ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03(04), April 2024, pp. 31-40

Article Title: Enhancement of VANETS Security against Gray Hole Attack with ANFIS-GWO and LBK

Enhancement of VANETS Security against Gray Hole Attack with ANFIS-GWO and LBK

A. T. R. Krishna Priya

PG Scholar, Department of Computer Science and Engineering, Rohini College of Engineering and Technology, Kanyakumari, Tamilnadu, India, priya.gita6@gmail.com

ABSTRACT

Vehicular Ad-Hoc Networks (VANETs) have emerged as a critical component of intelligent transportation systems, facilitating real-time communication among vehicles and infrastructure. However, the open and dynamic nature of VANETs makes them vulnerable to various security threats, among which gray hole attacks pose significant challenges. In gray hole attacks, malicious nodes manipulate or selectively drop data packets, disrupting communication and compromising network integrity. In response to these challenges, this paper proposes an innovative approach that integrates the Adaptive Neuro-Fuzzy Inference System (ANFIS) with Grey Wolf Optimization (GWO). The main objective of this research is to develop a robust ANFIS-GWO framework capable of identifying and mitigating gray hole attacks in real-time VANET scenarios. Through extensive simulations and experiments, the performance of proposed technique in terms of average energy consumed, throughput, Packet Delivery Ratio (PDR) and packet drop is examined. The results demonstrate that the ANFIS-GWO approach not only improves the resilience of VANETs against gray hole attacks but also guarantees reliable and secure communication among vehicles and infrastructure.

Keywords: VANET, Gray Hole Attack, ANFIS-GWO, Security, Network Integrity.

1 Introduction

VANETs represent a specialized form of ad hoc networks where moving vehicles (shown in Figure 1) and fixed Road Side Units (RSUs) connect wirelessly to ensure safe and secure traffic environments [1, 2]. These networks are increasingly adopted due to their practicality, accessibility, and adaptability. Modern vehicles are now equipped with onboard sensors that facilitate communication among themselves, leveraging VANETs to enhance safety, manage traffic and fleets, and provide entertainment services [3]. This technology finds diverse applications across various domains.

In VANETs, each vehicle is equipped with an On-Board Unit (OBU) responsible for gathering, analyzing, and transmitting data to nearby vehicles. Road Side Units (RSUs) installed along roadsides facilitate communication among vehicles, infrastructure, and a Trusted Authority (TA) [4, 5]. The TA acts as a registration unit overseeing OBUs, RSUs, and vehicle users within the VANET system. Integral to Intelligent Transportation Systems (ITS), VANETs provide real-time, critical information to drivers and traffic authorities. Another essential

component of ITS is the Internet of Things (IoT), which extends traditional VANETs into the Internet of Vehicles (IoV). This transformation enhances data collection and sharing capabilities across infrastructures, vehicles, people, and road conditions [6].

Gray hole attack involves a malicious node selectively dropping some packets while forwarding others, making detection more challenging because the node appears to behave normally most of the time [7]. These attacks disrupt communication and compromise the reliability of the network. Therefore, there is a crucial need for a method that effectively detect and prevent such malicious activities to enhance the security and efficiency of VANET.

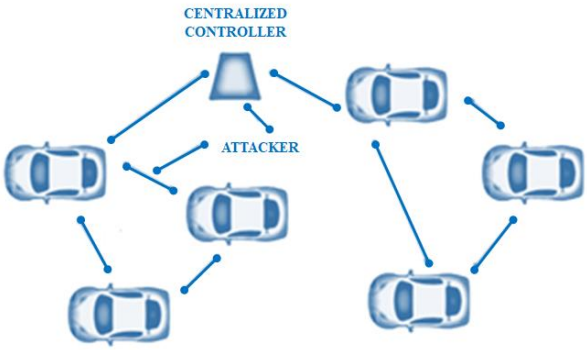

Figure 1: *VANET Architecture*

In VANETs, three primary types of routing techniques are employed: pre-emptive, reactive, and hybrid. Among these, the Ad hoc On-Demand Distance Vector (AODV) routing protocol [8] is particularly noteworthy due to its high performance and low latency. AODV is frequently utilized in the transmission of external messages for autonomous vehicles. One of the key advantages of AODV is its use of sequence numbers, which enhances its effectiveness compared to other routing protocols [9].

In the context of autonomous and semi-autonomous vehicles, ensuring the security of message and vehicle authentication in cooperative vehicular ad hoc systems is critical [10, 11]. Traditional security measures, such as encryption and decryption methods, are effective in preventing external attacks aimed at stealing sensitive data and intercepting communications between roadside units and autonomous vehicles [12]. However, these methods often fall short in protecting against internal threats. Each layer of a VANET is vulnerable to various attacks, making the overall protection of the network a significant challenge [13]. This vulnerability highlights the need for robust security measures to secure both internal and external communications within VANETs.

To address the issues in VANETs, Deep Neural Network (DNN) [14] model is proposed for detection, a deep learning technique capable of analyzing complex data patterns and distinguish between normal and malicious network behavior [15]. However, implementing DNNs in VANETs also has its drawbacks including computational complexity and resource demands of

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03(04), April 2024, pp. 31-40

DNNs, which may not be feasible for all vehicular units due to limited processing power and storage capacity.

Addressing the issues of security in VANETs, in existing literatures the proposed work adds benefit by

- Implementing LBK to prevent gray hole attacks by ensuring that only authorized nodes within a specific geographic area can decrypt and access the transmitted data.
- Introducing ANFIS-GWO enhances the system's ability to detect anomalies and malicious activities with high accuracy.
- The combined use of ANFIS-GWO and LBK optimizes the utilization of network resources, reduces computational burden, and improves energy efficiency. This leads to higher PDRs, reduced packet drop rates, and overall improved network performance.

The rest of paper is organized by proposed methodology in Section 2, followed by results and discussion in Section 3 and finally conclusion in Section 4.

2 Proposed Methodology

The conceptual framework for enhancing packet delivery in a network, as illustrated in Figure 2, begins with input packet data entering the system and being processed by the source node. This node encrypts the data using LBK encryption. The encrypted data is then split into two paths: packet transmission, which directly transmits the packets, and packet forwarding, which sends packets to intermediate nodes. This dual-path approach ensures an enhanced PDR and minimizes packet drop, leading to efficient delivery of packets to the destination node. Upon receiving the packets, the destination node decrypts them using LBK decryption, making the decrypted data available as output.

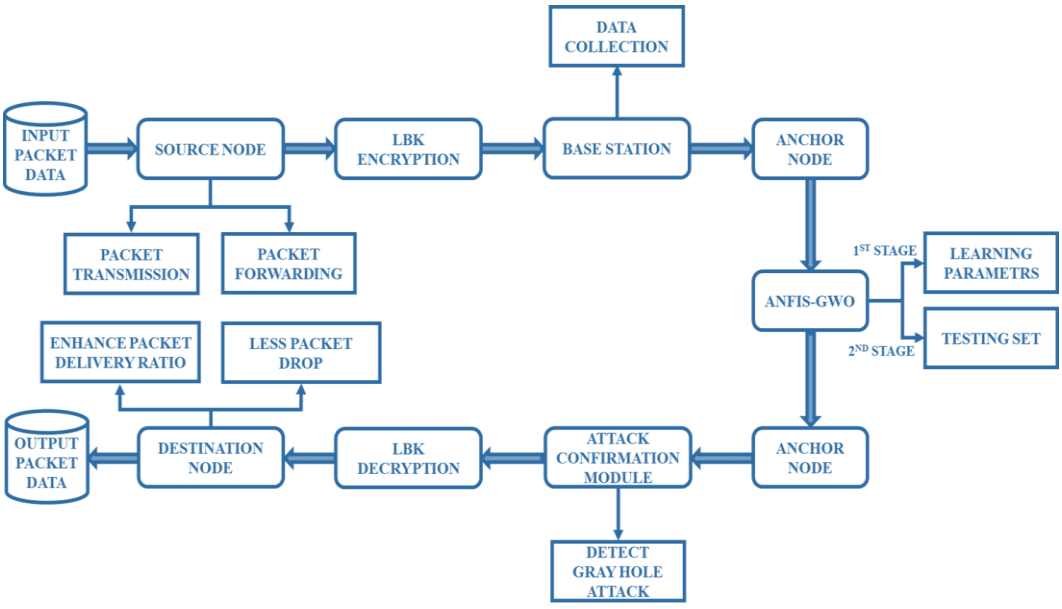

Figure 2: *Proposed System Architecture*

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03(04), April 2024, pp. 31-40

Article Title: Enhancement of VANETS Security against Gray Hole Attack with ANFIS-GWO and LBK

Simultaneously, a base station collects data for further analysis, while an anchor node plays a critical role in attack detection and confirmation. The anchor node employs an ANFIS-GWO, which operates in two stages: the first stage utilizes learning parameters, and the second stage applies these parameters to a testing set. An attack confirmation module verifies the presence of attacks, specifically detecting and confirming gray hole attacks. This comprehensive workflow ensures secure packet data transmission through encryption, optimizes delivery, and maintains network integrity by effectively identifying and mitigating gray hole attacks.

Encryption and decryption are essential for securing data transmission in networks. They ensure that sensitive information remains confidential and is protected from unauthorized access and potential attacks. LBK encryption and decryption is a process designed to enhance the security of data transmission in networks by tying encryption keys to specific geographic locations.

2.1 LBK Encryption Process

The process begins with the initial data packets entering the system, where a unique encryption key is generated based on the location of the source node. This location-based approach ensures that keys are context-specific, enhancing security by limiting the key's. The process is illustrated in Figure 3. The encryption algorithm then uses this location-based key to transform the plain text data into cipher text, making it unreadable to unauthorized entities. The encrypted data is transmitted securely over the network as cipher text.

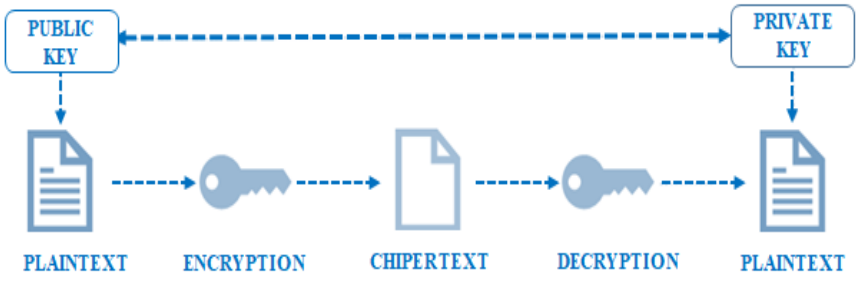

Figure 3: *LBK Based Encryption and Decryption*

2.2 LBK Decryption Process

Upon reception, the destination node, uses this key to apply the decryption algorithm to the cipher text. This process reverses the encryption, converting the cipher text back into its original plain text form. The decrypted data is then available for use by the destination node, with its integrity and confidentiality preserved throughout the transmission. LBK encryption and decryption add an additional layer of security by ensuring that even if data is intercepted, it remains secure unless the attacker is in the correct location and possesses the appropriate key.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03(04), April 2024, pp. 31-40

2.3 Attack Detection and Mitigation using ANFIS-GWO

The proposed research utilizes the combination of ANFIS and GWO to enhance security and efficiency in VANETs. This integration addresses the dynamic and complex nature of VANETs by providing a robust mechanism for attack detection and parameter optimization. Figure 4 represents the flow representation of ANFIS-GWO. The ANFIS is a hybrid intelligent system that merges the advantages of neural networks and fuzzy logic, utilizing the learning capability of neural networks to optimize fuzzy inference system parameters. This enables effective handling of uncertainties and nonlinearities in data. The ANFIS architecture consists of a multi-layer feed forward neural network structure where each layer represents a specific fuzzy logic operation. The key layers include the input layer (nodes representing input variables), fuzzification layer (nodes that map input variables to fuzzy sets using membership functions), rule layer (nodes representing fuzzy rules), normalization layer (nodes that normalize the output of fuzzy rules), and the output layer (nodes that generate the final output using defuzzification). ANFIS uses a hybrid learning algorithm combining gradient descent and least squares estimation to adjust the membership function parameters, allowing it to learn effectively from input-output data pairs.

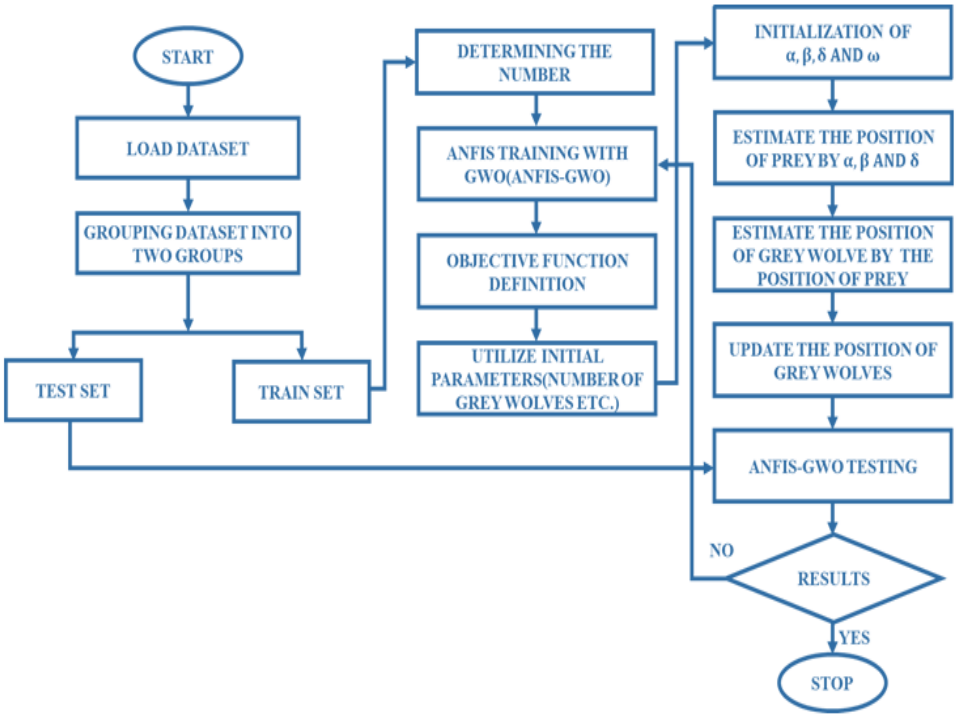

Figure 4: *Flow Chart Illustration of ANFIS-GWO*

To optimize ANFIS parameters in attack detection, GWO a swarm intelligence-based optimization algorithm inspired by the social hierarchy and hunting behavior of grey wolves is

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03(04), April 2024, pp. 31-40

utilized. The optimization process in GWO models the leadership hierarchy into four types of wolves: alpha, beta, delta, and omega. It involves initializing a population of wolves (candidate solutions) randomly and updating their positions based on alpha (best solution), beta, and delta wolves. GWO balances exploration (searching new areas) and exploitation (fine-tuning current solutions) phases to effectively navigate the solution space. In the tuning process of ANFIS, GWO fine-tunes the membership functions and fuzzy rules, ensuring that the system parameters are optimized for accurate attack detection. By effectively detecting and mitigating gray hole attacks, ANFIS-GWO helps maintain a high PDR, reduces the packet drop rate and ensuring more reliable and efficient data transmission across VANET.

3 Results and Discussion

The implementation and validation of the proposed framework is carried out using Ubuntu as the operating system and Network Simulator 2 (NS2) for simulation. The Tool Command Language (TCL) is employed for scripting within the NS2 environment, facilitating the design and execution of the network scenarios.

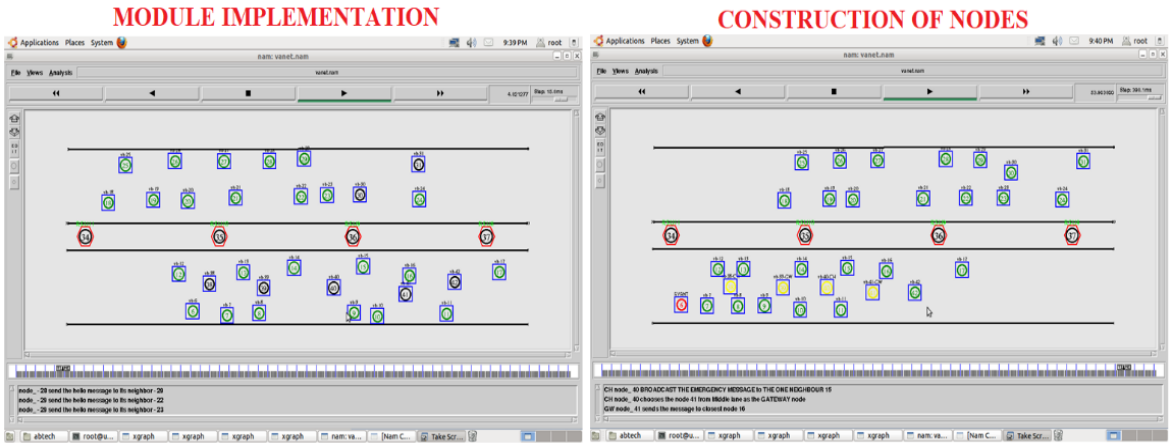

Figure 5: *Module Implementation and Construction of Nodes in the Network Simulation Environment*

The Figure 5 demonstrates the network simulation setup using NS2 in Ubuntu. The implementation module shows the deployment of various network modules, highlighting the interaction between source, destination, and intermediate nodes. It reflects the integration of LBK encryption and ANFIS-GWO attack detection. The construction of nodes illustrates the arrangement and connectivity of nodes within the network, depicting the overall network topology essential for simulating secure and efficient packet delivery.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03(04), April 2024, pp. 31-40

Article Title: **Enhancement of VANETS Security against Gray Hole Attack with ANFIS-GWO and LBK**

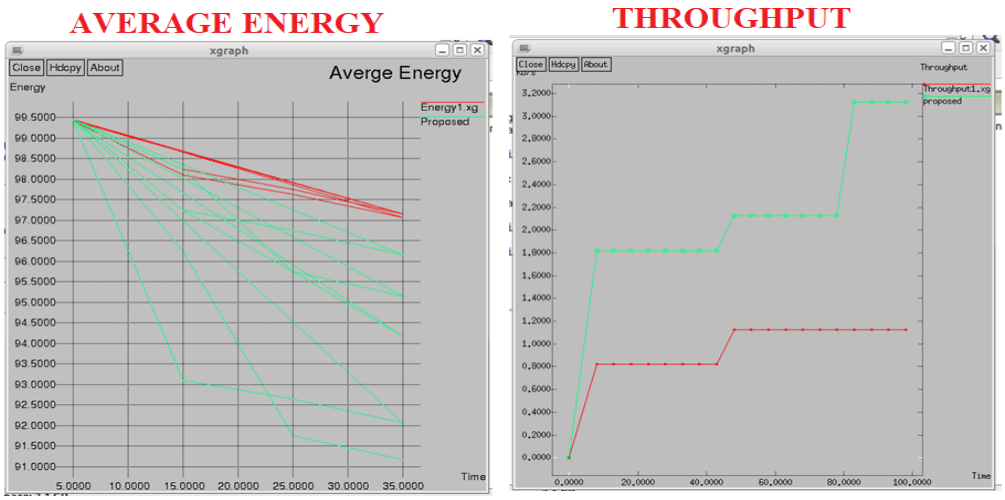

Figure 6: *Average Energy Consumption and Throughput Analysis*

The average energy and the throughput analysis is illustrated in Figure 6 for the proposed method compared to baseline. It is observed that the proposed method shows a significantly reduced and more stable average energy level, indicating efficient energy utilization. Similarly, higher throughput is accomplished utilizing the ANFIS-GWO approach, highlighting its effectiveness in delivering more data packets successfully over the network within the same time frame.

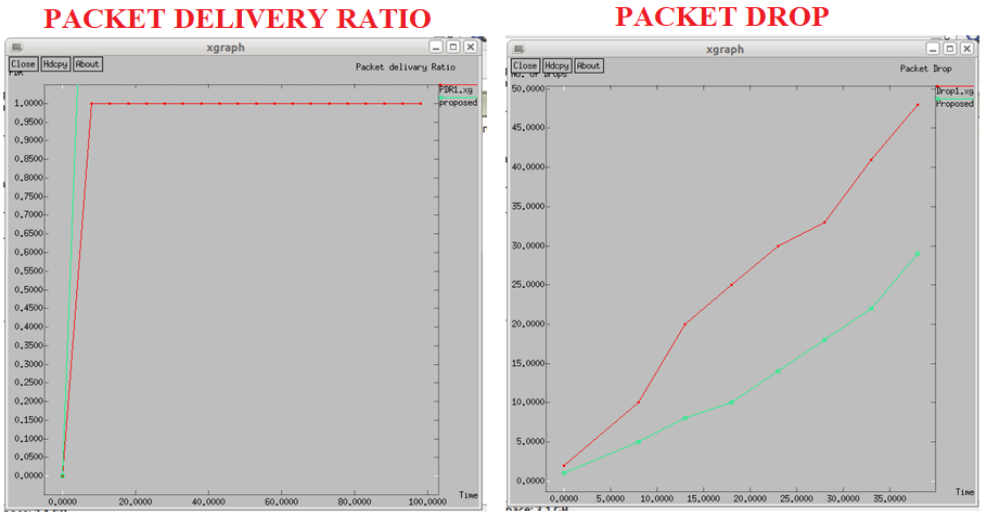

Figure 7: *Analysis of PDR and Packet Drop*

This Figure 7 provides a comparative analysis of PDR and packet drop rate for the proposed framework against a baseline network configuration. The proposed method achieves a near-perfect PDR, indicating that almost all transmitted packets successfully reach their destination. Moreover, the proposed ANFIS-GWO results with significantly lower packet drop rate, demonstrating its effectiveness in minimizing packet loss during transmission.

Table 1: *Comparison of Performance Measure*

Parameter	Existing System	Proposed System
Throughput (Mbps)	10	30
PDR (%)	5	20
Packet Drop (%)	50	25

Comparative analysis for performance metrics is listed in Table 1, highlighting the performance of proposed system over the existing system. It is noticed that, the proposed system results with better outcomes revealing higher throughput, reduced packet drop and higher packet delivery ratio.

4 Conclusion

The paper presents a novel approach for enhancing the performance of VANETs by integrating LBK with ANFIS-GWO attack detection. The proposed ANFIS-GWO model effectively detects gray hole attacks by using aptive learning and optimization techniques, thereby providing high accuracy and real-time adaptability in identifying malicious activities. The LBK method adds an extra layer of security by adding encryption keys to specific geographic locations, which helps in preventing unauthorized access and mitigates internal and external threats. The integration of these methodologies not only enhances the detection and prevention of attacks but also optimizes resource utilization, reduces computational burden, and improves overall network performance. The findings indicate that this combined approach significantly increases packet delivery ratios, reduces packet drop rates, and ensures secure data transmission, making VANETs more reliable and robust against sophisticated attacks. These advancements mark a significant step forward in securing vehicular networks and paves the way for safer and more efficient autonomous vehicle communication systems.

References

1. Alireza Aghabagherloo; Mahshid Delavar; Javad Mohajeri; Mahmoud Salmasizadeh; Bart Preneel, Year: 2022, “An efficient and physically secure privacy-preserving authentication scheme for Vehicular Ad-hoc NETworks (VANETs)”, IEEE Access, Vol: 10, pp. 93831-93844.

2. Pooja Rani; Sahil Verma; Gia Nhu Nguyen, Year: 2020, “Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network”, IEEE access, Vol: 8, pp. 121755-121764.

3. Zohaib Hassan; Amjad Mehmood; Carsten Maple; Muhammad Altaf Khan; Abdulaziz Aldegheishem, Year: 2020, “Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles”, IEEE Access, Vol: 8, pp. 199618-199628.

4. Muhammad Haleem Junejo; Ab Al-Hadi Ab Rahman; Riaz Ahmed Shaikh; Kamaludin Mohamad Yusof; Imran Memon; Hadiqua Fazal; Dileep Kumar, Year: 2020, "A privacy-preserving attack-resistant trust model for internet of vehicles ad hoc networks", Scientific Programming, no: 1, pp. 8831611.

5. Mohammed Ahmed Jubair; Salama A. Mostafa; Dilovan Asaad Zebari; Hussein Muhee Hariz; Nejood Faisal Abdulsattar; Mustafa Hamid Hassan; Ali Hashim Abbas; Fatima Hashim Abbas; Areej Alasiry; M. Turki-Hadj Alouane, Year: 2022, "A QoS aware cluster head selection and hybrid cryptography routing protocol for enhancing efficiency and security of VANETs", IEEE Access, Vol: 10, pp. 124792-124804.

6. Seyed Salar Sefati; Sara Ghiasi Tabrizi, Year: 2022, "Detecting sybil attack in vehicular ad-hoc networks (vanets) by using fitness function, signal strength index and throughput", Wireless Personal Communications, Vol: 123, no: 3, pp. 2699-2719.

7. Shamim Younas; Faisal Rehman; Tahir Maqsood; Saad Mustafa; Adnan Akhunzada; Abdullah Gani, Year: 2022, "Collaborative detection of black hole and gray hole attacks for secure data communication in VANETs", Applied Sciences, Vol: 12, no: 23, pp. 12448.

8. Yangfan Liang; Entao Luo; Yining Liu, Year: 2023, "Physically secure and conditional-privacy authenticated key agreement for VANETs", IEEE Transactions on Vehicular Technology, Vol: 72, no: 6, pp. 7914-7925.

9. Mahmood Ul Hassan; Amin A. Al-Awady; Abid Ali Sifatullah; Muhammad Akram; Muhammad Munwar Iqbal; Jahangir Khan; Yahya Ali Abdelrahman Ali, Year: 2024, "ANN-Based Intelligent Secure Routing Protocol in Vehicular Ad Hoc Networks (VANETs) Using Enhanced AODV", Sensors, Vol: 24, no: 3, pp. 818.

10. Sandeep Gupta; Carsten Maple; Roberto Passerone, "An investigation of cyber-attacks and security mechanisms for connected and autonomous vehicles", IEEE Access.

11. Callum Brocklehurst; Milena Radenkovic, Year: 2022, "Resistance to cybersecurity attacks in a novel network for autonomous vehicles." Journal of Sensor and Actuator Networks, Vol: 11, no: 3, pp. 35.

12. Abdul Malik; Muhammad Zahid Khan; Saeed Mian Qaisar; Mohammad Faisal; Gulzar Mehmood, Year: 2023, "An efficient approach for the detection and prevention of gray-hole attacks in VANETs", IEEE Access, Vol: 11, pp. 46691-46706.

14. Devaj Ramsamooj; Prinkle Sharma; Hong Liu, Year: 2024, "GenVRAM: Dataset Generator for Vehicle to Roadside Attacks and Misbehavior", IEEE Access.

14. Amalia Amalia; Yushintia Pramitarini; Ridho Hendra Yoga Perdana; Kyusung Shim; Beongku An, Year: 2023, "A deep-learning-based secure routing protocol to avoid blackhole attacks in VANETs", Sensors, Vol: 23, no: 19, pp. 8224.

15. Kanwal Rashid; Yousaf Saeed; Abid Ali; Faisal Jamil; Reem Alkanhel; Ammar Muthanna, Year: 2023, "An adaptive real-time malicious node detection framework using machine learning in vehicular ad-hoc networks (VANETs)", Sensors, Vol: 23, no: 5, pp. 2594.