BIBLIOGRAPHY

Abdelfatah, R.I., Abdal-Ghafour, N.M. and Nasr, M.E., 2021. Secure VANET authentication protocol (SVAP) using Chebyshev chaotic maps for emergency conditions. IEEE Access, 10, pp.1096-1115.

Abdelkader Abbassi et al., (2021). "Improved off- grid wind/photovoltaic/hybrid energy storage system based on new framework of Moth- Flame optimization algorithm", International Journal of Energy Research, 2021.

Abdueli Paulo Mdee., Malik Muhammad Saad., Murad Khan., Muhammad Toaha Raza Khan., Dongkyun Kim. 2022. Impacts of location-privacy preserving schemes on vehicular applications. Vehicular Communications. Volume 36, August 2022, 100499

Aghabagherloo, A., Delavar, M., Mohajeri, J., Salmasizadeh, M. and Preneel, B., 2022. An efficient and physically secure privacy-preserving authentication scheme for Vehicular Ad-hoc NETworks (VANETs). Ieee Access, 10, pp.93831-93844.

Akhter, A.S., Ahmed, M., Shah, A.S., Anwar, A. and Zengin, A., 2021. A secured privacy-preserving multi-level blockchain framework for cluster based VANET. *Sustainability*, *13*(1), p.400.

Aldhaheri et.al., (2020). Deepdca: novel network-based detection of iot attacks using artificial immune system. Applied Sciences, 10(6), p.1909.

Alfadhli, S.A., Lu, S., Chen, K. and Sebai, M. 2020 Mfspv: A multi-factor secured and lightweight privacy-preserving authentication scheme for VANET. IEEE Access, Vol 8, pp.142858-142874.

Alharthi, A., Ni, Q. and Jiang, R., 2021. A privacy-preservation framework based on biometrics blockchain (BBC) to prevent attacks in VANET. Ieee Access, 9, pp.87299-87309.

Almaraz-Rivera, J.G., Perez-Diaz, J.A. and Cantoral-Ceballos, J.A., 2022. Transport and application layer DDoS attacks detection to IoT devices by using machine learning and deep learning models. *Sensors*, *22*(9), p.3367.

Al-Shareeda, M.A. and Manickam, S., 2022. MSR-DoS: Modular square root-based scheme to resist denial of service (DoS) attacks in 5G-enabled vehicular networks. IEEE Access, 10, pp.120606-120615.

Al-Shareeda, M.A., Anbar, M., Manickam, S. and Hasbullah, I.H., 2020. Review of prevention schemes for man-in-the-middle (MITM) attack in vehicular ad hoc networks. International Journal of Engineering and Management Research, 10.

Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. 2021. SE-CPPA: A Secure and Efficient Conditional Privacy-Preserving Authentication Scheme in Vehicular Ad-Hoc Networks. Sensors 2021, 21, 8206. https://doi.org/10.3390/s21248206.

Amandeep Verma, Rahul Saha, Gulshan Kumar, Tai-hoon Kim. (2021). The Security Perspectives of Vehicular Networks: A Taxonomical Analysis of Attacks and Solutions, Appl. Sci. 2021, 11, 4682. https://doi.org/10.3390/app11104682.

Amit Kumar Singh, Rajendra Pamula., (2021). Vehicular Delay Tolerant Network Based Communication Using Machine Learning Classifiers. In book: Architectural Wireless Networks Solutions and Security Issues (pp.195-208)

Anurag Tiwari, Manuj Darbari. "Emerging Trends in Computer Science and Its Application - Proceedings of the International Conference on Advances in Emerging Trends in Computer Applications (ICAETC-2023), December 21–22, 2023, Lucknow, India", CRC Press, 2025.

Anyanwu, G.O., Nwakanma, C.I., Lee, J.M. and Kim, D.S., 2022. Optimization of RBF-SVM Kernel using Grid Search Algorithm for DDoS Attack Detection in SDN-based VANET. IEEE Internet of Things Journal.

Azam, S., Bibi, M., Riaz, R., Rizvi, S.S. and Kwon, S.J., 2022. Collaborative learning based sybil attack detection in vehicular ad-hoc networks (vanets). Sensors, 22(18), p.6934.

Bala, K., Upadhyay, R., Anwar, S.R. and Shrimal, G., 2023. A blockchain-enabled, trust and location dependent-Privacy preserving system in VANET. Measurement: Sensors, 30, p.100892.

Bangui, H., Ge, M. and Buhnova, B., 2022. A hybrid machine learning model for intrusion detection in VANET. Computing, 104(3), pp.503-531.

Bayat, M., Pournaghi, M., Rahimi, M. and Barmshoory, M. 2020 NERA: A new and efficient RSU based authentication scheme for VANET. Wireless networks, 26, pp.3083-3098. https://doi.org/10.1007/s11276-019-02039-x.

Bindu, G. and Karthika, R.A. 2020 Design of High Secured Multi Scroll Attractor Based Henon Map Chaotic Encryption Scheme for VANET Communication. Journal of Engg. Research, ICETET Special Issue, DOI: 10.36909/jer.ICETET.14973.

Gad, A.R., Nashat, A.A. and Barkat, T.M., 2021. Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset. IEEE Access, 9, pp.142206-142217.

Gaurav, A., Gupta, B.B., Peñalvo, F.J.G., Nedjah, N. and Psannis, K., 2022. Ddos attack detection in vehicular ad-hoc network (vanet) for 5g networks. In Security and Privacy Preserving for IoT and 5G Networks (pp. 263-278).

Gonçalves, F.; Macedo, J.; Santos, A. 2021. An Intelligent Hierarchical Security Framework for VANETs. Information 2021, 12, 455. https:// doi.org/10.3390/info12110455.

Goyal, A., Bhatia, A., Yadav, A. and Sharma, D.K., 2023, January. Misbehavior Detection in Cooperative Intelligent Transportation Systems using Temporal Fusion Transformer. 24th International Conference on Distributed Computing and Networking (pp. 431-437).

Jabar Mahmood, Zongtao Duan ,YunYang , Qinglong Wang , Jamel Nebhen , and Muhammad Nasir Mumtaz Bhutta., 2021. Security in Vehicular Ad Hoc Networks: Challenges and Countermeasures, Hindawi Security and Communication Networks, Volume 2021, Article ID 9997771, https://doi.org/10.1155/2021/9997771.

Jabar Mahmood, Zongtao Duan, Yun Yang, Qinglong Wang, Jamel Nebhenand Muhammad Nasir Mumtaz Bhutta.,2021. Security in Vehicular Ad Hoc Networks: Challenges and Countermeasures. Security and Communication Networks, Volume 2021 | Article ID 9997771.

Jagriti and Lobiyal, D.K., 2022. An efficient self-organized traffic maintenance scheme employing positive selection algorithm. Multimedia Tools and Applications, 81(23), pp.33107-33125.

Jamaesha, S.S., Gowtham, M.S. and Ramkumar, M., 2024. Deep Artificial Immune System With Malicious Node Detection and Secure Routing Protocol in MANET. Transactions on Emerging Telecommunications Technologies, 35(11), p.e70008.

Jim, L.E., Islam, N. and Gregory, M.A., 2022. Enhanced MANET security using artificial immune system based danger theory to detect selfish nodes. Computers & Security, 113, p.102538.

Kadam, N. and Krovi, R.S., 2021. Machine learning approach of hybrid KSVN algorithm to detect DDoS attack in VANET. International Journal of Advanced Computer Science and Applications, 12(7).

Kathole, A.B., Lonare, S., Katti, J., Vhatkar, K. and Dharmale, G., 2025. Efficient fuzzy ranking with ensemble machine learning network for attack detection and classification in VANET. Expert Systems with Applications, 279, p.127295.

Kaur, G. and Kakkar, D., 2025. A secure lightweight authentication model with interference aware routing and attack detection approach in VANET. Cluster Computing, 28(2), p.109.

Kaur, R., Ramachandran, R.K., Doss, R. and Pan, L., 2021. The importance of selecting clustering parameters in VANET: A survey. Computer Science Review, 40, p.100392.

Kolandaisamy, R., Noor, R.M., Kolandaisamy, I., Ahmedy, I., Kiah, M.L.M., Tamil, M.E.M. and Nandy, T., 2021. A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET. Journal of Ambient Intelligence and Humanized Computing, 12(6), pp.6599-6612.

Kumar, R., Khanna, R. and Kumar, S., 2021. Vehicular middleware and heuristic approaches for intelligent transportation system of smart cities. Cognitive Computing for Human-Robot Interaction, Principles and Practices, Cognitive Data Science in Sustainable Computing (pp. 163-175), Academic Press.

Manderna, Ankit, Sushil Kumar, Upasana Dohare, Mohammad Aljaidi, Omprakash Kaiwartya, and Jaime Lloret. 2023. "Vehicular Network Intrusion Detection Using a Cascaded Deep Learning Approach with Multi-Variant Metaheuristic" Sensors 23, no. 21: 8772. https://doi.org/10.3390/s23218772

Muhammet Ali Karabulut, A. F. M. Shahen Shah, HaciIlhan, Al-Sakib Khan Pathan, and Mohammed Atiquzzaman., 2023.Inspecting Vanet from Various Critical Angles – a Systematic Review.Ad Hoc NetworksVolume 150, 1 November 2023, 103281.

N. Nishanth., A Mujeeb., (2021). Modeling and detection of flooding-based denial-of-service attack in wireless ad hoc network using Bayesian inference. IEEE Systems Journal, vol. 15, no. 1, pp. 17-26.

Nandy, T., Idris, M.Y.I., Noor, R.M., Wahab, A.W.A., Bhattacharyya, S., Kolandaisamy, R. and Yahuza, M., 2021. A secure, privacy-preserving, and lightweight authentication scheme for VANETs. IEEE Sensors Journal, 21(18), pp.20998-21011.

Noura Adel Alsulaim, Raghad Abdullah Alolaqi, Reem Yaseen Alhumaidan. (2020) Proposed Solutions to Detect and Prevent DoS Attacks on VANET System, 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), IEEE Xplore, DOI: 10.1109/ICCAIS48893.2020.9096873.

Nova, K., Umaamaheshvari, A., Jacob, S.S., Banu, G., Balaji, M.S.P. and Srithar, S., 2023. Floyd–Warshalls algorithm and modified advanced encryption standard for secured communication in VANET. Measurement: Sensors, 27, p.100796.

Ogundoyin, S.O. 2020 An autonomous lightweight conditional privacy-preserving authentication scheme with provable security for vehicular ad-hoc networks. International Journal of Computers and Applications, 42(2), pp.196-211.

Polat, H., Turkoglu, M. and Polat, O., 2020. Deep network approach with stacked sparse autoencoders in detection of DDoS attacks on SDN- based VANET. IET Communications, 14(22), pp.4089-4100.

Poongodi, M., Hamdi, M., Sharma, A., Ma, M. and Singh, P.K., 2019. DDoS detection mechanism using trust-based evaluation system in VANET. IEEE Access, 7, pp.183532-183544.

Rajkumar, Y. and Kumar, S.S., 2024. An elliptic curve cryptography based certificate-less signature aggregation scheme for efficient authentication in vehicular ad hoc networks. *Wireless Networks*, *30*(1), pp.335-362.

Rama Mercy Sam Sigamani, Padmavathi Ganapathi. "GOF-SLFN- An Intelligent Attack Detection System against Denial of Service (DoS) attacks based on Glow Worm Swarm optimized Single Layer Feed Forward Networks for vehicular Cyber Physical Systems (VCPS)", IOP Conference Series: Materials Science and Engineering, 2020

Sadaf, Memoona, Zafar Iqbal, Abdul Rehman Javed, Irum Saba, Moez Krichen, Sajid Majeed, and Arooj Raza. 2023. "Connected and Automated Vehicles: Infrastructure, Applications, Security, Critical Challenges, and Future Aspects" Technologies 11, no. 5: 117. https://doi.org/10.3390/technologies11050117.

Sadkhan, S.B. and Jabbar, D. 2021, June The Security Challenges with Cognitive Radio Environments for VANET. IEEE International Conference on Communication & Information Technology (ICICT) (pp. 167-173).

Sajini, S., Anita, E.M. and Janet, J., 2023. Improved security of the data communication in VANET environment using ASCII-ECC algorithm. Wireless Personal Communications, 128(2), pp.759-776.

Setia, H., Chhabra, A., Singh, S.K., Kumar, S., Sharma, S., Arya, V., Gupta, B.B. and Wu, J., 2024. Securing the road ahead: Machine learning-driven DDoS attack detection in VANET cloud environments. Cyber Security and Applications, 2, p.100037.

Shawky, M.A., Jabbar, A., Usman, M., Imran, M., Abbasi, Q.H., Ansari, S. and Taha, A., 2023. Efficient blockchain-based group key distribution for secure authentication in VANETs. IEEE Networking Letters, 5(1), pp.64-68.

Shawky, M.A., Usman, M., Flynn, D., Imran, M.A., Abbasi, Q.H., Ansari, S. and Taha, A., 2023. Blockchain-based secret key extraction for efficient and secure authentication in VANETs. Journal of Information Security and Applications, 74, p.103476.

Shayea, G.G., Mohammed, D.A., Abbas, A.H. and Abdulsattar, N.F., 2022. Privacy-aware secure routing through elliptical curve cryptography with optimal RSU distribution in VANETs. Designs, 6(6), p.121.

Shu, J., Zhou, L., Zhang, W., Du, X. and Guizani, M., 2020. Collaborative intrusion detection for VANET: A deep learning-based distributed SDN approach. IEEE Transactions on Intelligent Transportation Systems, 22(7), pp.4519-4530.

Soujanya B K., Farooque Azam., 2024. Ensuring Security and Privacy in VANET: A Comprehensive Survey of Authentication Approaches. Journal of Computer Networks and Communications Volume 2024, Article ID 1818079, 32 pages https://doi.org/10.1155/2024/1818079.

Sripathi Venkata Naga, S.K.; Yesuraj, R.; Munuswamy, S.; Arputharaj, K. A Comprehensive Survey on Certificate-Less Authentication Schemes for Vehicular Ad hoc Networks in Intelligent Transportation Systems. Sensors 2023, 23, 2682. https://doi.org/10.3390/ s23052682.

Sudhakar, R.V., Haritha, P., Krishna B, V., Kalyani, K., Mithra, C., Palanisamy, K.C. and Tayubi, I.A., 2024. An Enhanced Lightweight Secure Authentication and Privacy-Preserving Approach for VANETs. International Journal of Sensors, Wireless Communications and Control.

Taoufik Yeferny and Sofian Hamad., 2020, Vehicular Ad-hoc Networks: Architecture, Applications and Challenges. IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.2.

Tejasvi Alladi, Bhavya Gera, Ayush Agrawal, Vinay Chamola, Fei Richard Yu. 2021 September. DeepADV: A Deep Neural Network Framework for Anomaly Detection in VANET. IEEE Transactions on Vehicular Technology.

Treiber, Martin and Hennecke, Ansgar and Helbing, Dirk , Congested traffic states in empirical observations and microscopic simulations, 2000.

Vamshi Krishna, K. and Ganesh Reddy, K., 2023. Classification of Distributed Denial of Service Attacks in VANET: A Survey. Wireless Personal Communications, 132(2), pp.933-964.

Wang, S., Mao, K., Zhan, F. and Liu, D. 2020 Hybrid conditional privacy-preserving authentication scheme for VANET. Peer-to-Peer Networking and Applications, 13, pp.1600-1615.

Wang, Z., Wang, J., Liu, Y., Yang, X., Qi, F. and Song, W., 2024. Privacy-Preserving Attribute-Based Access Control Scheme with Intrusion Detection and Policy Hiding for Data Sharing in VANET. IEEE Internet of Things Journal.

Zabeeulla, M., Sharma, S.K. and Chauhan, S.P.S., 2023. Design and Modelling of hybrid network security method for increasing security in vehicular ad-hoc network. Measurement: Sensors, 29, p.100878.

Zhang, D., Yu, F.R., Ruizhe, and Lizhu. 2022. Software-Defined Vehicular Networks With Trust Management: A Deep Reinforcement Learning Approach. IEEE Transactions on Intelligent Transportation Systems 23(2):1400-1414.

Avinashilingam Institute for HomeScience and Higher Education for Women
(Deemed to be University Estd. u/s 3 of UGC Act 1956, Category 'A' by MHRD
Re-accredited with A++ Grade by NAAC. CGPA 3.65/4, Category I by UGC
Coimbatore - 641 043, Tamil Nadu, India

Appendix L2

(Item No 5 of Check List) Details of Research Publications

S.No	Article	Journal	Other Details Vol/No/Page No/ Year	Published in UGC-CARE / Scopus Indexed/ Web of Science
1	Encrypted Access Mapping in a Distinctly Routed optimized Immune System to prevent DoS Attack variants in VANET Architecture	International Journal of Computer Network and Information Security	Vol-16 No. 3 8 June 2024	Scopus
2	Self-healing AIS with Entropy Based SVM and Bayesian Aggregate Model for the Prediction and Isolation of malicious Nodes Triggering DoS Attacks in VANET	International Journal of Computer Network and Information Security	Vol. 15 No. 3 8 June 2023	Scopus

*Proof of list of Journals from Internet to be attached along with copies of reprints.

Scholar : S. Rama Mercy

Supervisor : 27/06/2024

The scholar Ms. Rama Mercy, S (ITPHCSP011) has published her articles in the following journal:

1. International Journal of Computer Network and Information Security - indexed and active in Scopus.

This may be considered.

27.06.24

Checked By: 27/6/2024
HoD/Dean of Respective School

I. J. Computer Network and Information Security, **2023, 3, 90-105**
Published Online on June 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2023.03.07

Self-healing AIS with Entropy Based SVM and Bayesian Aggregate Model for the Prediction and Isolation of Malicious Nodes Triggering DoS Attacks in VANET

Rama Mercy. S.*
Avinashilingam Institute for Home Science and Higher Education for Women, Bharathi Park Rd, near Forest College Campus, Saibaba Colony, Coimbatore, Tamil Nadu 641043, India
E-mail: ramamercy_cs@avinuty.ac.in
ORCID iD: https://orcid.org/0000-0001-7557-973X
*Corresponding Author

G. Padmavathi
Avinashilingam Institute for Home Science and Higher Education for Women, Bharathi Park Rd, near Forest College Campus, Saibaba Colony, Coimbatore, Tamil Nadu 641043, India
E-mail: padmavathi_cs@avinuty.ac.in
ORCID iD: https://orcid.org/0000-0002-5377-4451

Received: 23 December 2022; Revised: 27 February 2023; Accepted: 03 April 2023; Published: 08 June 2023

Abstract: Vehicle ad hoc networks, or VANETs, are highly mobile wireless networks created to help with traffic monitoring and vehicular safety. Security risks are the main problems in VANET. To handle the security threats and to increase the performance of VANETs, this paper proposes an enhanced trust based aggregate model. In the proposed system, a novel adaptive nodal attack detection approach - entropy-based SVM with linear regression addresses the trust factor with kernel density estimation generating the trustiness value thereby classifying the malicious nodes against the trusted nodes in VANETs. Defending the VANETs is through a novel reliance node estimation approach - Bayesian self-healing AIS with Pearson correlation coefficient aggregate model isolating the malicious node thereby the RSU cluster communication getting secure. Furthermore, even a reliable node may be exploited to deliver harmful messages and requires the authority of both the data and the source node to be carried out by the onboard units of the vehicles getting the reports of incident. DoS attacks (Denial of Service) disrupting the usual functioning of the network leads to inaccessible network to its intended users thereby endangering human lives. The proposed system is explicitly defending the VANET against DoS attacks as it predicts the attack without compromising the performance of the VANET handling nodes with various features and functions based on evaluating the maliciousness of attacking nodes accurately and isolating the intrusion. Furthermore, the performance evaluations prove the effectiveness of the proposed work with increased detection rate by 97%, reduced energy consumption by 39% and reduced latency by 25% compared to the existing studies.

Index Terms: DoS Attacks, RSU, Cluster Network, Kernel Density Estimation, Pearson Aggregate Model, On-board Unit.

1. Introduction

Cyber threats are increasing to critical levels due to inclusiveness of Internet of Things (IoT) impacting every area of life with exchange of information. IoT threats between 2019 and 2020 arose to 100% and increased cyber-attacks in cyber-physical systems endanger human life and cause material damage. VANETs have gained popularity over the past ten years, and a number of applications, including early warning systems that can alert drivers to road construction, weather-related hazards, speed limits for curves, collisions, and pedestrian crossing warnings, merging lanes, are now prepared for widespread deployment [1]. The protection of the driver and passengers is now more important and difficult than ever before due to the ever-growing number of cars on the road. V2V communication is defined as communication

between two or more vehicles when they are travelling on a road [2]. Vehicles that are connected to one another transmit information about position, directions, quick turns, speed, brakes, and emergency situations in order to prevent any potential collisions. Thus, nodes with an ad hoc network were constructed. VANET, which is also a division of Mobile Ad-Hoc Network (MANET), is a technology whose purpose is to improve driving safety, traffic flow, and comfort. This entails the registration and management of roadside units and onboard transportation units (OBUs) (RSUs) [3]. Fig.1. shows the VANET communication.

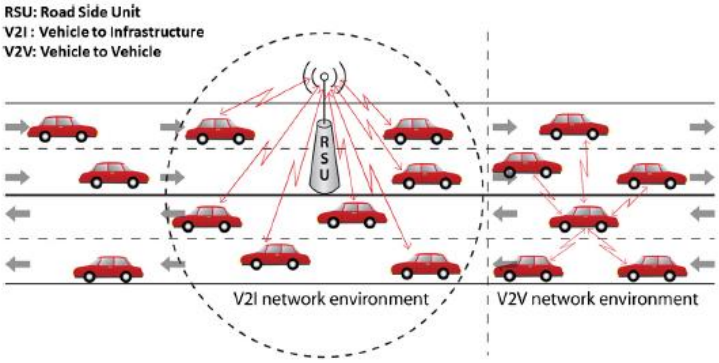

Fig.1. VANET communication

Information must be accurate, efficient, and dependable because information transmitted insecurely over VANET communication could have disastrous consequences [4]. By regularly exchanging information across network nodes, every project in the VANET field aims to effectively provide road safety [5]. Security is required in the VANET network to prevent attacker penetration from causing losses and privacy threats because any successful attack could result in serious accidents, the loss of life, or economic loss [6].

The biggest obstacle to putting VANETs into practice is the security issue because real-time VANETs include vital message exchange [7]. The timely transmission of messages has the power to either save or derail user lives. Denial of Service (DoS) attacks on the network are what lead to the lack of availability property of security [8]. As a result, denial-of-service (DoS) assaults become a significant issue when multiple vehicles conduct different forms of DoS operations to interfere with the network's normal operation and put human lives in danger [9]. Any form of DoS attack's primary objective is to prevent the targeted users from accessing the network service. Attacks of this nature are committed for a variety of motives, including monetary gain, rivalry, retaliation, self-gratification, diverting attention from more serious issues, etc. Due to their shorter length, DDoS assaults on VANET are become harder to detect [10]. A DDoS attack has the potential to cause mayhem and harm lives in this short amount of time. In order to prevent the Holocaust, an efficient detection mechanism should be created to identify DDoS attacks in their early phases [11].

This paper presents a novel hybrid model with self-healing AIS as a means to mitigate and immunize the VANETs without disrupting the normal functioning of the network. The security solutions provided in this paper are towards RSU cluster communication with response time and data transmission; isolating the attacked node on detection of maliciousness of the node thereby the proposed system performance is increased.

This work focuses on immunizing the network by isolating the node and deleting them in accordance with how of nodes behave within in the system. The work develops a learning strategy to identify and avoid DoS attackers without impacting the overall performance of the VANETs by utilizing the capabilities of anomaly detection and mitigation mixed with artificial immune system.

In this work, CICDDoS2019 dataset has been used to detect and isolate the affected node. The performance of the VANET that ensures seamless vehicular operation has been shown through the simulations and the assessment displays the system’s capability to detect abnormal behavior and act upon it to support the VANET operations. The paper is structured as follows. The state of the art in cyber-security for VANETs against DoS attacks is presented in section 2. The next, section 3, is dedicated to the hybrid model for the VANETs in securing the network performance and vehicular communications. Section 4 describes the simulation results and performance comparison. The section 5 presented the conclusion of the work.

2. State of the Art

Intelligent Transportation Systems are concentrating on focusing on cars that have significant computer, communication, and sensing capabilities (sometimes known as "smart" vehicles) (ITS). It might be challenging to safeguard wireless connections in automobile ad hoc networks. For the safety of individuals, security and its ensured level of implementation are crucial. This section provides a comprehensive analysis of the state-of-the-art literature on cyber security measures for VANETs, including associated work on glitch detection and mitigation techniques.

2.1. VANETs and Cyber Security Solutions

Vehicle communication for intelligent transportation systems (ITS) is quickly expanding, using wireless communication in vehicular ad hoc networks using specialized short-range communications. However, due to the different mobility of nodes in vehicles, the time it takes to connect a server to send or receive data with the cluster head from an external server is problematic, making it subject to security threats and causing packet losses in RSU cluster communication. Several surveys work exist in the literature which cover different security problems in vehicular networks and discuss challenges with solutions.

Fatemidokht et al [17] investigated how UAVs functioned in an ad hoc manner and how they interacted with other vehicles in VANETs to assist in the routing and identification of dangerous vehicles. Two distinct data routing techniques are included in the proposed VRU routing protocol: (1) using UAVs to convey data packets between automobiles using the VRU vu protocol, and (2) routing data packets between UAVs using the VRU u protocol. To evaluate the effectiveness of VRU routing components in an urban environment, Linux Ubuntu 12.04 and the NS-2.35 simulator are used. Additionally, the VanetMobiSim mobility generator and MobiSim are used, respectively, to create the motions of vehicles and UAVs. However, rural highways based on the suggested urban strategies require the introduction of a novel security protocol by enhancing energy saving, which is essential to UAV lifetime and enables the detection of hostile UAVs.

Brown et al [18] created the Blacksite framework for a revolutionary adaptive real-time intrusion detection in Internet of Things networks that integrates human intelligence with a synthetic immune system and uses a deep neural network-based validation model. They suggested a method that can handle the particular difficulties faced by IoT networks, and they presented implementation strategies in addition to a pilot implementation of Blacksite's key component. The suggested system is made to react to attacks quickly and change with evolving network topologies. It is necessary to look at other strategies, such as long short-term memory (LSTM) neural network algorithms, to counter sequence-specific traffic typical of DDoS attacks.

Nishanth et al [19] have discussed the flooding-based DoS assault, which led to a denial of sleep attack and targeted the mobile node's limited resources, which led to an excessive consumption of power. In a SYN flooding-based DoS attack, the attacker sends several spoof SYN packets, overflowing the target buffer and clogging the network. The three sections of the article are as follows: 1) Using Bayesian inference to mathematically represent SYN traffic in the network; 2) demonstrating that Bayesian inference and exponential weighted moving average are equivalent; and 3) creating an effective algorithm for the recognition of SYN flooding attacks via Bayesian inference. Any form of flooding-based DoS attack in a wireless ad hoc network is successfully defended by the suggested work's implementation. Data fusion techniques and an additional source of evidence are required for this method.

Alharthi et al [20] presented a biometrics blockchain (BBC) framework to secure data transfer among automobiles in VANET and to maintain archive data in a traditional and reliable manner. The benefit of biometric data in the suggested framework preserved privacy by keeping a record of the message sender's actual identity. Because of this, the proposed BBC approach creates security and trust among cars in VANET coupled with the ability to track down identities as needed. Simulations employing the urban mobility model were run in OMNeT CC, veins, and SUMO to show the proposed framework's feasibility. In terms of packet loss rate, packet delivery rate, and computing cost, the framework's performance is assessed. Future work will involve expanding the model for calculating the reputation and ranking of cars and drivers using machine learning methods.

Poongodi et al. [21] have presented a reCAPTCHA controller mechanism to stop automated attacks like botnet zombies. The majority of automated DDoS assaults are checked for and stopped by the reCAPTCHA controller. In order to implement this technique, the information theory-based metric is used to analyses the variance in user requests in terms of entropy. The criteria used to assess the attack's susceptibility are frequency and entropy. Large botnet-based attackers are deterred using the stochastic model-based reCAPTCHA controller. In the future, utilizing a hybrid technique to avoid and isolate assaults is performance- and security-wise efficient.

Yang et al [22] have created a method for the degradation-of-QoS (DeQoS) attack against mobile ad hoc networks. By using DeQoS, an attacker can waste the restricted connection resources of roadside units (RSUs) by relaying the verification relations between RSUs and distant vehicles in order to establish connections but not the service itself. The number of bogus connections could build up to the point where RSUs' resources are exhausted and they are unable to continue serving authentic cars. Due of the close relationship between vehicle mobility and the attacker's success likelihood, we simulate the arrival and departure of cars into a M=M=N-queue system. This illustrates how the attacker can choose alternative attack techniques in accordance with changing traffic situations. However, in future work, the distance-bounding-based defense mechanism to explore its practicability has to be implemented.

From the survey, for [17] a novel security protocol needs to be introduced to improve energy saving, for [18] supplementary mechanisms, such as LSTM neural network algorithms, are to be exposed to address sequence-specific traffic symbolic of DDoS attacks, for [19] On the basis of an additional source of evidence and data fusion techniques, future work is anticipated, [21] must be extend the model for computing ranking and reputation of vehicles and drivers using machine learning techniques, in [21] for avoiding and separating the attacks by using the fusion mechanism is performance- and security-wise efficient and for [22] the distance-bounding based protection mechanism to discover its operability has to be implemented. Hence, to overcome the above-mentioned issues a novel technique has to be implemented.

2.2. Contributions to Secure VANETs against DoS Attacks

Many academics have presented numerous algorithms for the limited network to be impervious to different attacks, and among them, the artificial immune systems (AIS) are categorized on inspired algorithms from biology [12]. These algorithms, as their name suggests, are computer-based algorithms whose principles and features are the outcome of a careful analysis of both adaptive qualities and the resistance of biological samples [13]. Theoretical immunology and observable immune activities, principles, and models provide as inspiration for these adaptive systems, which are used to tackle complicated problem areas. Various research areas are attempting to bridge the gap between immunology and engineering by using the methods of mathematical and computational modelling of immunology [14]. Many computer scientists suggested artificial immune-based computer models to address a variety of issues, from virus identification and fault analyzing to clustering [15], by carefully evaluating the effective natural mechanism. However, these algorithms have to be further enhanced for effective prevention of attacks with dimensionality reduction and less computational time [16]. Thus, to improve the security of the VANET platform subjected to DoS attacks, a novel algorithm based on AIS has to be implemented. The following are this paper's main contributions:

- A response feedback algorithm is suggested to identify the attacks in which micro cluster outlier detection monitors the abnormality behavior of the RSU cluster network based on temporal information is detected and linear regression is used to evaluate the attacks.
- An adaptive nodal attack detection approach is proposed to classify the new typical attacks in which entropy-based support vector machine is utilized for kernel density estimation and classify the attacks based on the trustiness value.
- The reliance node estimation approach is proposed in which the self-healing effect of AIS with Pearson correlation coefficient is utilized to check the similarity between the predicted data to estimate the maliciousness and the Bayesian aggregate model is utilized to check the credibility of the OBU to isolate the malicious node from the RSU cluster communication networks.

3. Proposed System with Aggregate Model for Prediction and Isolation of Malicious Nodes Triggering DoS Attacks in VANETs

Vehicle communication for intelligent transportation systems (ITS) is quickly expanding, using wireless communication in vehicular ad hoc networks using specialized short-range communications. However, due to the different mobility of nodes in vehicles, the time it takes to connect a server to send or receive data with the cluster head from an external server is problematic, making it subject to security threats and causing packet losses in RSU cluster communication. To close this gap, the proposed system introduces a novel Response Feedback Algorithm in which the microcluster outlier detection with linear regression utilizes to identify the attacks during the data communication and it considers the temporal information with variable speed range based on data transmission and response time between the RSU, deviation from the packets sent and loss, the relative speed between vehicles and their position. Moreover, to create a system capable of managing new typical DoS threats, such that no additional involvement in updating the attack repository is necessary to forecast attacks before they occur. To overcome this issue, the proposed system introduces a novel, Adaptive Nodal Attack Detection Approach in which an entropy-based SVM classifier utilized for kernel density estimation to detect the maliciousness of attacks based on trustiness value. Furthermore, different manufacturers' vehicles have varied features and functionalities, and these unique characteristics pose a variety of security risks, as well as being vulnerable to assaults. To bridge this gap, the proposed system introduces a novel Reliance Node Estimation Approach in which self-healing AIS with Pearson coefficient correlation used to check the similarity of the predicted value and the Bayesian aggregate model used to check the credibility of the OBU therefore the malicious attack node accurately identified and isolate the malicious node thereby the RSU cluster communication getting secure. As a result, the proposed system successfully identifies the attacks and classifies the attacks as well as isolates the attacked node thereby the proposed system performance is increased. The proposed system with the aggregate model against DoS attacks is shown in Fig.2.

3.1. Response Feedback Algorithm

Response feedback algorithm proposed to identify the threat in the RSU cluster communication. Because the RSU interacts with cluster members via cluster heads which change often owing to vehicles moving along the route. As a result, an attacker can launch an attack by overloading the network, causing packet failures in RSU cluster communication. Hence, the proposed system introduced a novel response feedback algorithm in which the transmission response time between RSU and the network is calculated by using temporal-based data with variable speed change. Then the RSU unit is utilizing micro cluster outlier detection with linear regression for identifying the attack in the RSU cluster region. The micro cluster outlier detection with linear regression identifies the attacks based on temporal information such as the data transmission and response time in-between network nodes, deviation from the packets sent and loss, the relative speed between vehicles and their position, and vehicle density from which the deviation from the forecasted transmission response time during data communication is derived. The micro cluster outlier detection algorithm is given below.

Algorithm1: Micro Cluster Outlier Detection Algorithm

Input: New message (R)
Output: Detect abnormal behavior

1. Start
2. Increase the counter by 1: a++ // based on parameters
3. If a% t = 0 then // t = threshold
4. E = current time – the previous time
5. s = t / E
6. else send the message to the RSU
7. end if
8. s input to MCOD
9. if s is normal then notify the node
10. otherwise, find out whether the abnormality is because of attacks (by using linear regression)

Micro-cluster outlier detection abnormality monitoring steps are given below.

- When a new message (R) received, the counter (a) for new messages is incremented by one.
- A specified maximum boundary for the number of fresh texts is derived using the modular division of counter (a) and threshold (t).
- The new message delivered to the RSU if the remaining is not zero. Else, the present time is recorded.
- The time lapsed (e) then determined by subtracting the current time from the prior time.
- The new message's rate (s) is determined by dividing the threshold by the amount of time elapsed.

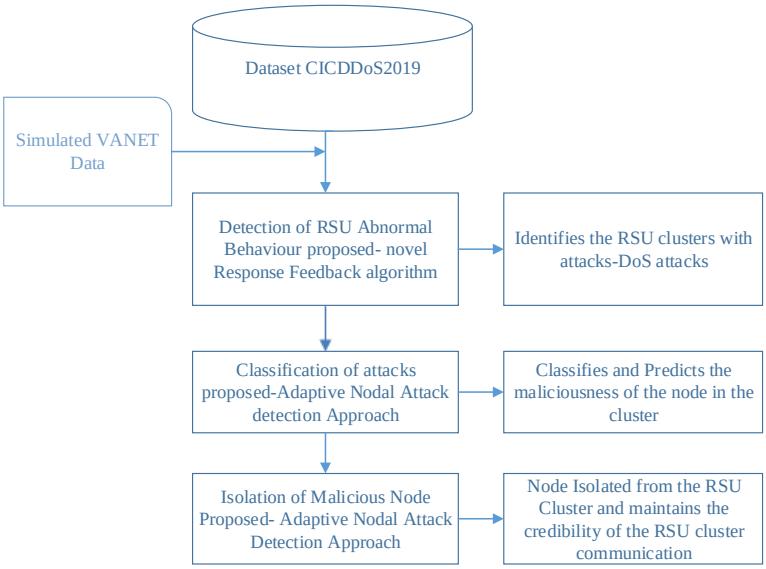

Fig.2. Proposed system with aggregate model

Then the proposed system added the linear regression with the micro cluster outlier detection for identifying the attacks in the RSU cluster network. The linear regression model identifies the attack by considering the number of new messages and the counter value. When the micro cluster outlier detection algorithm shows, that the numbers of a new message are raised then the counter is incremented by one, if the network is normal and then counter is increased based on the temporal information. Therefore, the linear regression takes into account of new message and counter values are used to identify the attacks. The mean absolute error of this line is derived using the formula

$$M = \frac{1}{n}\sum_{i=1}^{n}(|Xi - \acute{X}\imath|) \quad (1)$$

Where

- Xi – the number of counters
- $\acute{X}\imath$ – estimation of this value

In this way, the proposed system has identified the attacks in the RSU cluster communication network. If the attack is identified then the proposed system requires to find out the maliciousness of the attacks caused by the network, therefore, the suggested system introduces a novel adaptive nodal detection approach.

3.2. Adaptive Nodal Attack Detection Approach

To detect maliciousness of DDoS attacks from VANET, the proposed system used a trust-based assessment process. In the adaptive nodal attack detection approach, the maliciousness of attacks identified using the kernel density estimation for vehicle density, average latency, packet delivery ratio, detection rate, and energy consumption during communication of nodes between the RSU and cluster network depending on traffic data, which accurately identified using the using entropy-based support vector machine (SVM) classifier. The kernel density estimation, estimate the probability density function in the RSU cluster network and generates the trustiness values based on the parameters. If maliciousness of attack affects the node in the RSU or cluster network, the proposed system evaluates the trustiness value as 0 otherwise, if the cluster network or RSU is secure, the proposed system evaluates the trustiness value as 1. If the trustiness value is 0, then the entropy-based support vector machine classifies the maliciousness of attack to analyze the parameters such as vehicle density, energy consumption, average latency, packets delivery ratio, and detection rate.

The adaptive nodal attack detection approach algorithm is shows in algorithm 2 and the flowchart is shows in fig.3.

Algorithm 2: Adaptive Nodal Attack Detection Approach Algorithm

Input: parameters (x)
Output: maliciousness of attacks

1. Start
2. If (the parameters (x) is equal to the threshold value in the cluster network)
   // create a token for incrementing the trust value by one
   Token j = j + 1
3. Else (the parameter (x) is not equal to the threshold value in the cluster network)
   // create a token for decrementing the trust value by one
   Token j = j – 1
4. Find trust factor $TF = VD \times AL \times PDR \times DR \times EC$
5. If (trust factor less than Kernel density estimation)
   // find out how much the node is affected by the attack
   SVM classify and predict the maliciousness of the attacks
6. End

The adaptive nodal attack detection approach steps as follows

- The procedure starts by initializing the parameters VD, AL, PDR, DR, EC
- To classify the node Entropy-based SVM classifier takes the trustiness value of every parameter
- Then find out the trust factor using the formula

$$TF = VD \times AL \times PDR \times DR \times EC \tag{2}$$

- If the trust factor is not equal to the kernel density estimation (KDE) value, an entropy-based SVM classifier classifies and predicts the maliciousness of the node in the cluster network.

After predicting the maliciousness of attack from the node based on the trustiness kernel value by entropy-based support vector machine, then the malicious node must be isolated. Therefore, the proposed system uses a novel reliance node estimation approach to isolate the malicious node.

3.3. Reliance Node Estimation Approach

In the reliance node estimation approach, the proposed system checks the similarity between the predicted data within the VANET network by using the Pearson correlation coefficient method. In this work, the Pearson correlation coefficient shows the quality of the RSU cluster communication network. Pearson correlation coefficient captures the correlation between the predicted data that is measure the linear relationship between the low trustiness values for their diverse functions. Moreover, the correlation coefficient yields the value between -1 to 1, where,

- -1 indicates a strong negative relationship between nodes
- 1 indicates a strong positive relationship between nodes
- 0 (zero) indicates a no relationship between nodes

The Pearson coefficient correlation calculated by using

$$r = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2]}} \tag{3}$$

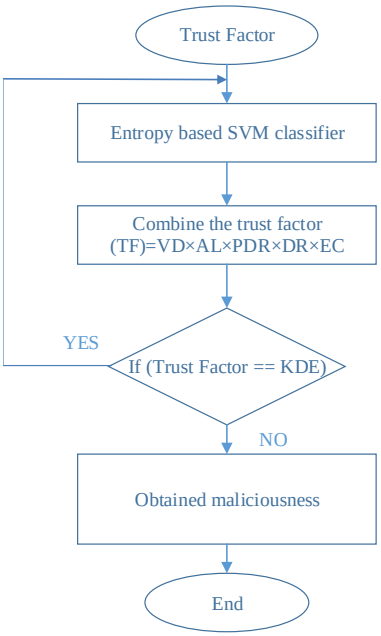

Fig.3. Flowchart of adaptive nodal attack detection approach

The variations are very high between the nodes; the correlation coefficient returns the value 1. If the variations are differing, then the correlation coefficient returns the value -1. If no relationship between the nodes, then the correlation coefficient returns zero. The scale of Pearson correlation coefficient factors measures [23] is tabulated in table 1.

Table 1. Pearson's coefficient's range

The scale of the correlation coefficient	Value
$0.8 \leq r \leq 1.0$	Very High Correlation
$0.6 \leq r \leq 0.79$	High Correlation
$0.4 \leq r \leq 0.59$	Moderate Correlation
$0.2 \leq r \leq 0.39$	Low Correlation
$0 < r \leq 0.19$	Very Low Correlation

Furthermore, vehicles from diverse manufacturers have varied features and functionalities, and these unique characteristics provide a variety of security risks and are vulnerable to assaults. For that reason, the proposed system is also considering the onboard unit (OBU) and it checks the credibility by using a Bayesian aggregate model based on the Pearson coefficient. The RSU and OBU is given in fig.4.

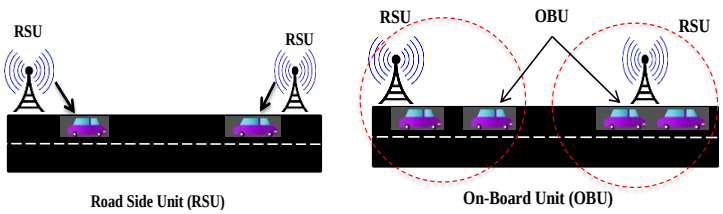

Fig.4. RSU and OBU

A hardware component placed on the vehicle, an on-board unit communicates with other OBCs and RSUs. The reliability of other cars it interacts with within the network is determined by the Bayesian aggregate model. Because even a truthful node could be used to send hateful messages. Consequently, the accuracy of the information and the reliability of the source node performed by the onboard components of the cars receiving the event reports This results in the on-board units in reception vehicles producing ratings for source vehicles, which are then utilized to update their individual faith values in the trust value. The proposed system is considering the trust level of the source node, and security status to check the credibility of the vehicle. Here the ratings (credibility score) of the vehicle are correct then the trust value is considered one otherwise the trust value is considered zero.

The Bayesian aggregate model continuous to check the credibility of the RSU cluster communication network therefore if any vulnerability action identified in the communication, the Bayesian aggregate model generates a credibility score of zero; therefore, the particular node is isolated with the self-healing effect of the artificial immune system (AIS).

The algorithm steps of the artificial immune system are as follows

Step 1: The algorithm starts with the initializing the predicted values in the cluster communication network.

Step 2: By transmitting Basic Safety Messages (BSM), it is sensing activities conducted by vehicles. The On-Board Unit (OBU) broadcasts BSMs based on the credibility value that contain information on the vehicle's density, energy consumption, average latency, detection rate, and packet delivery ratio.

Step 3: Evaluate the performance of each parameter.

Step 4: Decision is making based on the step 3, if the performance is less than threshold value the node is isolate from the cluster network.

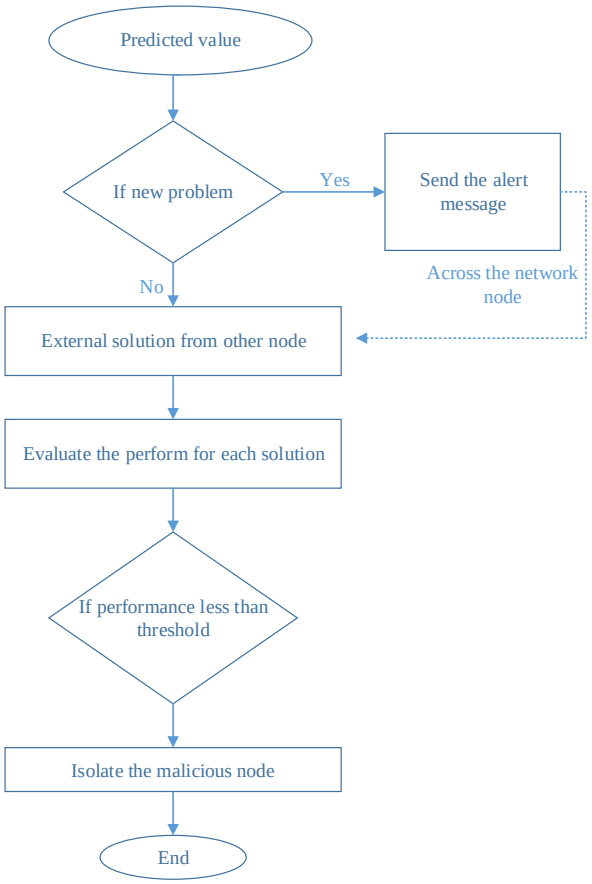

Fig.5. Flowchart of AIS

Fig.5. shows the flowchart of artificial immune system. As a result, the reliance node estimation approach evaluates the maliciousness of attacking nodes accurately and isolates the intrusion, and predicts the attack without compromising the performance of the VANET handling nodes with various features and functions.

4. Result and Discussion

This section includes a detailed explanation of the implementation outcomes, the performance of the suggested system, and a comparison section to guarantee the suggested system functions effectively. This work has been implemented in the working tool of NS-3 and CICDDoS2019 dataset used to detect and isolate the affected node. The benign and current common DDoS attacks in CICDoS2019 are a close reflection of actual data (PCAPs). Furthermore, it provides flows that have been labelled according to the time stamp, destination address IP addresses, input and output ports, protocols, and attack vectors, as well as the results of a network traffic analysis performed with CICFlowMeter-V3. Include many types of recent reflected DDoS attacks in this dataset, such as PortMap, UDP, LDAP, SYN, MSSQL, UDP-Lag, NTP, DNS, NetBIOS, and SNMP.

4.1. Simulation Results and Discussions

The simulation results of the proposed system are illustrated and discussed in this section. The proposed system uses a novel Response Feedback Algorithm in which micro cluster outlier detection with linear regression is used to identify attacks during data communication, and it takes into account temporal information with a variable speed range based on data transmission and response time between the RSU, deviation from the packets sent and loss, the relative speed between

vehicles and their position. Therefore, the proposed systems have successfully identified the attacks in the RSU cluster communication network with the deviation loss, vehicle density, send and received packets, time duration, throughput, and average end-to-end delay. Moreover, the proposed system used a novel adaptive nodal attack detection approach for identifying the maliciousness of attacks. Based on the parameters, the kernel density estimate gives the trustworthiness values. If a node in the RSU or cluster network is subjected to an attack, the proposed system assigns a trustiness value of 0; otherwise, if the cluster network or RSU is safe, the proposed system assigns a trustiness value of 1. If the trustiness value is 0, an entropy-based support vector machine is used to distinguish maliciousness of attacks and examine characteristics such as vehicle density, energy consumption, average delay, packet delivery ratio, and detection rate. Therefore, the proposed system is successfully predicted the maliciousness of the attack.

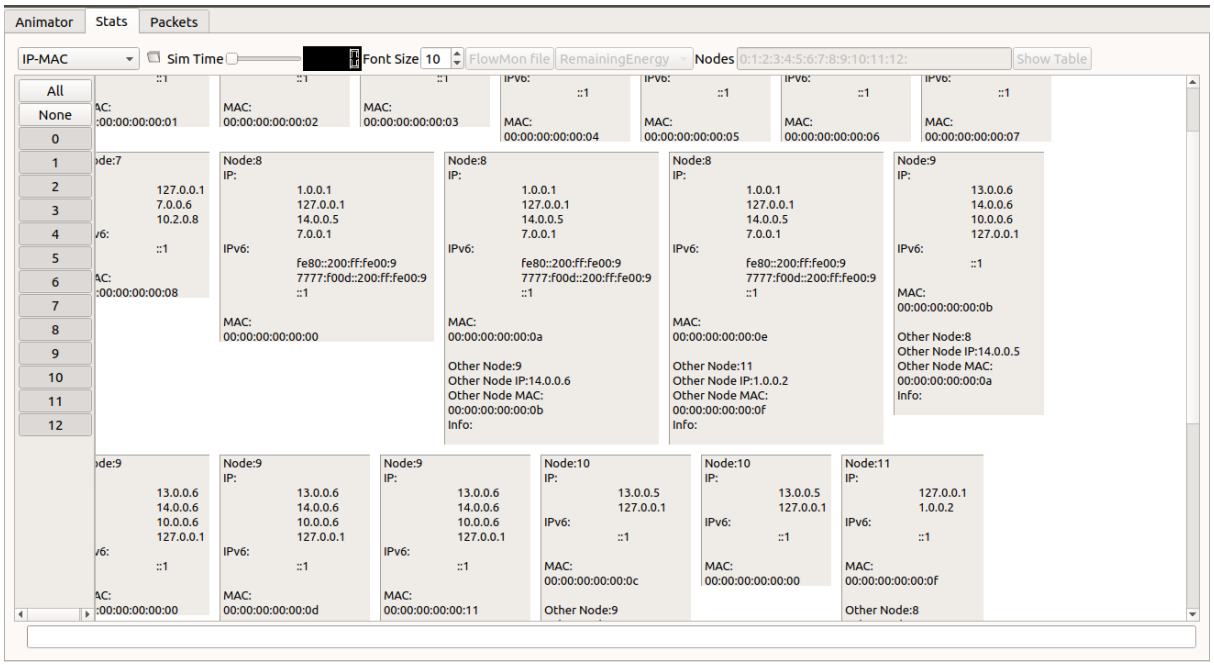

Fig.6. Simulation results of the proposed systems

Furthermore, the proposed system used a novel reliance node estimation approach to isolate the malicious node. The RSU cluster communication network's quality is represented by the Pearson correlation coefficient. The Pearson correlation coefficient measures the linear link between the low trustworthiness values for their various functions and represents the correlation between the anticipated data. The figure 6 shows the node's IP value and MAC values of the node in the RSU cluster communication network. The Bayesian aggregate model determines the reliability of other cars with whom it interacts in the network. The Bayesian aggregate model continuously checks the credibility of the RSU cluster communication network; as a result, if any vulnerability action is discovered in the communication, the Bayesian aggregate model generates a credibility score of zero, and the particular node is isolated using the automatic identification system's self-healing effect (AIS). As a result, it isolated the malicious node in the RSU cluster communication network.

4.2. Performance Metrics of the Proposed System

The transactions of packets in the proposed method explained in Fig.7. The network size grows from 60 to 200 nodes in the presented graph, while the suggested number of packet transactions scheme increases. The self-healing effect of AIS with Pearson correlation coefficient was used to check the similarity of the predicted data with the VANET in the reliance node estimation approach, and the Bayesian aggregate model used to check the credibility of the OBU. As a result, it accurately evaluates malicious nodes and isolates malicious nodes; lowering packet loss in the proposed system thereby the transactions of the packet ratio are also secure and increased.

The transactions of packets in the proposed method explained in Fig.7. The network size grows from 60 to 200 nodes in the presented graph, while the suggested number of packet transactions scheme increases. The self-healing effect of AIS with Pearson correlation coefficient was used to check the similarity of the predicted data with the VANET in the reliance node estimation approach. Which assesses the linear relationship between the low trustworthiness levels and depicts the association between the expected data. and the Bayesian aggregate model used to check the credibility of the OBU. As a result, it accurately evaluates malicious nodes and isolates malicious nodes linearly; lowering packet loss in the proposed system thereby the transactions of the packet ratio are also secure and increased 11000 p/sec.

The above-mentioned graph clearly explains the trust value of the suggested system. From the Fig.8, the network size increased from 25 nodes to 200 nodes as well as the proposed system of trust value also increased. Because the proposed system uses a novel adaptive nodal attack detection approach in which the kernel density estimation is estimated probability density function for vehicle density, energy consumption, average latency, packet delivery ratio, and detection

rate in the RSU cluster communication and it generates the trustiness value thereby the trust value of the proposed system is increased.

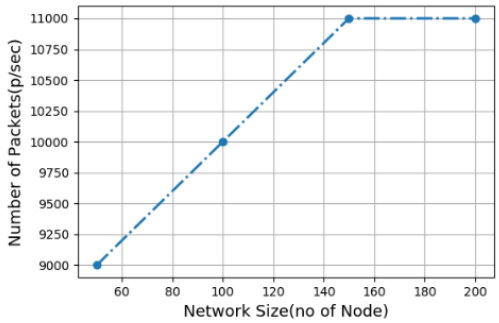

Fig.7. Transactions of packets

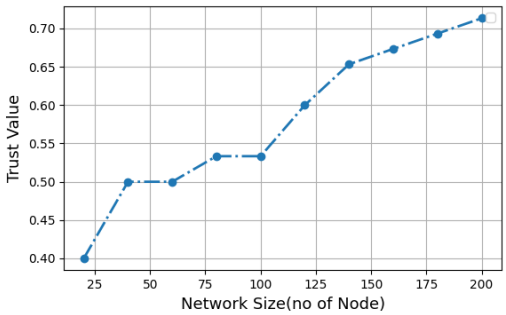

Fig.8. Trust value of the proposed system

The energy consumption of the proposed system is shows in fig.9. According to the graph, the network size has increased from 60 to 200 nodes, but the proposed energy consumption mechanism maintains the levels between from 10 to 40 as number of node increases. The Bayesian aggregate model used to check the credibility of the OBU, so it accurately evaluates malicious nodes and isolates the malicious node, thereby decrease the energy consumption in the proposed system.

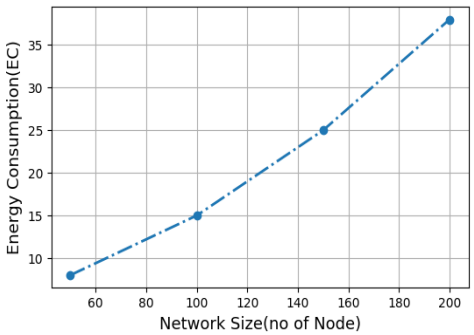

Fig.9. Energy consumption of the proposed system

The energy consumption of the proposed system is shows in fig.9. According to the graph, the network size has increased from 60 to 200 nodes, but the proposed energy consumption mechanism maintains the levels between from 10 to 40 as number of node increases. The entropy-based support vector machine categorizes the attack's maliciousness to examine energy usage and it generates the trustiness value in nonlinear regression. The Bayesian aggregate model used to check the credibility of the OBU, so it accurately evaluates malicious nodes and isolates the malicious node, thereby decrease the energy consumption of 39% in the proposed system.

Fig.10. clearly shows the latency of the proposed system. The latency of the suggested system improves by using a novel response feedback algorithm, in which micro-cluster outlier detection techniques with linear regression are used to monitor the abnormality behavior of the RSU cluster network and gives the feedback of the current cluster network thereby the attack RSU cluster is identified easily. As a result, the proposed system detects the attacks in a short amount of time, resulting in higher latency due to a response feedback algorithm that uses linear regression and micro-cluster outlier detection algorithms to track unusual network topology behavior, offer feedback based on temporal data, and detect attacks. From the graph, the network size increased from 60 to 200 nodes; the latency of the suggested system is also increased.

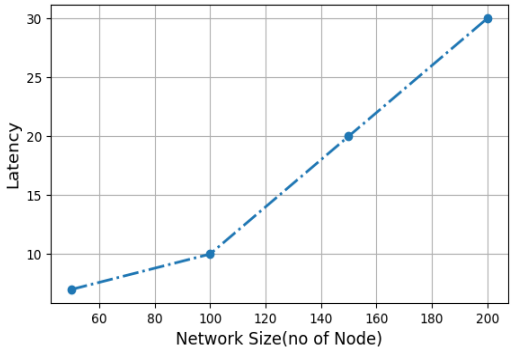

Fig.10. Latency of the proposed system

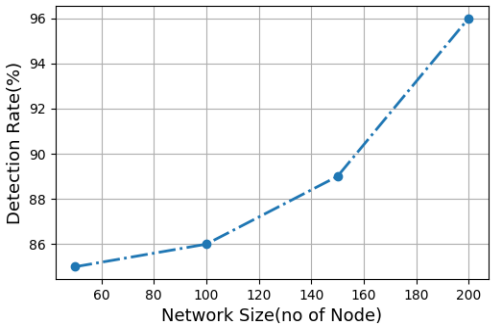

Fig.11. Detection rate of the proposed system

The detection rate of the suggested approach clearly illustrated, in fig.11. The network size has expanded from 60 to 200 nodes, and the suggested system of detection rate has increased, as seen in the graph. Because the proposed system employs a novel adaptive nodal attack detection approach, the entropy-based support vector machine classifier categorizes maliciousness based on their trustworthiness value, increasing the proposed system's detection rate.

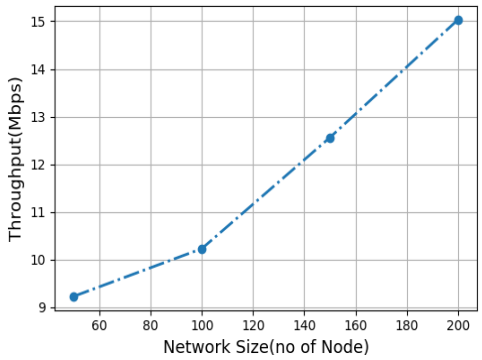

Fig.12. Throughput of the proposed system

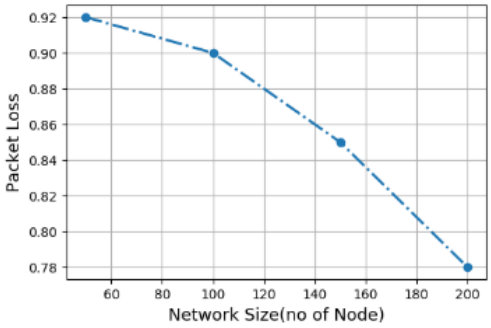

Fig.13. Packet loss of the proposed system

The throughput of the suggested technology is clearly, shown in fig.12. The throughput of the proposed system improved by using a novel response feedback algorithm in which micro-cluster outlier detection techniques used to

monitor the abnormality behavior of the RSU cluster network Which are added the linear function and provide feedback on the current cluster network considering the temporal relationship between them thereby the suggested system identifies assaults quickly, resulting in greater throughput.

Fig.13, clearly explains the packet loss of the proposed system. From the graph, the network size increased from 60 nodes to 200 nodes as well as the proposed system of packet loss also decreased. In reliance node estimation approach, the self-healing effect of AIS with Pearson correlation coefficient used to check the similarity of the predicted data with the VANET, and the Bayesian aggregate model also utilized to check the credibility of the OBU therefore it evaluates malicious node accurately and isolates the malicious node thereby the packet loss of the proposed system reduced. Table 2 lists the overall performance values of the proposed system.

Table 2. The performance value of the proposed system

Network Size	Number of Packets(p/sec)	Energy Consumption(EC)	Latency	Detection Rate (%)	Throughput	Packet Loss
50	9000	8	7	85	9.23	0.92
100	10000	15	10	86	10.23	0.9
150	11000	25	20	89	12.56	0.85
200	11000	38	30	96	15.03	0.78

4.3. Performance Comparison of the Proposed System

This section discusses how the proposed technique performs in many ways when compared to the outcomes of earlier methodologies and presents those outcomes using a variety of measures.

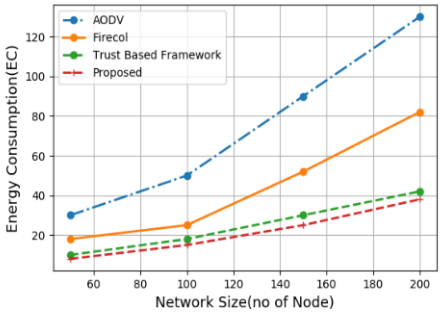

Fig.14. Comparison of energy consumption of the proposed system

The self-healing effect of AIS with Pearson correlation coefficient used to check the similarity of the predicted data with the VANET in the reliance node estimation approach in which the cluster network problems are resolved with the help of AIS. Moreover, the Bayesian aggregate model is also used to check the credibility of the OBU, so it accurately evaluates malicious nodes and isolates the malicious node, decreasing energy consumption in the proposed system. Fig14. and Table 3 shows the results of the energy consumption comparison of proposed method is given in table 3.

Table 3. Comparison of the proposed system's energy consumption

Number of Packets(p/sec)	AODV	Firecol	Trust Based Framework	Proposed system
50	30	18	10	8
100	50	25	18	15
150	90	52	30	25
200	130	82	42	38

The proposed system's energy consumption decreased by 39 than the existing output, when compared to the energy consumption of AODV (ad-hoc on-demand distance vector), which is 137, trust based framework, which is 40 and firecol, which is 82. In conclusion, AODV has the energy consumption, whereas our proposed system has the lowest energy consumption [24].

The proposed system's latency decreased by 25% than the existing output when compared to the latency of AODV, which is 95 percent, trust based framework, which is 27% and firecol, which is 58 percent. In conclusion, AODV has the latency, whereas our proposed system has the lowest latency. Fig.15. and Table 4 show the results of the latency comparison. The suggested system's latency decreases due to a response feedback algorithm that combines micro-cluster outlier detection techniques with linear regression to monitor anomalous network topology behavior and provide feedback based on the temporal information as well as identify the attacks. Consequently, the suggested system identifies the assaults quickly, resulting in reduced latency of the proposed system.

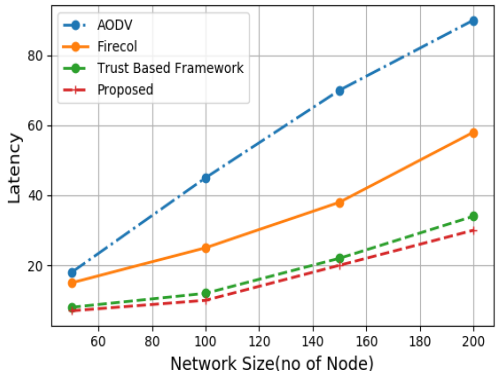

Fig.15. Comparison of latency of the proposed system

Table 4. Comparison of latency of the proposed system

Number of Packets(p/sec)	AODV	Firecol	Trust Based Framework	Proposed
50	18	15	8	7
100	45	25	12	10
150	70	38	22	20
200	90	58	34	30

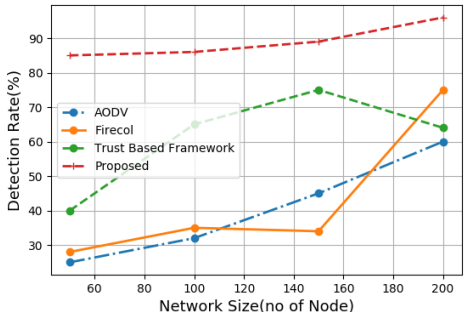

Fig.16. Comparison of detection rate of the proposed system

The suggested system uses a unique adaptive nodal attack detection technique that uses kernel density estimation to continually measure vehicle density, energy consumption, average latency, packet delivery ratio, and detection rate in RSU cluster communication and provide the trustworthiness value. Furthermore, the suggested system's detection rate improved by the entropy-based support vector machine classifier, which categorizes attacks depending on their trustworthiness value.

Table 5. Comparison of detection rate of the proposed system

Number of Packets(p/sec)	AODV	Firecol	Trust Based Framework	Proposed
50	25	28	40	85
100	32	35	65	86
150	45	34	75	89
200	60	75	64	97

Therefore, the proposed system's detection rate increased by 97% over the existing output, when compared to the detection rate of AODV, which is 60%, trust based framework, which is 65% and firecol, which is 77%. In conclusion, AODV has the lowest detection rate when the nodes are increases, whereas our proposed system has the highest detection rate. Fig.16. and Table 5 shows the results of the detection rate comparison.

When the attacker tries to put DDoS attack in the communication of VANET, the proposed system efficiently detects the affected node even if the number of attackers increase therefore the detection accuracy of the proposed system is high. Attackers Vs detection accuracy of the proposed system is show in fig.17 and the comparison values are tabulated in Table 6.

When compared to other techniques such as SVM that is 93%, Naïve Bayes that is 90%, K-nearest that is 92.3%, and multilayer perceptron (MLP) that is 83% but the proposed detection accuracy is high that is 97%. In which response feedback algorithm, adaptive nodal attack detection approach, and reliance node estimation approach are utilized to identify and isolate the attack nodes [25].

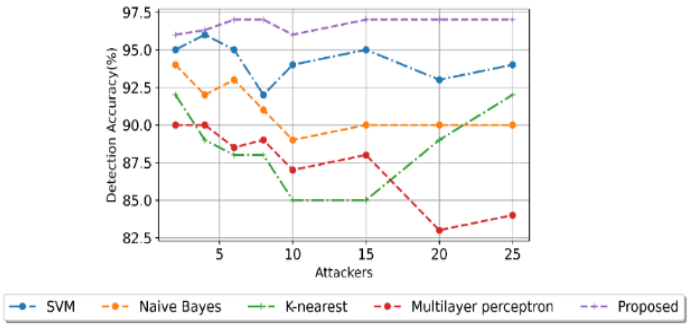

Fig.17. Attackers versus detection accuracy

Table 6. Attackers versus detection accuracy

Number of attackers	Detection Accuracy (%)				
	SVM	Naïve Bayes	K-nearest	MLP	Proposed
5	95.4	92.5	89.5	89.32	96.8
10	93.3	89.32	87.3	86.9	96
15	95	90	87.52	87.51	97
20	92.5	90	82.54	82.29	97
25	94.5	90	84.5	84	97

5. Conclusions

In this work, the attacks are identified by used a novel adaptive feedback response in which the micro cluster outlier detection with linear regression is utilized to recognize the attacks in the RSU cluster network. Moreover, the maliciousness of attacks classified used a novel adaptive nodal attack detection approach in which entropy-based SVM with kernel density estimation utilized to classify the attacks thereby the suggested system classifies the maliciousness of the node with trustiness value. Therefore, in a network of 50, 100, 150, and 200 nodes, the attempts to minimize packet loss in RSU cluster communication resulted in a drop in packet loss of 0.92, 0.9, 0.85, and 0.28, respectively. The proposed system of packet loss was also improved. The proposed system's output is 39% less energy-intensive. As compared to the latency of the current system, such as AODV, Firecol, and Trust based framework, which has latency of 95%, 27%, and 58% respectively, the recommended system's latency drops by 25% as a result of a response feedback algorithm than the existing output. The suggested system's detection rate performed 97% better than what was produced by the old method. The detection rates of AODV, Firecol, and Trust-based framework are 60%, 77%, and 65%, respectively, when compared to those of existing approaches. The proposed models detection accuracy is excellent, at 97%, compared to other approaches like SVM (93%), Naive Bayes (90%), K-nearest (92.3%), and multilayer perceptron (MLP) (83%). The proposed system effectively locates the afflicted node when an attacker attempts to disrupt VANET connection with a DDoS assault, even as the number of attackers grows. As a result, the proposed system's detection accuracy is high.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] Hamdi, Mustafa Maad, et al., "A review of applications, characteristics, and challenges in vehicular ad hoc networks (VANETs)," *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. IEEE, 2020.

[2] Hassija, Vikas, et al., "Dagiov: A framework for vehicle-to-vehicle communication using directed acyclic graph and game theory," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4182-4191, 2020.

[3] Hossain, Mohammad Asif, et al., "Comprehensive survey of machine learning approaches in cognitive radio-based vehicular ad hoc networks," *IEEE Access*, vol. 8, pp. 78054-78108, 2020.

[4] Wang, Yu, et al., "Efficient Privacy-Preserving Authentication Scheme with Fine-Grained Error Location for Cloud-Based VANET," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 10, pp. 10436-10449, 2021.

[5] Khatri, Sahil, et al., "Machine learning models and techniques for VANET based traffic management: Implementation issues and challenges," *Peer-to-Peer Networking and Applications*, vol. 14, no. 3, pp. 1778-1805, 2021.

[6] Jan, Sagheer Ahmed, et al., "A Survey on Privacy-Preserving Authentication Schemes in VANETs: Attacks, Challenges and Open Issues," *IEEE Access*, vol. 9, pp. 153701-153726, 2021.

[7] Malhi, Avleen Kaur, ShaliniBatra, and Husanbir Singh Pannu, "Security of vehicular ad-hoc networks: A comprehensive survey," *Computers & Security*, vol. 89, pp. 101664, 2020.

[8] Adhikary, Kaushik, et al., "Hybrid algorithm to detect DDoS attacks in VANETs," *Wireless Personal Communications*, vol. 114,

no. 4, pp. 3613-3634, 2020.
[9] Xiao, Shunyuan, et al., "Secure Distributed Adaptive Platooning Control of Automated Vehicles Over Vehicular Ad-Hoc Networks Under Denial-of-Service Attacks," *IEEE Transactions on Cybernetics*, 2021.
[10] Kolandaisamy, Raenu, et al., "A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 6, pp. 6599-6612, 2021.
[11] Fatemidokht, Hamideh, et al., "Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular Ad Hoc networks in intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, 2021.
[12] Mahmudova, Shafagat, "Developing an algorithm for the application of Bayesian method to software using artificial immune systems," *Soft Computing*, pp. 1-7, 2021.
[13] Lang, Wangjie, et al., "Artificial Intelligence-based Technique for Fault Detection and Diagnosis of EV Motors: A Review," *IEEE Transactions on Transportation Electrification*, 2021.
[14] Dagdia, ZainebChelly, Pavel Avdeyev, and MdShamsuzzohaBayzid, "Biological computation and computational biology: survey, challenges, and discussion," *Artificial Intelligence Review*, pp. 1-67, 2021.
[15] Kanwal, Summrina, Amir Hussain, and Kaizhu Huang, "Novel Artificial Immune Networks-based optimization of shallow machine learning (ML) classifiers." *Expert Systems with Applications*, vol. 165, pp. 113834, 2021.
[16] Zhang, Jun, et al., "Deep learning based attack detection for cyber-physical system cybersecurity: A survey, *IEEE/CAA Journal of AutomaticaSinica*, vol. 9, no. 3, pp. 377-391, 2021.
[17] Fatemidokht, Hamideh, et al., "Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular Ad Hoc networks in intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, 2021.
[18] Brown, James, and Mohd Anwar, "Blacksite: human-in-the-loop artificial immune system for intrusion detection in internet of things," *Human-Intelligent Systems Integration*, vol. 3, no. 1, pp. 55-67, 2021.
[19] N. Nishanth, and A. Mujeeb, "Modeling and detection of flooding-based denial-of-service attack in wireless ad hoc network using Bayesian inference," *IEEE Systems Journal*, vol. 15, no. 1, pp. 17-26, 2020.
[20] Alharthi, Abdullah, Qiang Ni, and Richard Jiang, "A Privacy-Preservation Framework based on Biometrics Blockchain (BBC) to Prevent Attacks in VANET," *IEEE Access*, 2021.
[21] M. Poongodi, et al., "Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information based metrics," *IEEE Access*, vol. 7, pp. 158481-158491, 2019.
[22] Yang, Anjia, et al., "DeQoS attack: Degrading quality of service in VANETs and its mitigation," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 4834-4845, 2019.
[23] Zamani, Nurfatihah, et al., "A study on customer satisfaction towards ambiance, service and food quality in Kentucky Fried Chicken (KFC), Petaling Jaya," *Malaysian Journal of Social Sciences and Humanities (MJSSH)*, vol. 5, no. 4, pp. 84-96, 2020.
[24] M. Poongodi, et al., "Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information based metrics," *IEEE Access*, vol. 7, pp. 158481-158491, 2019.
[25] L. Huang, "Design of an IoT DDoS attack prediction system based on data mining technology," *J Supercomput.*, vol. 78**,** pp. 4601–4623, 2022. https://doi.org/10.1007/s11227-021-04055-1

Authors' Profiles

Rama Mercy. S. is a temporary teaching assistant in the Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore. She involved in teaching post graduates based on cyber security in the recent years. Having 15 years of teaching experience, her areas of interest rooted in data mining, network security, cyber security and artificial intelligence. She is pursuing Ph.D as part time in cyber security.

Dr. Ganapathi Padmavathi is the Dean-School of Physical Sciences and Computational Sciences and Professor in the Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women (Deemed to be University), Coimbatore. She has more than 34 years of teaching experience and 26 years of research experience. Her areas of interest include Cyber Security, Wireless Communication and Real Time Systems. She has executed funded projects worth 267.368 lakhs Sponsored by AICTE, UGC, DRDO and DST. Supervised 22 scholars at Ph.D level, she has more than 200 publications in Prestigious conferences and peer-reviewed journals. She is the life members of various professional bodies like CSI, ISTE, ISCA, WSEAS, AACE and AICW. Reviewer for many IEEE Conferences and Journals. She has visited many countries for technical deliberations. She is the Course Co-ordinator for SWAYAM-MOOC on Cyber Security. So far, more than 1,13, 000 learners have enrolled for various sessions and benefitted. She has authored 10 books in Cyber Security and Data Science Domain.

Vidwan Profile Page: https://vidwan.inflibnet.ac.in/profile/132327

How to cite this paper: Rama Mercy. S., G. Padmavathi, "Self-healing AIS with Entropy Based SVM and Bayesian Aggregate Model for the Prediction and Isolation of Malicious Nodes Triggering DoS Attacks in VANET", International Journal of Computer Network and Information Security(IJCNIS), Vol.15, No.3, pp.90-105, 2023. DOI:10.5815/ijcnis.2023.03.07

I. J. Computer Network and Information Security, **2024, 3, 99-114**
Published Online on June 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2024.03.08

Encrypted Access Mapping in a Distinctly Routed Optimized Immune System to Prevent DoS Attack Variants in VANET Architecture

Rama Mercy. S.*
Avinashilingam Institute for Home Science and Higher Education for Women/ Department of Computer Science, Coimbatore, Pin/Zip code- 641043, India
E-mail: ramamercy_cs@avinuty.ac.in
ORCID iD: https://orcid.org/0000-0001-7557-973X
*Corresponding author

G. Padmavathi
Avinashilingam Institute for Home Science and Higher Education for Women/ Department of Computer Science, Coimbatore, Pin/Zip code- 641043, India
E-mail: padmavathi_cs@avinuty.ac.in
ORCID iD: https://orcid.org/0000-0002-5377-4451

Received: 16 February 2023; Revised: 27 April 2023; Accepted: 19 June 2023; Published: 08 June 2024

Abstract: The use of vehicle ad hoc networks (VANET) is increasing, VANET is a network in which two or more vehicles communicate with each other. The VANET architecture is vulnerable to various attacks, such as DoS and DDoS attacks hence various strategies were previously employed to combat these attacks, but the presence of end-to-end transparency and N-to-1 mapping of different IP addresses create failure in the blockage and not able to determine the twelve variants of DDoS attacks hence a novel technique, Encrypted Access Hex-tuple Mapping Attack detection was proposed, which uses triple random hyperbolic encryption, which performs triple random encoding to encrypt traffic signals and obtains the public key by plotting random values in hyperbola to strengthen the access control in the middlebox and Deep auto sparse impasse NN is used to detect twelve variant DDoS attacks in the VANET architecture. Moreover, to provide immunity against attack, the existing approach uses various artificial immune systems to prevent DDoS attacks but the selection of positive and negative clusters generates too many indicator packets. Hence a novel technique, Stable Automatic Optimized Cache Routing proposed, which uses a Deep trust factorization NN to detect irrational nodes without requiring prior negotiation about local outliner factor and direct evidence by automatically extracting trust factors of each node to manage the packet flows and detecting transmission of dangerous malware files in the network to prevent various types of hybrid DDoS attacks at VANET architecture. The proposed model is implemented in NS-3 to detect and prevent hybrid DDoS attacks.

Index Terms: VANET, DDoS, Hyperbolic Encryption, Middlebox, Packet Delivery Ratio, Routing, Nodes, Roadside Unit.

1. Introduction

A major problem in today's world is the traffic conjunction in major metropolitan cities which leads to traffic accidents due to human error or roadways so to overcome these problems vehicular ad hoc network (VANET) a self-organized network is used because in this architecture all the vehicles are interconnected to each other to produce a safe drive. The VANET reduces the number of collisions on the road and provides more comfortable, clean, and safer travel. However, the VANET architecture uses the internet to intercommunicate so it is vulnerable to based network attacks [1-2]. The VANET infrastructure creates communication between dynamic nodes that frequently change directions. Vehicle-to-vehicle communication inside the network is used to communicate information about alert messages and congestion in data transmission using the Roadside Unit (RSU), VANET node receives data from many RSUs, and there is the possibility of numerous hops to transport the information between the nodes. As a result, the network becomes more exposed to many types of attacks, particularly Denial of Service and Distributed Denial of Service

attacks [3-4]. DoS attacks in VANET disrupt legitimate node function by flooding packets to a specific node or network with redundant information and messages. Automated attackers to carry out large-scale DDoS attacks, blocking genuine users from accessing the network. Because of the peculiarities of the VANET design, such as shifting network node topology and decentralization, recognizing malicious assaults, disruptive nodes, and faulty vehicles is challenging [5-7].

Middleboxes are used in VANET to appropriately manage and secure its network resources. However, when end-to-end transparency is employed, any external host, including IPv4 and IPv6 hosts, could scan the entire IPv6 cellular network unless cellular carriers provide extra access control via the middlebox. As a result, an external host attacks the network by flooding packets to generate undesired traffic, acting as the attacker node in data transfer [8-10]. Furthermore, these attacker nodes act as rational nodes to produce hybrid DoS attacks, such as black hole attacks, by supplying incorrect routing information and reducing attack detection performance [11-12]. Black-hole attacks happen when all information from the router is erased. On rare occasions, a router is set up incorrectly to offer a cost-free path to every Internet destination. Previously, several Machine Learning (ML) approaches and Artificial Immune Systems (AIS) were employed to detect DDoS attacks and other hybrid threats [13-15]. However, previous systems were not focused on providing a solution for detecting various types of DDoS attacks. Furthermore, these solutions necessitate prior knowledge of critical network parameters, which adds additional load in a dynamic environment, lowering the attack detection rate and necessitating the use of an excessive number of detectors to enable secure communication. As a result, a unique framework must be developed to improve VANET security through efficient attack detection and trustworthy data transmission. The main contribution of this paper is as follows,

- To prevent hackers to penetrate the VANET architecture the presence of existing 1 to N mapping and not determining the variants of DDoS attacks is overcome by Deep auto sparse impasse NN, which is used to extract features from sensing and mapping reports in order to detect the 12 variants of DoS with blocking external host
- To prevent hybrid DDoS attacks without the selection of positive or negative clustering a novel technique Stable Automatic Optimized Cache Routing is used, in which a routing cache optimization algorithm is used to adopt time and frequency synchronized channel hopping, thereby effectively managing dynamic fluctuating constraints and transmission of dangerous malware files.

The content of the paper is structured as follows: section 2 denotes the literature survey, section 3 provides the technique and the novel solution, results obtained are provided in Section 4; finally, section 5 concludes the paper.

2. Literature Survey

Ahmed et al. [16] have presented a method that is more resistant to different attacks and attempts made by malicious code to access the entire network. It is built on a trust-management method. The scheme's goal is to find harmful data and phony nodes. The simulation results of VANSec are compared with those of trust and LT, two already existing techniques, in terms of trust computation error, end-to-end delay (EED), average link duration (ALD), and normalized routing overhead (NRO). The dependability of the proposed method, however, to jeopardise a node in the VANSec model disseminates fraudulent or faulty information.

Li et al. [17] have proposed an attack-resistant trust management system (ART) for VANETs to evaluate the trustworthiness of both data and mobile nodes in VANETs as well as to identify and react to malicious attacks. Functional trust and recommendation trust, which indicate a node's likelihood of carrying out its functionality and the veracity of its suggestions for other nodes, respectively, are the two dimensions in which node trust is assessed. Based specifically on the data sensed and gathered from multiple cars, a data trust assessment is made. But occasionally, the TrEPS may rely on murky, contradicting traffic information.

Othaman et al [18] developed Physically Safe Privacy-Preserving Message Authentication Using a Physical Unclonable Function (PUF). Even in the event of memory leakage, that protocol maintains security and privacy against passive and active attacks. The entities (i.e., vehicles, RSU) use their PUF to reassemble a secret polynomial-share in order to create pairwise temporal secret keys (PTKs) with other entities. In contrast to previous protocols, this protocol encrypts BSMs (using PTKs) to boost security and avoid vehicle tracing attacks, although it has difficulty mapping produced polynomials.

Bensaber et al. [19] developed an applied Adaptive Neuro-Fuzzy Inference System to develop a prediction model for the security index in VANET (ANFIS). The first step in the research process to build a database of attack occurrences is network simulations. After that, this latter is created and statistically evaluated. In order to achieve a high level of communication security, it is necessary to use robust routing algorithms that make it easier to detect and thwart unauthorized network intrusions in addition to secure communication frameworks.

Velayudhan et al. [20] developed the Emperor Penguin Optimization-based Routing protocol (EPORP), which aims to both detect Sybil attacks and enhance system efficiency. Improved VANET security and detection of the Sybil attack are the main objectives of the research. The original goal is achieved with the help of the Rumor riding strategy, which detects the Sybil assault in the urban VANET. The Split XOR (SXOR) process is employed like that to strengthen system security. The SXOR process employs Emperor Penguin Optimization (EPO) to aid in the creation of

the optimum key. DoS attack variations weren't found in this protocol model, though.

Aldhaheri et al. [21] develop a ground-breaking hybrid Deep Learning and Dendritic Cell Algorithm within the context of an Intrusion Detection System (DeepDCA). The framework uses the Self Normalizing Neural Network and the Dendritic Cell Algorithm (DCA) (SNNN). This study aims to categorize IoT infiltration and lessen the generation of erroneous alerts. By streamlining and automating the signal extraction process, classification performance be improved. The suggested IDS begins by choosing the most practical set of characteristics from the IoT-Bot dataset, followed by SNN signal categorization and DCA classification. This method needs too many detectors, and the system uses a negative selection technique in the sensing layer.

Raenu Kolandaisamy et al. [22] developed a DDoS attack detection based on the communication level of the entire VANET system. In this method, the source node will send data or information to the destination using immediate nodes and to minimize DDoS attacks, a proposed method of a packet marking based on adapted stream region (PMBASR) is used to trace back the source node and then the node of origin is used in the RSU server for the data request and at the same time, data will receive a response in the network. The (PMBASR) uses an analytical approach to detect DDoS attacks. This method only minimizes the DDoS attack, not prevent them.

Kaushik Adhikary et al. [23] This paper presents a hybrid detection-based algorithm based on the SVM kernel methods of AnovaDot and RBFDot for detecting DDoS attacks in VANETs. In this hybrid algorithm, features like collision, packet drop, and jitter have been used to simulate a real-time network communication scenario when the network is operating under normal conditions and a DDoS attack. This algorithm is superior in detecting DDoS attacks compared to the models based on single SVM kernel algorithms AnovaDot and RBFDot. This model only detects DDoS attacks, not prevents them.

Sousa et al [24] proposed an Intrusion Detection System (IDS) for detecting Flooding attacks in vehicular scenarios. The Network Simulator 3 (NS-3) can also be used to simulate 5G-enabled vehicle scenarios. Then create four datasets with various node, attacker, and mobility patterns taken from the Simulation of Urban MObility (SUMO) model. Each dataset included a unique scenario with a unique assortment of sender and receiver vehicles. A flooding attack was simulated in each dataset with a variable number of attackers. The resulting datasets were thoroughly merged and validated to provide accurate, precise, identifiable classification results for the flooding behaviour in the simulated scenarios (F-1 score). However, this method does not combine data from many attacks and scenarios to provide more complex information.

Gaurav et al. [25] created a DDoS detection technique that allows vehicles in the VANET to share critical information because the attacks are identified quickly. The model's fog-based DDoS detection technique. The model employs fuzzy logic to distinguish between attack and regular traffic. Only 5g networks can utilize this strategy.

Overall previous models [16] suffer from minimum reliability with inaccurate data [17] have poor connectivity due to high contradiction in traffic data [18] with low scalability issue the mapping of secret polynomial between users was difficult [19] as the routing algorithms were not robust enough the desired level security has not been possible [20] unable to find different types of attack and [21] require too many detectors to provide immunity in VANET architecture [22] minimize the DDoS attack not completely prevent them [23] only detect attack not prevent them [24] do not generate more complex data from different attacks and scenarios and [25] only used in 5g enable smart cities. Hence, there is a need for a novel DDoS attack detection system to eliminate all these limitations in the existing systems.

3. Encrypted Access Mapping in a Distinctly Routed Optimized Immune System

VANETs are vulnerable to numerous types of DDoS assaults. Various AIS strategies were previously employed in prior models to combat these attacks various Machine Learning (ML) techniques and Artificial Immune Systems (AIS) have been used previously but they have not focused on providing a solution for the detection of various forms of DDoS attacks and create an additional burden in the network environment. Hence a novel technique is proposed for Encrypted Access Hex-tuple Mapping Attack detection. Where the triple random hyperbolic encryption, performs random encoding three times to encrypt traffic signals and determine the public key by plotting random values as coefficients in hyperbola to strengthen the access control in the middlebox. Once the scanning is initiated hex-tuple matched mapping is used to map all the same IP addresses in a symmetrically matching hex-tuple value. Then Deep auto sparse impasse NN is used to extract features from the mapping report to detect twelve variants of DDoS attacks. Furthermore, to prevent these dangerous attacks various AIS techniques were used previously but they require positive or negative selection of clusters to provide immunity against DDoS attacks by arbitrarily generating too many indicator packet frames in dissimilar ways thereby not suitable for varying numbers of dangerous malware files in real-time. Hence a proposed technique Stable Automatic Optimized Cache Routing is used, in which Deep trust factorization NN detect irrational node without requiring prior negotiation and automatically extracts the trust factors of nodes. Then, the Moth Flame Optimization algorithm a population optimization algorithm used to create a balance between cluster groups with relation nodes to obtain a high packet delivery ratio without the need for positive or negative selection and Cache parallelized circulation link routing is applied to provide multiple parallelized path links in regular circular updation with adopting time and frequency synchronized channel hoping thereby effectively manage dynamically fluctuating constraints and transmission of dangerous malware files. Hence by preventing hybrid DoS attacks, the proposed model is used to detect and prevent various types of DDoS attacks.

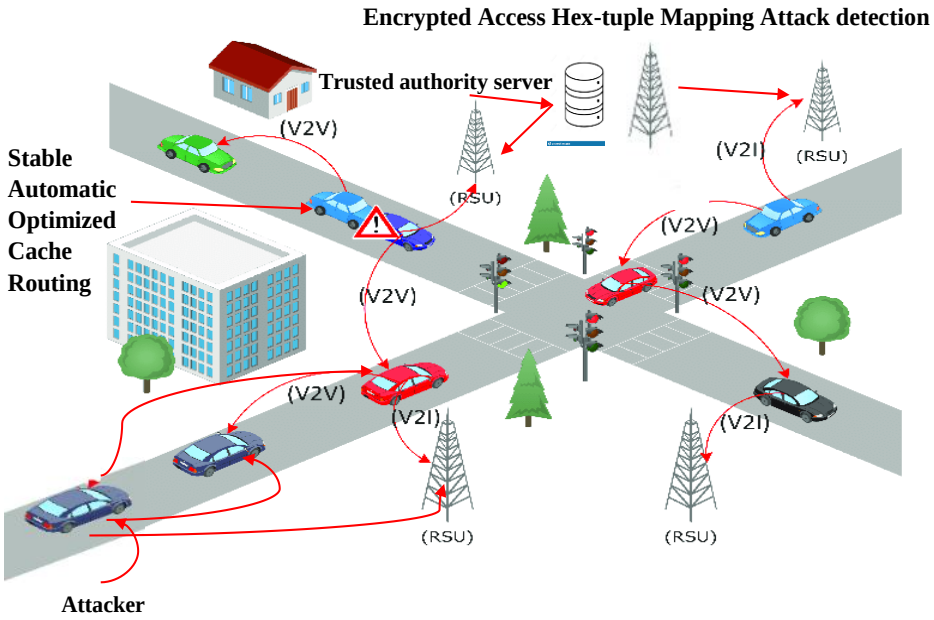

Fig.1. Block diagram for encrypted access mapping in a distinctly routed optimized immune system

Fig. 1 depicted the block diagram for the proposed model. The proposed model for Encrypted Access Mapping in a Distinctly Routed Optimized Immune system initially uses two methods for the detection and prevention of DDoS attacks. The Encrypted Access Hex-tuple Mapping Attack detection is used to perform a triple random hyperbolic encryption and map all the IP addresses in a systematic tuple value and uses Deep auto sparse impasse NN to extract information to detect twelve variants of DDoS attack. Stable Automatic optimized cache routing, which use deep trust factorization NN to detect irrational node without negating outline factor and direction. Then, the Moth Flame Optimization algorithm is used to collect and obtain a high packet delivery ratio, and Cache parallelized circulation link routing is used to manage dynamically fluctuating constraints and transmission of dangerous malware files hence preventing DDoS attacks.

3.1. Encrypted Access Hex-tuple Mapping Attack Detection

The traffic signals within the network are encrypted using triple random hyperbolic encryption, which performs an encoding three times to encrypt all the traffic in the VANET network and plot the values as a coefficient in a hyperbola to determine the public key. The architecture of Encrypted Access Hex-tuple Mapping Attack detection has been shown in fig. 2.

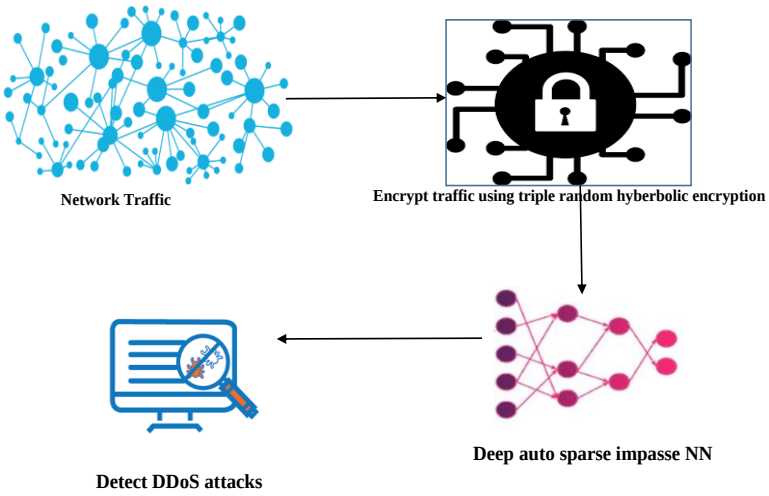

Fig.2. Block diagram for encrypted access hex-tuple mapping attack detection

In hyperbolic encryption to choose the coefficient the equation (1) follows:

$$x^2 - Dy^2 = 1 \tag{1}$$

The equation (1) is equation of hyperbola, and pick a base point $G = (x_0, y_0)$ with a large order r and this gives us $G^r = E$ and select an integer m and $m < r$ computes $B = G^m mod\ 2$, the private keys are formed by (G,B). In encryption process choose the secret integer k and Computes in following equation (2) & (3)

$$H = G^k mod\ n \tag{2}$$

$$T = B^k w mod\ n \tag{3}$$

The equation (2) and (3) produce the cipher text (H, T) and in decryption process the is compute as following equation:

$$R = H^m mod\ n \tag{4}$$

The data is recovered by the following equation:

$$w = T / R mod\ n \tag{5}$$

The proposed model uses a process called hex tuple matched mapping to map all the network resources such as source IP, destination IP, source port number, destination port number, public key, and IP address range in an N to N mapping. The mapping structure is shown in figure 3 and the mapping of the IP address in a tuple means the value is immutable.

Node:1 IP:192.168.0.1 Source IP: 192.168.0.3 Destination Source port: 4356 Destination port:8975 IP:192.168.0.10 MAC:44:02:EF:9C:09:4E Public key: C*F-JaNdRgUkXp2s5v8y/A?D(G+KbPeS	Node:2 IP:192.168.0.2 Source IP:192.168.0.7 Destination IP: 192.168.0.17 Source port: 4595 Destination port:7885 MAC:A9:4E:47:AC:DA:B9 Public key: C*F-JaNdRgUkXp2s5v8y/A?D(G+KbPeS	Node:3 IP:192.168.0.3 Source IP:192.168.0.1 Destination IP:192.168.0.8 Source port: 4686 Destination port: 8549 MAC:8C:9D:39:67:4C:59 Public key: C*F-JaNdRgUkXp2s5v8y/A?D(G+KbPeS	Node: N IP:N Source IP:N Destination IP:N MAC:N Source port: N Destination port: N Public key: C*F-JaNdRgUkXp2s5v8y/A?D(G+KbPeS

Fig.3. The value stored in hex tuple mapping

The discovery of misconfiguration in the middle box will lead to performance degradation making it vulnerable to attacks. In the proposed model, the middlebox is used to control the nodes and does N to 1 mapping IP address. To detect twelve variants of hybrid DDoS attacks by blocking external hosts and so provide end-to-end network transparency, the Encrypted Access Hex-tuple Mapping Attack Detection model uses Deep Auto Sparse Impasse NN, which gathers the data from sensing and mapping reports to detect the attacker node on the network. The diagram of Deep Auto Spare Impasse NN is given in fig. 4.

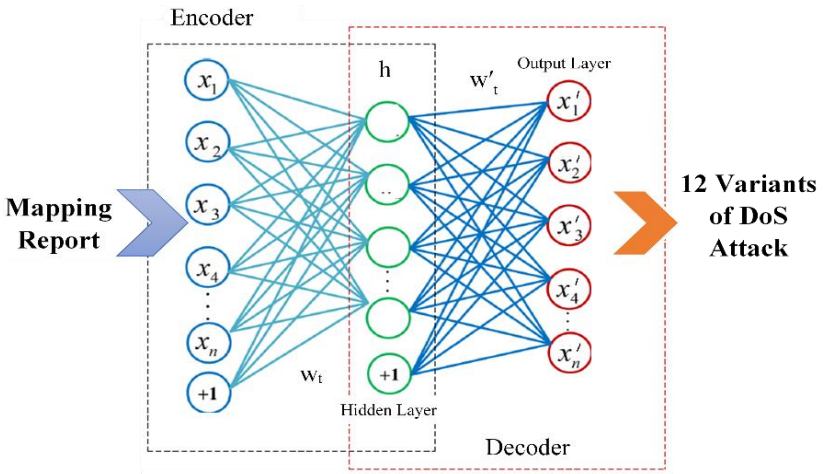

Fig.4. Deep auto sparse impasse NN

The Deep Auto Sparse Impasse Neural Network is a type of structure made up of numerous basic neurons acting as nodes or elements. These components are constantly working together in parallel. The connections between the neurons have a significant role in how the Deep Auto Sparse Impasse Neural Network functions. These neurons are linked together via links, and each link has weights that are adjustable values. The neural network consists of the input layer in which the mapping report is sent as an input and the connection between the neurons in the neural network is close to zero because if there is more connection between neurons it takes more memory and the connections do not affect the accuracy of the neural network. The prediction speed of the neural network is twenty-five times faster than a regular neural network.

When dealing with Deep Auto Sparse Impasse neural networks, the number of layers and nodes are chosen using similar concepts as in standard neural networks, but there are several concerns that are unique to these sparse networks. Neurons are grouped logically in three layers that make up the Deep Auto Sparse Impasse NN. The Deep Auto Sparse Impasse NN has three layers (the input layer, the hidden layer and the output layer), one neuron in the output layer, and a variable number of neurons in the hidden layer. The values of each output vector member fall between [-1,1]. Neurons on both layers have "tan-sigmoid" transfer functions. This function condenses the result into the range [-1,1] from an input that can be any value between plus and minus infinity. The Deep Auto Sparse Impasse NN contains fewer active connections or parameters, resulting in more efficient and interpretable models. Which connections are present and which are pruned or set to zero are determined by the sparsity pattern. The pruning approach used in this sparse neural network eliminates the superfluous connections and reduces the number of parameters.

The unformatted training set is used in the Auto Sparse Impasse NN to provide the mapping report as the auto-encoder input data and it is shown in equation (6) below

$$x = (x_1, x_2, x_3, ..., x_n) \tag{6}$$

The hidden and output layer neurons are activated by sigmoidal activation function which is shown in the below equation (7)

$$g(s_k) = \frac{1}{1+e^{-s_k}} \tag{7}$$

where, s_k represents the cumulative input signal of the k-th neuron in the hidden or output layer of the NN and it is given in equation (8) below,

$$s_k = \sum_{i=1}^{n} (w_{i,k}\ x_{i,k} + x_0\ f_k) \tag{8}$$

where, $w_{i,k}$ is the the link weight from the previous layer's i-th neuron to the hidden or output layer's k-th neuron, x_0 is the input link weight of neuron and the offset of k-th neuron is represented by f_k.

The below equation (9) shows the output data signal from the neural network having L number of neural layers,

$$h_{w,f}(x) = A^{(L)} \tag{9}$$

where, $A^{(L)}$ is the value array of output layer neuron.

The twelve variants of DDoS attack are identified and predicted by this Sparse Impasse output layer. Only a subset of connections or weights is active in the Deep Auto Sparse Impasse NN, with the remainder set to zero. Because zero-valued connections do not need to be processed, this sparsity minimizes computing costs during training and inference. Consequently, fewer procedures are needed, resulting in quicker training time and this NN has a high prediction accuracy for DDoS attacks. The mode used detects NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN, and TFTP DDoS attacks.

3.2. Stable Automatic Optimized Cache Routing

To detect the node that causes hybrid DDoS attack is detected and to provide immunity to DDoS attacks in the network, a novel method of Stable automatic optimization is used in which Deep trust factorization NN is used in which the nodes are connected using a trust score and provides access to nodes based on the trust score which is shown in fig. 5.

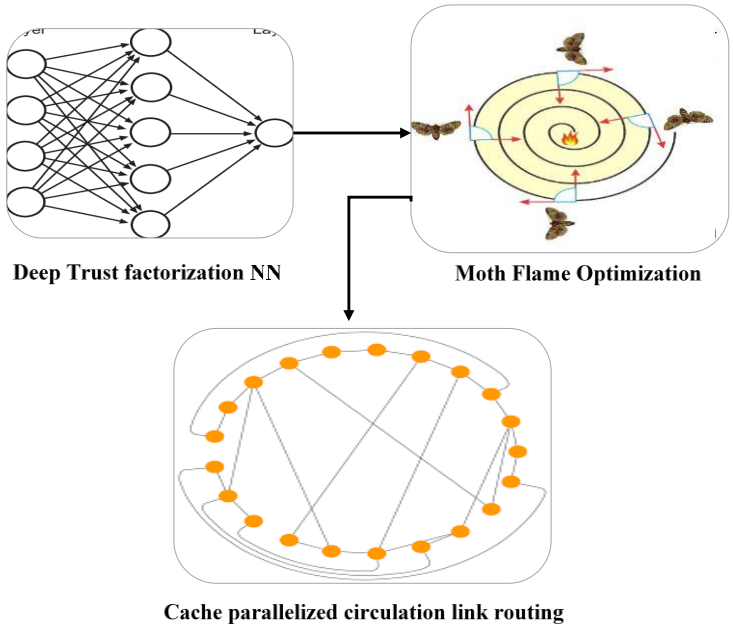

Fig.5. Block diagram for stable automatic optimized cache routing

The architectural diagram of Deep trust factorization NN has been shown in fig. 6 that is responsible for detecting the trust values thereby it predicts the rational nodes.

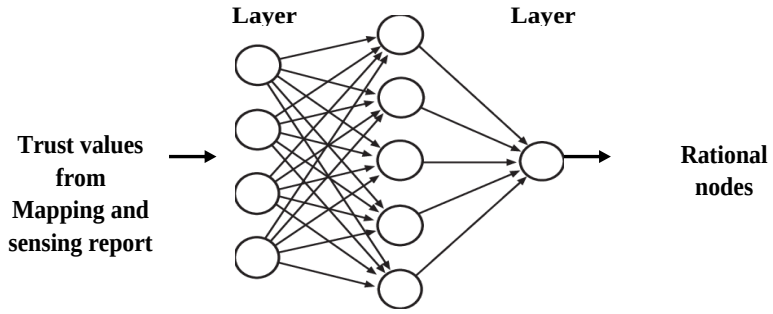

Fig.6. Deep trust factorization NN

In fig. 6 the structure of Deep trust factorization NN is given and the neural network consists of an input layer, a hidden layer, and one output layer. The data gathered from the detection of the DDoS attack is used to give the input in trust factorization. The output layer consists of one layer to ensure whether the node is trusted or not by the trust score added to each node by the hidden layer. Then, the Moth Flame Optimization algorithm is used to form a balanced cluster group and relation node to obtain the maximum packet delivery ratio (PDR). To ensure the connectivity of each node in the cluster group, the Moth Flame optimization algorithm is a population-based algorithm used to detect the best path in the network by updating each position in the node. Three different functions are used in the optimization of the proposed model as follows:

$$M = (I, P, T) \tag{10}$$

In equation (10) I refers to the random location of the vehicle node $(I : \phi \rightarrow \{M\})$, P refers to the motion of the vehicle node in the search space $(P : M \rightarrow M)$, T refers to finish the search process $(T : M \rightarrow \text{true, false})$ and the following represent the I function:

$$M(i, j) = (ub(i) - lb(j)) \times rand\ (j) + lb(i) \tag{11}$$

In equation (11) lb and ub indicate the lower and upper bounds of the variable. The search takes place in transverse orientation the spiral initial point should start from the vehicle node and the spiral final point should be positioned next vehicle node and fluctuation of range should not exceed search space. The spiral equation follows as.

$$S(M_i, F_j) = D_i . e^{bt} . cos(2\pi t) + F_j \tag{12}$$

In equation (12) the D_i refer to the space between the i^{th} node and j^{th} node, b indicates a fix to define the shape of the logarithmic spiral, and t indicates a random number between $[-1,1]$. The balancing between exploitation and exploration is guaranteed by the spiral motion of the node near the next node in the search space. The moth Flame optimization algorithm is given below.

Algorithm: Moth Flame Optimization Algorithm

Initialize the parameters for the vehicle
Initialize the vehicle at a position M_i randomly
for $i = 1$ to n **do**
  calculate the fitness function f_i
end for
while iteration ≤ Max_iteration **do**
  Update the position of M_i
  Calculate the number of vehicles
  Evaluate the fitness function f_i
if $iteration == 1$ **then**
  $F = sort(M_{t-1}, M_t)$ and $OF = sort(M_{t-1}, M_t)$
end if
for $i = 1$ to n **do**
 for $j = 1$ to **do**
  update the values of r and t
  calculate the value of D concerning its corresponding vehicle
  update $M(i.j)$ respect to its corresponding moth using
  end for
 end for
end while

The algorithm initials with a vehicle and M_i a random vehicle. The iteration took place to detect paths with a high packet delivery ratio (PDR). The Cache parallelized circulation link routing is applied to make time and frequency synchronization base channel hopping on a network to effectively manage the dynamic fluctuation of each node and remove the transmission of dangerous malware files on the network. The method eradication of the twelve variants of hybrid DDoS attacks without reducing the high packet delivery. The circular routing process packet and hoping process on circular link state is a process of the nodes instead of changing the channel randomly each node knows the sequence where they should be and is always able to communicate. The proposed optimization algorithm connects the node in the circular link to make the nodes in regular circular updation with effective hopping between one node and another node.

Overall, the Encrypted Access Mapping in a Distinctly routed Optimized Immune System has been proposed to provide immunity to the VANET network against the twelve types of hybrid DDoS attack by Encrypted Access Hex-tuple Mapping Attack detection, a process in which all the traffic in the network is encrypted using triple random hyperbolic encryption and the middlebox does the N to 1 mapping of IP address. The Stable Automatic Optimized Cache Routing used deep trust factorization NN to detect the irrational node by adding the trust score and Moth Flame Optimization algorithm to obtain the high packet delivery ratio. The Cache parallelized circulation link routing is applied to synchronize the time and frequency of each node, therefore, eliminating the malicious traffic in the network. So, the proposed model provides immunity to the DDoS attacks on the VANET architecture.

4. Result and Discussion

This section includes a thorough analysis of the performance of the proposed network model, the implementation results simulated in the NS-3 platform, and a comparison section to make sure the proposed model is immune to DoS attacks.

4.1. Experimental Setup

The proposed system is simulated in Python and this section provides a detailed description of the implementation results and the performance of the proposed system and a comparison section to ensure that the proposed system performs valuable.

Software: NS-3
OS: Windows 10 (64-bit)
Processor: Intel i3

RAM: 8GB RAM

4.2. Dataset Description

The dataset used in the proposed model is CICDDoS2019. The dataset contains the most common DDoS attacks, which resemble true real-world data. It also includes the result of the network traffic analysis using CICFlowMeter-V3 with labeled flows based on the time stamp, source, destination IP address, protocols, and attack (CSV files). This dataset has different modern reflective DDoS attacks such as NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN, and TFTP. The dataset itself is organized per day and the raw data is captured by the Pcaps. This data set is used in the proposed model to detect the DDoS attack on the VANET architecture.

4.3. Simulated Output of Proposed Model

The simulated output of the proposed model for attack detection and prevention has been explained in this section from initial setup itself.

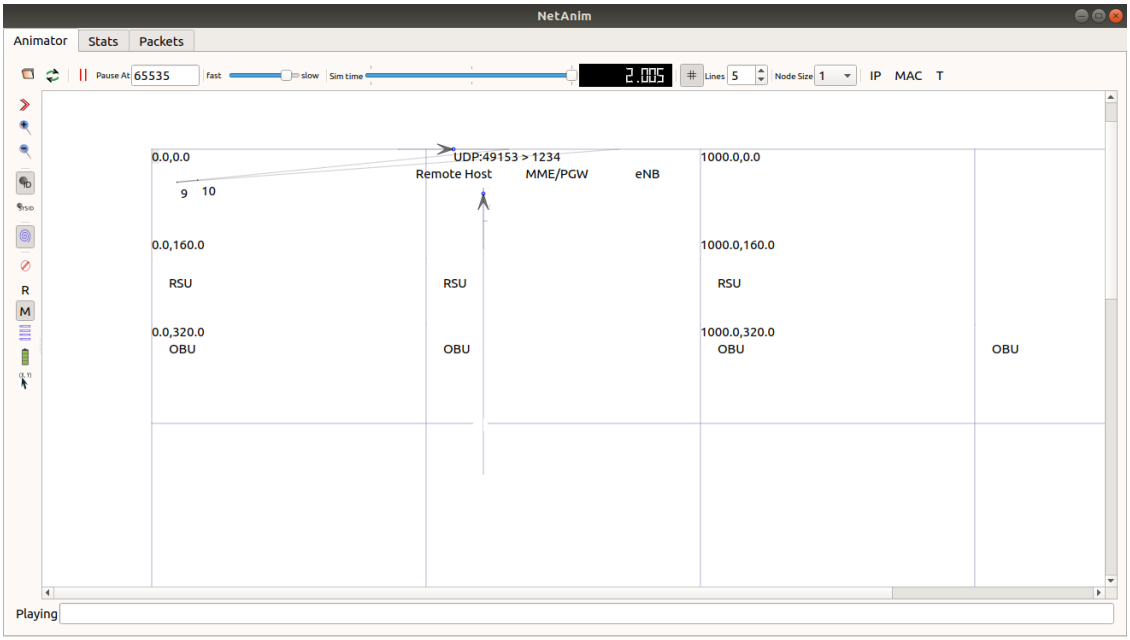

Fig.7. Simulation of the proposed model in NS-3

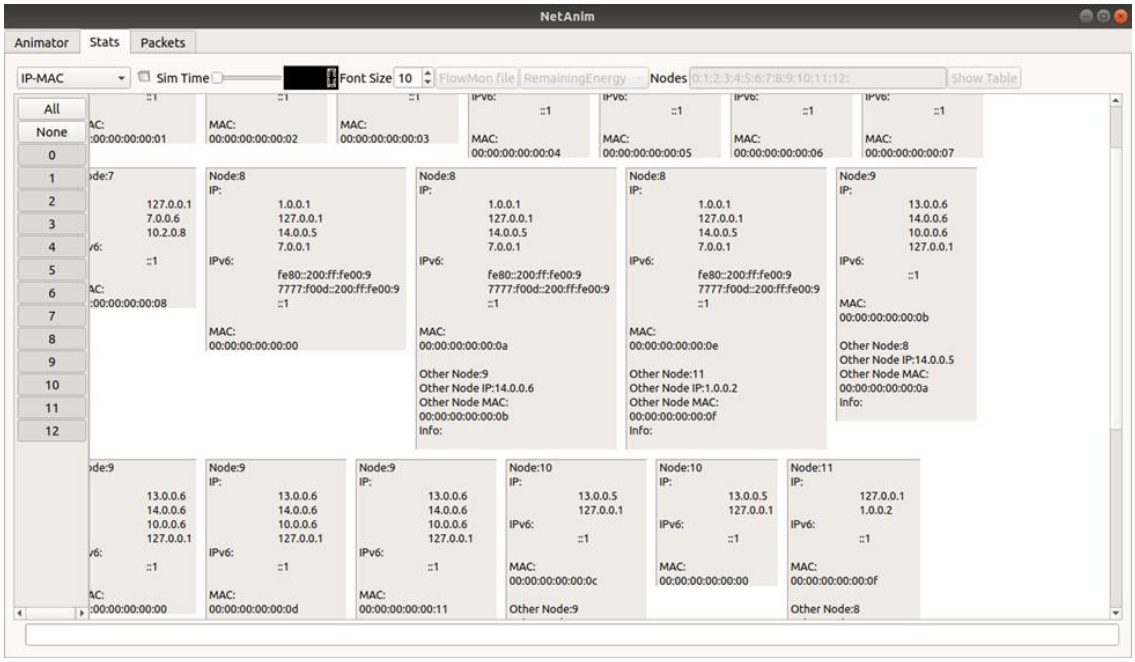

Fig.8. Statistics of the proposed model in NS-3

The animation of the proposed model is shown in fig. 7, an overall architecture of VANET. The main architecture of VANET consists of a Board Unit (OBU), which allows the vehicles to communicate with Road side unit (RSU) or other OBU, and the figure shows the number of nodes that are interconnected to each other. They represent the data flow from each node in fig. 4.

The network status of each node in the proposed system is given in fig. 8. The statistics of each node include the Media Access Control (MAC), IPv4 address, IPv6 address, and the details of the node connected. The proposed model uses triple random hyperbolic encryption to encrypt the traffic and deep auto sparse impasse NN to map the report to detect the DDoS attacks.

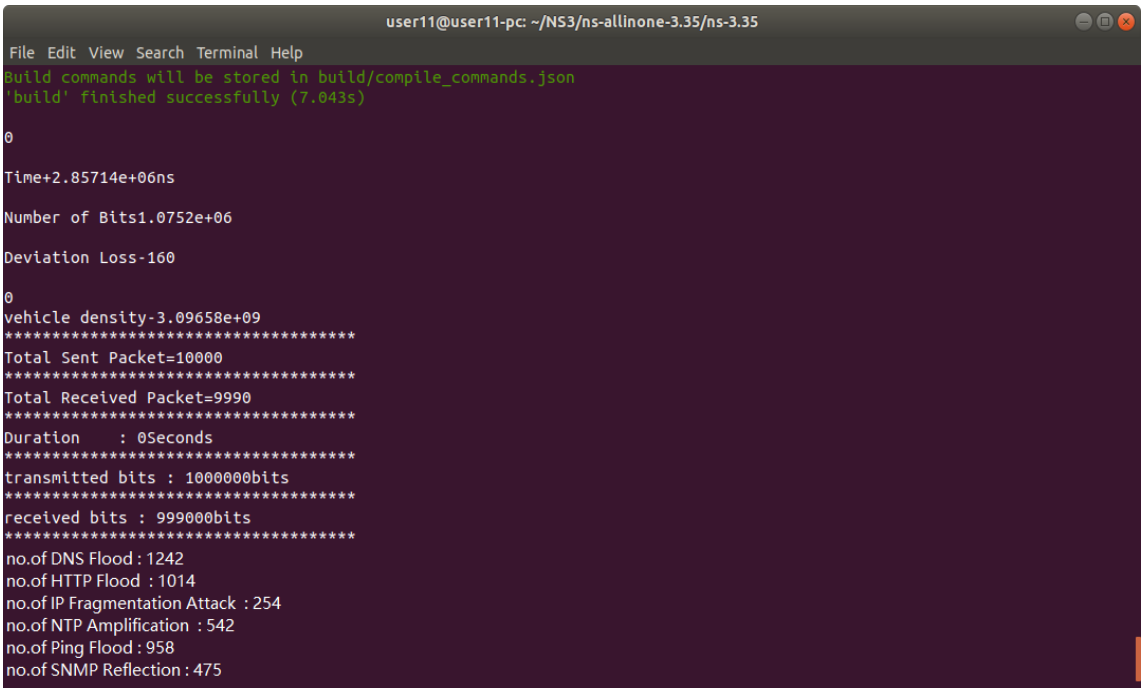

Fig.9. Output of the simulation

In fig. 9 the output simulation of the proposed system is given and it indicates the number of bits transferred in the time and the deviation loss or packet loss on the network. the vehicle density is how close the vehicle gets to and the total packets send & received in the network, the duration indicates the time taken to send & receive the packets. The output also indicates the number of requests sends to cause DDoS attacks such as DNS flood, HTTP flood, fragmentation attack, NTP amplification, Ping flood, and SNMP reflection, and the proposed model is able to detect twelve types of DDoS attacks and protect the network from packet loss and other hybrid attacks.

4.4. Performance Metrics of the Proposed System

The performance of the proposed approach and the achieved outcome was explained in detail. This section is to explain the proposed model detection of various types of DDoS attacks such as UDP Flood, DNS Flood, HTTP, NTP, Ping Flood, SNMP, SYN flood, Smurf, LDAP, MSSQL, NetBIOS, SSDP, WebDDoS and TFTP.

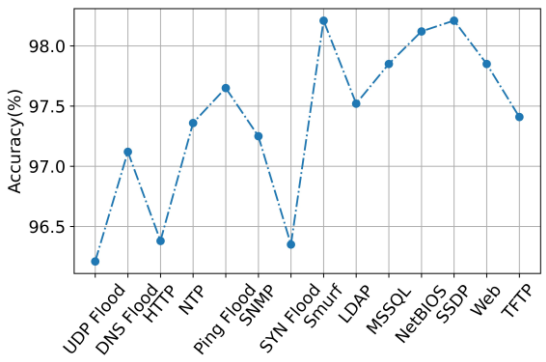

Fig.10. Accuracy of the proposed model in the prediction of different types of DDoS attacks

The graph in fig. 10 shows the accuracy of the proposed model as it detects UDP Flood with 96.2% accuracy, DNS Flood with 97.2% accuracy, HTTP with 96.4% accuracy, NTP with 97.45% accuracy, Ping Flood with 97.7% accuracy,

SNMP with 97.35% accuracy, SYN flood with 96.4% accuracy, Smurf with 98.4% accuracy, LDAP with 97.5% accuracy, MSSQL with 97.5% accuracy, NetBIOS with 98.2% accuracy, SSDP with 98.4% accuracy, WebDDoS with 97.7% accuracy and TFTP with 97.45% accuracy. The proposed model has high accuracy because Encrypted Access Hex-tuple Mapping Attack detection which uses Deep auto sparse impasse NN for attack detection which extracts features from sensing and mapping report to detect hybrid DDoS attacks.

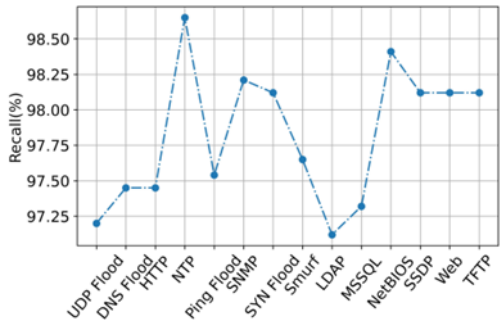

Fig.11. The recall of the proposed model in detecting different types of DDoS attacks

The graph in fig. 11 shows the recall of the proposed model as the graph explains the model detects UDP Flood with 97.2% recall, DNS Flood with 97.45% recall, HTTP with 97.45% recall, NTP with 98.65% recall, Ping Flood with 97.53% recall, SNMP with 98.2% recall, SYN flood with 98.15% recall, Smurf with 97.67% recall, LDAP with 97.15% recall, MSSQL with 97.3% recall, NetBIOS with 98.45% recall, SSDP with 98.15% recall, WebDDoS with 98.15% recall and TFTP with 98.15% recall. The proposed model Encrypted Access Hex-tuple Mapping Attack detection has high recall because it uses hex-tuple mapping in which the same IP address is mapped using a hex tuple value.

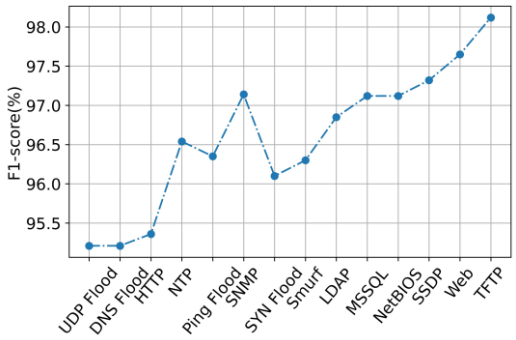

Fig.12. F1-Score of the proposed model

The F1-Score of the proposed model is shown in fig. 12, F1-Score is used to calculate the mean of precision and recall. The proposed model detects UDP Flood with 95.2% F1-Score, DNS Flood with 95.2% F1-Score, HTTP with 95.45% F1-Score, NTP with 96.5% F1-Score, Ping Flood with 96.4% F1-Score, SNMP with 97.2% F1-Score, SYN flood with 96.15% F1-Score, Smurf with 96.4% F1-Score, LDAP with 96.85% F1-Score, MSSQL with 97.1% F1-Score, NetBIOS with 97.1% F1-Score, SSDP with 97.4% F1-Score, WebDDoS with 97.6% F1-Score and TFTP with 98.15% F1-Score. The proposed model has high F1-Score because it uses the Encrypted Access Hex-tuple Mapping Attack detection which uses a Deep auto sparse neural network to detect various hybrid DDoS attacks.

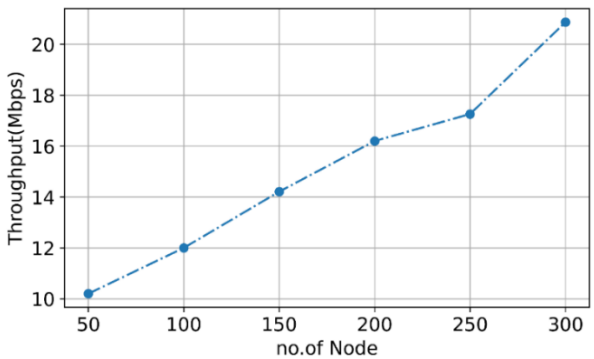

Fig.13. The throughput of the proposed system

The throughput is the amount of information that the system process in a given time the throughput of the proposed model is given in fig. 13. The number of nodes in the proposed model increases the throughput of the amount of data the network takes to transfer also increases. The time taken for the packet to transfer is 0 seconds because the proposed model uses Stable Automatic Optimized Cache Routing in which circular link state routing is used to adopt time and frequency synchronization channel hopping to get a high delivery ratio.

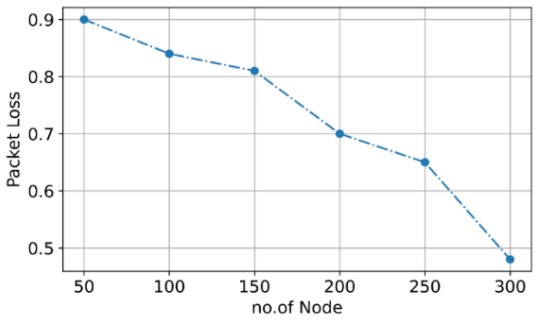

Fig.14. The packet loss of the proposed model

In fig. 14, the graph for packet loss of the proposed model is given. The proposed model has very low packet loss. The graph indicates the packet loss at the 50 nodes present in the VANET. The packet loss for each node is 0.9 bits, and as the number of nodes increases, the packet loss for each node increase to 300 the packet loss for each node decrease to 0.5 bits. The proposed model has low packet loss because the novel solution Stable Automatic Optimized Cache Routing uses Cache parallelized circulation link routing to effectively route the packages to minimize the packet loss.

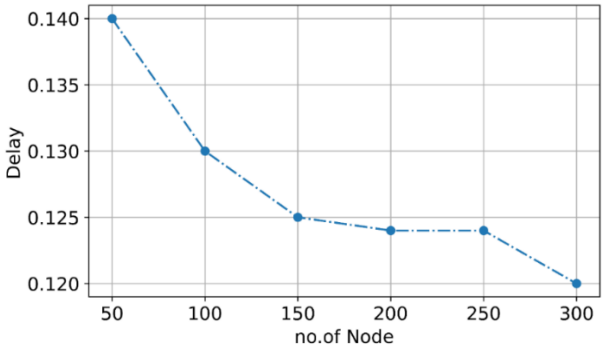

Fig.15. The delay of a packet in the proposed model

The delay in a network is known as lag or latency amount of time taken for the packet to travel through multiple nodes. The delay of the proposed model is given in fig. 15. The graph indicates the proposed model has a low delay of 0.14 seconds for 50 nodes; when the node value increases to 300 nodes, the delay decreases to 0.12 seconds. The proposed model has low delay because of a novel approach Stable Automatic Optimized Cache Routing which uses circular link state routing in which a time and frequency-based channel hopping takes place to minimize the packet delay.

4.5. Comparison Results of the Proposed Network Model

The comparisons are made from the previous techniques with various packet delivery ratios (PDR), attack detection, detection time, routing overhead, and false classification ratio. Comparisons are made with the existing techniques such as Trilateral trust, Host-based intrusion detection system (H-IDS), Multi filter, and Stream Position Performance Analysis (SPPA) [11].

The comparison of the packet delivery ratio of various models is shown in fig. 16. The packet delivery ratio of the proposed model is compared with the existing models such as Trilateral trust, H-IDS, Multi filter and SPPA. From the graphical representation, when the number of nodes increased, the packet delivery ratio of the proposed system also increased. When the proposed model's number of node is 20, the packet delivery ratio of the proposed model attains at 5%. The proposed model has high packet deliver ratio of 98% than existing models even though the number of nodes increased. The graph is used to assume that the model Trilateral trust has the least packet delivery ratio. The proposed model has a high packet delivery ratio because of the novel technique of Stable Automatic Optimized Cache Routing.

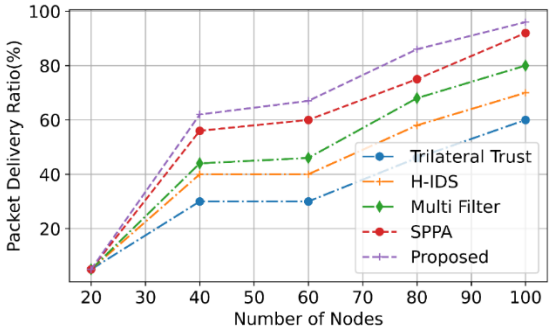

Fig.16. The packet delivery ratio comparison

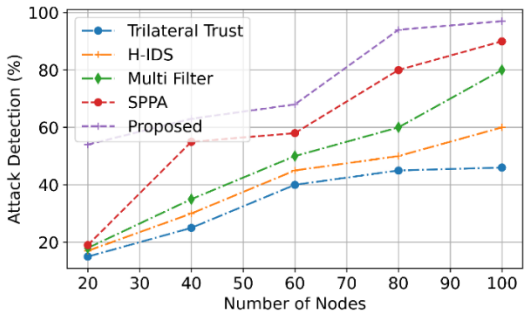

Fig.17. The attack detection comparison proposed model

The comparison of attack detection of various models is shown in fig. 17. The attack detection of the proposed model is compared with the existing models such as Trilateral trust, H-IDS, Multi filter and SPPA. From the graphical representation, when the number of nodes increased, the attack detection of the proposed system also increased. When the proposed model's number of node is 20, the attack detection of the proposed model attains at 55%. The proposed model has high attack detection accuracy of 99% than existing models when the number of nodes is 100. The graph also indicates the attack detection of an increase in the number of nodes has no deviation in detection accuracy. The graph used to assume that the model Trilateral trust has the least accuracy in attack detection. The proposed model has high attack detection accuracy because of the novel technique of Encrypted Access Hex-tuple Mapping Attack detection.

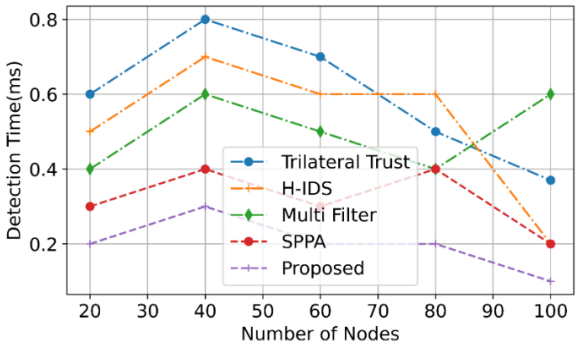

Fig.18. The comparison of time taken to detect the DDoS attacks in the proposed model

The comparison of time taken to detect various DDoS attacks in the previous model is shown in fig. 18. The detection time of the proposed model is compared with the existing models such as Trilateral trust, H-IDS, Multi filter and SPPA. When the proposed models number of node is 20, the detection time of the proposed model attains at 0.6ms. when the number of nodes increases, the proposed model takes less time to detect DDoS attacks of 0.2 *ms* that's extremely fast than existing models. The graph used to assume that the model Multi filter has taken more time to detect DDoS attacks than other models. The proposed model takes less time to detect DDoS attacks because of the proposed novel technique Encrypted Access Hex-tuple Mapping Attack detection.

The routing overhead is the amount of packet taken to check whether the neighbor node is active. Fig. 19 shows that the proposed model has a very low routing overhead than the existing model. The routing overhead of the proposed model is compared with the existing models such as Trilateral trust, H-IDS, Multi filter and SPPA. From the graphical representation, when the number of nodes increased, the routing overhead of the proposed system also increased. When the proposed models number of node is 20, the routing overhead of the proposed model attains at 225 packets. The

routing overhead of the proposed model, even after the number of node increase to 100, is still around 650 packets. The graph used to assume that the model. Trilateral trust has a very high routing overhead. The proposed model has very low routing overhead because of the novel solution Stable Automatic Optimized Cache Routing.

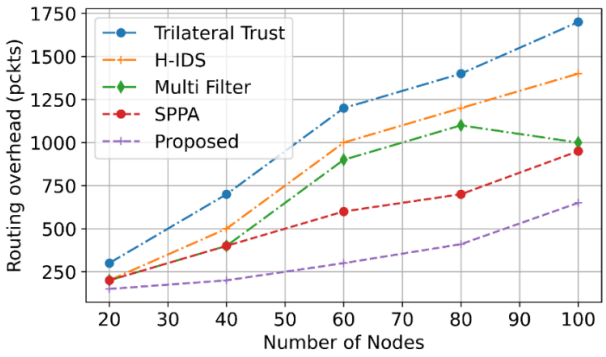

Fig.19. The routing overhead comparison

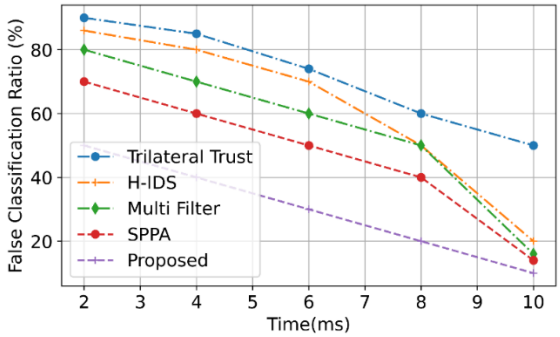

Fig.20. Comparison of false classification ratio

The false classification ratio is the number of negative cases mistakenly reported as positive. Fig. 20 shows that the proposed model has a low false classification ratio of 5%. The false classification ratio of the proposed model is compared with the existing models such as Trilateral trust, H-IDS, Multi filter and SPPA. From the graphical representation, when the time (ms) is increased, the false classification ratio of the proposed system is decreased. When the proposed models time is at 2ms, the false classification ratio of the proposed model attains at 225 packets. If the number of ms increase, the proposed model still has a very low false classification ratio. The Trilateral trust has a very high false classification ratio. The proposed model has a very low false classification ratio because of the novel solution novel technique, Encrypted Access Hex-tuple Mapping Attack detection.

Table 1. Overall table for the comparison of the previous model and the proposed model

Methods	Packet delivery ratio	Attack detection accuracy	Detection time	Routing overhead	False Classification ratio
Trilateral trust	60%	42%	0.3 ***ms***	1700 ***pkt***	50%
A host-based intrusion detection system (H-IDS)	70%	60%	0.2 ***ms***	1400 ***pkt***	20%
Multi filter	80%	80%	0.6 ***ms***	1000 ***pkt***	15%
Stream position performance analysis (SPPA)	90%	90%	0.2 ***ms***	990 ***pkt***	10%
Proposed	98%	99%	0.1 ***ms***	600 ***pkt***	5%

Table 1 gives the overall data of the comparison between the previous and proposed models. The proposed model is more effective and relevant when compared to the existing technologies, in which the other models have not acquired a high attack prediction ratio and the proposed model also has an efficient routing protocol to reduce routing overhead and ensure a high packet delivery ratio.

In the result area from the proposed methodology, a comparison is made with the previous study, and the techniques were explained using graphs. The table shows that the technique that is used here, Encrypted Access Mapping in a Distinctly routed Optimized Immune System, has a comparatively high packet delivery ratio (PDR) of 98%, an attack detection accuracy of 99%, an attack detection time of 0.1 ms, less routing overhead of 600 pkt and false classification ratio of 5%. The overall performance is above all existing methods.

5. Conclusions

The various types of DDoS attacks are carried out in vehicle ad hoc networks (VANET) thus it is essential to detect and prevent the attacks. To detect DDoS attacks, a novel attack detection framework is proposed in which Encrypted Access Hex-tuple Mapping Attack detection and Stable Automatic Optimized Cache Routing are used to provide immunity against DDoS attacks in the network. The Encrypted Access Hex-tuple Mapping Attack detection uses Triple random hyperbolic encryption to encode the traffic three times in a random manner and plot the values in co-efficient in hyperbolic encryption to determine the public key. The Hex-tuple Matched Mapping approach uses a Deep auto sparse impasse NN to map the IP addresses in hex tuple values and extract the features from the mapping report and classifies the twelve variants of DDoS attacks and arrest external hosts so as to prevent unauthorized access, interception, and interference with sensitive information and communication nodes. With this proposed attack detection approach, the detection time has been reduced and found to be 0.2 ms for 20 nodes when compared to other existing attack detection approaches. The accuracy of the proposed model is 96.2% for UDP flood detection, 97.2% for DNS flood detection, 96.4% for HTTP flood detection, 97.45% for NTP flood detection, 97.7% for Ping flood detection, 97.35% for SNMP flood detection, 96.4% for SYN flood detection, 98.4% for Smurf flood detection, 97.5% for LDAP flood detection, 97.5% for MSSQL flood detection. The recall of the proposed model identifies UDP Flood with 97.2% recall, DNS Flood with 97.45% recall, HTTP with 97.45% recall, NTP with 98.65% recall, Ping Flood with 97.53% recall, SNMP with 98.2% recall, SYN flood with 98.15% recall, Smurf with 97.67% recall, LDAP with 97.15% recall, MSSQL with 97.3% recall, NetBIOS with 98.45% recall, SSDP with 98.15% recall, WebDDoS with 98.15% recall and TFTP with 98.15% recall. The mean of recall and precision is computed using the F1-Score. The proposed model detects UDP Flood with 95.2% F1-Score, DNS Flood with 95.2% F1-Score, HTTP with 95.45% F1-Score, NTP with 96.5% F1-Score, Ping Flood with 96.4% F1-Score, SNMP with 97.2% F1-Score, SYN flood with 96.15% F1-Score, Smurf with 96.4% F1-Score, LDAP with 96.85% F1-Score, MSSQL with 97.1% F1-Score, NetBIOS with 97.1% F1-Score, SSDP with 97.4% F1-Score, WebDDoS with 97.6% F1-Score and TFTP with 98.15% F1-Score. Then the Stable automatic optimized cache routing is introduced in which Deep trust factorization NN adds trust value for each node and the moth flame optimization is used to form a balance between the cluster to produce the high packet deliver ratio of 98% thereby detecting the malicious nodes and ensuring the linkage of each node in the cluster. Cache parallelized circulation link routing is used to provide multiple parallelized paths to each node and time and frequency synchronization to packets thereby removing unwanted traffic from the network so the response time of each node is reduced to 0.1 ms. The proposed model detects the twelve variant DDoS attacks with an accuracy of 99% and less detection time of 0.1ms and thereby outperforming all other existing techniques. This framework creates a baseline of typical VANET operation and detects any substantial abnormalities, such as a rapid increase in traffic or unexpected communication patterns. This can prevent these anomalies and signal the presence of a DDoS assault by monitoring network flow and detecting rapid spikes in packet rates, strange packet sizes, or aberrant traffic patterns thereby prompting the implementation of suitable corrective measures. As a result, the proposed model achieves a comparatively high packet delivery ratio (PDR) of 98%, an attack detection accuracy of 99%, an attack detection time of 0.1 ms, less routing overhead of 600 pkt and false classification ratio of 5%. This approach can be used in the practical applications such as Road Transport Emergency Services that employ VANET communications by broadcasting the road safety warning and status information to cut down on delays and hasten emergency rescue operations in order to save the lives of individuals who have been injured.

References

[1] R. Shrestha, R. Bajracharya, A. P. Shrestha and S. Y. Nam, "A new type of blockchain for secure message exchange in VANET," *Digital communications and networks,* vol. 6, no. 2, pp. 177-186, 2020.

[2] A. K. Kazi, S. M. Khan and N. G. Haider, "Reliable group of vehicles (RGoV) in VANET," *IEEE Access,* vol. 9, pp. 111407-111416, 2021.

[3] A. Ilavendhan and K. Saruladha, "Comparative analysis of various approaches for DoS attack detection in VANETs," *In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) IEEE,* pp. 821-825, July 2020.

[4] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," *Cybersecurity,* vol. 4, no. 1, pp. 1-27, 2021.

[5] I. O. Olayode, L. K. Tartibu and M. O. Okwu, "Application of Fuzzy Mamdani Model for effective prediction of traffic flow of vehicles at signalized road intersections," *In 2021 IEEE 12th International Conference on Mechanical and Intelligent Manufacturing Technologies (ICMIMT) IEEE,* pp. 219-224, May 2021.

[6] M. A. Al-Absi, A. A. Al-Absi and H. J. Lee, "Comparison between DSRC and other Short Range Wireless Communication Technologies," *In 2020 22nd International Conference on Advanced Communication Technology (ICACT) IEEE,* pp. 1-5, February 2020.

[7] N. Ganeshkumar and S. Kumar, "Obu (on-board unit) wireless devices in vanet (s) for effective communication—A review," *Computational Methods and Data Engineering,* pp. 191-202, 2021.

[8] M. Poongodi, V. Vijayakumar, F. Al-Turjman, M. Hamdi and M. Ma, "Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information based metrics," *IEEE Access,* vol. 7, pp. 158481-158491, 2019.

[9] M. Poongodi, M. Hamdi, A. Sharma, M. Ma and P. K. Singh, "DDoS detection mechanism using trust-based evaluation system in VANET," *IEEE Access,* vol. 7, pp. 183532-183544, 2019.

[10] N. A. Alsulaim, R. A. Alolaqi and R. Y. Alhumaidan, "proposed solutions to detect and prevent DoS attacks on VANETs system," *In 2020 3rd international conference on computer applications & information security (ICCAIS) IEEE*, pp. 1-6, March 2020.
[11] R. Kolandaisamy, R. M. Noor, I. Kolandaisamy, I. Ahmedy, M. L. M. Kiah, M. E. M. Tamil and T. Nandy, "A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 6, pp. 6599-6612, 2021.
[12] S. Kumar and K. S. Mann, "Prevention of dos attacks by detection of multiple malicious nodes in VANETs," In 2019 International Conference on Automation, *Computational and Technology Management (ICACTM) IEEE*, pp. 89-94, April 2019.
[13] H. Bangui, M. Ge and B. Buhnova, "A hybrid machine learning model for intrusion detection in VANET," *Computing*, vol. 104, no. 3, pp. 503-531, 2022.
[14] K. Adhikary, S. Bhushan, S. Kumar and K. Dutta, "Hybrid algorithm to detect DDoS attacks in VANETs," *Wireless Personal Communications*, vol. 114, no. 4, pp. 3613-3634, 2020.
[15] S. Ercan, M. Ayaida and N. Messai, "Misbehavior detection for position falsification attacks in VANETs using machine learning," *IEEE Access*, vol. 10, pp. 1893-1904, 2021.
[16] S. Ahmed, M. U. Rehman, A. Ishtiaq, S. Khan and A. Ali, S. Begum, "VANSec: Attack-resistant VANET security algorithm in terms of trust computation error and normalized routing overhead," *Journal of Sensors*, 2018.
[17] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE transactions on intelligent transportation systems*, vol. 17, no. 4, pp. 960-969, 2015.
[18] W. Othman, M. Fuyou, K. Xue and A. Hawbani, "Physically secure lightweight and privacy-preserving message authentication protocol for VANET in smart city," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 12, pp. 12902-12917, 2021.
[19] B. A. Bensaber, C. G. P. Diaz and Y. Lahrouni, "Design and modeling an Adaptive Neuro-Fuzzy Inference System (ANFIS) for the prediction of a security index in VANET," *Journal of Computational Science*, vol. 47, pp. 101234, 2020.
[20] N. C. Velayudhan, A. Anitha and M. Madanan, "Sybil attack with RSU detection and location privacy in urban VANETs: An efficient EPORP technique," *Wireless Personal Communications*, vol. 122, no. 4, pp. 3573-3601, 2022.
[21] S. Aldhaheri, D. Alghazzawi, L. Cheng, B. Alzahrani and A. Al-Barakati, "Deepdca: novel network-based detection of iot attacks using artificial immune system," *Applied Sciences*, vol. 10, no. 6, pp. 1909, 2020.
[22] R. Kolandaisamy, R. M. Noor, M. R. Z'aba, I. Ahmedy and I. Kolandaisamy, "Adapted stream region for packet marking based on DDoS attack detection in vehicular ad hoc networks," *The Journal of Supercomputing*, vol. 76, no. 8, pp. 5948-5970, 2020)
[23] K. Adhikary, S. Bhushan, S. Kumar and K. Dutta, "Hybrid algorithm to detect DDoS attacks in VANETs," *Wireless Personal Communications*, vol. 114, no. 4, pp. 3613-3634, 2020.
[24] B. Sousa, N. Magaia, and S. Silva, "An Intelligent Intrusion Detection System for 5G-Enabled Internet of Vehicles," *Electronics*, vol. 12, no. 8, pp. 1757, 2023.
[25] A. Gaurav, B. B. Gupta, F. J. G. Peñalvo, N. Nedjah and K. Psannis, "Ddos attack detection in vehicular ad-hoc network (vanet) for 5g networks," *In Security and Privacy Preserving for IoT and 5G Networks Springer, Cham.*, pp. 263-278, 2022.

Authors' Profiles

S. Rama Mercy is a temporary teaching assistant in the Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore. She involved in teaching post graduates based on cyber security in the recent years. Having 15 years of teaching experience, her areas of interest rooted in data mining, network security, cyber security and artificial intelligence. She is pursuing Ph.D as part time in cyber security.

Dr. Padmavathi Ganapathi is the Dean-School of Physical Sciences and Computational Sciences and Professor in the Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women (Deemed to be University), Coimbatore. She has more than 34 years of teaching experience and 26 years of research experience. Her areas of interest include Cyber Security, Wireless Communication and Real Time Systems. She has executed funded projects worth 267.368 lakhs Sponsored by AICTE, UGC, DRDO and DST. Supervised 22 scholars at Ph.D level, she has more than 200 publications in Prestigious conferences and peer-reviewed journals. She is the life members of various professional bodies like CSI, ISTE, ISCA, WSEAS, AACE and AICW. Reviewer for many IEEE Conferences and Journals. She has visited many countries for technical deliberations. She is the Course Co-ordinator for SWAYAM-MOOC on Cyber Security. So far, more than 1,13, 000 learners have enrolled for various sessions and benefitted. She has authored 10 books in Cyber Security and Data Science Domain.

Vidwan Profile Page: https://vidwan.inflibnet.ac.in/profile/132327

How to cite this paper: Rama Mercy. S., G. Padmavathi, "Encrypted Access Mapping in a Distinctly Routed Optimized Immune System to Prevent DoS Attack Variants in VANET Architecture", International Journal of Computer Network and Information Security(IJCNIS), Vol.16, No.3, pp.99-114, 2024. DOI:10.5815/ijcnis.2024.03.08