ISSN No:-2456-2165

# Intrusion Detection System in Vehicular Ad-hoc Networks

Shubham R. Dhembare
Research Scholar, Dept.of Electronics and Telecom .Engineering,
Prof. Ram Meghe Institute of Technology and Reasearch , Badnera
Amravati, Maharashtra, India

Dr. Sharad W. Mohod
Dept.of Electronics and Telecom .Engineering,
Prof. Ram Meghe Institute of Technology and Reasearch , Badnera
Amravati, Maharashtra, India

**Abstract:- Over the past few years, the field of intrusion detection in wireless networks has become more important. Insecure features in some wireless networks make the victims vulnerable to that attacks so any action can take time to implement. And another is that, as new techniques are evolving today, by making progress in the field of hacking, attackers will make every effort to infiltrate the system. Therefore, it is important to constantly monitor the system and detect suspicious behavior. So at such times, the intrusion detection system works to monitor the data, suspicious intrusions, and respond appropriately. In this perspective, this article presents a survey on previous studies of intrusion detection in wireless networks.**

***Keywords:-*** *Intrusion Detection, NSL-KDD, DDoS, Deep Learning, Vehicular Communication, IDS, VANET, SVM.*

## I. INTRODUCTION

With developing technology, every day a new traffic attacks are come in networks with increasing number of intruders. Some attacks are known to system and some are unknown also, to detect these attacks various technologies also developed by many researchers. A well-known system of detecting traffic attacks is Intrusion Detection System(IDS).This system was firstly researched in 1980 by Dorothy Denning and Peter Neumann .Initially they named the system as Intrusion Detection Expert System (IDES). Regarding performance an intrusion detection system is built for the effective and accurate in attack detection when implemented using different techniques.

Vehicular communication is the vast area to detect the traffic attacks, intrusion detection, and many more. Nowadays, the main challenge is associated with this domain to maintain network security [1]. In last few years, there were very low intruders so the system intruder easily fined the attacks from known and unknown attacker, but currently the number of intruders are increasing day by day and new variety of attacks are also evolving in market so that it becomes tough to find attacks.So, adapting new types of attacks is a difficult task in intrusion detection system (IDS). To detect intrusion in VANET, machine learning and deep learning algorithms are used at various levels.

VANET is a particular case of wireless multihop network, which has the constraint of fast topology changes due to the high node mobility. With the increasing number of vehicles equipped with computing technologies and wireless communication devices, intervehicle communication is becoming a promising field of research, standardization, and development. VANETs enable a wide range of applications, such as prevention of collisions, safety, blind crossing, dynamic route scheduling, real-time traffic condition monitoring, etc. Another important application for VANETs is providing Internet connectivity to vehicular nodes.

Vehicular ad hoc network (VANET) is a subclass of mobile ad hoc networks (MANETs) where it is developed by moving vehicles. VANET is getting progressively well known in rush hour gridlock administration particularly in a portion of the created nations. It can be ordered into well-being-related application where it can spare a large number of lives every day and non-security applications for business reason. Because of its erratic portability and discontinuous network availability, a solid end-to-end way among the source and the goal is relatively incomprehensible and consequently specially appointed steering conventions are connected in VANET. Not with standing, the greatest test in VANET is not the steering issue, yet the collaboration between the hubs. Indeed, even the best directing convention would not be helpful when the hubs do not take part in sending the information. Hua et al. of article introduced a far-reaching survey on the existing participation components in VANETs; especially, those based on versatile social networking. To start with, it investigates the current difficulties in VANET. Next, it talks about a scientific categorization for the existing collaboration instruments in VANETs and audits the proposed arrangements of every participation write. In addition, these clarify the collaboration arrangements that can be connected from the idea of Mobile Social Networking.

## II. INTRUSION DETECTION SYSTEM

Vehicular communication has the main aim to detect various traffic attacks and prevent them by using Intrusion Detection System (IDS), shown in Figure 1 as data collection, vectorization and classification engine., IDS contains necessary components. Firstly, to trace the network

flow data collection mechanism is introduced. Second, the vectorization that is beneficial to pinpoint the attributes and vector of attributes or features will to be generated. At end by using this feature vector, a classification engine is accomplished and on the basis of data collected by system, the result is classified as normal or intrusion.

Classification engine is the most complex part of IDS as it includes the decision of converted feature vector that follows the rule of intrusion. Motivation of these IDS contains some facts, such as:V ehicular communication systems are complex and it has more number of errors. which is known or unknown. Generally IDS depends on some hardware components. Running such hardware components requires consistent, and robust software [2]. They are used to detect errors and also to fix them. Some intrusion prevention systems exits but not it will not prevent all attacks. At that time, IDS plays a crucial role.

Intrusion detection system is of two types: 1. Misuse based IDS 2. Anomaly based IDS Misuse based IDS type detects the much known attacks that are predefined but it fails to identify the unknown attacks. Unknown attack with high false alarms is detected by using anomaly based approach.

Main components of IDS is shown in following Fig.1

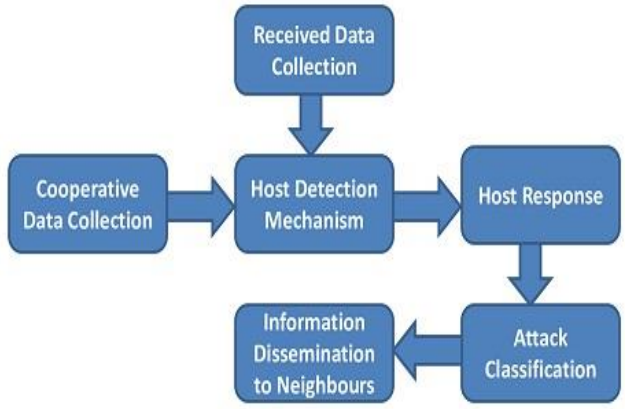


Fig. 1. Main components of IDS

IDS is designed to recognize and detect intrusion that somehow bypassed the firewall. IDS provide good traffic classification and forensic information effectively block an attack Gozde Karatas et. al. proposed the Intrusion Detection System (IDS) and to analyze the training function performance of the system. The proposed system is based on a neural network that contains 2 hidden layers for detecting the network intrusion. For performance analysis, the KDD Cup 99 dataset is used. In , presented the study on intrusion detection in VANET and analyzes the feasible solution for various types of attacks such as DOS, DDOS etc. Tuan a Tang et. Al. gives a detailed description on software-defined networking as a selected solution for detecting the intrusion in the network. The author mainly focused on DDoS attacks in IDS to increase the accuracy of the proposed NIDS model by using the deep learning technique which detects the intrusion and analyzes the NIDS model.

Konstantinos Pelechrinis et. al. presented a detailed review on the jamming attacks recorded in the paper by additionally describing various techniques suggested for detecting the presence of jammers. Finally, the work has reviewed voluminous mechanisms, which are beneficial to protect the network from various jamming Attacks. Bellardo et al , presented the experimental analysis of specific attack in network. In this research implemented the system for intrusion detection based on 802.11 MAC layer and analyzes the efficiency of system.

Ismail Butun, et. al. gives information about classification of IDS, contains detailed classification pf intrusion detection system as requirement of IDS, classification, decision making in IDS and intrusion response. IDSs that are proposed for Mobile Ah-hoc NETworks (MANET) are presented and their applicability to wireless sensor networks is discussed.

## III. TRAFFIC ATTACK

Traffic attack in vehicular communication system is different as follows:

- Normal
- DoS (Denial of Service)
- U2R (User to Root)
- R2L (Remote to Local)
- Probe (Probing Attacks)

The attacks are of 22 types each belongs to an attack category above .

1. DoS (Denial of Service): An attempt to make service unavailable to users is known as DoS (Denial of Service). In this attack, attacker's goal is that nodes cannot perform other necessary and essential task. This is the most severe and complex attack at all. This attack can overload the resource network nodes by jamming the channel in the network ways. This is a physical layer attack containing sub-type DDoS (Distributed Denial of Attack).
2. U2R (User to Root): The major attack in user to root (U2R) is buffer overflow which copies too many data into static buffer without checking the is properly fix or not.
3. R2L (Remote to Local): This attack affects the large number of network/system in the world daily.
4. Probing attack: Attacker tries to gain information about the target host.
5. Probe attack: A probe is a specially crafted attack on one or more honest monitor and its target detects and reports it with a recognizable data in the report.

## IV. TECHNIQUES USED IN VEHICULAR COMMUNICATION

IDS can be of various types to detect the traffic attacks on how system operates and collect information. Deep learning gives more accurate prediction compared to machine learning approach to detect intrusion and threats available in model. Below Fig. 2 gives the detailed block information of main methodology of DL-DAG network. Training dataset used in this method is AWID reduced dataset with

155attributes.

Main methodology of proposed model is shown in Fig.2

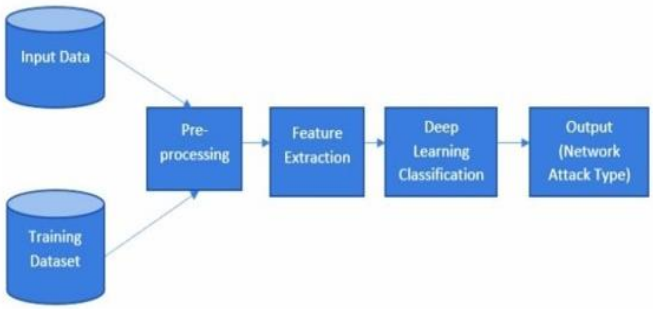


Fig.2. Main methodology of proposed model

. The very first step of the process methodology isto train the model with a dataset. The AWID data set is used totrainthe model i.e. AWID-CLS-R-Trn. Then this trained modelis passed for the pre-processing .The data which will be tested using AWID-CLS-R-Tst by the model for detection of network attacks such as normal or malicious one. This data is also forwarded to the pre-processing step. This block is used to process the data, which will be given by training dataset to model or test the data that is input data by using PCA technique. This data is then given as input to the feature selection/reduction block for selection of required features among dataset. In the next feature extraction process block ,the feature will be extracted on the basis of some requirement and order which are decided for extraction of feature with DAG network as deep learning classifier. After this the next step is classification using deep learning, here the extracted features are extracted and decides the final result based on binary classification or multiclass classification.

By using deep learning methods the data will classify into "flooding", "impersonation", "injection" and "normal" .After classification, it gives output that detects network attack type. The deep learning DAG algorithm is used for the detection of intrusion. For the classification purpose, Directed Acyclic Graph (DAG)algorithm is better option in deep learning approach. If the malicious data is found, then the alert is given to the system admin.

All above mention experimental work is carried out on Intel Corei3 8$^{th}$ generation, 4 GB RAM having windows 10 with MATLAB latestR2020b version to obtain the high accuracy and reduced the evaluation time of the model while testing and training. In this process, binary and multiclass both classification strategies are applicable while simulation. Finally for binary it opted 98.7% accuracy and for multiclass is gives 89.8% accuracy.

In offer to implement structured IDS, deep learning as well as machine learning approaches are used to detect the intrusion as normal or malicious data. Ideally, these techniques allow an IDS to function efficiently and effectively. The most success of an IDS originates from its ability to glimpse between normal and malicious attacks, the speed with which it identifies attacks, and how well it determines an attack's type. From denial service attacks, probes, unauthorized elevation of privilege and remote access attacks an IDS should differ which type of attack it is. Efficiency results from decreasing the time required for processing and the resources required for these identifications to happen. To remain sturdy, an IDS should balance efficiency and potential To detect intrusion in vehicular communication some machine learning and deep learning algorithms are used. Some algorithms are reviewed here below likewise:

Deep Belief Network (DBN): Deep Belief Network having the feed forward neural network with a deep architecture consist of many hidden layers. Some visible layer called as input layer and also some output layers are present. In [12] used intelligent routing protocol based on deep belief network for multimedia service in knowledge centric VANET's. DBN performs intrusion detection through various experiments after training with some datasets also is enhancing the security network with standard IDS algorithms. DBN have mostly fallen out now days and rarely used compared to other generative learning algorithms but still recognized for their important role in deep learning.

The most commonly used data sets for intrusion detection in IDS are: KDD Cup99, NSL-KDD, CIC IDS 2017, CSE- CIC-IDS 2018 KDD Cup99: The KDD Cup99 dataset was created in 1999 to detect intrusions. The dataset is used in data mining and machine learning techniques. This dataset contains about 4.9 million pieces of data, of which 83% are classified for all types of attack.

NSL-KDD: The machine learning algorithms on KDD-Cup99 are able to pre-process well and create new NSL-KDD datasets by removing duplicate records from them. So earlier, a lot of differences have been found in the new dataset compared to the old dataset

CIC IDS 2017: This dataset covers common attacks such as real world data, incorporates various criteria for identifying attacks as well as gives the right results for machine learning and deep learning.

CSE-CIC-IDS 2018: For vehicular systems, detailed information of attacks is included in it. This dataset contains seven types of attacks some are related to vehicular communications such as DoS attack, DDOS attack, Brute force attack.

## V. IDS SYSTYM ARCHITECT

Vehicle network operations should provide each node with intrusion detection techniques so that each node can participate in intrusion detection. Neighboring nodes can form associations and supervise each other's networks. VANET contains agents to detect the intrusion of each node and these agents act independently and control the communication activities in the radio range. If there is any change in the local data, agents from neighboring nodes will assist in detecting the intrusion.

The proposed intrusion detection system can detect intrusions using audit data if any data changes. This involves some general behavior for intrusion detection nodes. The audit data collected against intrusion is checked.

Intrusion Detection System framework in VANET shown in Fig.3

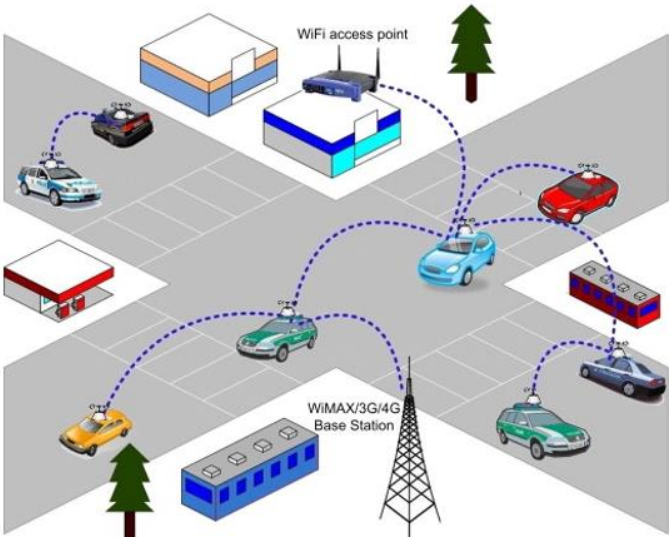


Fig. 3. Intrusion Detection System framework in VANET

## VI. CONCLUSION

VANET are highly vulnerable to attacks due to wireless media and lack of traditional security features. Safety should be the first priority for road users. So safety applications need to work on things like notifications before an accident occurs. In this paper we have discussed the different types of intrusion attacks and reviewed existing studies. Indicates whether a network is available for secure communication. This study found that most datasets do not recognize or tell how content and attacks are created. Also, dataset builders do not make theirdatasets publicly available for review. Intrusion detection systems can create preventive techniques to strengthen network security.

The main objective of this study is to create a large dataset to make the machine learning algorithm more efficient. All of these criteria need to be considered in order to create a large dataset, identify attacks, and create messages

## REFERENCES

[1]. D.E.Denning,“An intrusion detection model” IEEE Transactionson Software Engineering,vol.SE-13,no.2,pp.222–232, 1987,

[2]. T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi and M. Ghogho, "Deep learning approach for Network Intrusion Detection in Software Defined Networking," 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), Fez, Morocco, 2016, pp. 258-263,

[3]. A. Garg and P. Maheshwari, "A hybrid intrusion detection system: A review," 2016 10th International Conference on Intelligent System and Control (ISCO), Coimbatore, India, 2016, pp. 1-5,

[4]. F. Gonçalves etal., "A Systematic Review on Intelligent Intrusion Detection Systems for VANETs," 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Dublin, Ireland, 2019,pp.1-10

[5]. Pelechrinis, M. Iliofotou and S. V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers," in IEEE Communications Surveys & Tutorials, vol. 13, no. 2, pp. 245-257, 2011,

[6]. M. K. Lahre, M. T. Dhar, D. Suresh, K. Kashyap, and P. Agrawal, “Analyse different approaches for ids using kdd 99 data set,” International Journal on Recent and Innovation Trends in Computing and Communication, vol. 1, no. 8, pp. 645–651, 2013.

[7]. A. Mishra, K. Nadkarni and A. Patcha, "Intrusion detection in wireless ad hoc networks," in IEEE Wireless Communications, vol. 11, no. 1, pp. 48-60, Feb. 2004,

[8]. I. Butun, S. D. Morgera and R. Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," in IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 266-282, 2014,

[9]. V. L. Thing, ``IEEE 802.11 network anomaly detection and attack classification a deep learning approach, ”in Proc. Wireless communication networking configuration (WCNC) 2017

[10]. T. Zhang, X. Chen and C. Xu, "Intelligent Routing Algorithm Based on Deep Belief Network for Multimedia Service in Knowledge Centric VANETs," 2018 International Conference on Networking and Network Applications (NaNA), Xi'an, China, 2018, pp. 1-6,

[11]. J. V. Anand Sukumar, I. Pranav, M. Neetish and J. Narayanan, "Network Intrusion Detection Using Improved Genetic k-means Algorithm," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, India, 2018, pp. 2441-2446

[12]. L. Yong and Z. Bo, "An Intrusion Detection Model Based on Multi-scale CNN," 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 2019, pp. 214-218,

[13]. G. Karatas and O. K. Sahingoz, “Neural network bases intrusion detection systems with different training functions," 2018 6th international Symposium on Digital Forensic and Security (ISDFS),Antalya,Turkey,2018,pp.1-6

[14]. P.Satam and S.Hariri, "WIDS:An Anomaly Based Intrusion Detection System for Wi-Fi (IEEE 802.11) Protocol," in IEEE Transactions on Network and Service Management,vol.18,no.1,pp.1077-1091,2021,

[15]. W. Yang, X. Dai, J. Xiao and H. Jin, "LDV: A Lightweight DAG- Based Blockchain for Vehicular Social Networks, "in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5749-5759,June 2020, doi:10.1109/TVT.2020.2963906.
[16]. E. Chatzoglou, G. Kambourakis and C. Kolias, "Empirical Evaluation of Attacks Against IEEE 802.11 Enterprise Networks: The AWID3 Dataset," in IEEE Access, vol. 9, pp. 34188-34205,2021.
[17]. R.Abdulhammed,M.Faezipour,A.AbuzneidandA.Aless a, "Effective Features Selection and Machine Learning Classifiers for Improved Wireless Intrusion Detection," 2018 InternationalSymposiumonNetworks,ComputersandCo mmunications(ISNCC),2018,pp.1-6,
[18]. J. Tang, S. Alelyani, and H. Liu, "Feature selectionforclassification:Areview,"DataClassification, AlgorithmsApplication, vol. 37, 2014.
[19]. AWIDdata set URL. https://icsdweb.aegean.gr/awid/ download link.
[20]. Gao N, Gao L, Gao Q. et al., "An intrusion detection model based on deep belief networks / proceeding of Advanced Cloud and Big Data(CBD)",Second International Conference of IEEE,2014.
[21]. E. Chatzoglou, G. Kambourakis and C. Kolias, "Empirical Evaluation of Attacks Against IEEE 802.11 Enterprise Networks: The AWID3 Dataset," in *IEEE Access*, vol. 9, pp. 34188-34205,2021,