# A Systematic Review of the Intrusion Detection Techniques in VANETS

Ila Naqvi [1], Alka Chaudhary [1], Anil Kumar [2]

[1]*Amity Institute of Information Technology, Amity University, Noida, U.P., India*
[2] *DIT University, Dehradun, Uttarakhand, Indıa*

***Abstract*** **- Vehicular Ad hoc Networks are an important subset of MANETs. VANET is the group of vehicles that are connected to each other wirelessly. VANET security is a major issue that is being worked upon these days. One tiny security flaw can cause a huge loss of lives. For ensuring the security, Intrusion Detection Systems (IDS) are implemented in VANETs for detecting any intrusion. The IDS analyzes the network and detects any malicious node if present. This paper presents a comprehensive review of some of the recent and important intrusion detection research works and presents a comparative analysis of the techniques used in detecting intrusions as well as attacks focused.**

***Keywords*** **- Intrusion Detection System, IDS, VANET Security, Attacks on VANETs, Vehicular ad hoc Networks.**

## 1. Introduction

Vehicular Ad hoc Networks (VANET) are evolving as an important subset of MANETs. VANET is a group of vehicles that are interlinked to one another through wireless network.
The communication among vehicles in VANETs is performed mainly by two types, namely, Vehicle-to-Vehicle Communication and Vehicle-to-Infrastructure Communication commonly abbreviated as V2V and V2I communication respectively. V2V Communication refers to the communication among the vehicles while V2I communication refers to the communication of the vehicles with Roadside units (RSUs). IEEE 802.11p is a modification of the IEEE 802.11 standard for supporting the WAVE protocol. WAVE refers to Wireless Access in Vehicular Environment. This protocol helps in establishing Dedicated Short-Range Communications (DSRC) that could operate in 5.9 GHz frequency band [1].

Attacks in VANETs can be classified into five major groups, these are: Attack on Integrity, Attack on Confidentiality, Attacks on Availability, Attacks on Accountability and, Attacks on Authentication [2]. The Intrusion Detection Systems can be used for the network segments as well as on the individual nodes in VANET. The global IDS monitors the segment of VANET where it takes care of the group of vehicles in its segment, and detects intrusion for the segment while the local IDS work for specific node on which they are implemented. Local IDS monitor all network data coming and going in/out of the node [3]. In this paper, we will discuss the Intrusion detection system, its architecture and then we will present various literature related to intrusion detections and IDS algorithms in VANETs.

### 1.1. *Intrusion Detection Systems (IDS)*

Intrusion detection system is a system, implemented on a network for detecting any malicious activity in the target network. It is the software architecture that works by analyzing the network and detecting any intrusions tried or made in the network so that proper steps could be taken timely to prevent damage from such activities. When an IDS detects any malicious activity in the network or node, it also responds by blocking the malicious node from accessing the network to prevent any further damage to the network. The Intrusion Detection System responds to malicious activities by preventing a suspected IP address, port or user from accessing the network [4].

DOI: 10.18421/TEM112-51
https://doi.org/10.18421/TEM112-51

**Corresponding author:** Ila Naqvi,
*Research Scholar, Amity Institute of Information Technology, Amity University, Noida, U.P., INDIA,*
**Email:** naqviila92@gmail.com

*Received: 28 January 2022.*
*Revised: 09 May 2022.*
*Accepted: 14 May 2022.*
*Published: 27 May 2022.*

Intrusion Detection Systems are classified into different categories depending on different classifiers, (see Figure 1). Based on target of intrusion detection, the IDS are classified into three types: Network-based Intrusion Detection Systems (NIDS) that work at network level to detect any malicious node in the network or trial of intrusion into the network, Host based Intrusion Detection Systems (HIDS) work locally on a particular node to detect any intrusions and, Wireless-based Intrusion Detection Systems (WIDS) work on wireless networks with functionalities similar to NIDS. On the basis of detection approaches used, the IDS are classified into Misuse Detection and Anomaly Detection and, on the basis of the behaviour of IDS, these are classified as Passive IDS and Active IDS [5]. There are two types of IDS on the basis of the types of systems employed in IDS, namely, centralized IDS and distributed IDS. The data collection for intrusion detection can be network-based or host-based or can use a combined approach of both host and network-based methods [6].

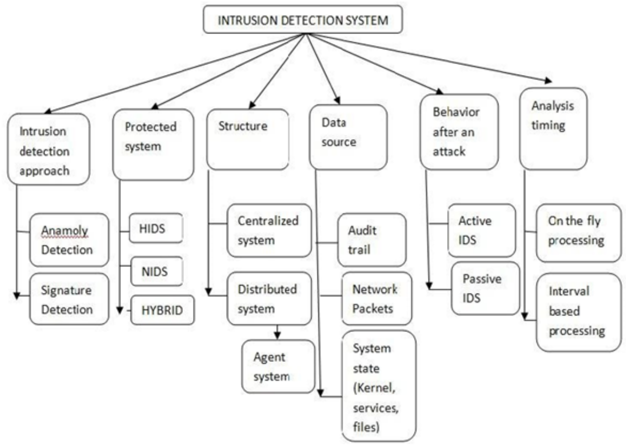

*Figure 1. Classification of Intrusion Detection Systems [7]: This Figure presents the classification of Intrusion Detection Systems on the basis of various factors.*

## 1.2. IDS Architecture

The architectures used in Intrusion Detection Systems can be centralized or decentralized. A centralized IDS is one in which the data collection and analyzing is done in centralized system while distributed intrusion detection system, the data collection and analyzing is performed on multiple distributed hosts. Intrusion detection for single system is effectively performed through centralized IDS. The locations for data analysis are fixed without being affected by the number of hosts under observation. In cases where multiple systems are involved, decentralized architecture is employed in IDS. In decentralized intrusion detection systems, multiple data security analysis at multiple network sites is carried out. The number of locations at which the data analysis is performed is proportional to the number of host machines under observation [8].

The very first architecture of IDS was proposed by Dorothy Denning [9]. Since then, many different models have been proposed for intrusion detection which differ from one another in one way or the other. However, there is a general basic architecture that is employed in most of the intrusion detection systems, which can be seen in Figure 2.

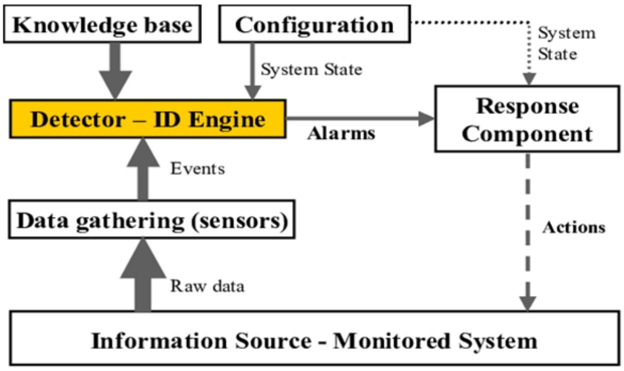

*Figure 2. Basic Architecture of an IDS [10]. This figure presents the basic archoitecture of an Intrusion Detection System, highlighting all its important components.*

## 2. Literature Review

### 2.1. Literature Sources

The literature used in the study consists of twenty research papers that are selected by searching various search strings on Google Scholar. The search strings include "Intrusion Detection in Vanets", "Intrusion Detection System in Vehicular Networks", "Vanet Security", "Vehicular-ad hoc Networks", "IDS", "Attack Detection in Vehicular Networks" etc., using synonyms of the given words. Figure 3 and Figure 4 present the distribution of studies selected for this study according to the publishing year and publisher respectively.

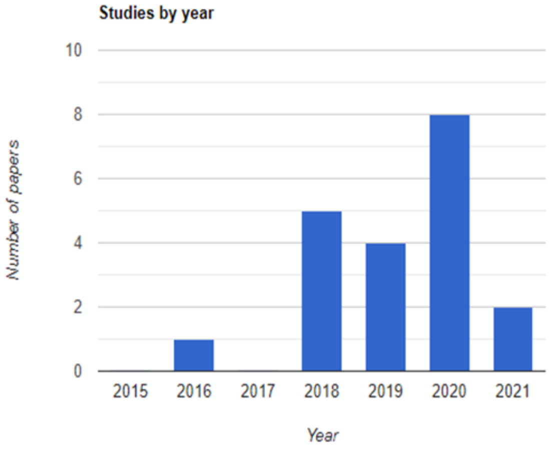

*Figure 3. This figure presents the number of papers taken from each year for this study*

The studies selected consists of research papers including:

- IEEE : 6 Papers
- Elsevier : 5 Papers
- Springer : 4 Papers
- Others : 3 Papers
- Wiley : 1 Paper

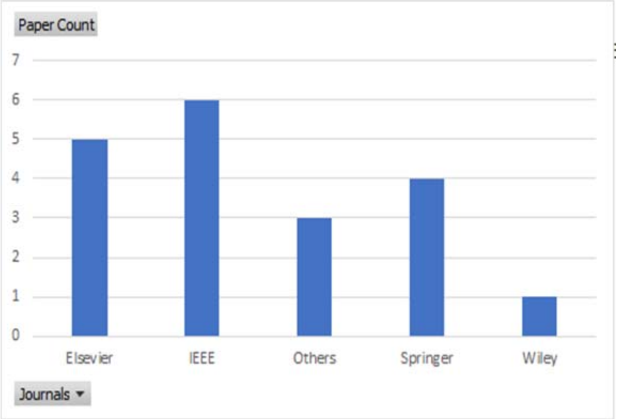

*Figure 4. This figure presents the Number of research paper taken for the study by each publisher*

### 2.2. Review of Literature

An IDS based on SVM is proposed in [11] that implements a penalty function that is utilized for minimizing the support vectors' number for controlling the complex nature of the classifiers. In this study, SVM was optimized using three Machine Learning algorithms including Ant colony optimization, Particle swarm optimization and Genetic algorithm. The simulation of the three algorithms was carried out on NSL-KDD dataset. Genetic Algorithm performed best among the three Machine Learning algorithms to detect the intrusions in the network.

An IDS is proposed in [12] is based on SVM that is optimized using Dolphin Swarm algorithm. The authors also propose an algorithm for decision making, which is called Hybrid fuzzy multi-criteria decision making algorithm. This algorithm employs Fuzzy Analytic Hierarchy Process and TOPSIS to make decisions regarding the selection of the cluster heads. The cluster heads examine the vehicles in their respective clusters in order to detect any malicious vehicle. In case a malicious vehicle is detected, it is prevented from using any network services. In this way, every vehicle in the network is checked in case of malicious behaviour. Supervised Machine learning technique, SVM has been optimised with the Dolphin Swarm algorithm to detect the malicious vehicles.

The authors in [13] propose an IDS based on SVM and feed forward neural network. The simulation generates a trace file in the process and extraction of features is done from that file by using the Proportional Overlapping Score and classification of features is done through fuzzy sets. The Feed Forward Neural Network and Support Vector Machine is used to detect the intrusion. The authors studied abnormal as well as normal behaviours of the system and compared the effectiveness of the developed system in both situations. The results have shown that the developed IDS performs very well in both situations.

An IDS called DeepVCM is proposed in [14], for On-board Units using Deep Learning. The raw data is captured in a PCAP file and cleaned for further process. Two deep learning methods, LSTM and CNN are employed. CNN is used for extracting the information and the three-layered LSTM is used for machine learning based on time-dependency. The output from the CNN becomes the input of the LSTM. The structure of the proposed DeepVCM is as follows: two layered CNN, two layered Max-pooling and two Local Response Normalization layers and a three-layered LSTM. The output of the CNN layer is inputted in Max-pooling for processing. DeepVCM has a feature to update itself automatically from time to time. The proposed model performed very well with limited resources.

An IDS is proposed in [15] employed the adaptive neuro fuzzy system to detect routing attacks in the network. The two features including the node scalability and the network range are studied and evaluated. MATLAB is used for simulation. The proposed method performs better than most of the existing techniques in terms of throughput, average download relay, end to end delay and packet loss rate.

The authors in [16] propose an IDS that uses a hybrid of Genetic Algorithm and the Artificial Neural Networks. The Genetic algorithm is used for optimization and the Artificial Neural Network for classification of the features. The proposed algorithm performed better than other algorithms when the malicious nodes are large in number and is better in terms of accuracy, false alarm rate, throughput and precision.

An IDS based on SVM, known as MA-CIDS is proposed in [17]. The study involves four processes, namely, the training, the trained classifiers sharing, evaluation of the received classifier and the collaboration. The random forest algorithm is used for training of the local classifier by every node. An algorithm for trained-data sharing is also proposed in the study. The received classifiers are evaluated by the receiver nodes and then some classifiers are selected. The output of these selected classifiers is aggregated and IDS classifier is developed. The results of the simulation of the developed system show that MA-CIDS performs better than existing algorithms.

In [18], the authors propose a hybrid IDS based on SVM for detecting Distributed Denial of Service attacks in VANETs. The study combines two major SVM kernel functions namely, AnovaDot and RBFDot. AnovaDot is used to train the model and the output from the AnovaDot are used as input for the RBFDot to train the model again. This double trained model is used for detecting DDoS attacks. The study also presents a comparative analysis of the proposed model with the single SVM models. The results show that the proposed study performed better than the other models to which comparisons are made.

A Machine Learning and Game Theory based IDS is proposed in [19]. The study utilized Artificial Neural Networks in the RSUs to detect any intrusion or attack on the RSUs or the cluster heads. SVM are utilized in clusters to detect any malicious node. In short, the study focuses on detecting intrusions in the nodes, clusters, cluster heads as well as RSUs. The results of the simulation prove that the proposed model performs better than other algorithms in terms of performance and trust.

In [20], authors propose an IDS based on Knot Flow Classification technique. The study combines spline based linear model with the clustering technique. This model is named as KFC and uses k-means clustering to implement the dynamic clustering in the data. Authors used the dynamic clustering for dividing the dataset into several clusters. To visualize the dataset the model used spline.

A big data based distributed NIDS is presented in [21]. The proposed model consists of two step intrusion detection. In first step micro batch processing is used for data collection and in detection step HDFS and Random Forest classification is used for detecting intrusion. The performance of the proposed model is measured through simulation and results show that the model performed better than other algorithms in terms of accuracy and false alarm detection.

An IDS based on invariant is proposed in [22]. The model is based on distributive collaboration and is named as DCDIV. The study proposes a clustering technique for divide the nodes into number of clusters. The clusters are formed on the basis of traffic density, link life of the nodes and the Global reputation State of nodes. The study proposes an IDS based on invariant for detecting betrayal attacks. For implementing the relationships among nodes and detecting any change in the relationships, Stochastic Petri net is used and global invariant is determined. The simulation results show that the proposed model performed better than other models in terms of rate of detection.

The authors in [23] propose an IDS based on stream position performance analysis that is named SPPA. This model includes selection of cluster heads through reputation method. The selected cluster heads maintain the trace files and analyze the stream position for every node in their respective clusters. The model calculates the legitimate weight of each vehicle by calculating the Attack Signature Sample Rate, Conflict Data and the Conflict Field. These calculations are then used to determine the intrusion in the network. The proposed technique performed very well in detection of Distributed Denial of Service attack. The simulation results show that the technique is very effective in detecting the DDoS attack.

An IDS based on pre-processing feature extraction is presented in [24]. The proposed method calculates the characteristics of the traffic flow of every node in the network and uses this data to determine the position of each node. On the basis of these calculations message fabrication/ suppression attacks are detected and the malicious node is identified. The technique uses the Accepted Signal Strength for detection of the position of the nodes. The results of the simulation show that the proposed system performed better than other intrusion detection systems.

The authors in [25] propose an IDS based on differences in traffic flow and the nodes' position. The proposed model utilizes feature extraction to extract data from the nodes and uses a self-organizing map-based classifier called I-GHSOM for the training of the model. In order to determine the traffic flow, a voting filter technique and a semi-co-operative technique are developed. For node's position, the authors involved some distance calculation mechanisms. The results of the simulation show that the proposed method is better than others in terms of efficiency, accuracy and scalability.

An IDS based on game theory is presented in [26]. The authors presented a clustering algorithm for dividing the nodes into clusters. After that a neural network-based classifier is used to detect the intruder nodes. Apart from these, the study employs Nash-equilibrium to monitor the intrusion in the network. The whole model was designed as a game consisting of two players where IDS and the intruder node are the main players. The simulation results shows that the model performed better than the other models in terms of accuracy.

A collaborative IDS based on deep learning algorithms is proposed in [27]. A distributed Software Defined Networking is employed in the model. The authors used cloud servers and the SDN controllers for training purposes. The model is tested on real world data and the results show that the proposed model is effective and efficient in detecting intrusions in VANETs.

The authors in [28] propose a collaborative IDS based on trust. The model is divided into two sub models including a local detector that utilizes k-nearest neighbour classifier that collects the data, processes the data and detects the intrusions. A score table is maintained by every node and is updated continuously as the communication takes place in the network. These score tables from all the nodes are combined and collaborated with all other nodes in order to identify and detect any intrusion in the network.

In [29], the authors employed various Machine Learning techniques to detect intrusions in the VANETs. The techniques include XGBoost, AdaBoost, Random Forest, k-nearest neighbour, SVM, Decision trees, Naïve Bayes and logistic regression. The authors worked on ToN-IoT datasets and tested all the mentioned techniques to detect intrusions in the network. For feature selection, Chi-square technique has been employed. The results have shown that the XGBoost method has performed the best among the all mentioned Machine Learning techniques.

An IDS based on SVM and modified promiscuous mode called as TSIDS is proposed in [30]. The promiscuous mode is utilized by the authors for collecting the data from the network and the SVM is utilized to process the data and detecting the intrusion. The main focus of combining the two techniques is to obtain common trust value that will be used by both the source vehicle as well as the mediator vehicle to ensure that the next vehicle is not an intruder. In case an intrusion is identified, both nodes collaborate and work to secure the network services available and maintain the performance of the network.

## 3. Comparison

Table 1 below presents a comparison of the selected studies:

*Table 1. The table presents a comparison of the various works selected for the study, with parameters including the techniques used and attacks focused in studies*

| Paper | Year | Technique Used | Attacks Focused |
|---|---|---|---|
| Alsarhan et al. | 2021 | SVM, Genetic algorithm (GA), Particle swarm optimization (PSO), and ant colony optimization (ACO) | Denial of service, Probing, Unauthorized access |
| Sharma & Kaul | 2018 | Dolphin Swarm Algorithm, Fuzzy Logic | Packet Drop, Selective Forwarding and Wormhole |
| Alheeti et. al | 2016 | Feed Forward Neural Network and SVM | Grey hole & Rushing attack |
| Zeng et al. | 2019 | Convolutional Neural Network (CNN) , Long Short-Term Memory (LSTM) | DoS,DDoS, Black Hole, Wormhole, and Sybil attack |
| Kaur et al. | 2019 | Adaptive Neuro Fuzzy system | Routing attack |
| Aneja et al. | 2018 | Artificial neural network and genetic algorithm | Flooding Attack |
| Ghaleb et al. | 2020 | RF, XGBboost, and SVM algorithms | Colluding attacks, Potent attacks, DOS , Sybil attacks etc |
| Adhikary et al. | 2020 | SVM kernel methods-Anova-Dot and RBFDot | Distrib-uted Denial of Ser-vice (DDoS) attacks |
| Zeng et al. | 2018 | SVM, ANN,trust based mechanisms, Game Theory | All attack types |
| Schmidt et al. | 2020 | Feature Extraction, k-means clustering | All attack types |
| Gao et al. | 2019 | Random Forest, Machine learning, Big Data | DDoS (Distributed Denial of Services) attacks |
| Zhou et al. | 2020 | Reputation based clustering and Invariant analysis, big data | Betrayal Attacks (Black hole, Denial of Service, Spoofing, gray hole) |
| Kolandaisamy et al. | 2020 | Stream Position Performance Analysis, reputation based clustering | DDoS (Distributed Denial of Services) attacks |
| Ayoob et al. | 2019 | Pre-processing feature extraction | Blackhole attack, Denial of Service (DoS), Sybil attack etc. |
| Liang et al. | 2020 | Feature Extraction | All attack types |
| Subba et. al. | 2018 | Game Theory, Vickrey-Clarke-Groves mechanism , Neural Network | Black Hole attack, Worm Hole attack, Sybil attack, Denial of service attack etc. |
| Shu et. al. | 2020 | Deep Learning, Distributed SDN | All attack types |
| Nandy et. al. | 2020 | K nearest neighbour non- linear classsifier | All attack types |
| Gad et. al. | 2021 | Machine Learning tech-niques: XGBoost, AdaBoost, Random Forest, k-nearest neighbour, SVM, Decision trees, Naïve Bayes and logistic regression | DoS,DDoS |
| Shams et. al. | 2018 | SVM, Machine Learning | All attack types |

## 4. Critical Findings

From the analysis of the selected studies, following results are obtained in terms of techniques used for detecting intrusions (see Figure 5):

- 30% of the selected research works have used Support Vector Machine (SVM) in their Intrusion Detection System, either alone or in combination with some other technique.
- 25% of the selected studies used Neural Networks in their Intrusion Detection Systems, these include Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN) and, Feed-Forward Neural Networks (FFNN).
- Next mostly used is the Random Forest technique followed by all other techniques.
- Among the reviewed works, the best performance was observed by the Feed Forward Neural Networks based IDS proposed by [13], that has shown an average detection rate of 99.81%.
- SVM based IDS in [13] is the second best that has shown an average detection rate of 99.72% followed by Genetic Algorithm optimized SVM based IDS in [11] with an average detection rate of 99%.

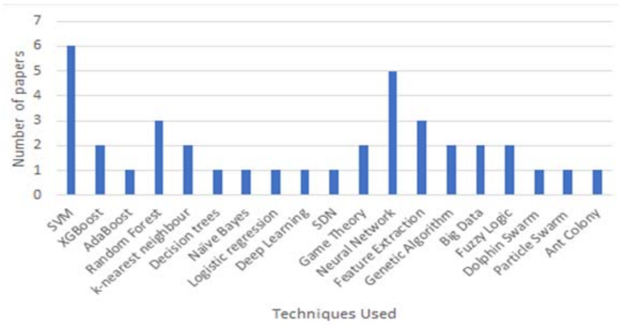

*Figure 5. Techniques Used in IDS: This figure presents the various techniques used for Intrusion Detection in papers under study, to the number of papers that employed those techniques in their IDS.*

The analysis of the data shows that Support Vector Machines and Neural Networks are the most used techniques for intrusion detection in VANETs and have shown a good performance in terms of effectiveness and accuracy in detecting intrusions.

From the analysis of the selected studies, following results are obtained in terms of attacks focused (see Figure 6):

- DoS and DDoS are the attacks that are mostly worked on in 24% and 20% of studies respectively.
- Next are the Black Hole and Sybil attacks that appeared in 16% of studies.
- Worm Hole attack followed by other attacks are least focused.

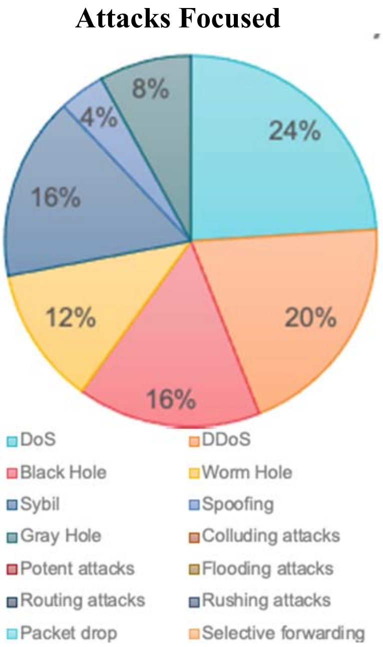

*Figure 6. Attacks focused in selected studies. The pie chart represents the percentage of research papers that focused on specific attack.*

The analysis of the data shows that Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks are the most focused attacks in researches these days in the field of intrusion detection in VANETs. Some studies have particularly worked upon the detection of these attacks while some have taken these in group with other attacks also. Sybil attack and black hole attacks are also popular in the studies.

## 5. Conclusion

VANET security is a vast field in which a lot of work has already been done and research is still being carried out. It has attracted academicians and researchers from around the world. VANET environment is very susceptible to attacks and a tiny security flaw can lead to a huge loss. Compromise in case of VANET security means compromising the life of people. For proper security implementations, Intrusion Detection Systems are used in VANETs for detecting any intrusions in the network. The IDS analyses the traffic and detects any malicious node if present. As the technology is growing, the techniques and methods of attacks are also evolving. Continuous research in the field is most important requirement right now.

This paper examined the various works done in the field of IDS in VANET systems. The selected works have been compared and it has been found that SVM and Neural networks are the most popular techniques that are being used in detecting intrusions in the VANET environment. The paper also analyzed the attacks that have been worked upon and found that

DoS and DDoS attacks are mostly used in the studies.

For future work, the main objective is to perform a deep comparative analysis by performing simulation and designing an IDS.

**References**

[1]. Saggi, M. K., & Sandhu, R. K. (2014, December). A survey of vehicular ad hoc network on attacks and security threats in vanets. In *International Conference on Research and Innovations in Engineering and Technology (ICRIET 2014)* (pp. 19-20).

[2]. Morgan, Y. L. (2010). Notes on DSRC & WAVE standards suite: Its architecture, design, and characteristics. *IEEE Communications Surveys & Tutorials*, *12*(4), 504-518.

[3]. Dang, N., & Mittal, P. (2012). Cluster based intrusion detection system for MANETS. *International Journal of Computer Applications & Information Technology*, *1*(1).

[4]. Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (idps). *NIST special publication*, *800*(2007), 94

[5]. Saxena, A., & Mueller, C. (2018). Intelligent Intrusion Detection in Computer Networks using Swarm Intelligence [J]. *International Journal of Computer Applications*, *179*(16), 1-9.

[6]. Azad, C., & Jha, V. K. (2013). Data mining in intrusion detection: a comparative study of methods, types and data sets. *International Journal of Information Technology and Computer Science (IJITCS)*, *5*(8), 75-90.

[7]. Kazienko, P., & Dorosz, P. (2004). Intrusion detection systems (IDS) Part 2-Classification; methods; techniques.

[8]. Spafford, E. H., & Zamboni, D. (2000). Intrusion detection using autonomous agents. *Computer networks*, *34*(4), 547-570.

[9]. Denning, D. E. (1987). An intrusion-detection model. *IEEE Transactions on software engineering*, (2), 222-232.

[10]. Lazarevic, A., Kumar, V., & Srivastava, J. (2005). Intrusion Detection: A Survey. *Managing Cyber Threats*, 19-78.

[11]. Alsarhan, A., Alauthman, M., Alshdaifat, E., Al-Ghuwairi, A. R., & 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.

[12]. Sharma, S., & Kaul, A. (2018). Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized IDS for VANET. *Vehicular Communications*, *12*, 23-38.

[13]. Ali Alheeti, K. M., Gruebler, A., & McDonald-Maier, K. (2016). Intelligent intrusion detection of grey hole and rushing attacks in self-driving vehicular networks. *Computers*, *5*(3), 16.

[14]. Zeng, Y., Qiu, M., Zhu, D., Xue, Z., Xiong, J., & Liu, M. (2019, May). Deepvcm: a deep learning based intrusion detection method in vanet. In *2019 IEEE 5th intl conference on big data security on cloud (BigDataSecurity), IEEE intl conference on high performance and smart computing,(HPSC) and IEEE intl conference on intelligent data and security (IDS)* (pp. 288-293). IEEE.

[15]. Kaur, J., Singh, T., & Lakhwani, K. (2019, April). An enhanced approach for attack detection in vanets using adaptive neuro-fuzzy system. In *2019 International Conference on Automation, Computational and Technology Management (ICACTM)* (pp. 191-197). IEEE.

[16]. Aneja, M. J. S., Bhatia, T., Sharma, G., & Shrivastava, G. (2018). Artificial intelligence based intrusion detection system to detect flooding attack in VANETs. In *Handbook of Research on Network Forensics and Analysis Techniques* (pp. 87-100). IGI Global.

[17]. A Ghaleb, F., Saeed, F., Al-Sarem, M., Ali Saleh Al-rimy, B., Boulila, W., Eljialy, A. E. M., ... & Alazab, M. (2020). Misbehavior-aware on-demand collaborative intrusion detection system using distributed ensemble learning for VANET. *Electronics*, *9*(9), 1411.

[18]. Adhikary, K., Bhushan, S., Kumar, S., & Dutta, K. (2020). Hybrid algorithm to detect DDoS attacks in VANETs. *Wireless Personal Communications*, *114*(4), 3613-3634.

[19]. Zeng, Y., Qiu, M., Ming, Z., & Liu, M. (2018, December). Senior2local: A machine learning based intrusion detection method for vanets. In *International conference on smart computing and communication* (pp. 417-426). Springer, Cham.

[20]. Schmidt, D. A., Khan, M. S., & Bennett, B. T. (2020). Spline-based intrusion detection for VANET utilizing knot flow classification. *Internet Technology Letters*, *3*(3), e155.

[21]. Gao, Y., Wu, H., Song, B., Jin, Y., Luo, X., & Zeng, X. (2019). A distributed network intrusion detection system for distributed denial of service attacks in vehicular ad hoc network. *IEEE Access*, *7*, 154560-154571.

[22]. Zhou, M., Han, L., Lu, H., & Fu, C. (2020). Distributed collaborative intrusion detection system for vehicular Ad Hoc networks based on invariant. *Computer Networks*, *172*, 107174.

[23]. Kolandaisamy, R., Noor, R. M., Kolandaisamy, I., Ahmedy, I., Kiah, M. L. M., Tamil, M. E. M., & Nandy, T. (2020). A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET. J Ambient Intell Human Comput.

[24]. Ayoob, A., Khalil, G., Chowdhury, M., & Doss, R. (2019, November). Intrusion Detection System Classifier for VANET Based on Pre-processing Feature Extraction. In *International Conference on Future Network Systems and Security* (pp. 3-22). Springer, Cham.

[25]. Liang, J., Chen, J., Zhu, Y., & Yu, R. (2019). A novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) based on differences of traffic flow and position. *Applied Soft Computing*, *75*, 712-727.

[26]. Subba, B., Biswas, S., & Karmakar, S. (2018). A game theory based multi layered intrusion detection framework for VANET. *Future Generation Computer Systems*, *82*, 12-28.

[27]. Shu, J., Zhou, L., Zhang, W., Du, X., & Guizani, M. (2020). Collaborative intrusion detection for VANETs: a deep learning-based distributed SDN approach. *IEEE Transactions on Intelligent Transportation Systems*, *22*(7), 4519-4530.

[28]. Nandy, T., Noor, R. M., Idris, M. Y. I. B., & Bhattacharyya, S. (2020, February). T-BCIDS: Trust-based collaborative intrusion detection system for VANET. In *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)* (pp. 1-5). IEEE.

[29]. 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.

[30]. Shams, E. A., Rizaner, A., & Ulusoy, A. H. (2018). Trust aware support vector machine intrusion detection and prevention system in vehicular ad hoc networks. *Computers & Security*, *78*, 245-254.