

Reputation-enhanced two-way hybrid algorithm for detecting attacks in WSN

Divya Bharathi Selvaraj, Veni Sundaram

Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, India

Article Info

Article history:

Received Oct 17, 2024

Revised Oct 18, 2025

Accepted Nov 5, 2025

Keywords:

Detecting attacks

Mitigating attacks

Secure hash algorithm

Two-way hybrid Algorithm

Wireless sensor networks

ABSTRACT

Wireless sensor networks (WSNs) are susceptible to a variety of attacks, such as data tampering attacks, blackhole attacks, and grayhole attacks, that can affect the reliability of communication. We proposed a reputation-enhanced two-way hybrid algorithm (RCHA) that uses cryptographic hash functions and reputation-based trust management to detect and de-escalate attacks accurately. The RCHA algorithm implements two hash functions RACE integrity primitives' evaluation message digest (RIPEMD) and secure hash algorithm (SHA-3), to initiate the integrity check for the entire packet sent across the network. Every node in the WSN tracks a reputation score for each neighbor the node is connected to, and this score is dynamically updated based on the behavior of each neighbor. If a neighboring node's reputation drops below a threshold, the node is sent a maliciousness designation. At that time, the node will broadcast an alert message to its neighboring nodes and begin to reroute its data through one of its trusted neighbors to ensure the reliability of the communication. The simulation results reported that the RCHA algorithm improved the accuracy of the attack detection rate and the number of packets delivered compared to traditional attack detection methods. The RCHA algorithm was able to maintain low computational and energy overhead for the WSN, making it an attractive option for a resource-constrained application in a WSN. Given the trends towards more collaborative networks, the reputation mechanism in the RCHA algorithm improves the overall reliability and capabilities of the WSN, regardless of adversaries.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Divya Bharathi Selvaraj

Department of Computer Science, Karpagam Academy of Higher Education

Coimbatore, India

Email: diya23nov@gmail.com

1. INTRODUCTION

The main text format consists of a flat left-right columns on A4 paper (quarto). The margin text wireless sensor networks (WSN) are spatially distributed sensor nodes that sense physical or environmental parameters and communicate the sensed data to sinks. Being deployed in open, mostly unattended locations, WSNs are very susceptible to several types of security attacks like eavesdropping, data tampering, denial-of-service (DoS), and node capture attacks. These security threats have a major impact on network performance and integrity of the data of utmost priority for military, healthcare, and environmental monitoring applications [1]-[6]. Existing security solutions, such as cryptographic protocols, represent a minimum requirement for protecting data transmission but tend to be insufficient in countermeasures against insider attacks and extremely dynamic malicious activities [7]-[11]. Reputation-based trust management has been a good complementary solution enabling nodes to make judgments about neighbors' trust on the basis of

experience. Nevertheless, reputation systems themselves are vulnerable to false positives and advanced attacks [12]-[15]. To surpass these limitations, hybrid mechanisms integrating cryptographic verification and reputation-based trust assessment have been explored. The reputation-enhanced two-way hybrid algorithm (RCHA) is introduced to advance security with two cryptographic hash functions, RACE integrity primitives' evaluation message digest (RIPEMD) and SHA-3, for strict data integrity testing, along with dynamic reputation scores for precise malicious node identification. With the use of these approaches, RCHA improves detection accuracy and repels attacks effectively while maintaining energy use under control, crucial in the scenario of the available resources in sensor nodes. Design, development, and testing of RCHA under various WSN attack strategies are presented in this paper, showing how it can provide secure and reliable communication.

The main contributions are:

- Introduces a novel two-way hybrid approach that integrates cryptographic hash functions (RIPEMD and SHA-3) with a dynamic reputation-based system to enhance attack detection and data integrity in WSNs.
- Develops a real-time reputation scoring mechanism that continuously updates based on node behavior, enabling accurate identification and isolation of malicious nodes.
- Proposes a trust-aware rerouting method that collaborates with high-reputation neighboring nodes to ensure reliable data delivery and prevent network disruption caused by compromised nodes.
- Demonstrates through simulation that RCHA achieves higher detection accuracy, improved packet delivery ratio (PDR), and lower energy consumption compared to traditional security mechanisms in WSNs.

Organization of the paper: In this paper, the introduction of detecting and mitigating attacks in WSN is explained. The related works are discussed in section 2. The development is explained in section 3. The results are discussed in section 4. The conclusions are discussed in section 5. Finally, the references are added in section 6.

2. RESEARCH METHOD

Keerthika and Shanmugapriya [16] addressed the serious security challenges of WSNs. They stressed the threats faced by WSNs from both active and passive attacks, even though WSNs operate in such a light and thin environment, i.e., resource-constrained. They presented WSNs by showing several attacks such as sinkhole, Sybil, eavesdropping and discussed their adverse effects on data integrity and the overall network performance. The authors explored many of the security countermeasures that had emerged and how they addressed these security threats with relevance to the fundamental lightweight and energy-efficient properties of WSNs. These authors' research provided the basis of understanding WSN security challenges in highly dynamic and resource-constrained environments. Khan *et al.* [17] examined how artificial neural networks (ANNs) enhance security in WSNs. They highlighted how traditional security measures were limited in detecting dynamic and advanced threats. They showed how the increasingly utilized ANNs offered an adaptive learning capability that allowed, among others, novel real-time threat detection and classification. Their research on the limitations of current approaches to enhance resilience improves efficiencies in threat responses for WSNs, allowed future implementation into WSNs with intelligent models. Kumar *et al.* [18] investigated the role of machine learning methodologies for securing WSN in 5G contexts. The authors were largely assessing eventual risk probabilities and the deployment of devices/strategies to enhance resiliency in the WSN. The authors' contribution was to demonstrate that intelligent models were being used to predict or proactively prevent potential security threats. This has been a major step forward in the development of adaptive and scalable security mechanisms in the WSN of today's world.

Lai *et al.* [19] examined the potential for online learning strategies to handle DoS attacks in WSN. The researchers focused on the dynamic nature of attacks and the immediacy of the need to provide detection. The authors were able to use adaptive models to provide improved accuracy and timeliness for potential malicious events. The article highlighted and explored the role of continual learning in developing WSN security. Madhuri and Gogte [20] presented a novel approach for an intrusion detection system that focuses on node-level drop attacks in WSNs. The research elaborated a detection approach that provided better accuracy in malicious node detection with an enhanced detection algorithm. The study underscored the potential node-level threats and even the need for localized protection. The study added knowledge towards lightweight and efficient security systems for resource-constrained WSNs.

Moundounga and Satori [21] proposed a stochastic machine learning-based framework for attack detection in WSNs. The study examined the uncertainty and variation of sensor data through probabilistic learning techniques. Their stochastic machine learning-based approach is robust in identifying an anomaly in a dynamic model. Their contribution enhanced the reliability of intrusion detection systems in WSNs. Oztoprak *et al.* [22] published a thorough review covering the aspects of security challenges, mitigation

strategies, and trends in WSNs. The paper outlined a variety of threat models, such as internal and external threats, as well as provided a review of current countermeasures. Furthermore, it focused on the necessity of evolving security methods for modern applications and the identification of future WSN security research directions.

Premkumar *et al.* [23] built a scalable and energy-friendly cluster-based anomaly detection system to protect against DoS attacks in WSNs. Where most previous research only analyzed methods to detect DoS attacks in WSNs, the hierarchical clustering-based model developed as part of their research could mitigate. Overall, the research addressed the intention of providing prolonged network lifetime, while not negotiating the protection of the WSN. The results indicated that the approach is effective for detection methods in much larger sensor deployments. Ramesh *et al.* [24] presented an optimized deep neural network model aimed at detecting DoS attacks in wireless video sensor networks. The work sought improvement over models' capability to retrieve greater real-time detection performance with reduced false positives. The convolutional neural network architecture was used with traditional methods and demonstrated significantly greater accuracy. These authors' work indicated that deep learning approaches provide opportunities to protect and secure multimedia-based WSN applications. Sadia *et al.* [25] developed an intrusion detection system based on machine learning specifically for WSNs. Their work offered a unique solution by harnessing multiple classifiers to improve the accuracy of threat detection and provide adaptability to the intrusion detection system. The study recognized challenges in the state of the art, including energy efficiency and data imbalance, while offering a practical answer regarding intelligent and lightweight security in WSN environments. Table 1 illustrates the various attacks on WSNs. The table shows the accuracy of each author's research.

Table 1. Comparison table of various authors' work on attack detection in WSNs

Authors	Year	Algorithm/Technique	Contribution	Accuracy
Salmi and Oughdir [26]	2023	Deep learning models (e.g., CNN, RNN)	Evaluated performance of deep learning techniques for DoS attack detection in WSNs	95%
Sujihelen <i>et al.</i> [27]	2022	Node replication attack detection algorithm	Proposed a distributed mechanism for detecting node replication attacks in WSNs	96.3%
Sudar and Deepalakshmi [28]	2022	Flow-based ML (e.g., SVM, random forest)	Detected and mitigated low-rate DDoS attacks in SDN using ML with traffic flow analysis	94%
Wang <i>et al.</i> [29]	2024	GD3N (Graph-based dynamic detection network)	Developed an adaptive clustering method for selective forwarding attack detection in harsh environments	97.5%
Zhai <i>et al.</i> [30]	2022	Timestamp-based MAC + Lightweight protocol	Designed a secure, energy-efficient service for attack detection in WSNs using MAC authentication	93.7%

3. MATERIALS AND METHODS

The RCHA algorithm identifies and removes attacks in WSNs while simultaneously fusing reputation-based trust evaluation and cryptographic integrity checks. Each node maintains a dynamic reputation score of its neighboring nodes by assessing their recent communication behavior. Each data packet is additionally hashed using RIPEMD and SHA-3 to detect tampering and unauthorized modifications. Whenever a malicious node is detected, special alert messages are propagated out to the rest of the nodes such that communication is rerouted through a string of trusted nodes. Further, by allowing the nodes to be aware of rehabilitation/mitigations of malicious nodes, it enhances the nodes' probability of having secure, reliable communications and further reduces the likelihood and effect of attacks. Figure 1 shows the overall architecture.

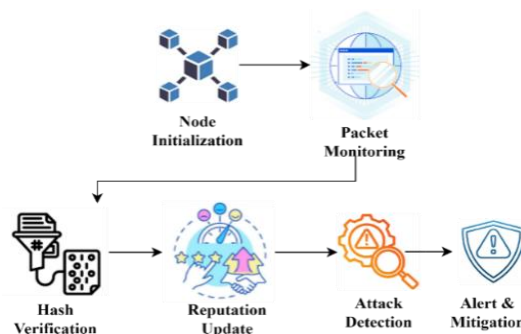


Figure 1. Overall architecture

RCHA WSNs' architecture uses several layers of security to provide effective attack detection and mitigation. Sensor nodes exchange messages and send information, and a behavior analysis module monitors them continuously. Two hash functions (RIPEMD and SHA-3) are utilized for data integrity checks. A reputation system quantifies node trust based on behavior and hash verification outcome. When such anomalies as hash mismatches or plain packet loss are identified, the system detects the evil node, sends alarm signals, and updates reputation values. Mitigation is ultimately realized by forwarding data through high-reputation, trusted nodes to ensure secure communication.

3.1. Detecting and mitigating attacks in WSNs

Attack detection and mitigation in WSNs consist of identifying rogue or malicious activities like data tampering, packet loss, or illegal access and attempting to lessen their effects. Detection is generally done using trust models, anomaly detection, or cryptography. Detection prompts mitigation through the isolation of rogue nodes, notification of border nodes, and data re-routing through trusted channels. The objective is to uphold data integrity, network availability, and system-wide dependability in the event of attacks. Figure 2 shows an example of a WSN such that nodes (A to N) are established to create an information network. All the nodes are sensors, and information moves amongst them in multi-hop mode. It shows some of the attacks in WSN.

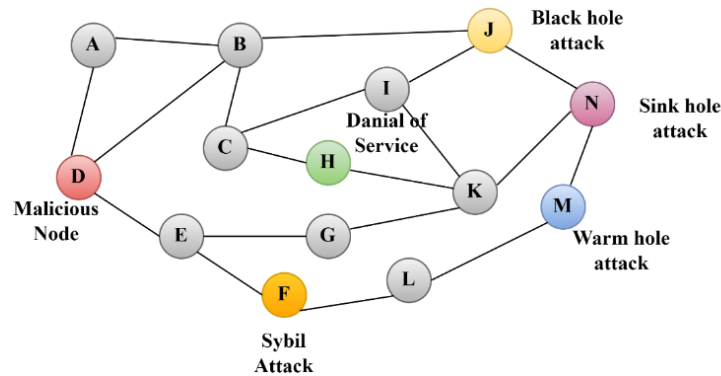


Figure 2. Some of the attacks in WSN

3.2. Reputation-enhanced two-way hybrid algorithm

The two-way hybrid algorithm with reputation enhancement (RCHA) identifies and prevents WSN attacks by applying the intersection of reputation-based monitoring and cryptographic hash functions (RIPEMD and SHA-3). Nodes hold a dynamic neighboring node reputation score based on their activities, including packet forwarding and integrity. Malicious nodes are identified and marked as suspicious by using low-scoring nodes, and warning messages are forwarded to surrounding nodes. The network subsequently steers clear of routing through malicious nodes, ensuring secure and credible data transmission. Figure 3 illustrates a secure data transfer process in the WSN using RCHA.

It starts with the deployment of sensor nodes and data transfer, then dual hashes (SHA-3 and RIPEMD) are generated to ensure data integrity verification. There is a reputation module that monitors node activity, labeling them as trusted or malicious. Once an anomaly is detected, alarms are activated, and data is passed through trusted nodes in order to deliver it in a secure way to the base station.

3.2.1. Setup simulation environment

There are many ways to execute and test the RCHA algorithm. A variety of simulation environments are available, including NS2/NS3, OMNeT++, MATLAB, or Contiki-Cooja; each will vary depending on how complex and/or visual the simulation needs to be. In this simulation assignment, an arbitrary number of sensor nodes can be deployed either in a random manner or in a grid manner into a deterministic area, which can be a WSN. The nodes can communicate with each other using CBR, UDP, or TCP traffic models to simulate the real transmission of real-time data. Modalities of attacks can also occur to test how well the RCHA can detect and mitigate threats, such as blackhole (packet dropping), grayhole (selective forwarding), Sybil (identity spoofing), and data tampering (payload tampering) attacks, to assess how much trust is degraded, how stable the misrouting gets, or how severely the data can be compromised. All of these attacks were included in the simulation setup to emulate WSN conditions while under threat appropriately.

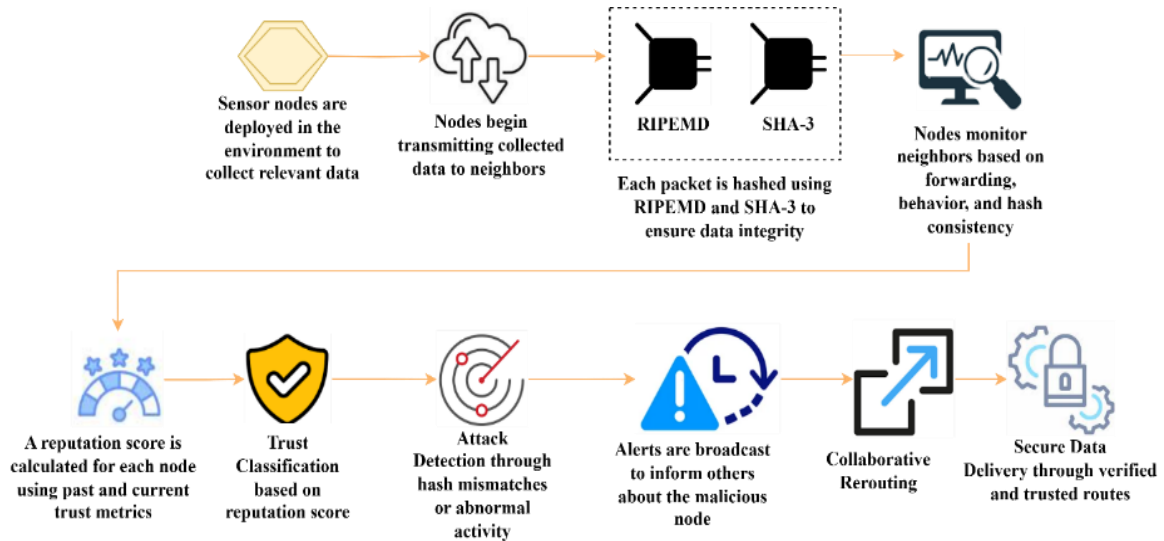


Figure 3. RCHA architecture

3.2.2. Node reputation system

In the RCHA algorithm, each sensor node in the WSN starts with a neutral reputation score of 0.5, which indicates a semi-trust state with the sensor node. As nodes perform actions, their neighboring nodes will create a set of measurements based on the three parameters: the accuracy of packet forwarding (confirming packets get relayed), response time (confirming whether responses or acknowledgments occur on time), and data integrity (verifying that the data transmitted remains unchanged through cryptographic hash functions such as SHA-3 or RIPEMD). Each sensor node, based on its observations of a node's actions, will produce binary trust values B , where $B=1$ indicates trust behavior as a sensor node and $B=0$ indicates trust for untrustworthy or malicious behavior. This will supply a base for dynamically updating the node's reputation score over time.

$$R_{new} = \alpha \cdot R_{old} + (1 - \alpha) \cdot B \quad (1)$$

Where R_{new} is updated reputation, α is the weighting factor (e.g., 0.7), and B is a binary trust behavior (1 for good, 0 for malicious). In (1) is an approach that ensures trust is adaptively assigned based on consistent behavior.

3.2.3. Attack detection logic

In the RCHA algorithm, attack detection relies on ongoing monitoring and reasoning of node behavior through both reputation and received data integrity checking. A node's behavior becomes suspect when one or more of the following occurs: If a node continuously drops packets, or shows evidence that it modified data along the way, through acknowledgments or mismatched hash values, it is considered suspicious behavior. Each node's behavior is scored over time, as established by the reputation scoring mechanism. If a node's received reputation dips beneath a threshold (e.g., < 0.3 given a scale from 0-1), it is considered not trustworthy behavior. Essentially, this decrease in score can be expected by multiple binary trust violations (e.g., not forwarding data, tampering). If the receiver encounters an excessive amount of mismatched recomputed hash values with those received in the packet (RIPEMD and SHA-3), there is strong evidence of disagreement at which suspicion lies with the sender. Once a node is flagged as malicious: upon sensing a suspicious node, the detecting node notifies its neighbors by broadcasting an alert message.

3.2.4. Mitigation strategy

In the RCHA algorithm, the mitigation approach consists of an alerting phase, in which the detecting node transmits a warning to all its neighbor nodes about the node suspected of being malicious. The algorithm can also perform routing actions to mitigate over bad routes by trying to avoid routes with reputation of zero, and try to use high reputations over low reputations when possible. Additionally, there is provision for reputation recovery, where if the node improves over time (i.e., forwards packets correctly and does not change packets), they can begin to increase its reputation gradually and have a chance of rejoining

the network fairly. Overall, these approaches will enable both secure and efficient use of WSN for communication. Algorithm 1 demonstrate the essential definition of RCHA. The aim is to enhance security through a performance-based reputation mechanism of continuously evaluates node behaviors intended to secure communication in WSNs.

Algorithm 1. Reputation-enhanced two-way hybrid algorithm (RCHA)

```

Input:
  N ← Set of all sensor nodes
  P ← Set of packets transmitted
  T ← Reputation threshold (e.g., 0.3)
  α ← Weight factor for reputation update (e.g., 0.7)
Initialize:
  For each node ni ∈ N:
    Set reputation[ni] ← 0.5
  For each packet p ∈ P:
    sender ← Source node of p
    receiver ← Destination node of p
Step 1: Data Integrity Check
  hash1 ← RIPEMD(data)
  hash2 ← SHA3(data)
  if hash1 and hash2 match the expected values:
    Behavior ← 1
  else:
    Behavior ← 0
Step 2: Update the Reputation of the sender
  reputation[sender] ← α * reputation[sender] + (1 - α) * Behavior
Step 3: Detection and Alert
  if reputation[sender] < T:
    Mark the sender as malicious
    Broadcast an ALERT to the neighbors of the sender
Step 4: Mitigation
  For each neighbor node n:
    if reputation[n] ≥ T:
      Reroute packets via node n
    if else:
      Avoid sending packets through node
  else:
    Continue normal communication
End For
Output:
  Secure routing paths, avoiding malicious nodes
  Reputation scores of all nodes

```

4. RESULTS AND DISCUSSIONS

The results of this study evaluated the RCHA algorithm based on WSN simulation parameters and determined a positive impact on attack detection as well as a positive impact on data delivery reliability. RCHA method was able to achieve a better detection accuracy when measuring reliability systems than the common trust-based approach or the common cryptographic approach, as it was able to use dual hash verification (RIPEMD and SHA-3) along with adaptive reputation scoring and successfully found malicious nodes while maintaining a better PDR. Also, the overhead from using hashing was near negligible in comparison to the enhancement in security offered by hashing. Energy consumption was found to be balanced with the RCHA method offering trust-based selective rerouting. Overall, the RCHA method performed better than baseline methods when securing communication in WSN systems. Table 2 shows the simulation parameters used in mitigation attacks in WSNs. These parameters can be tuned based on the scenario (e.g., military vs environmental WSN) and the size of the network. Figure 4 shows the detection accuracy of watchdog, pathrater, SAODV and proposed RCHS. This shows the efficiency of the proposed methods in detecting and mitigating attacks in WSNs. In this chart, the x-axis shows the node sizes and the y-axis shows the accuracy values. Figure 5 shows the PDR of watchdog, pathrater, SAODV and proposed RCHS. This shows the efficiency of the proposed method in detecting and mitigating attacks in WSNs. In this chart, the x-axis shows the node sizes and the y-axis shows the PDR values in percentage.

Figure 6 shows the energy consumption of watchdog, pathrater, SAODV and proposed RCHS. This shows the efficiency of the proposed methods in detecting and mitigating attacks in WSNs. In this chart, the x-axis shows the node sizes and the y-axis shows the energy consumption values in joules. Figure 7 shows the delay of watchdog, pathrater, SAODV and proposed RCHS. This shows the efficiency of the proposed methods in detecting and mitigating attacks in WSNs. In this chart, the x-axis shows the node sizes and the y-axis shows the delay values in seconds. Figure 8 shows the throughput of watchdog, pathrater, SAODV and

proposed RCHS. This shows the efficiency of the proposed methods in detecting and mitigating attacks in WSNs. In this chart, the x-axis shows the node sizes and the y-axis shows the throughput values in Mbps. Figure 9 shows the overhead comparison of watchdog, pathrater, SAODV and proposed RCHS. This shows the efficiency of the proposed methods in detecting and mitigating attacks in WSNs. In this chart, the x-axis shows the node sizes and the y-axis shows the overhead values based on packets.

Table 2. Simulation parameters

Parameter	Typical value/range	Description
Simulation area	500m × 500m / 1,000m × 1,000m	Defines the physical space for WSN deployment.
Number of nodes	50 – 200	Total sensor nodes deployed in the network.
Node placement	Random / Grid	How are nodes distributed across the area.
Transmission range	50 – 100 meters	Maximum communication distance between nodes.
Initial energy per node	2 – 5 Joules	Used to evaluate energy efficiency.
MAC protocol	IEEE 802.15.4 / CSMA/CA	Medium access control protocol for WSNs.
Routing protocol	AODV / LEACH / RCHA (custom)	Routing method to evaluate and compare.
Traffic type	CBR (Constant Bit Rate)	Type of data transmission pattern.
Packet size	64 – 512 bytes	Size of each transmitted data packet.
Simulation time	500 – 1000 seconds	Total duration of the simulation.
Hash algorithms used	RIPEMD, SHA-3	Used for a data integrity check.
Attack type simulated	Blackhole, grayhole, data tampering	To evaluate RCHA's detection and mitigation ability.
Reputation threshold	0.3 – 0.5	Below are which nodes that are considered malicious.
Reputation update rate	Based on α (e.g., 0.7)	Weighting factor in reputation calculation.

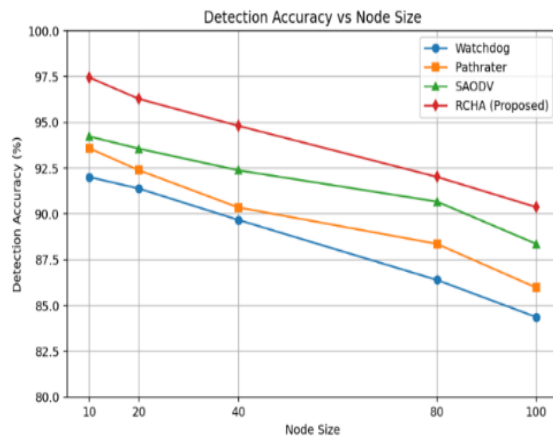


Figure 4. Detection accuracy comparison chart

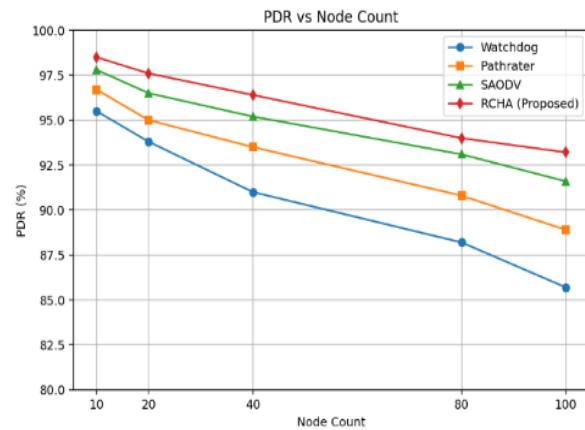


Figure 5. PDR comparison chart

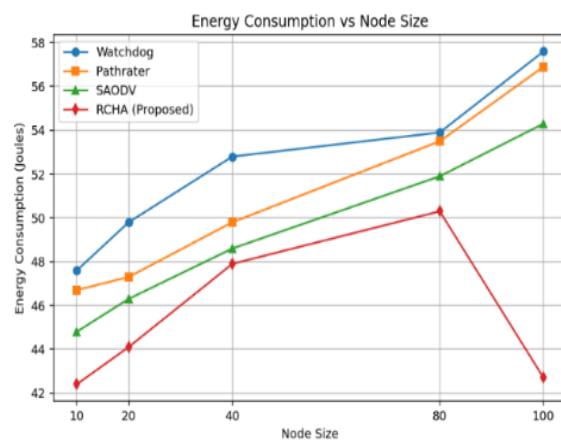


Figure 6. Energy consumption comparison chart

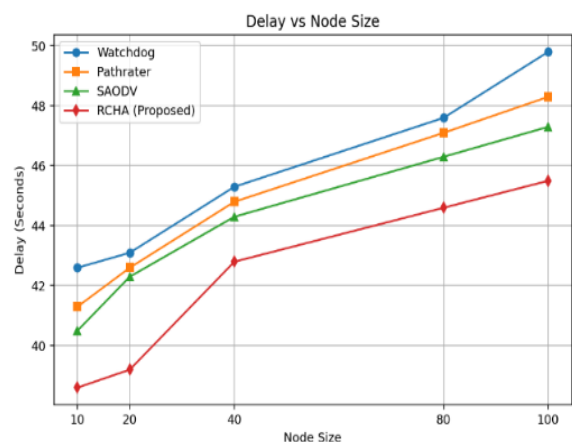


Figure 7. Delay comparison chart

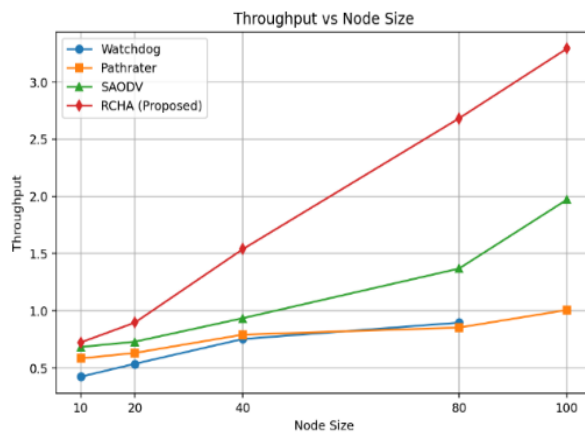


Figure 8. Throughput comparison chart

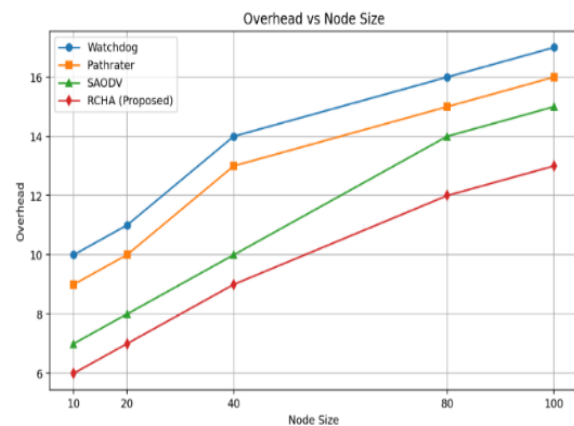


Figure 9. Overhead comparison chart

5. CONCLUSION

The RCHA provides a robust security framework for identifying and addressing attacks in WSNs. The algorithm combines two cryptographic hash functions (RIPEMD and SHA-3) with a dynamic reputation-based trust management mechanism to ensure data integrity along with a secure channel of communication. RCHA is effective at detecting malicious nodes based on abnormal packet flow and communication patterns through both layers and then adapts the routing process to remove compromised nodes dynamically. RCHA's dual-layer of security provides a high degree of internal and external attack detection, along with a relatively low delegate rate. The use of a weighted reputation model provides dynamic updates to node trust levels based on actual behavior in real time. This dynamic approach to reputation reinforces the network's resilience against evolving forms of attacks, including blackhole, grayhole, and data modification attacks. After running simulation experiments, the RCHA is a more secure and effective method than previously available methods; it also produces less computational or energy over (both of which are very important considering that nodes are energy-constrained). The mitigation options to combat the malicious node include cooperation among nodes, which adds even more reliability to the mitigation plan, increasing the chances of successful delivery of messages in hostile environments. Future work could explore how machine learning techniques could be used to predict patterns of malicious behavior accurately, and also by incorporating energy-aware trust updates in WSN with very limited resources.

FUNDING INFORMATION

This research did not receive any external funding. The publication charges were personally funded by the authors.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Divya Bharathi Selvaraj	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Veni Sundaram	✓		✓	✓			✓			✓	✓		✓	✓

C : **C**onceptualization

M : **M**ethodology

So : **S**oftware

Va : **V**alidation

Fo : **F**ormal analysis

I : **I**nterpretation

R : **R**esources

D : **D**ata Curation

O : **O**riginal Draft

E : **E**diting

Vi : **V**isualization

Su : **S**upervision

P : **P**roject administration

Fu : **F**unding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.




DATA AVAILABILITY

- Data availability does not apply to this paper as no new data were created or analyzed in this study.




REFERENCES

- [1] A. P. Abidoye and B. Kabaso, "Lightweight models for detection of denial-of-service attack in wireless sensor networks," *IET Networks*, vol. 10, no. 4, pp. 185–199, Jul. 2021, doi: 10.1049/ntw2.12011.
- [2] Z. Alansari, N. B. Anuar, A. Kamsin, and M. R. Belgaum, "A systematic review of routing attacks detection in wireless sensor networks," *PeerJ Computer Science*, vol. 8, p. e1135, Oct. 2022, doi: 10.7717/peerj-cs.1135.
- [3] N. Alikh and A. Rajabzadeh, "Using a lightweight security mechanism to detect and localize jamming attack in wireless sensor networks," *Optik*, vol. 271, p. 170099, Dec. 2022, doi: 10.1016/j.ijleo.2022.170099.
- [4] M. A. Almaiah, "A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology," in *Artificial intelligence and blockchain for future cybersecurity applications*, 2021, pp. 217–234.
- [5] E. Alotaibi, R. Bin Sulaiman, and M. Almaiah, "Assessment of cybersecurity threats and defense mechanisms in wireless sensor networks," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 47–59, Feb. 2025, doi: 10.63180/jcsra.thestap.2025.1.5.
- [6] M. Dener, C. Okur, S. Al, and A. Orman, "WSN-BFSF: a new data set for attacks detection in wireless sensor networks," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 2109–2125, Jan. 2024, doi: 10.1109/IIOT.2023.3292209.
- [7] R. K. Dhanaraj, R. H. Jhaveri, L. Krishnasamy, G. Srivastava, and P. K. R. Maddikunta, "Black-hole attack mitigation in medical sensor networks using the enhanced gravitational search algorithm," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 29, no. Supp02, pp. 297–315, Dec. 2021, doi: 10.1142/S021848852140016X.
- [8] K. Doshi, Y. Yilmaz, and S. Uludag, "Timely detection and mitigation of stealthy DDoS attacks via IoT networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 1–1, 2021, doi: 10.1109/TDSC.2021.3049942.
- [9] M. A. Elsadig, "Detection of denial-of-service attack in wireless sensor networks: a lightweight machine learning approach," *IEEE Access*, vol. 11, pp. 83537–83552, 2023, doi: 10.1109/ACCESS.2023.3303113.
- [10] G. G. Gebremariam, J. Panda, and S. Indu, "Localization and detection of multiple attacks in wireless sensor networks using artificial neural network," *Wireless Communications and Mobile Computing*, vol. 2023, pp. 1–29, Jan. 2023, doi: 10.1155/2023/2744706.
- [11] M. Hanif *et al.*, "AI-based wormhole attack detection techniques in wireless sensor networks," *Electronics*, vol. 11, no. 15, p. 2324, Jul. 2022, doi: 10.3390/electronics11152324.
- [12] M. N. U. Islam, A. Fahmin, M. S. Hossain, and M. Atiquzzaman, "Denial-of-service attacks on wireless sensor network and defense techniques," *Wireless Personal Communications*, vol. 116, no. 3, pp. 1993–2021, Feb. 2021, doi: 10.1007/s11277-020-07776-3.
- [13] S. Ismail, Z. El Mrabet, and H. Reza, "An ensemble-based machine learning approach for cyber-attacks detection in wireless sensor networks," *Applied Sciences*, vol. 13, no. 1, p. 30, Dec. 2022, doi: 10.3390/app13010030.
- [14] K. J. Nithya and K. Shyamala, "A systematic review on various attack detection methods for wireless sensor networks," in *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2021*, 2022, pp. 183–204.
- [15] A. John, I. F. Bin Isnin, S. H. H. Madni, and M. Faheem, "Cluster-based wireless sensor network framework for denial-of-service attack detection based on variable selection ensemble machine learning algorithms," *Intelligent Systems with Applications*, vol. 22, p. 200381, Jun. 2024, doi: 10.1016/j.iswa.2024.200381.
- [16] M. Keerthika and D. Shanmugapriya, "Wireless sensor networks: active and passive attacks - vulnerabilities and countermeasures," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 362–367, Nov. 2021, doi: 10.1016/j.gltp.2021.08.045.
- [17] S. Khan, M. A. Khan, and N. Alnazzawi, "Artificial neural network-based mechanism to detect security threats in wireless sensor networks," *Sensors*, vol. 24, no. 5, p. 1641, Mar. 2024, doi: 10.3390/s24051641.
- [18] P. Kumar *et al.*, "Machine learning enabled techniques for protecting wireless sensor networks by estimating attack prevalence and device deployment strategy for 5G networks," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, Jan. 2022, doi: 10.1155/2022/5713092.
- [19] T. T. Lai, T. P. Tran, J. Cho, and M. Yoo, "DoS attack detection using online learning techniques in wireless sensor networks," *Alexandria Engineering Journal*, vol. 85, pp. 307–319, Dec. 2023, doi: 10.1016/j.aej.2023.11.022.
- [20] K. Madhuri and N. Gogte, "A new level intrusion detection system for node level drop attacks in wireless sensor network," *Journal of Algebraic Statistics*, vol. 13, no. 1, pp. 159–168, 2022.
- [21] A. R. A. Moundounga and H. Satori, "Stochastic machine learning based attacks detection system in wireless sensor networks," *Journal of Network and Systems Management*, vol. 32, no. 1, p. 17, Jan. 2024, doi: 10.1007/s10922-023-09794-5.
- [22] A. Oztoprak, R. Hassanpour, A. Ozkan, and K. Oztoprak, "Security challenges, mitigation strategies, and future trends in wireless sensor networks: a review," *ACM Computing Surveys*, vol. 57, no. 4, pp. 1–29, Apr. 2025, doi: 10.1145/3706583.
- [23] M. Premkumar, S. R. Ashokkumar, V. Jeevanantham, G. Mohanbabu, and S. Anupallavi, "Scalable and energy efficient cluster based anomaly detection against denial of service attacks in wireless sensor networks," *Wireless Personal Communications*, vol. 129, no. 4, pp. 2669–2691, Apr. 2023, doi: 10.1007/s11277-023-10252-3.
- [24] S. Ramesh, C. Yaashuwanth, K. Prathibanandhi, A. R. Basha, and T. Jayasankar, "An optimized deep neural network based DoS attack detection in wireless video sensor network," *Journal of Ambient Intelligence and Humanized Computing*, Jan. 2021, doi: 10.1007/s12652-020-02763-9.
- [25] H. Sadia *et al.*, "Intrusion detection system for wireless sensor networks: a machine learning based approach," *IEEE Access*, vol. 12, pp. 52565–52582, 2024, doi: 10.1109/ACCESS.2024.3380014.
- [26] 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.
- [27] L. Sujihelen *et al.*, "Node replication attack detection in distributed wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, Jan. 2022, doi: 10.1155/2022/7252791.
- [28] K. M. Sudar and P. Deepalakshmi, "Flow-based detection and mitigation of low-rate DDOS attack in sdn environment using machine learning techniques," in *Lecture Notes in Networks and Systems*, vol. 244, 2022, pp. 193–205.
- [29] H. Wang, X. Huang, and Y. Wu, "GD3N: adaptive clustering-based detection of selective forwarding attacks in WSNs under variable harsh environments," *Information Sciences*, vol. 665, p. 120375, Apr. 2024, doi: 10.1016/j.ins.2024.120375.
- [30] Z. Zhai *et al.*, "Lightweight secure detection service for malicious attacks in WSN with timestamp-based MAC," *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 5299–5311, Dec. 2022, doi: 10.1109/TNSM.2022.3194205.

BIOGRAPHIES OF AUTHORS

Divya Bharathi Selvaraj    pursuing her Ph.D. in Computer Science at Karpagam Academy of Higher Education, India. She completed her M.Phil. in Computer Science at PSG College of Arts and Science, India. She has 5 years of teaching experience. Her areas of research interest include networking, WSNs, IoT, and network security. She has published Two paper in a Scopus-indexed international journal and three papers in reputed international and National conferences. Additionally, she has authored a book and holds a patent in the networking domain. Her publications focus on enhancing the efficiency and security of WSNs and IoT systems. She is currently working as an assistant professor at Karpagam Academy of Higher Education, India. She can be contacted at email: diya23nov@gmail.com.



Veni Sundaram    working as a professor in the Department of Computer Science in Karpagam Academy of Higher Education. She has completed her Doctoral degree from Bharathiar University. She has 19 years of experience in teaching and has published 47 research articles and has attended various national and international conferences. Her research area includes networks and data mining. She can be contacted at email: venikarthik04@gmail.com.