WJCMS

Wasit Journal of Computer and Mathematics Science

Journal Homepage: https://wjcm.uowasit.edu.iq/index.php/WJCM

e-ISSN: 2788-5879 p-ISSN: 2788-5879

Review Vehicular Ad hoc Networks Security Challenges and Future Technology

Sahar Wahab khadim[1,*] and Haifa Ahmed Hassan[2]

[1]Ministry of Education, Karkh Second Directorate of Education, Iraq
[2]University of Mosul, College of Engineering, Iraq

*Corresponding Author: Sahar Wahab khadim

DOI: https://doi.org/10.31185/wjcm.50
Received: June 2022; Accepted: August 2022; Available online: September 2022

ABSTRACT: Vehicular Ad hok Networks (VANET) is an emerging technology with both a bright future and significant concerns, particularly in terms of security. This study focuses on three-part VANET security frameworks. The first gives a thorough review of the needs, difficulties, and characteristics of VANET security. In order to create a secure VANET architecture with effective party communication, certain needs should be taken into account. We provide information on current security designs as well as widely used security standard protocols. The second concentrates on a brand-new categorization of the various assaults described in the VANET literature and the remedies that go with them. The third compares a few of these options using established security standards for VANET. Then, in order to assist researchers for future usage, we call attention to many outstanding topics and technological obstacles linked to VANET security.

Keywords: VANET, V2V, V2I, OBU, RSU

1. INTRODUCTION

By enhancing traffic flow, VANET intends to ensure safe driving and hence considerably lower the number of auto accidents. By giving the driver or the vehicle the necessary information, the latter problem is resolved. However, any modification to this real-time data might result in a system failure that compromises traveller safety. Securing this information becomes essential to ensuring its proper operation, making it a major priority for security experts.

A particular kind of mobile ad hoc network called VANET has predetermined paths (roads). For registration and administration, it depends on certain agencies, roadside units (RSUs), and on-board units (OBUs). To provide specialized services, RSUs are widely dispersed around the boundaries of the roads, and OBUs are placed in the cars via VANET. Every vehicle is able to move freely on the road network and communicate with other vehicles, RSUs, and certain authorities. The communication mechanism is either V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure), or hybrid using DSRC (Dedicated Short Range Communication) in a single or multi-hop. As illustrated in Figure, the majority of vehicles participating in VANET in the future will be outfitted with on-board wireless devices (OBU), GPS (Global Positioning System), EDR (Event Data Recorder), and sensors (radar and ladder) (1). This apparatus is used to monitor traffic conditions. Then, the vehicle will automatically perform the necessary measures and transmit this information over V2V or V2I inside the vehicular network. Users of VANET benefit from a variety of applications that fall under the categories of active road safety, entertainment, traffic efficiency, and management [1]; the latter includes cooperative navigation and speed management.

Being safe from harm or danger is the condition of being in security. Security refers to both safety and the steps taken to protect or keep oneself safe. For instance, local authorities often employ more guards in order to ensure proper security for

*Corresponding author: Saharwahab2001@gmail.com

the procession. Because VANET utilizes wireless connection, which is more difficult to protect, it is essential to prevent abuse activities and to clearly describe the security architecture. People's safety is impacted by security and its promised degree of implementation. Many experts studied security breaches a few years ago and looked for remedies that could have anything to do with them. Others attempted to standardize standards and protocols or create security infrastructures. Even still, there is much to learn about the relationship between a node's reliability and the detection of misbehavior [2].

The majority of the VANET security difficulties, as well as the available solutions, are thoroughly investigated in this study, which also outlines the features of VANET security. We first describe the most current security designs and the widely used security standards protocols before presenting and discussing the most recent frameworks that deal with the relevant problems. We emphasize an unique taxonomy of the many attacks described in the literature on VANET security, as well as those attacks' countermeasures.

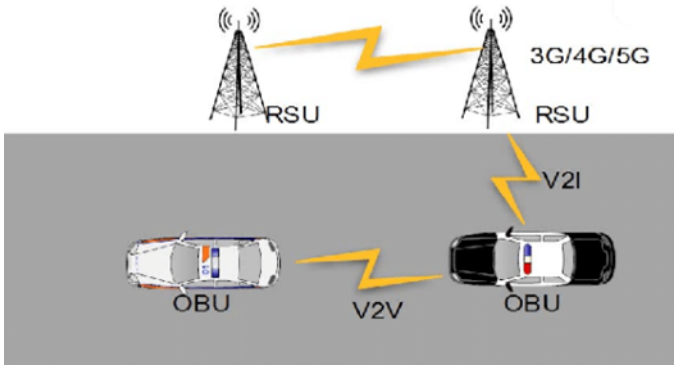


FIGURE 1. Future vehicle design in VANET.

2. LITERATURE REVIEW

In this paragraph, the range of research that has been used vanet security below:

A review of the routing issues and characteristics in VANETs was published by Sharef et al. in 2014 [3], and may be considered while developing the routing scheme for VANETs. Engoulou et al. [4] conducted a research on the security challenges and risks associated with VANETs in 2014. They also discussed the security needs as well as applications of VANETs, although not all security-related subjects. Qu et al. [5] released a thorough article in 2015 that included numerous models and experimental techniques. Azees et al. [6] raised the security and privacy risks of VANETs in 2016. Hasrouny et al. [7] provide the most modern security architecture utilizing VANET routing protocols. Reviewed VANET security, issues, causes, and solutions; this comprehensive examination is limited to 2017. Lu et al. [8] comprehensively explored the architecture, security, privacy, as well as trust management mechanisms in VANETs in a 2018 paper. They addressed network simulators as well as integrated simulators, with less emphasis on security and confidentiality in VANETs. To address security concerns, vehicle networks like as VANETs and VANET clouds incorporate systems for intrusion detection (IDS) as well as security procedures. Sharma and Kaul [9] conducted research on these systems. This survey looked into the challenging issues associated with using IDS in VANETs. Boualouache et al. [10] investigated pseudonym-changing techniques in VANETs. This survey assessed and contrasted several techniques based on relevant criteria and identified any differences.

3. VANET ARCHITECTURE

Typically, wireless technology known as wireless access in vehicular environment is used for communication between cars and RSUs (WAVE). By updating data on vehicles and traffic flow, WAVE communication ensures passenger safety, and the WAVE architectural outlines how security signals are exchanged [12]. This application improves traffic flow and the efficacy of a traffic management system all while assuring motorist and pedestrian safety. OBUs, RSUs, and TA are a few of the units that make up the VANETs. Specifically, each car has an OBU installed on it that gathers relevant information about the vehicle, such as speed, acceleration, and fuel. The RSU frequently includes an application for interacting with the other network devices. Then comes that, this data are sent through wireless network to the neighbouring automobiles. All RSUs that are linked to one another via wired networks are likewise linked to TA. In addition, TA is the head of all the parts and is in charge of managing the VANETs [13].

3.1 ROADSIDE UNIT (RSU)

A roadside unit is indeed a computer equipment located alongside a road or at a designated location, such as a parking lot or even a crossroads [14]. Its goal is to create a local link for passing autos. The RSU is made up of IEEE 802.11p radio-based network devices for specialized short-range communication (DSRC). RSUs can be used to connect to specific network devices that are part of other network infrastructure [14].

3.2 ONBOARD UNIT (OBU)

Every vehicle typically has an OBU, a GPS-based vehicle tracking device that sends data to RSUs and some other OBUs the OBU's electrical components include the resource control processors (RCP), sensing devices, user interface, plus read/write storage and storing information. The primary purpose of an OBU is to establish a wireless connection with an RSU or other OBU using IEEE 802.11p [15] and to communicate with those entities through messages. Additionally, OBU draws power from the vehicle's battery for input, Furthermore, every car contains sensors such as the global position system (GPS), and data recorder (EDR), forward and backward sensors which send data into the OBU [13].

3.3 TRUSTED AUTHORITY (TA)

The trusted authority manages the entire VANET network, such as the registration of RSUs, OBUs, as well as vehicle users. It is also responsible for assuring the security management of VANETs by validating vehicle identification, user ID, plus OBU ID and avoid vehicle damage. The TA consumes a large amount of power and memory, and it could offer OBU ID as well as information with in event of malicious messages or suspicious activity [16]. In addition to this, TA contains a mechanism for identifying the attackers.

4. VANET SECURITY CHALLENGES

Security in VANET must ensure that added or modified messages are not sent. Additionally, it is crucial for drivers to be accountable for accurately and quickly informing themselves on the traffic situation. Due to VANET's unique properties, new security concerns have arisen. Mishandling these security issues will result in several restrictions. Some of these security issues are listed below:

The network's size, the geographic importance, the high mobility, this same dynamic topology, the short connection times, and also the frequent disconnections: A network's size can be geographically unbounded. Very scalable, and rapidly expand without any worldwide authority to set its rules.

• **Network management:** Because of high mobility, the channel state and network architecture are constantly changing. Due to the fact that structures like trees cannot be built up and maintained as quickly as the topology changes, as shown in Figure 2, we are unable to employ them.

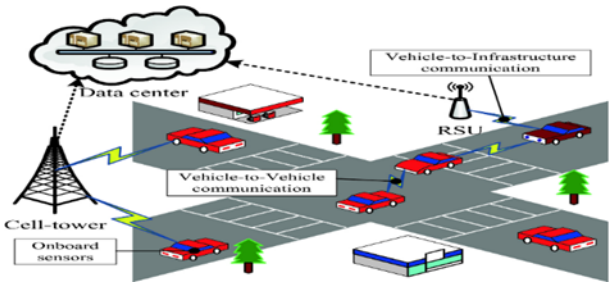


FIGURE 2. **Network Management.**

• **Congestion and collision Control**: Unbounded network size is another problem. Even at night, traffic is light in urban and rural locations alike. Due to this, the network regularly divides during rush hours when the traffic load is extremely high, causing the network to get clogged and a collision to occur, as seen in Figure (3).

• **Environmental Impact**: Electromagnetic waves are used in VANETs for communication. The environment has an impact on these waves. Consequently, the environmental effect of deploying the VANET must be taken into account as indicated in Figure (4).

• **MAC Design:** Because VANET typically uses a shared media for communication, the MAC design is the main problem. Many strategies, including TDMA, SDMA, and CSMA, have been offered. The CSMA-based Mac was accepted by IEEE 802.11 for VANET.

FIGURE 3. **3.Congestion and collision Control.**

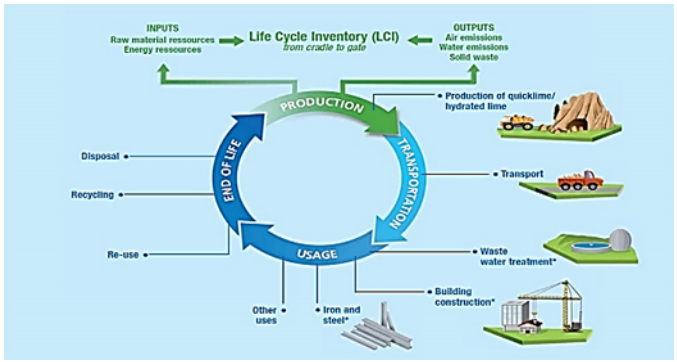


FIGURE 4. **4.Environmental Impact.**

• **Anonymity, privacy, and liability:** Nodes receiving data must have confidence in the sender. Anonymous vehicle identities protect privacy. Even authorized nodes sometimes engage in harmful behavior. Therefore, a compromise between anonymity, privacy, and liability is required.

The Trust and information verification: As a result of the nodes' motivation to obtain data from other cars and RSUs due to the ad hoc nature of the VANET, trust is necessary. Since this information is shared often, its reliability must be established the dependability of the information is more significant than the dependability of the nodes that deliver it.

Key Distribution: Keys are required for all security measures deployed in VANET. Each **message** is encrypted, as well as the recipient must decode it using either the same key or even a new key. Furthermore, various companies may install keys for different ways, as well as the public-key infrastructure, trust in the CA has evolved into a big issue. As a result, implementing security measures is difficult due to the dispersion of keys across cars, as illustrated in Figure (5).

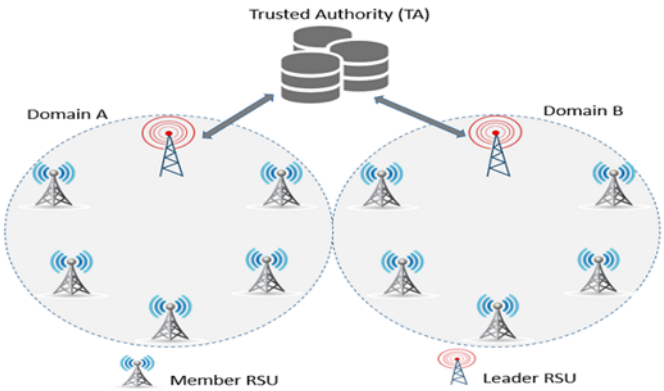


FIGURE 5. **Key Distribution.**

• **The Forwarding algorithms:** Which is more difficult, unicast, broadcast, V2V, V2I, or hybrid communication, after

determining the optimum route, in terms of the quantity of packets transferred? (6).

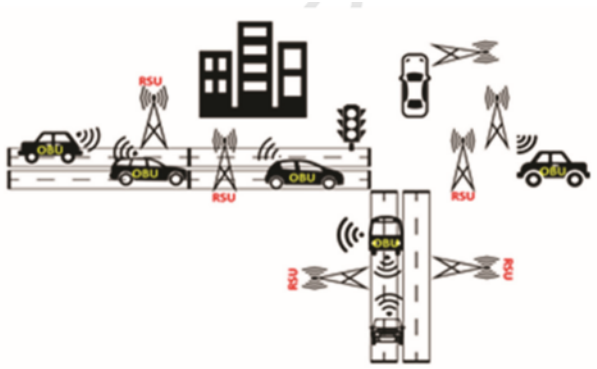


FIGURE 6. **The Forwarding algorithms.**

• **Real time Constraint:** Due to the urgency of the VANET, safety-related messages must be sent with a 100ms delay. Therefore to meet the real time constraint, a rapid cryptographic approach should be used. Timely completion of message and entity authentication is required.

• **Data Consistency Liability :** Even authenticated nodes in VANET are capable of engaging in malicious actions that may result in mishaps or upset the network. Therefore, a system should be created to prevent this contradiction. This kind of discrepancy may be avoided by correlating the data that was received from various nodes on a certain piece of information.

• **Low tolerance for error:** Some protocols are created using probabilistic principles. When performing an activity in a hurry, VANET employs life-critical information. In a probabilistic algorithm, even a minor inaccuracy might be harmful [17].

• **Incentives:** Manufacturers are keen to develop the apps which consumers want. Few consumers will support a vehicle that automatically alerts them to any violations of traffic regulations. As a result of the requirement for incentives from car manufacturers, customers, and the government, integrating security in VANET will be tough.

• **High Mobility:** A VANET node has the same computational energy and power supply as a wired network node; but, because to their great mobility, VANET nodes should execute security measures faster quickly to obtain the same efficiency as wired networks. As a result, strategies for accelerating execution must be employed in the design for security protocols. Two ways can be utilized to meet this criterion.

• **Low complexity security algorithms:** Most modern security protocols, including SSL/TLS, DTLS, and WTLS, rely on public key cryptography based on the RSA algorithm. The NP-Hard integer factorization on big prime numbers is used by the RSA algorithm. Decryption of the message using the RSA technique thus becomes highly difficult and time-consuming. Therefore, it is necessary to build alternative cryptographic methods like lattice-based and elliptic curve cryptosystems. AES may be used to encrypt large amounts of data.

• **Transport protocol choice:** Since DTLS uses a connectionless transport layer, it should be chosen over TLS when it comes to IP transaction security. Avoid IPsec because it involves too many messages to set up and protects IP traffic. However, as illustrated in Figure, IPsec and TLS may be employed when moving vehicles are not present (7).

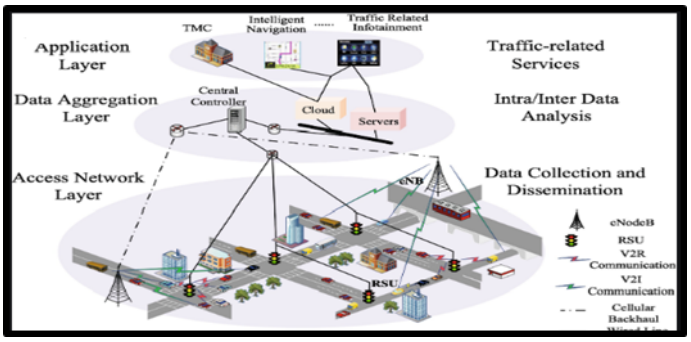


FIGURE 7. **Transport protocol choice.**

5. METHODOLOGY

We suggest for the widespread use of ML in all facets of VANET security. A computer-based approach called machine learning (ML) finds unprogrammed latent insights in a data collection. Work performance enhances the educational process. A common machine learning model comprises three stages:

1. The training step involves preprocessing raw data to extract characteristics. An ML model is built using features to find trends and types of data.

2. Test phase, when an ML model evaluates a fresh batch of data and ranks them according to their learnings from the training phase.

3. The prediction step, sometimes referred to as the assessment stage, is when the effectiveness of the ML model is assessed using quality indicators (such as accuracy, false positives, false negatives, etc.).

The training phase modifies its data and/or features to improve outcomes as proficiency declines. Figure displays a typical machine learning model (8).

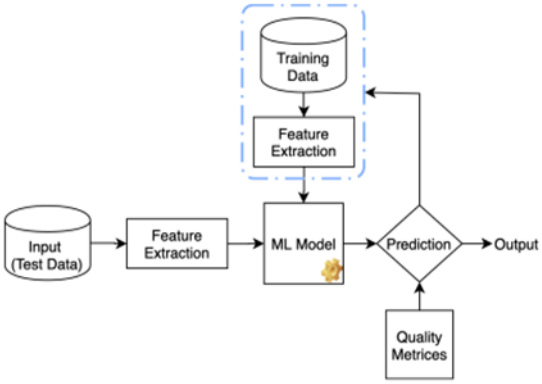


FIGURE 8. proposal of VANET.

The ML techniques are further classified into three key categories: supervised, unsupervised, reinforcement, and hybrid learning. As demonstrated in Figure, these classes have evolved into a variety of learning types, including DL, TL, as well as FL (9). These types coexist alongside the three major classes and have drawn a lot of attention thanks to their aptitude for a variety of jobs. The popular machine learning (ML) techniques for vehicle network security are described here.

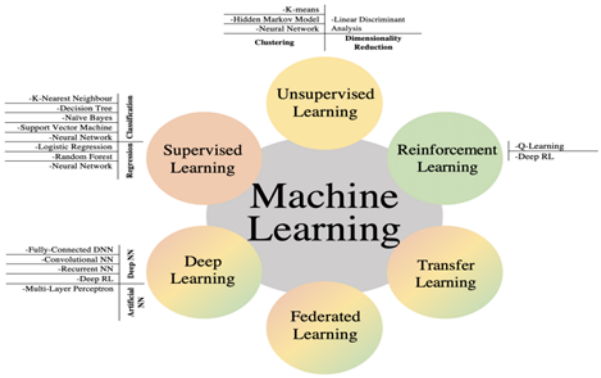


FIGURE 9. ML approaches in the context of VENET.

5.1 SUPERVISED LEARNING

In supervised learning, every item with in training dataset includes an input value as well as the label which goes with it. By understanding the link between both the input sample and also the label of a training set, the supervised algorithm uses this relationship for map new occurrences of the testing data. Although supervised learning may be used to

secure vehicular networks in a variety of fields, our study focuses on one application. The two subcategories of supervised learning are classification and regression. The categorization model produces discrete or categorical dataSome of the categorization models that are frequently used for security in vehicle networks include K-Nearest Neighbor (KNN), Decision Tree Naive Bayes, Support Vector Machine (SVM), as well as Neural Network (NN). A continuous value is the regression model's output. The most common regression models for safeguarding vehicular networks are logistic regression, random forests, as well as NN. The application of supervised learning within vehicular networks is suitable to a wide range of tasks, include driver identification, misbehaviour classification, attack detection, and trust computation.

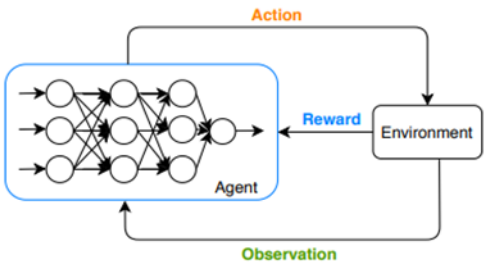
5.2 UNSUPERVISED LEARNING

Unsupervised learning, as contrast to supervised learning, solely uses input values from the training dataset. In unsupervised learning, the dataset's pre-assigned labels are not used. Finding hidden patterns in data from unlabeled data is the goal of unsupervised learning. As a consequence, data structures with comparable characteristics are grouped together. Unsupervised algorithms handle data more quickly and effectively.

Applications for clustering and dimensionality reduction are categorized under unsupervised techniques. During clustering, the input samples were grouped together based on multiple similarity criteria, including such relative or total similarity. For grouping, cluster centroids are picked at random, and similarity features for all values were computed from the centre. The centroid selection is iterated until the best match is found. The most often utilized clustering approaches for security in automotive networks are K-means clustering, Hidden Markov Models (HMM), as well as NN. During dimensionality reduction, the data is projected from the higher dimension to a smaller one without surrendering any critical information. The learning process can suffer as a result of the shorter optimization timeframes and lower complexity of dimensionality reduction algorithms. When it comes to dimensionality reduction methods, the usage of Linear Discriminant Analysis (LDA) is taken into account in the literature.

5.3 REINFORCEMENT LEARNING

In contrast to both supervised and unsupervised learning, RL incorporates a variety of learning methodologies. The figure represents the conceptual basis behind RL (9). The objective is to find a strategy that allows an agent can behave optimally inside the given environment. A trial-and-error approach is used by an agent to interact with its environment in an effort to maximize positive rewards. The agent creates data to learn depending on the rewards gained. A Markov decision process governs the environment, and observation and the choice of actions determine the reward and state transition probability [18]. Finding acts that maximize potential benefits is RL's policy. Q-learning is one of the most well-liked and often used RL techniques. To maximize the cumulative rewards, Q-learning constrains itself using the Bellman equation. By using a policy for the choice of activities, it seeks to maximize the projected total reward. To record a mix of actions and anticipated rewards, Q-learning creates a lookup table in real life. When a continuous series of operations are utilized for the data, this sometimes becomes inefficient and necessitates more memory. The DRL network, which combines DL and RL to handle bigger datasets, is suggested as a remedy. For the purpose of enhancing security in vehicle networks, RL, DRL, and its variations are commonly used.



5.4 DEEP LEARNING

Although DL is a subset of ML, it operates differently from the conventional ML techniques. Instead of requiring feature engineering as in conventional ML, it does not. In DL, an algorithm that self-optimizes picks up on the data pattern on its own. DL identifies patterns that are too challenging for conventional ML to learn. [19] The DL approach may be used directly to do classification, regression, as well as decision-making on raw data in its natural shape (without pre-processing). DL functions in a supervised, partly supervised, unsupervised, or reinforcement learning way and is ideally suited for non-linear data patterns. Recently, DL use in transportation networks has become more prevalent. To address

various security issues in vehicle networks, many deep architectural versions have been proposed in the literature. The simplest and most often used form of an artificial neural network (ANN), a multilayer perceptron (MLP) is developed from one of the early neural network architectures. A feedforward-ANN is another term for an MLP. The multiple levels that comprise an MLP are the input layer, the middle hidden and computation levels, [20], and the output layer. Both supervised and unsupervised learning processes may be used to simulate MLP. Due to its completely linked architecture, MLP has an issue with poor convergence efficiency and high operating complexity. Regardless of these flaws, ANN architectures are used in VANET and applications including such driver ID fingerprint, assault detection, as well as intrusion detection. A deep neural network (DNN) is a kind of ANN with numerous (deep) hidden layers.

1) Making the architecture adaptable for learning bigger datasets is one benefit of utilizing a deep layer structure. Deep network topologies are helpful in obtaining better accuracy, and a deep network learns more complicated tasks than a shallow network. Deeper networks, however, they add significantly higher complexity in terms as processing time as well as convergence. It can be further subdivided based just on optimization function as well as information flow. We go over three distinct DNN types that are used in automotive networks for security in the sections below.

1) A Fully-Linked DNN (FCDNN) is a neural network that has all of its inputs connected to every neuron in every layer below it, and so on. It is referred to be a fully linked network as a result of its varied connection.

2) Convolutional Neural Network (CNN) has outstanding performance for multi-dimensional data and is one of the well-known and often used DDNNs in the literature. CNN is so named because it employs convolution as a mathematical process at various levels of its network architecture. CNN often employs both supervised and unsupervised techniques. This makes unlabelled datasets appealing for use in intrusion detection systems. (IDS). CNN 12 offers the advantage of good training performance while employing fewer parameters because of the weight sharing but also pooling processes. Multidimensional data processing, such as speech and image processing, CNN performs well. For security applications, CNN architecture is used in a number of studies in the literature.

A recursive DNN, a recurrent neural network (RNN), has a feedback looping architecture where each neuron's new output is reliant on both its prior output and its current input. RNN is capable of tracking changing states through time. CNN falls inadequate in various applications, including understanding temporal features in films (i.e., a succession of photos) or text blocks. RNN is designed primarily for processing data sets where the current piece of data has some link to the previous one. The Long Short-Term Memory (LSTM), a typical RNN architecture used in vehicular networks, generates long sequences of time-series data including such traffic flows, sensor readings, including vehicle trajectories.

6. CONCLUSION

Due to the misbehavior and maliciousness of others, users want more protection and security on the road. In the future, further work will be needed to solve these issues in order to create a safe VANET environment. offered a thorough review of the majority of VANET security issues, their root causes, and the remedies already in place. According to our perspective, the VANET system's future research path should concentrate on security and privacy concerns including privacy preservation, which called for further study to address the dangers to security and privacy. Strong authentication mechanisms must also be added to the security system in order to provide secure communication in VANETs. Additionally, handling all types of security assaults calls for an effective algorithm.

Vehicles may exchange traffic data, such as vehicle ID and position, and weather conditions because to the rising need for V2X, C-V2X, and LTE-V communications in the ITS. The vast volume of data and information transferred, which requires privacy and security, is being scrutinized by drivers and passengers to determine its accuracy and dependability. Therefore, customers need a sophisticated VANET algorithm that can guarantee reliable V2V and V2I communication while simultaneously protecting the privacy of their vehicle's ID and position. In order to provide secure communication in automotive networks, ML approaches offer significant advantages. The primary issues with preserving security and privacy inside a network include high vehicle mobility, easily accessible wireless channels, poor authentication, and insufficient trust among nodes.

FUNDING

None

ACKNOWLEDGEMENT

None

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions," *Communications Surveys & Tutorials, IEEE*, no. 4, pp. 584–616, 2011.

[2] R. S. Raw, M. Kumar, and N. Singh, "Security Challenges, issues and their solutions for VANET," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 5, 2013.

[3] . M. Azees, L. Deborah, and P. Vijayakumar, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intelligent Transport Systems*, vol. 10, no. 6, pp. 379–388, 2016.

[4] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications*, vol. 44, pp. 1–13, 2014.

[5] . H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: a survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017.

[6] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[7] M. Azeez, L. Deborah, and P. Vijayakumar, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intelligent Transport Systems*, vol. 10, no. 6, pp. 379–388, 2016.

[8] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760–776, 2019.

[9] S. Sharma and A. Kaul, "A survey on intrusion detection systems and honeypot based proactive security mechanisms in VANETs and VANET Cloud," *Vehicular Communications*, vol. 12, pp. 138–164, 2018.

[10] A. Boualouache, S. M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 770–790, 2018.

[11] A. Ali Hassan, and F. Li, Authentication and privacy schemes for vehicular ad hoc networks (VANETs): a survey, Vehicular Communications, vol. 16, pp. 4561, 2019.

[12] X. Liang, T. Yan, J. Lee, and G. Wang, "A distributed intersection management protocol for safety, efficiency, and driver's comfort," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1924–1935, 2018.

[13] J. Gauge and Mittag, "Feasibility of virtual traffic lights in non-line-of-sight environments," in *Proceedings of the Ninth ACM International Workshop on Vehicular Inter-Networking, Systems, and Applications-VANET'12*, pp. 103–105, 2012.

[14] "Draft guide for wireless access in vehicular environment (WAVE) architecture," 2012. http://ieeexplore.ieee.org/servlet/opac?punumber-6320593.

[15] O and A. Hassen, "Big Data Based Machine Learning and Predictive Analytics using Apache Mahout and Storm," *International Refereed Journal of Reviews and Research*, vol. 5, 2017.

[16] M. Ghosh, A. Varghese, A. A. Kherani, and A. Gupta, "Distributed misbehavior detection in VANETs," in *Proceedings of the IIEEE Wireless Communications and Networking Conference (WCNC)*, 2009.

[17] O. A. H. K. Ibrahim and Hassen, "Preventive Approach against HULK Attacks in Network Environment," *International Journal of Computing and Business Research (IJCBR)*, vol. 7, no. 3, pp. 1–11, 2020.

[18] X. Cheng, C. Chen, W. Zhang, and Y. Yang, "5G-Enabled cooperative intelligent vehicular (5GenCIV) framework: when Benz meets Marconi," *IEEE Intelligent Systems*, vol. 32, no. 3, pp. 53–59, 2017.

[19] N. Hayder, "An Effective Implementation of Face Recognition Using Deep Convolutional Network," *Journal of Southwest Jiaotong University*, vol. 54, no. 5, 2019.

[20] A. A. Abdulhussein, O. A. B. Informatics, and Hassen, "A Pragmatic Review and Analytics of Gait Recognition Techniques in Biometric Domain of Research," *International Journal of Computing and Business Research (IJCBR)*, vol. 10, pp. 2020–2020.