

# DDoS-attacks prevention using MinE-DT an adaptive security and energy optimization integration of NIPS in wireless sensor networks

Bharathi Ramachandra<sup>1,2,3</sup>, T. P. Surekha<sup>2,4</sup>

<sup>1</sup>Department of Electronics and Communication Engineering, Vidyavardhaka College of Engineering, Mysuru, India

<sup>2</sup>Visvesvaraya Technological University, Belgaum, Karnataka, India

<sup>3</sup>Department of Electronics and Communication Engineering, GSSS Institute of Engineering and Technology for Women, Mysuru, India

<sup>4</sup>Department of Electronics and Communication Engineering, Vidyavardhaka College of Engineering, Mysuru, India

## Article Info

### Article history:

Received Jan 11, 2024

Revised Jul 28, 2024

Accepted Aug 5, 2024

### Keywords:

DDoS attack

Direct transmission

Minimum energy routing

NIPS

WSN

## ABSTRACT

Wireless sensor networks (WSNs) have revolutionized data collection in diverse environments, from industrial settings to natural ecosystems. However, their decentralized nature and energy constraints pose unique security and operational challenges. Previous research provided foundational insights into WSN security but lacked comprehensive strategies for real-time intrusion prevention and efficient energy utilization. Our work employs a multi-layered approach, integrating network intrusion prevention systems (NIPS) with WSNs and leveraging machine learning for threat detection. We developed MinE-DT (minimum energy-direct transmission) hybrid routing an integrated WSN model that not only identifies and mitigates distributed denial-of-service (DDoS) attack but also optimizes energy consumption, ensuring prolonged network longevity without compromising security. The proposed model's distinctiveness lies in its fusion of NIPS with energy-saving algorithms, offering a dual advantage of enhanced security and energy efficiency. Utilizing a combination of simulations and theoretical analysis, our methodology yielded promising results, showcasing significant improvements in threat detection rates and energy conservation.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



## Corresponding Author:

Bharathi Ramachandra

Department of Electronics and Communication Engineering, Vidyavardhaka College of Engineering

Mysuru, India

Email: bharathi.08r@gmail.com

## 1. INTRODUCTION

In the contemporary era of digital technology, the protection of sensitive data and vital infrastructure from malicious actions has become a matter of utmost significance, hence emphasising the crucial role of cyber-security. The ever-evolving nature of cyber threats [1], [2], which encompass advanced attacks and breaches of data, underscores the need for strong defence methods. Network intrusion prevention systems NIPS play a vital function in this context, serving as a primary line of defence against invasions and unauthorised attempts to acquire access. Developing a prevention system for distributed denial-of-service (DDoS) [3] attack is a challenging task. Several papers have addressed this issue by using the methods of network intrusion detection system (NIDS) [4] and NIPS, where [5] gives the comparative analysis of machine learning algorithms. Sahu and Pandey [6] provides a comprehensive overview of DDoS attacks, their impact, and defense mechanisms, making it a valuable resource for researchers, practitioners, and policymakers in the field of cybersecurity. Alshambri *et al.* [7] insights into the challenges, threats [3], and

potential solutions such as encryption techniques, authentication mechanisms, intrusion detection systems (IDS), and secure routing protocols in safeguarding critical infrastructure and services by DDoS attack. Ahmad *et al.* [8] addresses the growing challenges in network security and focuses on IDS that inspect network traffic to ensure its confidentiality, integrity, and availability. The work presents machine learning (ML) and deep learning (DL)-based IDS as potential solutions, offering a systematic review of recent advancements in these technologies for NIDS.

Challenges of maintaining security and performance in WSNs are also reported [9]. It highlights the inadequacy of traditional security mechanisms for WSNs, which are prone to issues like nodes misbehavior and vulnerabilities to various attacks. To overcome these challenges, a fuzzy logic [10], fully distributed trust management system (DTMS). Where DTMS distinguishes itself from existing TMSs through its fuzzy-nature trust calculation, criteria trust calculation procedure, and trust forecasting capability. It integrates direct and indirect trust, combining past misbehavior with current status to robustly evaluate trustworthiness. Each node in DTMS monitors its neighbors' behavior, calculates their trustworthiness, and can even forecast future trust values. The system's performance, in terms of energy consumption, accuracy, scalability, fault tolerance, and execution speed, is demonstrated.

The message analyser scheme (MAS) can detect compromised sensor nodes susceptible to DDoS attacks and identify malicious messages transmitted to the base station [11]. This scheme stands out for its ability to distinguish between legitimate and compromised messages, thus minimizing computation and energy consumption, and enhancing message authentication. The work emphasizes the necessity of securing data packets from source nodes to destination nodes, integrating measures like data authentication and integrity. It utilizes a hash function and pre-shared keys for encryption to ensure data authenticity and integrity.

Investigating the challenges and advancements in IDS specifically designed for the internet of things (IoT) is observed in paper [12]. The work proposes a novel software-defined IDS based on distributed cloud architecture, aimed at creating a secure IoT environment. The paper highlights the importance of securing data packets from source to destination, incorporating data authentication, and integrity measures to mitigate the threats. The future direction includes developing more robust and reliable IDS technologies specifically tailored for the diverse and growing field of IoT. Another research focuses on managing DDoS attacks in WSNs [13]. Their main contribution is the development of a trace back technique (TBT) to control unwanted traffic and reduce the impact of DDoS flood attacks. This technique aims to detect DDoS attacks with high reliability, and operates in a distributed network mode, attempting to filter out most attack packets without compromising the quality of legitimate traffic. The results indicate that it significantly reduces DDoS-based flood attacks on a large scale. The study of DDoS attack detection and mitigation strategies in WSNs, which gives the overview of various attack detection mechanisms such as UDP flood attack detection, smurf DDoS attack detection, and others, analyzing their effectiveness and limitations in terms of energy consumption and resource utilization [14]. One of the key contributions of the work is the proposal of enhanced detection mechanisms and future enhancements in the field. The authors suggest dynamic threshold mechanisms and strategies to reduce resource wastage and improve attack detection efficiency.

The latest technique of exploring the use of deep learning techniques in detecting denial of service (DoS) attacks in WSNs [15], where the systems are trained on a specialized dataset for WSNs, known as WSN-DS, to detect four types of DoS attacks: blackhole, grayhole, flooding, and scheduling attacks. The paper evaluates the performance of different DL architectures, such as dense neural network (DNN), convolutional neural networks (CNN), recurrent neural networks (RNN), and a combination of CNN and RNN, using performance metrics like accuracy, precision, recall, and F1-score. The results demonstrate the effectiveness of these models in detecting DoS attacks in WSNs, with the CNN model achieving the highest performance. Another scheme software-defined trust systems (SDTS) which was designed to cope with various internal attacks like on-off attacks, bad-mouthing attacks, and garnished attacks [16]. The SDTS scheme is unique in its ability to adjust the trust range according to the application requirements and includes components such as direct and indirect communication trust, data trust, and misbehavior-based trust. The research work demonstrates how the SDTS model operates based on nodes' behavior and incorporates methods to handle natural calamities and internal attacks effectively. It compares SDTS against three recent state-of-the-art methods, showcasing its efficiency in terms of trust assessment accuracy, low false-positive and false-negative rates, attack detection rate, energy consumption, and throughput. Chaitra *et al.* [17] have proved that modifying the game theory energy balancing algorithm and use of relay nodes, improves the overall network lifetime. The routing protocol designed to optimize throughput in clustered IoT [18] demonstrate improvements in throughput, energy efficiency, and network reliability.

Based on the analysis of the solutions that has been provided, to overcome the above said limitations, a NIPS system is proposed in this paper. Given the escalating magnitude and intricacy of cyber-attacks, it has become imperative for organisations to adopt proactive security solutions capable of promptly and resolutely addressing potential threats. The NIPS system serves the dual purpose of avoiding successful

assaults and mitigating potential vulnerabilities and weak points within the network, thereby lowering the overall attack surface.

## 2. METHOD

In order to mitigate the DDoS attack in the WSNs, we proposed a novel algorithm: minimum energy and direct transmission (MinE-DT). The block diagram of the proposed work is shown in Figure 1. Here each sensor node has to pass through the NIPS module to reach the base station. The NIPS module runs with the Mine-DT algorithm, which is a combination of MinE-DT hybrid routing algorithm. The direct transmission (DT) is a straightforward approach where each sensor node sends data directly to the base station. While it's simple, it can be energy-intensive for distant nodes. On the other hand, minimum energy routing (MER) focuses on finding the path that consumes the least energy, often involving multiple hops through intermediate nodes. Both methods have their advantages and limitations. We have combined the strengths of both DT and MER to create a hybrid routing algorithm that optimizes energy consumption while ensuring efficient data transmission in WSN. The detailed working of the proposed work is explained in the algorithm steps.

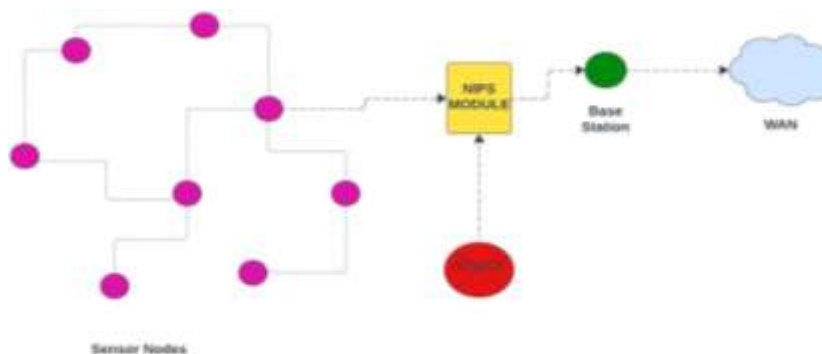


Figure 1. The general structure of the MinE-DT

The algorithm steps of Mine-DT is as follows:

- i) Initialization:
  - Determine the location of each node relative to the base station.
  - Calculate the energy required for direct transmission from each node to the base station.
- ii) Threshold setting:
  - Define a distance threshold,  $T$ . Nodes closer to the base station lesser than  $T$  will use DT, while those farther away will use MER.
- iii) For nodes within threshold (using DT):
  - Transmit data directly to the base station.
  - Update the energy status of the node after transmission.
- iv) For nodes outside threshold (using MER):
  - Use a localized search to identify the neighbouring node that results in the minimum energy consumption for data transmission.
  - Forward data to this selected neighbour.
  - The neighbour then checks its own distance threshold. If it's within the threshold, it uses DT; otherwise, it continues with MER.
  - Update the energy status of nodes involved in the transmission.

In the context of the MinE-DT algorithm for WSN, “localized search” [19] refers to a method used by nodes that are outside the threshold distance  $T$ . These nodes, instead of transmitting data directly to the base station, engage in a localized search to find the most energy-efficient path for data transmission.

Dynamic threshold adjustment:

- Periodically, or after a set number of data transmissions, re-evaluate the average energy of all nodes.
- Adjust the distance threshold  $T$  based on the network's energy status to balance the load between DT and MER.

- v) Data aggregation (optional enhancement):
  - Before data transmission, especially in the MER part, nodes can aggregate data to reduce the amount of data transmitted, further saving energy.
- vi) Energy monitoring and node replacement:
  - Continuously monitor the energy levels of all nodes.
  - If a node's energy drops below a critical level, consider it for replacement or put it to sleep to avoid network disruption.

Advantages of MinE-DT:

The advantages using the novel algorithm are

- i) Optimized energy consumption: by intelligently choosing between DT and MER based on node proximity and network energy status, the algorithm ensures efficient energy usage.
- ii) Flexibility: the dynamic threshold adjustment allows the network to adapt to changing energy conditions, ensuring longevity.
- iii) Reduced latency: nodes closer to the base station benefit from the reduced latency of DT, ensuring timely data delivery.
- iv) Scalability: the hybrid nature of MinE-DT makes it suitable for both small and large-scale WSN deployments.

Overall, the MinE-DT algorithm offers a novel approach to WSN routing by synergistically combining the strengths of direct transmission and minimum energy routing. This hybrid method promises enhanced network longevity, reduced energy consumption, and efficient data delivery, making it a promising solution for future WSN applications.

### 3. RESULTS AND DISCUSSION

The results and discussion of the MinE-DT algorithm is simulated using Python and described in this section. The parameters and metrics used for model without NIPS are the standard ones for evaluation [16]. Few parameters which are considered for the evaluation of NIPS model in this paper are given below.

#### 3.1. Detection rate

Detection rate (DR) typically refers to the percentage of actual intrusions that the system successfully detects. With NIPS, the detection rate is higher due to proactive monitoring and advanced algorithms. Detection rate is calculated by the ratio of malicious activities or intrusions correctly identified by the system out of the total number of actual malicious activities or intrusions.

$$DR = (Number\ of\ intrusions\ correctly\ detected / Total\ number\ of\ actual\ intrusions) \times 100\%$$

#### 3.2. False positive rate

The false positive rate (FPR) is one of the important metric in evaluating the performance of NIPS. FRP [20] refers to the percentage of benign activities mistakenly flagged as intrusions. A lower value of FPR indicates that the system is better at distinguishing between malicious and non-malicious activities, while a higher value of FPR may lead to more false alarms. NIPS reduce false positives through refined algorithms and continuous learning.

$$FPR = (Number\ of\ benign\ activities\ flagged\ as\ intrusions / Total\ number\ of\ benign\ activities) \times 100\%$$

#### 3.3. Latency

Latency (L) in a NIPS system impacts the system's ability to respond promptly to detected threats. Lower latency means that the system can react quickly to potential intrusions, thereby reducing the window of opportunity for attackers to exploit vulnerabilities in the network. On the other hand, higher latency can lead to delays in response times, allowing attackers more time to carry out their malicious activities. NIPS introduce a slight delay due to the additional processing required for intrusion prevention.

$$L = Time\ packet\ exits\ system / Time\ packet\ enters\ system$$

#### 3.4. Energy consumption

The energy consumed (EC) per packet. NIPS increases energy consumption due to the added computational requirements.

$$EC = Total\ energy\ consumed\ during\ transmission / Total\ number\ of\ packets\ transmitted$$

### 3.5. Network lifetime

Network lifetime (NL) in the context of a NIPS system typically refers to the duration the network remains operational before nodes start to fail due to energy depletion [10]. NIPS might reduce the network's lifetime slightly due to increased energy consumption.

$$NL = \text{Initial energy of network (sum of all nodes)} / \text{Average energy consumption rate of a node}$$

### 3.6. Packet drop rate

The packet drop rate (PDR) refers the percentage of packets that are not delivered successfully which might be dropped or lost during transmission within a network [21]. NIPS reduces packet drops by preventing malicious nodes from disrupting the network.

$$PDR = (\text{Number of packets dropped} / \text{Total number of packets sent}) \times 100\%$$

### 3.7. Throughput

Throughput (T) is an important performance metric for a NIPS system as it reflects the system's capacity to handle network traffic while performing intrusion detection and prevention tasks effectively. In a NIPS system, throughput refers to the rate at which the number of packets processed per second. There might be a slight reduction in throughput with NIPS due to the added processing overhead.

$$T = \text{Total number of packets successfully processed} / \text{Total time taken}$$

### 3.8. Node compromise rate

Node compromise rate (NCR) in a NIPS system refers to the percentage of nodes that get compromised by the attackers over a given period. A high NCR indicates that the system may be failing to detect and prevent intrusions effectively, allowing attackers to compromise a significant number of nodes within the network. While a low value of NCR results in effectiveness of a NIPS system in protecting network assets and preventing unauthorized access or malicious activities NIPS significantly reduces the node compromise rate by preventing and mitigating attacks.

$$NCR = (\text{Number of nodes compromised in a period} / \text{Total number of nodes in the network}) \times 100\%$$

The Table 1 presents these metrics with a comparison to our proposed model and Table 2 depicts these metrics and compares it with the ideal values after the simulated results.

Table 1. Metrics of evaluation with and without the function of NIPS

Sl. no	Metrics with NIPS (proposed model)	Metrics without NIPS
1	Detection rate: 98%	Detection rate: 75%
2	False positive rate: 2%	False positive rate: 10%
3	Latency: 10 ms	Latency: 5 ms
4	Energy consumption: 60 mJ/packet	Energy consumption: 40 mJ/packet
5	Network lifetime: 2 years	Network lifetime: 1.5 years
6	Packet drop rate: 1%	Packet drop rate: 8%
7	Throughput: 90 packets/sec	Throughput: 100 packets/sec
8	Node compromise rate: 0.5%	Node compromise rate: 5%

Table 2. Simulated metrics values compared with ideal values

Sl. no	Metrics	Simulated values
1	Detection rate	97%
2	False positive rate	3%
3	Latency	12ms
4	Energy consumption	58 mJ/packet
5	Network lifetime	23 months
6	Packet drop rate	2%
7	Throughput	88 packets/sec
8	Node compromise rate	1%

A mind-map in Figure 2 illustrates the novelty of the proposed system. Here's a deeper dive into the innovative facets of this proposed model:

- 1) **Advanced anomaly detection:** at the heart of the NIPS integration lies a sophisticated anomaly detection mechanism. Unlike traditional systems that rely on known signatures, this work employs machine learning algorithms to identify and respond to unprecedented threats. By continuously analyzing network traffic patterns, the system can detect even subtle deviations, ensuring that emerging threats are promptly identified and mitigated.
- 2) **Energy-efficient algorithm:** energy consumption is a paramount concern in WSNs. The proposed work introduces energy-saving algorithms that optimize NIPS operations. These algorithms ensure that nodes consume minimal energy during intrusion detection and prevention, striking a balance between security and energy conservation.
- 3) **Minimum energy algorithms:** beyond just energy-efficient security, the work incorporates algorithms designed to minimize overall energy consumption in the network. These algorithms optimize data transmission routes, sensor node activation schedules, and data processing tasks, ensuring that the network operates at peak energy efficiency.
- 4) **Adaptive learning capabilities:** the dynamic cyber threat landscape necessitates an evolving defense mechanism. The work's adaptive learning capabilities, powered by advanced machine learning techniques, allow the system to learn from its environment and past threats, refining its defense mechanisms continuously.

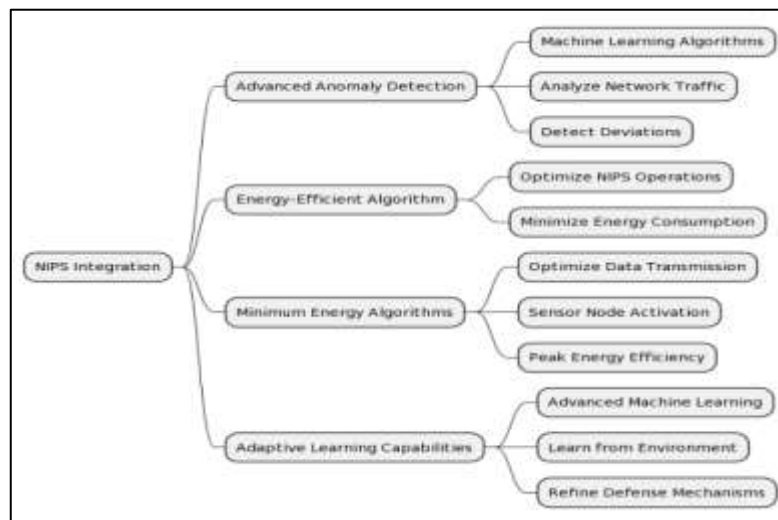


Figure 2. A mindmap diagram illustrating the novelty features

The performance of the MinE- DT was also analysed with SDTS, trust frameworks for routing, trust modeling [16], [22], [23] with AI, location-based trustworthiness using optical localization [24] and Watchdog optimization [25] as shown in Table 3, which shows that both energy consumption and anomaly detection are supported by the proposed approach. Our work shows that the MinE-DT model appears to be an innovative approach to mitigate DDoS attack. By integrating NIPS functionalities, the MinE-DT model can detect suspicious or malicious activities in real-time and take proactive measures to mitigate the impact of DDoS attacks. Future studies may explore the hybrid algorithm with feasible ways for their research work.

Table 3. Comparison of MinE-DT algorithm with other works

Sl. No	Metrics	SDTS scheme [16]	Trust frameworks for routing [22]	Trust modelling with AI [23]	Location-based Trustworthiness using optical localization [24]	Watchdog optimization [25]	Our approach
1	Behavioral analysis	Yes	Yes	No	No	Yes	No
2	Data consistency	No	Yes	No	No	No	No
3	Energy consumption	No	No	No	No	Yes	Yes
4	Anomaly detection	No	No	Yes	Yes	No	Yes

#### 4. CONCLUSION

The developed MinE-DT an integrated WSN model that not only proactively identifies and mitigates DDoS attack but also optimizes energy consumption through innovative algorithms, ensuring prolonged network longevity without compromising security. The proposed model's distinctiveness lies in its fusion of NIPS with energy-saving algorithms, offering a dual advantage of enhanced security and energy efficiency. This synergy, combined with adaptive learning, positions our work at the forefront of WSN research. Utilizing a combination of simulations and theoretical analysis, our methodology yielded promising results, showcasing significant improvements in threat detection rates and energy conservation. The MinE-DT model demonstrated superior performance compared to other approaches such as direct transmission and minimum energy routing. The MinE-DT performance was analysed using various methods including SDTS, trust frameworks for routing, trust modeling with AI, location-based trustworthiness using optical localization, and Watchdog optimization. The analysis showed that the proposed approach effectively addresses both energy consumption concerns and anomaly detection. This indicates that the MinE-DT approach offers promising capabilities in terms of efficient data transmission and robust anomaly detection, especially in environments where energy conservation and trustworthiness are critical factors. The future of NIPS is intertwined with emerging technologies, from quantum computing to the proliferation of IoT devices. As we transition to cloud-centric architectures and embrace zero-trust security models, NIPS will play even more critical role in safeguarding digital infrastructures.





#### REFERENCES

- [1] R. Soliman, "The nature of cyber threats has changed dramatically over the past three decades," *Research gate*, 2022.
- [2] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, 2021, doi: 10.1016/j.egy.2021.08.126.
- [3] M. Faris, M. N. Mahmud, M. F. M. Salleh, and A. Alnoor, "Wireless sensor network security: a recent review based on state-of-the-art works," *International Journal of Engineering Business Management*, vol. 15, p. 184797902311572, Jan. 2023, doi: 10.1177/18479790231157220.
- [4] C. Ioannou and V. Vassiliou, "An intrusion detection system for constrained WSN and IoT nodes based on binary logistic regression," in *Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, Oct. 2018, pp. 259–263, doi: 10.1145/3242102.3242145.
- [5] I. Ahmad, M. Basher, M. J. Iqbal, and A. Rahim, "Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection," *IEEE Access*, vol. 6, pp. 33789–33795, 2018, doi: 10.1109/ACCESS.2018.2841987.
- [6] S. S. Sahu and M. Pandey, "Distributed denial of service attacks: a review," *International Journal of Modern Education and Computer Science*, vol. 6, no. 1, pp. 65–71, 2014, doi: 10.5815/ijmecs.2014.01.07.
- [7] H. Alshambri, M. A. AlZain, B. Soh, M. Masud, and J. Al-Amri, "Cybersecurity attacks on wireless sensor networks in smart cities: an exposition," *International Journal of Scientific and Technology Research*, vol. 8, no. 1, 2020.
- [8] Z. Ahmad, A. S. Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: a systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, p. e4150, Jan. 2021, doi: 10.1002/ett.4150.
- [9] H. Jadidoleslamy, M. R. Aref, and H. Bahramgiri, "A fuzzy fully distributed trust management system in wireless sensor networks," *AEU - International Journal of Electronics and Communications*, vol. 70, no. 1, pp. 40–49, 2016, doi: 10.1016/j.aeue.2015.09.017.
- [10] Bhupesh, R. Nandal, K. Joshi, and O. Dahiya, "A modified approach to decrease packet loss ratio and PDR in AODV using fuzzy technique," in *2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Oct. 2022, pp. 1–6, doi: 10.1109/ICRITO56286.2022.9964527.
- [11] A. P. Abido and I. C. Obagbuwa, "DDoS attacks in WSNs: detection and countermeasures," *IET Wireless Sensor Systems*, vol. 8, no. 2, pp. 52–59, 2018, doi: 10.1049/iet-wss.2017.0029.
- [12] J. C. S. Sicato, S. K. Singh, S. Rathore, and J. H. Park, "Comprehensive analyses of intrusion detection system for IoT environment," *Journal of Information Processing Systems*, vol. 16, no. 4, pp. 975–990, 2020, doi: 10.3745/JIPS.03.0144.
- [13] R. Soni, R. Pachouri, and A. Jain, "DDoS attack detection and prevention on wireless sensor network by using TBT method," *International Research Journal of Engineering and Technology (IRJET)*, vol. 8, no. 3, pp. 737–742, 2021.
- [14] A. Dogra and T. Kaur, "DDOS attack detection and handling mechanism in WSN," *International Journal of Recent Technology and Engineering*, vol. 8, no. 3, pp. 4990–4993, 2019, doi: 10.35940/ijrte.C5644.098319.
- [15] S. Salmi and L. Oughdir, "Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network," *Journal of Big Data*, vol. 10, no. 1, p. 17, Feb. 2023, doi: 10.1186/s40537-023-00692-w.
- [16] T. Khan, K. Singh, K. Ahmad, and K. A. Bin Ahmad, "A secure and dependable trust assessment (SDTS) scheme for industrial communication networks," *Scientific Reports*, vol. 13, no. 1, p. 1910, Feb. 2023, doi: 10.1038/s41598-023-28721-x.
- [17] H. V Chaitra *et al.*, "Delay optimization and energy balancing algorithm for improving network lifetime in fixed wireless sensor networks," *Physical Communication*, vol. 58, p. 102038, 2023.
- [18] S. B. Shah, Z. Chen, F. Yin, I. U. Khan, and N. Ahmad, "Energy and interoperable aware routing for throughput optimization in clustered IoT-wireless sensor networks," *Future Generation Computer Systems*, vol. 81, pp. 372–381, Apr. 2018, doi: 10.1016/j.future.2017.09.043.
- [19] G. G. Gebremariam, J. Panda, and S. Indu, "Secure localization techniques in wireless sensor networks against routing attacks based on hybrid machine learning models," *Alexandria Engineering Journal*, vol. 82, pp. 82–100, 2023, doi: 10.1016/j.aej.2023.09.064.
- [20] M. Mathews, M. Song, S. Shetty, and R. McKenzie, "Detecting compromised nodes in wireless sensor networks," in *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007)*, Jul. 2007, pp. 273–278, doi: 10.1109/SNPD.2007.538.





- [21] Y. Cho and G. Qu, "A hybrid trust model against insider packet drop attacks in wireless sensor networks," *Sensors*, vol. 23, no. 9, p. 4407, Apr. 2023, doi: 10.3390/s23094407.
- [22] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: attack analysis and countermeasures," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 867–880, 2012, doi: 10.1016/j.jnca.2011.03.005.
- [23] M. M. Alqhatani and M. G. M. Mostafa, "Trust modeling in wireless sensor networks: state of the art," *Journal of Information Security and Cybercrimes Research*, vol. 1, no. 1, pp. 59–72, 2018, doi: 10.26735/16587790.2018.007.
- [24] L. B. Hormann, M. Pichler-Scheder, C. Kastl, H.-P. Bernhard, P. Priller, and A. Springer, "Location-based trustworthiness of wireless sensor nodes using optical localization," in *2020 IEEE MTT-S International Conference on Microwaves for Intelligent Mobility (ICMIM)*, Nov. 2020, pp. 1–4, doi: 10.1109/ICMIM48759.2020.9299094.
- [25] P. Zhou, S. Jiang, A. Irissappane, J. Zhang, J. Zhou, and J. C. M. Teo, "Toward energy-efficient trust system through watchdog optimization for WSNs," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 613–625, 2015, doi: 10.1109/TIFS.2015.2389145.

## BIOGRAPHIES OF AUTHORS



**Bharathi Ramachandra**     received the Bachelor of Engineering in Electronics and Communication Engineering from SJCE in the year 2008. Received Master Degree on Computer Network Engineering from NIE Mysuru in the year 2013. Currently working as an assistant professor in the Department of ECE, GSSSIETW, Mysuru. Her area of interests are WSNs, attacks in WSN, cryptography, cyber security, IoT, and communication systems. She can be contacted at email: bharathi.08r@gmail.com.



**Dr. T. P. Surekha**     is Professor and Dean (Student Welfare), Department of Electronics and Communication Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India. She has completed her Ph.D. in Communication Systems from Visvesvaraya Technological University, Belagavi, Karnataka, India. She has more than 30 years of teaching experience. She has published 32 national/international journals. Her areas of interests are wire and wireless communication systems, bio-medical signal processing and engineering education. She can be contacted at email: drtps@vvce.ac.in.