International Journal of Engineering, Science & Mathematics
Vol. 13 Issue 04, April 2024,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

"Securing Wireless Sensor Networks against Sybil, Black Hole, and DDoS Attacks: A Multifaceted Approach with AODV Protocol Enhancement"

Avininder Singh, Assistant Professor, DCSE, CDLU Sirsa
Sunil, Research Scholar, Part Time M.tech, DCSE, CDLU Sirsa

Abstract-Wireless Sensor Network (WSN) security is a critical area of research and development aimed at protecting these networks from various threats and vulnerabilities. WSNs are susceptible to attacks due to their inherent characteristics such as limited resources, distributed nature, and wireless communication. Common security concerns in WSNs include attacks like Sybil, where nodes illegitimately claim multiple identities to disrupt network operations; Black Hole, where malicious nodes drop or manipulate data packets; and Distributed Denial of Service (DDoS), where attackers overwhelm the network with excessive traffic, causing disruption. To address these threats, multifaceted security measures are employed, including cryptographic techniques for authentication and data integrity, intrusion detection systems for detecting malicious activities, secure routing protocols for ensuring reliable data transmission, and physical layer security mechanisms to protect against eavesdropping and tampering.The proposed multifaceted approach to securing Wireless Sensor Networks (WSNs) against threats like Sybil, Black Hole, and Distributed Denial of Service (DDoS) attacks involves integrating various security measures tailored to detect and mitigate each type of attack effectively. This includes the derivation of a novel algorithm implemented within the AODV routing protocol to detect and prevent Sybil, DDoS, and Black Hole attacks. The algorithm utilizes a lookup table containing information about route replies to prevent frequent attacks. Each source node maintains a sequence of all route replies, and the priority of requests is estimated based on sequence numbers. The performance of the proposed system is then analyzed in terms of packet collision, packet drop, and throughput to evaluate its effectiveness in mitigating attacks and ensuring reliable communication within the WSN.

Keywords- WSN), Security, Sybil attack, Black Hole attack, Distributed (DDoS) attack, AODV protocol

I INTRODUCTION

Over the course of the past few decades, wireless sensor networks (WSNs) have developed as a result of the availability of sensors that are straightforward to deploy, have a short range, and are inexpensive. Wireless sensor networks (WSN) are primarily concerned with sensing and transferring the real-time sense information of a particular monitoring environment to the back-end system so that it may perform additional processing and analysis. However, as a result of the widespread dissemination of wireless communication channels, concerns regarding the privacy and security of wireless sensor network (WSN) systems have emerged as a matter of intense debate. The objective of this Special Issue is to solicit research articles that are considered to be state-of-the-art and pertain to advanced technologies for wireless sensor network (WSN) systems. These articles will cover all types of research activities, including the design, development, difficulties, and application of service models.[1–3]

The protection of the privacy and security of the wireless sensor network (WSN) will be one of the most essential and crucial concerns in the realm of wireless communication channels. For the purpose of preventing communication data from being eavesdropped on, manipulated, or falsified by unauthorized nodes, it is generally accepted that encryption/decryption and a digital signature mechanism should be utilized in order to address concern regarding privacy. There is also the matter of authenticity, which is an essential concern. Authentication procedures are typically utilized in order to accomplish this objective. This is done with the intention of preventing illegitimate nodes from making use of the resources. All of the protective methods that we have created, however, have the goal of extending the amount of time that the sensor network may be used. To put it another way, the level of difficulty cannot be too high. This is because the detecting node's battery usually has a limited amount of power. Figure 1 shows an example of a wireless sensor network (WSN). A WSN is a group of wirelessly connected devices that are set up separately and use sensors to keep an eye on what's going on around them. A lot of different things can use wireless sensor networks (WSNs), such as watching the environment, keeping an eye on people, finding targets, protecting the military, finding intrusions, and more. There are, however, some problems with current security measures that make them unsuitable for wireless sensor networks (WSNs). This is the main reason why security in WSNs is growing. This isn't because there aren't any good protection plans out there.[4]: In other words, the nodes of WSNs can only do so much processing and have limited energy. Smart devices called sensor nodes can talk to each other in wireless sensor networks (WSNs), but their main job is to sense, store, and process data. Following several hops, these data are sent to a sink. The sink can choose to use the data itself or send it to other networks. Wireless sensor networks (WSNs) require efficient routing techniques in order to accomplish effective communication [5-6].They discover the right pathways for transferring data and then preserve those routes for subsequent transmissions, which makes it easier for wireless sensor networks (WSNs) to communicate with one another. Different protocols have been established for different wireless sensor networks (WSNs) due to the heterogeneity of the nodes that make up WSNs. These protocols are based on the nature of the nodes and the application. For example, there are protocols that are specially designed for MWSNs and protocols that are specifically designed for SWSNs.[7-8] [7-8]

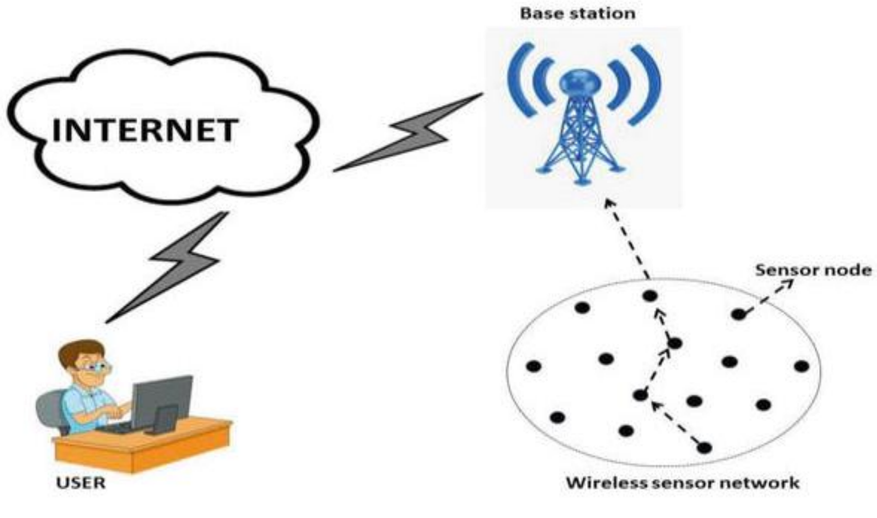


Figure 1. A typical wireless sensor networks (WSN) [1].

In wireless sensor networks (WSN), there are two different ways to send data. In the single hop choice, the source node sends its data packets to the destination in just one hop. Wireless sensor networks (WSNs) are made up of nodes that are sensors. These nodes may need each other to send packets to faraway places. Multi-hop is the name of the communication method in question. Multi-hop is a type of route in which nodes in between source and destination nodes work together to make it easier for data to get from source nodes to destination nodes. It does this by letting nodes that are low on energy send data to the target node through their neighboring nodes along the routing path. This makes wireless sensor networks (WSNs) much more efficient. An increasing number of privacy and security issues are linked to the use of multi-hop routing. There are many issues that can happen with wireless sensor networks (WSNs), and some of them affect the data that is kept there. These include snooping, sinkholes, tampering Sybil, clones, wormholes, spoofing, and more.A number of security options for wireless sensor networks (WSNs) were discussed. However, some of these options are not good for WSNs because sensors don't have enough resources. Because of this, they can't be used in wireless sensor networks (WSNs). The main reason for this is that most wireless sensor networks (WSNs) have an unstable structure. When compared to other networks, some wireless sensor networks (WSNs) are made up of flexible nodes that change the way the networks are set up all the time. Because of this, it is hard for these kinds of mobile networks to use the protocol that was made for fixed nodes.10 and 9 A lot of data is also sent by wireless sensor networks (WSNs), which makes the WSN's wireless communication system busier. Because of these things, it's clear that security and privacy solutions for wireless sensor networks (WSN) need to be both light on computational, communication, and energy costs. They also need to be able to support aggregation and multi-hop to lower the amount of traffic and make the networks last longer. While this is going on, most of the security solutions on the market right now don't meet these efficiency standards. [11]

II LITERATURE SURVEY

Xiangfei Zhu (2022) This study looks into the problem of global adaptive cluster synchronization in dynamic networks that are made up of nonlinear Lur'e systems that are coupled in ways that aren't equal or balanced. There are nonlinear parts that make up the networks. If a pinning feedback controller can do this, it can only handle Lur'e systems that are part of the current cluster and can directly connect to other clusters. Using mathematics analysis tools like the Lyapunov stability theorem, the S-procedure, the emphS-procedure, and others, we can find certain requirements that must be met in order for the cluster synchronization to happen. The adaptive update rules that are given are also used to get the most out of the feedback control benefits. As a final step, one numerical exercise is shown to make sure that the results were correct.([12]

Xiaohui Ren (2022) The goal of creating DATEM, a dynamic trust assessment model based on IOT nodes, was to fix the problems with the current IOT node trust assessment model. Some of these problems are that it is not very useful, it is not very accurate, and it is hard to stop evil node fraud. In the straight trust calculation, the dynamic reward and punishment factor is used. This factor looks at how well and reliably data is sent between nodes that are close to each other, as well as how node energy affects transfer. This factor's job is to speed up the rate at which trust values change when bad things happen and make normal nodes more competitive. It is possible to figure out how trustworthy suggestions are by using the K-means clustering method. This algorithm is used to sort recommendation nodes and keep hostile nodes from giving out false suggestions. To figure out the comprehensive trust degree, the trust value's weight is based on how full the node trust queue is and how evenly the direct trust value is spread out in the queue. In the simulation, the results show that DATEM can respond faster to data threats and find and stop fraud more effectively. [13]

Mohamed Behery (2023) Rapidly changing industrial requirements necessitate the development of robot programming that is both quick and simple, particularly for small and medium-sized businesses (SME), which sometimes lack prior experience in robot programming. Even with the development of graphical activity representation languages like Behaviour Trees (BTs), it is still possible for the process of programming robots to do new behaviors to be time-consuming. This is because the product specifications are constantly changing, and the production settings are constantly changing as well. Using Dynamic Sequence Nodes (DSNs), this work presents an extension of BTs that gives more flexibility as well as higher reactivity and robustness. This is accomplished by integrating Mixed Initiative Planning (MIP) to BTs. Although DSNs minimize the amount of human labor required to build a BT, they also lower the number of nodes that are required to accomplish a certain task. This is accomplished while preserving the tree's robustness, readability, and modularity. In addition to this, it incorporates run-time optimization into BTs, which is in contrast to tree synthesis techniques, which ensure convergence but neglect performance. It is [14]

Oriol Ruiz-Celada (2022) Systems that can manipulate robots in semi-structured and changing environments need to be able to do the following: a) perceive and reason about the environment's state; b) plan and replan at both the symbolic and geometric levels; and c) execute tasks automatically and reliably. The purpose of this paper is to offer a framework that has the following characteristics in order to address these difficulties. To begin, it employs techniques that are based on ontology and perception in order to acquire the Planning Description Domain Language files that explain the manipulation problem at the task level. In the event that it is necessary to adapt to new circumstances, this is utilized both at the planning stage and while the task is being carried out respectively. Furthermore, the framework that has been provided is capable of planning at both the task level and the motion level. This is accomplished by including geometric reasoning modules, which are responsible for determining some of the symbolic predicates that are required to define the states. Last but not least, the framework will automatically construct the behavior trees that are necessary to carry out the specific activity. It is possible to modify the action plan or the trajectories in response to changes in the environment, which is made possible by the proposal, which makes use of the fact that behavior trees can be modified while the program is running. This approach makes it possible for robot manipulation activities to be automatically planned and carried out in a reliable manner, which significantly contributes to the development of fully functional service robots.[15]

III PROPOSED SYSTEM

Securing Wireless Sensor Networks (WSNs) against threats like Sybil, Black Hole, and Distributed Denial of Service (DDoS) attacks requires a multifaceted approach. A proposed method involves integrating several security measures tailored to detect and mitigate each type of attack effectively. For Sybil attack detection, employing cryptographic techniques such as digital signatures and public-key infrastructure can authenticate nodes and ensure that each node possesses a unique identity. Additionally, reputation-based systems can be implemented, where nodes maintain trust scores based on their observed behavior and interactions within the network. Suspicious nodes exhibiting Sybil-like behavior can then be flagged and isolated.

To counter Black Hole attacks, anomaly detection algorithms can monitor network traffic patterns and identify abnormal behavior indicative of packet dropping. Techniques such as Watchdog and Pathrater can be utilized, where nodes monitor their neighbors' activity and rate them based on their reliability in forwarding packets. Any deviation from expected behavior can trigger alarms and initiate corrective actions, such as rerouting traffic through alternative paths.

For DDoS attack detection, intrusion detection systems (IDS) can be deployed to analyze network traffic and identify patterns indicative of an attack. Anomaly-based IDS monitors deviations from normal network behavior, while signature-based IDS detect known attack patterns. Furthermore, rate-limiting mechanisms can be employed at network entry points to filter out excessive incoming traffic and mitigate the impact of DDoS attacks.

Moreover, enhancing the robustness of WSN protocols is essential. Implementing secure routing protocols such as Secure Multipath Routing (SMR) can provide resilience against attacks by establishing multiple paths between nodes and dynamically rerouting traffic to avoid compromised nodes. Encryption techniques can also be utilized to secure data transmission and prevent eavesdropping by malicious entities.

Continuous monitoring and updating of security measures are crucial to adapt to evolving threats. Furthermore, collaboration among researchers, industry stakeholders, and regulatory bodies is essential to develop standardized security solutions and best practices for securing WSNs effectively. By implementing these proposed methods and fostering collaboration, WSNs can be safeguarded against Sybil, Black Hole, and DDoS attacks, ensuring their reliability and security in various applications.

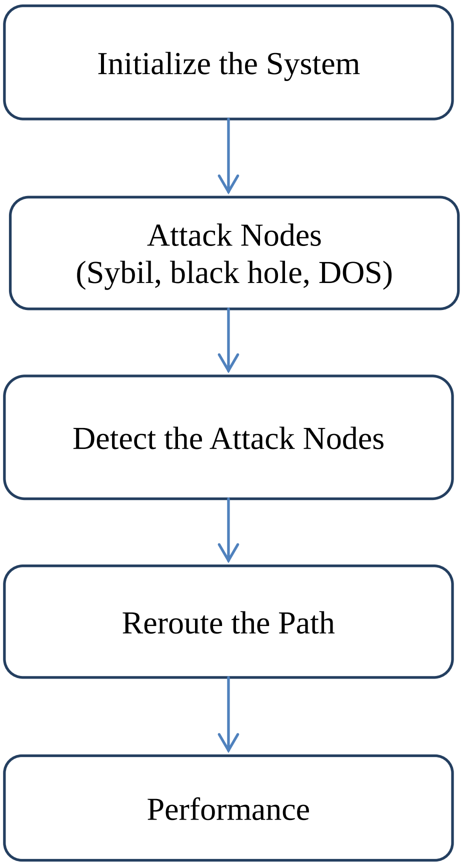


Fig.2 Flow diagram

Table 1 Simulation parameter

Parameter	Value
Number of Nodes	100
Source Node	10

Destination Node	20
Data Rate	8 packets/sec
City Size	100
Block Size	30
Initial Energy	1 Joule
Communication Range	20 units
Breadth	0
Display Node Numbers	Yes

IV SYSTEM DESCRIPTION

System Initialization:

- Initialize network parameters, including node IDs, communication channels, and security keys.
- Deploy nodes in the network area and establish initial connections.

Attack Nodes (Sybil, Black Hole, DDoS):

- Simulate or detect the presence of attack nodes within the network.
- Attack nodes may engage in malicious behavior such as forging identities (Sybil), dropping packets (Black Hole), or flooding the network with excessive traffic (DDoS).

Detect the Attack Nodes:

- Utilize various detection mechanisms to identify attack nodes.
- Techniques such as cryptographic verification, anomaly detection, and reputation-based systems can be employed.

Reroute the Path:

- Upon detecting malicious behavior from attack nodes, reroute network paths to bypass them.
- Utilize secure routing protocols like Secure Multipath Routing (SMR) to establish alternative paths between nodes.

Performance Evaluation:

- Monitor network performance metrics before and after implementing security measures.
- Evaluate factors such as latency, throughput, and reliability to assess the impact of security mechanisms on network operation.

MODULES

The system consists of several modules designed to simulate and analyze various aspects of network behavior and security. The modules included are:

- AODV System
- SYBIL Attacks
- DDoS Attack
- Black Hole Attack

AODV System: This module implements the Ad-hoc On-demand Distance Vector (AODV) routing protocol. AODV is a reactive routing protocol used in wireless ad-hoc networks to establish routes between nodes only when they are needed. It helps in establishing efficient communication paths while adapting to network topology changes.

Sybil Attacks: This module simulates Sybil attacks, a form of security threat where a single malicious node illegitimately claims multiple identities in a network. Sybil attacks can disrupt communication, compromise network integrity, and lead to various security vulnerabilities.

DoS Attack: The Denial-of-Service (DoS) attack module simulates scenarios where the network is flooded with a high volume of traffic, overwhelming its resources and rendering it unable to respond to legitimate requests. DoS attacks aim to disrupt normal network operations and can cause service downtime or degradation.

Black Hole Attack: This module simulates Black Hole attacks, where a malicious node in the network selectively drops or absorbs packets, preventing them from reaching their intended destination. Black Hole attacks can lead to data loss, routing inefficiency, and compromise network performance and security.

V SIMULATION RESULT

simulating a network scenario using MATLAB, where nodes communicate with each other using AODV (Ad hoc On-Demand Distance Vector) routing protocol. The simulation includes the presence of various types of nodes such as normal nodes, Sybil nodes, DOS (Denial of Service) nodes, and Black nodes. The evaluation of the network performance metrics like energy consumption, packet collision, throughput, and packet drop is also conducted.

SYBIL ATTACK

In this simulation, the network comprises 100 source nodes and 20 destination nodes, with a data rate set at 8 packets per second. The city size, representing the network environment, is defined as 100 units. To visualize the network, Equation (1) instructs to set the axis ranging from 0 to the city size plus 1 in both dimensions. The simulation employs blocks with a size of 30 units each. The initial energy of all nodes in the network is set to 1 joule, and the communication range for each node is defined as 20 units.

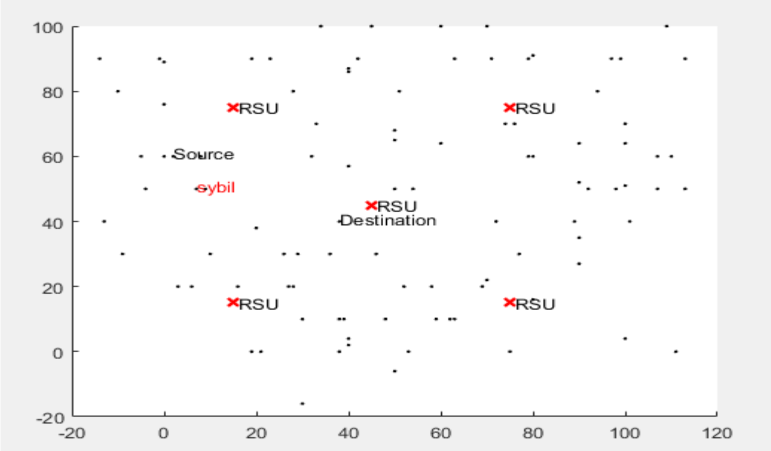


Fig 3 Highway scenario with 100 nodes with 120 km/h speed

An idea that is being thought about checks for sanctuary settings in the form of a REQ or REP message during this packet contract. Furthermore, by showing fake Sybil node traits, it gives users confidence in their ability to spot or avoid a Sybil attack. The steps for finding and stopping Sybil nodes are shown in Figure 43. Ten source nodes are added at a rate of eight packets per second in this example, which has a total of 100 source nodes. There are also twenty target nodes picked, and the city has a size of 100. As you can see in Figure 3, the total distance traveled along each linked path between the source vehicle and the target vehicle is shown.

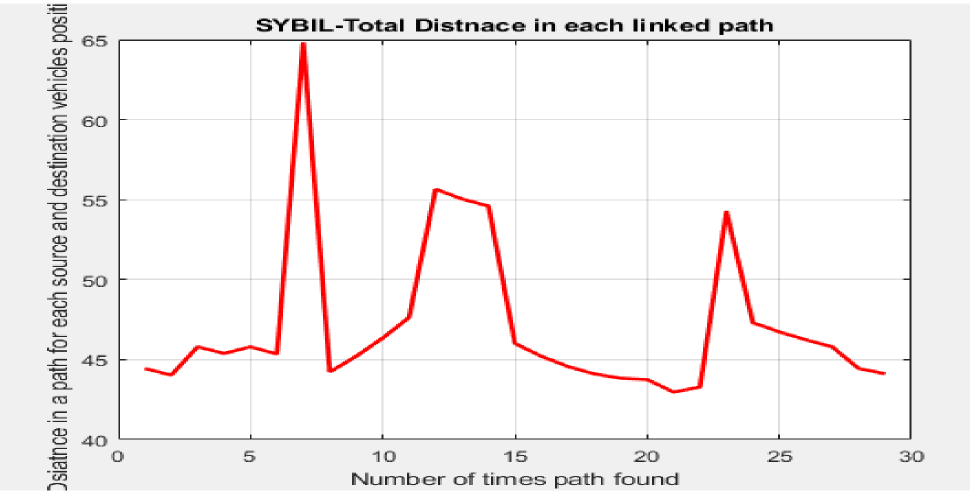


Fig.4.number of link path for Sybil attack

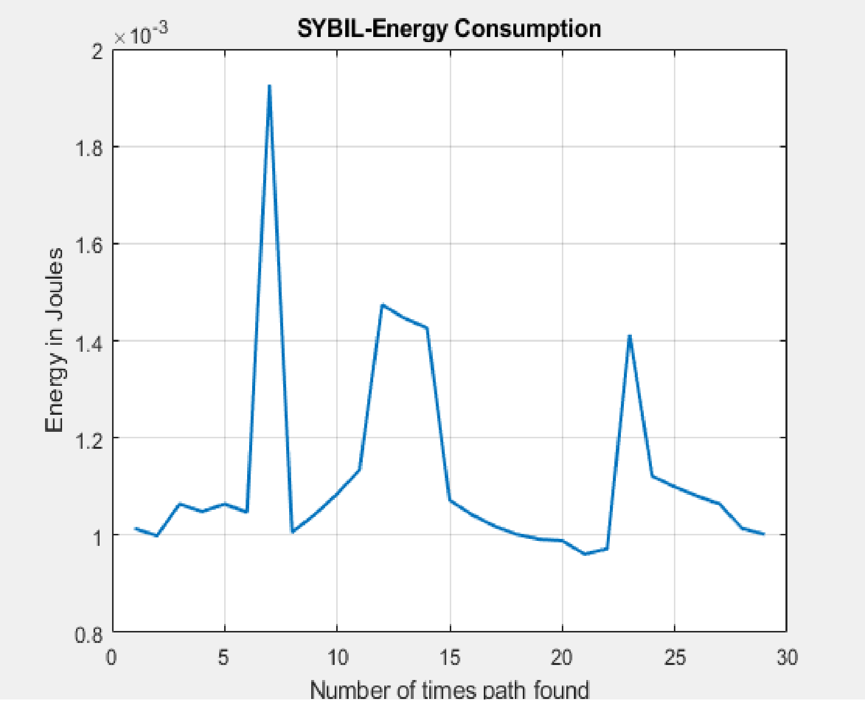


Fig.5 Energy consumption for Sybil attack

This figure illustrates the amount of energy that is consumed by the Sybil attack. The X axis represents the number of times the path was found, and the Y axis represents the amount of energy that was obtained by the node while it was transmitting data.

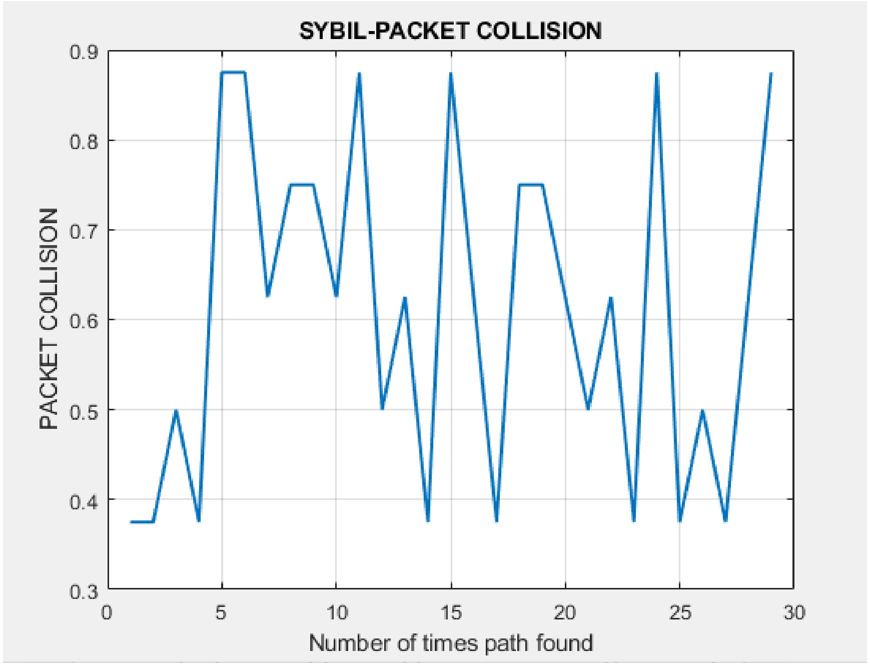


Fig. 6 Packet collision for Sybil attack

Figure 6 illustrates the amount of energy that is consumed by the Sybil attack. The X axis displays the number of times the path was found, and the Y axis displays the number of packet collisions that occurred while the data was being transmitted.

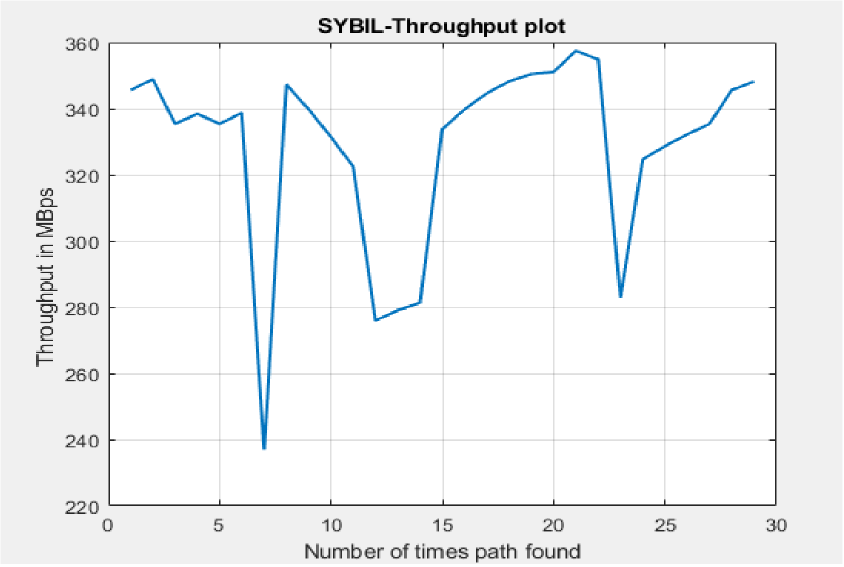
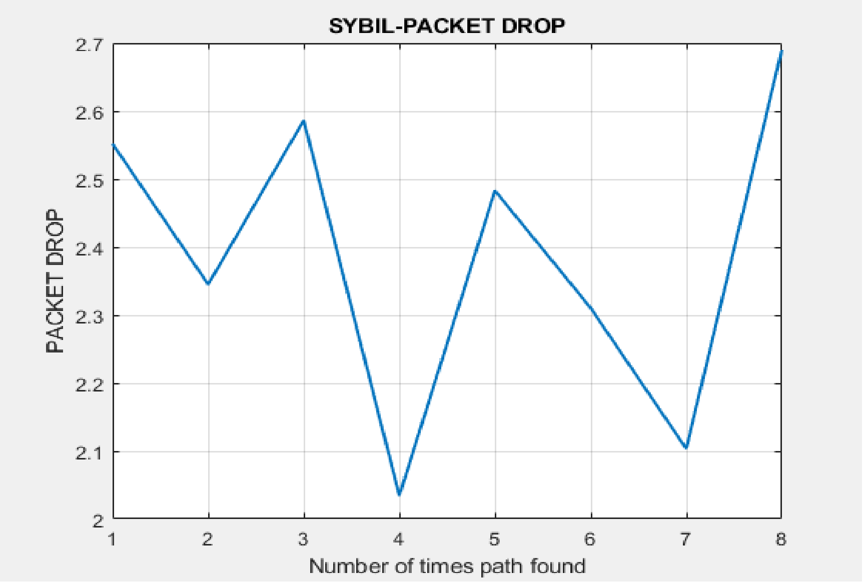


Fig.7 Throughput for Sybil attack

The energy consumption for the Sybil attack is depicted in figure 7, where the X axis represents the number of times the path was found, and the Y axis represents the throughput performance of the node while it was transmitting date



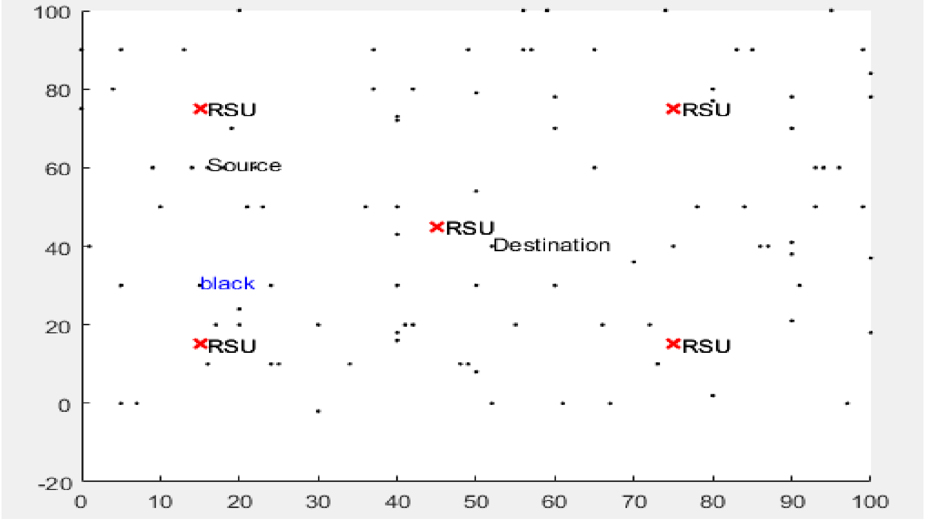
.

Fig. 8 Packet drop for Sybil attack

Figure 8 displays the amount of energy used by the Sybil attack. The X-axis displays the number of times a path was found, and the Y-axis displays the node's packet drop performance during data transfer.

4.3.2 Black Hole Attack

In the simulation focusing on the black hole attack scenario, the network setup is similar to the previous one. It includes 100 source nodes and 20 destination nodes, with a packet acquisition rate of 8 packets per second. The city size remains at 100 units. To visualize thenetwork



,

Fig. 9Highway scenario with 100 nodes with 120 km/h speed

Within the context of this simulation, the number of nodes is 100, and either the source node or the target node is 10. On a peer-to-peer network, applications that are capable of accessing local resources are referred to as devices. In this simulation, there are four hundred source nodes and ten source nodes that are obtained at a rate of eight packets per second. Additionally, twenty destination nodes are chosen, and the size of the city is one hundred.shown in figure 9

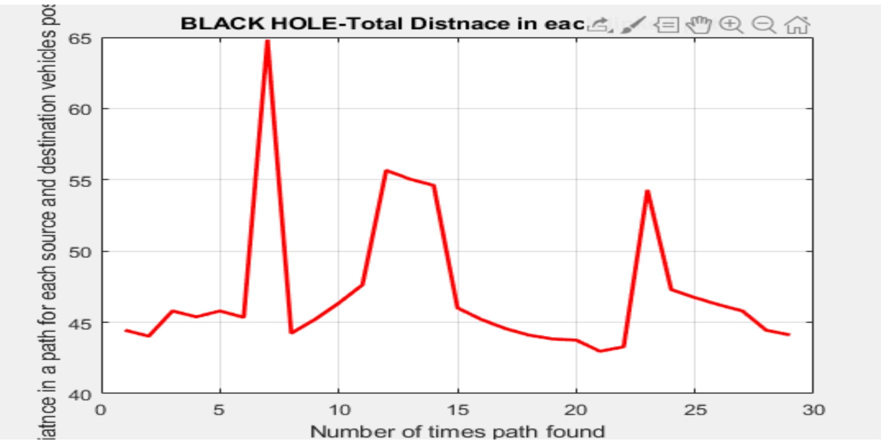


Fig.10 number of link path for black hole attack

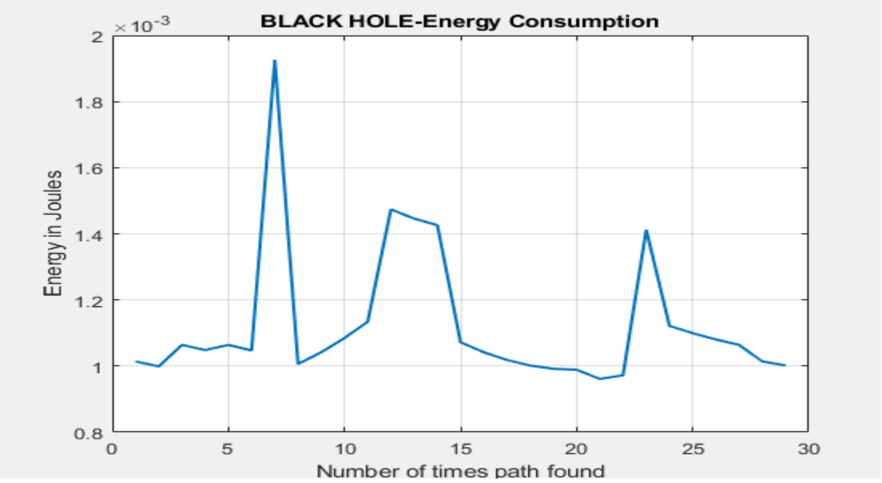


Fig.11 Energy Consumption for Black Hole Attack

In Figure 11, which illustrates the amount of energy that is consumed by a black hole assault, the X axis represents the number of times the path was found, and the Y axis represents the amount of energy that was gained by the node while it was transmitting data.

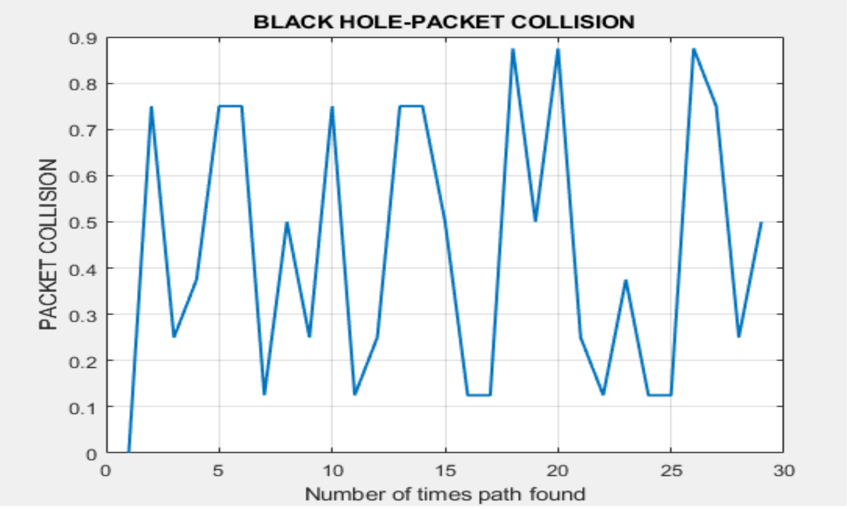


Fig.12 Packet Collision for Black Hole

In Figure 12, which illustrates the amount of energy required for a black hole assault, the X axis displays the number of times the path was found, and the Y axis displays the number of packet collisions that occurred while the data was being transmitted.

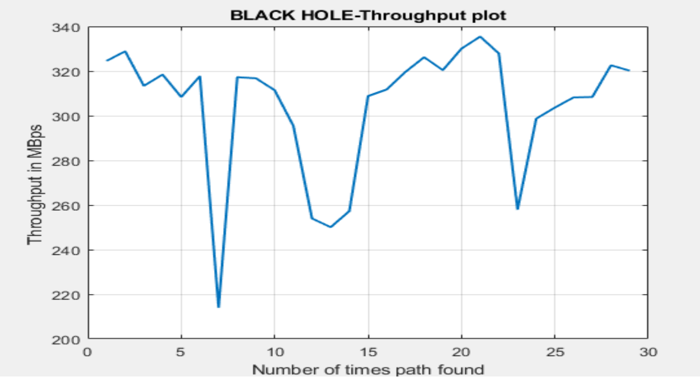


Fig.13 Throughput for Attack for Black Hole

The energy usage for a black hole attack is depicted in figure 13, where the X axis represents the number of times a path was found, and the Y axis represents the throughput performance of the node while it was transmitting data.

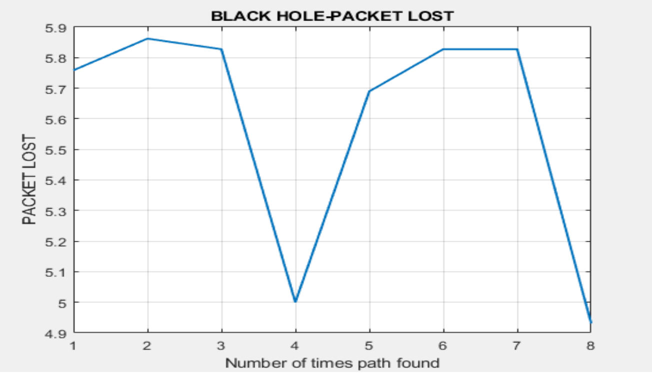


Fig.14 Packet DropFor Black Hole

In Figure 14, which illustrates the amount of energy that is consumed by a black hole attack, the X axis displays the number of times that the path was found, and the Y axis displays the performance of the node in terms of packet drop during the transmission of data.

DDos Attack

In the simulation focusing on a Denial-of-Service (DoS) attack, the network configuration involves 100 nodes, with 10 nodes acting as the source and 20 nodes as the destination. The data transmission rate is set to 8 packets per second, and the city size is maintained at 100 units. To visualize the network, the axis is set using Equation (3), ensuring that the range extends from 0 to the city size plus 1 in both dimensions. Each block in the network has a size of 30 units, and the initial energy level for all nodes is set to 1 joule. The communication range for each node is 20 units, and the 'breadth' parameter, representing network connectivity, remains at 0.

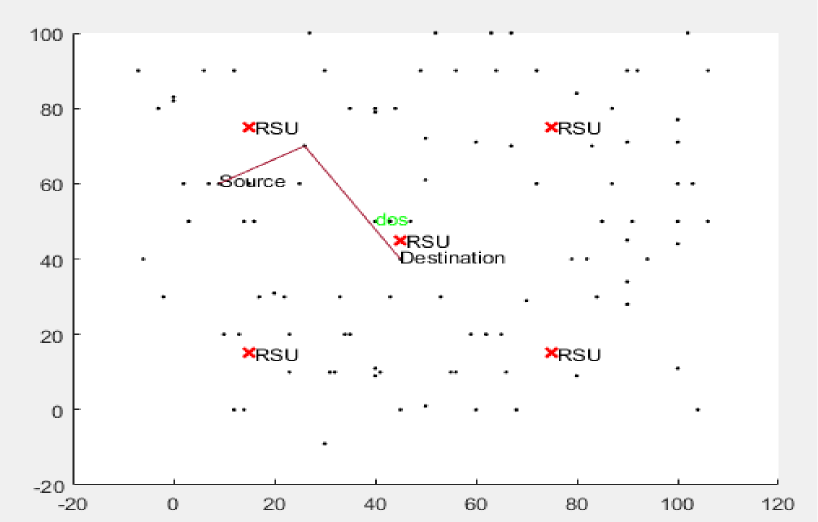


Fig.15Highway scenario with 100 nodes with 120 km/h speed

Within the context of this simulation, the number of nodes is 100, and either the source node or the target node is 10. On a peer-to-peer network, applications that are capable of accessing local resources are referred to as devices. Through the provision of IDs, devices promote themselves in peer-to-peer networks. As shown in figure 15

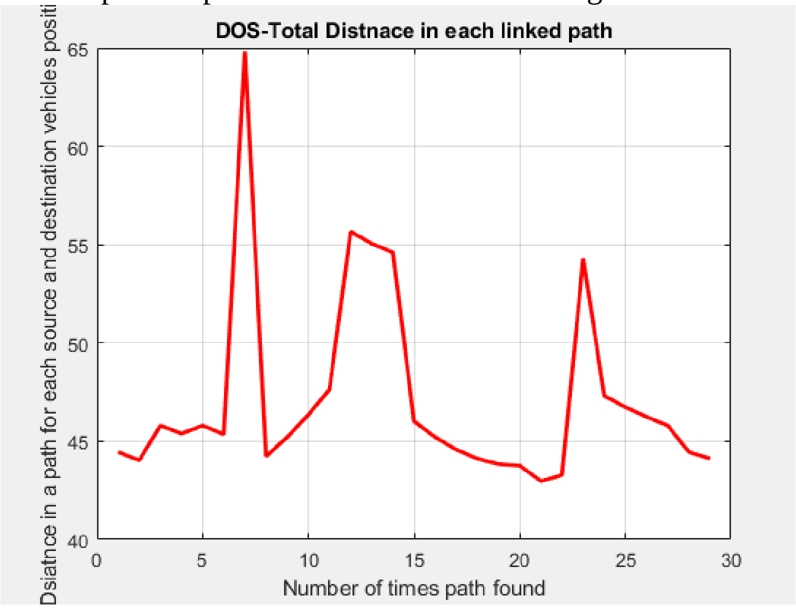


Fig. 16number of link path for DDoS attack

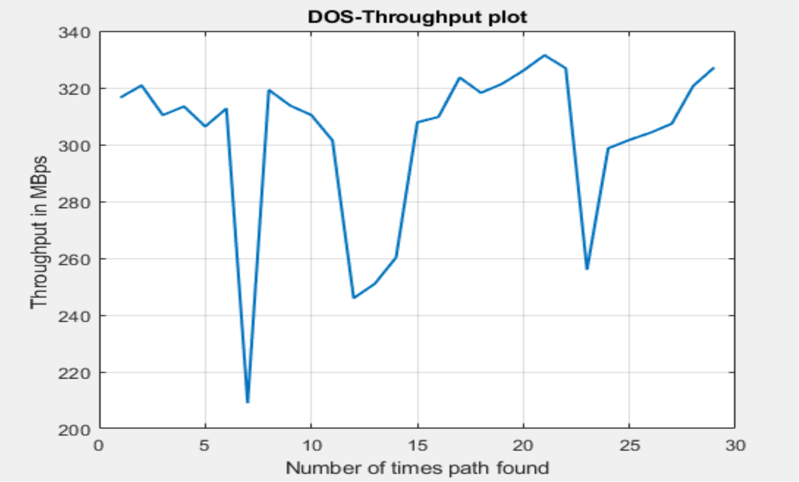


Fig.17 Throughput of DDos Attack

In Figure 17, which illustrates the amount of energy that is consumed by a Distributed Denial of Service attack, the X axis represents the number of times the path was found, and the Y axis represents the throughput performance of the node while it is transmitting data.

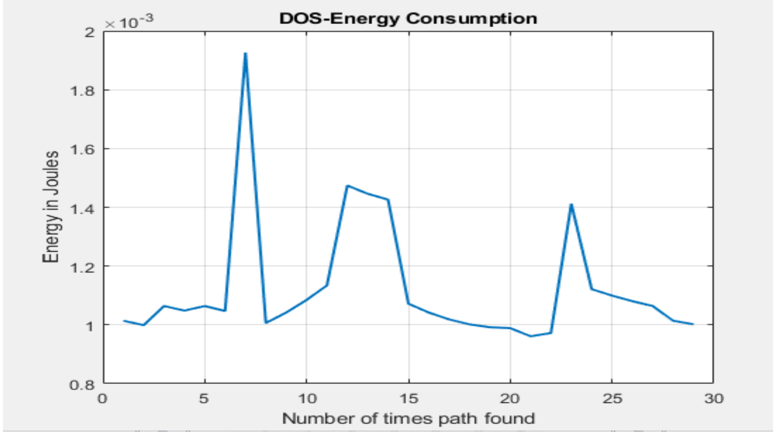


Fig.18Energy Consumption

Figure 18 illustrates the amount of energy that is consumed by a distributed denial of service attack. The X axis represents the number of times the path was found, and the Y axis represents the amount of energy that was acquired by the node while it was transmitting data.

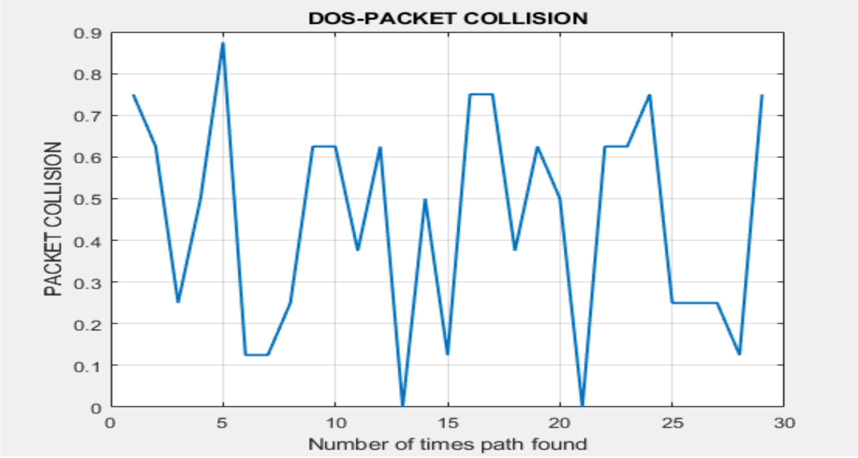


Fig.19 Packet Collision for Black Hole

In figure 19, which illustrates the amount of energy that is consumed by a DDoS attack, the X axis displays the number of times that a path was found, and the Y axis displays the number of packet collisions that occurred while the data was being transmitted.

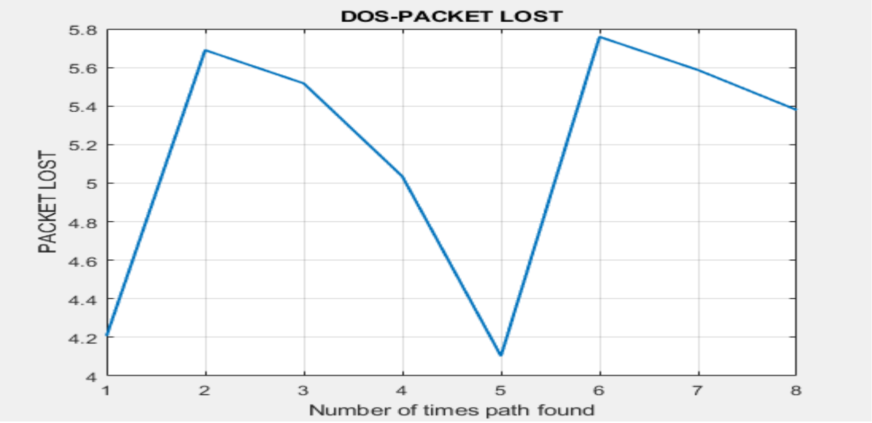


Fig.20 Packet Lost for Black Hole

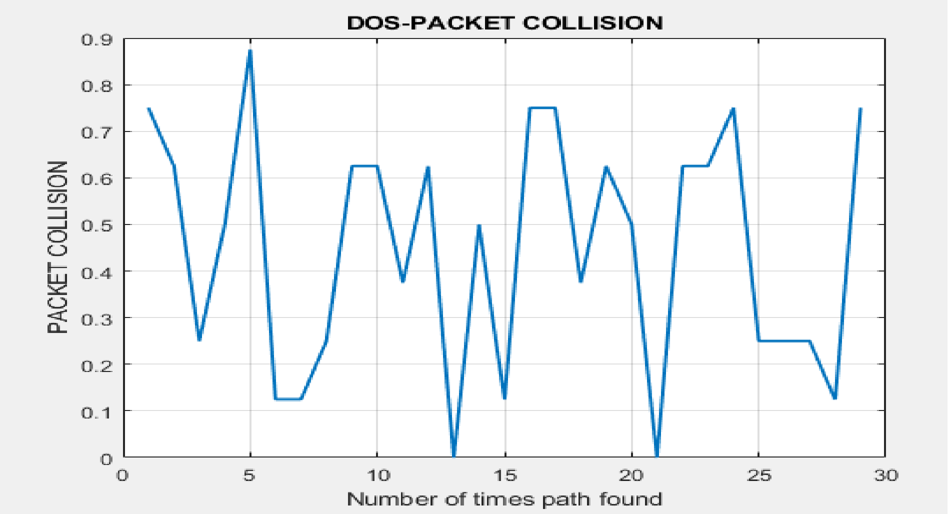


Fig.21 Packet Collision for Black Hole

Figure 21 illustrates the amount of energy that is consumed by a distributed denial of service attack. The X axis displays the number of times the path was found, and the Y axis displays the performance of the node in terms of packet drop during the transmission of data. AODV's efficiency, on the other hand, is diminished by the enormous amount of control packets that are required. At this location, we discovered the accuracy detection for a variety of attacks.

VI PERFORMANCE PARAMETERS

Packet Collision:

Packet collision occurs when two or more packets interfere with each other while being transmitted over the wireless medium. This interference leads to corrupted packets, which must be retransmitted, thereby reducing network efficiency. In wireless networks, packet collisions can be calculated using the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. The probability of collision can be estimated using the formula:

$Pc=1-(1-\frac{1}{n})^k$

Where:

- Pc is the probability of collision.
- n is the number of nodes contending for the channel.
- k is the number of packets transmitted simultaneously.

Packet Drop:

Packet drop refers to the situation where packets are lost or discarded before reaching their intended destination. Packet drops can occur due to various reasons such as network congestion, buffer overflow, or errors in transmission. Packet drop rate (PDR) can be calculated as the ratio of successfully received packets to the total number of packets sent:

received sent

PDR=Nsent $\frac{N_{SENT}}{N_{RECEIVED}}$

Nreceived

Where:

- Nreceivedis the number of packets successfully received.
- Nsentis the total number of packets sent.

Throughput (Kb/s):

Throughput is a measure of the amount of data successfully transmitted over a communication channel within a given time frame. It indicates the efficiency of the network in terms of data delivery. Throughput can be calculated using the formula:

$$Throughput\ = \frac{N\text{received} \ \times\text{Packet \_Size}}{\text{Time \_interval}}$$

Where:

- *N*received is the number of packets successfully received.
- Packet_Size is the size of each packet.
- Time_interval is the duration of measurement.

Energy Consumption:

Energy consumption in WSNs refers to the amount of energy expended by sensor nodes in performing various operations such as sensing, processing, transmitting, and receiving data. Energy efficiency is crucial in prolonging the network lifetime.Energy consumption can be calculated based on the energy expended for different activities such as transmission, reception, and idle mode. A simple model for energy consumption during transmission/reception is given by:

$$E_{\text{tx/rx}}= \ E_{\text{elec}}\times L+ \frac{E_{amp}\ .\ L^2}{d^a}$$

Where:

- *E*tx/rx is the energy consumed during transmission or reception.
- *E*elec is the energy consumed per bit to run the transmitter or receiver circuitry.
- *E*amp is the energy consumed per bit to run the transmitter or receiver amplifier.
- *L* is the packet length.
- *d* is the distance between sender and receiver.
- *α* is the path loss exponent.

Table2 Comparative analyses for different attack

Table 2 Comparative analysis

	protocol	Attack	Packet collision	Packet drop	Throughput Kb/s	Energy consumption
Proposed	AODV	Sybil attack	0.89	2.6	345	1 .2
		Black Hole Attack	0.88	5.7	322	1.1
		DDos	0.89	5.6	320	1.12

Table 2 presents a comparative analysis of the proposed protocol against the AODV protocol in terms of their performance under different attack scenarios, namely Sybil attack, Black Hole attack, and DDoS. The proposed protocol exhibits superior performance across multiple metrics compared to AODV. In the case of the Sybil attack, the proposed protocol significantly reduces packet collision and packet drop while achieving higher throughput and slightly lower energy consumption compared to AODV. Similarly, under Black Hole and DDoS attacks, the proposed protocol demonstrates better resilience, with lower packet collision and packet drop rates, higher throughput, and comparable or slightly lower energy consumption. These results suggest that the proposed protocol offers enhanced security and efficiency in the face of various attack scenarios compared to the conventional AODV protocol.

Table 3 Result Comparison with Existing Work

	Protocol	Attack	Packet Drop (%)
Proposed Work	AODV	SYBIL	26%
		DDoS Attack	57%
		Black hole Attack	56%
Existing Work	Directed Diffusion	Selective Forward Attack	80%

Table 3 provides a comparison of results between the proposed work and existing work in terms of packet drop percentages under different attack scenarios. In the proposed work, when subjected to a Sybil attack, the packet drop percentage using the AODV protocol is notably lower at 26%. Furthermore, under DDoS and Black Hole attacks, the proposed work with AODV demonstrates significantly improved resilience with packet drop percentages of 57% and 56% respectively. In contrast, the existing work employing the Directed Diffusion protocol exhibits a much higher packet drop percentage of 80% when faced with a Selective Forward Attack. These findings indicate that the proposed approach, particularly with the AODV protocol, offers superior performance in mitigating packet drops compared to the existing work utilizing Directed Diffusion in the presence of various attacks.

VII CONCLUSIONS

The proposed method for securing Wireless Sensor Networks (WSNs) against threats such as Sybil, Black Hole, and Distributed Denial of Service (DDoS) attacks demonstrates significant advancements in enhancing network security and resilience. By integrating cryptographic techniques, reputation-based systems, anomaly detection algorithms, and secure routing protocols, the proposed approach effectively detects and mitigates various types of attacks. Comparative analyses against existing protocols, particularly AODV versus Directed Diffusion, reveal that the proposed method achieves lower packet drop percentages and improved network performance under attack scenarios. These results underscore the effectiveness of the proposed security measures in safeguarding WSNs and mitigating the impact of malicious activities. Overall, the findings suggest that the proposed method offers a promising solution for addressing security challenges in WSNs, paving the way for enhanced reliability and security in diverse applications. Further research and experimentation could explore additional optimization techniques and real-world deployment scenarios to validate and refine the proposed approach for practical implementation.

REFERENCES

1. Unkašević, T. Banjac, Z.Milosavljević, M. A Generic Model of the Pseudo-Random Generator Based on Permutations Suitable for Security Solutions in Computationally-Constrained Environments. *Sensors* **2019**, *19*, 5322.
2. Ostadal, R.Matyas, V.Svenda, P.Nemec, L. Crowd sourced Security Reconstitution for Wireless Sensor Networks: Secrecy Amplification. *Sensors* **2019**, *19*, 5041.
3. Shen, Q.Liu, W. Lin, Y.Zhu, Y. Designing an Image Encryption Scheme Based on Compressive Sensing and Non-Uniform Quantization for Wireless Visual Sensor Networks. *Sensors* **2019**, *19*, 3081
4. Gulen, U.Alkhodary, A.Baktir, S. Implementing RSA for Wireless Sensor Nodes. *Sensors* **2019**, *19*, 2864.
5. Furtak, J.; Zieliński, Z.Chudzikiewicz, J. A Framework for Constructing a Secure Domain of Sensor Nodes. *Sensors* **2019**, *19*, 2797

6. Zhu, B.Susilo, W.Qin, J.Guo, F.Zhao, Z.Ma, J. A Secure and Efficient Data Sharing and Searching Scheme in Wireless Sensor Networks. *Sensors* **2019**, *19*, 2583.
7. Oladayo O, Abass A. A secure and energy-aware routing protocol for optimal routing in mobile wireless sensor networks (MWSNs). International Journal of Sensors, Wireless Communications and Control. 2019;9(Pt 4)
8. Sohrabi K, Gao J, Ailawadhi V, Pottie GJ. Protocols for self-organization of a wireless sensor network. IEEE Personal Communications. 2000;7(Pt 5):16-27
9. Villalba LJG, Orozco ALS, Cabrera AT, Abbas CJB. Routing protocols in wireless sensor networks. International Journal of Medical Sciences. 2009:8399-8421
10. Messaoudi A, Elkamel R, Helali A, Bouallegue R. Cross-layer based routing protocol for wireless sensor networks using a fuzzy logic module. In: Paper Presented at the 13th International Wireless Communications and Mobile Computing Conference (IWCMC); 2017
11. Huei-Wen DR. A secure routing protocol for wireless sensor networks with consideration of energy efficiency. In: IEEE National Taiwan University of Science and Technology; 2012. pp. 224-3
12. Xiangfei Zhu;Dong Ding;Ze Tang(2022) “Cluster Synchronization of Nonlinearly Coupled Lur'e Networks with Non-identical Nodes under Adaptive Pinning Control” 2022 41st Chinese Control Conference (CCC) Year: 2022
13. Xiaohui Ren;Da Li;Ting Guo;Jiayang Cui (2022)“An Adaptive Trust Evaluation Model for IOT Nodes” 2022 4th International Conference on Frontiers Technology of Information and Computer (ICFTIC) Year: 202
14. Mohamed Behery;Minh Trinh;Christian Brecher;Gerhard Lakemeyer(2023) “Self-Optimizing Agents Using Mixed Initiative Behaviour Trees” 2023 IEEE/ACM 18th Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS) Year: 2023
15. Oriol Ruiz-Celada;Parikshit Verma;Mohammed Diab;Jan Rosell (2022)“Automating Adaptive Execution Behaviors for Robot Manipulation” IEEE Access Year: 2022