IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Solving Vehicular Ad hoc Networks Issues using Machine Learning

[1]Saleha I. Saudagar, [2] Dr. Rajendra Prasad Mahajan

[1]Assistant Professor, [2]Professor

[1]Information Technology,

[1]Prof. Ram Meghe Institute of Technology and Research Badnera, Amaravati, India

Abstract: As an emerging technology various researches are going on in Vehicular ad hoc networks which helps in development of smart cities across the world and while doing this various issues are exploring in it like Clustering/Platooning concept, routing strategies, security issue while exchange of information among vehicles. In this paper, various issue in vehicular Ad hoc networks are discussed and its solution with the help of Machine learning. If machine learning concepts are used to handle issues in vehicular ad hoc networks, it can give a new way to Smart Transportation system**.**

Index Terms **- Machine learning, Vehicular network, clustering, routing, Security.**

I. INTRODUCTION

Due to development in transportation system vehicle can communicate with each other and are autonomous. Also there is rapid growth of number of vehicles on road which leads to shortage of space, high accident-rate and wrong driving habits. Vehicular Ad hoc network is a technology which ease and facilitate vehicle driving, which uses recent wireless technology IEEE802.11p and communicate among vehicles and Infrastructure and can improvise road safety and sustainable transportation and form intelligent transportation system (ITS).

As the future technology, machine learning/Artificial Intelligence is included in almost all field of science and technology. Consider an example of vehicle which learn to predict and make decision of routing.

I am going to discuss various issue in vehicular Ad hoc networks like Routing, Energy efficiency issues of Vehicles while connected with VANET infrastructure, Clustering of Vehicles and various security aspects in VANET one by one then its solution with the help of Machine learning. Various researches are going on in Vehicular ad hoc networks which helps in smart transportation system. Vehicular networks are susceptible to variety of attacks and there are variation of mechanism developed which help to detect and prevent the attacks. Misbehavior detection system (MDS) is mechanism used to detect and prevent insider attacks. MDS identify attackers with the help of cooperative scheme which is used for the fast eviction of misbehaving vehicles. Machine learning based misbehavior detection system it has false alert verification scheme, position falsification verification scheme and fast exclusion of misbehaving vehicles.

II. LITERATURE WORK

Ad hoc networks are a wireless networking standard for mobile node/hosts. Unlike centralized mobile wireless networks, ad hoc networks do not depend on any fixed infrastructure. Instead, each node rely on other to keep the network connected. Due to unique properties, ad hoc networks there is a trend to adopt ad hoc networks for commercial use. As wireless network the nodes in Ad hoc network can be movable called it as Mobile Ad hoc network (MANET).

Singh et al (2011) have mentioned that Mobile ad hoc networks are self-organized, self-monitored ad hoc network of laptop, cellular phone, PDA's and can be used for various communications for information sharing. It has dynamic topology, limited physical security, and energy, power constraints. A Vehicular Ad hoc networks is a special type of MANET which helps to provide communications among nearby vehicles and nearby fixed road side unit (RSU). The main aim of vehicular ad hoc network is to provide safety to riders and drivers to make better travel judgement to alleviate traffic congestion, improve traffic operation efficiency, and reduce carbon emissions. The development and deployment of Intelligent Transportation System (ITSs) provide better accuracy Traffic flow prediction.

Ayappan and Mohan kumar (2016) have mentioned the dynamic nature of VANET and frequent change in its topology, also the use of IEEE 802.11 family communication standard for routing and benefits of its use. As fast moving vehicles need efficient communication there are several issue which should be handled efficiently like mobility domain, infrastructure domain and routing domain.it has focused on improving routing of vehicular technology.

Along with routing, energy conservation is also considered as one of the most important issue in Vehicular Ad hoc Networks. VANETs flood uninterrupted broadcasting of messages and allow considerable amount of power and storage, involve communication between vehicles and other battery-fed devices—pedestrian smartphones, road transceivers, sensors. Thus, the power consumption by wireless communications becomes a major concern, and the use of energy-efficient communications is highly desirable. Hence energy efficient techniques are always welcome in this area, further I will focus on some literature related to energy efficient communication.

Toutouh et al (2012) have introduced a fast automatic methodology to search for energy efficient OLSR configurations by using a parallel evolutionary algorithm. Optimized Link State Routing (OLSR) is a well-known proactive routing protocol used in VANETs which conceived for mobile ad hoc networks with low bandwidth and high mobility and its power consumption can be improved by modifying the standard parameter configuration, in order to reduce the routing overhead. The standard OLSR parameter values can be fine-tuned automatically by using an optimization technique, with the aim of obtaining efficient OLSR configurations for VANETs. This procedure allows reducing the power consumption without incurring a significant loss of QoS.

Chang et al (2014) have stated about a VANET that the bandwidth, power, speed of mobile node, density of topology, and distances between mobile nodes are all factors that can affect the energy consumption. As these factors may cause packet losses, performance degradation or poor link stability. Thus, one of the challenge for future VANETs is the reduction of wasted bandwidth and power, while quickly responding to network changes and keeping a stable information transmission. And hence they have proposed energy efficient geographic routing algorithm that uses the direction, density and distance between nodes in the crossroad routing strategy, to improve the link stability to minimize packet loss rate and average end-to-end delay in VANETs to reduce the power consumptions.

Bali et al (2015) have stated as vehicles in VANETs are constrained with respect to the available resources such as computation and storage, lot of energy is consumed to perform a number of complex operations, which may lead to the emission of harmful CO2 that effect the global warming system. Moreover, because of high velocity of vehicles there are constant topological changes, it is a challenging task to maintain quality of service with respect to parameters such as high throughput, and minimum end-to-end delay. Predictive clustering approach optimize the various complex operations in this environment and led energy aware clustering technique and minimize the emission of CO2 and other gasses.

Laroiya and Lekhi (2017) have briefed about energy efficient routing protocol in VANET. Here the algorithm finds reliable and stable route for packet transmission from source to destination by using real-time traffic information such as energy utilized during transmission is less. And thus propose routing protocol that minimizes energy consumption and ensures apt information delivery in real-time.

Satheshkumar and Mangai (2020) have suggested an algorithm which reducing message distribution delay with minimal communication overhead named as energy efficient-fast message distribution routing protocol (EE-FMDRP). It is using both time and direction routing model. The protocol introduced here realizes the VANET prospective to improve the traffic safety and traffic management and to provide smart transportation model. Moreover, EEFMDRP works on considering the direction in which the vehicle running and the message delivery time for minimizing the message distribution delay and communication overhead in emergency situations. The fast message distribution model works on four phases: adaptive beaconing (AB) initialization, vehicle direction (VD) based authorization, message delivery time (MDR) based confirmation and energy efficient route framing.

Mehmood et al. (2018) have elucidated about Formation of Stable Clustering in VANET with the help of Naïve Bayesian Probabilistic Estimation for Traffic Flow. As VANETs raise many innovative challenges due to their high-class and unique features, such as high node mobility, dynamic topology changes, wireless links breakage, network constancy, and network scalability, a well-organized routing with clustering approach is one of the most promising solution. Clustering is an eminent method to form groupings of vehicles and thus organize ad hoc networks, and is also an effective method to make the VANET global topology less dynamic. The clustering approach is a well-organized and efficient key to the scalability issue. The hidden terminal problem can also be reduced by clustering. Clustering in VANETs is an operative method to shorten some significant functions, such as vehicle management, routing, medium access management, the provision of resources and bandwidth. The process of clustering involves formation of cluster head (CH), here the heavy traffic flow lane use information, speed alteration, direction, connectivity level, cluster size and vehicle distance is taken into consideration, for selecting a long-lasting cluster head and achieve stability.

Lou et al. (2010) have introduced an algorithm for cluster based routing where geographical area is divided into a series of logical grids and the data packets are routed by cluster headers across some grids one by one. Each grid has its own cluster header and transports the data packets through it to one of its neighbor cluster headers. The CBR have low packet delivery delay and average routing overhead, also the packet delivery ratio is very high.

Information safety is considered to be one of the most important issue in Vehicular technologies and in any network. VANET is blend of sensors and ad hoc sites, and have dynamic nature, it uses wireless shaft, satellite communication, and additional communication medium to interact. While Running vehicles communicate with each other and infrastructure unit if get attacks and some wrong information is conveyed, it can be risky as a life threatening situation. Rapid growth in ITS (Intelligent Transport system) leads to various attacks on system, there can be delay to message delivery, Denial of service attack, eavesdropping attack. The Security of VANET greatly depends on the secure delivery of message. Kaur (2018) has described entities concern with VANET security like vehicles, infrastructure, driver, third parties, attacker and also mention security requirement in VANET. As Deeksha et al (2017) have mentioned, VANET facilitate vehicles to give information about safety through its communication with other vehicles included in VANET security which can be achieve with various countermeasure. It is found that Encryption and authentication plays an important role in VANET security.

In current safety system the detection algorithm are used to detect attack which cause delay overhead, RosalineMarry et al (2013) have defined attacked Packet detection algorithm (APDA) which is helpful to detect Denial of Service(DoS) attack and minimize overhead delay and can detect attack in early manner overall improve security. Authentication is provided to prevent nodes in VANET from various attack and block unauthorized node and this secure data transmission is

arrange in cluster in timely manner. Vampire attack attacks on cluster head in cluster where routing depletion affect the path and resource depletion affect the power and bandwidth. To prevent VANET from this attack Jagnade et al (2016) have introduced a technique of Low Energy adaptive Clustering Hierarchy (LEACH) protocol. Hence increases network lifetime and usefulness of system.

Mejri et al (2014) have mentioned about the communication architecture of VANETs and outlines the privacy and security challenges that need to be overcome to make such networks safety usable in practice. The classification of VANET in VANET from a cryptographic point of view is Attacks on availability, availability, authentication, non-repudiation/accountability, integrity and data trust.

Samara et al (2010) have also studied various attacks in VANET and studies its solution. An analysis of VANET attack and attackers is shown here. The various security concern like attack and attackers are enlisted along with the security requirement like availability authentication, non-repudiation, real time constraints, confidentiality also overviewed with its probable solution.

Manivannan et al (2020) have surveyed the secure authentication and privacy-preserving techniques in Vehicular Ad-hoc Networks (VANETs) in last 10 years based on tools and technique used in excellent way. Nowadays every field is trying to achieve the self-automated devices whether a medical, education, marketing field, airlines or any other transportation. Machine learning or Artificial intelligence which help machine/device to learn from its own experience is the way to achieve automated devices. Consider an example of vehicle which learn to predict and make decision of routing. It will improve the routing decision as it gathers more information. As stated by Ray et al (2019), the process of learning begins with observation, or data, direct experience or guidelines which gradually collect data and make approximate decision and this would refine gradually as information gathered. Rely on the type and category of training data available, Machine learning methods can be supervised learning, unsupervised learning, semi-supervised learning and reinforcement leaning to apply appropriate machine leaning algorithm.

Routing protocols play a central role in the design of smart vehicular network. To meet the challenging requirements of the vehicular networks we analyze the suitability of a machine learning based routing algorithm. RSAR (rewarding smart Ad hoc routing) protocol for Mobile Vehicular Ad hoc Network is discussed by Zhang et al (2019). In VANET various issue are identified like such as security areas, safety notification, road barrier warnings, and calamity circumvention issue, and issue such as in-car show business. Routing is one of the most important issue intelligent transportation system design which can be improved and have scope of research, it is one of prime problem of a routing protocol development with better reliability and low latency and machine leaning can help improve routing. As VANET is a derived from traditional MANET, routing protocol used here are same and are active routing, reactive routing, geo-based beacon routing, and geo-based beaconless broadcast routing.

As there are high-speed mobile nodes/cars in VANET, network topology changing frequency is very high which causes routing efficiency to decrease For increasing the routing efficiency and traffic protection, and avoid the happening of traffic accidents (such as collision, rear-end), a reliable and adaptive routing protocol. The reliability of the whole link depends on the links between each hop. Here a reliable model of the link between nodes through a detailed study of the motion characteristics of vehicles and calculating the probability of link reliability have been established, hence it uses the result as a parameter in the D-Learning algorithm to design the RSAR protocol.

Zhang et al (2018) have discussed about software-defined trust based optimal routing with deep reinforcement learning for VANETs. As deep reinforcement learning (DRL) algorithm mark big improvements paralleled with the traditional machine learning algorithms. The DRL algorithm uses a deep Q-network to develop a novel artificial agent that can learn successful policies from high-dimensional inputs, and has gotten quite good results. DRL is used here to attain routing selection policy in the application for ITS, applying the deep reinforcement learning algorithm and the core idea of SDN into VANET routing. Specifically, by decoupling the control and data forwarding plane in VANETs, we deploy the DRL algorithm into a logically centralized controller. Therefore, this scheme will have some features like high flexibility, self-learning capability, and programmability.

Zhao et al. (2016) have introduced machine learning algorithm in particular Support Vector Machine (SVM) to process the vehicle data and generate routing metric to enhance the effect of these features by studying features of vehicle nodes and drivers and compare the feature of Greedy Perimeter stateless protocol.

As I have discussed the issue of Energy conservation earlier about vehicular ad hoc network, it can also be solved with the help of machine leaning usage.

Meena et al (2020) have given one of the energy conservation way by focusing on predicting real-time and exact traffic information. When vehicle moves on road there can be number of factors which affect driving like rallies, road reconstructions, traffic jam and many more. If we got prior information which is very near approximate about all the above and man more daily life situations which can affect traffic then, a driver or rider can make an informed decision and this way help in future autonomous vehicles. Nowadays traffic emission is huge and data generated from it much bigger hence big data handling way would be more efficient and to access real time information and make prediction machine leaning technique is best suited. In Traffic Prediction for Intelligent Transportation System the algorithm have been developed here for identifying and classifying congested situation.

Balico et al (2018) have used the localization prediction as an extension of a data fusion localization system in order to improve efficiency of VANET. In such an approach, a future position of a vehicle is predicted for a given future time and used to take advantage of a future time-space window of a vectorial trajectory rather than a static localization point. The use of localization prediction can be a natural way to improve VANET applications and hence increase energy saving. The approach for localization, target tracking and time series prediction techniques can be used to estimate the future position of a vehicle.

VANETs based safety models require high reliability and low latency in their performance. Machine Learning/Deep Learning algorithms can be one of the milestone for security issues analysis and detection in VANETs. The success of ML/DL count on the model ability to handle the dynamic nature of vehicular networks. Eziama et al (2018) have developed the trust model which provides a data-driven approach in solving the security challenges in dynamic networks. Here the classification process and the extraction of relevant features using a hybrid model like Bayesian Neural Network is used to create trust model and combines deep learning with probabilistic modeling and effective generalization in trust computation to identify honest and dishonest nodes in the network for smart decision.

Wireless medium allow access to any spreading packets for an intruder in the area, and decentralization in VANET allows any random node to involve in packet forwarding. Because of this the faulty or malicious node can simply affect integrity, availability or confidentiality of the network. There are many more measures taken to prevent or detect misbehaving vehicles/ nodes in the network. The first is known as Intrusion Prevention System (IPS) which are programmed to detect the unauthorized or malicious node to access the data and by this is validate the integrity of the network, the latter is an Intrusion Detection System (IDS). Zeng et al (2018) have introduced the combination of a modified promiscuous mode along with Support Vector Machine (SVM) classification establish a precise trust score table for both IPS and IDS in VANET. Every node/ vehicle in network in packet forwarding route checks the behavior of their next hop to detect if there is any signs of a mischievous node and whether it can affect the performance of the system.

Zeng et al (2018) have enlightened an intrusion detection system that deals with monitoring malicious activity. VANET have IDS but machine learning based intrusion detection system is robust in environment changes which is frequent in VANET.

Intruders can be passive or active violating the privacy of users or disrupting and otherwise consistent data flow. Trust Aware SVM-Based IDS use modified promiscuous mode in an efficient way together with SVM for analyzing active network nodes and mark them as trusty or malicious vehicles based on the reputation of their performance data gathering, we use promiscuous mode with altered behavio457\4r for more efficiency and security to capture and analyze packet headers. As SVM is a reliable machine learning tool for various non-linear classification scenarios

Shamsa et al (2018) have stated that SVMs are supervised machine learning tools which expertize a high detection ratio for malicious node detection, it is a reliable machine learning tool for various non-linear classification scenarios. After collecting the predefined statistics used in intrusion detection, they are used in the detection module for additional analysis. This makes it a suitable method for identifying network intruders by providing applicable parameters as the input of the machine, and its effectiveness is proved in different environments before.

As VANET's wireless communication increase driver's and vehicle sensors line-of sight, hence enhancing situational awareness. The safety and performance of VANET depends on exactness of data exchange, location spoofing can be one of the menace for it. Steven et al (2018) have explored the common ML techniques and provide detection scheme baseline to the machine learning community. Plausibility check is used to validate correctness of data. Here Location Plausibility Check and Movement Plausibility Check are integrated into feature vector then supervised ML techniques like K-Nearest Neighbor and Support Vector Machines (SVM) are implemented to improve the overall Precision value of misbehavior detection system. He proved that a misbehavior detection system that uses plausibility checks and machine learning provides 20% higher accuracy and maintains a recall within 5% percent of the recall of plausibility checks.

Sroka et al (2020) have proposed the distributed VDSA (Vehicular Dynamic Spectrum Access) framework for vehicles operating in platoon formations concept where *Platooning* is one forthcoming application of the developing autonomous driving technology, where a more than one self-driving cars and/or trucks forms a group, it is led by a lead vehicle(called as cluster head in clustering) for safety operations of autonomous driving, *e.g.* using the Complaisant Adaptive Cruise Control (CACC), intra-platoon communication will be done in wireless way. The communication schemes like Dedicated Short-Range Communications (DSRC) is responsible for exchange of information within a platoon formation. However, study have shown that solutions based on the IEEE 802.11p and Wireless Access in Vehicular Environment (WAVE) standards are susceptible to medium congestion when the number of communicating cars is large. An alternative approach to remedy this issue is to offload traffic to other frequency bands, such as underutilized television channels (known as TV White Spaces (TVWS) and this technology is VDSA. As concept of platoon formation execute the concept that all platoon vehicles share their information with platoon head which is responsible for the selection of transmission band.

Sroka et al (2020) have explored the idea of partial intra-platoon traffic offloading from the Control Channel (CCH) in congested 5.9 GHz band to TVWS using the VDSA framework is considered and to select transmission channel dynamically in TVWS in distributed manner Bumblebee-based algorithm are used. The proposed distributed VDSA framework using computer simulations aided with realistic DTT signal power obtained with the measurements described. There are challenges while deploying of VANETs like bad effect of malicious vehicles and bad utilization of network. Numerous researchers have already made some excellent mechanism on trust-based security schemes in VANETs, they are still hard to ensure safety because most existing security works couple data forwarding with control. Meanwhile, a lot of researchers proposed various schemes based on machine learning algorithms to solve the VANET challenges.

Mukhtaruzzaman et al (2020) have stated that number of vehicles are increasing, scalability will become an issue and due to absence of centralized structure, VANET faces packet loss as there is a high sharing. It also faces issues such as the hidden terminal problem, high latency for safety message transmission, message security, broadcast storm problem, quality of service (QoS), packet routing, congestion control, and resource management. To solve these issues, a clustering concepts are used here. Clustering concepts are used in MANET which is prototype VANET to cluster mobile nodes, is also used in machine learning and Data mining. Clustering plays an important role in Vehicular ad hoc network, here a group of vehicles form a group based on some common features. Here clustering techniques such as intelligence-based clustering algorithms, mobility-based algorithms, and multi-hop-based algorithms by means of a scrutiny on the mobility metrics, assessment criteria, challenges, and future directions of machine learning, fuzzy logic, mobility, NEMO, and multi-hop clustering algorithms and also hybrid algorithm is introduced where machine learning algorithm are integrated in fuzzy logic system to make the cluster formation process and CH selection process more efficient in a hybrid manner.

III. SOLUTION FRAMEWORK

In vehicular network, as the traffic management and navigation messages are disseminated periodically, these messages are vulnerable to a number of attacks from passive eavesdropping to active interfering. Vehicular networks are susceptible to variety of attacks such as denial of service (DoS) attack, Sybil attack and false alert generation attack. . Different cryptographic methods have been proposed to protect vehicular networks from these kind of attacks. However, cryptographic methods have been found to be less effective to protect from insider attacks which are generated within the vehicular network system. Misbehavior detection system (MDS) is found to be more effective to detect and prevent insider attacks.

However, MDS faces several challenges in the dynamic ad hoc or vehicular environment. The high dynamics of vehicular network topology affects network, routing and security. MDS should be able to identify various threats in such dynamically changing topology. MDS in vehicular communications are mainly categorized into three types: signature, specifications and anomaly detection system. Signature and specifications based system cannot identify a new type of attacks whereas the anomaly detection system can identify both known and unknown attacks. Thus, anomaly or machine learning-based MDS can give fast and efficient malicious node detection.

There are mainly three categories of architecture for MDS in vehicular networks. The first one is standalone MDS where each node collects data on its own using its local resources and apply misbehavior detection to detect anomaly. Each node has no information about the position of other nodes and make decision without any cooperation. The second one is cooperative and distributed MDS where different nodes cooperate with each other to detect an anomaly.

Here I choose machine learning based MDS to identify attackers and cooperative scheme is used for the fast eviction of misbehaving vehicles. As we further study Machine learning based misbehavior detection system it has false alert verification scheme, position falsification verification scheme and fast exclusion of misbehaving vehicles. Talking about false alert verification scheme, following diagram shows mechanism for misbehavior detection.

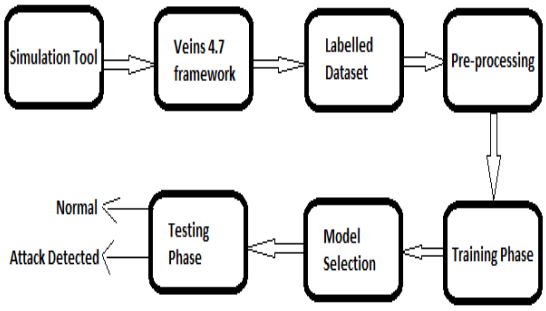

Figure 3.1 Misbehavior Detection Mechanism.

Here simulation of urban mobility model (SUMO) is to generate real world traffic, Veins 4.7 framework is used to make vehicular network simulations as realistic as possible. Veins is an open source framework and is based on two simulators: OMNET++ and SUMO. OMENT++ is an event based network simulator and SUMO is road traffic simulator for generation of mobility traces. For false alert analysis, Veins source code can be modified to model false alert attacker which broadcast false alert messages.

IV. CONCLUSION

Vehicular networks are vulnerable to variety of attacks such as denial of service (DoS) attack, Sybil attack and false alert generation attack. Misbehavior detection system (MDS) is found to be more effective to detect and prevent insider attacks. MDS identify attackers with the help of cooperative scheme which is used for the fast eviction of misbehaving vehicles. Machine learning based misbehavior detection system it has false alert verification scheme, position falsification verification scheme and fast exclusion of misbehaving vehicles.

REFERENCES

[1] Ayyappan B. and Kumar P. M., 2016, "Vehicular Ad Hoc Networks (VANET): Architectures, methodologies and design issues", *Second International Conference on Science Technology Engineering and Management (ICONSTEM), Chennai.*

[2] Bali R. S., Kumar N., Joel J.P.C. Rodrigues, 2015, "An efficient energy-aware predictive clustering approach for vehicular ad hoc networks", *International Journal of Communication Systems Published online in Wiley Online Library.*

[3] Balico L. N., Loureiro A. A. F., Nakamura E. F., Barreto R. S., Pazzi R. W., Oliveira H. A. B. F., 2018, "Localization Prediction in Vehicular Ad Hoc Networks," in *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2784-2803, Fourthquarter.

[4] Chang J. M., Lai C.F., Chao H.C., Zhu R., *2014*, "An energy-efficient geographic routing protocol design in vehicular ad-hoc network", *Computing Springer-Verlag Wien.*

[5] Deeksha, Ajay kumar and Bansal M., 2017, "A review of VANET security attacks and their Counter Measure", *4th International Conference on signal Processing, IEEE.*

[6] Eziama E., Tepe K., Ali Balador, Nwizege K. S., Luz Jaimes M. S., 2018, "Malicious Node Detection in Vehicular Ad-Hoc Network Using Machine Learning and Deep Learning", *IEEE global com workshop..*

[7] Jagnade G., Saudagar S., Chorey S., 2016, "Secure VANET from Vampire attack using LEACH protocol", *SCOPES IEEE Xplore.*

[8] Kaur R., 2018, "Security Issues in Vehicular Ad-hoc Network (VANET)", *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI).*

[9] Laroiya N., Lekhi S., 2017, "Energy Efficient Routing Protocols in Vanets", *Advances in Computational Sciences and Technology ISSN 0973-6107 Volume 10, Number 5 pp. 1371-1390 © Research India Publications.*

[10] Luo Y., Zhang W., Hu Y., 2010, "A New Cluster Based Routing Protocol for VANET", *Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, Wuhan, Hubei, pp. 176-180.

[11] Manivannan D., Moni S. S., Zeadally S., 2020, "Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc Networks (VANETs)", Vehicular Communications, Volume 25, 100247, ISSN 2214-2096.

[12] Meena G., Sharma D., *2020* , "Traffic Prediction for Intelligent Transportation System using Machine Learning", *3rd International Conference on Emerging Technologies in Computer Engineering: Machine Learning and Internet of Things (ICETCE), Jaipur, India, 2020, pp. 145-148.*

[13] Mehmood A., Khanan A., Mohamed A. H. H. M, Mahfooz S., Song H., Abdullah S., *2018,* "ANTSC: An Intelligent Naïve Bayesian Probabilistic Estimation Practice for Traffic Flow to Form Stable Clustering in VANET," *in IEEE Access, vol. 6, pp. 4452-4461.*

[14] Mohamed N., Mejri, Jalel Ben-Othman, Mohamed Hamdi, 2014, "Survey on VANET security challenges and possible cryptographic solutions", *Vhicular communication, volume1 issue 2, pages 53-66, ISSN 2214-2096.*

[15] Mukhtaruzzaman M., Atiquzzaman M., 2020, "Clustering in vehicular ad hoc network: Algorithms and challenges", *published by elsevier.*

[16] Patel N., Jhaveri R., 2015, "Trust based approaches for secure routing in VANET: A Survey", *Procedia Computer Science 45- 592 – 601.*

[17] Ray S., 2019, "A Quick Review of Machine Learning Algorithms", *International conference on machine Learning, Big data, Cloud and parallel Computing (COMITCon), Faridababd, India pp.35-39.*

[18] RosalineMarry M., Maheshwari M., Thamaraiselvan M., *2013*, "Early detection of DoS attack in VANET using Attacked Packet Detection Algorithm", *Internal conference on Information communication and embedded system.*

[19] Samara G., Al-Salihy W. A. H., Sures R., 2010, "Security Analysis of Vehicular Ad Hoc Nerworks (VANET)", *Second International Conference on Network Applications, Protocols and Services*, Kedah, 2010, pp. 55-60.

[20] Satheshkumar K., Mangai S., 2020, "EE-FMDRP: energy efficient-fast message distribution routing protocol for vehicular ad-hoc networks", *J Ambient Intell Human Comput*.

[21] Shamsa E.A., Rizanerb A., Ulusoyb A. H., 2018, "Trust Aware Support Vector Machine Intrusion Detection and Prevention System in Vehicular Ad hoc Networks", *published in Computers and security*..

[22] Singh A., Kumar M., Rishi R., Madan D.K., 2011," A Relative Study of MANET and VANET: Its Applications, Broadcasting Approaches and Challenging Issues", Communications in Computer and Information Science, volume 132. Springer, Berlin, Heidelberg.

[23] Sroka P., Kryszkiewicz P., Sybis M., 2020, "Radio Environment Maps for Dynamic Frequency Selection in V2X Communications", *IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, Antwerp, Belgium, pp. 1-5.

[24] Sroka P., Kryszkiewicz P., Sybis M., Kliks A., Gill K. S., Wyglinski A.,2020, "Distributed Vehicular Dynamic Spectrum Access for Platooning Environments," *IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, Antwerp, Belgium, pp. 1-5.

[25] Steven S., Sharma P., Petit J., 2018, "Integrating Plausibility Checks and Machine Learning for Misbehavior Detection in VANET", *17th IEEE International Conference on Machine Learning and ApplicationS*..

[26] Toutouh J., Nesmachnow S., Enrique Alba, *201, 3*"Fast energy-aware OLSR routing in VANETs by means of a parallel evolutionary algorithm", *Cluster Comput 16:435–450 DOI 10.1007/s10586-012-0208-9.*

[27] Yasser A., M. Zorkany & Neamat Abdel Kader, 2017, "VANET routing protocol for V2V implementation: A suitable solution for developing countries", Cogent Engineering, 4:1, 1362802.

[28] Zeng Y., Qiu M., Ming Z., Liu M., 2018, "A machine leaning based intrusion detection in VANET", *International conference on Smart computing Communication*..

[29] Zhang D., Liu X.H., Cui Y. Y., Chen L., Zhang T., 2010, "A kind of novel RSAR protocol for mobile vehicular Ad hoc network", *CCF Transactions on networking.*

[30] Zhang D., Richard F. Yu, Yang R., 2018, "A Machine Learning Approach for Software-defined Vehicular Ad Hoc Networks with Trust"., *IEEE global communication conference, IEEE Xplore digital library.*

[31] Zhao L., Li Y., Meng C., Gong C., Tang X., 2016, "A SVM based routing scheme in VANETs," *2016 16th International Symposium on Communications and Information Technologies (ISCIT)*, Qingdao, pp. 380-383.