International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 17s,2025
https://theaspd.com/index.php

Enhancing for IoT based Network Security on Wormhole Attack Detection Techniques using Wireless Sensor Network

J. Saranya [1*] & Dr. P. Bharathisindhu [2]

[1] Ph.D Research Scholar, Department of Computer Science, Vellalar College for Women Thindal, Erode, Tamil Nadu, India
Assistant Professor, Department of Information Technology, Hindusthan College of Arts & Science, Coimbatore, Tamil Nadu, India
[2] Assistant Professor, Department of Computer Science, Vellalar College for Women Thindal, Erode, Tamil Nadu, India
[*] Corresponding Author: saranyaphd6@gmail.com

Abstract: *The security of Internet of Things (IoT) enabled Wireless Sensor Networks is increasingly challenged by sophisticated attacks that exploit their unique characteristics, including resource constraints, heterogeneity, and decentralized architectures. Understanding and protecting IoT networks against wormhole attacks requires a multifaceted approach encompassing the attack mechanics, their impact on IoT, and appropriate detection and mitigation strategies adapted to IoT's specific constraints. The primary goal of Proposed Enhanced Network Security with Wormhole Attacks (ENS-WHA's) which covers the several cutting-edge strategies that have been successfully employed over the years to identify WHA in wireless networks. The current WHA detection methods are inefficient due to the requirement for more technology, longer latency, and increased energy usage. Due to the lack of extra hardware requirements, round-trip time (RTT) related detection approaches are becoming more successful. The Existing of Two Machine learning Models, a Support Vector Machine (SVM) and Deep Neural Network (DNN), to classify the traffic data and identify malicious node in the network. Results from performance evaluations indicate that the ENS-WHA's method achieves better efficiency than SVM and DNN methods. The enhancement in Packet delivery ratio, Delay time, Energy consumption and Throughput analysis confirm that can reduce the latency, Energy wastage and improve the data delivery success rates, Positioning it as a more robust and effective network strategy.*

Keywords: *Wireless Sensor Network, Wormhole attack, Internet of Things, AODV routing Protocol, Round-Trip Time, Machine Learning Approach.*

1. Introduction

IoT networks, in particular, face increasing vulnerabilities due to the rapid proliferation of connected devices within smart infrastructures. Wireless sensor networks (WSNs) comprise software, gateways, and small sensors that wirelessly transmit and receive data[1].The growing penetration of the Internet of Things (IoT) in major industries such as health, industrial automation, and smart cities has accompanied remarkable progress in real-time data processing, automation, and decision-making**.** To identify wormhole attacks in IoT networks by analyzing network traffic patterns with the aid of machine learning. The detection process is systematic, beginning from dataset preparation, where inconsistencies and missing values are addressed [2]. Significant progress has been made in the area of wireless networks during the past few years, including the emergence of numerous new mobile handheld devices including laptops, smartphones and Internet of Things (IoT) related components [3]. Wireless Sensor networks enable data sharing and communication between wireless devices through networks with minimal or no infrastructure [4]. The nodes in a Wireless Sensor network must locate neighboring nodes in order to construct a dynamic network for the transfer of data from source to destination. The nodes travel back and forth inside the network [5] and interact with other nodes arbitrarily, which results in a random and unpredictable change

in the network structure [6]. Wireless Sensor network nodes have the ability to gather, store, process, and transmit data. In an ad hoc network, mobile nodes self-organize their operations and build a dynamic topology. Due to nodes' ability to recognize one another, the network is dependable and capable of securely exchanging information [7]. In WSN and IoT, the attacks are occurred during the communication between the devices by sending and receiving the data, Capturing the confidential information, tracking the details which is been monitored by a third party or intruder [8]**.** A wormhole attack is generally termed as a hard to detect a problem, though it is easily lodged in any wireless adhoc network. An attacker can simply launch a malicious wormhole attack without even having or compromising information about the network or any legal nodes. Most of the prevailing solutions involve special hardware devices or count on making solid postulations to discover vortex wormhole attacks that limit their usability [9]. Wireless Sensor networks are consequently non-collapsed networks because of the additional capability that some nodes have to leave and join the network as necessary [19]. Due to nodes' capacity to act as routers due to their constrained transmission range inside the network, Wireless Sensor networks are also known as multi-hop networks [20]. The packets should be forwarded uninterruptedly to the target point by each node in the network. Researchers have lately tackled the problems of wormhole attack (WHA) detection in Wireless Sensor networks [21] by employing a range of innovative IoT with Wireless Sensor Network (WSN) techniques together with other hybrid traditional [22] approaches. So, in order to familiarize the readers with the benefits and drawbacks of the most recent IoT with WSN techniques, we undertake a systematic literature review (SLR). The current study additionally concentrates on examining the problems that the proposed approaches for detecting WHAs have. Furthermore, we emphasized future directions for WHA early identification and detection study and focused on potential remedies. Because of this, the provided SLR can be very helpful to readers and the research community in selecting a suitable approach to develop a successful strategy for WHA diagnosis. In this work, we assess many traditional and machine learning methods along with their application in WHA identification and categorization.

2. Literature Survey

Asma Hassan Alshehri [2024] Improved a wormhole attacks detection focuses on detecting and analyzing the connectivity details of network nodes. Machine learning (ML) techniques are proposed as effective solutions to address these modern challenges in wormhole attack detection within sensor networks. The proposed method is to classify traffic data and identify malicious nodes in the network. **Manar Almalki et.al [2025]** Proposed a Machine Learning-Based Detection of Wormhole Attacks in IoT Networks Using Classification Models are striking a balance between detection accuracy and computational efficiency when selecting models for dynamic Internet of Things (IoT) networks. **Masoud Abdana et.al [2020]** A wormhole attack is to detect wormhole attacks using machine learning, a training dataset is required to train models in any training mode. Training datasets can be obtained from real-time conditions or tests for classification. The classification is performed with several methods of machine learning consisting of K-Nearest Neighbor (KNN), Support Vector Machine (SVM), Decision Tree (DT), Linear Discrimination Analysis (LDA), Naive Bayes (NB), and Convolutional neural network (CNN). To conclude, the results show that the accuracy of KNN, SVM, DT, LDA, NB, and CNN methods is 97.1%, 98.2%, 98.9%, 95.2%, 94.7%, and 96.4%, respectively. Based on results, the sensitivity of the DT method outperforms other approaches. **Mohammad Masoud et.al [2019]** the extracted information may be used to compromise the security and the privacy of humans in the era of Internet of Everything (IoE). In this research work is attempt to review the process of inferring meaningful data from smart devices' sensors, especially, smartphones. Moreover,

different side channel attacks utilizing the same sensors and the same machine learning algorithms are overviewed. **Liu, Z. Li et.al [2017]** in this survey paper can be divided into two parts: ICMANET and the content routing. For the former, we firstly demonstrated the current advances in ICN and subsequently analyzed its development trends. **F.A.Khan et.al[2017]**propose a Detection and Prevention System (DPS) to detect and block malicious nodes in MANETs. When a DPS node finds a node with a suspicious behavior, it declares that suspicious node as a wormhole node by broadcasting a message. NS-2 simulations show that the proposed DPS considerably reduces the number of packets dropped by the malicious nodes with very low false positive rate. **Parvathy.K [2021]** in this survey focuses on wormhole attacks in wireless sensor network (WSN) and Internet of Things (IoT) creating a tunnels i.e., wormhole link in between source and the destination node in the network. The classification of wormhole attack in both WSN and IoT are presented based on the mode of attacker. The detection mechanisms of wormhole attack are specified in both WSN and IoT. **AbrarM. et.al [2022]** a new multi-step detection (MSD) scheme is introduced that can effectively detect the wormhole attacks for WSN. The MSD consists of three algorithms to detect and prevent the simplex and duplex wormhole attacks. Furthermore, the proposed scheme integrated five detection modules to systematically detect, recover, and isolate wormhole attacks. finally, the proposed MSD has lower false detection and false toleration rates. **F.Qamar el.al[2017]** Coordinated Multi-Point (CoMP) operation system provides a valid solution to enhanced throughput and coverage performance by reducing the interference, especially for cell-edge users. In CoMP operation, multiple Base Stations (BS) coordinate with each other in such a way that the user's information signal from neighboring evolved Node B (eNB) reduces interference or even can be combined to improve received signal quality. **R.H.Jhaveriand et.al[2017]** propose a trust-based scheme founded on nodes' historical behaviors which adopts a pattern discovery mechanism in order to detect suspicious activities from the malevolent nodes before they start dropping data packets. We also present the detailed mode of operations of three distinct adversary models launching various kinds of packet forwarding misbehavior.

3. Spontaneous Attacks on Wireless Sensor Networks

Wireless Sensor networks must to be capable of managing any issues that emerge following the use of network reconfiguration strategies, such as node malfunctions and topological alterations. To maintain continuous network transmission in the event that a node leaves the network and breaks links, the affected nodes can immediately request new routing paths. Although there may be delays and traffic jams due to broken links and node complaints about new routing updates, the network is nevertheless functional. The performance of Wireless Sensor networks may be impacted by several attacks in addition to the problems mentioned above. Several factors make Wireless Sensor networks vulnerable to network assaults:

1. The lack of a centralized authority capable of approving the nodes
2. Multiple-hop networking
3. A changeable topology that is always changing
4. The consumption of little energy and
5. The absence of secure routing protocols because the nodes' processing capacity is so low.

3.1. Attack Classification

Figure 2 illustrates how attacks on ad hoc networks can be roughly classified into two categories: active attacks and passive attacks. Active attacks aim to destroy the content of messages delivered across the network, whereas passive attacks exploit the data for malicious purposes without disrupting the regular operations of the network. The following section goes into great detail about both sorts of attacks.

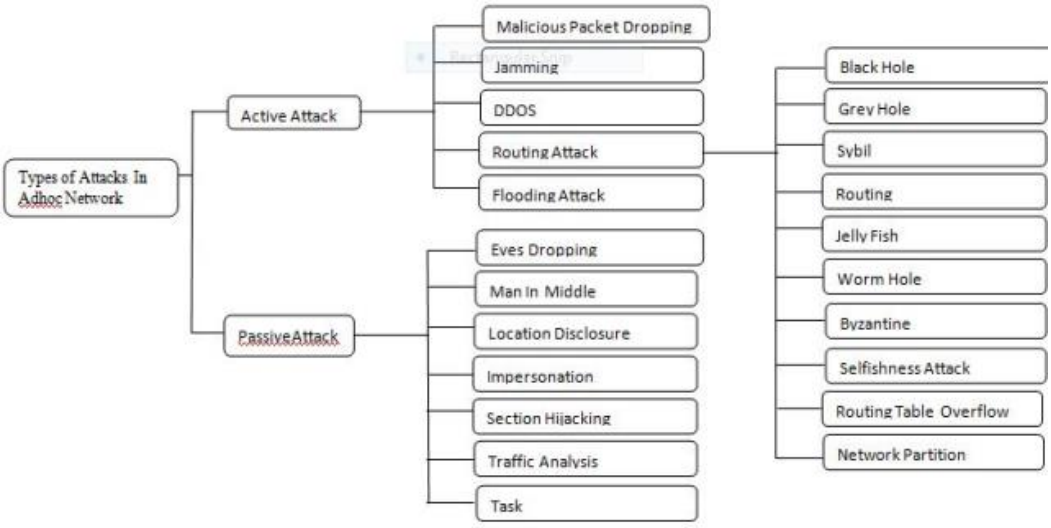

Figure 2: Types of attacks on Wireless Sensor Network

3.1.1. Active Attack

Major attacks on a network that stop data from being transmitted between nodes are called active attacks. When conducting active attacks, the prowler causes malfunctions by altering, mixing, forging, fabricating, and discarding data packets, which prevents the network from operating normally. It can cause the entire network to fail or reduce the network's overall performance. Active attacks are started by selfish nodes, which can then be dealt with as malicious nodes. While unselfish nodes avoid sending the packet to other nodes for the sake of their own interests, especially for energy conservation, malicious nodes drop or change packets to impede network performance. Additional categories for active attacks include malevolent packet dropping, system jamming, disruption of service (DoS), routing attacks and flooding assaults. Routing attacks are the primary types of attacks that have the ability to compromise a network by intercepting routing information. A few examples of routing assaults are selfishness attack, byzantine attack, black hole attack, grey-hole attack, Sybil attack, rushing attack, jellyfish attack, wormhole attack, routing table overflow attack, and network partition attack. These attacks interfere with the normal operation of routing protocols by inserting fake information, altering data packets, and deleting control header resource over the protocol's routing data discovery phase. Malicious nodes that disregard the set of protocols are to blame for these attacks. The correct operation of the routing mechanism is disrupted by several assaults, such as the jellyfish, jelly-hole, and rushing attacks.

3.1.2. Passive Attack

Passive assaults don't directly affect how networks work. However, the intrusive party observes the data that is flowing through the internet without changing anything. In the passive assault scenario depicted in Figure 3, node 3 observes data as it travels from source to destination via the network.

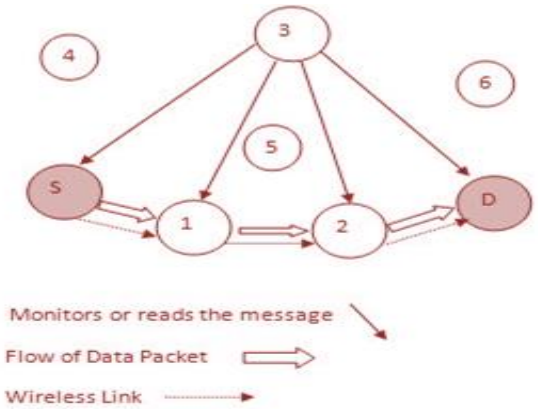

Figure 3: Wireless Sensor network- Passive Attack

Passive assaults are hard to spot since they don't impede the network's ability to operate normally. Malicious nodes are the source of the passive assaults. The frequency of passive assaults can be reduced with the use of strong encryption algorithms, albeit at the expense of additional overhead. The phrase "passive attacks" encompasses a wide range of attacks, such as traffic analysis, impersonation, location disclosure, eavesdropping, and man-in-the-middle attacks.

3.1.3. Limitations on Bandwidth and Power

The amount of accessible bandwidth in Wireless Sensor networks is a difficulty because of shared and open wireless links. In wireless networks, the effects of interference, sound, and attenuation of signals are more likely to occur. Multiple connections cause bandwidth problems in Wireless Sensor networks since a node's bandwidth is shared by several connections. How many connections are generated in the AODV routing protocol was described. To solve the bandwidth problem, the AODV routing protocol determines the bandwidth of intermediary stations at the route-finding stage. A new way must be found when the intermediary nodes are not powerful enough to manage every connection, particularly new ones. Only then can the path be built.

Ad hoc networks are composed of hundreds of thousands of nodes that use the power at each node to gather data and send it to the appropriate node. The low battery capacity of ad hoc network nodes might lead to severe power limits. Due to power limitations, some nodes frequently dropped other nodes' packets, which boosted the number of malicious activities. Thus, in order to stop packets from readily dropping at the affected nodes, it is imperative to conserve node power. Numerous scientists and researchers have proposed numerous power control algorithms for the same purpose, that utilize node level, geographical data, the theory of graphs, and the theory of games. Both local and global strategies were proposed to save electricity in ad hoc networks. The network nodes reduce the amount of energy used during transmission by employing a local strategy. The MAC and physical layers of the network are impacted by local laws. To maximize the network lifetime, some nodes in the global strategy are placed in a resting state while the others are in an active state of operation. Introduced the Intelligent routing AODV methodology to lower

the energy consumption of ad hoc networks by predicting the distance between nodes. The distance was ascertained using a technique known as received signal strength (RSS) indicator. In the case of acknowledgement, a node from that region was selected for transmission, while nodes that were not in the identical region had been disabled for transmission.

4. Proposed Method of ENS-WHA IoT Enabled Wireless Sensor Network

Algorithm of Wormhole Attack in Wireless Sensors using IoT

Step 1: INPUT

Sensor Network N = {S1, S2, ..., Sn}

Malicious Nodes M = {Ma, Mb}

Routing Protocol P using AODV

Routing Table R

Communication Range R 100 * 100 meter

Threshold Values T = {RTT_max, RSSI_min, Hop_max}

Step 2: Deploy Ma (Primary Attack) at Strategic Location L1

Deploy Mb (Secondary) at Strategic Location L2

Step 3: Establish Out-of-Band Tunnel T

Step 4: Real-time Monitoring, Detection and Response Action

Steps 5: Route Discovery and Packet Processing

Steps 6: Route Request and Replay Manipulation

Step 9: Attack Objective Application

Step 10: Packet Tunneling and Packet Forwarding

Step 11: Tunnel Connectivity Maintenance

Step 12: Network Topology Adaptation

Step 13: Detection Evasion

The Enhanced Network Security using Wormhole Attack (ENS-WHA) Wormhole Attack Algorithm for IoT Sensor Networks is a systematic approach that demonstrates how attackers can exploit routing protocols in wireless sensor networks to create malicious tunnels between distant network locations. This algorithm illustrates the complete attack lifecycle from initial deployment to persistent network compromise.

The wormhole attack targeting IoT sensor networks represents a sophisticated security threat that exploits fundamental vulnerabilities in wireless sensor network architectures. The target sensor network consists of numerous individual sensor nodes (N = {S1, S2, ..., Sn}) characterized by limited processing power, memory, and battery life, typically deployed in clusters or mesh configurations for environmental monitoring purposes.

The attack infrastructure involves two strategically positioned malicious nodes: **Ma** serves as the primary attack node positioned within the sensor network, while **Mb** functions as the secondary attack node positioned near critical network infrastructure such as gateways or base stations. These malicious nodes possess significantly superior capabilities compared to legitimate sensors, including higher computational power, extended communication range, unlimited power supply and advanced communication equipment. The attack exploits AODV routing protocols, which typically assume trusted nodes and lack robust authentication mechanisms, making their route discovery processes vulnerable to manipulation.

In our Proposed ENS-WHO technique communication range of typical IoT sensors spans 10-100 meters, but the wormhole attack bypasses these range limitations through the establishment of a high-speed out-of-band tunnel between the malicious nodes. This tunnel creates the illusion of a direct connection between distant network locations, allowing attackers to manipulate routing decisions and intercept network traffic. The attack execution begins with comprehensive network reconnaissance where **Ma** is strategically deployed at location **L1** to maximize attack effectiveness. Simultaneously, **Mb** is deployed at strategic location **L2** to complete the wormhole tunnel infrastructure. This positioning emphasizes proximity to base stations, gateways, or network exits where intercepted data would naturally flow, while maintaining sufficient distance from **Ma** to create an effective tunnel spanning multiple legitimate network hops.

The establishment of the out-of-band tunnel **T** creates a high-speed communication channel between **Ma** and **Mb** using various communication media including WiFi, 4G/5G, Ethernet, or dedicated radio links. This tunnel provides significant advantages over the legitimate sensor network, offering bandwidth of 10-100 Mbps compared to the sensor network's typical 250 Kbps capacity, latency under 1ms versus multi-hop delays of 50-200ms, reliability exceeding 99% uptime. The tunnel characteristics enable the attackers to create false shortest path impressions while maintaining stealth operation.

Algorithm of Real-time Monitoring, Detection and Response Action

```
WHILE (network operational) DO
        FOR each active route R DO
            MEASURE round-trip time RTT(R)
            ANALYZE received signal strength RSSI(R)
            COUNT hop distance HD(R)
            CALCULATE packet delivery ratio PDR(R)
        IF (RTT(R) < RTT_threshold) THEN
            FLAG as suspicious_RTT
        END IF
        IF (RSSI(R) inconsistent with distance) THEN
            FLAG as suspicious_RSSI
        END IF
        IF (HD(R) < expected minimum) THEN
            FLAG as suspicious topology
        END IF
        IF (multiple flags for route R) THEN
            ADD R to Suspicious Links SL
            TRIGGER detailed analysis
            CROSS-REFERENCE with neighbor reports
            VALIDATE using multi-path verification
        END IF
        END FOR
Response Action
    IF (wormhole confirmed) THEN
        ISOLATE malicious nodes
        UPDATE routing tables
        BROADCAST security alert
        INITIATE recovery procedures
    END IF
END WHILE
```

Network traffic monitoring forms a crucial component of the attack strategy, enabling attackers to understand network behavior and identify attack opportunities. The monitoring activities include routing pattern analysis to observe packet flow through the network, protocol identification to determine which

routing protocols are in use, traffic characterization to analyze data types, frequency, and destinations, and topology mapping to create detailed network maps showing sensor locations and connections. The route discovery manipulation phase represents the core attack mechanism, involving continuous monitoring of network activity through an algorithm that runs perpetually while the network remains active.

Algorithm of Route Request, Replay and Packet processing

```
WHILE (network is active) DO
 IF (RREQ received at Ma) THEN
    RECORD packet details (source, destination, sequence)
    TUNNEL RREQ to Mb via T with minimal delay
     BROADCAST RREQ from Mb location
     CREATE false shortest path impression
  END IF
  IF (RREP received at Mb) THEN
     TUNNEL RREP to Ma via T
     FORWARD RREP to create false route
 END IF
END WHILE
   WHILE (data packets flowing through wormhole) DO
   FOR each packet P DO
    INTERCEPT packet at Ma
     ANALYZE packet content
     APPLY attack objective:
        CASE eavesdropping: COPY data, FORWARD packet
        CASE modification: ALTER payload, FORWARD packet
        CASE disruption: SELECTIVELY drop packets
        CASE denial: DROP all packets
     TUNNEL processed packet to Mb
     FORWARD from Mb to maintain route
   END FOR
END WHILE
```

The manipulation process targets Route Request (RREQ) packets by monitoring for these packets arriving at Ma, identifying them based on protocol headers, analyzing source nodes and their requirements, and evaluating target destinations for attack value. When RREQ packets are detected, the system records critical information including the source node, destination node, sequence number, hop count, and route

requirements, creating a comprehensive data structure that captures the original routing request details. The RREQ is then instantly transmitted to Mb via the high-speed tunnel, providing a significant speed advantage over legitimate multi-hop forwarding and ensuring arrival before legitimate route discovery can complete. Mb rebroadcasts the RREQ from its strategic location near the destination with manipulated hop counts that make the wormhole path appear optimal, causing legitimate nodes to update their routing tables with false information.

The process completes with Route Reply (RREP) manipulation, where Mb monitors for route reply packets, correlates them with previously intercepted RREQs, and tunnels them back to Ma via the bidirectional high-speed channel. Ma then forwards the RREP to complete the false route establishment, ensuring all intermediate nodes update their routing tables and activating the wormhole as the preferred route for data transmission. This manipulation results in network convergence on the malicious path due to its apparent optimality in terms of hop count and delay.

Traffic interception and manipulation begin once the wormhole is established, with continuous data flow monitoring enabling systematic processing of intercepted packets. The system performs deep packet inspection to analyze packet headers and payloads, implements protocol parsing to extract information based on network protocols, and conducts metadata extraction to collect routing information and timestamps. Content analysis categorizes intercepted data by type, including sensor readings, control commands, network management messages, security communications, and application data, with sensitivity assessment determining data importance and confidentiality levels.

Detection evasion employs sophisticated techniques including behavior randomization to avoid creating detectable patterns, traffic mimicry to make malicious communications appear legitimate, signature avoidance to prevent security systems from identifying attack characteristics, and countermeasure intelligence to monitor for and respond to security measures. The evasion strategy involves randomizing attack timing, limiting attack frequency, mimicking legitimate traffic patterns, avoiding consistent behavioral signatures, and continuously monitoring for security responses to maintain stealth operation while maximizing attack effectiveness against the compromised IoT sensor network infrastructure.

5. Wireless Sensor Network Performance Statistics

The performance of an ad hoc network can be assessed using efficient throughput, transmission of packets ratio, capability, and delay from end to end. When constructing the routing protocol, many considerations must be made, such as scalability, energy-efficient, privacy, and QoS support. Worm hole detection techniques are generally evaluated based on a number of variables, such as discovery rate, total efficient throughput, total delay from end to end, transmission of packets rate, and loss of packets rate. The following description can be applied to these parameters.

5.1. The Data Packet Distribution Ratio, or PDR

The protocol's ability to transport data packets to the target node even when there are hostile nodes in the network is known as PDR. PDR is determined by splitting the entire number of packages collected at the end point through the complete number of packages broadcast by the source, as per equations (1) and (2).

$$PDR=\frac{\sum \text{packet obtain at the receiver edge}}{\sum \text{packet sent by the sender edge}}\times 100\% \quad (1)$$

$$\text{Therefore PDR}=\frac{\sum_{k=1}^{n} Xk}{\sum_{k=1}^{n} Yk}\times 100\% \quad (2)$$

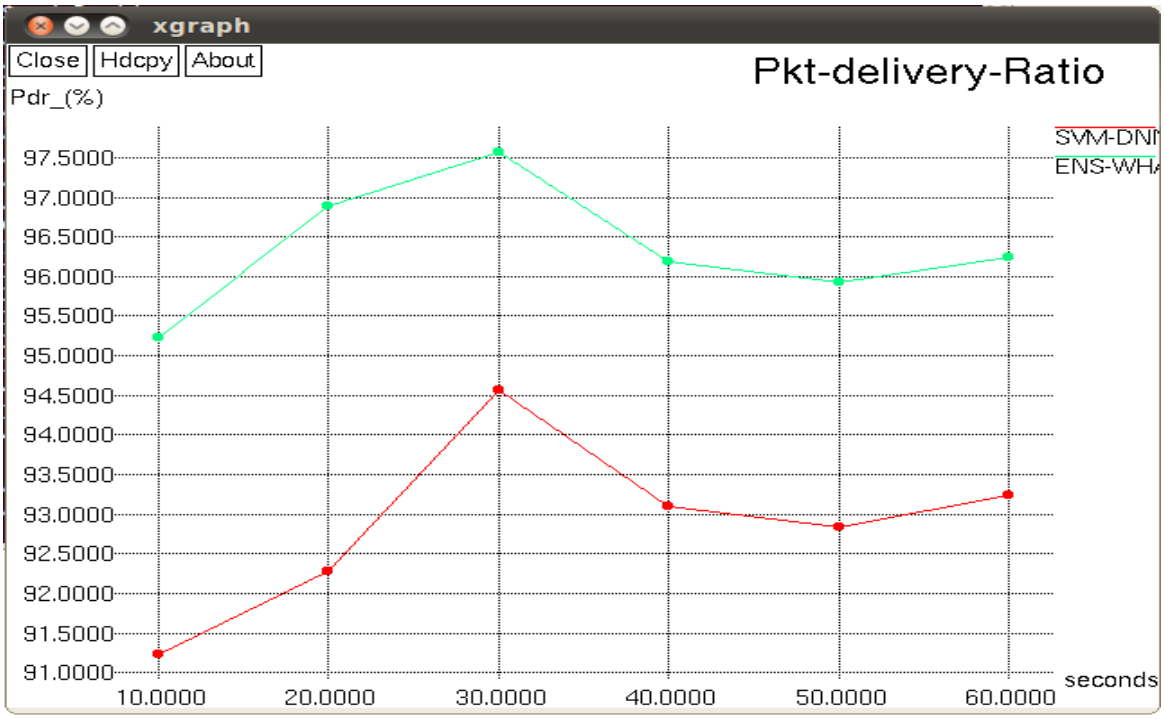

Figure 5.1 Packet Delivery Ratio

5.2. Average Duration to Finish (End-End Delay)

The average total delay, or AEED, is the average duration of time that passes between sent and received packets. The overall amount of time lost as a result of route discovery, data accusation, propagation time, and data processing at intermediate nodes is known as AEED in equation (6).

$$AEED=\frac{\sum_{1}^{N}(T\_received-T\_sent)}{N} \quad (3)$$

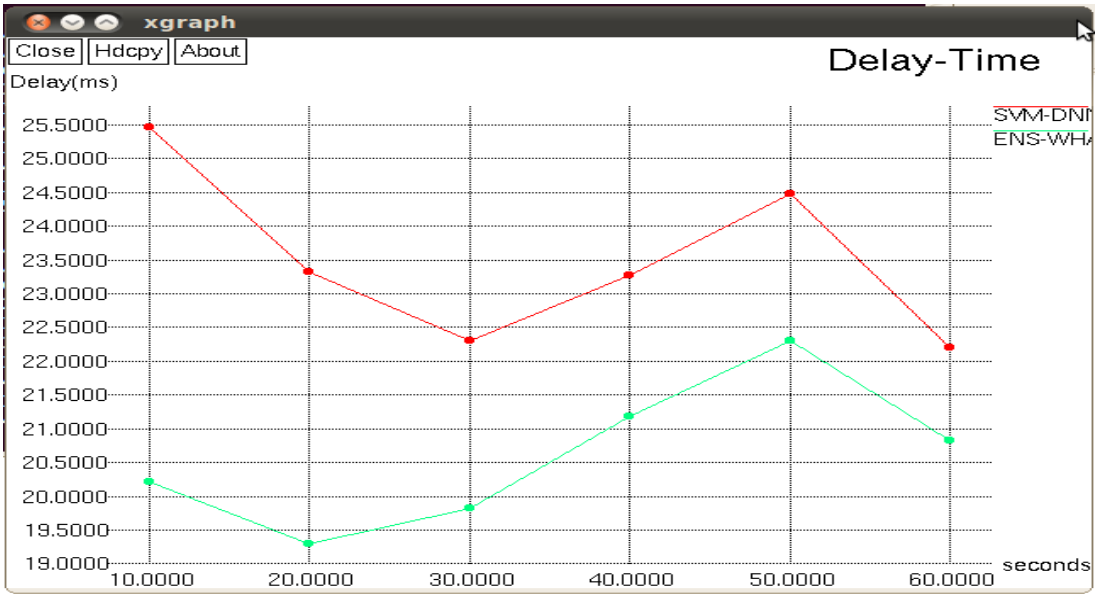

Figure 5.2 Delay time

5.3. Average Throughput

Average throughput is characterized as the proportion of the total size of packets collected at the desired location to the time period between the start and stop times of the simulated network in equation (5).

$$\text{Average\_Through-put} = \frac{PS}{T\_Start - T\_stop} \quad (4)$$

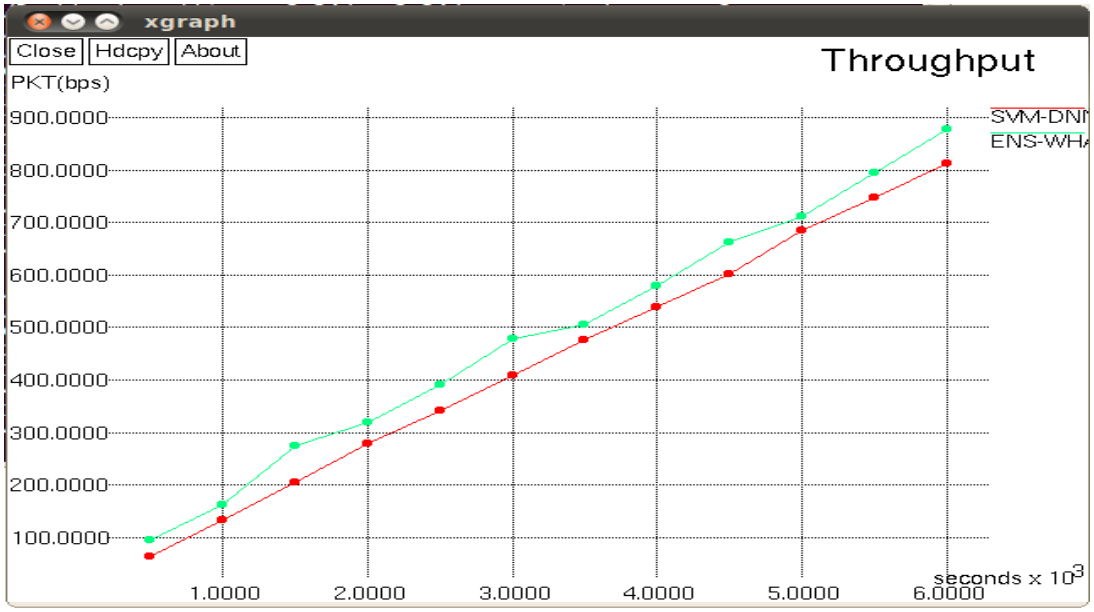

Figure 5.4 Throughput

5.4. Energy Consumption

Energy consumption is the quantity of energy needed for various network functions. A joule Measures how much energy is used by the proposed model, SVM and DNN. The proposed model is more secure and energy-efficient than the formerly supplied SVM and DNN, as shown by the actual effects of nodes' energy usage.

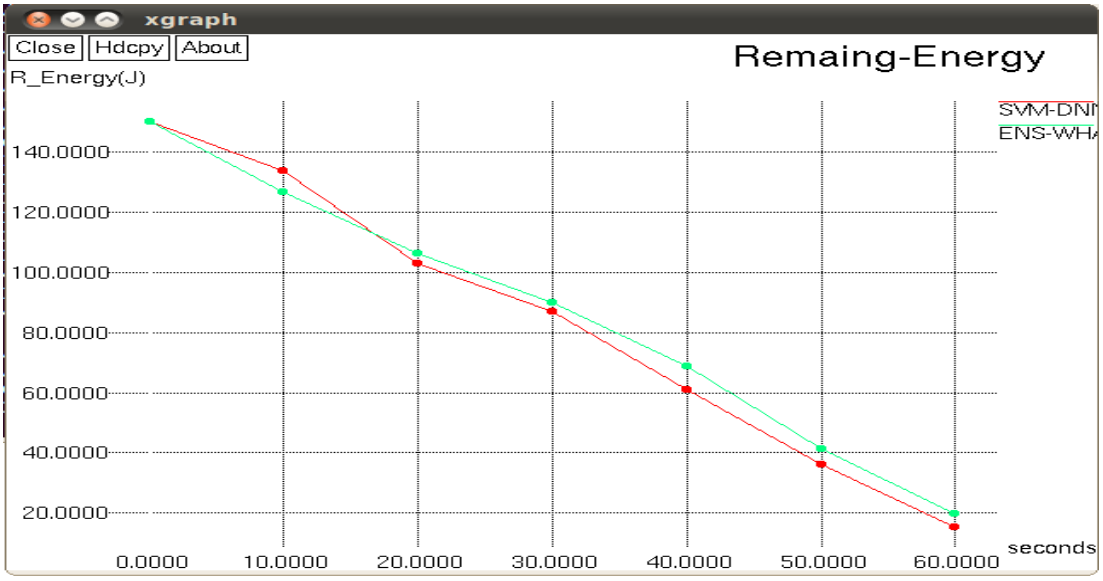

Figure 5.4: Energy Consumption

5.5. Rate of Detection

Detection rate (DR) is the probability that wormhole nodes will be accurately detected by the intrusion detection system. The ratio of actual mal-behaving nodes to the identified problematic nodes is what defines the Detection rate (DR) in equation (5).

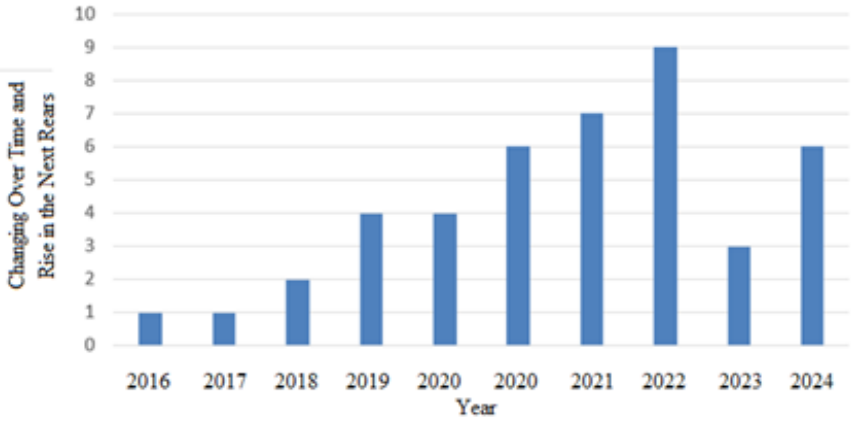

Figure 5.5: IoT with WSN using Wormhole Attack Detection

$$\text{Detection Rate} = \frac{\text{No of NDMNs found to be misbehaving}}{\textit{Actual misbehaving nodes in total } (NTMN)} \quad (5)$$

The classification stage is considered to be the core of WSN anomaly detection, to sum up. Various WSN have been used as classifiers for WHA detection in our review. Figure 4 displays the growth rate of Internet of Things wireless sensor network Technique for WHA identification articles from 2016 to 2024. The graph shows that the number of publications is progressively changing over time and may rise in the next years, even if anomaly detection is not an advanced area of study. The graph demonstrates how IoT approaches have been used extensively for anomaly detection. According to a literature assessment, the year 2020 contains the most WHA detection papers. Figure 5 shows the number of articles from 2016 to 2024 that used a certain IoT with WSN techniques.

6. Conclusion

The Wormhole Attack Algorithm for IoT Sensor Networks represents a sophisticated multi-phase attack strategy that exploits fundamental vulnerabilities in wireless sensor network routing protocols. The algorithm's systematic approach demonstrates how attackers can achieve persistent network compromise through careful planning, strategic positioning, and adaptive behavior. Understanding this algorithm is crucial for developing effective countermeasures and implementing robust security mechanisms in IoT sensor networks. The detailed explanation provided here serves as a foundation for both attack analysis and defense strategy development in wireless sensor network security research.

References

Asma Hassan Alshehri “Wormhole attack detection and mitigation model for Internet of Things and WSN using machine learning” pp(1-24),*PeerJ Computer Science-2024,* http://doi.org/10.7717/peerj-cs.2257.

Manar Almalki, Samah Alajmani “Machine Learning-Based Detection of Wormhole Attacks in IoT Networks Using Classification Models” International Journal of Recent Technology and Engineering (IJRTE), Vol.14(1),pp(31-40),2025.

Masoud Abdana and Seyed Amin Hosseini Seno “Machine Learning Methods for Intrusive Detection of Wormhole Attack in Mobile Ad-Hoc Network (MANET)” pp(1-22),Research Square-2020, https:// doi.org/10.21203/rs.3.rs-544233/v1.

M. Masoud, Y. Jaradat, A. Manasrah, and I. Jannoud,“Sensors of smart devices in the internet of everything (IoE) era:big opportunities and massive doubts,” J.Sens.,vol.2019.

Liu, Z. Li, P. Yang, and Y. Dong, “Information-centric mobile ad hoc networks and content routing: Asurvey,”AdHocNetw.,vol.58,pp.255–268,2017.

H.Kim,M.Bae,W.Lee,andH.Kim,“ Adaptive decision of wireless access network for higher user satisfaction,”Wirel.Commun.Mob.Comput.,vol.2018,p.19,2018.

F.A.Khan,M.Imran,H.Abbas,andM.H.Durad,“A detection and prevention system against collaborative attacks in mobile ad hoc networks,”FutureGener.ComputerSyst.,vol.68,pp. 416–427, 2017.

Parvathy.K "Wormhole Attacks in Wireless Sensor Networks (Wsn) & Internet of Things (IoT): A Review" International Journal of Recent Technology and Engineering (IJRTE), Vol.10 (1), pp(199-203),2021.

AbrarM. Alajlan "Multi-Step Detection of Simplex and Duplex Wormhole Attacks over Wireless Sensor Networks" Computers,Materials & Continua, vol.70(3),pp(4241- 4258),2022.

F.Qamar,K.B.Dimyati,M.N.Hindia,K.A.Noordin, M. B. Mazid, and A. M. Al-Samman, "A comprehensive review on coordinated multi-point operation for LTE-A Computer,"Network,vol.123,pp.19–37,2017.

R.H.Jhaveriand N.M.Patel," Attack-pattern discovery based enhanced trust model for secure routing in mobile Wireless Sensornetworks,"Int.J.Commun.Syst.,vol.30,no.7.p.e3148,2017.

M.WangandZ. Yan, "AsurveyonsecurityinD2Dcommunications," Mob.Netw.Appl.,vol.22,no.2. pp.195–2008,2017.

M.S.Pathan,N.Zhu,J.He,Z.A.Zardari,M.Q.Memon,and M.I.Hussain, "An efficient trust-based scheme for secure and quality of service routing in MANETs,"FutureInternet,vol.10,no.2.p.16,2018.