International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

Enhanced Secure AODV for Real-Time IoT WSN Applications under Black Hole and Selective Forwarding Attacks

[1]Abhishek Chouhan, [2]Professor Amit Thakur

[1,2]School of Engineering & Technology, Samrat Vikramaditya Vishwavidyalaya, Ujjain, Madhya Pradesh

ABSTRACT

The rapid advancement of the Internet of Things (IoT) has led to the widespread deployment of Wireless Sensor Networks (WSNs) in various real-time applications, including healthcare monitoring, industrial automation, environmental surveillance, smart agriculture, and intelligent transportation systems. These applications require reliable, secure, and energy-efficient communication among sensor nodes. However, the open and decentralized architecture of IoT-enabled WSNs makes them highly vulnerable to routing attacks such as Black Hole and Selective Forwarding attacks. These attacks can significantly degrade network performance by increasing packet loss, reducing throughput, disrupting communication reliability, and compromising Quality of Service (QoS). The traditional Ad Hoc On-Demand Distance Vector (AODV) routing protocol lacks sufficient security mechanisms to effectively identify and mitigate such malicious activities, making it unsuitable for secure real-time IoT environments.

Keywords- Internet of Things (IoT) , Wireless Sensor Networks (WSNs) , Ad Hoc On-Demand Distance Vector (AODV) , Enhanced Secure AODV and Machine Learning.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are distributed networks composed of numerous small, low-cost, and energy-efficient sensor nodes that are deployed to monitor and collect information from physical or environmental conditions such as temperature, humidity, pressure, vibration, sound, light intensity, and motion. These sensor nodes are equipped with sensing, processing, communication, and power units, enabling them to gather data from the surrounding environment and transmit it wirelessly to a central base station or sink node for further processing and analysis. The development of microelectromechanical systems (MEMS), wireless communication technologies, and embedded computing has significantly contributed to the rapid advancement and widespread adoption of WSNs across various domains [1].

A typical Wireless Sensor Network consists of hundreds or even thousands of sensor nodes deployed over a geographical area to perform collaborative sensing tasks. Each node operates autonomously and communicates with neighboring nodes through wireless links. Due to limited transmission ranges and energy constraints, data is often forwarded through multiple intermediate nodes before reaching the destination [2]. This multi-hop communication mechanism enables efficient coverage of large monitoring areas while conserving energy resources. The sink node acts as a gateway between the sensor network and external networks, collecting data from sensor nodes and forwarding it to users or cloud-based applications [3].

International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

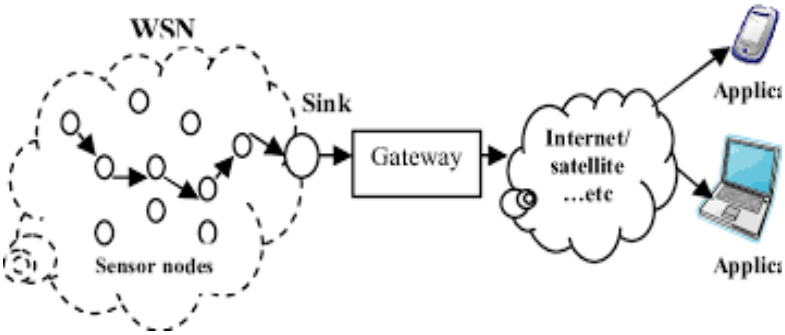

Fig.1.1 Network path selection and communication.

2. SECURITY CHALLENGES IN IOT-ENABLED WIRELESS SENSOR NETWORKS (WSNS)

The integration of Wireless Sensor Networks (WSNs) with the Internet of Things (IoT) has revolutionized modern communication systems by enabling intelligent monitoring, automation, and real-time data exchange across a wide range of applications. IoT-enabled WSNs are extensively utilized in smart healthcare, industrial automation, environmental monitoring, smart agriculture, transportation systems, and smart city infrastructures. Despite their numerous benefits, these networks face significant security challenges due to their distributed architecture, wireless communication medium, resource-constrained sensor nodes, and large-scale deployment. Security has become a critical concern because any compromise in network integrity, confidentiality, or availability can lead to severe consequences, particularly in mission-critical applications [4].

One of the primary security challenges in IoT-enabled WSNs is the limited computational and energy resources of sensor nodes. Most sensor devices possess restricted processing power, memory capacity, and battery life, making it difficult to implement complex cryptographic algorithms and advanced security mechanisms. While strong encryption techniques can enhance security, they often require substantial computational resources and energy consumption, which may significantly reduce network lifetime. Therefore, designing lightweight yet effective security solutions remains a major research challenge in IoT-enabled WSN environments [5].

3. AD HOC ON-DEMAND DISTANCE VECTOR (AODV) ROUTING PROTOCOL

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol is one of the most widely adopted reactive routing protocols designed for Mobile Ad Hoc Networks (MANETs), Wireless Sensor Networks (WSNs), and Internet of Things (IoT)-enabled communication environments. AODV was developed to provide efficient routing in dynamic wireless networks where nodes frequently join, leave, or move within the network. Unlike traditional routing protocols that maintain complete routing information for all nodes at all times, AODV establishes routes only when communication is required. This on-demand routing approach significantly reduces routing overhead, conserves network resources, and improves communication efficiency, making it highly suitable for resource-constrained wireless environments [6].

AODV combines the advantages of the Destination-Sequenced Distance Vector (DSDV) routing protocol and Dynamic Source Routing (DSR) protocol while minimizing their limitations. The protocol utilizes a distance vector routing mechanism along with destination sequence numbers to ensure loop-free routing and route freshness. Because routes are created only when needed, AODV efficiently supports dynamic network topologies and reduces unnecessary control message exchanges. These characteristics have contributed to its widespread adoption in wireless communication research and practical network deployments [7].

4. OVERVIEW OF THE PROPOSED HYBRID SECURITY FRAMEWORK

The proposed research introduces a Hybrid Security Framework for Enhanced Secure Ad Hoc On-Demand Distance Vector (AODV) Routing Protocol designed specifically for real-time Internet of Things (IoT)-enabled Wireless Sensor Networks (WSNs) operating under Black Hole and Selective Forwarding attacks. The primary objective of the framework is to provide secure, reliable, energy-efficient, and attack-resistant routing by combining the strengths of Trust-Based Routing Mechanisms and Machine Learning-Based Attack Detection Techniques**.** Traditional AODV routing protocols establish communication routes based primarily on route discovery information such as sequence numbers and hop counts, without considering node trustworthiness or malicious behavior. As a result, malicious nodes can exploit routing procedures and disrupt network communication [8]. The proposed hybrid framework addresses these vulnerabilities by incorporating intelligent security mechanisms capable of detecting, isolating, and preventing malicious nodes from participating in routing operations.

The proposed framework consists of two complementary security layers. The first layer is a Trust Evaluation Layer**,** which continuously monitors the behavior of neighboring nodes and calculates trust values based on multiple network performance indicators. These indicators include packet forwarding ratio, packet delivery success rate, residual energy level, communication reliability, and link quality. Nodes that consistently exhibit cooperative behavior receive higher trust scores, while nodes demonstrating suspicious or abnormal activities receive lower trust values. This trust evaluation mechanism helps identify potentially malicious nodes at an early stage and provides an initial level of routing security [9].

Although trust-based approaches are effective in evaluating node behavior, they may sometimes produce inaccurate results due to network congestion, wireless interference, temporary link failures, or environmental disturbances. To overcome these limitations, the second layer of the framework incorporates a Machine Learning-Based Attack Detection Module. This module analyzes various routing and communication features collected from network nodes, including trust values, packet drop ratios, forwarding behavior, route reply frequencies, throughput, delay characteristics, and residual energy levels. Using a trained machine learning classifier, such as Random Forest, Support Vector Machine (SVM), or K-Nearest Neighbor (KNN), the system classifies nodes as normal, suspicious, Black Hole attackers, or Selective Forwarding attackers. Machine learning provides intelligent decision-making capabilities that improve attack detection accuracy and reduce false positive rates [10-13].

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

5. PROPOSED SYSTEM ARCHITECTURE

The proposed system architecture is designed to enhance the security and performance of the Ad Hoc On-Demand Distance Vector (AODV) routing protocol in Internet of Things (IoT)-enabled Wireless Sensor Networks (WSNs) operating under Black Hole and Selective Forwarding attacks. The architecture integrates Trust-Based Routing and Machine Learning-Based Attack Detection into a unified hybrid security framework capable of identifying malicious nodes, selecting secure communication routes, and maintaining reliable data transmission. The proposed architecture aims to improve network security, Packet Delivery Ratio (PDR), throughput, energy efficiency, and Quality of Service (QoS) while minimizing the impact of routing attacks.

The proposed framework consists of several interconnected modules that work collaboratively to monitor node behavior, evaluate trustworthiness, detect malicious activities, and establish secure communication paths. These modules include the IoT Sensor Node Layer, AODV Routing Layer, Trust Evaluation Module, Feature Extraction Module, Machine Learning Detection Module, Decision Engine, Malicious Node Isolation Module, and Secure Route Selection Module. Together, these components provide a multi-layered security mechanism capable of protecting the network from sophisticated routing attacks.

6. NETWORK MODEL

The Network Model describes the structure, operational environment, assumptions, and communication characteristics of the proposed Hybrid Machine Learning and Trust-Based Enhanced Secure AODV Routing Protocol for Internet of Things (IoT)-enabled Wireless Sensor Networks (WSNs). It provides the foundation upon which the proposed security framework is designed, implemented, and evaluated. The network model defines how sensor nodes are deployed, how communication occurs among nodes, the behavior of legitimate and malicious nodes, and the assumptions considered during protocol development and performance analysis. A well-defined network model is essential for accurately assessing the effectiveness of the proposed routing protocol under normal and attack scenarios.

7. ENHANCED SECURE AODV ALGORITHM

The Enhanced Secure Ad Hoc On-Demand Distance Vector (ESAODV) Algorithm is the core routing mechanism proposed in this research to provide secure, reliable, and efficient communication in Internet of Things (IoT)-enabled Wireless Sensor Networks (WSNs) operating under Black Hole and Selective Forwarding attacks. The algorithm extends the conventional AODV routing protocol by incorporating Trust-Based Node Evaluation**,** Machine Learning-Based Attack Detection**,** Malicious Node Isolation**, and** Route Optimization Mechanisms**.** Traditional AODV protocols establish routes based primarily on destination sequence numbers and hop counts without considering the trustworthiness of participating nodes. As a result, malicious nodes can easily exploit the route discovery process by advertising false routing information and attracting network traffic. Once included in a route, these attackers may drop packets, manipulate routing information, or disrupt communication. The proposed Enhanced Secure AODV Algorithm addresses these vulnerabilities by introducing

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

intelligent security mechanisms that continuously evaluate node behavior and ensure that only trusted nodes participate in routing operations.

The algorithm begins with the deployment of IoT sensor nodes within the network area. Each node is assigned a unique identification number and is initialized with routing, trust, and energy parameters. During network operation, when a source node intends to communicate with a destination node, it initiates the route discovery process by broadcasting a Route Request (RREQ) packet. Similar to conventional AODV, neighboring nodes receive the RREQ packet and forward it toward the destination. However, unlike traditional AODV, the proposed algorithm does not immediately accept all routing information. Instead, it evaluates the trustworthiness of nodes involved in route formation before establishing communication paths.

8. RESULT AND SIMULATION

The figure shows the simulation results of the proposed Framework under a Black Hole attack scenario in an IoT-enabled Wireless Sensor Network (WSN). The results demonstrate strong network performance with a Packet Delivery Ratio (PDR) of 99.40%, throughput of 5.09 kbps, and a very low end-to-end delay of 0.0285 seconds. The framework also achieves a detection accuracy of 95.96% while maintaining a low false positive rate of 1.46%, indicating effective attack detection and mitigation. Furthermore, the network exhibits reduced energy consumption (2.24 J), extended network lifetime (978 rounds), and manageable routing overhead (9.60%), highlighting the robustness and reliability of the proposed approach in securing WSN communications against malicious routing attacks.

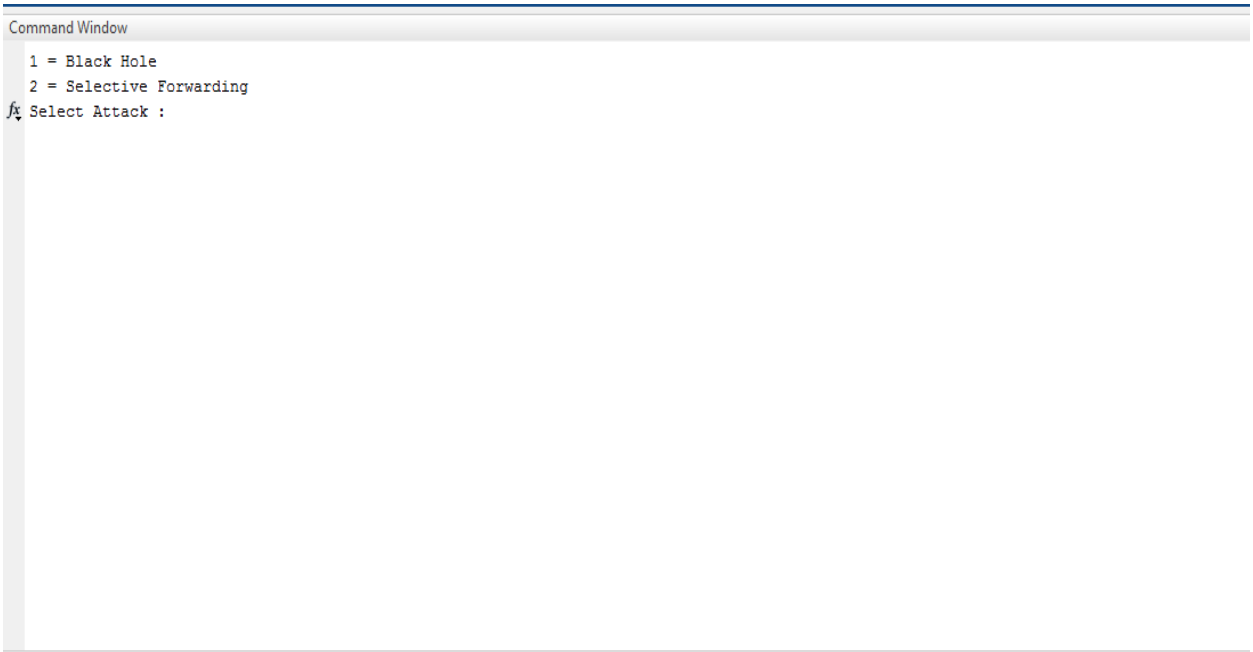

Fig.6.1 Selection.

International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

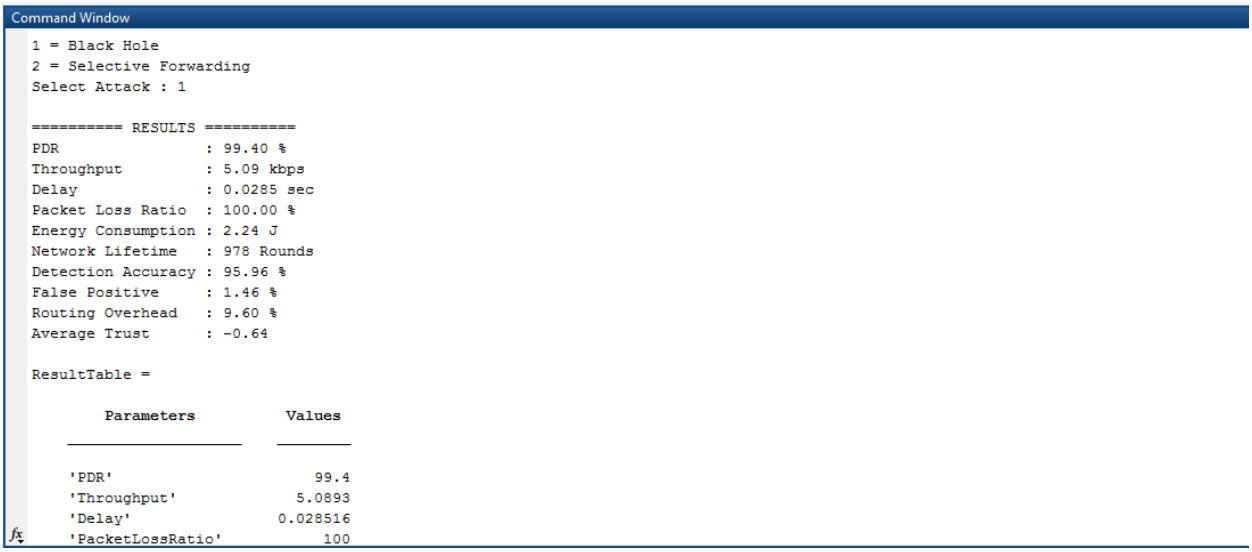

Fig.6.2 When select Input 1 Results Obtained.

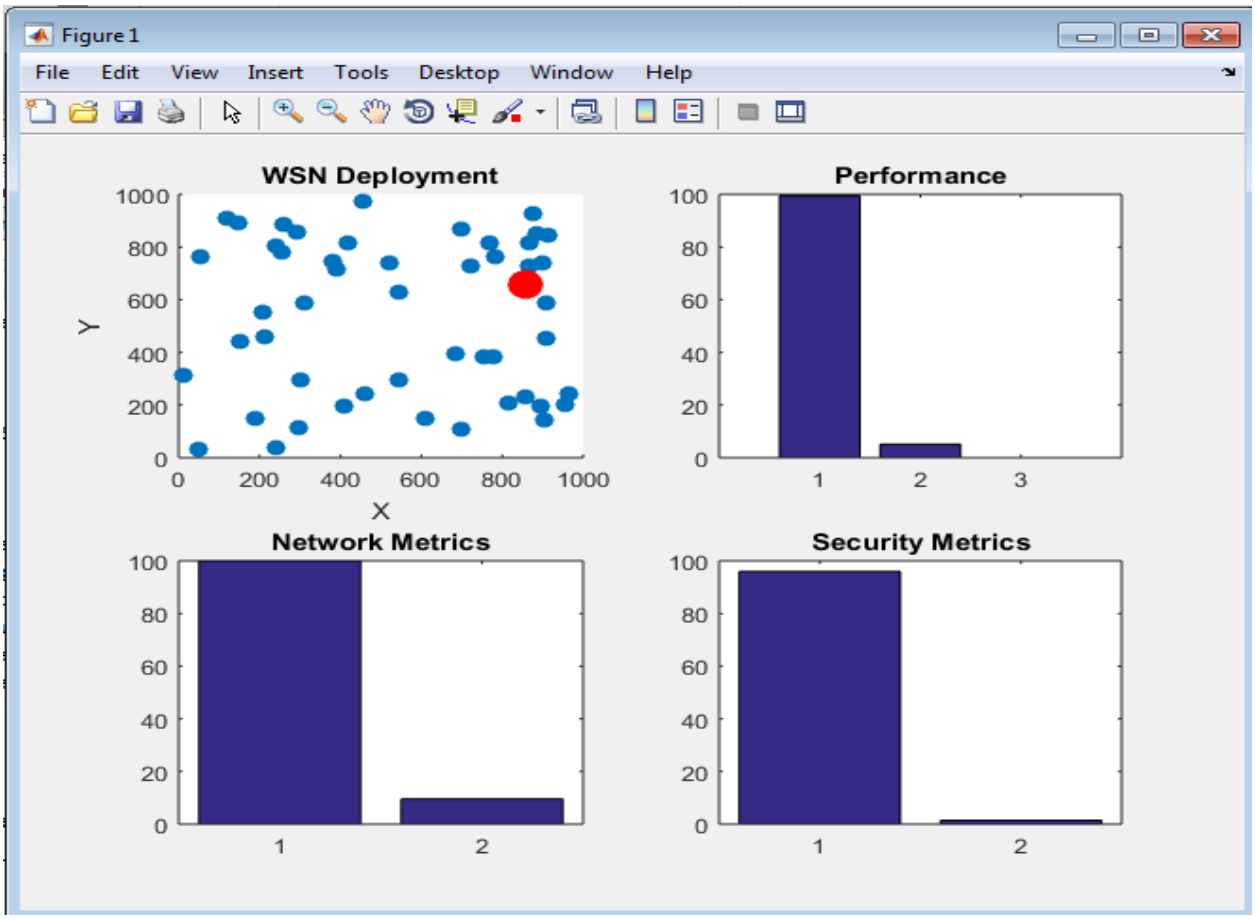

Fig.6.3 When select Input 1 Results Obtained Metrics.

International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

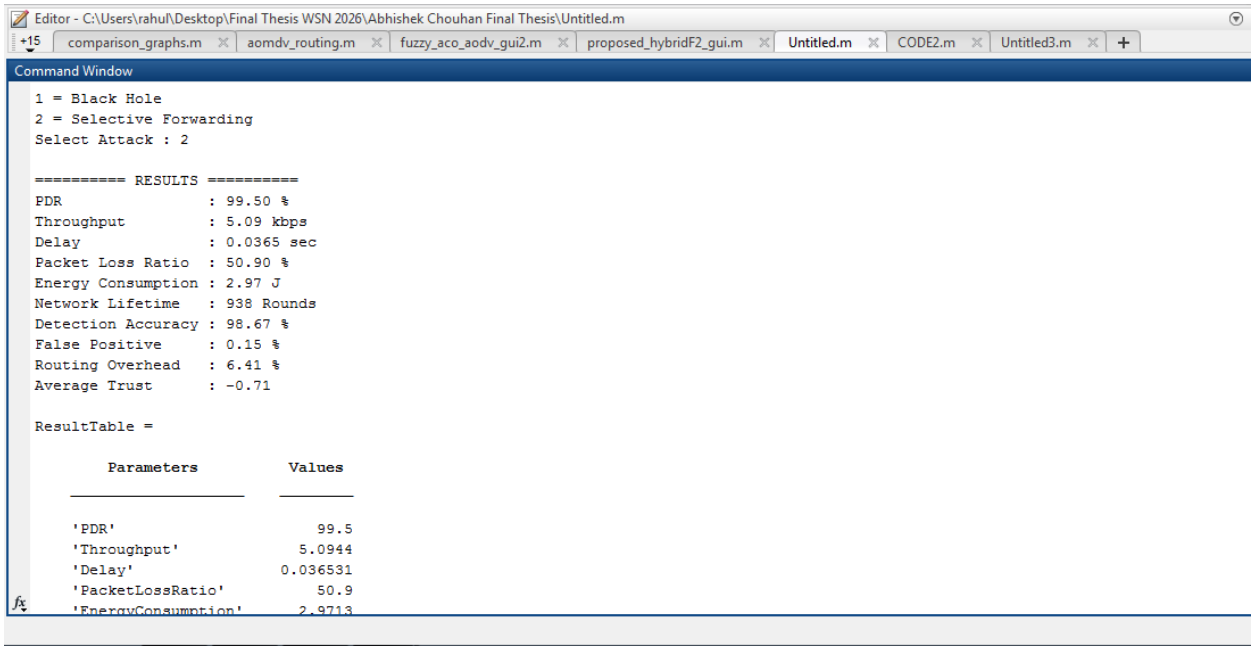

Fig.6.4 Selection 2.

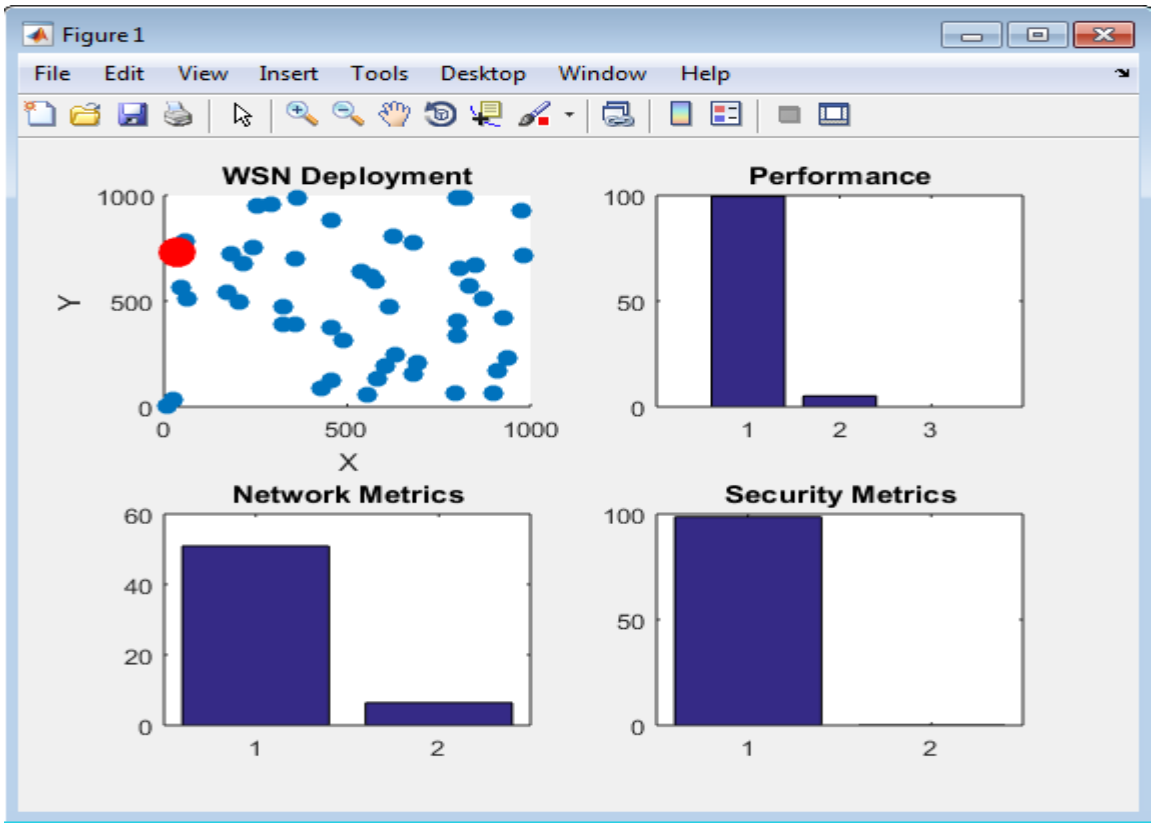

Fig.6.5 When select Input 2 Results Obtained Metrics.

9. CONCLUSION

The rapid growth of Internet of Things (IoT) technologies and Wireless Sensor Networks (WSNs) has significantly increased the demand for secure, reliable, and efficient communication mechanisms capable of supporting real-time applications. However, the open and decentralized nature of IoT-enabled WSNs makes them highly vulnerable to routing attacks such as Black Hole and Selective Forwarding attacks, which can severely degrade network performance, compromise data integrity, and reduce communication reliability. Traditional routing protocols, particularly the Ad Hoc On-Demand Distance Vector (AODV) protocol, are primarily designed to establish routes based on hop count and sequence numbers without considering the trustworthiness of participating nodes. As a result, malicious nodes can easily exploit routing procedures and disrupt network operations. To address these challenges, this research proposed a Hybrid Machine Learning and Trust-Based Enhanced Secure AODV Routing Framework that integrates trust evaluation, machine learning-based attack detection, malicious node isolation, and route optimization techniques into the conventional AODV protocol.

10. FUTURE SCOPE

Although the proposed Hybrid Machine Learning and Trust-Based Enhanced Secure AODV Routing Framework demonstrates promising results in improving routing security and network performance, several opportunities exist for further enhancement and future research. One potential direction is the integration of advanced Deep Learning techniques such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and Transformer-based models for attack detection. These approaches may improve the capability of the framework to identify complex, evolving, and previously unseen attack patterns in large-scale IoT environments. Future studies may also investigate reinforcement learning-based routing mechanisms that can dynamically adapt routing decisions according to changing network conditions and attacker behaviors.

REFERENCE

1. Ramesh, R. B., Thangaraj, S. J. J., Sagayee, G. M. A., & Saravanan, K. (2025). Detection and prevention in WSN security framework using deep learning against black hole and wormhole attacks. Ain Shams Engineering Journal, 16(10), 103624.
2. Satori, H. (2024). Machine learning attack detection based-on stochastic classifier methods for enhancing of routing security in wireless sensor networks. Ad Hoc Networks, 163, 103581.
3. Sangaiah, A. K., Javadpour, A., Ja'fari, F., Pinto, P., Ahmadi, H., & Zhang, W. (2022). CL-MLSP: The design of a detection mechanism for sinkhole attacks in smart cities. Microprocessors and Microsystems, 90, 104504.
4. Jain, J. K., & Chauhan, D. (2025). Optimized secure and energy-efficient approach for IoT-enabled wireless sensor networks. Pervasive and Mobile Computing, 110, 102049.
5. Babu, E. S., Padma, B., Nayak, S. R., Mohammad, N., & Ghosh, U. (2023). Cooperative IDS for Detecting Collaborative Attacks in RPL-AODV Protocol in Internet of Everything. Journal of Database Management (JDM), 34(2), 1-33.

6. Dhand, G., Rao, M., Chaudhary, P., & Sheoran, K. (2025). A secure routing and malicious node detection in mobile Ad hoc network using trust value evaluation with improved XGBoost mechanism. Journal of Network and Computer Applications, 235, 104093.
7. Mali, S. D., & Govinda, K. (2023). A study on network routing attacks in IoT. Materials Today: Proceedings, 80, 2997-3002.
8. Ceviz, O., Sadioglu, P., Sen, S., & Vassilakis, V. G. (2025). A novel federated learning-based IDS for enhancing UAVs privacy and security. Internet of Things, 31, 101592.
9. Fan, N., Wu, C., Benabdallah, S., Li, J., Gao, Y., & Wang, Q. (2024). On a security scheme against collusive attacks in vehicular ad hoc networks. Vehicular Communications, 49, 100821.
10. Yang, Z., Li, L., Gu, F., Ling, X., & Hajiee, M. (2022). TADR-EAODV: A trust-aware dynamic routing algorithm based on extended AODV protocol for secure communications in wireless sensor networks. Internet of Things, 20, 100627.
11. Mishra, R. (2024). Raspberry Pi Performance analysis across its Operating System in LED Control Operation. International Journal of Advanced Research and Multidisciplinary Trends (IJARMT), 1(2), 01-11.
12. Mishra, R. (2025). IOT and DSP (combination of hardcore Virtex-5 FPGA and soft core DSP processor) OFDM System PAPR Reduction Using Artificial Intelligence Algorithm. International Journal of Advanced Research and Multidisciplinary Trends (IJARMT), 2(1), 135-149.
13. Mishra, R., & Sharma, A. (2026). Enhanced Trajectory Tracking of a 6-DOF Robotic Manipulator Using GA–PID and ANN–PID Controllers. International Journal of Research & Technology, 14(2), 53-70.