MACHINE INTELLIGENCE RESEARCH
ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

EVALUATING AD-HOC NETWORK PERFORMANCE AGAINST BLACK HOLE, SYBIL, AND DDOS ATTACKS

Akash Thakur[1] ,Dr. Sanjay Kumar Sharma[2],Dr. Rajesh Kumar Bhogey[3],Dr. Bhupendra verma[4]
M.Tech.Scholar[1], Professor[2,3,4]
akash5993thakur@gmail.com[1], sanjaysharmaemail@gmail.com[2], rajeshboghey@gmail.com[3], bkverma3@gmail.com[4]
Technocrats Institute of Technology (Excellence) Bhopal

ABSTRACT: End users' safety when using applications in vehicular networks is a growing concern. Therefore, it's crucial to make these applications highly secure to guarantee dependable service for users and sufficient human life safety. Though unwanted, the attacker is also one of the major entities that can critically affect a new potentially lifesaving vehicular network. These bothersome attackers behave in very unpredictable ways and can launch various kinds of attacks. VANET aims to maintain traffic congestion by keeping in touch with nearby vehicles. Ad-hoc networks are decentralized wireless networks where nodes communicate directly with each other without relying on a fixed infrastructure. Ad-hoc networks, characterized by their decentralized and dynamic nature, are vulnerable to various security threats that can severely impact their performance. The results indicate that black hole attacks cause significant packet drops and throughput reductions due to malicious nodes discarding packets. Sybil attacks lead to increased packet collisions and routing inconsistencies, resulting in higher energy consumption. DDoS attacks overwhelm the network with excessive traffic, drastically reducing throughput and increasing both packet collisions and energy usage. This analysis provides critical insights into the distinct impacts of each attack type, highlighting the need for robust security mechanisms to ensure the reliability and efficiency of ad-hoc networks.
Keywords: VANET, Sybil attack, DDoS attack, Black Hole Attack, AODV Protocol

I INTRODUCTION

The Vehicle Node-based Vehicle Self-Organization Network (VANET) is made up of drones that have high mobility and provide connectivity to remote areas. A drone is an airplane without a pilot on board. The UAV can be remotely controlled (i.e. controlled by the pilot at the ground control station), or it can fly autonomously according to a predefined flight plan. Civilian uses for drones include 3D terrain modelling, package delivery (Amazon), etc. The US Air Force also uses drones for data collection and situational understanding without the risk of flying in hostile alien environments. By integrating ad hoc wireless network technology into drones, multiple drones can communicate with each other and perform tasks and tasks as a team. If an unmanned aircraft is destroyed by the enemy, its data can quickly evolve into new technology or air technology, surveillance of inaccessible areas or surveillance of disasters. In this case, the Vehicle Node Self-Organizing Vehicle Network (VANET) will be displayed, which is a self-organizing network configuration composed of Unmanned Aerial Vehicles (UAVs).[1-2]

Overview of VANETs %e VANETs architecture contains the OBU, RSU, and TA. %ere are two types of communication technologies in VANETs architecture, i.e., (1) vehicle to vehicle (V2V) and (2) vehicle to infrastructure (V2I) communication as shown in Figure 1. V2V contact vehicles converse with one another and exchange the traffic-related information inside the wireless network range [3,4].

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

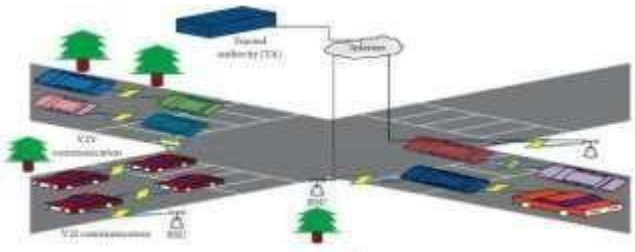


Figure 1: VANETs architectures

In such networks, when any unforeseen incident happens, such as accident or traffic blockage on the road, instantly a vehicle sends an alert signal to the other nodes or vehicles in the network suggesting to avoid that particular road or area. %e vehicle, employing V2I communication, shares the information with RSU which is part of infrastructure installed on the road. %e V2I based communication notifies the driver about traffic and weather updates to keep an eye on the nearby environment [5]. RSU and OBU are registered by a trusted authority [6-7], which is used to keep up and supervise the VANETs system. %e road-side unit positions itself on the road for authentication and communication between TA and OBU. With the use of dedicated short-range communication (DSRC) [8], the OBU fitted in each vehicle can transmit traffic information to nearby vehicles and RSU [9]

3. Security Issues in VANETs %e security issue is very crucial in VANETs which ensures safety for the drivers as well as passengers. %is is obligatory to design essential algorithms to assure safety and protection. %e security challenges as posed to VANETs are availability, authentication, integrity, confidentiality, nonrepudiation, pseudonymity, privacy, mobility, data and location verification, access control, and key management issues [9, 10,11].

Security Issues. In this section, we provide details about various security issues in VANETs.

Availability. Availability [17] is considered a significant factor in VANETs security. %is ensures that all resources are accessible forever in a network in the face of vulnerabilities and denial of service attack-based attempts. Cryptography and trust-based algorithms and protocols are helpful to protect the VANETs from these attacks [9, 10, 17, 18].

Authentication. Authentication enables the right participants to enter the network after dual verification. It also ensures that the sender or user who sends a message is not an intruder. Besides, the privacy of the user is preserved using pseudonyms [17–19].

Integrity. Integrity or data integrity ensures that there is no change in the original data packets sent by the sender. Alternatively, it must be protected from the adversary on the way. Data accuracy is one of the fundamental security issues in VANETs. Digital signature, public key infrastructure, and cryptography revocation mechanism may be employed to ensure the integrity between the sender and receiver [9, 10].

Confidentiality. Confidentiality means to hide data from adversaries. In confidentiality we make sure only authenticated users access the data with the help of encryption and decryption. In this way the data remains confidential, while the other unauthorized users may not access this confidential information [9, 20].

Privacy. In VANETs, the privacy refers to concealing driver identity as well as the location's information from other unauthorized users in the network [9, 18, 21].

Scalability. %e capability of the network to respond to the dynamically changing requirements is termed as scalability. %e frequently changing topology of the vehicular network is another challenge for the researchers [18].

Mobility. Mobility is ubiquitous in VANETs because nodes communicating in VANTEs change their location very quickly and frequently in a network. VANETs nature is dynamic because

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

every second, the node position is changed. %is mobility factor focuses on the need of more secure and dynamic algorithms maintaining quality of service requirements [18]

Ad Hoc On-Demand Distance Vector (AOVD). AOVD [20], in MANETs, AODV protocol, is used for on-demand routing purposes with reactive routing. In the AODV protocol, routing table is maintained to store the next node routing information, i.e., for the target location nodes, and each routing table is used for a specific time period. If the path is demanded within a specific time, it becomes expired. Later, if a node wants to communicate, then again it finds a new route. In AODV, when the source node sends data, it checks the routing table and sends if the route is available. Otherwise, it needs to start the path finding process again to discover the finest route source to the target location for the purpose of transmitting packets through the broadcasting of route/path request (RREQ) message to its neighbor node. AODV was geared towards reducing the distribution of control traffic and stopping data traffic overhead, improving scalability and efficiency [16]. Figure 2 shows that in AODV the messages RREQ and RREP are used. In this figure, node S wants to communicate with node D, and all nodes are connected to their neighbor nodes and submit an RREQ message while every node sends REEQ message to the neighbor node. After receiving the RREQ message, every node sends back an RREP message. When all RREP messages are received, the source node chooses the best path and starts communication [57].

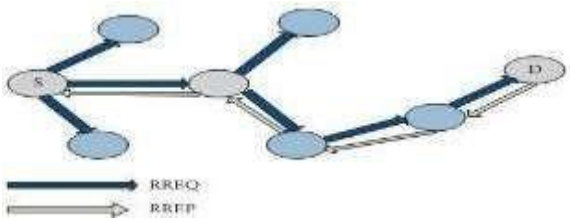


Figure 2: AODV RREQ and RREP message.

II RELATED WORK

Xiangfei Zhu (2022) addresses the problem of global adaptive cluster synchronization in complex dynamic networks of nonlinear Lur'e systems with asymmetrical and non-identical couplings. A pinning feedback controller targets Lur'e systems in the current cluster connected to other clusters. Conditions for cluster synchronization are derived using the Lyapunov stability theorem, S-procedure, and other analyses. Adaptive update laws achieve optimal feedback control gains, and numerical simulations verify the results [22]

Xiaohui Ren (2022) proposes the DATEM model for dynamic trust evaluation in IoT nodes, improving effectiveness, accuracy, and resilience against malicious node fraud. The model uses fault-tolerant data transmission, node energy impact, and a dynamic reward-punishment factor for direct trust calculation. K-means clustering filters recommendation nodes to prevent malicious recommendations, and trust value weight is determined by trust queue sufficiency and direct trust value dispersion. Simulations show DATEM's superior response to data attacks and fraud detection.[23]Mohamed Behery (2023) introduces an extension to Behavior Trees (BTs) with Mixed Initiative Planning (MIP) using Dynamic Sequence Nodes (DSNs) for flexible, reactive, and robust robot programming. DSNs reduce the effort and nodes needed for BT design, maintaining robustness, readability, and modularity while enabling run-time optimization for improved performance in dynamic production environments.[24]Oriol Ruiz-Celada (2022) presents a framework for robotic manipulation in semi-structured environments, featuring perception and ontology-based reasoning for planning and execution adaptation. The framework plans at both symbolic and geometric levels, using behavior trees for task execution adaptation.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

This approach allows for automatic planning and robust execution of manipulation tasks, enhancing the functionality of service robots.[25]

IV PROPOSED SYSTEM

Long-term protocols are essential for maintaining stable communication in vehicular ad hoc networks (VANETs). These protocols rely on route information, which is established and maintained as nodes change positions. A commonly used protocol in VANETs is the Ad hoc On-demand Distance Vector (AODV) protocol, which is topology-based and stores routes for efficient routing.In the AODV protocol, when a source node needs to communicate with a destination node, it sends out a Route REQuest (RREQ) message to its neighboring nodes. The message propagates through the network until it reaches a node that either has a route to the destination or is the destination itself. Upon receiving the RREQ, intermediate nodes forward it towards the destination, potentially causing damage to one of the intermediate nodes. If a malicious node intercepts the RREQ and responds with a false Route REPly (RREP), the source node may unwittingly choose this malicious route, leading to a "black hole" situation.

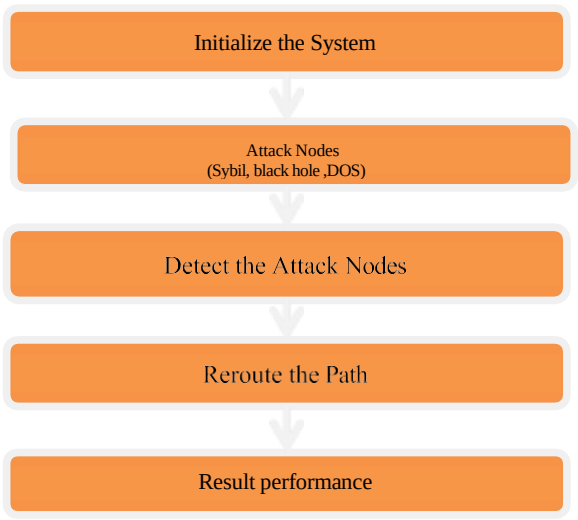


Fig 3. Proposed flow

In a black hole attack, the malicious node claims to have a valid route to the destination and intercepts RREQ messages. It then sends false RREPs, diverting legitimate traffic through itself. As a result, legitimate data packets are lost, and the network suffers from a denial-of-service (DoS) attack. Defending against black hole attacks requires robust mechanisms to authenticate nodes and verify the integrity of route information. Research in this area focuses on developing methods to detect and mitigate such attacks, ensuring the reliability and security of communication in VANETs.

V RESULT ANALYSIS

A vehicular network scenario using nodes and RSUs, employing the AODV routing protocol. It initializes parameters and places nodes and RSUs within a city area. The AODV algorithm is then simulated to find routes between a source and destination node, visualizing the paths and storing them for analysis. Additionally, the code incorporates simulations of various attacks like DOS, Sybil, and Black Hole, altering route visualization upon attack detection. It evaluates network

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

performance metrics such as energy consumption, packet collisions, throughput, and packet drops. Finally, results are plotted for analysis, providing insights into network behavior under different conditions and attacks.

Network Model Parameters

In this network model, N nodes are randomly deployed and controlled by an administrator. These nodes are configured to be energy efficient and capable of efficient data communication. The following parameters define the network setup:

Table 1 simulation parameters

Parameter	Value
Num Of Nodes	**100**
src_node	**10**
dst_node	**20**
data rate	**8 packets/sec**
citysize	**100 units**
blksiz	**30 units**
Eini	**1 joule**
Range	**20 units**
breadth	**0 units**
display_node_numbers	**1 (True)**
src_node1	**10**

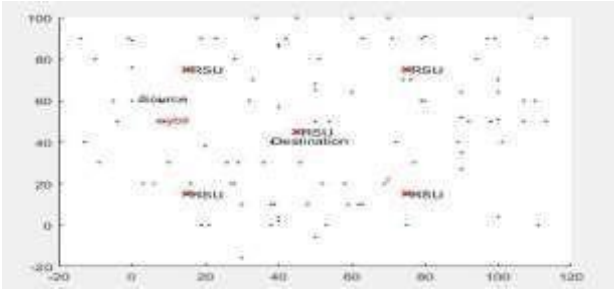


Fig.4 Highway scenario with 100 nodes with 120 km/h

The nodes represent vehicles equipped with communication devices that allow them to connect with other vehicles (vehicle-to-vehicle, V2V) and potentially with roadside infrastructure (vehicle-to-infrastructure, V2I). Each vehicle is moving at high speeds, up to 120 km/h, which affects the network topology and communication link stability. A highway environment typically features linear or slightly curved roads, multiple lanes, and high vehicle density showing in fig. 4

Sybil Attack

Devices on a peer-to-peer network advertise their presence by providing multiple identities. The impact of a Sybil attack can be measured by the number of fake identities and their effect on network parameters.

N_{total} be the total number of nodes in the network. N_{sybil} be the number of Sybil nodes (fake identities). N_{legit} be the number of legitimate nodes.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

Thus,

$$N_{total}=N_{legit}+N_{sybil}$$

The fraction of Sybil nodes in the network can be expressed as:

$$Fsybil = \frac{N_{sybil}}{N_{total}}$$

The impact on the Packet Delivery Ratio (PDR) due to Sybil attacks can be modeled by:

$$PDRaffected= PDRnormal\times(1-Fsybil)$$

Where

PDR_{normal} is the PDR under normal conditions without Sybil attacks.

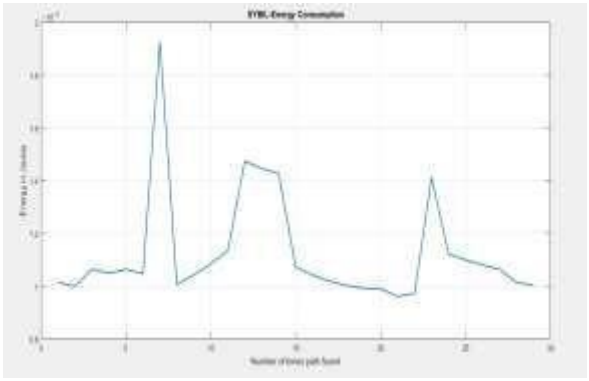


Fig.5 Energy consumption for Sybil attack

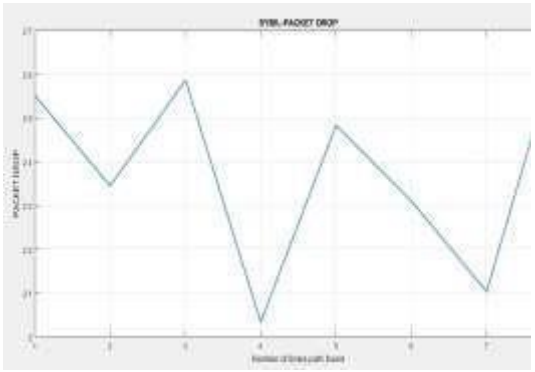


Fig.6 Packet collision for Sybil attack

Figures 5 to 8 illustrate the impacts of a Sybil attack on a network's performance. Figure 5 shows the energy consumption, where a Sybil attack significantly increases the energy drain on legitimate nodes due to the need to handle numerous fraudulent identities, leading to more processing and communication overhead. Figure 6 depicts packet collisions, highlighting that the presence of multiple Sybil nodes causes frequent collisions as the network becomes congested with illegitimate traffic, disrupting normal communication. Figure 7 focuses on packet drops, demonstrating a substantial rise in dropped packets as the network struggles to manage the additional and often conflicting traffic generated by the Sybil nodes. Finally, Figure 8 presents the throughput, which typically decreases under a Sybil attack as the network's capacity is overwhelmed by the fraudulent traffic, reducing the effective data transmission rate for legitimate nodes. These figures collectively underscore the detrimental effects of Sybil attacks on network performance, emphasizing the need for robust detection and mitigation strategies.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

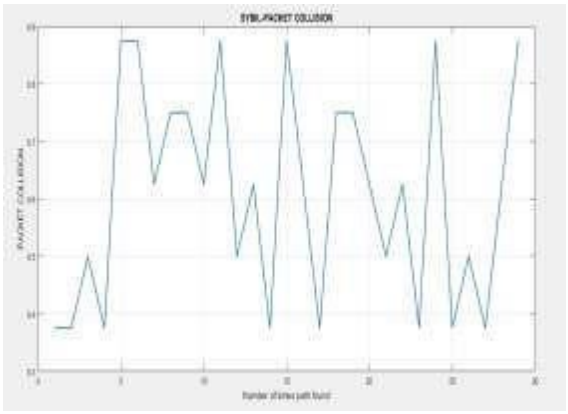


Fig. 7 Packet drop for Sybil attack

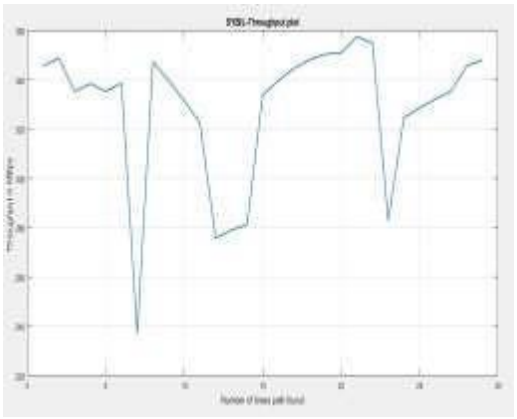


Fig.8 Throughput for Sybil attack

Black Hole Attack

Black hole attacks involve nodes that drop packets instead of forwarding them. The impact of a black hole attack can be quantified by the packet loss rate.

N_{drop} be the number of packets dropped.

$N_{total\_packets}$ be the total number of packets sent.

The packet loss rate due to black hole attacks is:

$$PLRblackhole=NdropNtotal\_packets$$

$$PLR_{blackhole}= \frac{N_{drop}}{N_{total\_pa\boldsymbol{w}kets}}$$

The effective throughput can be expressed as:

$$Throughput_{affected}=Throughput_{normal}\times(1-PLR_{blackhole})$$

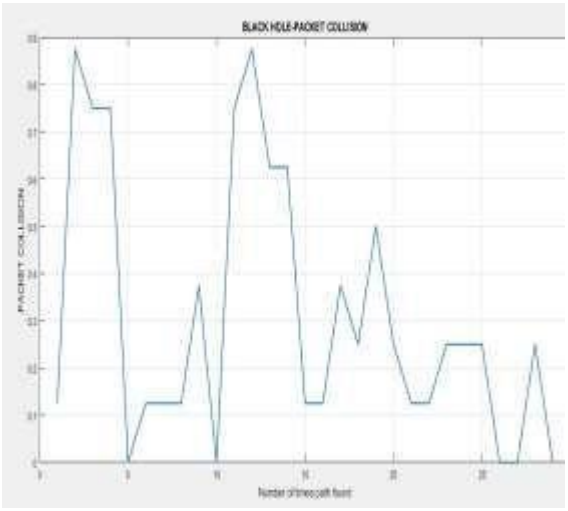


Fig.9 Packet Collision for Black Hole

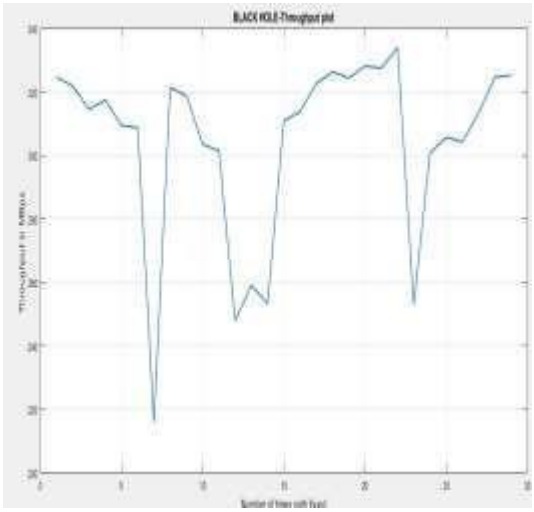
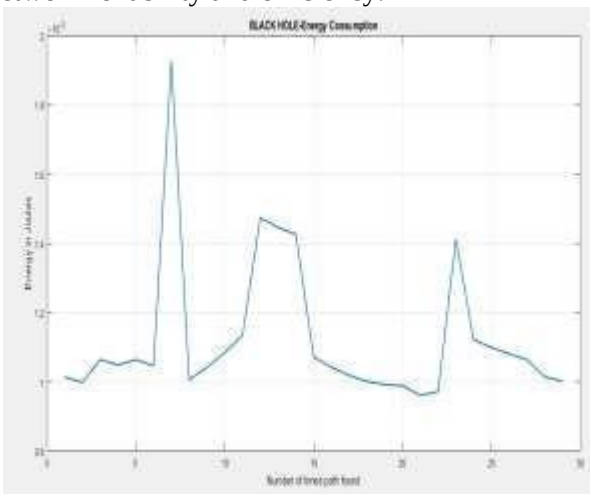


Fig.10 Throughput for Attack for Black Hole

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

Figures 9 to 12 demonstrate the effects of a Black Hole attack on network performance. Figure 9 illustrates packet collisions, showing an increase in collisions as malicious nodes disrupt normal traffic by falsely claiming to have the optimal route to the destination. Figure 10 highlights the throughput, which significantly decreases during a Black Hole attack due to the malicious nodes intercepting and dropping packets, preventing them from reaching their intended destination. Figure 11 presents energy consumption, revealing that energy usage spikes as nodes repeatedly attempt to resend lost packets and reestablish disrupted connections caused by the Black Hole nodes. Figure 12 depicts packet drops, showing a sharp rise in the number of dropped packets, as the malicious nodes deliberately absorb and discard the data, leading to significant data loss and communication breakdown. These figures collectively underscore the severe impact of Black Hole attacks on network reliability and efficiency.



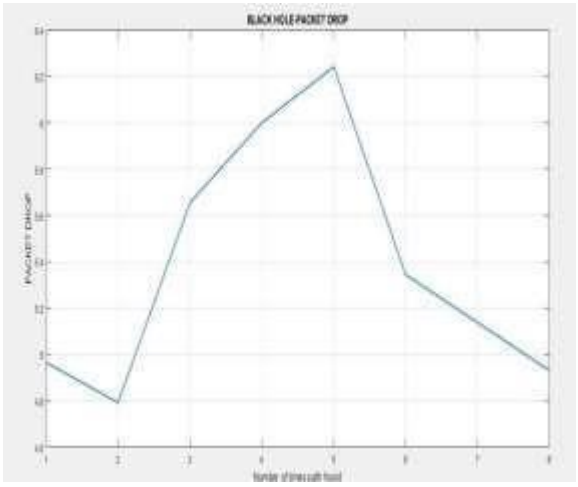


Fig.11 Energy Consumption for Black Hole **Fig.12 Packet Drop For Black Hole Attack**

DDoS Attack

DDoS attacks overwhelm network resources, leading to increased delay and reduced throughput. Application layer DDoS attacks, in particular, target specific services, leading to significant degradation in service quality.

R_{attack} be the rate of malicious traffic.
R_{legit} be the rate of legitimate traffic.
C_{total} be the total network capacity.

The total traffic load on the network is:

$$L_{total} = R_{attack} + R_{legit}$$

The delay introduced by the DDoS attack can be modeled as:

$$Delay_{ddos} = Delay_{normal} \text{ X.} \frac{L_{total}}{C_{total}}$$

$$\text{PDRddos} = \frac{\text{Rlegit}}{\text{Ltotal}}$$

If $Lt_{total} > C_{total}$ then packets will be dropped, and the effective Packet Delivery Ratio (PDR) will be:

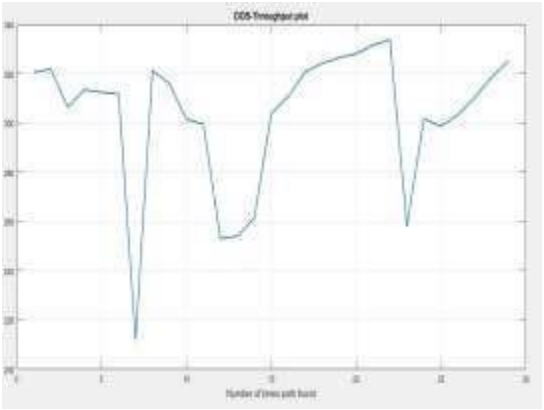
ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

The impact on throughput can be expressed as:

$$Throughput_{ddos} = Throughput_{normal} \times \frac{R_{egit}}{L_{total}}.$$

Figures 13 to 16 illustrate the detrimental effects of DDoS and Black Hole attacks on network performance. Figure 13 depicts the throughput under a DDoS attack, showing a substantial decline as the attack overwhelms the network with excessive traffic, thereby degrading the overall data transmission rate. Figure 14 presents energy consumption during the DDoS attack, highlighting increased energy usage as nodes expend more power to handle the excessive traffic and maintain connectivity.

Figures 15 and 16 both address packet collisions and Packet Drop during a Black Hole attack, illustrating a marked increase in collisions. These figures emphasize how malicious nodes disrupt normal traffic by falsely advertising optimal routes and then dropping the packets. This deception causes repeated packet transmissions and collisions as the network attempts to reroute traffic, significantly impairing communication efficiency and reliability. Together, these figures demonstrate the severe impact of both DDoS and Black Hole attacks on network throughput, energy consumption, and packet collision rates.



g13 Throughput of Ddos Attack

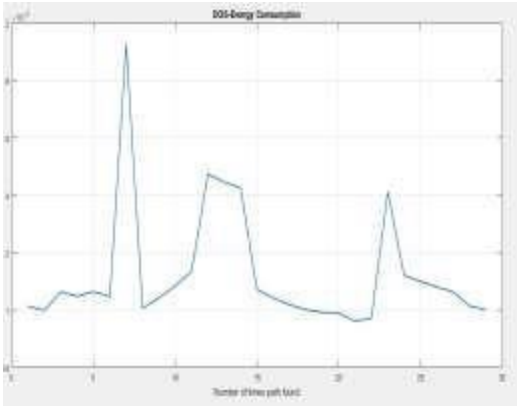
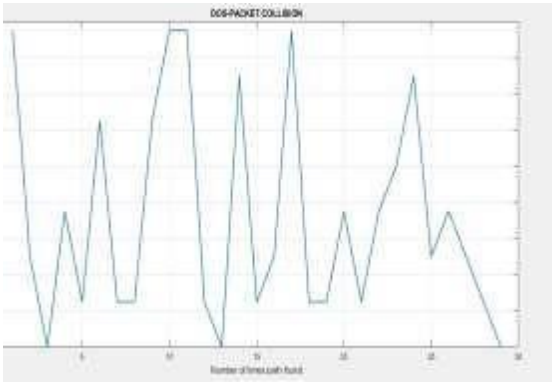
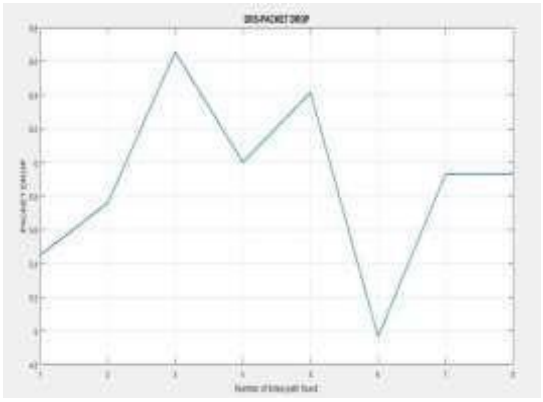


Fig.14 Energy Consumption





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

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

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:

$$PDR=N_{\text{sent}}^{\text{Received}} \quad \frac{N_{SENT}}{N_{RECEIVED}}$$

Where:

N_{received} is the number of packets successfully received.

N_{sent} is 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:

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

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:

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

Where:

$E_{\text{tx/rx}}$ 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.

Table 2 Comparative analyses for different attack

Table 2 Comparative analysis

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

	protocol	Attack	Packet collision	Packet drop	Throughput Kb/s	Energy consumption

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

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.

REFERENCES

1. R. Geng, X. Wang, and J. Liu, “A software defined networking-oriented security scheme for vehicle networks,” IEEE Access, vol. 6, pp. 58195–58203, 2018.
2. N. S. Samaras, “Using basic manet routing algorithms for data dissemination in vehicular ad hoc networks (VANETs),” in Proceedings of the 2016 24th Telecommunications Forum (TELFOR), pp. 1–4, IEEE, Belgrade, Serbia, November 2016.
3. J. Wantoro and I. W. Mustika, “M-aodv+: an extension of aodv+ routing protocol for supporting vehicle-to-vehicle communication in vehicular ad hoc networks,” in

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

Proceedings of the 2014 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT), pp. 39–44, IEEE, Jakarta, Indonesia, November 2014

4. L. Feng, Y. Xiu-Ping, and W. Jie, "Security transmission routing protocol for mimo- vanet," in Proceedings of the 2014 International Conference on Cloud Computing and Internet of 9ings, pp. 152–156, IEEE, Changchun, China, December 2014.
5. C. Pathak, A. Shrivastava, and A. Jain, "Ad Hoc on demand distance vector routing protocol using dijkastra's algorithm (aodv-d) for high throughput in vanet (vehicular Ad Hoc network)," in Proceedings of the 2016 11th International Conference on Industrial and Information Systems (ICIIS), pp. 355–359, IEEE, Roorkee, India, December 2016.
6. I. U. Rasool, Y. B. Zikria, and S. W. Kim, "A review of wireless access vehicular environment multichannel operational medium access control protocols: quality-of- service analysis and other related issues," International Journal of Distributed Sensor Networks, vol. 13, no. 5, 2017.
7. M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: communication, applications and challenges," Vehicular Communications, vol. 19, Article ID 100179, 2019.
8. S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETs): status, results, and challenges," Telecommunication Systems, vol. 50, no. 4, pp. 217–241, 2012.
9. Z. Afzal and M. Kumar, "Security of vehicular ad-hoc networks (vanet): a survey," Journal of Physics: Conference Series, vol. 1427, no. 1, Article ID 012015, 2020.
10. M. S. Sheikh, J. Liang, and W. Wang, "Security and privacy in vehicular ad hoc network and vehicle cloud computing: a survey," Wireless Communications and Mobile Computing, vol. 202025 pages, Article ID 5129620, 2020.
11. A. Awang, K. Husain, N. Kamel, and S. Aissa, "Routing in vehicular ad-hoc networks: a Survey on single- and cross-layer design techniques, and perspectives," IEEE Access, vol. 5, pp. 9497–9517, 2017.
12. S. A. Chaudhry, "Correcting "palk: password-based anonymous lightweight key agreement framework for smart grid"" International Journal of Electrical Power & Energy Systems, vol. 125, Article ID 106529, 2021.
13. X. Li, Y. Han, J. Gao, and J. Niu, "Secure hierarchical authentication protocol in vanet," IET Information Security, vol. 14, no. 1, pp. 99–110, 2019.
14.] A. Sari, O. Onursal, M. Akkaya et al., "Review of the security issues in vehicular ad hoc networks (vanet)," International Journal of Communications, Network and System Sciences, vol. 8, no. 13, pp. 552–566, 2015.
15. Z. A. Abdulkader, A. Abdullah, M. Taufik Abdullah, and Z. Ahmad Zukarnain, "Vehicular ad hoc networks and security issues: survey," Modern Applied Science, vol. 11, no. 5, Article ID 30, 2017.
16. R. C. Poonia, D. Bhargava, and B. S. Kumar, "Cdra: clusterbased dynamic routing approach as a development of the aodv in vehicular ad-hoc networks," in Proceedings of the 2015 International Conference on Signal Processing and Communication Engineering Systems, pp. 397–401, IEEE, Guntur, India, January 2015.
17. 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)
18. 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
19. Villalba LJG, Orozco ALS, Cabrera AT, Abbas CJB. Routing protocols in wireless sensor networks. International Journal of Medical Sciences. 2009:8399-8421

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

20. 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
21. 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
22. 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
23. 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
24. 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
25. Oriol Ruiz-Celada;Parikshit Verma;Mohammed Diab;Jan Rosell (2022)"Automating Adaptive Execution Behaviors for Robot Manipulation" IEEE Access Year: 2022