BŞEÜ Fen Bilimleri Dergisi
9(2), 1160-1175, 2022

BSEU Journal of Science
https://doi.org/10.35193/bseufbd.1102897

e-ISSN: 2458-7575 (https://dergipark.org.tr/tr/pub/bseufbd)

Derleme Makalesi - Review Article

A Review on Machine Learning Techniques Used in VANET and FANET Networks

VANET ve FANET Ağlarda Kullanılan Makine Öğrenimi Teknikleri Üzerine İnceleme

Sumeyra Muti[1*], Eyüp Emre Ülkü[2]

Geliş / Received: 13/04/2022 ***Revize / Revised: 16/11/2022*** ***Kabul / Accepted: 16/11/2022***

ABSTRACT

The widespread use of the Internet and the increase in the number and variety of devices connected to the internet have led to the emergence of new methods in wireless communication. Dynamic and temporary Ad-Hoc networks, which do not require a fixed infrastructure as in traditional wireless network communication, are one of these new methods. The fact that Ad-Hoc networks do not need a fixed infrastructure has revealed a network structure with a lower cost and less configuration. Mobile Ad-Hoc networks play an important role, especially in the communication of nodes on the move. FANET (Flying Ad-Hoc Networks) networks, which are called flying ad hoc networks, are mobile Ad-Hoc networks used for communication of unmanned aerial vehicles (UAV), and VANET (Vehicular Ad-Hoc Networks) networks, which are called vehicular ad hoc networks, are mobile Ad-Hoc networks used for communication of road vehicles. The development and dissemination of these networks make a significant contribution to the development of autonomous vehicles and UAVs. The increase in the use of FANET and VANET networks, which are specialized subnets of mobile Ad-Hoc networks, and the increase in the number of nodes in these networks have caused problems related to security, efficiency, and sustainability in these networks. Machine learning methods, one of today' s effective and common approaches, are one of the ways that are frequently used in solving the problems specified in FANET and VANET networks. The rapid topology change, which is one of the most important features of these networks, makes it difficult to provide traffic management, trust management, routing, and data transmission. In this direction, machine learning approaches play an active role. In this study, it is presented by examining which machine learning techniques are used in the literature to perform important tasks such as traffic management, trust management, routing, and data transfer. Thus, it is aimed for those who will work in these fields to acquire information about machine learning approaches that can be used. Since the FANET network type is a new approach, it has been observed that there are few studies using machine learning. In VANET systems, studies using machine learning methods are especially intense in 2021. This study was carried out to give the reader an idea about which machine learning methods can be used in which problems in FANET and VANET networks.

Keywords- Ad Hoc, Wireless Communication, VANET, FANET, Machine Learning

[1*]Corresponding Author Contact: sumeyramuti@marun.edu.tr (https://orcid.org/0000-0001-6489-0258)
Institute of Pure and Applied Sciences Department of Computer Engineering, Marmara University, Istanbul, Turkey
[2] Contact: emre.ulku@marmara.edu.tr (https://orcid.org/0000-0002-1985-6461)
Faculty of Technology Department of Computer Engineering, Marmara University, Istanbul, Turkey

ÖZ

İnternetin yaygınlaşması ve internete bağlı cihaz sayısı ve çeşitliliğinin artması kablosuz iletişimde yeni yöntemlerin ortaya çıkmasını sağlamıştır. Geleneksel kablosuz ağ iletişiminde olduğu gibi sabit bir alt yapı gereksinimi olmayan dinamik ve geçici Ad-Hoc ağlar bu yeni yöntemlerden bir tanesidir. Ad-Hoc ağların sabit bir altyapıya ihtiyaç duymamaları daha düşük maliyetli ve daha az konfigürasyona ihtiyaç duyan bir ağ yapısını ortaya koymuştur. Özellikle hareket halindeki düğümlerin haberleşmesinde mobil Ad-Hoc ağlar önemli rol oynamaktadır. Uçan tasarsız ağlar olarak adlandırılan FANET (Flying Ad-Hoc Networks) ağlar insansız hava araçlarının (İHA) haberleşmesini, araçsal tasarsız ağlar olarak adlandırılan VANET (Vehicular Ad-Hoc Networks) ağlar ise karayolu araçlarının haberleşmesini sağlamada kullanılan mobil Ad-Hoc ağlardır. Bu ağların gelişimi ve yaygınlaşması otonom araçların ve İHA' ların gelişimine önemli katkı sağlamaktadır. Mobil Ad-Hoc ağların özelleşmiş alt ağları olan FANET ve VANET ağlarının kullanımının artması ve bu ağlar içerisinde yer alan düğüm sayılarındaki artış bu ağlarda güvenlik, verimlilik ve sürdürülebilirlik ile ilgili problemlerin ortaya çıkmasına neden olmuştur. Günümüzün etkin ve yaygın yaklaşımlarından biri olan makine öğrenmesi yöntemleri FANET ve VANET ağlarda belirtilen problemlerin çözümünde sıklıkla başvurulan yollardan bir tanesidir. Bu ağların en önemli özelliklerinin başında gelen hızlı topoloji değişimi trafik yönetiminin, güven yönetiminin, yönlendirmelerin ve veri iletiminin sağlanmasını zorlaştırmaktadır. Bu doğrultuda makine öğrenmesi yaklaşımları etkin rol oynamaktadır. Bu çalışmada, literatürde trafik yönetimi, güven yönetimi, yönlendirme ve veri transferi gibi önemli görevleri gerçekleştirmede hangi makine öğrenmesi tekniklerinin kullanıldığı incelenerek sunulmuştur. Böylelikle bu alanlarda çalışacakların kullanılabilecek makine öğrenimi yaklaşımları ile ilgili bilgileri edinmeleri hedeflenmiştir. FANET ağ türünün yeni bir yaklaşım olması nedeniyle makine öğrenimi yaklaşımlarının kullanıldığı az sayıda çalışma olduğu gözlemlenmiştir. VANET sistemlerde ise makine öğrenmesi yöntemlerinin kullanıldığı çalışmalar özellikle 2021 yılında yoğunluk göstermektedir. Bu çalışma, FANET ve VANET ağlarda hangi problemlerde hangi makine öğrenmesi yöntemlerinin kullanılabileceği hakkında okuyucuya fikir vermek amacıyla gerçekleştirilmiştir.

Anahtar Kelimeler- Tasarsız Ağlar, Kablosuz Haberleşme, VANET, FANET, Makine Öğrenmesi

I. INTRODUCTION

In wireless networks, there are two basic approaches to providing wireless connectivity between hosts. The first of these is based on an established cellular network infrastructure. The first approach is the network structure, which requires an infrastructure such as a base station. An example of this approach is cellular network infrastructure. Cellular network structure is one of the most important examples of this type of wireless networks. The second approach is ad hoc networks, which is an arbitrary and temporary network structure that does not need infrastructure support, that we also examine in this study. We will present a literature review about Machine Learning (ML) algorithms used in Vehicular Ad-Hoc Networks (VANET), which is a specialized sub-branch for vehicles, of networks that provides communication between mobile nodes, defined as MANET and Flying Ad-Hoc Networks (FANET), which is another specialized sub-branch for Unmanned Aerial Vehicles (UAV) of MANET [1].

The most important feature of Ad-Hoc networks is that they do not need an infrastructure support such as a base station. Thus, nodes that need to communicate with each other can have a low cost and fast communication network. In recent years, technological developments in autonomous vehicles, the concept of the Internet of Things (IoT), and unmanned aerial vehicles (UAVs) have increasingly given importance to ad hoc networks. In this direction, vehicles that need to communicate with each other have led to the emergence of VANET networks, and UAVs to FANET networks. Both of these networks are a specialized type of mobile ad-hoc networks. The widespread use of these networks and the increase in the number of nodes in these networks have caused various problems. Routing, traffic management, data transmission are among these problems. The rapid topology change experienced by the movement of many nodes in these networks has accelerated the search for faster and more efficient solutions, especially in routing and data transmission. In recent years, machine learning algorithms have also been used in VANET and FANET networks to perform tasks such as routing, data transmission, trust management and traffic management more efficiently and faster. In this study, studies in the literature using machine learning approach in VANET and FANET networks were examined. While examining these studies, it is presented which machine learning approaches are used while performing which task in VANET and FANET networks.

VANETs used in road vehicles consist of three components: Application Unit (AU), On-Board Unit (OBU) and Roadside Unit (RSU). OBU are wireless structure that are usually mounted on the vehicle and enable the vehicle to communicate with another vehicle or RSU. AU is the in-vehicle structure that provides applications with the information it receives through the OBU. RSUs are on-road units that provide various status information or internet access to vehicles that are in communication with the vehicles' OBUs [2]. Rapid advances in autonomous vehicles, 5G and IoT technologies increase the need for a large number of nodes to communicate with each other quickly. Each concept such as traffic light, traffic sign, vehicle, parking lot becomes a separate node. In this case, it makes it very important for these nodes to establish a temporary connection with each other. Therefore, operations such as routing, trust management and traffic management within VANET networks require much more efficient and faster execution.

FANETs, on the other hand, are vehicle ad hoc networks that allow unmanned aerial vehicles (UAVs) to communicate with each other in real time. Location information sharing (LIS) in FANETs allows a large number of UAVs to be aware of each other and thus to make a safe flight [3-4]. In recent years, there are many tasks where UAVs are used, especially in military applications. In addition, UAVs are also used in various civil applications such as post-disaster aid and communication [5].

Machine learning methods are used to solve various problems in VANET and FANET systems. Machine learning methods especially in VANET systems are used in routing algorithms for a safe, fast and efficient data transfer, in intrusion detection systems (IDS) to prevent attacks such as DoS (Denial of Service Attack), DDoS (Distributed Denial of Service Attack), Sybil, blackhole and fake location information, in various clustering problems, traffic control applications.

In this study, it is aimed to inform the reader about which machine learning methods can produce more successful results in solving which problems in studies carried out after 2019. We have gathered the studies in which machine learning methods are used to solve some basic problems for VANET and FANET systems under five main headings as “Trust Management”, studies in which machine learning is used to prevent attacks that threaten VANET and FANET networks, “Routing Algorithms”, “Data Transmission”, “Traffic Management” and “Other”.

In Section II, we will explain which databases we used for our research, our search method, and how we included the results we found in our research. In Section III, we will analyze the studies we have selected for review. In Section IV, we will share information about what the machine learning methods used in these studies are, which problem they are used to solve, and what results have been achieved.

II. METHODS

We obtained the studies that we will examine in this article by using the query expressions we determined through the Scopus, IEEE and Science Direct databases, which are among the most popular and frequently used databases. We then rearranged our results according to our inclusion and exclusion criteria to determine whether they were appropriate for our study. Our inclusion criteria are that the studies are related to VANET or FANET concepts, developed using machine learning algorithms, written language is English and published after 2019. Studies in which the full text cannot be reached, do not match the research title, and where machine learning techniques are not applied to VANET or FANET networks are excluded. These inclusion and exclusion criteria are presented below. Due to the rapid change of currency in computer science, we have included studies done after 2019 in order to address more current studies within the study.

Inclusion;

- Studies must have keywords belonging to machine learning algorithms.
- Studies must be related to VANET or FANET.
- The language of writing must be English.
- Studies must be 2019 and later publications.

Exclusion;

- The full text of the studies could not be reached
- Studies do not suitable for our research topic
- Studies do not provide experimental data.
- Used machine learning methods in studies have not been applied in VANET or FANET.

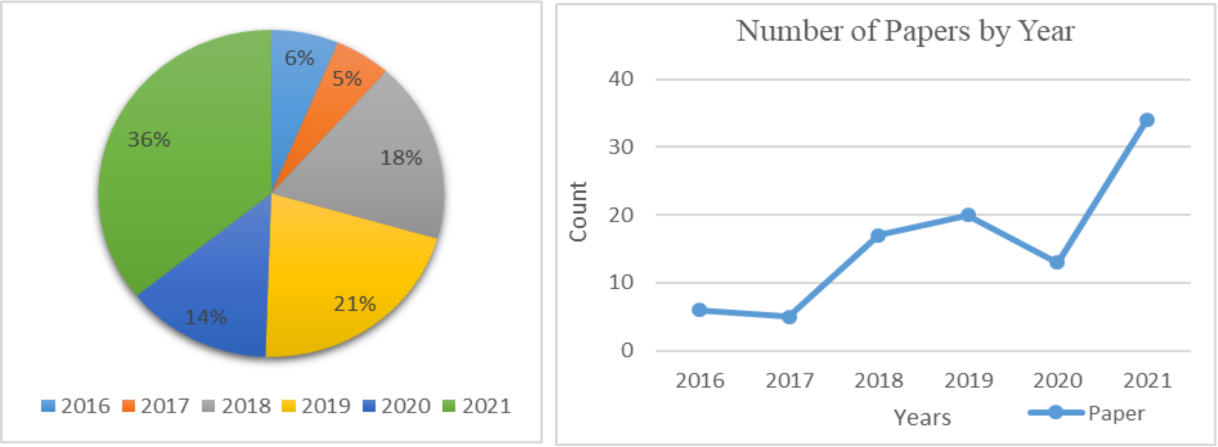
With the search queries listed in Table 1, we reached a total of 242 results for VANET and 15 results for FANET in IEEE and Scopus. Since we found very few results related to FANET, we additionally searched the ScienceDirect database and found 85 results. However, we found that the majority of these results were either related to only ML or only to FANET, and we eliminated irrelevant studies. When we eliminated those results that were not suitable for our study, there were 5 studies left to be examined and we have shown this value as the result in Table 1.

Table 1. Search queries and results

Subject	Database	Search Query	Results
VANET	IEEE	("All Metadata":machine learning) AND ("All Metadata":vanet)	129
	Scopus	TITLE-ABS-KEY(Machine Learning Algorithms Vanet)	113
FANET	IEEE	("All Metadata":FANET) AND ("All Metadata":machine learning)	8
	Scopus	TITLE-ABS-KEY (machine AND learning AND fanet)	7
	ScienceDirect	Fanet, Machine Learning	5

We examined whether the studies we obtained had at least one of the keywords including “Machine Learning (ML)”, Deep Learning (DL)”, “Support Vector Machine(SVM)”, “Neural Network (NN)”, “Reinforcement Learning (RL)”, “K-Nearest neighbor (KNN)”, “Q-learning”, “Artificial Neural Networks (ANN)”, “Convolutional Neural Networks (CNN)”, “Bayesian model”, “Naive Bayes (NB)”, “Random Forrest (RF)”, “Decision Tree (DT)” and removed those that did not have any of these keywords from our research area. Then, we eliminated the duplicate studies in different databases. Finally, after performing another elimination process according to our inclusion and exclusion criteria, we selected 37 studies for VANET and 5 studies for FANET for detailed review.

In Figure 1, the graphs of the distribution of the studies we obtained as a result of the search queries by years are given. In the graphs in Figure 1, only the distribution of studies on VANET by years is given, and it is observed that the number of researches in this field has increased significantly with more than 30 studies in 2021.



a) Percentage distribution of papers by years

b) Variation in the total number of papers by years

Figure 1. Using ML for VANET by years

As can be seen from the pie chart, 36% of the studies made since 2016 belong to 2021. These data show that there has been a significant increase trend in studies using machine learning approaches in VANET networks in recent years.

A density map of which countries the studies we examined belong to is given in Figure 2. The size of the blue dots indicating the studies on the VANET shows the density in that region. Studies on FANET are shown in red and density is indicated by color darkness. Table 2 presents the numerical distribution of the studies we examined by country. In the studies we examined, India was the country with the highest number of publications with nine articles. It is followed by China and the USA with five articles each.

Table 2. Number of studies reviewed by country

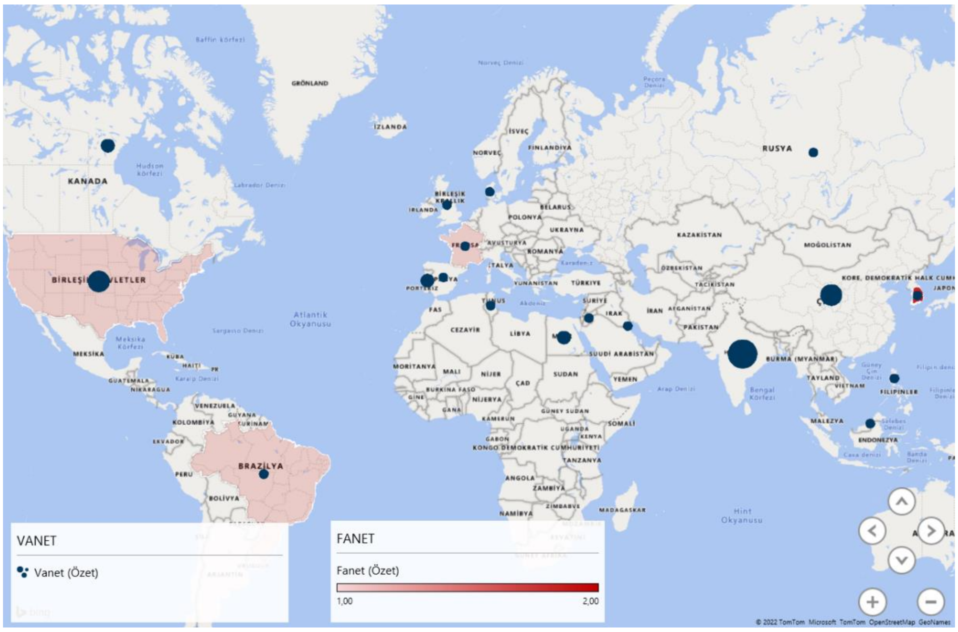


Figure 2. Distribution of reviewed studies by country

Country	VANET	FANET
America	5	1
Brazil	1	1
China	5	
Denmark	1	
Philippines	1	
France	1	1
South Korea	1	2
India	9	
Spain	1	
Canada	2	
Kuwait	1	
Malaysia	1	
Egypt	2	
Portugal	2	
Russia	1	
Tunisia	1	
Jordan	1	
United Kingdom	1	

III. MACHINE LEARNING METHODS USED IN VANET AND FANET

As a result of the examinations, while there are many studies on VANET, the number of studies on FANET is very few. In the studies reviewed, the use of machine learning methods in trust management in order to protect VANETs against attacks has been the subject of more research than other subjects. As in many areas of computer science, security is one of the most important problems in ad-hoc networks. It has been seen that machine learning approaches are a frequently used way in recent years against network attacks that may come from outside in VANET and FANET networks. The most commonly used ML methods in studies on VANET and FANET networks are SVM, kNN, RF methods. A general table of all the studies examined is given in Table 3, and sub-tables related to the subject are given in each subject heading.

Table 3. Studies examined according to their subjects and machine learning methods used

Source	Year	ML method	Subject	Country	FANET/VANET
[6]	2021	SVM	Routing	China	VANET
[7]	2021	Q-learning	Routing	Brazil	FANET
[8]	2021	SVM, k-NN	Trust Management	Amerika	VANET
[9]	2021	Q-learning	Routing	South Korea	FANET
[10]	2021	SVM, KNN	Trust Management	India	VANET
[11]	2021	SVM	Traffic Management	China	VANET
[12]	2021	KNN, RF, NB, DT	Trust Management	Canada	VANET
[13]	2021	RF	Trust Management	France	FANET
[14]	2021	FSVM, krill herd	Trust Management	India	VANET
[15]	2021	ML	Trust Management	Portugal	VANET
[16]	2021	ANN	Routing	Spain	VANET
[17]	2021	RF	Trust Management	India	VANET
[18]	2021	DL	Routing	India	VANET
[19]	2021	ML	Trust Management	Egypt	VANET
[20]	2021	ML	Traffic Management	Kuwait	VANET
[21]	2021	SVM	Trust Management	Jordan	VANET
[22]	2021	Federate ML	Trust Management	USA	VANET
[23]	2021	RF, kNN	Trust Management	France	VANET
[24]	2021	SVM	Trust Management	Philippines	VANET
[25]	2021	DT, LR, GNB, RF	Routing	South Korea	VANET
[26]	2021	kNN, RF, SVM	Trust Management	Russia	VANET
[27]	2021	DML	Trust Management	India	VANET
[28]	2021	RF	Trust Management	Denmark	VANET
[29]	2021	NN	Data Transmission	USA	VANET
[30]	2021	ANN	Trust Management	Portugal	VANET
[31]	2021	Bayes	Data Transmission	Malaysia	VANET
[32]	2021	Fuzzy Logic	Routing	South Korea	FANET
[33]	2021	Federate ML	Other	Amerika	FANET
[34]	2020	ELM	Trust Management	Brazil	VANET
[35]	2020	SVM, KNN, RF	Trust Management	Tunisia	VANET
[36]	2020	SVM	Data Transmission	China	VANET

Table 4. *(Continues)*

Source	Year	ML method	Subject	Country	FANET/VANET
[37]	2020	SVM Kernel	Trust Management	India	VANET
[38]	2020	DL	Data Transmission	USA	VANET
[39]	2020	RF, SVM	Traffic Management	India	VANET
[40]	2019	ML	Trust Management	Amerika	VANET
[41]	2019	Q-learning	Data Transmission	UK	VANET
[42]	2019	RF, AdaBoost	Traffic Management	India	VANET
[43]	2019	CNN	Traffic Management	China	VANET
[44]	2019	O-PNN	Traffic Management	Canada	VANET
[45]	2019	DRL	Other	China	VANET
[46]	2019	RF	Other	India	VANET
[47]	2019	OS-ELM	Traffic Management	Egypt	VANET

A. Trust Management

The rapid change of topology in VANET networks also complicates the implementation of security mechanisms. In this case, it causes various security vulnerabilities to occur in these networks. Cryptology techniques, which are one of the most frequently used ways to ensure security, are also used in this type of networks. However, the use of cryptology techniques sometimes requires significant processing power. Sometimes processing power can be a significant constraint for nodes in VANET networks. Against this limitation, an extra layer of security can be created with intrusion detection systems (IDS) [15]. Apart from these methods, there are ML-based approaches developed to ensure trust management and prevent various attacks in VANET networks. These approaches are presented under this title. ML-based solutions developed to provide a solution to the trust management problem are examined and presented in Table 4. Especially in VANET networks, SVM, RF and KNN are the most commonly used machine learning methods to ensure trust management and make the network more secure.

H. Mankodiya et al. aimed to detect defective data by using ML algorithms (RF, DT, Adaboost) in data transmission within the scope of trust management. Decision tree-based algorithms were used to classify offensive AVs (autonomous vehicles) that sent false or malicious information, and the RF algorithm performed better in the test set. As a result, 98.5% accuracy score was obtained in the VeRiMi dataset [17].

Table 5. Studies examined for trust management

Source	Year	ML method	Subject	Country	FANET/VANET
[8]	2021	SVM, k-NN	Trust Management	Amerika	VANET
[10]	2021	SVM, KNN	Trust Management	India	VANET
[12]	2021	KNN, RF, NB, DT	Trust Management	Canada	VANET
[13]	2021	RF	Trust Management	France	FANET
[14]	2021	FSVM, krill herd	Trust Management	India	VANET
[15]	2021	ML	Trust Management	Portugal	VANET
[17]	2021	RF	Trust Management	India	VANET
[19]	2021	ML	Trust Management	Egypt	VANET
[21]	2021	SVM	Trust Management	Jordan	VANET
[22]	2021	Federate ML	Trust Management	USA	VANET
[23]	2021	RF, kNN	Trust Management	France	VANET
[24]	2021	SVM	Trust Management	Philippines	VANET
[26]	2021	kNN, RF, SVM	Trust Management	Russia	VANET
[27]	2021	DML	Trust Management	India	VANET
[28]	2021	RF	Trust Management	Denmark	VANET
[30]	2021	ANN	Trust Management	Portugal	VANET
[34]	2020	ELM	Trust Management	Brazil	VANET
[35]	2020	SVM, KNN, RF	Trust Management	Tunisia	VANET
[37]	2020	SVM Kernel	Trust Management	India	VANET
[40]	2019	ML	Trust Management	Amerika	VANET

A. R. GAD et al. used machine learning methods such as RF, DT, kNN, SVM, XGBoost on the network data of the ToN-IoT data set for attack detection and observed that the XGBoost algorithm gave the most successful results in binary and multiple classification problems. In addition, the effects on the success of the system of using Chi2 and SMOTE pre-processing techniques separately and together were compared [19].

SVM, which is one of the algorithms that gives successful results in predictive applications, is used in studies within the scope of trust management. A. Alsarhan et al. examined the optimization of three different ML algorithms, Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), on SVM to classify attacks in the NSL-KDD dataset and found that GA was more successful than the others [21]. In another study, J. D. Cabelin et al. designed an SVM-based IDS to detect false data injection (FDI) attack. The data set obtained from a one-way four-lane highway simulation using MATLAB and NS-3 was tested in the SVM-based IDS model and it was concluded that it has high accuracy in detecting malicious information. The system has also been shown to reduce traffic congestion by reducing malicious packets [24].

I. Bolodurina et al. examined the efficiency of various ML algorithms in identifying new features to increase the efficiency of ML methods used in intrusion detection applications in VANETs. As a result, it was seen that most ML methods increased the accuracy by an average of 0.137%, while the RF method was found to decrease the efficiency by 0.53% [26].

G. Raja et al. propose a secure and private collaborative intrusion detection system (SP-CIDS) using distributed machine learning (DML) that leverages the potential of V2V (Vehicle to Vehicle) collaboration in the learning process to improve the accuracy, storage efficiency, and scalability of IDS. The model is evaluated with LR, NB, and ensemble classifiers, and as a result, 96.94% accuracy is obtained with the training data secured with differential privacy [27].

It is important to effectively evaluate the information received from VANETs in IDS systems. F. Gonçalves et al. evaluated the effects of publicly available VANET data on IDS systems at four different levels: vehicle, RSU, cluster, and all using the ANN method [30].

Drones can face various attacks from within the network and from outside. C. Guerber et al. propose an SDN solution for external threats and an RF classifier-based ML solution for intra-network attacks. As a result, they observed that the proposed system was successful in detecting abnormal behavior [13].

New methods using machine learning are introduced to detect some specific types of attacks encountered in VANETs. M. T. Garip et al. presented SHIELDNET, in which they use ML algorithms for the detection of a vehicle botnet communication protocol called GHOST, which endanger traffic safety in VANETs. According to the simulation results, they showed that the proposed framework correctly identified 77% of the bots [40].

We have classified the studies on the prevention of DoS, DDoS, Sybil, blackhole attacks and location spoofing, which are some types of attacks frequently encountered in VANETs, under separate headings.

1) DoS and DDOS Attacks:

Distributed denial-of-service (DDoS) attacks are known as attacks where several tools perform various denial-of-service (DoS) attacks to disrupt the normal functioning of the network in VANETs. Detection and prevention of DDoS attacks in VANET is very important because these attacks endanger human life. There are various studies carried out for this purpose.

In the work of Gonçalves et al., a four-stage hierarchical intrusion detection system using a different ML method at each stage is proposed with the data obtained using Simulation of Urban Mobility (SUMO) and Network Simulator (ns-3). According to the results obtained, it was observed that it was successful in detecting DoS and non-attack messages, but the performance decreased in detecting other attack types [15].

D. C. Ananth et al. proposed the FLC-OFSVM model, which provides an efficient fuzzy logic-based clustering with optimal fuzzy support vector machine to ensure security and communicate effectively. This model consists of two processes as intrusion detection and clustering in VANETs. FLC was used to select the appropriate cluster head, and an optimized FSVM with the krill herd algorithm was used for the IDS stage. The effectiveness of OFSVM was tested in the NSL-KDD 2015 dataset and it was seen that the proposed model gave successful results [14].

Another study for the detection of DDoS attacks proposes the KSVM model as a hybrid model based on KNN and SVM algorithms. Compared to SVM, KNN, DT, ANN, this model has the highest accuracy and sensitivity values, as well as the lowest error rate [10].

M. Zang and Y. Yan proposed an IDS framework in which anomalous flows are labeled with an RF classifier using real data in the Mininet-Wifi emulator. The results showed that the model's prediction accuracy in DoS/DDoS attacks was high and the false positive rate was low [28].

Adhikary et al. presented a hybrid detection algorithm based on SVM kernel methods to detect DDoS attacks in VANETs. The performance of the model based on the proposed hybrid algorithm is compared with the models based on SVM kernel algorithms. Experimental results have shown that the proposed hybrid algorithm-based model is more successful in detecting DDoS attacks compared to single SVM core algorithms. The results also proved that an efficient and effective hybrid algorithm can be developed by combining SVM kernel algorithms [37].

2) Black Hole Attacks:

In the studies of A. Acharya and J. Oluoch developed a model in which logistic regression, k-NN, Gaussian Naive Bayes, SVM, Gradient Boost methods are applied to prevent blackhole attacks, which are an example of DDoS attacks. The ROC AUC performance score was found to be an average of 96.78% for these five methods [8].

3) Sybil Attacks:

In their work, A. Haddaji et al. proposed a Blockchain Multi Levels Trust mechanism against Sybil Attacks (BMLT-SA) to prevent Sybil attacks that threaten the security of VANET by creating multiple false identities. In their study, they used SVM, kNN and RF algorithms to classify malicious and normal nodes. Simulation results show that the proposed method is successful in detecting Sybil attacks [35].

Quevedo et al. proposed a structure called SyDVELM, which uses the Extreme Learning Machine (ELM) method to prevent Sybil attacks. The results showed that this new proposed model has a high detection rate with very low error rates and provides a scalable detection system [34].

4) Location Spoofing

Another problem related to VANET is location spoofing. Incorrect delivery of vehicle location information to other vehicles may cause accidents. In their studies, A. Sharma and A. Jaekel tested k-NN, Random Forest, Naive Bayes and Decision Tree algorithms to detect such attacks and it was seen that the best results were k-NN and Random Forest algorithms [12].

In the study of A. Uprety et al., it is aimed to prevent location spoofing in VANETs by using Federated ML on VeReMi dataset. At the same time, in this study, central education and federated education were compared and it was observed that federated education gave acceptable results [22].

S. Ercan et al., a study was conducted to determine whether a vehicle exhibits misbehavior by using kNN and RF algorithms in the VeReMi dataset. As a result, it was seen that the proposed approach increased the misbehavior detection performance [23].

B. Data Transmission

Factors such as the dynamic nature of VANET networks, fast topology change, bandwidth and spectrum constraints are the reasons for the difficulties encountered in data transmission. Creating clustering algorithms plays an important role to ensure secure and fast data transmission. In this direction, ML-based approaches used in VANET networks in order to provide a safer and faster data transmission are presented in Table 5.

Table 6. Studies examined for data transmission

Source	Year	ML method	Subject	Country	FANET/VANET
[29]	2021	NN	Data Transmission	USA	VANET
[31]	2021	Bayes	Data Transmission	Malaysia	VANET
[36]	2020	SVM	Data Transmission	China	VANET
[38]	2020	DL	Data Transmission	USA	VANET
[41]	2019	Q-learning	Data Transmission	UK	VANET

In their work, M. A. Hossain et al. introduced a hybrid segment-based CR-VANET (Seg-CR-VANET) architecture that combines fuzzy logic and Bayesian algorithms to solve the spectrum scarcity problem and offer a better data transmission. As a result, when compared to previous studies, it has been seen that the proposed model gives successful results with better spectrum detection, better packet delivery ratio (PDR), higher accuracy, lower packet loss and lower delays [31].

There are studies in which ML methods are used to develop an efficient clustering algorithm for solving the problems caused by the dynamic structures of VANETs in the communication between vehicles. S. Chavhan et al. proposed a self-learning hybrid clustering approach with adaptive network fuzzy inference system (ANFIS) for cluster head (CH) prediction and update. After the CH update, Djkstra's algorithm is used to group the cluster members. As a result, it was seen that the proposed algorithm gave successful results in terms of PDR, end-to-end delay, CH selection delay [29].

X. Liu proposed a QoS scheme using DL to optimally distribute a restricted spectrum band to users in Marine-VANETs [38].

T. Koshimizu et al. developed a new model for clustering problems in VANETs, which they named Normalized Multidimensional Proximity Distribution Clustering (NMDP-APC). In this study, SVM-based ML was used to determine the desired clustering size and range. The simulation results have proven that the system performs successfully with less access delay in the Public Land Mobile Network (PLMN) system [36].

A. Pressas et al. presented the Q-Learning-based MAC protocol for efficient data communication between VANETs. With this study, they have presented a self-learning structure to ensure that the stations use the bandwidth in the most appropriate way. As a result, they achieved short-term accuracy, high efficiency and faster convergence [41].

C. Traffic Management

Traffic flow information in VANETs can be useful in guiding drivers. In recent years, studies have been carried out on the use of big data applications in subjects such as intelligent traffic control and management. Table 6 shows a sub-table of the studies examined within the scope of traffic management and, SVM and RF are the most used methods.

Table 7. Studies examined for traffic management

Source	Year	ML method	Subject	Country	FANET/VANET
[11]	2021	SVM	Traffic Management	China	VANET
[20]	2021	ML	Traffic Management	Kuwait	VANET
[39]	2020	RF, SVM	Traffic Management	India	VANET
[42]	2019	RF, AdaBoost	Traffic Management	India	VANET
[43]	2019	CNN	Traffic Management	China	VANET
[44]	2019	O-PNN	Traffic Management	Canada	VANET
[47]	2019	OS-ELM	Traffic Management	Egypt	VANET

J. Tong et al. proposed a new SVR model developed by applying particle swarm optimization to the parameter optimization of SVR for traffic flow prediction. When this model is applied to real traffic flow data in the UK, it has been found that the developed model is more successful than the existing models. This new method, applied to real traffic flow data in England, gives more successful prediction results than grid search method and decision tree regression [11].

Accurately determining the location of vehicles is critical in road safety applications used to prevent traffic accidents. For this purpose, A. Ashtaiwi proposed the Localization and Driving Direction Estimation System LDDES, which is a prediction system using Multiple Input Multiple Output (MIMO) and ML, indicating the position and driving direction of other vehicles in the vicinity. When LDDES is tested on two vehicles with different antenna characteristics, it has been observed that it can detect the driving direction of other vehicles with an accuracy close to 90% [20].

In another road estimation application, some ml methods that predict whether autonomous vehicles will go right, left or straight are compared. Mamatha G. et al. examined the prediction success of ML algorithms such as RF and SVM for route selection in autonomous vehicles and showed that SVM gave more successful results for prediction [42].

One of the difficulties encountered in VANETs is to achieve an effective clustering in urban areas with many intersections. G. H. Alsuhli et al. proposed an OS-ELM machine learning-based CANI (Clustering Adaptation Near Intersection) model that can perform fast and continuous learning to maintain clustering stability at intersections. They concluded that this developed model is successful in terms of stability and efficiency performance [47]. In another study, S.J. Kamble and M.R. Kounte presents a route estimation application based on RF and AdaBoost algorithms that determines which direction VANETs will take at intersections. In this study, firstly, vehicle trajectory data is collected from the GPS sensors of the vehicles, and then vehicles with similar deviation angles are clustered and a route planner is presented route planner that gives the shortest route to other vehicles [42].

VANETs allow the use of various applications in vehicles by connecting to the internet via RSUs. However, due to their high mobility, their connection with RSUs may be interrupted, which may cause some services to be disrupted. N. Aljeri and A. Boukerche used the PNN model to increase the performance of the next RSU prediction in order to ensure the continuity of mobile connections in the vehicles. They concluded that the method, which was compared with Network Simulator NS-2 and various classifiers, was successful in terms of time complexity and accuracy. In the focus of this study, a new hybrid model can be created by combining the advantages of different machine learning methods [44].

Another study on traffic management is about determining the probability of a traffic accident with machine learning methods. H. Zhao et al. proposed the CNN algorithm as a solution to the disadvantage that traditional machine learning methods used for traffic accident prediction cannot automatically extract the features of the data. When the traditional back propagation neural network (BPNN) and CNN methods applied on the data collected from VANETs are compared, it is seen that the CNN method gives a lower training loss value. As a result, they observed that the proposed CNN-based traffic accident prediction algorithm has lower loss and higher prediction values than traditional ML methods [43].

D. Routing

VANETs; It can offer security, internet access, various applications for passengers and users. Therefore, it is important to make data transmission between vehicles more efficient and reliable [48]. For this purpose, there are studies on ML-based routing algorithms. The sub-table of the studies examined within the scope of the routing is given in Table 7. Various machine learning methods have been used in this area, and most of the work belongs to South Korea. In addition, most of the studies on FANET are within the scope of this subject.

Table 8. Studies examined for routing

Source	Year	ML method	Subject	Country	FANET/VANET
[6]	2021	SVM	Routing	China	VANET
[7]	2021	Q-learning	Routing	Brazil	FANET
[9]	2021	Q-learning	Routing	South Korea	FANET
[16]	2021	ANN	Routing	Spain	VANET
[18]	2021	DL	Routing	India	VANET
[25]	2021	DT, LR, GNB, RF	Routing	South Korea	VANET
[32]	2021	Fuzzy Logic	Routing	South Korea	FANET

In their work, S. Zhang et al. present a new approach to improve vehicle network performance and data transmission security. In this study, big data analysis was made with the help of location-based routing protocols and SVM algorithms in VANETs using 5g technology, so that the data can be transmitted securely by accurately detecting non-line of sight (NLoS) conditions. The results showed that the accuracy of the data increased by 15% for highways, 8% for suburban areas and 4.5% for urban areas [6].

Due to the high mobility of FANETs nodes, maintaining acceptable network latency remains a significant challenge. R. Kunst et al. address this issue by proposing a routing scheme based on a Q-Learning algorithm developed to reduce network latency in high-mobility scenarios called Q-FANET. The performance of this proposal has been evaluated and compared to other state-of-the-art methods using the WSNET simulator. Experiments provide evidence that Q-FANET offers lower latency, a small increase in packet delivery rate, and significantly lower jitter compared to other reinforcement learning-based routing protocols [7].

L. L. Cárdenas et al. developed a new routing protocol based on multi-metric prediction based artificial neural network (MPANN). Five different routing metrics taken from a large number of urban scenarios were recorded and different ML algorithms were tried and it was seen that the best result was ANN-based routing algorithm. To measure the flexibility and adaptability of the MPANN model, tests were conducted in regions with different city maps and vehicle densities. Compared to previous multi-metric routing protocols, an improvement of 20% in packet losses and up to 60% in average end-to-end packet delay has been observed [16].

J. Nadarajan and J. Kaliyaperumal proposed a new routing method called SCARP (stochastic chaos-based predictive adaptive routing) in their work. It is said that this method, which has a strengthened LSTM algorithm, has high predictive ability and chooses the most appropriate routing path according to traffic flow information. The experiments performed on SUMO-OMNET with the data of Indian roads were compared with the existing routing algorithms and it was found to be successful in terms of prediction accuracy, sensitivity average delay and PDR [18].

In their study, G. Raja et al. designed a DT predictive compliance-based Vehicular Ad-Hoc reliable (DT-VAR) routing protocol using SUMO simulation. Four ML algorithms, DT, GNB, RFC, and LR, were used to estimate the best message routing with the highest connection time. Short cuts selected in the existing schemes gave a PDR of 4%, while the proposed DT-VAR protocol achieved a PDR value of up to 16% [25].

In their study, S. Ali et al. presented a routing scheme in FANETs consisting of two phases: energy sensitive and predictive fuzzy logic based route discovery phase and route maintenance phase. In the route selection stage, a fuzzy logic-based system was applied for a more suitable route for data transfer. When the proposed model is compared with three different routing methods, it has been observed that it is more successful in terms of delay rate in data transmission [32].

In their study, M. Y. Arafat and S. Moh proposed a Q-Learning-based topology-aware routing (QTAR) protocol that can adapt to the dynamic nature of FANETs. Re-adjustment of the Q-Learning method according to the changes in the topology produces successful results as it adapts to the dynamic structure of FANET [9].

F. Others

Studies outside of the four main titles mentioned before are gathered under this title.

Table 9. Others articles

Source	Year	ML method	Subject	Country	FANET/VANET
[33]	2021	Federate ML	Other	Amerika	FANET
[45]	2019	DRL	Other	China	VANET
[46]	2019	RF	Other	India	VANET

In their study, J. Yu et al. proposed an energy sensitive dynamic computation offload scheme that evenly distributes energy consumption and also allows for parallel execution of tasks. In the study, Kernel-Ridge Regression, Gaussian-Process Regression, RF and SVR-RBF machine learning methods were used to estimate the resource processing time in video processing tasks. It was observed that the Kernel-Ridge Regression model gave the best performance in transmission time results, while SVR-RBF algorithms were the best model in processing time results [33].

In their study, J. Li et al. propose a DRL-based maximization matching algorithm for VANETs to dynamically collect data from RSUs and reduce resource waste. According to the experimental results, they concluded that the proposed algorithm is more successful than the traditional methods [45].

There are also studies in which ML methods are applied in determining driver behavior profiles. In their study, R. Das and P.M Khilar examined the data collected from OBUs for the success of three different RF algorithms in classifying the driver behavior profile [46].

IV. CONCLUSIONS

Machine learning techniques have been widely used in many different fields recently. In Ad-Hoc networks which is one of these areas, new ideas are put forward to solve various problems with ML methods. In this study, we talked about various studies in which machine learning methods are used to create efficient routing algorithms, to design IDS applications to detect various attacks in advance, to predict how autonomous vehicles will make decisions in traffic, and to provide efficient and fast data transmission in VANET and FANET systems.

As a result of systematic literature review, it has been observed that the use of machine learning methods has increased in VANET networks in recent years, especially in 2021. In VANET networks, although many different methods have been tried to solve the routing problem, it is seen that Q-learning algorithms are more widely used. In solving the trust management problem, although many different methods are used, it has been seen that SVM and KNN algorithms come to the fore. It can be said that the use of RF and SVM algorithms is more common in traffic management. In data transmission, many different algorithms have been used and it is not possible to say that any of them has more widespread use.

When the studies in which machine learning algorithms are used in FANET networks are examined, we encountered a much more limited number of studies. The new widespread use of FANET networks and their more frequent use, especially in military applications, can be cited among the reasons for this limitation. In FANET networks, there are studies in which machine learning algorithms are used to solve the routing problem. It has been observed that Q-Learning and Fuzzy logic approaches are used in these studies. In addition, there are studies in which the RF algorithm is used in trust management.

At the end of the systematic literature review in the study, which machine learning approaches are frequently used in routing, traffic management, trust management and data transmission in VANET networks, and which algorithms are used in routing and trust management processes in FANET networks are presented to the readers. Thus, those who examine the study will gain the knowledge of which machine learning approaches are used in the literature to solve the problems encountered in VANET and FANET networks.

In the future, it is planned to conduct a study on the optimization methods used to make the routing process, which is one of the most important problems in VANET and FANET networks, more efficient and faster. In addition, it is also aimed to conduct a study in which deep learning algorithms that have recently become widespread in these networks are examined.

REFERENCES

[1] Ayyash, M., Alsbou Y., &Anan M. (2015). *Wireless Sensor and Mobile Ad-Hoc Networks. Introduction to Mobile Ad-Hoc and Vehicular Networks*. Springer, New York, 33-46.

[2] Benek, Ö., (2019). *Vanet sistemlerinde kullanilan iletişim protokollerinin analizi*.Yüksek Lisans Tezi, İstanbul Üniversitesi, Cerrahpaşa Lisansüstü Eğitim Enstitüsü, İstanbul.

[3] Bekmezci, İ. &Ülkü, E. E., (2015) Location information sharing with multi token circulation in Flying Ad Hoc Networks. *7th International Conference on Recent Advances in Space Technologies (RAST)*.16-19 June, İstanbul, 669-673.

[4] Ulku, E. E., Dogan, B., Demir, O., & Bekmezci, I. (2019). Sharing Location Information in Multi-UAV Systems by Common Channel Multi-Token Circulation Method in FANETs. *ElektronikaIrElektrotechnika*, *25*(1), 66-71.

[5] Ulku, E. E., & Bekmezci, I. (2016). Multi token based locations haring for multi UAV systems. *International Journal of Computer and Electrical Engineering*, *8*(3), 197.

[6] Zhang, S., Lagutkina, M., Ovaz Akpinar, K. & Akpinar, M. (2021). Improving performance and data transmission security in VANETs. *Computer Communications*, *180*, 126-133.

[7] Costa, L. A. L. d., Kunst, R., & Freitas, E. P. d. (2021). Q-FANET: Improved Q-learning based routing protocol for FANETs. *Computer Networks*, *198*, 108379.

[8] Acharya, A., & Oluoch, J. (2021). A Dual Approach for Preventing Blackhole Attacks in Vehicular Ad Hoc Networks Using Statistical Techniques and Supervised Machine Learning. *IEEE International Conference on Electro Information Technology (EIT).* 14-15 May, USA, 230-235.

[9] Arafat, M. Y., & Moh, S. (2021). A Q-Learning-Based Topology-Aware Routing Protocol for Flying Ad Hoc Networks. *IEEE Internet of Things Journal*, *9*, 1985-2000.

[10] Kadam, N., & Sekhar, K. R. (2021). Machine Learning Approach of Hybrid KSVN Algorithm to Detect DDoS Attack in VANET. *International Journal of Advanced Computer Science and Applications*, *12.*

[11] Tong, J., Gu, X., Zhang, M., Wan, J., & Wang, J. (2021). Traffic flow prediction based on improved SVR for VANET. *4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE).* 26-28 March, China, 402-405.

[12] Sharma, A., & Jaekel, A. (2021). Machine Learning Approach for Detecting Location Spoofing in VANET. *International Conference on Computer Communications and Networks (ICCCN).*19-22 July, Greece, 1-6.

[13] Guerber, C., Royer, M., & Larrieu, N. (2021). Machine Learning and Software Defined Network to secure communications in a swarm of drones. *Journal of Information Security and Applications*, *61*, 102940.

[14] Krishna, M. V. B. M., Ananth, C. A., & Raj, N. K. (2021). Intrusion Detection System for Energy Efficient Cluster based Vehicular Adhoc Networks. *International Journal of Advanced Computer Science and Applications, 12.*

[15] Gonçalves, F., Macedo, J., & Santos, A. (2021). An intelligent hierachical security framework for vanets. *Information, 12,* 455.

[16] Cárdenas, L. L., Mezher, A. M., Bautista, P. A. B., León, J. P. A., & Igartua, M. A. (2021). A Multimetric Predictive ANN-Based Routing Protocol for Vehicular Ad Hoc Networks. *IEEE access, 9,* 86037 – 86053.

[17] Mankodiya, H., Obaidat, M. S., Gupta, R., & Tanwar, S. (2021). XAI-AV: Explainable Artificial Intelligence for Trust Management in Autonomous Vehicles. *International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)*. 15-17 October, Beijing, China, 1-5,

[18] Nadarajan, J., & Kaliyaperumal, J. (2021). QOS aware and secured routing algorithm using machine intelligence in next generation VANET. *International Journal of System Assurance Engineering and Management*, 1-12.

[19] Gad, A. R., Nashat, A. A., & Barkat, T. M. (2021). Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset. *IEEE Access*, *9*, 142206-142217.

[20] Ashtaiwi, A. (2021). ML-Based Localizing and Driving Direction Estimation System for Vehicular Networks. *International Conference on Artificial Intelligence in Information and Communication (ICAIIC).* 13-16 April, Jeju Island, South Korea, 465-470.

[21] Alsarhan, A., Alauthman, M., Alshdaifat, E., Al-Ghuwairi, A., & Al-Dubai, A. (2021). Machine Learning-driven optimization for SVM-based intrusion detection system in vehicular ad hoc networks. *Journal of Ambient Intelligence and Humanized Computing,* 1-10.

[22] Uprety, A., Rawat, D. B., & Li, J. (2021). Privacy Preserving Misbehavior Detection in IoV using Federated Machine Learning. 1*8th Annual Consumer Communications Networking Conference (CCNC).* 9-12 January, Las Vegas, NV, USA, 1-6.

[23] Ercan, S., Ayaida, M., & Messai, N. (2021). New Features for Position Falsification Detection in VANETs using Machine Learning. *ICC 2021 - IEEE International Conference on Communications*. 14-23 June, Montreal, QC, Canada, 1-6.

[24] Cabelin, J. D., Alpano, P. V., & Pedrasa, J. R. (2021). SVM-based Detection of False Data Injection in Intelligent Transportation System. *International Conference on Information Networking (ICOIN)*. 13-16 January, Jeju Island, South Korea, 279-284.

[25] Kumbhar, F. H., & Shin, S. Y. (2021). DT-VAR: Decision Tree Predicted Compatibility-Based Vehicular Ad-Hoc Reliable Routing. *Ieee Wireless Communications Letters, 10,* 87-91.

[26] Bolodurina, I., Parfenov, D., & Grishina, L. (2021). Investigation of Feature Engineering Methods for Identifying Attacks in the VANET. *International Russian Automation Conference (RusAutoCon)*. 5-11 September, Sochi, Russian Federation, 1031-1035.

[27] Raja, G., Anbalagan, S., & Vijayaraghavan, G. (2021). SP-CIDS: Secure and Private Collaborative IDS for VANETs. *IEEE Transactions On Intelligent Transportation Systems,* 22, 4385-4393.

[28] Zang, M., & Yan, Y. (2021). Machine Learning-Based Intrusion Detection System for Big Data Analytics in VANET. *3rd Vehicular Technology Conference (VTC2021-Spring)*. 25-28 April, Helsinki, Finland, 1-5.

[29] R, D. K., Chavhan, S., Gupta, D., Khanna, A., & Rodrigues, J. J. P. C. (2021). An Intelligent Self-learning Drone Assistance Approach towards V2V Communication in Smart City. *Proceedings of the 4th ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond (DroneCom '21)*. 29 October, New York, NY, United States, 19-24.

[30] Gonççalves, F., Macedo, J., & Santos, A. (2021). Evaluation of VANET Datasets in Context of an Intrusion Detection System. *2021 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. 23-25 September, Split, Hvar, Croatia, 1-6.

[31] Hossain, M. A., Noor, R. M., Yau, K.-L. A., Azzuhri, S. R., Z'aba, M. R., Ahmedy, I., & Jabbarpour, M. R. (2021). Machine Learning-Based Cooperative Spectrum Sensing in Dynamic Segmentation Enabled Cognitive Radio Vehicular Network. *Energies*, *14*, 1169.

[32] Lee, S.-W., Ali, S., Yousefpoor, M. S., Yousefpoor, E., Lalbakhsh, P., Javaheri, D., Rahmani, A. M., & Hosseinzadeh, M. (2021). An Energy-Aware and Predictive Fuzzy Logic-Based Routing Scheme in Flying Ad Hoc Networks (FANETs). *IEEE Access*, *9*, 129977-130005.

[33] Yu, J., Vandanapu, A., Qu, C., Wang, S., & Calyam, P. (2020). Energy-aware Dynamic Computation Offloading for Video Analytics in Multi-UAV Systems. *2020 International Conference on Computing, Networking and Communications (ICNC)*. 17-20 February, Big Island, HI, USA, 641-647.

[34] Quevedo, C. H. O. O., Quevedo, A. M. B. C., Campos, G. A., Gomes, R. L., Celestino, J., & Serhrouchni, A. (2020). An Intelligent Mechanism for Sybil Attacks Detection in VANETs. *IEEE International Conference on Communications (ICC)*. 7-11 June, Dublin, Ireland, 1-6.

[35] Haddaji, A., Ayed, S., & Fourati, L. C. (2020). Blockchain-based Multi-Levels Trust Mechanism Against Sybil Attacks for Vehicular Networks. IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE). 31 December - 1 January, Guangzhou, China, 155-163.

[36] Koshimizu, T., Gengtian, S., Wang, H., Pan, Z., Liu, J., & Shimamoto, S. (2020). Multi-Dimensional Affinity Propagation Clustering Applying a Machine Learning in 5G-Cellular V2X. *IEEE Access*, *8*, 94560-94574.

[37] Adhikary, K., Bhushan, S., Kumar, S., & Dutta, K. (2020). Hybrid Algorithm to Detect DDoS Attacks in VANETs. *Wireless Personal Communications*, *114*, 3613-3634.

[38] Liu, X. (2020). Deep Learning for Resource Allocation of a Marine Vehicular Ad-Hoc Network. *2020 IEEE Latin-American Conference on Communications (LATINCOM)*. 18-20 November, Santo Domingo, Dominican Republic, 1-6.

[39] Mamatha, G., Sharan, H. S.., Prathik, R., Priya, D. S., & Prajwal, U. (2020). Smart Vehicular communication for Road status analysis and Vehicle trajectory prediction. *Third International Conference on Smart Systems and Inventive Technology (ICSSIT 2020)*. 20-22 August, Tirunelveli, India, 1081-1087.

[40] Garip, M. T., Lin, J., Reiher, P., & Gerla, M. (2019). SHIELDNET: An Adaptive Detection Mechanism against Vehicular Botnets in VANETs. *2019 IEEE Vehicular Networking Conference (VNC)*. 4-6 December, Los Angeles, California, 1-7.

[41] Pressas, A., Sheng, Z., Ali, F., & Tian, D. (2019). A Q-Learning Approach With Collective Contention Estimation for Bandwidth-Efficient and Fair Access Control in IEEE 802.11p Vehicular Networks. *IEEE Transactions On Vehicular Technology*, *68*, 9136-9150.

[42] Kamble, S. J.,& Kounte, M. R. (2019). On Road Intelligent Vehicle Path Predication and Clustering using Machine Learning Approach. *Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2019).* 12-14 December, Palladam, India, 501-505.

[43] Zhao, H., Cheng, H., Mao, T., & He, C. (2019). Research on Traffic Accident Prediction Model Based on Convolutional Neural Networks in VANET. *2019 2nd International Conference on Artificial Intelligence and Big Data (ICAIBD).* 25-28 May, Chengdu, China, 79-84.

[44] Aljeri, N., & Boukerche, A. (2019). A Novel Online Machine Learning Based RSU Prediction Scheme for Intelligent Vehicular Networks. *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*. 3-7 November, Abu Dhabi, United Arab Emirates, 1-8.

[45] Li, J., Xing, Z., Wei, S., Qian, Y., & Zhang, W. (2019). Dynamic Vehicle Data Gathering via Deep Reinforcement Learning Approach. *2019 IEEE 5th International Conference on Computer and Communications (ICCC)*. 6-9 December, Chengdu, China, 1916-1920.

[46] Das, R., & Khilar, P. M. (2019). Driver Behaviour Profiling in VANETs : Comparison of Ensemble Machine Learning Techniques. *2019 IEEE 1st International Conference on Energy, Systems and Information Processing (ICESIP)*. 4-6 July, Chennai, India, 1-5.

[47] Alsuhli, G. H., Khattab, A., Fahmy, Y. A., & Massoud, Y. (2019). Enhanced urban clustering in VANETs using online machine learning. *IEEE International conference on vehicular electronics and safety (ICVES).* 4-6 September, Egypt, 1-6.

[48] Kandali, K., Bennis, L., & Bennis, H. (2021). A New Hybrid Routing Protocol Using a Modified K-Means Clustering Algorithm and Continuous Hopfield Network for VANET. *IEEE Access*, *9*, 47169-47183.