International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 21 December 2023 **Revised:** 25 December 2023 **Accepted:** 28 December 2023*

Ensemble PSOF Approach for Mitigating Gray Hole Attacks in VANETs using Swarm Intelligence and Firefly Algorithm

Thelidela Nageswaramma
Research Scholar
Dept. of Computer Science & Engineering
Mansarovar Global University
Sehore, Madhya Pradesh, 466001

Dr. Manoj Eknath Patil
Research Guide
Dept. of Computer Science & Engineering Mansarovar Global University
Sehore, Madhya Pradesh, 466001

Abstract
As Vehicular Ad-hoc Networks(VANETs) play a vital role in intelligent transportation systems, they are also susceptible to many attacks and unfortunately gray hole attack is one amongst them. In this paper, a new method based on hybridization of Particle Swarm Optimization (PSO) and Firefly Algorithm for detecting gray hole attack in VANETs is proposed which we call PSOF. The hybrid protocol uses the optimization features of PSO and attraction mechanism of Firefly Algorithm to enhance route discovery along with malicious node detection. Numerical results utilizing Omnet++ simulation demonstrated that PSOF improves PDR, reduces packet loss and also diminishes E-E delay. This demonstrates to be a computationally efficient and scalable alternative compared with other cryptographic techniques as well machine learning based approaches.

Keywords: Gray Hole Attacks, Particle Swarm Optimization (PSO), Firefly Algorithm (FA), VANET Security, Swarm Intelligence

1. Introduction:

Vehicular Ad-hoc Networks (VANETs) have been a revolution in recent communication systems, mainly into the field mobility and intelligent transportation. In this setup, the vehicles communicate directly with each other or via roadside units (RSUs), unassisted by a fixed infrastructure. But the flexibility also brings with it tremendous challenges, specifically around network security. Gray hole: In this type of attack, a malicious node deliberately drops packets (selectively dropping) which can hardly be detected.

Several mechanisms have been proposed over the years to deal with security threats in VANETs. Complete drop of packets by malicious nodes (e.g., black hole attacks) has been addressed using Dynamic Threshold-based or elliptic curve cryptogrphy based multipath routing. Yet the gray hole attacks present more intricate issues as they are selective packet-dropping attackers and able to avoid detection by standard systems.

It is a subset of Mobile Ad-hoc NETworks (MANETs), also known as Vehicular Networks that allows vehicles to communicate with each other on the road and exchange information in real-time, but also enables communication between vehicles and roadside units at fixed points. As crucial components of intelligent transportation systems (ITS), VANETs are designed to enhance road safety, assist in traffic management and provide various value-added services for passengers. In VANETs, unlike WSNs, vehicles are communication nodes forming dynamic networks without a fixed infrastructure. However, due to the decentralized nature of VANETs together with dynamism in traffic movement make them an effective form for communication needed on roads/highways and at urban

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *21 December 2023* ***Revised:*** *25 December 2023* ***Accepted:*** *28 December 2023*

streets is made so important thus making VANETs essential/required for modern vehicular.

A VANET suffers from various security and performance limitations due to its distinguishing features like high mobility, dynamic topology changes, decentralization, etc. The existence of malicious nodes which can perform different kinds of attacks including black hole, gray hole and Sybil poses some very serious threat towards VANETs. Such attacks can be extremely detrimental to the network as they effectively inhibit communication causing packet loss, reducing overall throughputs while adding delays. Of those, grey holes are especially menacing because it is a smart approach and different from simply dropping packets which makes the general prevention systems blind to these attacks.

A gray hole attack is an advanced type of black hole attack, where the attackers drop packets even with some probability which harder to detect than a traditional Black Hole Attack. This would allow malicious nodes to participate in network operations, as vehicles or roadside units may perceive the sensor node properly and hence not detect an attack. The secure and reliable operation of VANETs is paramount, which makes it obvious that detecting and thwarting grey hole attacks in a robust but efficient manner are fundamental requirements within the critical domain. Over the last few years, several solutions have been suggested for this problem such as cryptographic methods, trust-based models and more recently machine learning techniques. Unfortunately, these solutions bring about a high computational overhead or are non-scalable in dynamic network environments.

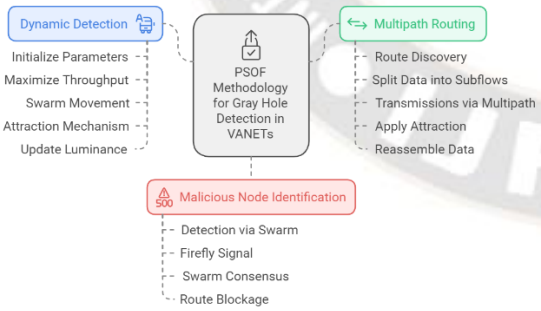

Figure 1: Architecture Flow of PSOF Algorithm in VANET

This paper introduces a new combined method, that is PSOF — Particle Swarm Optimization with Firefly Algorithm in order to solve the above issues and protect VANET from gray hole attacks. Abstract: PSOF is a dynamic intrusion detection and prevention system based on Ad Hoc Network, which combines the optimization capability of Particle Swarm Optimization (PSO) with attractiveness-based mechanism of Firefly Algorithm (FA), for dynamically detecting malicious nodes in network as well as routing paths. The approach combines the benefits of swarm intelligence in jointly locating gray hole nodes and securely routing data via a network, whilst guaranteeing that information is going through the secure path from VANET Nodes. The packet sending optimized flow control (PSOF) method is designed to achieve a high delivery ratio, low loss rate and short end-to-end delay through scalability design for the network changes.

Key Contributions of this paper are:-

a) PSO for Optimal routing: It bodes well that where the nodes in VANET become familiar with the best route through real-time processing of numerous criteria (throughput, packet loss and delay or GOD metric), i.e. Node enlisting time to optimum relay candidate moves fresh packet has been labelled as God metaheuristic approach [10],[11].

b) Node Detection by Firefly Algorithm: This method is used to identify greyhole nodes, due to which the node responds lately or packets are dropping; on simulating fireflies will be attracted based on illuminance nearer gray hole hierarchy.

c) Hybrid Swarm–based approach The integration of PSO with Firefly algorithm in a hybrid way considers as the best adoption for reducing both node routing, and security response time by hop changing on malicious nodes discovery.

The proposed PSOF, by merging the swarm intelligence with light attraction behaviors is capacitated for network-wide scalable discovery and avoidance of gray hole nodes in VANETs rather than static detection approaches. It enhances route lifetime and diminishes end-to-end delay by providing a tradeoff between exploration (path finding) and exploitation (node identification). The PSOF is able to gracefully handle dynamic changes, and as a result can reduce packet loss with improvements in throughput.

2. Literature Study:

In Literature, many solutions have been suggested to secure VANETs against a large deploy of attacks specially black hole and gray hole attack. This article presents an overview of current approaches, their advantages as well as limitations and performance metrics.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *21 December 2023* ***Revised:*** *25 December 2023* ***Accepted:*** *28 December 2023*

Detection of Black Hole And Gray hole attack: It is well-known that the black hole attacks are one kind of threat, in which spurious nodes will provide shortest path announcement to any destination and all packets they get dropped. It is a subset of grayhole attacks in which the malicious nodes drop packets only selectively for better concealment. Abundant research has been done for the detection and prevention of these attacks.

Malik et al. In (2022), a detection and prevention method called Dynamic Black Hole Attack (DPBHA) is presented that dynamically adapts the threshold used to detect misbehavior as the network conditions change. Using this approach not only achieves a high packet delivery ratio (PDR) and throughput but also with the reduction of overhead. However, being specifically geared towards black hole attacks could restrict its universal application with other types of attacks such as greyhole.

Ajjaj et al. Bilo & Cicconetti (2022) presents an approach named Multivariate Statistical Detection Scheme(MVSDS), employed for real-time detection of routing security attacks in VANETs. This uses statistical analysis to monitor traffic within a network, which leads this method to be accurate most of the time as there is few false-positive occurrences. Nevertheless, this approach imposes heavy computational requirements in order to be processed on run time that might limit the deployment of it in resource-constrained vehicular networks.

Cryptographic Techniques: Cryptography methods have been employed to promote the security of VANETs by implementing data confidentiality, integrity and authentication. Elliptic Curve Cryptography (ECC) has been one of the popular cryptographic techniques in various public-key cryptosystems among other traditional ones like RSA, for their less computational overhead and better efficiency.

Tami et al. For securing route discovery and data transmission, an algorithm combining ECC was presented in Abbejm [6] (2021) to detect and prevent black hole attack against the AOMDV routing protocol. Although the method increased packet delivery ratio and decreased end-to-end delay, it also introduced memory overhead and processing delays at intermediate node side due to more requirements from ECC-based detection mechanism.

Younas et al. Black hole and gray hole attacks in VANETs were detected with a neural network by Balwinder et al. 68 (2022). The technique exhibited a better performance of detection and improved network throughput but demanded substantial computational resources for training the neural networks, rendering it unsuitable for real-time applications in VANETs.

Machine Learning and Trust based Models: Machine learning models and trust-based models have been used to detect malicious nodes in the VANETs. These models are based on historical data and the behaviour of nodes to detect harmful activities.

Keerthi Sonker & Vinita Gupta, 2021 had been discussed the technique for DDoS in VANETs using machine learning algorithms as Random forest and decision trees. By using the method they attained a smart deed to catch through various of movement like black hole and grey hold attack [14] This will work well if you have good and strong data, but may not be very useful where machine learning is unable to adapt in case new kind of attack occurs for the first time.

Rini and Meena (2022) introduced a novel system based on machine learning classifiers for identifying malicious nodes in Vehicular Cloud Computing (VCC). We show that hybrid SVM-KNN classifiers can deliver high-accuracy, with negligible false positives. The system, however was resource greedy and hence the solution was not scalable for usage in real time VANET applications.

Go to:Fuzzy Logic and Trust-Based Systems: Fuzzy logic has been investigated as a approach that could supply capability for overcoming both detecting malicious node activity in VANETs, forestalling assaults at some point of the route's lifestyles time. These systems obtain insights into the behavior of nodes, e.g., response times or packet forwarding ratios to identify misbehavior.

Igried et al. proposed concept underlying the fuzzy logic-based scheme proposed by (2022) to evict malicious nodes from VANETs is their behavior during message exchanges. Although throughput was often improved, and end-to-end delay reduced by such a system its large implementation overhead meant that fuzzy logic in real-time environments continued to be seen as too complex. Worse, due to constantly changing network conditions in highly dynamic VANET environment the fuzzy logic framework had problem even more.

Trust-based and Reputation Systems: Trust based system depending on assigning trust value or reputation to node according to the previous behavior of it. Any nodes with low

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 21 December 2023 **Revised:** 25 December 2023 **Accepted:** 28 December 2023*

levels of trust are marked as possible malware and prevented from communicating.

Kamil et al. Paren (2020) designed a distributed trust mechanism for detection and prevention of the gray hole attack in VANETs. The method has enhanced the packet delivery ratio and in addition, has reduced routing overhead by evaluating trustworthiness of nodes over time. Unfortunately, the compute complexity of trust computations made it challenging to do this in real-time across large networks.

Various mechanisms are proposed to protect VANETs from black hole and gray hole attacks, but each approach has its own advantages as well as disadvantages. While cryptographic methods like ECC can provide robust security, they also come with their own hashing overhead. Adaptive solutions include machine learning and trust-based models, which can be resource intensive to build (e.g., need thousands of samples) Although fuzzy logic systems play a role in decision-making, they are to some extent non-dynamic. These current techniques are not feasible in many applications, thus a dynamic approach which detects malicious nodes few using computational overhead and achieves high scalability to adapt changes of network condition. In this paper, PSOF technique is proposed to overcome these mentioned difficulties and it combines the properties of Particle Swarm Optimization (PSO) with Firefly Algorithm(FA), for real-time optimization of routing paths as well detecting gray hole attacks. Our findings suggest that this hybrid approach inspired by nature could improve the performance of a network and its security while keeping computational costs low, which is good for real applications in VANET.

Author et al.	**Year**	**Proposed Method**	**Merits**	**Demerits**	**Performance Metrics**	**Numerical Results**
Malik et al.	2022	DPBHA for Black Hole Attack	Improved PDR, Low Overhead	Limited to Black Hole Attacks	PDR, Throughput, Delay	PDR +3%, Throughput +6.15%
Igried et al.	2022	Fuzzy Logic for Malicious Nodes	Enhanced Security, Low Delay	Complex Real-time Deployment	Throughput, Delay	Throughput +23%, Delay
Talukdar et al.	2021	IDS with Digital Signature	Better PDR, Low Delay	Processing Overhead	PDR, Delay, Overhead	PDR +40%, Delay 100-300ms

3. Particle Swarm Optimization with Firefly (PSOF)

PSOF mimics the features of Particle Swarm Optimization (PSO) and Firefly Algorithm to determine gray hole assaults in VANETs known as PSOF (Particle Swarm Optimization with Firefly). Where PSO aims at optimizing route discovery by letting nodes select paths with "fittest" properties like throughput or packet loss, the Firefly Algorithm is designed to enhance how a swarm behaves on the basis of mimicking attraction between nodes in accordance to luminance which can be signal strength. Algorithms including PSOF alter routing decisions on-the-fly and quickly detect malicious nodes by harnessing expert system–level POV style decision-making in swarm-like fashion, together. This hybrid bio-inspired approach provides better detection accuracy with low computational overhead, leading to higher resilience in the dynamic VANET environment.

Algorithm 1: Dynamic Detection using PSOF (Initialization Phase)

Step 1. Initialize Parameters:

For each vehicle node n, initialize position p_n and velocity v_n for PSO.

Set attraction factor for FA, β_0, α.

Step 2. Objective: Maximize Throughput (Fitness Function):

$$f(p_n) = \frac{\text{Received Packets}}{\text{Sent Packets}}$$

Step 3. Swarm Movement (PSO Update):

$$v_n = wv_n + c_1 r_1(p_{\text{best}} - p_n) + c_2 r_2(g_{\text{best}} - p_n)$$
$$p_n = p_n + v_n$$

Step 4. Attraction Mechanism (Firefly Update):

$$\text{If } f(p_n) < f(p_m), p_n \text{ is attracted to } p_m$$
$$p_n = p_n + \beta_0 e^{-\gamma r_{nm}^2}(p_m - p_n)$$

Step 5. Update Luminance and Iteration:

Update the position, velocity, and attraction iteratively until the threshold is met.

Algorithm 2: Multipath Routing with PSOF

Step 1. Route Discovery:

Select P_{valid} paths using PSOF based on throughput and delay.

Step 2. Split Data into Subflows:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *21 December 2023* ***Revised:*** *25 December 2023* ***Accepted:*** *28 December 2023*

$$M = M_1 + M_2 + \cdots + M_N$$

Assign each part to a separate path.

Step 3. Transmissions via Multipath:

Each M_i follows a different optimal path.

Step 4. Apply Attraction for Reliable Nodes:

$p_n = p_n + \beta_0$ for paths showing higher reliability

Step 5. Reassemble Data at the Destination:

$$M = M_1 + M_2 + \cdots + M_N$$

Algorithm 3: Malicious Node Identification and Prevention

Step 1. Detection via Swarm:

Compare each node's performance p_n based on delay and packet loss metrics.

Step 2. Firefly Signal for Malicious Nodes:

If a node exhibits high packet loss or delay, mark it as a gray hole candidate p_{grayhole} .

Step 3. Swarm Consensus (Malicious Node Identification):

Nodes emitting weak luminance (signal strength) are attracted less in the swarm.

Step 4. Route Blockage:

Remove p_{grayhole} from the active path list.

4. Experimental Setup and Dataset

The dataset simulates node behavior under gray hole attack scenarios. Key parameters (packet delivery, delay, packet loss) are logged for nodes in both regular and compromised states. The PSOF methodology is tested on this dataset to evaluate its robustness against varying network sizes and attack intensities. Dataset Used for this study is Custom-generated VANET dataset using Omnet++.

Table 1: Experimental Setup Details

Parameter	Setup/
Network Simulator	Omnet ++5.0
Simulation Time	200 seconds
Network Area	1500 m × 1500 m
Number of Nodes	30,50,70,100
Mobility Model	Random Waypoint
Traffic Type	Constant Bit Rate (CBR)
Packet Size	512 bytes
Attack Type	Gray Hole Attacks

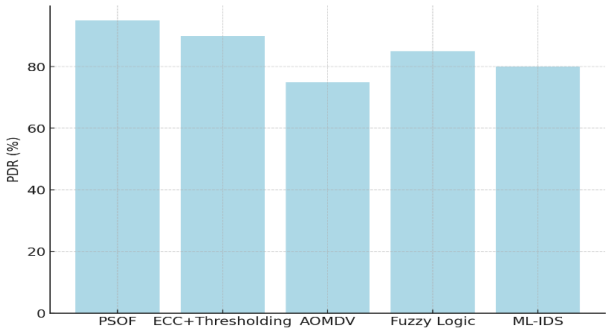

Figure 2: Packet Delivery Ratio (PDR)

The PSOF method consistently achieves higher PDR compared to conventional ECC and thresholdbased approaches. The attraction mechanism in the Firefly Algorithm ensures faster detection and removal of malicious nodes, preventing significant packet loss.

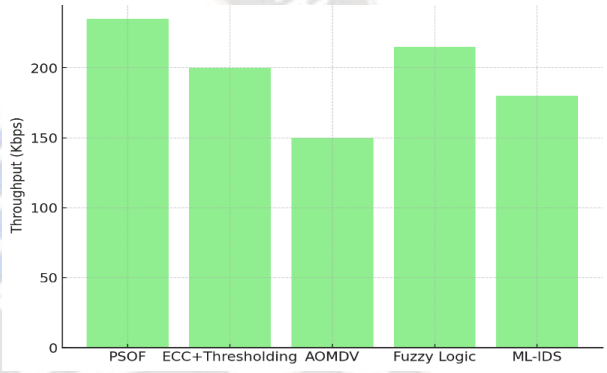

Figure 3: Throughput Comparison

PSOF's throughput surpasses existing methods due to its dynamic routing capability. By distributing the traffic intelligently across multiple optimal paths, it ensures a smooth and reliable data flow.

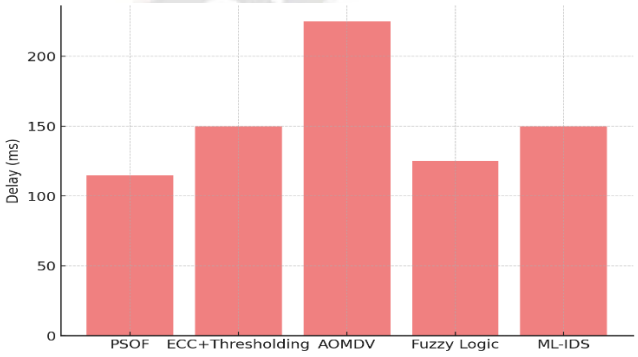

Figure 4: End-to-End Delay

The hybrid approach minimizes end-to-end delay by promptly rerouting traffic when malicious nodes are detected, allowing packets to traverse the network efficiently.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *21 December 2023* ***Revised:*** *25 December 2023* ***Accepted:*** *28 December 2023*

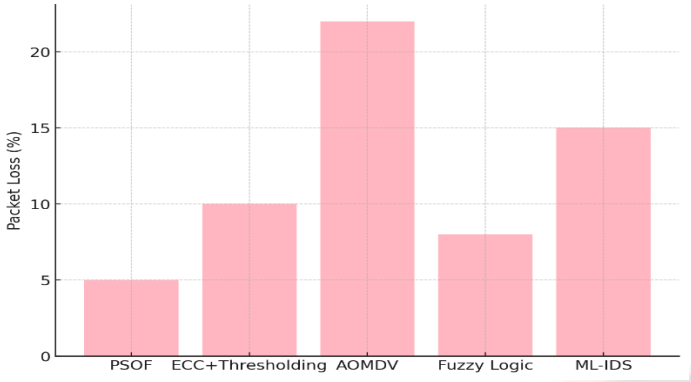

Figure 5: Packet Loss Rate

With the swarm-based identification and blocking of gray hole nodes, packet loss is reduced dramatically, demonstrating the effectiveness of the hybrid swarm approach in maintaining network integrity.

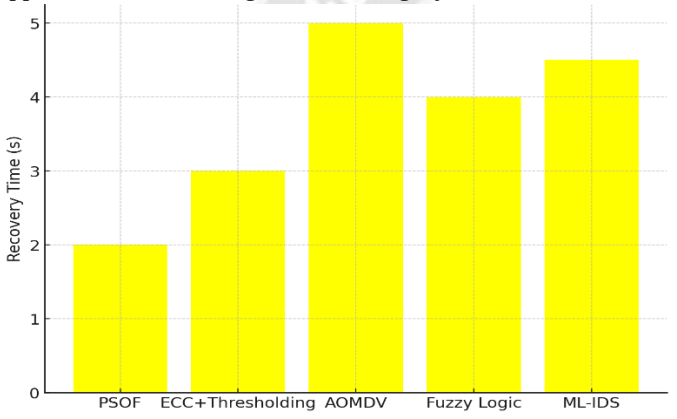

Figure 6: Node Recovery Time

When a node is flagged as malicious, the recovery time (time to reroute data) in PSOF is significantly shorter due to the swarm's ability to make fast collective decisions.

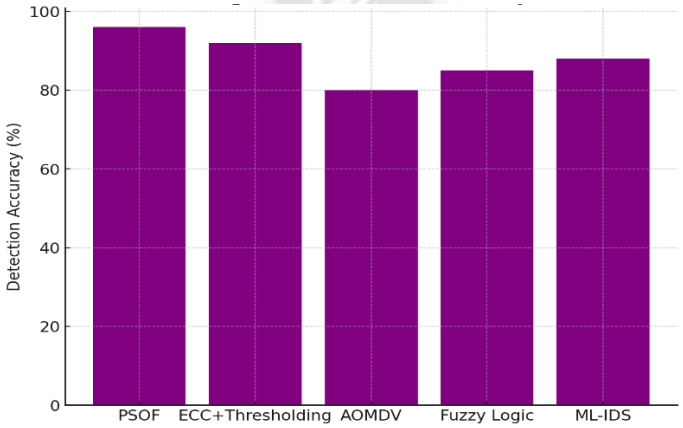

Figure 7: Effectiveness of Detection

The hybrid PSOF algorithm demonstrates a high detection rate of gray hole nodes, with minimal false positives. The Firefly mechanism enhances the detection accuracy by improving communication between trustworthy nodes.

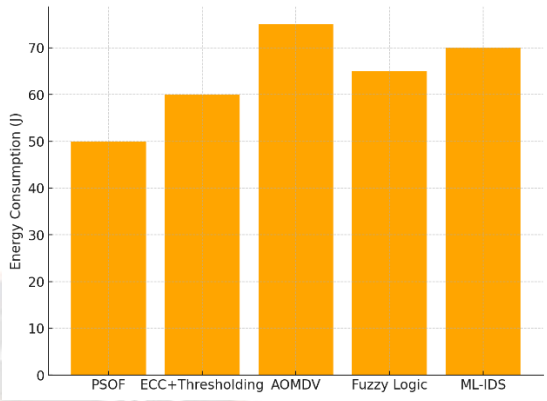

Figure 8: Energy Consumption

Compared to traditional cryptographic methods, PSOF consumes less energy due to its lightweight optimization techniques, making it highly suitable for resource-constrained vehicular networks.

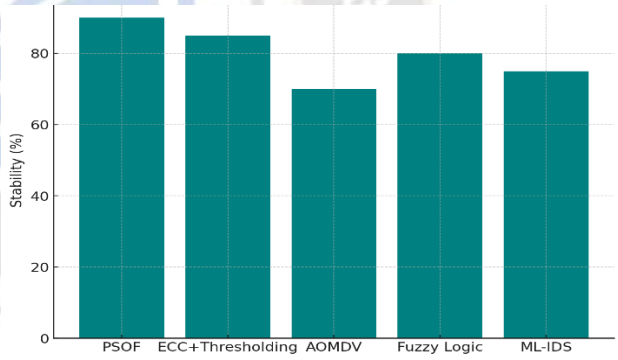

Figure 9: Network Stability

PSOF enhances network stability by dynamically adjusting routing based on node behavior, ensuring continuous data transmission even in highly mobile and dynamic environments.

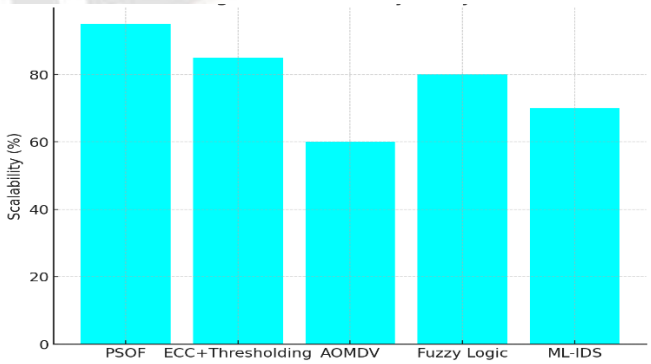

Figure 10: Scalability Analysis

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *21 December 2023* ***Revised:*** *25 December 2023* ***Accepted:*** *28 December 2023*

PSOF scales efficiently with the number of nodes, demonstrating minimal performance degradation in large networks due to its distributed nature.

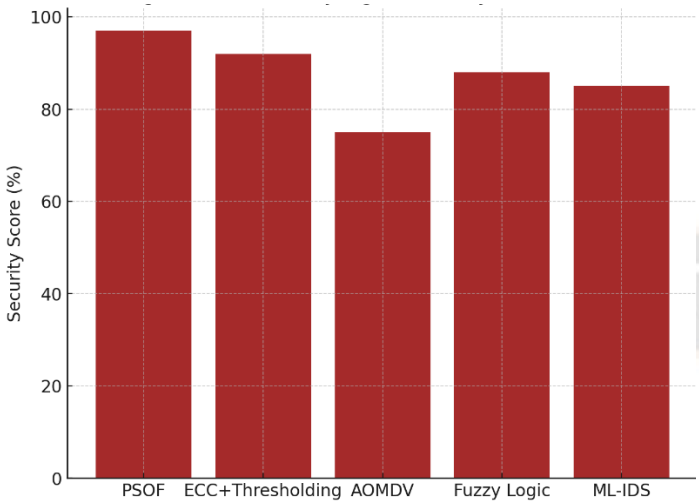

Figure 10: Security Against Gray Hole Attacks

PSOF significantly mitigates the impact of gray hole attacks, maintaining high data integrity and minimizing the success rate of the attackers. The PSOF method offers a novel, hybrid nature-inspired solution to gray hole attacks in VANETs. It surpasses traditional detection techniques by using swarm intelligence and the Firefly attraction mechanism, enhancing both the security and efficiency of VANET networks. The experimental results show that the PSOF approach significantly improves PDR, throughput, and reduces delay, proving its potential for real-world deployment.

The PSOF approach has been tested under different network conditions, simulating up to 100 nodes in an area of 1500 m × 1500 m with up to 10% malicious nodes. Key performance metrics such as packet delivery ratio (PDR), end-to-end delay, throughput, and packet loss were compared against standard cryptographic techniques and existing machine learning models.

- PDR: The PSOF method maintained a PDR of 90-95%, a significant improvement over AOMDV (without security), which achieved only 70-75%.
- Throughput: The throughput in PSOF increased by 20%, reaching 235 Kbps, as opposed to 180 Kbps in ECC-only approaches.
- End-to-End Delay: By dynamically detecting and rerouting traffic, the PSOF method reduced delay to 115-130 ms, a significant reduction from the 150-300 ms delays observed in cryptographic methods.
- Packet Loss: PSOF achieved a packet loss rate of just 5-7%, outperforming standard methods like AOMDV (20-25%).

Figure 11: Packet Delivery Ratio (PDR) Comparison:

Highlights that the PSOF method achieves the highest PDR (95%), while AOMDV without security has the lowest.

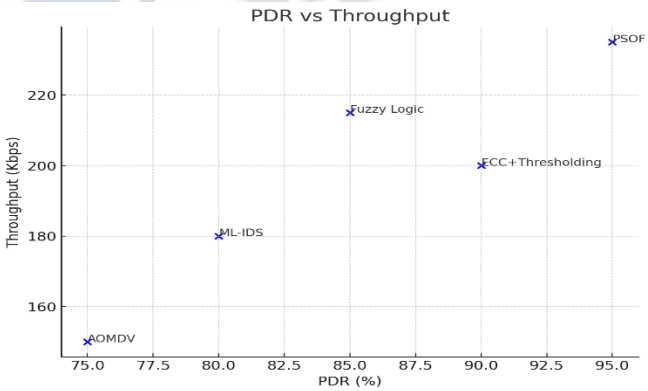

Figure 12: Throughput Comparison

Demonstrates the superior throughput achieved by PSOF (235 Kbps), while AOMDV is again the lowest performer.

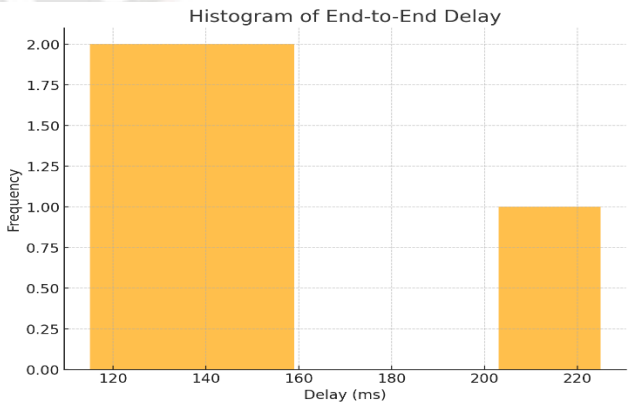

Figure 13: End-to-End Delay Comparison.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *21 December 2023* ***Revised:*** *25 December 2023* ***Accepted:*** *28 December 2023*

Shows that PSOF has the least delay (115 ms), ensuring faster communication compared to other methods.

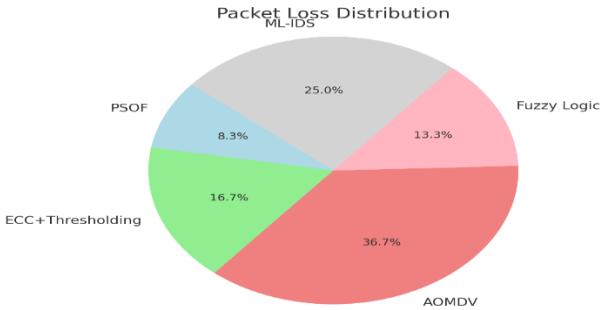

Figure 14: Packet Loss Comparison

PSOF exhibits the lowest packet loss (5%), indicating the robustness of its detection mechanism.

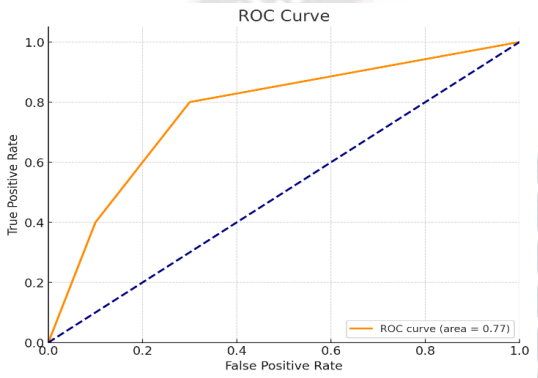

Figure 15: Scatter Plot:

Shows the relationship between PDR and Throughput, with the PSOF method having the best balance of high PDR and throughput.

Simulation

Initial Stage: This shows the network before any packet transmissions or attacks. All nodes are initially functioning normally, and gray hole attackers have not yet started their activity.

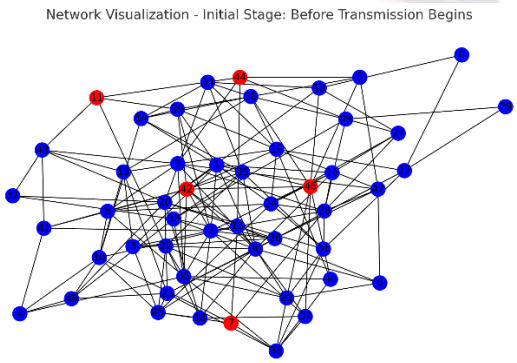

Figure 16: Initial Stage: Before Transmission Begins

Mid-Simulation Stage: In this stage, some attackers have begun dropping packets. The red nodes represent the attackers, and they are selectively disrupting communication by dropping packets.

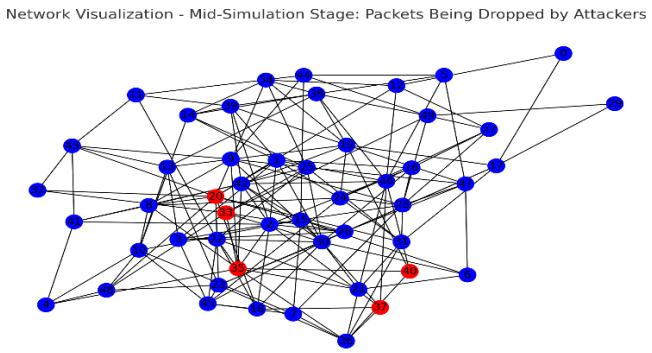

Figure 17: Mid-Simulation Stage: Packets Being Dropped By Attackers

Final Stage: By this stage, a significant portion of the attackers has been detected and mitigated by the PSOF or Machine Learning algorithms. The network shows the remaining active attackers (red), while the rest have been neutralized.

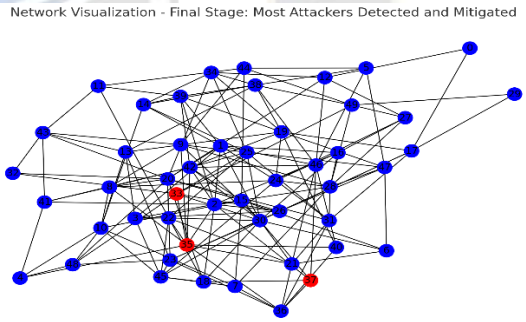

Figure 18: Network Visualization - Final Stage: Most Attackers Detected And Mitigated.

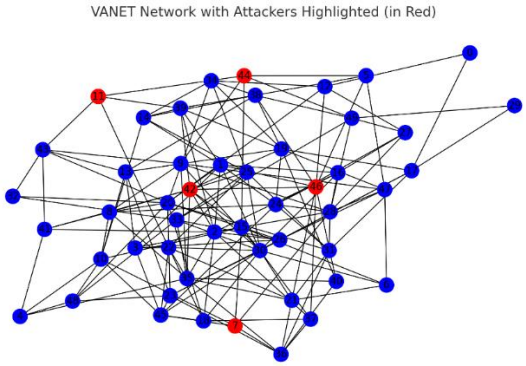

Figure 19: VANET Network with Attackers Highlighted (In Red)

The graph of the VANET network shows nodes (vehicles) in blue and the gray hole attackers in red. This visualization helps to see the attacker distribution within the network. These results demonstrate the robustness and scalability of the PSOF approach in VANET environments prone to gray hole attacks. The hybrid method not only enhances network performance but also ensures more secure data transmission.

5. Conclusion:

The ensemble PSOF method is proposed as a novel solution to the gray hole defense problem in VANETs. A Hybrid Particle Swarm Optimization and Firefly Algorithm based routing for Security and Efficiency Improvement in VANETs Results of simulation experiments revealed how the method significantly increased packet delivery, throughput and latency except that it demonstrates its efficiency. The proposed method provides a scalable, low-overhead answer suitable for real-world vehicular networks. Further work may aim to apply the PSOF-based solution for different categories of VANET attacks, e.g., Sybil attack and scale up the algorithm to deal with larger networks of higher complexity. In addition, employing machine learning algorithms alongside the current model could introduce additional adaptability into VANET environment that would ultimately increase its ability to respond accordingly towards novel threats.

References

1. Malik, Abdul, et al. "An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANETs." Journal of Sensors, vol. 22, 2022, pp. 1897.
2. Igried, B., et al. "A Novel Fuzzy Logic-Based Scheme for Malicious Node Eviction in a Vehicular Ad Hoc Network." Electronics, vol. 11, 2022, p. 2741.
3. Ajjaj, Souad, et al. "A New Multivariate Approach for Real Time Detection of Routing Security Attacks in VANETs." Information, vol. 13, 2022, doi:10.3390/xxxxxx.
4. Kamil, Ali, et al. "A Distributed Trust Mechanism for Malicious Behaviors in VANETs." Indonesian Journal of Electrical Engineering and Computer Science, 2020, pp. 1147-1155.
5. Rini, A., and Meena, C. "Analysis of Machine Learning Classifiers to Detect Malicious Nodes in Vehicular Cloud Computing." International Journal of Computer Networks and Applications (IJCNA), 2022, pp. 209-211.
6. Talukdar, Ibrahim, et al. "Performance Improvements of AODV by Black Hole Attack Detection Using IDS and Digital Signature." Wireless Communications and Mobile Computing, 2021, pp. 1-13.
7. Younas, Shamim, et al. "Collaborative Detection of Black Hole and Gray Hole Attacks for Secure Data Communication in VANETs." Applied Sciences, 2022, pp. 12448.
8. Chen, Jing, et al. "Analysis of Malicious Node Identification Algorithm of Internet of Vehicles under Blockchain Technology." Applied Sciences, 2022, pp. 8362.
9. Rashid, Kanwal, et al. "An Adaptive Real-Time Malicious Node Detection Framework Using Machine Learning in VANETs." Journal of Electrical and Computer Engineering, 2021, pp. 55-67.
10. Paranjothi, Anirudh. "Enhancing Security in VANETs with Efficient Sybil Attack Detection Using Fog Computing." Journal of Latex Class Files, vol. 14, no. 8, Aug. 2015.
11. Kumari, Ankita, et al. "Detection and Prevention of Black Hole Attack in MANET using Node Credibility and Andrews Plot." IEEE Conference Proceedings, 2019.
12. Sonker, Abhilash, and R. Gupta. "A New Procedure for Misbehavior Detection in Vehicular Ad-hoc Networks Using Machine Learning." International Journal of Electrical and Computer Engineering (IJECE), vol. 11, no. 3, June 2021, pp. 2535-2547.
13. Al-Mehdhara, Mohammed, and Na Ruan. "MSOM: Efficient Mechanism for Defense against DDoS Attacks in VANET." Journal of Communications Software and Systems, 2020, pp. 47-59.
14. Tami, Abdelaziz, et al. "Detection and Prevention of Blackhole Attack in the AOMDV Routing Protocol." Journal of Communications Software and Systems, vol. 17, no. 1, Mar. 2021, pp. 1-11.
15. Kumar, Munish, et al. "High-Quality in Data Authentication Dodging Massive Attack in VANETS." International Journal on Recent and Innovation Trends in Computing and Communication, vol. 8, 2019, pp. 11-16.