iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: IV Month of publication: April 2025

DOI: https://doi.org/10.22214/ijraset.2025.69932

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Secure and Selective Geographic Opportunistic RoutingAgainst DoS Attacks

M.V.H.Bhaskara Murthy[1], Doki Harikrishna[2], Majji Prasanth Reddy[3], Battala Purna Chandra[4], Nabelli Bhargavi[5]
Aditya Institute of Technology and Management, JNTUGV

Abstract: WSNs serve as fundamental components for IoT applications to develop smart homes systems alongside traffic monitoring and control of smart grids and environment surveillance capabilities. Security and reliability of data delivery represents a primary requirement in these networks. Network security becomes achievable through the introduction of Secure and Selective Geographic Opportunistic Routing (SelGOR) protocol. The SelGOR security approach utilizes authentication selection with geographic opportunistic routing to create an attack defense against Denial-of-Service (DoS) incidents. The protocol develops a trust model from Statistical State Information (SSI) systems to maximize operational data productivity. SelGOR protects data integrity with automatic intruder detection through an encryption mechanism based on entropy which enables both strong authenticity and low calculations cost. By implementing a distributed verification system one can detect attackers more rapidly and simultaneously prevent duplicate data by using smart routing decision-making.The routing system of SelGOR adds trust capabilities to Mobile Ad Hoc Networks (MANETs) through its trust-based mechanism. The protocol uses node reputation and monitoring results to make route decisions so it chooses routes from trusted sources. Through its combination of geographic opportunistic routing with entropy-driven encryption and statistical trust models and cooperative attacker verification SelGOR delivers complete protection to WSNs against attacks and simultaneous enhancement of energy efficiency along with throughput and end-to-end performance. The system functions well for secure huge-scale IoT smart infrastructure applications through its detection methods.

Keywords: Authentication, DoS, Opportunistic Routing, Tool Command Language (TCL)

I. INTRODUCTION

WSNs in IoT operations face DoS attack vulnerability because they have restricted capabilities and open accessibility. Approximately one-third of node authentication in Geographic Opportunistic Routing (GOR) helps maintain secure communication without adding excess overhead to the network. The approach enhances marketplace safety and maintains optimal data transfer operations in IoT-based WSNs.[1], [2], [3]. IOT enhances Wireless Sensor Network (WSN) data collection ability while making both networks more susceptible to Denial of Service attacks. Selective Authentication implemented with Geographic Opportunistic Routing (GOR) creates a secure environment for IoT-enabled WSNs by reducing overhead while simultaneously maintaining resilient and efficient communication.[4, 5] This security approach works well in all IoT-driven WSN domains. The solution provides secure data communications that support credible transmission operations throughout smart cities, healthcare, precision agriculture, industrial IoT and military together with disaster response systems.[6], [7], [8] The proposed method protects WSN security in IoT systems through DoS attack reduction alongside resource and energy conservation. The combination of Selective Authentication with GOR produces stronger networks that have less operational overhead next to enhancing resistance and maintaining dependable data exchange in evolving IoT frameworks.[6, 9, 10]. The research conducted by Swami et al.[11] developed an intrusion detection system hybrid that implements rule-based filtering alongside DT and SVM machine learning classifiers for detecting WSN DoS attacks. The system begins by identifying regular traffic and abnormal patterns with rules before it applies ML models to detect particular DoS attacks. The DT classifier improved accuracy rates along with greater speed than standard ML methods while being implemented by their approach. The hybrid security solution merges rule-system speed performance with ML accuracy to present a practical method for improving WSN protection effectiveness.Mohamed et al.,[13] conducted a detailed study on techniques for improving and maintaining coverage in Mobile Wireless Sensor Networks (M-WSNs), focusing on coverage enhancement and node failure recovery. They presented mathematical formulations for various coverage types and reviewed approaches from the literature. The study categorized algorithms and techniques used for optimizing coverage in M-WSNs. By analysing these approaches, they identified their strengths and limitations, emphasizing strategies to ensure effective coverage and connectivity in dynamic and failure-prone scenarios.

They concluded that maintaining and enhancing coverage in M-WSNs requires context-specific algorithms that balance mobility, coverage, and connectivity while adapting to environmental and network changes.
Sathishkumar et al.,[5]developed an intrusion detection system for wireless sensor networks (WSNs) with deep learning (LSTM) and fuzzy logic features supported by Crow Search Algorithm feature selection optimization. The Fuzzy LSTM approach of their research showed better detection performance across DoS attacks in WSNs by achieving higher accuracy levels with excellent precision and recall measures and F1-score values. The reliable and efficient security system provides robust protection to vital infrastructure and IoT applications thus establishing itself as a vital security tool for WSNs. Researchers have developed Geographic Opportunistic Routing (GOR) as a protocol to assess its benefits for strengthening wireless networks while improving their performance. The proposed approach demonstrates a dual effect of extending network lifetime while delivering dependable data transmission regardless of environmental dynamic or unpredictable conditions by focusing on energy optimization. This system reduces both transmission costs and response delays to enhance the selection of candidates as well as forwarding processes thus improving decision-making efficiency. The established research fills in critical gaps in routing to enable scalable and connected operations for large-scale wireless network implementations. The research resolves such problems to support the development of dependable and adaptive routing systems applicable for contemporary wireless networks.

II. LITERATURE SURVEY

F. Lagrange and F. Jacq.[7] developed the APG/RMD818 High-Speed Liquid Unit Dose Packaging Machine, integrating advanced pharmaceutical automation engineering and process control to streamline liquid dose preparation, significantly enhancing efficiency and production capacity in hospital pharmacies, and concluding it as an innovative, user-friendly solution with clear advantages over solid dose systems. Riti Achammal.Set al.[8] developed an affordable and reliable automatic drug dispenser using Raspberry Pi and facial recognition, effectively delivering medication, verifying identity, and providing low-stock alerts, ultimately reducing caregiver dependency and improving medication adherence for the elderly. Shanthini E et al.[9]. developed an automated drug dispenser using QR code technology to enhance medication management, integrating prescription encoding, secure payment gateways, and a helical spring drawer mechanism for dispensing. Adopting a technology-driven approach, they ensured accuracy, transparency, and efficiency, resulting in improved dispensing accuracy, reduced waiting times, and enhanced patient convenience. They concluded that the dispenser revolutionizes healthcare delivery, aligning with modern advancements in healthcare technology.
Rekhitha Sree Ankireddypalli and Kandi Sriya Sushrutha Reddy [10] developed an IoT-based smart drug administration system using real-time monitoring, authentication, and intelligent alerts to improve prescription management and reduce drug addiction. They concluded that the system enhances medication adherence, detects abuse early, and promotes responsible prescription practices, ultimately improving patient outcomes. Riitta TurjamaaRN's[11] systematic review found that smart medication systems improve medication adherence and safety, particularly for older adults, offering valuable insights for developing effective solutions to enhance healthcare outcomes. M. Shanthini et al. [12] designed an automatic medicine dispenser that improves adherence, reduces errors, and enhances patient safety through programmable scheduling, reminders, and tracking.

III. METHODOLOGY

WSNs represent infrastructure-less self-configuring wireless networks that measure environmental or physical criteria such as temperature and sound and humidity while furnishing collected data to a base station (sink) through cooperation so the data becomes available for further analysis. The deployment locations of WSN consist mainly of unfriendly and unsafe environments. WSNs face numerous limitations that create advanced problems for their deployment. Security mechanisms become hard to implement because sensor nodes face poorly reliable networks along with scarce resources. Previous protocols of WSN operation typically made trust and cooperation assumptions regarding all devices. Several attacks are possible in WSN despite the untrue assumption that exists in modern sensor network applications.

1) *Protocol Initialization:* DSR implements dynamic source routing as a reactive protocol which reduces control packet bandwidth usage through the elimination of table-driven proactive approach update packets. The protocol chooses source routing because it does not depend on routing tables which exist at intermediate nodes. The beaconless operation of DSR eliminates the need for periodic hello packets therefore it operates without beacons.
2) *Node Stability:* A group of forwarding nodes requires stable members for better delivery of packets. The movement of nodes near their current position allows us to determine node stationary characteristics. The identification of stable forwarding nodes for packet transmission between source nodes and Anycast nodes makes use of Node stability metrics.

The quality of connectivity in mobile networks depends on two stability measurements that include self stability and neighbor nodes stability.Residualenergy-basedneighbor nodeselection.

3) *Request Phase:*A source node discovers the path to its multiple targets by transmitting RQ packets. The route request phase starts with following sequence operations. The source node creates a RQ packet which contains both node density and residual energy information as a part of phase (1). Phase (2) involves RQ packet transmission toward adjacent neighbors that fulfill power level and node density requirements. Phase (3) receives intermediate nodes discard RQ packets which they have received before using the sequence number contained in the RQ message. The procedure starts by generating an RP packet when RQ packet passes the duplicate check along with reviewing the Routing Information table for route existence to begin reply forwarding toward the source. The transmission of RQ packets must stop when a duplicate packet is detected in phase (5). The updating procedure for RQ packet transmission continues according to step 2 when the packet is not a duplicate and no routes exist in Routing Information table. The procedure of reaching the destination consists of repeating steps 3 to 6 until success while phase 8 executes RQ packet transmission as a failure response to the source node in cases where the receiver remains unreachable beyond specific hop count limitations.

During the Reply Phase all Multicast destinations take the lead to start their replies. Several operations play a key role at the destination node upon receiving an RQ packet during the reply phase. During the first phase of RP packet generation from RQ packet multiple operations are applied including swapping source and destination addresses along with reversals of the route record followed by an update of visited history records that store power level as residual energy and node density values. The destination node should receive updated route data including destination IP, path information and Power level, node density and time information during Phase (2). The forwarding process of RP packets begins with phase (3) where it proceeds to the next hop node based on route information contained in the route record if both power levels and node density values match the requirements. The receiving source checks power level availability above the threshold value combined with node density under threshold in order to update its routing table by using the packet contents.

WSN networks utilize a power-based neighbor selection strategy for finding reliable multicast routes through the network. The network defines neighbor nodes as any pair of nodes that their signal transmission ranges intersect. The two components of neighbor node selection are covered in this section which starts with node energy model definition to determine node degree and then proceeds into removing high energy-consuming nodes. Energy model of a node Dimensions of operation exist for WSN nodes between four functional states. (1) Transmission mode, (2) Receiving mode, (3) Idle or standby mode, and Sleep mode. A node requires little energy while it remains in sleep state in comparison to the energy needed during transmission. Scientific research demonstrates that rest mode energy usage of a single node is 1 while both receiving mode and transmission mode energy consumption is at 1.2 and 1.8 times higher respectively. The following energy model was established through literature review and assumptions that enables residual energy calculation of a single node.

The Node pruning process adopts differential dominant set theory All nodes that plan to transmit data to specific network locations start identifying neighbors by flooding HELLO packets containing their tables periodically to collect data about all neighbors including power calculations and density statistics. Nodes should remove those neighboring nodes from their consideration if their remaining energy level falls below the defined threshold value. The proposed network requires stable multicast routes consisting of dense nodes and excluding those neighbors below the threshold energy value. Balanced Multipath Routing & Scheduling Neighbor node selection constructs stable multicast routes by using residual energy and density as the basis for choosing next nodes. The following section presents details about RQ and RP packet structure as well as request-reply phase sequence and establishment of route processes along with maintenance procedures.

SSAGOR (Secure and Selective Authentication Geographic Opportunistic Routing) The secure authentication system SSAGOR provides both safety measures and chooses which nodes can participate in geographic opportunistic routes. This protocol allows admission of authorized nodes within the network system. Before accessing the network nodes need to undergo an identity verification process for authentication purposes.

SELGOR (Selective Authentication Geographic Opportunistic Routing) SELGOR functions as a sub-section of SSAGOR to perform selective authentication procedures for geographic opportunistic routing networks. Authentication procedures deployed by the system provide enhanced network security together with fast data transmission capabilities.

Decision Process (IF-YES Condition) The decision node checks that all authentication standards are passed. The security needs assessment sets the node course for multiple additional network-based operations that include inserting nodes and route discovery and path visualization. The failure of authentication will prevent the node from entering the network.

Opportunistic Routing Run The process selects routing decisions from the most appropriate node according to geographical location. The system employs automatic selection of relay nodes that results in more reliable and efficient data transmission. Cooperative Verification Run Many nodes unite through a collaborative process to examine the validity of new network members during this phase. Security increases through this collaborative system because it blocks unauthorized nodes from entering the network.
Add Node The network accepts newly authenticated nodes after their integration and admission process has finished successfully. Authenticated network nodes form the only acceptable members for system access because this approach protects network integrity while blocking unauthorized access.

- *Route Discovery*

A method used to find optimal data transmission paths exists. The routing algorithm uses multiple pathways to find optimal connections between a source point and its destination with both low response times and energy efficiency.

- *View Node & View Path*

The authenticated nodes display with their routing path connections visible. Ease of network troubleshooting and monitoring occurs because the feature provides insights into node connectivity and improves route optimization.

- *Show Network*

The complete network architecture displays both the interconnected behavioral pattern and authentication process of all networked nodes. The shown network enables analysis of both network parameters and system performance on an overview level.

- *Show Node*

The function provides an extensive overview of a specific node by revealing status information together with location data and authorization details. Monitoring the activities of individual nodes becomes possible through this feature.

- *Show Route Path*

The display of data packet routing routes enables network administrators to check data transmission speed while locating potential performance problems.

- *Admission of New Nodes*

The network provides supervised access for permitting new nodes to join its system. Verified nodes must gain explicit access to join the network because this requirement ensures secure communications as well as blocking unauthorized users from the system.

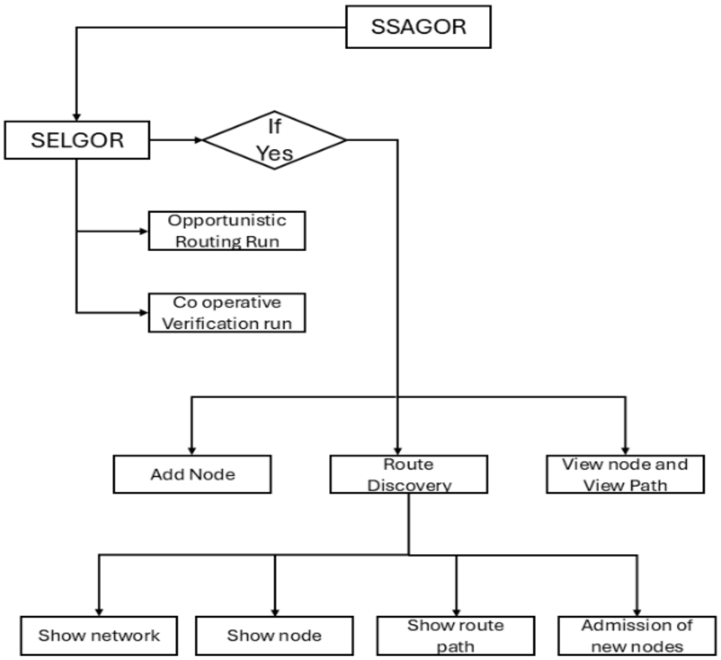

Fig.1 Flowchart

- *Route Discovery*

A method used to find optimal data transmission paths exists. The routing algorithm uses multiple pathways to find optimal connections between a source point and its destination with both low response times and energy efficiency.

- *View Node & View Path*

The authenticated nodes display with their routing path connections visible. Ease of network troubleshooting and monitoring occurs because the feature provides insights into node connectivity and improves route optimization.

- *Show Network*

The complete network architecture displays both the interconnected behavioral pattern and authentication process of all networked nodes. The shown network enables analysis of both network parameters and system performance on an overview level.

- *Show Node*

The function provides an extensive overview of a specific node by revealing status information together with location data and authorization details. Monitoring the activities of individual nodes becomes possible through this feature.

- *Show Route Path*

The display of data packet routing routes enables network administrators to check data transmission speed while locating potential performance problems.

- *Admission of New Nodes*

The network provides supervised access for permitting new nodes to join its system. Verified nodes must gain explicit access to join the network because this requirement ensures secure communications as well as blocking unauthorized users from the system.

IV. RESULTS AND DISCUSSIONS

The proposed Dominant Optimization System (DOS) algorithm is examined by Network Simulator-2 (NS-2) for assessing its capabilities to provide efficient and secure wireless sensor network transmission. Virtual movements of mobile nodes through 40 nodes within a 1000m × 1000m rectangular zone happen based on Random Waypoint Model between 100 to 200 seconds. The simulation utilizes a 2 Mbps wireless channel combined with DCF MAC protocol of IEEE 802.11 for managing network layer link breaks. The simulation of node mobility occurs through speed variations ranging from 2 to 10 m/s and from 5 to 25 m/s according to normal distribution. Continuous data transfer requires Network traffic to operate under Constant Bit Rate (CBR) conditions. A power management system which utilizes fixed packet reception power of 200-400 mW joins forces with an energy-efficient mathematical model that manages energy levels for making effective routing choices.

Two main parameters evaluate the performance of the proposed DOS technique including Energy consumption and Packet Delivery Ratio (PDR) together with Energy Consumption. The Packet Delivery Ratio decreases when non-pruned nodes' energy falls which leads to unstable multipath routing. The system maintains a foreseeable PDR through selecting nodes with larger remaining energies as routing points while operating regardless of node failures or link failures. The end-to-end delay experiences significant reduction during the transit of data packets from the source node to the destination node when the optimized route method is used. The research pays special attention to energy efficiency because Wireless Sensor Network nodes operate with minimal power supplies. The presented mathematical energy model enhances routing decisions through low energy consumption while minimizing both retransmission volume and control overhead. The system optimizes energy waste through its operations to extend network runtime as node energy supplies stay intact. The implemented system operates reliably under different mobility conditions and achieves high packet delivery performance and extends network operational time by efficiently utilizing energy resources. The dynamic route-selection based on node energies in the proposed DOS method delivers optimal packet-loss performance while maintaining consistent PDR and improved throughput alongside high scalability and security for multiple actual WSN applications.

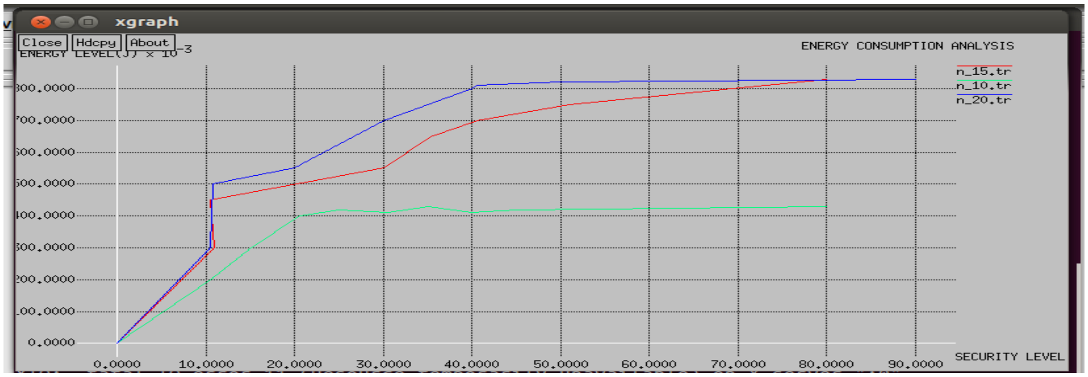

Fig.2 Energy consumption analysis(Comparison between different technologies[Green line—SSGOR])

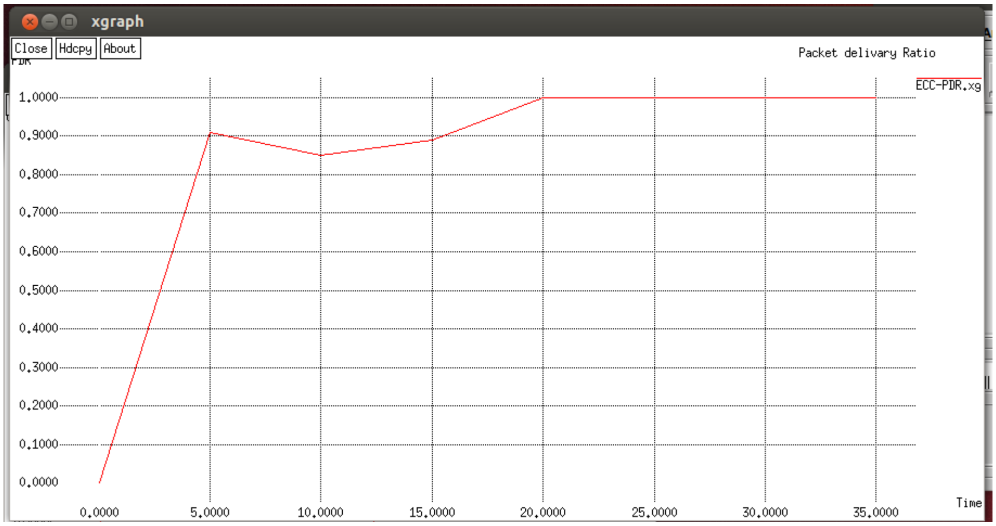

Fig. Packet Delivery Ratio PDR vs Time

REFERENCES

[1] M. Soula, B. Mbarek, A. Meddeb, and T. Pitner, “A Survey of Intrusion Detection-Based Trust Management Approaches in IoT Networks,” in Advanced Information Networking and Applications, vol. 655, L. Barolli, Ed., in Lecture Notes in Networks and Systems, vol. 655. , Cham: Springer International Publishing, 2023, pp. 504–517. doi: 10.1007/978-3-031-28694-0_48.

[2] C. Liu, J. Yang, R. Chen, Y. Zhang, and J. Zeng, “Research on immunity-based intrusion detection technology for the Internet of Things,” in 2011 Seventh International Conference on Natural Computation, Shanghai, China: IEEE, Jul. 2011, pp. 212–216. doi: 10.1109/ICNC.2011.6022060.

[3] L. Wallgren, S. Raza, and T. Voigt, “Routing Attacks and Countermeasures in the RPL-Based Internet of Things,” Int. J. Distrib. Sens. Netw., vol. 9, no. 8, p. 794326, Aug. 2013, doi: 10.1155/2013/794326.

[4] H. Sharma, B. Shajahan, R. Elangovan, and M. Thirumalaisamy, “DoS Attack Detection Mechanism in Wireless Sensor Networks,” Salud Cienc. Tecnol., vol. 2, p. 244, Dec. 2022, doi: 10.56294/saludcyt2022244.

[5] P. Sathishkumar, A. Gnanabaskaran, M. Saradha, and R. Gopinath, “Dos attack detection using fuzzy temporal deep long Short-Term memory algorithm in wireless sensor network,” Ain Shams Eng. J., vol. 15, no. 12, p. 103052, Dec. 2024, doi: 10.1016/j.asej.2024.103052.

[6] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, “Denial-of-Service detection in 6LoWPAN based Internet of Things,” in 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, France: IEEE, Oct. 2013, pp. 600–607. doi: 10.1109/WiMOB.2013.6673419.

[7] R. Wang, S. Gao, W. Yang, and Z. Jiang, “Energy aware routing with link disjoint backup paths,” Comput. Netw., vol. 115, pp. 42–53, Mar. 2017, doi: 10.1016/j.comnet.2017.01.015.

[8] K. Aravind and P. K. R. Maddikunta, “Multiobjectives for Optimal Geographic Routing in IoT Health Care System,” Complexity, vol. 2022, no. 1, p. 7568804, Jan. 2022, doi: 10.1155/2022/7568804.

[9] D. Oh, D. Kim, and W. Ro, “A Malicious Pattern Detection Engine for Embedded Security Systems in the Internet of Things,” Sensors, vol. 14, no. 12, pp. 24188–24211, Dec. 2014, doi: 10.3390/s141224188.

[10] M. Saideh, J.-P. Jamont, and L. Vercouter, “Opportunistic Sensor-Based Authentication Factors in and for the Internet of Things,” 2024, doi: 10.48550/ARXIV.2404.07675.

[11] S. Swami, P. Singh, and S. S. Chauhan, “An Integrated Rule-Based and Machine Learning Technique for Efficient DoS Attack Detection in WSN,” in 2024 2nd International Conference on Disruptive Technologies (ICDT), Greater Noida, India: IEEE, Mar. 2024, pp. 847–851. doi: 10.1109/ICDT61202.2024.10489560.

[12] B. J. Santhosh Kumar and S. Sinha, “An Intrusion Detection and Prevention System against DOS Attacks for Internet-Integrated WSN,” in 2022 7th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India: IEEE, Jun. 2022, pp. 793–797. doi: 10.1109/ICCES54183.2022.9835838.

[13] S. M. Mohamed, H. S. Hamza, and I. A. Saroit, “Coverage in mobile wireless sensor networks (M-WSN): A survey,” Comput. Commun., vol. 110, pp. 133–150, Sep. 2017, doi: 10.1016/j.comcom.2017.06.010.