Engineering and Technology Journal for Research and Innovation (ETJRI)
ISSN 2581-8678, Vol. VI, Issue II, Jul 2024

Identifying Anomalies in Vehicular Adhoc Networks

Thuvva Anjali[1], Rajeev Goyal[2], Balaji G.N[3]

[1],[2] Department of Computer Science and Engineering, Amity University Madhya Pradesh, Gwalior
[3]Department of Computer Science and Engineering, Vellore Institute of Technology, Vellore
[1] anjali.thuvva@gmail.com; [2] goyal.rajeev@gmail.com; [3] balaji.gnb@gmail.com

*Abstract—****The integration of Vehicular Ad Hoc Networks (VANETs) into intelligent transportation systems has become imperative in order to improve traffic efficiency and road safety. However, because VANETs are open and dynamic, they are vulnerable to a variety of security risks, such as anomalies that may interfere with regular network operations. This research focuses on a thorough analysis and assessment of several anomaly detection techniques in relation to VANETs. Vehicle-to-infrastructure systems and automobiles can communicate wirelessly thanks to vehicular ad hoc networks, or VANETs. Enhancing road safety, comfort, and convenience is the main objective of VANETs. VANETs are not like ad-hoc networks; they have special features. But since they lack centralized management and infrastructure, they are vulnerable to abuse, which poses a serious risk to a number of VANET features. This precious network needs strong security measures because of its significance in order to guarantee secure communication. Anomalies can take many different forms in VANETs, including hostile attacks, hiccups in communication, or unexpected car behavior. By choosing verifiers to identify malicious nodes, the suggested Detection of Anomalies algorithm in VANETs is effectively improved, leading to an improvement in network performance.***

Keywords— Vehicular Adhoc Network, Intelligent Transport System, Vehicle to Vehicle, Vehicle to Infrastructure, Anomaly Detection, Attacks.

I. INTRODUCTION

Vehicle Ad Hoc Networks (VANETs) are essential for facilitating vehicle-to-vehicle communication, which improves traffic flow and road safety. Nevertheless, VANETs are susceptible to a range of security risks due to their dynamic topology and open nature. An effective study aimed at mitigating attacks in the setting of vehicular ad hoc networks is presented in this paper. In order to guard against security risks, traditional wired networks come equipped with firewalls and other built-in protective systems.

However, wireless networks, like VANETs, are more vulnerable to attacks that can target the entire network from any direction. This is because VANETs operate ad hoc networks without centralized administration, making them susceptible to various misbehaviors like message tampering, eavesdropping, spamming, and masquerading. Ensuring the security of VANETs is a major challenge, especially considering that these networks support real-time communication and handle critical information. To effectively address this challenge, VANETs must adhere to security requirements such as integrity, confidentiality, privacy, non-repudiation, and authentication. These measures are crucial in protecting against attackers and malicious vehicular nodes. Many Researchers have proposed different schemes for detecting and identifying malicious nodes and abnormal activities in VANETs. Detecting these nodes and activities is essential for implementing precautionary measures. This paper introduces a node-centric detection scheme called DMN (Detection of Mischievous Nodes), which utilizes a monitoring approach to effectively identify malicious nodes that drop and duplicate packets in the network. Verifiers monitor the behavior of nodes and apply a selection threshold to determine their qualification.

The proposed analysis in the future integrates state-of-the-art security mechanisms tailored to VANETs, addressing both active and passive attacks. Active attacks involve malicious activities such as injecting false information, while passive attacks aim to eavesdrop on sensitive communication. Our approach combines cryptographic techniques, secure key management, and anomaly detection to fortify the VANET infrastructure. Key components of our analysis include a robust cryptographic framework to ensure secure communication between vehicles and infrastructure, dynamic key management protocols for timely key updates, and anomaly detection algorithms to identify and mitigate suspicious activities. The study evaluates the performance of the proposed analysis through extensive simulations and real-world experiments, demonstrating its effectiveness in preventing a wide range of attacks.

The primary objective is to analyze the effectiveness and performance of existing anomaly detection methods in identifying and mitigating abnormal behaviors in vehicular communication. The work encompasses a diverse range of anomaly detection techniques, including statistical approaches, machine learning-based methods, and hybrid models that combine multiple strategies. Each algorithm's strengths and limitations are systematically evaluated based on its ability to detect various types of anomalies, false-positive rates, computational efficiency, and scalability.

Figure 1 shows a nice illustration of a VANET. As more vehicles are equipped with wireless communication devices and computing technology, intervehicle communication is developing into available areas for study, standardization, and development. Numerous applications, such as collision stoppage, security, blind crossing, dynamic routing, real-time traffic situation monitoring, and others, are possible with VANETs. Connecting vehicle nodes to the Internet is a significant additional Application of VANETs.

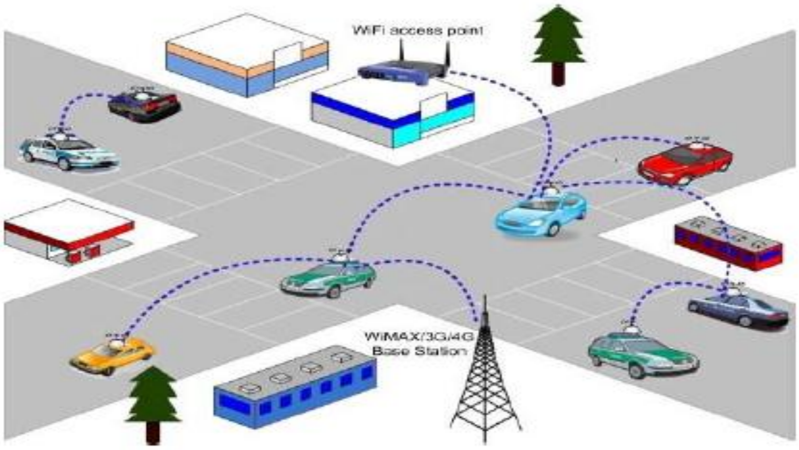

Figure 1. Communication in VANETS.

II. VEHICLE DEPLOYMENT

Several anomaly detection algorithms have been studied for enhancing security in Vehicular Ad Hoc Networks (VANETs). Detecting malicious nodes in Vehicular Ad Hoc Networks (VANETs) is crucial for ensuring the security and reliability of communication among vehicles. VANETs are susceptible to various security threats, including attacks on communication channels, misinformation dissemination, and denial of service attacks.

"Vehicle Deployment and Network Construction" typically refers to the strategic planning and implementation of vehicular networks, specifically in the context of Vehicular Ad Hoc Networks (VANETs) or Intelligent Transportation Systems (ITS). This process involves deploying vehicles equipped with communication devices and constructing the underlying network infrastructure to enable communication between vehicles and with infrastructure components. Here are key aspects associated with vehicle deployment and network construction. Vehicle Deployment: Equipping Vehicles: Vehicles are outfitted with communication devices, such as Dedicated Short-Range Communication (DSRC) units or cellular modems, enabling them to communicate with each other and with infrastructure components. Sensor Integration: Integration of sensors (e.g., GPS, accelerometers) to enhance data collection and improve situational awareness.

Vehicle-to-vehicle (V2V) communication has been proven to enhance road safety and transportation systems. Currently, there are two different approaches to enable transmission between moving vehicles. The first approach is the 3rd Generation Partnership Project (3GPP) cellular vehicle-to-everything (V2X) specifications. Another approach is based on the IEEE 802.11 family of standards, which is commonly referred to as dedicated short-range communications (DSRC). While the 3GPP V2X approach may offer higher throughput through the use of the millimeter-wave (mmWave) spectrum, its reliability relies on the availability of the necessary infrastructure. On the other hand, DSRC is more widely deployed, but it does have a significantly lower supported throughput compared to the new radio (NR)-based technology. However, this limitation can be overcome by leveraging the concept of DSRC.

III.NETWORK CONSTRUCTION

Communication Infrastructure: Establishment of the communication infrastructure necessary for vehicles to exchange information. This may involve roadside units (RSUs), base stations, and other network elements. Implementation of communication protocols suitable for VANETs, ensuring reliable and secure data exchange among vehicles and infrastructure. Utilization of wireless technologies (e.g., Wi-Fi, cellular) for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication.

Network Architecture: Designing the network architecture to support efficient and scalable communication, considering factors such as network topology and coverage areas.

Security Infrastructure: Implementation of security measures to protect communication channels from unauthorized access, data manipulation, and cyber threats.

Authentication and Encryption: Integration of authentication and encryption mechanisms to secure communication between vehicles and infrastructure components.

Traffic Signal Integration: Integration with traffic signals and control systems to optimize traffic flow and enhance safety.

Dynamic Routing: Implementation of dynamic routing algorithms to optimize vehicle routes based on real-time traffic conditions.

Simulation and Testing: Conducting simulations and tests to validate the effectiveness of the deployed network and the communication between vehicles and infrastructure.

Calculating the coverage area in Vehicular Ad Hoc Networks (VANETs) involves determining the geographical area over which communication can be established between vehicles or between a vehicle and an infrastructure node. The coverage area is influenced by factors such as communication range, transmission power, and the environment. Communication range represents the maximum distance over which a vehicle can communicate with another vehicle or an infrastructure node. It is a critical parameter for coverage area calculation. The communication range can be influenced by the transmission power of the communication devices on the vehicles and the signal propagation characteristics in the environment. Transmission power refers to the amount of power used by a vehicle's communication device to transmit signals. Higher transmission power generally leads to a longer communication range. The transmission power is often specified in decibels (dB) or watts (W).

Consider the path loss and signal attenuation over distance, which are affected by factors such as obstacles, terrain, and interference. Path loss models, such as the free-space path loss model or the log-distance path loss model, can be used to estimate signal attenuation. The effective coverage area (A) can be calculated using the formula:

$A=\pi(R*R)$ Where R is the communication range.

Vehicular Ad Hoc Network (VANET), attack construction refers to the process by which adversaries plan, design, and execute cyber-attacks to compromise the security and functionality of the vehicular network. VANETs are susceptible to various security threats, and attackers may employ specific strategies to exploit vulnerabilities within the network.

IV. RELATED WORK

In recent years, there has been a growing interest in the field of inter-vehicle communications research. This is due to the need for new algorithms and solutions that can accommodate the unique movement patterns of each vehicle.

Many techniques have been developed in recent years to detect irregularities in conventional VANET networks. This report presents a survey of VANET anomaly detection and mitigation techniques. Numerous VANET research initiatives, attack types, anomaly detection techniques, and mitigation mechanisms are examined in this review. Wireless communication between automobiles and infrastructure is made possible via VANETs. Enhancing comfort, convenience, and road safety is its main goal. Because of its unique characteristics, VANET differs from ad hoc networks. Over time, several techniques for spotting irregularities in traditional VANET networks have been developed. [1]

Our daily commutes and travel patterns are significantly impacted by autonomous transportation systems. These systems are inherently linked, and applications for intelligent transportation systems make this possible. The Vehicular Ad hoc Network (VANET) is a network system utilized by these applications. However, malevolent users can quickly compromise the security that VANETs provide. Thus, an intrusion detection system (IDS) is required. We created an IDS model that is capable of cooperatively gathering network data from cars and Roadside Units (RSUs). We created synthetic network data with the aid of the popular simulation tools Simulation of Urban Mobility (SUMO) and Network Simulator 3 (ns-3) to train the core of our proposed IDS. [2]

Intelligent transportation solutions that greatly improve road safety and management are now possible thanks to vehicle ad hoc networks. With this new technology, vehicles can now exchange information about the route and speak with one another. On the other hand, fraudulent users may introduce fictitious emergency warnings into vehicle ad hoc networks (VANETs), preventing nodes from accessing reliable road data. In automobile ad hoc networks, determining a node's reputation has become essential to guaranteeing data reliability and trustworthiness. This paper suggests a novel security method that enhances communication and intrusion detection in VANET for smart transportation by using machine learning techniques. Here the security of the VANET is enhanced through the application of ciphertext game theory encryption analysis for smart transportation. [3]

One approach to enhance the resilience and scalability of networks is by clustering nodes that are in close physical proximity to each other. It is worth mentioning that there are several techniques available, with most of them focusing on specific performance metrics. Furthermore, the algorithms used and the raw data they depend on exhibit a wide range of complexities. [4]

Vehicles can communicate with each other using a type of network called vehicular ad hoc networks, or VANETs, to share information about traffic conditions and any incidents happening on the road. However, VANETs are vulnerable to various attacks due to their lack of infrastructure. One such attack is the Sybil attack, which poses a significant threat to the security of data distribution in VANETs. Without proper security measures, accidents can occur while driving. The challenge of defending against and detecting Sybil attacks, especially when they are carried out by coordinated attackers using false identities, has sparked a growing interest in VANET research in recent years. [5]

Vehicular Ad Hoc Networks (VANETs) are a new class of efficient information dissemination technology that has gained popularity among user communities in the past few years. This is primarily due to their extensive range of applications in various domains, including Intelligent Transport Systems (ITS), safety applications, online entertainment while driving, and more. [6] Within VANETs, vehicles function as intelligent machines that offer end users a variety of resources, either with or without the assistance of the current infrastructure. However, routing the messages to their destination is a difficult issue because of the high mobility and sparse dispersion of vehicles on the road. Clustering has been widely employed in numerous existing approaches in the literature to overcome this problem. One mechanism is clustering. [7]

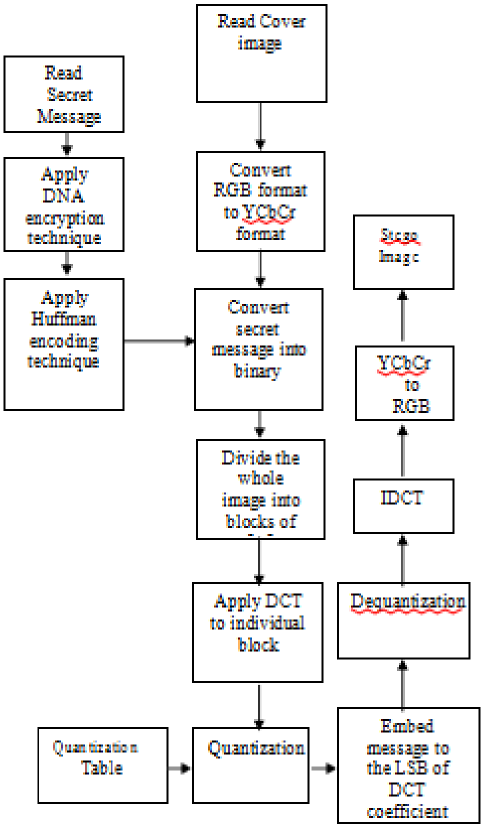
Read Cover image
Read Secret Message
Apply DNA encryption technique
Convert RGB format to YCbCr format
Stego Image
Apply Huffman encoding technique
Convert secret message into binary
YCbCr to RGB
Divide the whole image into blocks of
IDCT
Apply DCT to individual block
Dequantization
Quantization Table
Quantization
Embed message to the LSB of DCT coefficient

Figure 2 Data Embedding Process

Table 1. Attacks in VANETs.

Attack Type	**Description**
Gray Hole Attacks	It selectively drops or alters a portion of the messages, introducing subtle disruptions in communication to avoid detection.
Sybil Attacks	It creates multiple fake identities to increase their influence within the network.
Denial of Service (DoS)	It generates a large volume of malicious traffic to overwhelm network resources, leading to service unavailability.
Replay Attacks	It captures and later replays legitimate messages to deceive network participants, disrupting normal network operations.
Black Hole Attacks	It attracts and absorbs messages without forwarding them, selectively dropping messages and disrupting communication.
Gray Hole Attacks	It selectively drops or alters a portion of the messages, introducing subtle disruptions in communication to avoid detection.
Routing Attacks	It manipulates routing protocols to misdirect traffic, potentially causing congestion, delays, or isolating vehicles from the network.
Node Misbehavior	It intentionally deviates from cooperative behavior, violating

	communication protocols and undermining trust within the network.
Jamming Attacks	It transmits interference signals to disrupt wireless communication, blocking or degrading the quality of communication channels.

V. DRIVING ARCHITECTURES WITH AUTOMATION

Autonomous driving architectures refer to the systems and components that enable vehicles to operate without human intervention. Several key architectures exist, each with its approach to integrating sensors, processing units, decision-making algorithms, and actuators necessary for autonomous driving.

In recent decades, there has been a significant increase in research on fully autonomous driving systems, leading to major disruptions in the automobile industry. According to statistical analysis, over 94% of all traffic accidents are attributed to driver error, such as offensive maneuvers and distraction [8]. By automating cars, the occurrence of human error can be reduced as it eliminates the risks associated with inebriated behavior and distraction. The presence of autonomous vehicles on the road decreases the likelihood of accidents caused by human error and distraction. These vehicles can be programmed to take corrective actions and avoid collisions. With the elimination of human error in autonomous driving, there is great potential to save numerous lives. Moreover, specific demographics, including the young, elderly, disabled, and those unable to drive, will benefit from autonomous cars. Additionally, autonomous driving has the potential to enhance driving efficiency, which is advantageous for both the bottom line and the environment.

Legitimate data is typically derived from a specific distribution that is dependent on the application. When the data generation process deviates from the norm, it can result in abnormal data points known as outliers. These outliers can serve as valuable indicators of unexpected behavior within a system [9]. Our approach focuses on the identification and analysis of outliers for anomaly detection and classification.

Anomaly detection algorithms can be categorized into two main types: statistics-based and machine learning-based [10]. Statistics-based methods involve calculating statistical properties within a dataset and establishing rejection criteria based on assumptions about the data distribution to identify anomalous samples. On the other hand, machine learning-based methods utilize supervised or unsupervised learning techniques to train a model using a set of training samples, enabling it to effectively address anomalies.

In this decade, numerous self-driving applications have emerged as a result of the significant advancement in the launch of highly anticipated self-driving cars. These applications utilize innovative technologies, as depicted in the Figure below, to ensure that drivers are no longer necessary for the complete automation of a car. Instead, the driver becomes a passenger, just like any other individual in the vehicle. These self-driving cars rely on various tools, including Lidar and radar, to prevent accidents by providing a comprehensive 360-degree field of view. Ultrasonic sensors are also employed to detect obstacles such as pedestrians and animals. Additionally, these cars heavily rely on the Global Navigation Satellite System (GNSS) to communicate with nearby vehicles, remote service providers, highway infrastructure, and important events through a communication system known as V2X. [11]

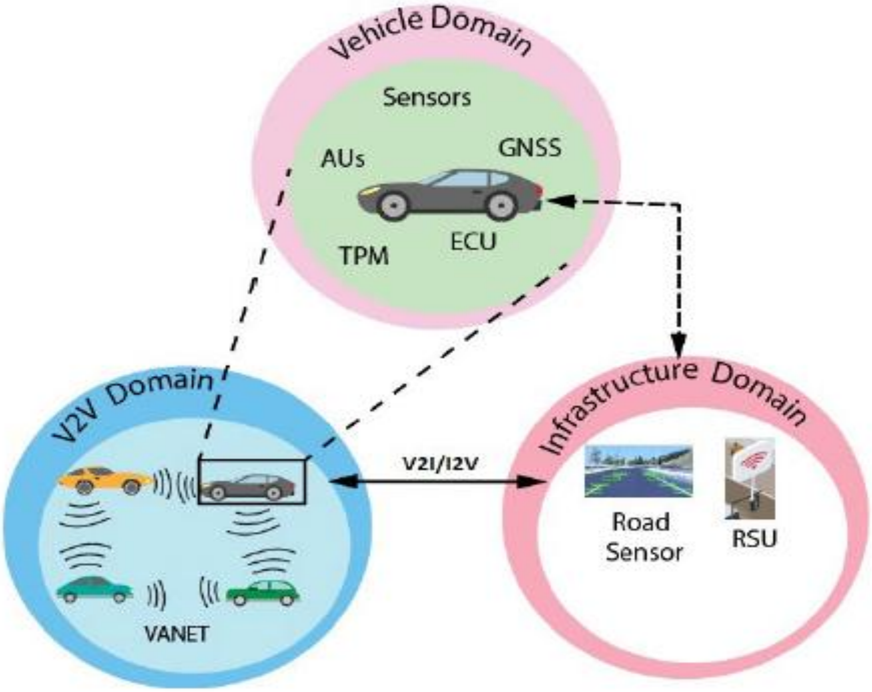

Figure 3. ITS Architecture in VANETS.

The clustering methods need to be adjusted to account for the particular mobility and channel conditions that are specific to VANETs. Many techniques are employed to create, locate, and link pre-existing VANET clusters and maintain them, including machine learning, agility prediction, channel monitoring, and security assessment. The most current attempts are the result of newly developed methods for categorizing dimensions, and form profiles of vehicles. Research has been done on how to monitor changes in the topology of the vehicles inside a cluster to sustain it over time. [12]

VI. CONCLUSION

In conclusion, our efficient analysis provides a comprehensive strategy for countering attacks in Vehicular Ad Hoc Networks, contributing to the overall reliability and security of vehicular communication systems. The findings of this research can inform the development of robust security frameworks for future smart transportation systems, fostering trust and resilience in the connected vehicular environment. By fostering a deeper understanding of the strengths and limitations of various algorithms, this research contributes to the development of robust and adaptive security solutions, ensuring the integrity and reliability of communication in Vehicular Ad Hoc Networks.

REFERENCES

[1] Anjali, T., Goyal, R., & G.N, B. (2024). Prevention of Attacks in Vehicular Adhoc Networks. 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), 1-8.

[2] E. A. Shams, A. Rizaner, and A. H. Ulusoy, ‘‘Flow-based intrusion detection system in vehicular ad hoc network using context-aware feature extraction,” Veh. Commun., vol. 41, Jun. 2023, Art. no. 100585.

[3] R. Chakraborty, S. Kumar, A. Awasthi, K. Suneetha, A. Rastogi, and G. Jethava, ‘‘Machine learning based novel frameworks developments and architectures for secured communication in VANETs for smart transportation,’’ Soft Comput., vol. 27, pp. 1–11, May 2023.

[4] Y. Sadovaya and S. V. Zavjalov, "Dedicated Short-Range Communications: Performance Evaluation Over mmWave and Potential Adjustments," in IEEE Communications Letters, vol. 24, no. 12, pp. 2733-2736, Dec.2020, doi:10.1109/LCOMM.2020.3016634.

[5] Vehicular Communications. 1. 10.1016/j.vehcom.2014.05.004.

[6] Chaubey, N., & Yadav, D. (2020). A Taxonomy of Sybil Attacks in Vehicular Ad-Hoc Network (VANET).

[7] H. Ye, L. Liang, G. Y. Li, J. Kim, L. Lu, and M. Wu, "Machine Learning for Vehicular Networks: Recent Advances and Application Examples," IEEE Vehicular Technology Magazine, vol. 13, no. 2, pp. 94-101, 2019.

[8] C. Dutta and N. Singhal, "A Cross Validated Clustering Technique to Prevent Road Accidents in VANET," 2018 International Conference on System Modelling & Advancement in Research Trends (SMART), Moradabad, India,2018, pp.183-187, doi: 10.1109/SYSMART.2018.8746930.

[9] Yurtsever, E., Lambert, J., Carballo, A., & Takeda, K. (2020). A survey of autonomous driving: Common practices and emerging technologies. IEEEAccess,8,58443–58469. http://dx.doi.org/10.1109/ACCESS.2020.2983149.

[10] C. C. Aggarwal, Outlier Analysis, 2nd ed. Cham, Switzerland: Springer, 2016.

[11] Chowdhury, Abdullahi & Karmakar, Gour & Kamruzzaman, Joarder & Jolfaei, Alireza & Das, Rajkumar. (2020). Attacks on Self-Driving Cars and Their Countermeasures: A Survey. IEEE Access. 8. 207308-207342. 10.1109/ACCESS.2020.3037705.

[12] M. Ahmed, A. N. Mahmood, and J. Hu, ‘‘A survey of network anomaly detection techniques,’’ J. Netw. Comput. Appl., vol. 60, pp. 19–31, Jan. 2016.

[13] Krishnakumar, KG & Fredrik, ET 2017, ‘QOS enabled data dissemination in hierarchical VANET using machine learning approach’, International Journal of Signal and Imaging Systems Engineering, vol. 10, no. 5, pp. 231-236.

[14] Tang, Y, Cheng, N, Wu, W, Wang, M, Dai, Y & Shen, X 2019, ‘Delay-minimization routing for heterogeneous VANETs with machine learning based mobility prediction’, IEEE Transactions on Vehicular Technology, vol. 68, no. 4, pp. 3967-3979.

[15] Mohammad Mukhtaruzzaman, Mohammed Atiquzzaman, Clustering in vehicular ad hoc network: Algorithms and challenges, Computers & Electrical Engineering, Volume 88, 2020, 106851, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2020.106851.

[16] (https://www.sciencedirect.com/science/article/pii/S0045790620307047)

[17] Maglaras, Leandros & Basaras, Pavlos & Katsaros, Dimitrios. (2013). Exploiting Vehicular Communications for Reducing CO2 Emissions in Urban Environments. 2013 International Conference on Connected Vehicles and Expo, ICCVE 2013 - Proceedings. 10.1109/ICCVE.2013.6799765.

[18] Jabar Mahmood, Zongtao Duan, Yun Yang, Qinglong Wang, Jamel Nebhen, Muhammad Nasir Mumtaz Bhutta, "Security in Vehicular Ad Hoc Networks: Challenges and Countermeasures", Security and Communication Networks, vol. 2021, Article ID 9997771, 20 pages, 2021. https://doi.org/10.1155/2021/9997771

[19] Asad Iqbal, Insaf Ullah, Abeer Abdulaziz AlSanad, Muhammad Inam Ul Haq, Muhammad Asghar Khan, Wali Ullah Khan, Khaled Rabie, "A Cost-Effective Identity-Based Signature Scheme for Vehicular Ad Hoc Network Using Hyperelliptic Curve Cryptography", Wireless Communications and Mobile Computing, vol. 2022, Article ID

5012770, 8 pages, 2022. https://doi.org/10.1155/2022/5012770

[20] Zhang, L, Men, X, Choo, KKR, Zhang, Y & Dai, F 2018, ‘Privacy-preserving cloud establishment and data dissemination scheme for vehicular cloud’, IEEE Transactions on Dependable and Secure Computing, p. 1.

[21] Lim, B.S.; Keoh, S.L.; Thing, V.L. Autonomous vehicle ultrasonic sensor vulnerability and impact assessment. In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018; pp. 231–236.

[22] Appathurai, A.; Manogaran, G.; Chilamkurti, N. Trusted FPGA-based transport traffic inject, impersonate (I2) attacks beaconing in the Internet of Vehicles. IET Netw. 2019, 8, 169–178. [CrossRef]