Anomaly Detection of Attempt Through Genetic Algorithm and ANN

Suhas Chavan[1](✉), N. Jagadisha[2], Parikshit Mahalle[3], and Vinod Kimbahune[1]

[1] Computer Engineering Department, Nutan Maharashtra Institute of Engineering and Research, Talegoan, Pune, Maharashtra, India
chavan.suhas18@gmail.com, vinod.kimbahune@nmiet.edu.in
[2] Information Science and Engineering, Canara Engineering College, Manglore, Karnataka, India
[3] VIIT AIDS, Pune, Maharshtra, India

Abstract. Vehicular ad-hoc network, commonly known as VANET, is an enabling technology for supplying security and useful information in modern transport systems but subject to a multitude of attacks, ranging from auditing passively to hostile interfering. When suspicious actions are discovered, intrusion detection systems (IDS) are essential instruments for risk reduction. Additionally, by sharing interactions among their nodes, VANET vehicle collaborations improve detection accuracy. Because of this, the machine learning distribution system is efficient, scalable, and useful for developing cooperative detection methods over VANETs. Because data is exchanged between nodes during collaborative learning, privacy concerns are a basic barrier. Through the data that is observed, a rogue node may be able to obtain sensitive information about nodes other than itself. This research suggests cooperative IDS for VANETs that protects machine learning privacy. Additionally, an intrusion detection classifier is trained on the VANET and the proposed alternating multiplier direction approach is employed to solve a class of empirical risk minimization issues. In order to apply a vector approach of dual disturbance to dynamically varying privacy and provide secure network communication, the usage of privacy differential is done to capture the notation of privacy.

Keywords: VANET · Security · Algorithm · IDS · Machine learning · Genetic Algorithm · ANN

1 Introduction

Road safety is a growing concern as the number of vehicles on the road rises and autonomous vehicle technology develops quickly. Information about safety, traffic control, navigation, and road services can be shared over VANET's communication system. VANETs are consequently thought to be susceptible to a variety of attacks, from passive eavesdropping to direct interference [1]. An intruder might seek and replay other vehicle messages, for instance, to acquire tools comparable to toll services. A targeted vehicle

S. Tamane et al. (Eds.): ICAMIDA 2022, ACSR 105, pp. 355–365, 2023.
https://doi.org/10.2991/978-94-6463-136-4_30

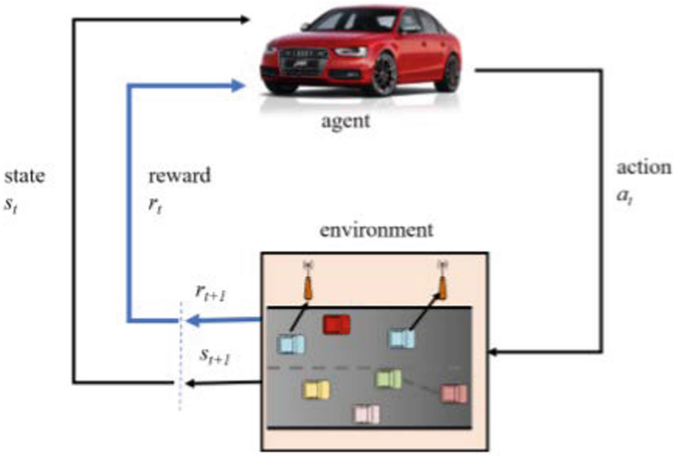

Fig. 1. VANET architecture using intermediator

may be interfered with an intruder, who may also imitate it and provide a false alert that could impede traffic [1].

Machine learning, often known as ML, is the application of artificial intelligence (AI) to teach a computer about unfamiliar concepts and make accurate decisions. ML is used in almost every industry, including manufacturing, robotics, the arts, Biotechnology, smart automated transportation systems, and automated systems. It has gained popularity because it is in expensive, available from highly capable machines with large amounts of data storage and high computing power. It enables quick and intelligent decision-making to raise the system's efficiency in terms of energy, quality of service (QoS), and dependability [1]. Congestion on the roads and health has become dynamic and trouble some concerns in many urban areas as a result of the exponential increase of the population and the motor industry. Around 1.25 million individuals worldwide pass away in traffic accidents each year, making it the leading cause of death for people between the ages of 15 and 29 [2]. Congestion causes expensive delays, heat, pollutants, and fuel wastage. The cost of congestion in the US in 2017 was $305 billion [3]. Less traffic accidents, a greener environment, and smooth traffic flow are all possible with an intelligent and effective transportation network, which improves performance. The Vehicular Ad Hoc Network, or VANET, is used to improve traffic flow, especially during rush hours, and increase road safety, both of which help cut down on travel time for passengers (see Fig. 1). We now need a large amount of spectrum to accommodate large volume capacity allocation over demand due to the rapidly rising demand for wireless devices. This has been a barrier to the implementation and scaling of next generation switching technologies, such as smart cities, high-definition 3D video streaming services, augmented reality, the Internet of Things, and virtual reality (VR).

Development, deployment, and scaling of next generation communication networks, such as high-definition 3D video streaming, smart cities, Internet of Things (IoT), augmented reality, and virtual reality, have been hampered by the need for a broad network to support the high-capacity data usage compared to demand.

Because of this, this work suggests a shared VANET IDS that focuses on machine learning that protects privacy. To detect whether an operation is a natural occurrence or an attack, the classifier is first trained by creating a distributed problem of minimising empirical risk on a VANET using ADMM. At CIDS, we are extending differential privacy to dynamic differential privacy and proposing a conserving strategy for privacy called the dual variable destruction in order to capture the concept of privacy in distributed machine learning. By creating a convex optimization problem and using data sets based on statistical tests to show how the privacy mechanism function optimally, we also examine the DVP's utility and define the DVP's fundamental interplay between security and privacy.

2 Literature Review

Following the part on the numerous research pertinent to VANET, many studies have investigated various designs of intrusion detection systems that are well suited to MANET [3].

Carlos H. O. O. Quevedo et al. [1], author, notes that vulnerability and weaknesses in VANETS are the main problems. In addition to traditional network attacks, VANETs are influenced by modern threats based on the disruption of authentication and false information dissemination, such as threats by Sybil. This paper proposed a system in this context for detecting Sybil attacks in VANETs called SyDVELM. It is based on Intensive Learning Tech techniques, providing more robustness, efficiency and high precision to allow road protection, traffic congestion, digital entertainment and other services to be provided. SyDVELM's proposed approach explains the mobility pattern of the vehicle nodes in urban scenarios. Comparing real vehicle reliability in terms of inaccuracies in the relocation of Sybil nodes. They showed that the use of SyDVELM in VANETS guarantees a high detection rate with very low error rates and a versatile detection process. These features reflect the advantages of SyDVELM, as opposed to the existing Sybil Attack Detection system. They intend to validate the suggested approach in low density (sparse) scenarios and combine the ELM solution with other machine learning algorithms as possible implementation.

Technical developments that result in a wired, mobile, cooperative transport system are described by Stefan Mihai et al. in [2]. They present a thorough review of the currently available potential techniques for maintaining vehicle network communications privacy, stability, and confidentiality as they examine the most significant safety ramifications of VANETs. To close the remaining unresolved challenges, however in terms of both safe automotive accessibility and road networks is necessary for widespread acceptance. The author also discusses the necessity of consistent practices and governance to guarantee adaptability and dependability while maintaining adequate levels of security and privacy. For the information to be delivered securely, network security must also be improved.

Fabio Gonclves et al. publication.'s [3] contains a thorough SLR on how VANET Smart IDs are used. The most popular network traffic simulator and SUMO combo used in the study is Ns-2. It appears that NN (and its different versions) is the preferred machine learning algorithm. The necessary datasets are typically created for each investigation, either from the trace file of the network simulator or from the simulation.

Finding extremely reliable datasets that are available to the general public was one of the SLR's goals. Unfortunately, it doesn't seem that this was feasible. According to the study assessment, the most of them don't explicitly state how their databases and assaults are created. Furthermore, neither of them offers open access to their databases for peer review. Any of them make use of well-known, publicly available databases like the Kyoto dataset and the NSL-KDD. Additionally, they discuss the development of an infrastructure for the sophisticated detection of threats. Making datasets that are sufficiently large to enable successful ML algorithm training should be one goal of this endeavor. A full explanation of the creation of the dataset, assaults, and daily messages should also be provided. Additionally, this needs to be publicly available for peer review.

Machine learning (ML), according to Mohammad Asif Hossain et al. [4], is one of the fastest-evolving computational techniques and is frequently employed to find solutions to pressing issues in a variety of sectors. It is anticipated that the ad hoc vehicle network, or VANET, will be crucial in reducing traffic congestion and accidents. This location has to exchange a huge amount of data in order to be secure. Therefore, the VANET's current connectivity is unable to handle such massive amounts of data. VANET thus faces a spectrum shortage issue. Cognitive radio, i.e. for dealing with problems of this nature, CR may be the solution. One of the numerous steps for performance improvement that a VANET based on CR or CR-VANET may achieve is connectivity with ultra-reliability and low latency. In order to make CR-VANET extremely intelligent, to achieve accelerated adaptability to environmental conditions, and to boost service efficiency in a way that is energy efficient, ML techniques can also be integrated with CR-VANET. They give an overview of CR, VANET, CR-VANET and ML including information on their architecture, features, unresolved concerns, and problems. In CR-VANET scenario testing, the specification and functions of methods of ML were assessed. It also provides details on how ML is applied to automated or driverless vehicles. The implementations and most recent developments of ML techniques covered in various CR-VANETs domains, such as routing, spectrum sensing, security, and resource utilisation, are also defined. Many facets of the use of ML in AVs have been identified, and its functions have been expanded to reduce traffic jams and traffic accidents. Using ML techniques to take advantage of the benefits of research because those domains are still in their early phases. In his thesis, he talked about some of these perspectives, unanswered issues, and potential directions for the discipline.

In this work, WANG TONG et al. [5] discuss not only the architecture, elements, and operations of SDN based VANETs, but also how these VANETs provide better communication than conventional VANETs. We can lower the overall network load by managing the network as a whole from a single remote controller. SDN controllers can also keep track of security threats. In this article, it was stressed how tracking and managing the entire transportation networks, which had previously been a challenge, is greatly aided by the modern vehicle technology.

Hussein et al. [7], author, comments that many of the method's SDN adoptions are still hampered by many security issues. In this report, they analyzed security vulnerabilities, risks, and solutions in the current SDN stage. The capabilities of the SDN show a host of new challenges to the network. Therefore, it is important to make them more robust and efficient in order to adhere to the standards of these networks. Since the techniques

are primarily designed for certain aggressive scenarios, they work well in the after math of such attacks but fail under unanticipated attacks. While the amount of funding and research within the SDN domain is rising, the security community is hesitant to embrace the SDN technology and to adopt it. It is difficult to find research that examine the practicability, feasibility, reliability, and effectiveness of SDN-based network security technologies. A more ambitious aim for SDN security is therefore to create a multifence safety strategy that is embedded into every part of the network, resulting in deep coverage that offers several lines of defense against both known and unknown security threats.

In this paper, Boutaba et al. [8] presented a thorough overview of the limitations, difficulties and threats in the architecture of the SDN, in various de-facto scenarios. Authors also implemented an innovative approach to define and secure the SDN-based networks using fine-grained semantic analysis of the defense network. Also aim to strengthen overall network security, particularly the SDN stack, by advancing the state of the art through upgrades and a hardened network-operating system. It provided SDN controller and other SDN domain communication instruments with technical challenges. They also developed a legislative-focused security framework. This software will guard and track behaviour on the SDN domain. Also, ONOS SDN manager for designing this software and evaluating the threat scenarios. Finally, they reflect those possibilities of attacks that we use our mechanism to counteract. We are also showcasing our findings for the test.

S. Pouyanfar et al. [9], author explains the vulnerability to DoS assaults, and to indicate diagnosis, models for DoS assault detection need to be established rather quickly. In this report, they proposed one approach that centered on changing the packet propagation ratio. This will sense the existence of attacks like DoS as soon as their attacks are successful. They also state that in future work, the black list will be encrypted to be sent to the RSU for delivery to network users to discourage packets from being collected by attackers. We'll also review the DOS problem, based on learning's stochastic game.

Y. Gordienko et al. [10], Writers have a thorough overview of SDN-based literature of the Next Decade. An overview of the SDN architecture is given along with SDN implementation code. It tackles SDN's features. The numerous approaches to building next-generation networks with SDN are being discussed in detail. Combining SDN with the smart house, smart buildings, smart mobility, optical networks, and handheld wireless sensor network can solve the key problems. In order to extend SDN's reach to other smarter networks, there are still several problems to be discussed.

L. Liang et al. [11], In order to make vehicle networks feasible and suitable for customers, it is important to establish reliable protocols which follow the strict requirements of this application field. The creation of secure protocols is complicated by consumers, automakers and government's seemingly conflicting requirements, particularly when attempting to provide successful vehicle identification while preserving driver privacy. Fortunately, vehicle network properties provide various approaches to these concerns, helping us to create new primitives based on, for example, vehicle trajectory interference and basic reanonymizers. They hope that the challenges raised in this paper and possible solutions inside vehicle networks will encourage other researchers to begin investigating this important and exciting area of study. The mechanics of various intrusion detection systems that are ideally suited for MANET have been the subject of numerous studies

[3]. The MANET architecture can be divided fundamentally into three kinds. The fragmented life of MANET is first addressed by distributed and cooperative IDS, which can be expanded via network cooperation.

For instance, Zhang and Lee employed this type of MANET in [10] to develop a model for a sizable, cooperative IDS. Albers et al. are the last. A shared IDS that was centered on local IDS was launched in [11] using mobile agents. Each MANET network uses the local IDS to address local network-based security issues, but by enhancing local IDS cooperation throughout the MANET, the local IDS can be expanded to address global security issues. The second kind of IDS system integrates relational structures and cooperative models inside a hierarchical framework.

In [12] H. Ye, L. Liang, and colleagues created a complicated hierarchical IDS using multilevel clustering. The third architecture is based on the concept of a virtual agent that can go throughout the vast network. Each mobile agent in this system is assigned to work on a certain task, and one or more mobile agents are subsequently distributed throughout the MANET to each node. The work of Kachirski and Guha [13], who introduced distributed IDSs using several mobile agent-based sensors, is among earlier investigations. As a result, the workload is divided into realistic tasks and assigned to specific agents. ML and data processing have also been studied in literature. These techniques enable IDS to gain experience in security systems, relate unexpected events, learn about threats and how they operate, and foresee attacks. The clustering process, which is an unattended investigation of trends, was one example of the unattended learning in IDSs that researchers were exploring. There are several methods for grouping unlabeled data; for instance, Blowers and Williams' density-based spatial clustering of applications with noise clustering algorithms [14] was developed to combine regular network packets with abnormal ones. The grouping based on hierarchy [15] and the K-means [16] are two instances of clustering. Guided learning is covered in IDS literature as well, for instance, assistance for vectors. To locate the fault based on the time position of the data, Wagner et al. [18] built an SVM classifier of a single class using a kernel of new window. Numerous techniques, including decision trees, artificial neural networks, and sequential data aggregation, are a part of supervised learning. Additionally, work was done on non-ML-based intrusion prediction-dependent detection.

For example, B. Khalfi et al. [13] created a game theoretical model to identify intrusions in the VANET. This model predicts that further denial-of-service attacks on the controlled nodes are likely to occur. In the area of privacy differentials, there are numerous studies on the use of differential privacy to machine learning. A corpus of literature has been studying the relationship between privacy and performance in ML ever since researchers began studying the differential privacy theory. Many experts are also focusing on the condition of the transmitted differentials. Eigner and Maffei developed a fully automated mechanism for verifying distributed difference protection while constructing cryptographic protocols. They presented a technique that is differentially private to solve a distributed constrained optimization based on distributed simulated gradient descent in order to protect the privacy of constraint collection.

S. Shahrestani et al. [15] private differential computations were performed on a cloud computer, preventing state leakage throughout the network's distribution of results to all agents. The concept of dynamic differential privacy is employed in this study to

build a mutual IDS using distributed machine learning in order to safeguard the identity of the research dataset used in the learning process. In the first scenario, the open loop solutions prevent interference from occurring Utilizing measuring techniques that gauge the quantity of messages in the queue, the channel's use level and its.

occupancy, congestion can be identified. As stated in the introduction, hybrid techniques and strategies based on costs, resources, CSMA/CA, priority setting, and scheduling are two sub categories of VANET congestion management solutions [17]. We will go over those strategies in more detail below. Several different VN-attacks [7, 10] are as follows.

1. Phony data in this case, the inward-looking, rational and active square attacker's test. They will relay incorrect data within the network because it influences the actions of different drivers.
2. Cheating with sensing element data this attack is undertaken by UN company attacker AN is corporate officer, fair and engaged. He uses this attack to change the expected position, distance, and trajectory of multiple nodes to prevent liability in case of failure.
3. ID speech act an intruder is a business executive who is passive and bad. It may trace the trajectories of a target vehicle and can use the data to identify a car.
4. Denial of Service (DOS) In this case the Attacker is hostile, violent and local. Assailant can try to bring down the network by causing unwelcome messages on the guide. Examples of this attack include insertion of clear, automated Counter measure and dummy messaging.
5. Replaying and Dropping Packets An attacker has the ability to lose valid packets. As an example, AN intruder would remove all warning messages intended to warn vehicles that will move to the crash site. Similarly, AN intruder would recover the packets at the moment the incident occurred to establish the illusion of an accident.
6. Hidden Vehicle This form of attack is feasible in a very situation anywhere automobiles conveniently attempt to reduce congestion on the wireless channel. As an example, a car has sent a warning message to its neighbour, expecting a response. If the vehicle receives a response, it knows that its neighbour is in a much better position to forward the warning message and prevents sending the warning to multiple nodes.
7. Worm Hole Attack is hard to detect and forestall this attack. A malicious node will catch packets at one location within the network and relay them to multiple locations via a specific network connected to malicious nodes. Attack strength would increase if the malicious node only sends management messages through the channel, rather than packets of information.
8. Sybil Attack In this assault a vehicle forges the identities of multiple vehicles. Inside the scheme these identities can be used to perform a form of attack. Furthermore, these false identities generate AN illusion that additional vehicles are numbered squarely on the road. The effect of this attack is that if different node positions or personalities within the network are spoofed, each attack variant will compete.

3 Research Gap

Common VANETs are peculiar for their maximum decentralization where a network lacks a selected server and their infrastructure and functionality are spreaded among hosts. Today, VANETs support many new services and protocols. This feature defines a number of problems caused by the improvement of the level of service provisions when using a new type network, as well as by its low mobility capabilities and long response a midst aggressive external influences.

The lack of connectivity and the consequent lack of VN authorization facilities hinders the normal procedure of forming a security line, separating nodes into trusted and untrusted ones. Such a distinction may have centered on a compliance policy, possession of the necessary credentials and node authentication capability. The properties of VNs, notably communication in an open access environment, make security and privacy issues a serious challenge. VNs are also made up of all manner of machines, and certain networks are resource-constrained nodes, thus reducing complexity as much as possible, and network security must be guaranteed.

The sources of problems related to information security in VANETs are as follows:

1. The absence of the tools of host protection from intruders.
2. The possibility of wire tapping the channels and substitution of messages due to shared access to the communication environment.
3. The impossibility of using a usual system of security due to the features of the VANET architecture.
4. The need to use complex routing algorithms that take into consideration the probability of receiving incorrect information from hosts that are compromised as a result of changing the network's topology.
5. Any host that is nearby the signal source and is aware of the data transfer frequency and other physical parameters (such as the modulation and coding method) may be able to intercept and decode the signal.
6. The VANET's decentralisation makes it impossible to apply security polcies, and there are no conventional security techniques that can function with dynamic topology.

4 Problem Statement

In particular, VNs must be highly flexible in order to adapt to certain situations and use cases, and have very low latency. It then has to be reconstituted to break into the rigid structure of the network and simplify hardware operation. Network nodes can be intercepted, hacked, and used to communicate with attackers, and node communications can be faked and introduced into the network or replayed there. Malicious nodes deliberately obstruct the network's normal operations in an effort to stop it from functioning normally.

The deployment of VN would be significantly impacted by these problems. As a result, the defence at VNs has a more difficult duty. These problems include a lack of source-destination connectivity and a lack of data connectivity caused by the poor

performance of wireless networks between different nodes. As a result, VNs must be exceedingly adaptable in order to handle any circumstance.

However, there are number of challenges remain to be addressed. Some of it's as follow:

1. Performance & Flexibility
2. Scalability
3. Interoperability

Since VN is made up of all kinds of devices and certain networks are Resource-constrained nodes, the security of the network must be assured, thereby reducing overhead as much as possible.

5 Objectives

Intrusion detection alone or in conjunction with the prediction feature can be an effective way of detecting fraud and discovering odd behavior in large and complex network.

1. Study & Analysis of various attack &security issue in VANET.
2. Review of real-time data behavior in VANET Network using existing system.
3. Development of ML-based system to increase Intrusion detection system
4. Performance & preventing harmful warnings for false positive/negative factors.
5. Performance analysis of proposed model by comparing different ML algorithm for
6. Intrusion detection system in VANET network.
7. Anomaly detection of attack through genetic algorithm and ANN.

6 Proposed Work

The proposed model architecture, which consists of various VANET building elements, is described in this section of the study. Application AU, on-board - RSU, and OBU modules make up most VANET systems. Vibration or wireless communication in the vehicle environment is the basis for contact between OBUs (car to car) or an OBU with an RSU (vehicle to infrastructure) [3]. RSUs may also be connected to other infrastructures, such as other RSUs and traffic control centers, and these connections are made using additional wireless communication (infrastructure to infrastructure). It has an OBU in addition to a few AUs. Additionally, the OBU has a variety of sensors that it makes use of to communicate information with other RSUs or OBUs and gather information on them. For interested readers, information on the three essential components of a VANET's architecture is offered. Each vehicle has a local PML-CIDS agent, which, as can be seen in Fig. 2, monitors local operations such as those in OBU and AU communications.

The collaborative framework is essentially made up of three key components: a local detection engine for the system, a collaborative ML engine, and a privacy-preserving pre-processing engine. The pre-processing engine, which controls the actions of the vehicle system in real time and aids in security from unauthorized access, collects and preprocesses data from the VANET framework.

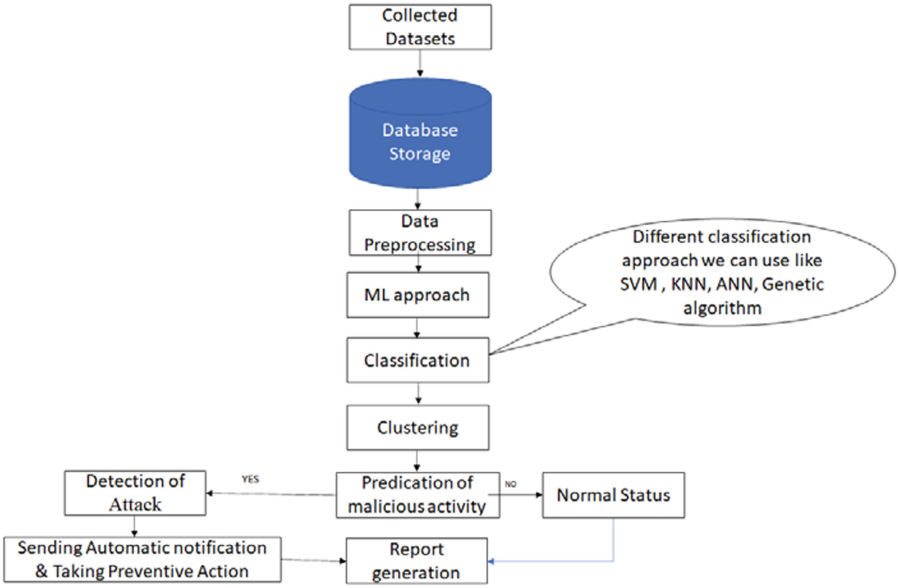

Fig. 2. Architecture of Proposed IDS System using ML

References

1. Carlos H. O. O. Quevedo, Ana M. B. C. Quevedo, Ahmed Serhrouchni.: "An Intelligent Mechanism for Sybil Attacks Detection in VANETs", 978–1–7281–5089–5/20/$31.00 ©2020 IEEE.
2. Stefan Mihai, NedzhmiDokuz, Meer Saqib Ali, Purav Shah, and Ramona Trestian.:" Security Aspects of Communications in VANETs", 978-1-7281-5611-8/20/$31.00 c 2020 IEEE.
3. Fabio Gonc¸alves, Bruno Ribeiro, Oscar Gama,:"A Systematic Review on Intelligent Intrusion Detection Systems for VANETs", 978-1-7281-5764-1/19/$31.00 ©2019 IEEE.
4. WANG TONG, AZHAR HUSSAIN , WANG XI BO , AND SABITA MAHARJAN.:"Artificial Intelligence for Vehicle-to-Everything: a Survey", 2169–3536 (c) 2019 IEEE.
5. C. Chembe, D. Kunda, I. Ahmedy, R. Md Noor, A. Q. MdSabri, and M. A. Ngadi.: "Infrastructure based spectrum sensing scheme in VANET using reinforcement learning," Veh. Commun., vol. 18, p. 100161, 2019.
6. Dimitrios Kosmanos, Apostolos Pappas , Francisco J. Aparicio-Navarro.: "Intrusion
7. Detection System for Platooning Connected Autonomous Vehicles", 978-1-7281-4757-4/19/$31.00 c 2019 IEEE.
8. W. Tong, A. Hussain, W. X. Bo, and S. Maharjan.: "Artificial Intelligence for Vehicle-to-Everything: A Survey," IEEE Access, vol. 7, pp. 10823–10843, 2019.
9. R. Boutaba et al., "A comprehensive survey on machine learning for networking: evolution, applications and research opportunities," J. Internet Serv. Appl., vol. 9, no. 1, p. 16, 2018.
10. S. Pouyanfar et al., "A Survey on Deep Learning: Algorithms, Techniques, and Applications," ACM Comput.Surv., vol. 51, no. 5, pp. 92:1--92:36, Sep. 2018.
11. Y. Gordienko et al., "Deep learning with lung segmentation and bone shadow exclusion techniques for chest x-ray analysis of lung cancer," in International Conference on Theory and Applications of Fuzzy Systems and Soft Computing, 2018, pp. 638–647: Springer.

12. L. Liang, H. Ye, and G. Y. Li, “Towards Intelligent Vehicular Networks: A Machine Learning Framework,” IEEE Internet Things J., vol. PP, no. c, p. 1, 2018.
13. 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 Veh. Technol. Mag., vol. 13, no. 2, pp. 94–101, 2018.
14. B. Khalfi, A. Zaid, and B. Hamdaoui, “When machine learning meets compressive sampling for wideband spectrum sensing,” in 2017 13th International Wireless Communications and Mobile Computting Conference (IWCMC), 2017, pp. 1120–1125.
15. Ara and A. Ara, "Case study: Integrating IoT, streaming analytics and machine learning to improve intelligent diabetes management system," in 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), 2017, pp. 3179-3182.
16. S. Shahrestani, “Assistive IoT: Deployment Scenarios and Challenges,” in Internet of Things and Smart Environments: Springer, 2017, pp. 75-95.
17. S. Pandit and G. Singh, “Spectrum Sensing in Cognitive Radio Networks: Potential Challenges and Future Perspective BT -Spectrum Sharing in Cognitive Radio Networks: Medium Access Control Protocol Based Approach,” S. Pandit and G. Singh, Eds. Cham: Springer International Publishing, 2017, pp. 35–75.
18. N. Muchandi and R. Khanai, “Cognitive Radio Spectrum Sensing: A Survey,” Int. Conf. Electr. Electron. Optim. Tech. - 2016 Cogn., pp. 3233–3237, 2016.
19. J. Qadir, “Artificial intelligence based cognitive routing for cognitive radio networks,”Artif.Intell.Rev., vol. 45, no. 1, pp. 25–96, 2016.
20. S. M. Baby and M. James, “A Comparative Study on Various Spectrum Sharing Techniques,” Procedia Technol., vol. 25, no. Raerest, pp. 613–620, 2016.