International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

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

Abhishek Chouhan, Professor Amit Thakur
School Of Engineering and Technology, Vikram University, Ujjain University in Ujjain, Madhya Pradesh

ABSTRACT
Wireless sensor networks (WSNs) are being used to facilitate monitoring of patients in hospital and home environments. These systems consist of a variety of different components/sensors and many processes like clustering, routing, security, and self-organization. Routing is necessary for medical-based WSNs because it allows remote data delivery and it facilitates network scalability in large hospitals. However, routing entails several problems, mainly due to the open nature of wireless networks, and these need to be addressed. This paper looks at two of the problems that arise due to wireless routing between the nodes and access points of a medical WSN (for IoT use): black hole and selective forwarding (SF) attacks. A solution to the former can readily be provided through the use of cryptographic hashes, while the latter makes use of a neighbourhood watch and threshold-based analysis to detect and correct SF attacks.

Keywords: routing attacks, black hole, selective forwarding, sensor networks, medical WSN, IoT-Internet of Things

I. INTRODUCTION

A Wireless Sensor Network (WSN) consists of large number of sensor nodes working in cooperation manner to gather the information from the monitoring region. Generally WSN have little or no infrastructure. There are two types of WSNs: structured and unstructured [1]. In unstructured WSN there are huge numbers of nodes deployed randomly to monitor the region. Due to unavailability of physical presence on the region, network maintenance activities are difficult. In a structured WSN, all the nodes are deployed in fixed and planned manner. Positive point of a structured network is that fewer nodes can be deployed and requires fewer maintenance and management cost. In a WSN the object performing task of sensing is called a sensor. Sensor nodes are low power devices equipped with one or more sensors, processor, memory, power supply, a radio, and an actuator [2]. A variety of mechanical power, thermal sensor, biological, chemical, optical sensor, and magnetic sensors can be attached to enhance the power of sensor nodes [1]. Since the sensor nodes have limited memory and are deployed in harsh environment and in difficult locations, radio transmitter is implemented to transfer the collected data to base station. WSNs have many applications such as military target tracking and surveillance, disaster relief, health monitoring, environment exploration seismic sensing to measure the environment.

In modern times, security remains a significant concern in wireless networks. Wireless sensor networks are widely employed in different practical situations. WSNs struggle with numerous internal and external threats, and detecting and defending against insider attacks is difficult.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

Insider attacks, in which intruders discard received data packets selectively, pose a significant risk to WSNs. The presence of black hole nodes within the network causes this issue. This research paper presents a secure and reliable route management methodology for WSNs that selects nodes and routing paths based on trust metrics. The proposed mechanism employs intelligent routing and node selection to defend against various types of assaults encountered during the routing process, including selective forwarding and black hole attacks. As a result, the paper identifies secure routes and establishes secure network routing. This scheme uses throughput, latency, and packet drop ratio as performance metrics. Experimentation demonstrates that the proposed system effectively increases the probability of secure network routing paths while extending the network lifecycle.

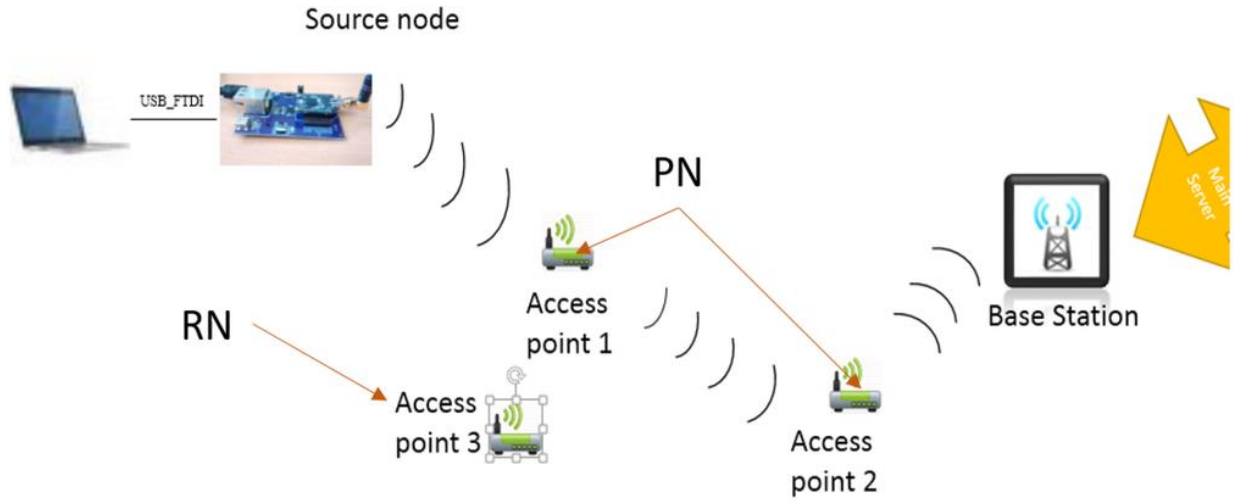

Fig.1. Selective Attack.

II. MULTI HOP MOBILE AD HOC NETWORK (MANET)

A Multi hop Mobile Ad hoc Network (MANET) is an infrastructure less in which mobile nodes communicate directly and cooperatively with each other. Each and every mobile node is highly distributed where it deals with Multicast technology. Since there is no proper access points or routers, and no configuration prior to setup of a MANET is required, it's very difficult to centralize administration on MANET where such set up make different issues such as routing, authentication, or congestion control. Also, due to high mobility, resource constrains (power, storage, and bandwidth) in MANET environment, and nodes operating in a dynamic topology, more challenges are encountered in routing. The need of Ad-hoc On-Demand Distance Vector (AODV) routing protocol ensures the design principles of ADHOC mobile network. This protocol will be proactive when router is initiated. In enhance predefined routing table with entry destination and sequence number to figure out routing information. Further such incorporation leads to routing loop mechanism. Another important feature of AODV protocol is time based node state maintenance. It ensures control packets like RREQ (routing request message) to communicate with other node for broadcasting message. The need for IDS in MANET develops various security standards to make Mobile network reliable towards data transmission. The attack in MANET varies from general network attack and further classified based on the criteria. The classifications were listed as passive or active, internal or external,

stealthy or non-stealthy. Black Hole attack is a kind of attack holds the above mentioned property.

The node which makes such kind of attack was declared to be malicious and hence the attack known as Black Hole attack. A Malicious node absorbs all kind of packets and terminates further packet transmission. In other words, the network packets were further will not be send beyond malicious node. In this way, all packets in the network are dropped. Deploying IDS in wireless sensor networks (WSNs) for mission critical applications (such as intruder detection and tracking) often face the fundamental challenge of meeting stringent spatial and temporal performance requirements imposed by users. For instance, a surveillance application may require any intruder to be detected with a high probability (e.g., >90%).

III. CONSTRAINTS FOR WSNS

In the wireless sensor network, sensors are organized into the specific configuration to satisfy the requirements of adhoc applications. Unfortunately, the connectivity cannot remain unchanging at any working time. The sensor network is a broadcast network in which any signal can be captured by adversaries at any time. These features make wireless ad-hoc sensor networks more vulnerable than wired networks [2].

Resource Constraints: Energy Constraints: Energy is one of the important constraints for WSNs. In sensor nodes energy consumption can be categorized in three parts: Sensor transducer, Communication among sensor nodes, microprocessor computation.

Memory Limitation: A sensor is a tiny device with a small amount of memory and storage space. Sensor nodes memory is usually includes flash memory and RAM (used for storing application programs, sensor info & intermediate results of computations). Usually, there is not sufficient space to run complicated programs or codes after loading the OS and application code.

Lack of Central Control: Because of resource constraints and network dynamics it is not feasible to have a central point of control in sensor networks. Therefore security solutions must be decentralized and nodes must be able to achieve security [5].

Remote Locations: As sensor nodes are deployed in hardto-reach locations so it will be infeasible to continuously monitor and protect the nodes from attacks. That why it will be difficult maintain a secure network.

Error-prone Communication: Unreliable communication is a dangerous threat to sensor security. Packets in WSNs may be lost due to collision, channel errors or routing failures. This may interfere with security mechanisms.

IV. BLACK HOLE ATTACK

In this attack, a malicious node falsely advertises optimal paths (e.g. the shortest path or the most stable path) to the destination node during the path-finding process (in reactive routing protocols), or in the route updates messages (in proactive routing protocols). The intention of the malicious node could be to hinder the path-finding process or to intercept all data packets being sent to the destination node. A more delicate form of this attack is known as the grayhole attack, where the malicious node intermittently drops the data packets thereby making its detection even more difficult [4].

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

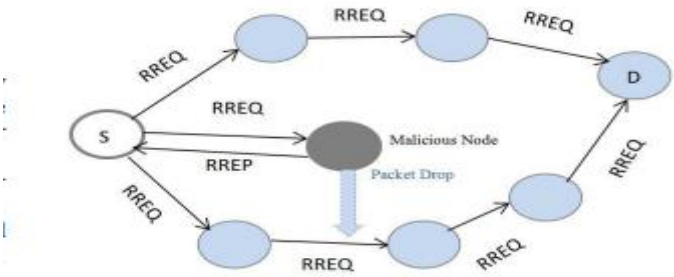

Fig. 2. Black Hole Attack

Black hole attacks are classified into two categories:

- Single Black Hole Attack: In single black hole attack only one node act as malicious or compromised node which misbehaves within the network. It is also known as black hole attack with single malicious node.
- Collaborative Black Hole Attack: In collaborative black hole attack multiple nodes behaves as malicious node in the network and work in co-operative manner. It is also known as the black hole attack with multiple malicious nodes.

V. PROBLEM IDENTIFICATION

In real-time Internet of Things (IoT) based Wireless Sensor Network (WSN) applications, reliable and secure routing is a critical requirement due to strict constraints on latency, energy consumption, and packet delivery. The Ad hoc On-Demand Distance Vector (AODV) routing protocol is widely adopted in WSNs because of its simplicity and low control overhead; however, it was originally designed without built-in security mechanisms. As a result, AODV is highly vulnerable to routing attacks, particularly Black Hole and Selective Forwarding attacks, where malicious nodes either absorb all data packets or selectively drop them, leading to severe packet loss, increased end-to-end delay, reduced throughput, and rapid energy depletion. These attacks are especially harmful in real-time IoT applications such as healthcare monitoring, industrial automation, and smart surveillance, where timely and trustworthy data delivery is essential. Existing secure AODV variants and trust-based solutions either focus on a single attack, introduce high computational and communication overhead, or fail to meet real-time performance requirements under dynamic network conditions. Therefore, there exists a significant research gap in designing an enhanced secure AODV routing mechanism that can efficiently detect and mitigate both Black Hole and Selective Forwarding attacks simultaneously, while maintaining low latency, energy efficiency, and high packet delivery ratio suitable for real-time IoT-based WSN environments.

VI. RESEARCH SIGNIFICANCE

The proposed research on Enhanced Secure AODV for Real-Time IoT-based Wireless Sensor Network (WSN) Applications under Black Hole and Selective Forwarding Attacks is significant due to the increasing deployment of IoT-enabled WSNs in mission-critical and real-time environments such as healthcare monitoring, smart grids, industrial automation, and intelligent transportation systems. These applications demand not only high data delivery reliability and low latency but also strong resilience against malicious routing attacks. Traditional AODV and its existing secure variants are inadequate in such environments, as they

either lack effective attack detection mechanisms or introduce excessive computational and communication overhead that degrades real-time performance.

VII. LITERATURE REVIEW

R Barath Ramesh et al.[1] This paper proposed an energy-aware and adaptive IDS for WSNs with the main focus of tackling the Black Hole and Wormhole attacks on the routing systems. Based on the achieved results, the advanced feature generation is delivered by the use of the GANs, while the WOA is used for the tuning of the parameters of the method; furthermore, deep Q-learning is used for the adaptive learning of the attacks' patterns. Several simulation experiments were performed with the help of a MATLAB-based WSN environment.

Anselme R. Affane M et al.[2] Wireless Sensor Networks (WSNs) are vulnerable to attacks during data transmission, and many techniques have been proposed to detect and secure routing data. In this paper, we introduce a novel stochastic predictive machine learning approach designed to discern untrustworthy events and unreliable routing attributes, aiming to establish an artificial intelligence-based attack detection system for WSNs. Our methodology leverages real-time analysis of the features of simulated WSN routing data. By integrating Hidden Markov Models (HMM) with Gaussian Mixture Models (GMM), we develop a robust classification framework. This framework effectively identifies outliers, pinpoints malicious network behaviors from their origins, and categorizes them as either trusted or untrusted network activities.

Arun Kumar Sangaiah et al.[3] This research aims to represent a novel approach to detect malicious nodes in Ad-hoc On-demand Distance Vector (AODV) within the next-generation smart cities. Smart city applications have a critical role in improving public services quality, and security is their main weakness. Hence, a systematic multidimensional approach is required for data storage and security. Routing attacks, especially sinkholes, can direct the network data to an attacker and can also disrupt the network equipment. Communications need to be with integrity, confidentiality, and authentication.

Jay Kumar Jain et al.[4] Wireless communication is pivotal in the modern era, enabling seamless connectivity across diverse applications. However, the increasing complexity and sophistication of cyber threats pose significant challenges to the security of wireless communication systems. This paper proposes an innovative approach to enhance wireless communication security through integrating artificial intelligence (AI) techniques. First, we construct the network using the Horizontal Partitioning Sierpinski Triangle to reduce the network's high traffic and perform the authentication process.

Erukala Suresh Babu et al.[5] Internet of everything (IoET) is one of the key integrators in Industry 4.0, which contributes to large-scale deployment of low-power and lossy (LLN) networks to connecting people, processes, data, and things. The RPL is one of the unique standardized routing protocols that enable efficient use of smart devices energy, compute resources to address the properties and constraints of LLN networks. The authors investigate the RPL-AODV routing protocol's performance in combining the advantages of both RPL and AODV routing protocol, which works together in a low power resource-constrained network.

Geetika Dhand et al.[6] Mobile ad hoc networks (MANETs) are beneficial in a wide range of sectors because of their rapid network creation capabilities. If mobile nodes collaborate and have mutual trust, the network can function properly. Routing becomes more difficult, and vulnerabilities are exposed more quickly as a result of flexible network features and frequent relationship flaws induced by node movement. This paper proposes a method for evaluating trust nodes using direct trust values, indirect trust values, and comprehensive trust values. Then, evaluating the trust value, the network's malicious and non-malicious nodes are identified using the Improved Extreme Gradient Boosting (XGBoost) algorithm. From the detected malicious nodes, the cluster head is chosen to ensure effective data transmission.

Shrikant D. Mali et al.[7] IoT (IoTs) is a collection of autonomous things. IoTs is a new pattern that includes the existing presence of different devices. It is one of the latest technologies that provide global connectivity, management of sensors, users and information. The connectivity helps devices to be connected in a ubiquitous manner. Therefore, it can be deployed in different domains such as smart home, health, city, retail, logistics, industries and farming. This has brought a new dimension to connect with objects. There are many issues associated with IoTs such as fading, energy consumption, data security, network security, etc. The ultimate aim of this assessment is to show the different kinds of routing methods to solve the problem of network routing attacks in IoTs. This paper categorizes the attacks in terms of sinkhole, black hole and wormhole attacks in tabular format.

Ozlem Ceviz et al.[8] However, these approaches face challenges including computation and storage costs, along with a single point of failure risk, threatening data privacy and availability. The widespread dispersion of data across interconnected devices underscores the need for decentralized approaches. This paper introduces the Federated Learning-based Intrusion Detection System (FL-IDS), addressing challenges encountered by centralized systems in FANETs. FL-IDS reduces computation and storage costs for both clients and the central server, which is crucial for resource-constrained UAVs. Operating in a decentralized manner, FL-IDS enables UAVs to collaboratively train a global intrusion detection model without sharing raw data, thus avoiding delay in decisions based on collected data, as is often the case with traditional methods.

Na Fan et al.[9] Vehicular Ad Hoc Networks (VANETs) offer a promising solution to bring drivers comfortable driving experiences and also improve road safety in intelligent transportation systems, but also faces many security issues. Collusive attack is one of the most challenging threats in VANETs because it violates the fundamental assumption made by VANET-based applications that all received information be correct and trustworthy. Collusive attackers can not only generate and send false or forged messages, but also purposely manipulate the reputation value of normal or malicious vehicular nodes.

Zhe Yang et al.[10] Compliance with security requirements in Wireless Sensor Networks (WSNs) is known as an important phenomenon in conserving energy consumption due to its dynamic topology. Energy consumption management in WSN can be achieved through secure routing protocols. Authentication, firewall and intrusion detection, and trust management are common ways to provide security on the WSNs. Meanwhile, trust

management provides better performance due to ensuring distributed security through collaboration. In this paper, a Trust-Aware Dynamic Routing algorithm based on Extended AODV protocol for secure communications in the WSN (TADR-EAODV) is proposed.

VIII. CONCLUSION

This review paper analyzed Enhanced Secure AODV routing techniques for real-time IoT-enabled Wireless Sensor Network (WSN) applications under Black Hole and Selective Forwarding attacks. The study highlighted that conventional AODV protocols are highly vulnerable to malicious node behavior, which degrades network reliability, packet delivery, and communication security. Various security enhancement mechanisms including trust-based routing, intrusion detection systems, cryptographic approaches, and intelligent optimization techniques were reviewed to improve routing resilience and attack detection capability. The findings indicate that enhanced secure AODV protocols significantly improve packet delivery ratio, throughput, network lifetime, and data confidentiality while reducing packet loss and routing overhead. The review concludes that secure and intelligent routing frameworks are essential for achieving reliable, energy-efficient, and attack-resistant communication in future real-time IoT-WSN applications.

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.