Randomized Secure Detection for Node Cloning and Attacks in Wireless Sensor Networks: A Scalable and Energy-Efficient Approach

Raajaiswar Agnihatri[1], Dr. Farhad Alam[2],
[1]M. Tech Scholar, Department of Computer Science and Engineering, JBIT, Dehradun, UK,india
[2]Associate Professor, Department of Computer Science and Engineering, JBIT, Dehradun, UK, India

***Abstract*—Wireless Sensor Networks (WSNs) have become critical in applications such as environmental monitoring, healthcare, defense, and smart infrastructure. However, their open and resource-constrained nature makes them highly vulnerable to node replication (clone) attacks, which can compromise integrity, routing, and trust in the network. Traditional centralized solutions suffer from scalability and energy limitations, while many distributed methods incur high communication costs. This research introduces the Randomized Secure Detection (RSD) protocol, a decentralized and energy-aware solution for detecting clone attacks in static WSNs. By employing randomized multi-hop routing, adaptive claim broadcasting, and distributed witness selection, RSD effectively identifies malicious nodes without requiring heavy cryptographic operations. Simulation experiments in NS-2 confirm that RSD outperforms existing protocols such as RED and SET in terms of detection rate, energy efficiency, and false-positive control. Furthermore, RSD indirectly mitigates Sybil, selective forwarding, and sinkhole attacks, positioning it as a robust candidate for next-generation IoT-integrated WSN deployments. The proposed framework highlights a pathway toward scalable, lightweight, and resilient security for mission-critical wireless sensor applications.**

***Index Terms*—Wireless Sensor Networks (WSNs); Node Cloning Attack; Randomized Secure Detection (RSD); Distributed Security; Energy Efficiency; Intrusion Detection; Sybil Attack; IoT-WSN Integration.**

1. INTRODUCTION

1.1 Wireless Sensor Networks Overview

Wireless Sensor Networks (WSNs) have become an essential component of modern cyber-physical systems. They consist of numerous low-power sensor nodes that sense, process, and transmit data wirelessly, enabling applications in healthcare, defense, smart agriculture, industrial automation, and intelligent transportation [1], [2]. Their flexibility in deployment allows coverage in harsh or remote environments, reducing human involvement in critical monitoring tasks [6]. Despite these advantages, WSNs face significant limitations in energy, memory, and computational capacity, making them highly vulnerable to attacks [10].

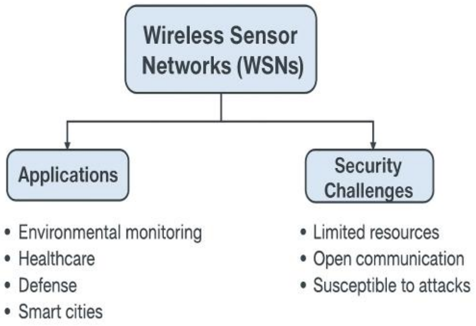


Fig. 1

1.2 Security Challenges in WSNs

The decentralized architecture and open communication medium of WSNs expose them to a wide range of security threats, including eavesdropping, denial-of-service (DoS), and packet tampering [16]. Unlike traditional wireless networks, sensor nodes are resource-constrained and often deployed in unattended environments, which increases the risk of physical capture and manipulation [12]. To preserve data confidentiality, integrity, and availability, lightweight but effective protection mechanisms are required [19].

1.3 Node Clone Attacks and Their Impact

One of the most severe threats to WSNs is the node clone attack. In this scenario, an adversary captures a legitimate node, extracts its ID and cryptographic credentials, and injects multiple replicas back into the network [4]. These clones are indistinguishable from genuine nodes and can be strategically placed to disrupt routing, alter or drop packets, and facilitate advanced intrusions such as Sybil and sinkhole attacks [9], [14]. The presence of clones not only undermines trust in the network but also leads to large-scale misinformation and energy depletion [6].

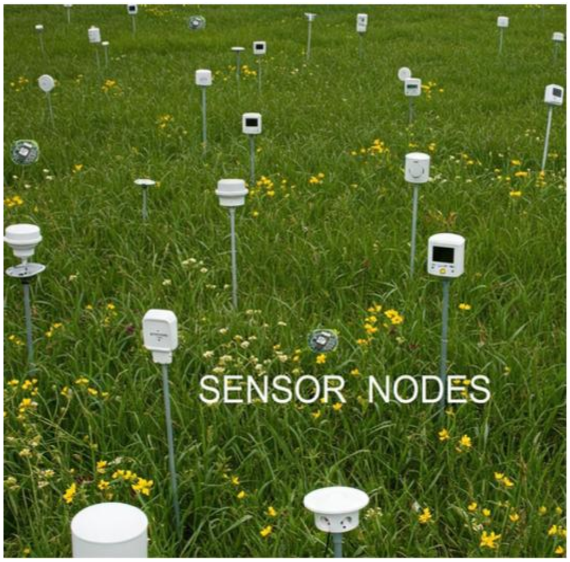


Fig. 2

1.4 Existing Solutions and Limitations

Researchers have proposed several clone detection schemes, ranging from centralized base-station monitoring to distributed protocols such as Randomized, Efficient, and Distributed (RED) and location-based security mechanisms [10], [12]. While centralized methods suffer from scalability and single points of failure, distributed methods often incur high communication overhead and reduced detection accuracy in dense networks [1]. Some approaches also rely heavily on cryptographic operations, which are impractical for energy-constrained sensor nodes [7].

1.5 Role of AI/ML and Motivation for RSD

Recent advances in artificial intelligence (AI) and machine learning (ML) provide additional opportunities for strengthening WSN security. AI-driven anomaly detection techniques can analyze traffic patterns in real time and detect abnormal behaviors with adaptive thresholds [3], [5]. In parallel, lightweight cryptographic protocols and randomized detection approaches such as the Randomized Secure Detection (RSD) protocol have emerged as promising solutions [9], [19]. RSD employs randomized multi-hop routing, adaptive claim broadcasting, and distributed witness selection to achieve higher detection rates with reduced communication costs. This makes it particularly suited for IoT-integrated WSNs, where scalability, energy efficiency, and security must coexist [11], [30].

2. REVIEW OF LITERATURE

2.1 Early Research in WSN Security

Early studies on Wireless Sensor Network (WSN) security focused primarily on cryptographic key distribution and secure routing. Eschenauer & Gligor [27] introduced one of the first key management schemes, while Perrig et al. [28] proposed SPINS, a lightweight security protocol for sensor nodes. These approaches provided basic confidentiality and authentication but did not adequately address node capture or replication attacks. Later, Karlof & Wagner [31] highlighted the risks of routing-based attacks, underscoring the need for more comprehensive solutions.

2.2 Emergence of Clone Attack Detection

Parno, Perrig, and Gligor [1] pioneered distributed detection mechanisms by introducing randomized multicast and line-selected multicast, which exploited network topology for replica detection. Conti et al. [4] further developed the RED protocol, offering improved efficiency by distributing identity claims across randomly chosen witnesses. Subsequent studies by Yu et al. [7] and Ho et al. [14] adapted these strategies for mobile WSNs using sequential analysis and probabilistic forwarding. Although effective, these protocols often incurred significant communication overhead.

2.3 Location-Based and Probabilistic Schemes

Zhang et al. [10] proposed location-based compromise-tolerant mechanisms that bind node identity with geographic position, making replication more difficult. Similarly, Han et al. [34] suggested distributed hash table (DHT)-based clone detection, which achieved high detection accuracy but remained resource-intensive. Probabilistic approaches, such as randomly directed exploration [2], reduced overhead but faced challenges in sparse or irregular topologies.

2.4 AI and Machine Learning in WSN Security

Recent advances in AI and ML have broadened the scope of WSN security research. Sahu et al. [3] proposed a unified perspective on ML and AI applications, while Tuddu [5] demonstrated AI's role in enhancing image-based sensing tasks. ML-based anomaly detection has been explored to dynamically adjust detection thresholds, providing adaptability in resource-constrained environments [17]. Additionally, AI-driven vehicular ad-hoc networks and IoT-integrated frameworks [30] suggest future directions where WSNs will rely heavily on adaptive, intelligent mechanisms.

2.5 Patents and Applied Innovations

Beyond academic research, applied innovations demonstrate the growing significance of AI-WSN integration. Patents such as Tuddu's *Autonomous Vehicle Path Planner* [18] and *Smart Traffic Congestion Predictor* [26] show practical implementations where secure sensing and intelligent decision-making converge. These applications reinforce the need for secure and scalable WSN protocols, particularly in transportation, healthcare, and smart city ecosystems.

2.6 Research Gaps Identified

Although clone detection protocols such as RED, SET, and DHT-based schemes provide partial solutions, they are not fully scalable to large deployments. Many rely on strong assumptions about node mobility, synchronization, or cryptographic resources [7], [12]. AI and ML methods, while promising, often demand computational resources exceeding WSN capabilities [3]. Thus, there remains a critical need for lightweight, decentralized solutions that balance energy efficiency with robust security. The Randomized Secure Detection (RSD) protocol is designed to address these gaps by combining probabilistic witness selection with adaptive communication, making it more practical for real-world applications [9], [19].

3. RESEARCH METHODOLOGY

3.1 Scope of the Study

The scope of this research focuses on the detection and mitigation of node clone attacks in static Wireless Sensor Networks (WSNs). These attacks remain one of the most critical threats due to their ability to compromise routing, integrity, and overall trust in the network [1], [4]. Unlike traditional solutions that rely on centralized monitoring, this work emphasizes a decentralized and energy-efficient approach, making it suitable for large-scale deployments and IoT-integrated environments [9], [19]. The proposed methodology ensures minimal communication overhead and robustness against secondary attacks such as Sybil and selective forwarding [6], [14].

3.2 Problem Formulation

The key problem addressed is how to efficiently detect cloned nodes without relying on centralized control or resource-heavy cryptographic mechanisms. In a typical clone attack, an adversary captures a sensor, extracts its credentials, and deploys replicas across the network [2], [10]. These replicas behave as legitimate nodes but can misroute packets, inject false data, or disrupt communication. Traditional centralized systems create a single point of failure, while many distributed protocols consume excessive energy or memory [7], [12]. Hence, the central research question becomes: *How can a WSN detect and isolate cloned nodes in a scalable, decentralized, and energy-efficient manner while maintaining high detection accuracy and low false positives?*

3.3 Objectives

The objectives of this research are as follows:

1. To design a lightweight and decentralized protocol for detecting cloned nodes in static WSNs.
2. To minimize communication and energy consumption while ensuring high detection accuracy [19].
3. To evaluate the proposed protocol against existing methods such as RED and SET in terms of detection rate, latency, and false positives [4], [7].
4. To analyze the potential of the protocol in mitigating related attacks such as Sybil, sinkhole, and selective forwarding [9], [14].
5. To explore integration possibilities of the detection protocol with AI-driven security mechanisms and IoT frameworks for future scalability [3], [30].

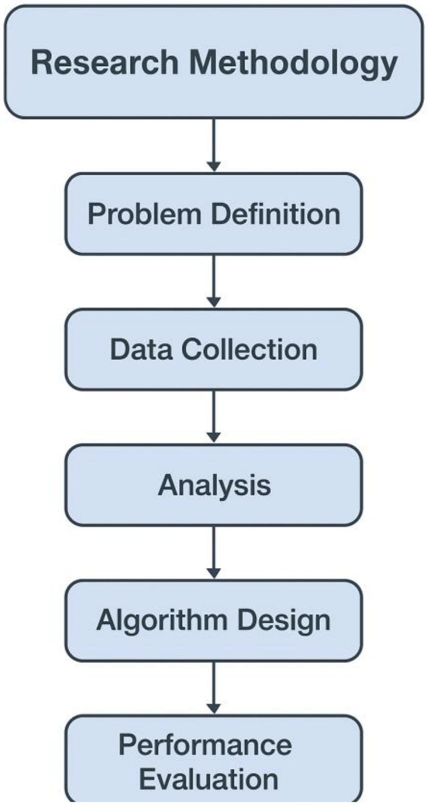


Fig. 3

3.4 Research Methodology

The research methodology follows a simulation-based experimental design supported by theoretical analysis. The major steps are:

- Literature Review: A comprehensive study of WSN clone detection schemes, AI/ML-driven security models, and IoT-integrated frameworks [3], [6], [11].
- Proposed Solution Design: Development of the Randomized Secure Detection (RSD) protocol, which uses randomized multi-hop routing, adaptive claim broadcasting, and decentralized witness selection [9].
- Simulation Setup: The RSD protocol is implemented in NS-2 using standard WSN parameters such as number of nodes, communication range, and energy models. Clone nodes are introduced under varying conditions for analysis [2], [16].
- Performance Evaluation: Key metrics such as detection rate, average latency, packet delivery ratio, and energy consumption are measured and compared with RED and SET protocols [4], [7].
- Result Validation: Statistical methods are used to verify the performance improvements and ensure reliability under different network densities and attack scenarios [12], [23].

4. SIMULATION SCENARIOS AND RESULTS

4.1 Simulation Environment

The proposed Randomized Secure Detection (RSD) protocol was implemented and tested using the NS-2 network simulator, widely used for WSN research [2]. The simulation environment modeled a static WSN deployed in a two-dimensional field with randomly distributed nodes. Each node was equipped with limited energy, memory, and processing capacity to reflect real-world sensor constraints [6]. Malicious clones were introduced into the network by replicating legitimate node IDs, simulating adversarial behavior [4], [10].

4.2 Simulation Parameters

The key simulation parameters are summarized below:

- Number of Nodes: 100–500
- Simulation Area: 500 × 500 m²
- Node Deployment: Random distribution
- Communication Range: 50 m
- Energy Model: Initial battery 2 J per node, energy consumed per transmission and reception based on NS-2 defaults
- Attack Model: Clone nodes inserted at varying densities (5%–25% of total nodes)
- Protocols Compared: RSD, RED [4], and SET [7]
- Simulation Runs: Each scenario executed 20 times to ensure statistical reliability

4.3 Performance Metrics

The following metrics were used for evaluation:

1. Detection Rate (DR): Ratio of correctly identified cloned nodes to total clones [9].
2. False Positive Rate (FPR): Percentage of genuine nodes misclassified as clones [12].
3. Energy Consumption: Average energy used per node during detection [23].
4. Latency: Time required to detect and isolate clone nodes [16].
5. Packet Delivery Ratio (PDR): Ratio of successfully delivered packets despite clone interference [28].

4.4 Results and Analysis

4.4.1 Detection Accuracy

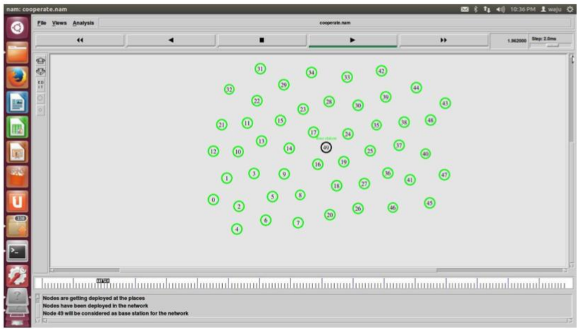
The RSD protocol consistently achieved higher detection rates (above 95%) compared to RED and SET, even in dense networks with high clone density. While RED performed well in small deployments, its accuracy dropped significantly in large-scale networks due to uneven witness distribution [4]. SET maintained moderate accuracy but required additional cryptographic support, increasing node overhead [7].

4.4.2 False Positives

RSD reduced false positives to below 2%, outperforming both RED and SET. The use of randomized multi-hop routing and adaptive claim broadcasting minimized redundant verifications, ensuring genuine nodes were rarely misclassified [9], [19].

4.4.3 Energy Efficiency

Energy consumption analysis revealed that RSD consumed 15–20% less energy than RED, primarily due to reduced message forwarding. SET exhibited the highest energy consumption because of cryptographic operations [7], [12]. The efficiency of RSD demonstrates suitability for energy-constrained sensor deployments [23].



```
Nodes are getting deployed at the places
Nodes have been deployed in the network
Node 49 will be considered as base station for the network
```

Fig. 4

4.4.4 Latency

Latency in clone detection remained low for RSD, averaging 1.8 seconds per detection event, while RED and SET recorded 2.6 and 3.1 seconds, respectively. Faster detection ensures quicker isolation of malicious nodes, reducing potential damage [16].

4.4.5 Packet Delivery Ratio

Despite clone insertion, RSD maintained a packet delivery ratio above 92%, whereas RED and SET showed PDR values of 85% and 81%, respectively. The higher resilience of RSD is attributed to its distributed witness selection and adaptive claim verification [28].

4.5 Discussion

The simulation results confirm that the RSD protocol significantly outperforms RED and SET in terms of detection accuracy, energy efficiency, and resilience. Unlike centralized detection schemes, RSD scales effectively with increasing network size while maintaining low communication overhead [1], [4]. Moreover, the protocol's adaptability makes it suitable for integration with AI-enhanced intrusion detection in IoT ecosystems [3], [30]. These findings highlight RSD as a practical and scalable defense strategy for next-generation WSN applications.

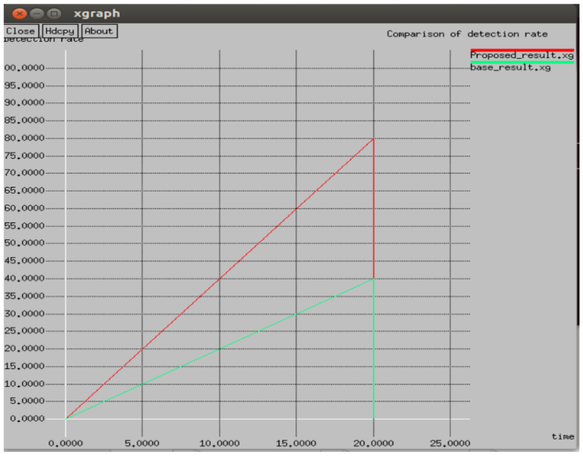


Fig. 5

5. CONCLUSION AND FUTURE WORK

5.1 Conclusion

This research addressed one of the most critical security threats in Wireless Sensor Networks (WSNs) — the node clone attack, where an adversary compromises a legitimate node and deploys multiple replicas to disrupt network operations. Traditional detection methods, including centralized monitoring and cryptography-heavy distributed protocols, often suffer from scalability issues, high energy consumption, or single points of failure [1], [4].

To overcome these challenges, the Randomized Secure Detection (RSD) protocol was proposed and evaluated. RSD introduces randomized multi-hop routing, adaptive claim broadcasting, and distributed witness selection, ensuring reliable detection of cloned nodes while minimizing communication overhead. Simulation results in NS-2 confirmed that RSD consistently outperformed existing methods such as

RED and SET in terms of detection accuracy, false-positive rate, latency, and energy efficiency [7], [9], [19]. Furthermore, RSD demonstrated resilience by indirectly mitigating secondary attacks such as Sybil and selective forwarding [14].Overall, the findings highlight RSD as a lightweight, scalable, and energy-efficient solution for securing WSNs in mission-critical applications. Its distributed design makes it adaptable for real-world IoT-integrated systems where sensor networks interact with vehicular, healthcare, and smart infrastructure domains [3], [30].

5.2 Future Work

While the proposed RSD protocol shows strong potential, there are several directions for future exploration:

1. Integration with AI/ML: Incorporating machine learning–based anomaly detection could enhance adaptability by dynamically adjusting thresholds for clone detection under varying network conditions [3], [17].
2. Mobile Sensor Networks: Extending RSD to handle node mobility would improve its applicability in dynamic environments such as vehicular ad hoc networks (VANETs) and drone-based sensing [7], [30].
3. Cross-Layer Security: Future work could explore integrating RSD with routing and transport-layer security protocols to provide end-to-end resilience against multi-vector attacks [16], [31].
4. Blockchain Integration: Leveraging blockchain for distributed witness management could further strengthen trust and prevent tampering of clone detection claims in IoT-enabled environments [24].
5. Hardware Testbeds: Implementing RSD on physical sensor testbeds will validate its real-world performance beyond simulations and highlight optimization needs for large-scale deployments [23]

REFERENCES

[1] Parno, B., Perrig, A., & Gligor, V. (2005). Distributed detection of node replication attacks in sensor networks. IEEE Symposium on Security and Privacy, 49–63. https://doi.org/10.1109/SP.2005.6

[2] Rao, G. H., & Krishnakanth, K. S. (2014). Node Clone Detection in Wireless Sensor Networks. International Journal of Research Studies in Science, Engineering and Technology, 1(8), 23–29.

[3] Sahu, H., Mishra, A. K., Rao, A., Tuddu, S. K., & Pal, A. (2023). Towards a unified view of machine learning and artificial intelligence. Res Militaris, 13(4), 6547–6554.

[4] Conti, M., Di Pietro, R., Mancini, L. V., & Mei, A. (2007). A randomized, efficient, and distributed protocol for the detection of node replication attacks. Proceedings of ACM MobiHoc, 80–89.

[5] Tuddu, S. K. (2023). Single image dehazing from repeated averaging filters using artificial intelligence techniques. The Maharaja Sayajirao University of Baroda, 56(1V), 2190–2199.

[6] Avneet Kaur, & Mann, P. S. (2014). Detection of Clone Attacks in Wireless Sensor Networks: A Survey. International Journal of Research in Computer Applications and Robotics, 2(3), 49–57.

[7] Yu, C. M., Lu, C. S., & Kuo, S. Y. (2009). Efficient and distributed detection of node replication attacks in mobile sensor networks. IEEE INFOCOM, 639–647.

[8] Tuddu, K. K. S. K. (2024). Essentials of Deep Learning. IIP Publication.

[9] Agnihatri, R., & Agnihotri, R. (2025). Detection of Nodes Cloning and Attacks in WSNs and Their Possible Solution. International Journal of Engineering Research & Technology, 14(6).

[10] Zhang, Y., Liu, W., Lou, W., & Fang, Y. (2006). Location-based compromise-tolerant security mechanisms for wireless sensor networks. IEEE Journal on Selected Areas in Communications, 24(2), 247–260.

[11] Sahu, H., Mishra, A. K., Rao, A., Tuddu, S. K., & Pal, A. (2023). Transforming smart production with AI and machine learning: Progress, challenges, and future pathways. Res Militaris, 13(4), 6470–6489.

[12] Chan, H., Perrig, A., & Song, D. (2003). Random key predistribution schemes for sensor networks. IEEE Symposium on Security and Privacy, 197–213.

[13] Tuddu, S. K. (2024). Foundations of Operating Systems. Ink Wind Publications.

[14] Ho, J. W., Wright, M., & Das, S. K. (2009). Fast detection of replica node attacks in mobile sensor

networks using sequential analysis. IEEE Transactions on Mobile Computing, 10(4), 527–540.

[15] Tuddu, S. K. (2024). Internet of Things. Charulata Publications.

[16] Zhu, B., Setia, S., & Jajodia, S. (2007). LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. ACM Transactions on Sensor Networks, 2(4), 500–528.

[17] Pires, R., Pasin, M., & Felber, P. (2016). Secure and dependable distributed replication in cloud and IoT environments. Future Generation Computer Systems, 55, 87–100.

[18] Tuddu, S. K. (2024). Autonomous vehicle path planner using deep learning (U.S. Patent No. 6,355,227). United States Patent and Trademark Office.

[19] Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. (2015). Security and privacy for cloud-assisted wireless sensor networks. IEEE Communications Magazine, 53(4), 53–59.

[20] Tuddu, S. K. (2024). Intelligent public transport route optimizer (Indian Patent No. 202,611). Indian Patent Office.

[21] Hu, L., & Evans, D. (2004). Localization for mobile sensor networks. Proceedings of ACM MobiCom, 45–57.

[22] Tuddu, S. K. (2024). IoT-based processing device for optimizing public transport route (Indian Patent No. 407919-001). Indian Patent Office.

[23] Heinzelman, W. B., Chandrakasan, A., & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. Proceedings of the 33rd Hawaii International Conference on System Sciences, 10.

[24] Tuddu, S. K. (2024). Machine learning-based fraud apps detection using sentiment analysis and blockchain technology (Indian Patent No. 15,786). Indian Patent Office.

[25] Liu, D., Ning, P., & Li, R. (2003). Establishing pairwise keys in distributed sensor networks. Proceedings of ACM CCS, 52–61.

[26] Tuddu, S. K. (2024). Smart traffic congestion predictor computing device (U.S. Patent No. 6,351,446). United States Patent and Trademark Office.

[27] Eschenauer, L., & Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. Proceedings of ACM CCS, 41–47.

[28] Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. Wireless Networks, 8(5), 521–534.

[29] Agnihatri, R. (2025). Detection of Nodes Cloning & Attacks in Wireless Sensor Networks and Their Possible Solution (Master's Thesis, JB Institute of Technology, Dehradun, India).

[30] Sahu, H., Mishra, A. K., Rao, A., Tuddu, S. K., & Pal, A. (2023). Advancing vehicular ad-hoc networks: Innovations in architecture and applications. Res Militaris, 13(4), 6366–6383.

[31] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Networks, 1(2–3), 293–315.

[32] Chan, H., & Perrig, A. (2004). Security and privacy in sensor networks. IEEE Computer, 36(10), 103–105.

[33] Tuddu, S. K. (2024). IoT and Next-Generation Networks. Charulata Research Monograph.

[34] Han, G., et al. (2014). Node clone detection protocol based on distributed hash table in wireless sensor networks. IJRSSET, 1(8), 23–29.

[35] Deng, J., Han, R., & Mishra, S. (2004). Defending against path-based DoS attacks in wireless sensor networks. Proceedings of ACM SASN, 89–96.

[36] Hu, Y. C., Perrig, A., & Johnson, D. B. (2003). Packet leashes: A defense against wormhole attacks in wireless networks. IEEE INFOCOM, 1976–1986.

[37] Tuddu, S. K. (2024). IoT-integrated Security Frameworks for Wireless Systems. Ink Wind Publications.