2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)
Amity University, Noida, India. Sep 3-4, 2021

2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) | 978-1-6654-1703-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICRITO51393.2021.9596141

Intrusion Detection in VANETs

Ila Naqvi[1], Alka Chaudhary[2], Ajay Rana[3]
[1]Research Scholar, Amity Institute of Information Technology, Amity University,
Noida, Uttar Pradesh, India
[1]naqiila92@gmail.com
[2,3]Amity Institute of Information Technology, Amity University,
Noida, Uttar Pradesh, India
2achaudhary4@amity.edu
3ajay_rana@amity.edu

***Abstract*— Vehicular Ad hoc Networks commonly abbreviated as VANETs, are an important component of MANET. VANET refers to the group of vehicles that are interlinked to one another through wireless network. Along with technology, comes the threats. Like other wireless networks, VANETs also are vulnerable to various security threats. Security in VANETs is a major issue that attracted many researchers and academicians. One small security breach can cause a big damage in case of VANETs as in this case human lives are involved. Intrusion Detection Systems (IDS) are employed in VANETs in order to detect and identify any malicious activity in the network. The IDS works by analysing 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. This paper reviews Intrusion Detection systems, classification of IDS based on various factors and then the architecture of IDS. We then reviewed some of the recent and important intrusion detection research works and then compared them with one another.**

Keywords*— *Intrusion Detection System, IDS, VANET Security, Vehicular ad hoc Networks, Attacks on VANET

I. Introduction

Vehicular ad hoc networks (VANETs) are a sub-division of mobile ad hoc network (MANETs) [1]. In comparison to MANETs, VANETS have a very fast and continuous changing network topology and frequent node density [2]. VANETs are an important component for Intelligent Transportation Systems that are reliable, secure as well as efficient solutions to many problems [3].

Basically, a Vehicular Ad Hoc Network is a mobile network composed of a number of vehicles, road side units called RSUs, and some infrastructure that helps in establishing connections among the various vehicles in the network [4]. There are enormous benefits of these networks in terms of road safety and traffic control, but there are many security issues and challenges associated with its implementation. The major challenge is the authentication of the vehicles that join the network and identification of the misbehaving vehicle. A small security breach in VANETs can cause a huge loss, it could even cost the lives of people. Hence it is necessary to have security frameworks in VANETs that ensure road safety.

A number of researchers as well as research organizations are working day and night in order to develop efficient security mechanisms for protecting VANETs against the attackers and for minimising the security attacks. Many solutions have already been proposed by researchers in the field of VANET security and defence mechanisms [5].

II. Intrusion Detection System

Intrusion Detection System (IDS) is a network security technique that is employed on networks for detection of any intrusion or attack on the network. IDS is implemented in VANETs for monitoring the incoming data as well as the vehicles for any malicious activity [6][7]. On detection of the intrusion, it is the responsibility of the IDS to block the particular malicious node, network port or IP address from doing any further damage to the network.

A. IDS Architecture

There are two types of architectures that can be employed in Intrusion Detection Systems- centralized architecture and decentralized architecture [8]. A centralized architecture involves the collection of data and its analysis carried out centrally while distributed architecture involves the data collection process and analysis to be performed on a number of hosts at various locations. A thorough elaboration of the centralized and decentralized architectures of the IDS is presented by Azad and Jha [9].

The architecture of Intrusion Detection System as given by Lazarveic et. al. [10] consists of following components (Figure 1):

1) *Detector-ID Engine:*
This is one of the most important components of the IDS. The Detector-ID Engine is involved in the data processing of the Knowledge base. It fires an alarm to the Response Component of the system if it detects any malicious activity in the system.

2) *Response Component:*
The component receives alarm signal from the detector-ID Engine when an intrusion is detected. It takes action as per the system security requirements.

3) *Knowledge Base:*
The database of an Intrusion Detection System is called its Knowledge Base. The data contained in a knowledge base is collected by the sensors in the IDS.

4) *Sensors:*
The main function of the Sensors in the Intrusion Detection System is collecting the data from the monitored system.

5) *Configuration System:*
The IDS is incorporated with a configuration component that is responsible for determining the state of the system.

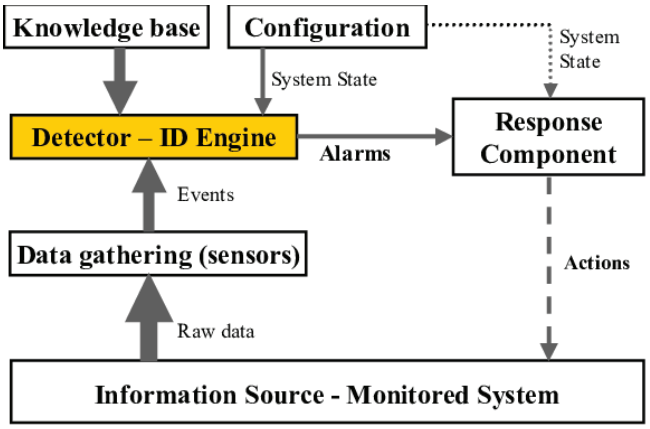

Fig. 1 Components of Intrusion Detection System [11].

III. REVIEW OF LITERATURE

Zhou et al. [12] proposed an intrusion detection algorithm called DCDIV that employs an invariant based distributed collaborative framework. The main focus of the paper is intrusion detection of the betrayal attacks in VANETs, e.g., Spoofing, Denial of Service attacks, black hole attacks etc. For the big data collection, storage as well as performing calculations of the data collected, the authors implemented a distributed collaborative framework utilizing the resources of both edge computing and cloud computing. The paper then presents a vehicle clustering method based on the GRS (Global Reputation State), vehicles' link life and the density of the traffic, in order to establish a stable and smooth communication in VANET and thus reducing the overhead. Direct reputation values calculated through beta distribution, and aggregated reputation values calculated through applying entropy weight method in reputation evaluation matrix, are used to evaluate the reputation of vehicles. The authors then proposed an invariant based intrusion detection model for VANETs where invariant is mined from the data from communication flow, traffic flow and the behavioural relationship state in order to detect the betrayal attacks in VANETs. The Stochastic Petri net (SPN) is utilized for establishing dynamic behavioural relationships among vehicles and analysing the changes in the established behavioural relationships and to find the global invariant. Finally, the system's security state is defined. The results of the simulation have shown that the algorithm performed better than other systems with regard to intrusion alarming rate and detection rate.

Kolandaisamy et al. [13] present SPPA, a stream position performance analysis-based intrusion detection system that fits the requirement of VANETs. The proposed model uses a clustering-based attack detection where cluster head is chosen by reputation method. The algorithm uses the trace files maintained by the chosen cluster heads to perform the stream position analysis for each node. Next stage involves the calculations of the Conflict Field, Conflict Data, and Attack Signature Sample Rate (CCA). Based on these calculations, the legitimate weight of each node is calculated and compared with the CCA weight to determine whether a node is intruder or not. The proposed method is effective in detecting the DDoS (Distributed Denial of Service) attack in VANETs. The paper also presents the analysis of the data generated through simulation including the throughput ratio, the packet delivery ratio, end to end delay, the attack detection time and rate, routing overhead, and false alarm rate. Results have shown that the model effectively detects the DDoS attack and the intruder node.

Adhikary et al. [14] presented a hybrid intrusion-detection algorithm for VANETs for detection of the DDoS (Distributed Denial of Service) attacks. The algorithm employs two SVM kernel functions, namely RBFDot and AnovaDot for DDoS detection. The proposed hybrid algorithm works by combining the two algorithms. Firstly, the AnovaDot is employed for training the model by using a dataset that contains the mixed data of both the normal and DDoS attacks. The predictions obtained from this model are then inserted into the RBFDot along with the same dataset for training the model. The obtained dual trained model called as hybrid model is then used to predict and detect the DDoS attacks and VANETs. The paper uses various features including delay, jitter, collision, throughput, and packet drop. The paper presents a comparison of the performance of proposed hybrid algorithm with single SVM techniques of AnovaDot and RBFDot. The experimentation results show that the presented hybrid method works well to detect DDoS attack from normal behavior.

Nandy et. al. [15] proposed a trust-based collaborative intrusion detection system for Vehicular ad hoc Networks. The proposed system consists of two major sub-systems: a local IDS based on k-nearest neighbors non-linear classifier and a collaborative learning environment. The local IDS performs three tasks: data gathering, pre-processing and intrusion detection using kNN classifier. The data gathering is performed, and then the data is pre-processed and possible malicious nodes are separated based on three factors namely, PTI, PTD and PDC that refer to packet transfer interval, packet transfer delay, and packet drop count (PDC), (PTD) and (PTI). The intrusion detection is carried out on the pre-processed data. Every vehicle maintains a score table based on their network use. This score table is updated every-time a vehicle tries to communicate with other vehicle using collaborative learning using kNN classifier. The updated score tables of all the vehicles are then merged and distributed to identify any intruder in the network.

Liang et al. [16], proposed a novel Intrusion Detection System for the dynamic and the wireless networks. The proposed IDS consists of an improved hierarchical self-organizing map-based classifier (I-GHSOM) and used feature extraction algorithm for extraction of various features from the messages of the participating vehicles for the training and testing purposes of the IDS. The proposed algorithm works on two prime features including difference in vehicles' position and difference in the traffic flow. The difference in vehicle's position is determined by calculating the range of distance among the various vehicles. The authors designed a semi cooperative mechanism and voting filter mechanism for determining the traffic flow. Two mechanisms including recalculation mechanism and the relabelling mechanism are also proposed in addition in order to obtain precision in the results of the classification. Simulation results have shown that the proposed intrusion Detection System performed better than other systems in terms of stability, accuracy, processing and efficiency.

Gao et al. [17] proposed a distributed network intrusion detection system for detecting Distributed Denial of Service (DDoS) attack. The proposed IDS employs big data technology for detecting intrusions in Vehicular Ad Hoc

Networks. The system comprised of two distinct phases including network traffic collection phase and detection phase. In network traffic collection phase, traffic feature collection is carried out by using micro-batch data processing. Authors employed Spark for speeding up the processing of data. In the detection phase, the system employs Random Forest based classification algorithm and HDFS was used for storing the suspicious nodes' details. The proposed system is evaluated through experiments and simulation and results have shown that the system performed better than other algorithms in terms of detecting false alarms, and accuracy in intrusion detection.

IV. Comparison

A comparison table that summarizes each paper reviewed is given below (Table 1). Every algorithm or method proposed for intrusion detection, employed different approaches and methods, focusing on different kinds of attacks or employed a combined approach of both host and network-based methods.

TABLE I
Comparison Table

Paper Title	Journal	Authors	Method Used	Attacks focussed	Contribution	Performance Analysis
"Distributed collaborative intrusion detection system for vehicular Ad Hoc networks based on invariant"	Computer Networks, 2020 – Elsevier	Zhou et al.	Reputation based clustering and Invariant analysis	Betrayal Attacks (Black hole, Denial of Service, Spoofing, gray hole)	This paper proposed an intrusion detection algorithm called DCDIV that employs an invariant based distributed collaborative framework where invariant is mined from the data from communication flow, traffic flow and the behavioural relationship state. The main focus of the paper is intrusion detection of the betrayal attacks in VANETs.	The performance of the proposed method has been compared with three detection methods- CEAP [18], AECFV [19] and HF-MCDM [20] and the comparison parameters are intrusion detection rate, detection time, and FPR[21]. According to the results, the DCDIV performs better than all the other three techniques.
"A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET"	Journal of Ambient Intelligence and Humanized Computing-2020, - Springer	Kolandaisamy et al.	Stream Position Performance Analysis	Distributed Denial of Service (DDoS) attack	This paper present SPPA, a stream position performance analysis-based intrusion detection system that uses a clustering-based attack detection. The cluster head is chosen by reputation method. The trace files maintained by the chosen cluster heads are used to perform the stream position analysis for each node. Next stage involves the calculations of the conflict Field, Conflict Data, and Attack Signature Sample Rate (CCA). Based on these calculations, intrusion detection is performed focusing on the DDoS attacks in VANETs.	The proposed model shows a high packet delivery ratio, decreased end-to-end delay, increased throughput ratio, increased attack detection rate, minimum attack detection time, lower routing overhead and lower false classification ratio.
"Hybrid Algorithm to Detect DDoS Attacks in VANETs"	Wireless Personal Communications, 2020- Springer	Adhikary et al.	SVM kernel methods-AnovaDot and RBFDot	Distributed Denial of Service (DDoS) attacks	The paper proposes a hybrid algorithm that is a combination of two SVM kernel methods, namely AnovaDot and RBFDot for DDoS detection. The proposed hybrid algorithm works by combining the two algorithms. Firstly, the AnovaDot is employed for training the model by using a dataset that contains the mixed data of both the normal and DDoS attacks. The predictions obtained from this model are then inserted into the RBFDot along with the same dataset to train the model. The obtained dual trained model called as hybrid model is then used to predict and detect the DDoS attacks and VANETs. The paper uses	The performance of the proposed method has been compared with SVM kernels-based algorithms taken individually- AnovaDot and RBFDot. The proposed hybrid model has shown improved accuracy, improved prediction, high performance, and produced minimum error rate.

					various features including delay, jitter, collision, throughput, and packet drop.	
"T-BCIDS: Trust-Based Collaborative Intrusion Detection System for VANET"	National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), 2020- IEEE	Nandy et al.	Trust based mechanism, kNN non-linear classsifier	All intrusive activities	The paper proposed a trust-based collaborative intrusion detection system for Vehicular ad hoc Networks. The system used a local IDS based on k-nearest neighbors non-linear classifier and a collaborative learning environment for intrusion detection. The system works by maintaining a score	The proposed framework seems to be very effective in detecting intrusions. Use of kNN classifier for intrusion detection is a simple and effective technique that is quick and provides high accuracy. Hence the system will be accurate as well as time saving.
"A Novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) based on Differences of Traffic Flow and Position"	*A.* **Applied Soft Computing, 2020- Elsevier**	Liang et al.	Feature Extraction	All attack types	The proposed IDS consists of an improved hierarchical self-organizing map-based classifier (I-GHSOM) and used feature extraction algorithm for extraction of various features from the messages of the participating vehicles for the training and testing purposes of the IDS. It works on two prime features including difference in vehicles' position and difference in the traffic flow. The authors designed a semi cooperative mechanism and voting filter mechanism for determining the traffic flow. Two mechanisms including recalculation mechanism and the re-labelling mechanism are also proposed in addition in order to obtain precision in the results of the classification.	The performance of the proposed method has been compared with the works of Yan et. al. [22] and Yu et. al. [23] and others comparison metrices include true and false detection rates, average processing time, uncertainty rate and average number of output messages. The results have shown that the proposed system works better than most of the other IDS with an accuracy rate that reaches upto 99.69%.
"A Distributed Network Intrusion Detection System for DDoS Detection in VANET"	*B.* **IEEE Access- 2019**	Gao et al.	Big Data Technology	Distributed Denial of Service (DDoS) attack	Gao et al. proposed an IDS that employs big data technology for detecting intrusions in VANETs. The system comprised of two distinct phases including network traffic collection phase and detection phase. In network traffic collection phase, traffic feature collection is carried out by using micro-batch data processing. Authors employed Spark for speeding up the processing of data. In the detection phase, the system employs Random Forest based classification algorithm and HDFS was used for storing the suspicious nodes' details.	Naive Bayes, SVM, Logistic Regression, XGBoost were used for performance evaluation of the proposed IDS. The proposed NIDS performed better on various metrices with accuracy rate of 99.95% and a lowest False Alarm Rate of 0.05%.

V. Conclusions

Security in VANETs is a major issue that attracted many researchers and academicians. One small security breach can cause a big damage in case of VANETs as in this case human lives are involved. Intrusion Detection Systems (IDS) are employed in VANETs in order to detect and identify any malicious activity in the network [24]. The IDS works by analysing 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. In this paper Intrusion Detection systems are discussed in detail. We discussed about the classification of IDS based on various factors and then the architecture of IDS is explained. We then presented some of the recent and important intrusion detection algorithms and then compared them.

There are several open issues that need to be addressed in IDS implementation in practical VANET systems. Various existing machine learning based intrusion detection systems involve massive computations and a huge amount of training data is needed. The features extraction also is a complex task in such systems with high communication overhead.

With the growing technology, variability is also seen in attacks, their methods and types. There is a need of continuous new research to be carried out in the field as

attacks are also evolving with time. Among the algorithms we covered in this paper, almost all of them try to detect intrusions in VANETs but covering all attacks altogether is a complicated task.

REFERENCES

[1] J. Noh, S. Jeon, and S. Cho, "Distributed Blockchain-Based Message Authentication Scheme for Connected Vehicles" *Electronics*, vol. 9, 2020.

[2] M. Baqer, and A. Krings, "Reliability of VANET Bicycle Safety Applications in Malicious Environments" *27th Telecommunications Forum (TELFOR),* pp. 1-4. IEEE, 2019.

[3] R. G. Engoulou, M. Bellaíche, S. Pierre, A. Quintero, "VANET security surveys". *Computer Communications*, vol. 44, pp. 1–13, 2014.

[4] Chaudhary, Alka, V. N. Tiwari, and Anil Kumar. "Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc networks." *2014 IEEE International Advance Computing Conference (IACC)*. IEEE, 2014.

[5] R. Nandakumar K. Nirmala "Security Challenges in Mobile Ad Hoc Networks - A Survey" Australian Journal of Basic and Applied Sciences, Vol. 10(1), pp. 654-659, January 2016.

[6] Chaudhary, Alka, Anil Kumar, and V. N. Tiwari. "A reliable solution against packet dropping attack due to malicious nodes using fuzzy logic in MANETs." *2014 International Conference on Reliability Optimization and Information Technology (ICROIT)*. IEEE, 2014.

[7] M. Aloqaily, S. Otoum, I. Al Ridhawi, and Y. Jararweh,. "An intrusion detection system for connected vehicles in smart cities". *Ad Hoc Networks*, *90*, 101842, 2019.

[8] Chaudhary, Alka. "Mamdani and sugeno fuzzy inference systems' comparison for detection of packet dropping attack in mobile ad hoc networks." *Emerging technologies in data mining and information security*. Springer, Singapore, 2019. 805-811.

[9] C. Azad, and V. K. Jha, "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, 2013.

[10] A. Lazarevic, V. Kumar, and J. Srivastava, "Intrusion detection: A survey" *Managing Cyber Threats* (pp. 19-78). Springer, Boston, MA, 2005.

[11] P. K. P. Dorosz, "Intrusion Detection System.s (IDS) Part 2 - Classification;methods; techniques". Available: TechGenix. http://techgenix.com/ids-part2-classification-methods-techniques/, June 14, 2017.

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

[13] R. Kolandaisamy, R. M. Noor, I. Kolandaisamy, I. Ahmedy, M. L. M. Kiah, M. E. M., Tamil, and T. Nandy, "A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET". *Journal of Ambient Intelligence and Humanized Computing*, 1-14, 2020.

[14] K. Adhikary, S. Bhushan, S. Kumar, and K. Dutta, "Hybrid Algorithm to Detect DDoS Attacks in VANETs". *Wireless Personal Communications*, *114*(4), 3613-3634, 2020.

[15] T. Nandy, R. M. Noor, M. Y. I. B. Idris, and S. Bhattacharyya, ""T-BCIDS: Trust-Based Collaborative Intrusion Detection System for VANET". *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)* (pp. 1-5). IEEE.0, February 2020.

[16] J. Liang, J. Chen, Y. Zhu, and R. Yu, "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, 2019.

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

[18] O. A. Wahab, A. Mourad, H. Otrok, and J. Bentahar, "CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks". *Expert Systems with Applications*, *50*, 40-54, 2016.

[19] H. Sedjelmaci, and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks". *Computers & Electrical Engineering*, *43*, 33-47, 2015.

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

[21] Chaudhary, Alka, V. N. Tiwari, and Anil Kumar. "A cooperative intrusion detection system for sleep deprivation attack using neuro-fuzzy classifier in mobile ad hoc networks." *Computational Intelligence in Data Mining-Volume 2*. Springer, New Delhi, 2015. 345-353.

[22] S. Yan, R. Malaney, I. Nevat, and G. W. Peters, "Optimal information-theoretic wireless location verification". *IEEE Transactions on Vehicular Technology*, *63*(7), 3410-3422, 2014.

[23] B. Yu, C. Z. Xu, and B. Xiao, "Detecting sybil attacks in VANETs". *Journal of Parallel and Distributed Computing*, *73*(6), 746-756, 2013.

[24] Chaudhary, Alka, V. N. Tiwari, and Anil Kumar. "A new intrusion detection system based on soft computing techniques using neuro-fuzzy classifier for packet dropping attack in manets." *International Journal of Network Security* 18.3 (2016): 514-522.