is actually infeasible to be hosted within resource-constrained sensor nodes in WSN. AI processes using machine learning, deep learning, and nature-inspired algorithms demand significant training data size, which can learn the environmental vulnerabilities and safeguard them. There are ongoing works in this direction but it is more on IoT [17] and less on conventional WSN ecosystem. Therefore, there is a need to evolve with a robust and resilient solution within WSN to offer optimally secure data transmission in the presence of undefined vulnerable environments.

Various related work has been reviewed in order to identify the methodologies adopted towards frequently used secure data transmission. Babaeer and Al-Ahmadi [18] have used watermarking and homomorphic encryption schemes for identifying sinkhole attacks in WSNs. The adoption of blockchain and learning methodology was also witnessed for secured routing in WSN, as noted in the work of Prasad and Periyasamy [19], where game theory, along with generative adversarial networks, has been used for forming a multipath data routing scheme. A similar study of the adoption of encryption and blockchain was witnessed in the work of Awan *et al.* [20], where the Rivest-Shamir Adleman (RSA) is used for encryption. Ahmad *et al.* [21] have presented multi-level encryption with dynamic clustering for accomplishing higher trust in data transmission in WSN. Cheng *et al.* [22] have used an asymmetric encryption scheme with a key distribution scheme for higher reliability in data transmission with a reduction in communication load. The adoption of a symmetric key is witnessed in the work of Sipani *et al.* [23], considering cellular automata for the generation of dynamic rules. Zhang *et al.* [24] have used a homomorphic encryption scheme and digital twin technology for validating aggregated data in WSN. The adoption of trust-based computing along with energy awareness has been witnessed in the work of Han *et al.* [25], where genetic routing has been utilized for exploring optimally secure routes. Hussein *et al.* [26] have used a hierarchical routing scheme along with the integration of elliptical curve encryption and key exchange scheme. Nagaraju *et al.* [27] have presented a simplified multipath routing scheme by improving the conventional hierarchical routing scheme in WSN in order to improve the capacity of load balancing. The study presented by Nagaraj *et al.* [28] has addressed both security and energy optimization using an encryption scheme considering WSN deployed in the IoT ecosystem. Saeed *et al.* [29] and Singla *et al.* [30] have discussed cooperative and optimized routing schemes, respectively, which are known to balance both energy and security issues.

Hence, there are mainly two types of reviewed schemes, i.e., secured data transmission using symmetric or asymmetric encryption [18]-[24] and resource-efficient routing schemes [25]-[30]. The identified research problems noted from these related works are as follows: i) majority of the existing systems towards secured data transmission in WSN are biased; they either emphasize majorly incorporating encryption for security or induce certain clustering strategies for resource optimization, but not equally. ii) adoption of a complex form of encryption results in tedious key management affecting data transmission performance, iii) existing secure data transmission scheme demands apriori information of attackers and hence such schemes don’t work out effectively when WSN is integrated with exceptionally larger structure of IoT, iv) there is no reported solution towards identifying the malicious intention of any node under no-trust environment.

Hence, the aim of the proposed system is to address the above-stated identified research problem by introducing a novel secure data transmission scheme that is capable of identifying potentially unknown threats by gauging the vulnerabilities associated with their malicious intention in WSN. The scheme is anticipated to accomplish a cost-effective modelling with robust detection and mitigation capability. The proposed system offers the following novel features as value-added contributions viz. i) a topology of group communication with a distinct selection of group leader nodes for secure data transmission has been introduced, ii) a novel strategy of identifying malicious requests and vulnerable behaviour of potentially unknown adversary is designed by introducing a new attacker model, iii) the scheme can significantly confirm the presence of vulnerable node followed by restricting their intrusive movement further within the data transmission process, iv) benchmarking of proposed scheme is carried out compared with existing strategies to realize the level of effective security and data transmission performance in WSN.

2. METHOD

The core aim of the proposed study is to construct a secure data transmission scheme that is capable of resisting potential threats in any scale and form of sensor-based networks. Different from prior studies towards security-based solutions in WSN [18]-[30], the architecture of the proposed study shown in Figure 1 introduces a novelty towards resisting maximum form of threats, especially those that target to compromise the security keys within the sensors. Another essential novel contribution of the proposed scheme is towards its consistent threat-resisting performance for both WSN as well as any large-scale applications (e.g., IoT) where sensors play an integral part in communication. The architecture formed for this purpose is shown in Figure 1.

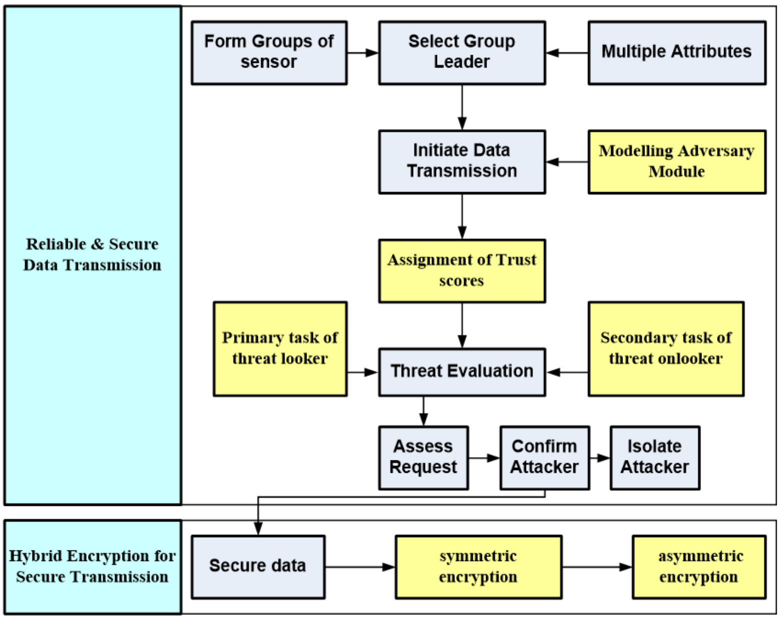
Reliable & Secure Data Transmission
Form Groups of sensor
Select Group Leader
Multiple Attributes
Initiate Data Transmission
Modelling Adversary Module
Assignment of Trust scores
Primary task of threat looker
Threat Evaluation
Secondary task of threat onlooker
Assess Request
Confirm Attacker
Isolate Attacker
Hybrid Encryption for Secure Transmission
Secure data
symmetric encryption
asymmetric encryption

Figure 1. Illustrates proposed system architecture

A closer look into Figure 1 shows that the proposed implementation model is classified into two core modules viz. i) reliable and secure data transmission and ii) hybrid encryption for secured transmission.

a) Reliable and secure data transmission: this is the first module that shapes the WSN deployment compatible for both small and large-scale data transmission using secure group-based communication. The sensors are deployed in a region to be working as a group where a specific sensor node with higher resource availability is considered as group leader (GL) where the communication takes place either both single-hop or multi-hop communication mode. The sink node is remotely mounted within the transmission region. The modelling of this topology is carried out considering i) the probability of a number of intruders, ii) the initialized energy of the node, and iii) the probability of the node playing the role of GL. The scheme introduces a specific role of threat onlooker responsible for monitoring the level of threats. Following are the events of threat detection:
   - Modelling adversary module: different from any existing approaches, the proposed study considers the presence of a highly potential adversary whose identity is challenging to be disclosed by any security module. The proposed scheme hypothesizes that all attackers, irrespective of their attack strategies, will have to incur certain costs to introduce an attack in WSN. The scheme also hypothesizes that an attacker will try to evade being detected by acting as a friendly node within WSN groups where no member of the groups will eventually distinguish its presence. The prime task of this adversary module is to gain maximum trust by cooperating highest number of nodes in their data transmission. The attacker will only launch a malicious program when the cost of the attack is very less. This is only possible when this attacker is enlisted in trust tables of a maximum number of nodes.

- Assignment of trust scores: the proposed scheme works on a no-trust network system where all the nodes present in communication will be required to be assessed for their trust scores. The proposed scheme introduces two forms of trust viz. i) the initial trust score is assigned by local GL and is maintained in trust score tables of all GL. This score is assigned when each member nodes are successfully registered by the GL node during group formation, ii) the secondary trust score is assigned by the neighbouring GL node in the form of global trust (or reputation) by using neighbourhood trust monitoring. Hence, an initial trust may remain the same, but secondary trust scores consistently keep changing and are stored within each neighbouring GL node's memory.
- Primary task of threat looker: one specific way to identify the proposed attacker module is to look for abnormal number of routing requests sent by unregistered nodes, especially using multi-hop and not much in single-hop communication. It can be justified as attacks propagated on multi-hop mode will introduce higher damage with less cost of attack compared to single hop mode. The proposed scheme solves this issue by introducing a threat onlooker, which could be any sensor node that has identified an abnormal number of requests from unregistered nodes. The onlooker node could usually be a member node and not much on the GL node as the latter is already endowed with massive data aggregation tasks. The onlooker will check both the trust scores. In the case of an attacker, the initial trust score may be compromised but they will not have a possession of secondary trust scores. This fact can be exploited by a threat onlooker module where the forged trust score presented by an attacker will not match the secondary trust computed by neighbouring GL nodes. Hence, the primary task of the threat onlooker is to confirm the presence of an adversary.
- Secondary task of threat onlooker: once the adversary has been identified, the secondary task of threat onlooker is initiated. The request to connect with a certain sensor node present in multi-hop by the adversary node is considered by the onlooker which then responds with sharing information of routes. The onlooker shares the route information between the attacker node and certain nodes which doesn't exist in the entire network, with the last node in the advertisement message connecting with the requested target node (victim). The requestor node (i.e., attacker) will need to accept this response and perform allocation of resources to transmit their data via their counterfeited routes. There are two possibilities viz: i) if the adversary chooses to perform data transmission via that route, they will end up draining complete resources with no positive exploration of the destination node as no such node ever exists, and ii) if the adversary node chooses not to accept the response route, they will be immediately blacklisted. Hence, either way, the adversary will end up in a vicious cycle of data transmission, isolating them from the core network.

b) Hybrid encryption for secure transmission: This is the second module of implementation where symmetric and asymmetric encryption have been used to resist further entry of any malicious adversaries. This justification of this module is that there is still a possibility that certain violaters (i.e., requestor nodes) will amend their identity information and further try to intrude on the network. In such cases, newly evolving violators will be stopped using this security module. The proposed scheme will initially construct a many-logic scheme where multiple rules will be formed based on the distance among the nodes, sink, residual energy, and the security assumption in the previous module to further select the optimal GL node. The data forwarded by the GL is initially secured by a symmetric encryption key followed by encrypting with asymmetric encryption. It is to be noted that the network doesn't store any form of key information in order to resist any malicious reutilization of secret keys. In such cases, the private keys must be computed by the destination node (sink), where there is an abundant resource. Hence, the proposed module doesn't offer any form of surplus resource consumption by incorporating a hybrid encryption scheme, as no sensors (either member nodes or GL) are required to perform decryption. Even if the sensors perform multi-hop communication, the intermediate node is not required to perform decryption as they only give the address to the next destination node. Apart from accessing addresses of the following neighbouring nodes, the auxiliary GL node doesn't need any other information. In case of the presence of any curious or rogue GL node, the first module will be operational to identify the malicious behaviour and restrict them by blacklisting such nodes. Hence, the proposed scheme offers a solution by resisting any unknown and potential threats in WSN.

3. RESULT

This section highlights the outcome accomplished by implementing the proposed study model. It should be noted that implementing the proposed system includes users and novel actors (threat onlookers), hence, a specific assessment strategy. The discussion of the outcomes is carried out concerning the adopted environment of simulation, accomplished outcomes, and discussion of the study's core findings.

3.1. Simulation environment

The assessment of the proposed study implemented in MATLAB is carried out considering 500-1,000 sensor nodes deployed in a simulation area of 500×900 m^2 with randomly deployed sensors. All the sensors are initialized with 50J of energy, while 50 nj/bit is considered for transmission and reception energy. The simulation is carried out for 2,500 iterations with 2,000 bits of data packet size and 32 bits of control message. As the proposed study introduces a secured data transmission scheme, therefore, it has been compared with two types of existing schemes briefed in related work of section 1 viz. i) Exist1: secured routing schemes using symmetric and asymmetric encryption [18]-[24] and ii) Exist2: resource-efficient routing schemes [25]-[30]. The proposed scheme implements the advanced encryption standard (AES) as symmetric encryption and the RSA as asymmetric encryption. The assessment is carried out considering multiple performance metrics, e.g., remnant energy, throughput, energy fluctuation, and processing time.

3.2. Results accomplished

The outcome accomplished from the analysis of the model adopting the above-mentioned simulation model is that the proposed scheme achieves approximately 35% increased retention of energy (Figure 2), 57% of increased threat detection via increased resource fluctuation identification (Figure 3), 27% of increased throughput (Figure 4), and 68% of faster processing time (Figure 5). The outcomes eventually exhibited better performance of the proposed system with respect to both security and data transmission performance cost-effectively.

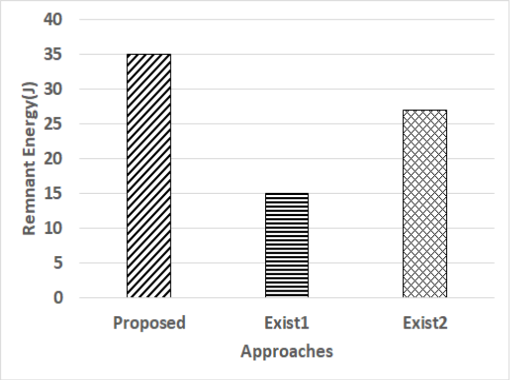

Figure 2. Analysis of remnant energy

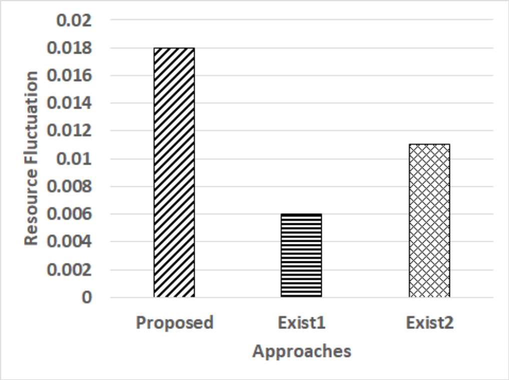

Figure 3. Analysis of resource fluctuation

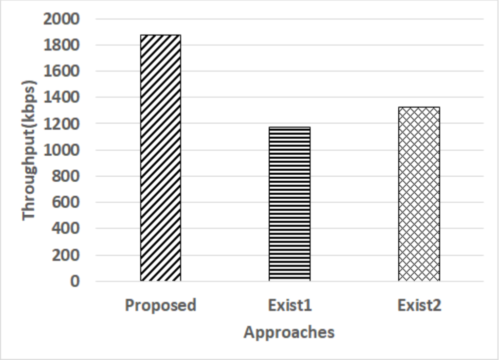

Figure 4. Analysis of throughput fluctuation

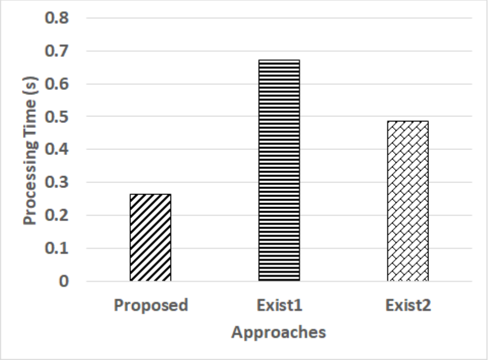

Figure 5. Analysis of processing time

Remnant energy is computed as monitoring the current amount of available energy. The event of resource fluctuation will be noticeable, especially during an attack. Hence, higher identification of resources is an indicator towards attacker confirmation. Once the attack has been identified, the allocation of resources drops down to a normal state. Throughput is computed by monitoring the amount of data transmitted to the destination over unit time while processing time is computed by observing total duration consumed to securely transmit the data to the destination node.

3.3. Discussion of results

The essential interpretation based on key findings is manifold. The study's outcome evidently showcases the significantly high resource effectiveness with better consistently towards the resource utilization. This can be witnessed in Figure 2 and Figure 3 as a key piece of supporting evidence. Based on the outcome, it can be stated that the proposed scheme, without using any complex encryption, is capable of identifying and resisting threats. From the perspective of data transmission performance, it was noted that the proposed scheme accomplished noticeable performance, which is mainly because it uses a well-channeled network that performs three parallel tasks at one instance, viz. i) consistent identification of nodes with malicious intention, ii) executing encryption to secure transmission, and iii) continuing ongoing transmission. Hence, throughput is less affected, as noticed in Figure 4.

In the perspective of comparison and contrast with a previous study, a closer look into the outcomes (Figures 2-5) showcases that encryption-based schemes (Exist1) underperform in contrast to non-encryption-based schemes (Exist2). The prime reasons behind this are: Exist1 scheme mainly includes multiple and iterative encryption steps with a higher dependency on managing the secret key. Further, this scheme is only subjective to stop intrusion when apriori information of an adversary is considered in a model, which is quite a less practical measure. The Exist2 schemes are mainly related to hierarchical routing schemes whose data transmission performance is much better owing to the non-inclusion of sophisticated encryption schemes. Although this scheme can offer better resource management, their resiliency to resist potentials is quite degraded.

On the other hand, the prime strength of the proposed scheme is the inclusion of hybrid encryption using AES and RSA, which is used only once for encrypting the final aggregated data, which doesn't induce extensive resource consumption. Another significant strength is proposed scheme uses a scheme that can detect and isolate the node with malicious intentions on varied nodes with large interconnections. Hence, it offers more scalable performance in contrast to the existing system.

It should be noted that the purpose of the proposed study is to accomplish a secure communication system capable of protecting WSNs from unknown threat definitions. Additionally, a deeper insight into the proposed scheme showcases that the prime contribution towards strengthening security is accomplished by the threat onlooker module. The task within this module is carried out by any legitimate and registered node while it is only operated upon positive confirmation of malicious node. Hence, there is no computational burden induced by the proposed scheme towards secured data transmission in WSN.

4. CONCLUSION

The prime discovery of information from current work is that-it is feasible to design a potential security solution without deploying a complex encryption standard, which otherwise increases the saturation state of resource-restricted sensor nodes. At present, there are various cadres of research work carried out to strengthen the secure data transmission in WSN. However, the majority of security approaches in WSN are based on encryption-based routing approaches, which subjectively offer success with dependency on the apriori definition of an attacker. Hence, the proposed study introduces a novel data transmission model that uses both encryption and non-encryption-based strategies to identify and resist the potential form of unknown threats in WSN. The novel features introduced in a proposed study in the form of contribution are as follows: i) a group-based communication system with unique selection strategy of GL node based on probability aspect of the intruder is presented in the proposed study, ii) a threat onlooker module is presented in a study which is capable of identifying the malicious form of a request from the unknown or vulnerable node, iii) a unique form of isolating the adversary from participating in normal data transmission in WSN has been introduced which either results in complete drainage of resources or end up being blacklisted, iv) hybrid encryption is used for securing the aggregated data after confirming the threat to ensure second level of security, v) the study outcome is compared with existing data transmission scheme to find proposed scheme excel better transmission performance. Based on the stated-accomplishment, it can be stated that the proposed study can be used for securing sensors deployed in IoT, which encounters an exponentially higher number of threats. Future work can be continued towards further optimizing the security strength by considering more vulnerable conditions with multiple and heterogeneous attacks on a larger scale. Various intelligent and optimization algorithms can be investigated to explore solutions in this perspective.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Chaya Puttaswamy	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Nandini Prasad Kanakapura Shivaprasad		✓				✓		✓	✓	✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis

I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting

Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

- The data that support the findings of this study are available from the corresponding author, upon reasonable request.

REFERENCES

[1] R. Sridhar and N. Guruprasad, “Energy efficient chaotic whale optimization technique for data gathering in wireless sensor network,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 4, pp. 4176–4188, Aug. 2020, doi: 10.11591/ijece.v10i4.pp4176-4188.

[2] M. Majid *et al.*, “Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: a systematic literature review,” *Sensors*, vol. 22, no. 6, p. 2087, Mar. 2022, doi: 10.3390/s22062087.

[3] A. H. Najim and S. Kurnaz, “Study of integration of wireless sensor network and internet of things (IoT),” *Wireless Personal Communications*, Aug. 2023, doi: 10.1007/s11277-023-10556-4.

[4] Q. He, H. Zhao, Y. Feng, Z. Wang, Z. Ning, and T. Luo, “Edge computing-oriented smart agricultural supply chain mechanism with auction and fuzzy neural networks,” *Journal of Cloud Computing*, vol. 13, no. 1, p. 66, Mar. 2024, doi: 10.1186/s13677-024-00626-8.

[5] R. Sharma, “Advanced wireless sensor networks,” in *Emerging Computing Paradigms*, Wiley, 2022, pp. 177–191.

[6] R. S. Rathore, S. Sangwan, O. Kaiwartya, and G. Aggarwal, “Green communication for next-generation wireless systems: optimization strategies, challenges, solutions, and future aspects,” *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, Jan. 2021, doi: 10.1155/2021/5528584.

[7] E. A. Evangelakos, D. Kandris, D. Rountos, G. Tselikis, and E. Anastasiadis, “Energy sustainability in wireless sensor networks: an analytical survey,” *Journal of Low Power Electronics and Applications*, vol. 12, no. 4, p. 65, Dec. 2022, doi: 10.3390/jlpea12040065.

[8] A. R. Gaidhani and A. D. Potgantwar, “A review of machine learning-based routing protocols for wireless sensor network lifetime,” *Engineering Proceedings*, vol. 59, no. 1, 2023, doi: 10.3390/engproc2023059231.

[9] F. Alharbi, M. Zakariah, R. Alshahrani, A. Albakri, W. Viriyasitavat, and A. A. Alghamdi, “Intelligent transportation using wireless sensor networks blockchain and license plate recognition,” *Sensors*, vol. 23, no. 5, p. 2670, Feb. 2023, doi: 10.3390/s23052670.

[10] A. Rehman *et al.*, “Ensuring security and energy efficiency of wireless sensor network by using blockchain,” *Applied Sciences (Switzerland)*, vol. 12, no. 21, p. 10794, Oct. 2022, doi: 10.3390/app122110794.

[11] A. Meleshko and V. Desnitsky, “The modeling and detection of attacks in role-based self-organized decentralized wireless sensor networks,” *Telecom*, vol. 5, no. 1, pp. 145–175, Feb. 2024, doi: 10.3390/telecom5010008.

[12] J. Sen, “A survey of cryptography and key management schemes for wireless sensor networks,” in *Wireless Sensor Networks - Design, Applications and Challenges*, IntechOpen, 2023.

[13] S. K. Erskine, “Secure data aggregation using authentication and authorization for privacy preservation in wireless sensor networks,” *Sensors*, vol. 24, no. 7, p. 2090, Mar. 2024, doi: 10.3390/s24072090.

[14] Y. A. Yahya, S. Raed, A. M. H. Darghaoth, and S. A. Majeed, “Secure routing protocol for wireless sensor networks: survey,” in *2022 8th International Engineering Conference on Sustainable Technology and Development (IEC)*, Feb. 2022, pp. 155–160, doi: 10.1109/IEC54822.2022.9807582.

[15] S. Szymoniak, “Key distribution and authentication protocols in wireless sensor networks: a survey,” *ACM Computing Surveys*, vol. 56, no. 6, pp. 1–31, Jun. 2024, doi: 10.1145/3638043.

[16] S. El khediri *et al.*, “Integration of artificial intelligence (AI) with sensor networks: trends, challenges, and future directions,” *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 1, p. 101892, Jan. 2024, doi: 10.1016/j.jksuci.2023.101892.

[17] M. Karthikeyan, D. Manimegalai, and K. RajaGopal, “Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection,” *Scientific Reports*, vol. 14, no. 1, p. 231, Jan. 2024, doi: 10.1038/s41598-023-50554-x.

[18] H. A. Babaeer and S. A. Al-Ahmadi, “Efficient and secure data transmission and sinkhole detection in a multi-clustering wireless sensor network based on homomorphic encryption and watermarking,” *IEEE Access*, vol. 8, pp. 92098–92109, 2020, doi: 10.1109/ACCESS.2020.2994587.

[19] K. H. V. Prasad and S. Periyasamy, “Secure-energy efficient bio-inspired clustering and deep learning-based routing using blockchain for edge assisted WSN environment,” *IEEE Access*, vol. 11, pp. 145421–145440, 2023, doi: 10.1109/ACCESS.2023.3345218.

[20] S. Awan, N. Javaid, S. Ullah, A. U. Khan, A. M. Qamar, and J. G. Choi, “Blockchain based secure routing and trust management in wireless sensor networks,” *Sensors*, vol. 22, no. 2, p. 411, Jan. 2022, doi: 10.3390/s22020411.

[21] R. Ahmad, R. Wazirali, T. Abu-Ain, and T. A. Almohamad, “Adaptive trust-based framework for securing and reducing cost in low-cost 6LoWPAN wireless sensor networks,” *Applied Sciences (Switzerland)*, vol. 12, no. 17, p. 8605, Aug. 2022, doi: 10.3390/app12178605.

[22] Y. Cheng, Y. Liu, Z. Zhang, and Y. Li, “An asymmetric encryption-based key distribution method for wireless sensor networks,” *Sensors*, vol. 23, no. 14, p. 6460, Jul. 2023, doi: 10.3390/s23146460.

[23] L. Sipani, J. Patel, and G. S. G. N. Anjaneyulu, “Dynamic symmetric key encryption in wireless sensor networks over cellular automata centred on groups,” in *Lecture Notes in Electrical Engineering*, vol. 700, 2021, pp. 1859–1863.

[24] Z. Zhang, W. Yang, F. Wu, and P. Li, “Privacy and integrity-preserving data aggregation scheme for wireless sensor networks digital twins,” *Journal of Cloud Computing*, vol. 12, no. 1, p. 140, Oct. 2023, doi: 10.1186/s13677-023-00522-7.

[25] Y. Han, H. Hu, and Y. Guo, “Energy-aware and trust-based secure routing protocol for wireless sensor networks using adaptive genetic algorithm,” *IEEE Access*, vol. 10, pp. 11538–11550, 2022, doi: 10.1109/ACCESS.2022.3144015.

[26] S. M. Hussein, J. A. López Ramos, and A. M. Ashir, “A secure and efficient method to protect communications and energy consumption in IoT wireless sensor networks,” *Electronics (Switzerland)*, vol. 11, no. 17, p. 2721, Aug. 2022, doi: 10.3390/electronics11172721.

[27] R. Nagaraju *et al.*, “Secure routing-based energy optimization for IoT application with heterogeneous wireless sensor networks,” *Energies*, vol. 15, no. 13, p. 4777, Jun. 2022, doi: 10.3390/en15134777.

[28] S. Nagaraj *et al.*, “Improved secure encryption with energy optimization using random permutation pseudo algorithm based on internet of thing in wireless sensor networks,” *Energies*, vol. 16, no. 1, p. 8, Dec. 2023, doi: 10.3390/en16010008.

[29] K. Saeed, W. Khalil, S. Ahmed, I. Ahmad, and M. N. K. Khattak, “SEECR: secure energy efficient and cooperative routing protocol for underwater wireless sensor networks,” *IEEE Access*, vol. 8, pp. 107419–107433, 2020, doi: 10.1109/ACCESS.2020.3000863.

[30] R. Singla, N. Kaur, D. Koundal, S. A. Lashari, S. Bhatia, and M. K. I. Rahmani, “Optimized energy efficient secure routing protocol for wireless body area network,” *IEEE Access*, vol. 9, no. 1, pp. 116745–116759, 2021, doi: 10.1109/ACCESS.2021.3105600.

BIOGRAPHIES OF AUTHORS

Chaya Puttaswamy received the B.E. degree in information science and engineering from Coorg Institute of Engineering, Ponnampet, Karnataka, India, in 2004, and the M.Tech. degree in software engineering from SJCE, Mysore, Karnataka, India in 2011. She is currently working as asst. professor in department of information science and engineering, GSSS Institute of Engineering and Technology for Women, Mysore, and Research Scholar at Dayananda Sagar Academy of Technology and Management (DSATM), Bangalore, under VTU, Belagavi, Karnataka, India. Her research interests include wireless sensor networks and communication networks. She has 18 years of teaching experience and published research articles in international journals, international conferences, and national conferences. She can be contacted at email: chayaneetha@gmail.com.

Nandini Prasad Kanakapura Shivaprasad received the B.E. degree in Computer Science and Engineering from PESIT, in 2001, M.Tech. degree in computer science and engineering from VTU, Belagavi, India, in 2005, and the Ph.D. degree in engineering from UBDT, Kuvempu University in 2014 and Postdoc Fellowship (London) in 2023. Presently, she is the dean of foreign affairs, and HOD ISE at Dayananda Sagar Academy of Technology and Management (DSATM), Bangalore. She received the best paper awards at various conferences and also received the “Bharat Jyothi Award” from India International Friendship Society, New Delhi, in August 2012. She has received appreciation certificates from NPTEL and ARPIT. She was appointed as a CSI Editorial Board Member in 2017, a AICTE Expert Member for AICTE Expert Committee in 2017 and 2016 for AICTE Expert Committee and is a member of Indian Society for Technical Education (ISTE), Institute for Smart Structures and Systems (ISSS), CSTA, and Cryptology Research Society of India (CRSI). She has served as a reviewer for IEEE, Springer, and Elsevier Conferences and for the Journal of Computational and Theoretical Nanoscience, September 2018, and had obtained various funds from AICTE, India. She can be contacted at email: drnandini.prasad1@gmail.com.