Proceedings of the Fifth International Conference on Trends in Electronics and Informatics (ICOEI).
IEEE Xplore Part Number:CFP21J32-ART; ISBN:978-1-6654-1571-2

Sum up Work on Intrusion Detection System in Vehicular Ad-hoc Networks

[1]Pooja Badukale
Department of Electronics Engineering
Amravati,Maharashtra, India
poojabadukale22@gmail.com

[2]Samrat Thorat
Department of Electronics Engineering
Amravati,Maharashtra, India
samratthorat@gmail.com

[3]Dinesh Rojatkar
Department of Electronics Engineering
Amravati,Maharashtra, India
dinesh.rojatkar@gmail.com

***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 attacks so that 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 rhis 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

2021 5th International Conference on Trends in Electronics and Informatics (ICOEI) | 978-1-6654-1571-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICOEI51242.2021.9452961

I. INTRODUCTION

Vehicular communication is the vast area to detect the traffic attacks, intrusion detection, and many more. Nowadays, the main challenge associated with this domain is 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.

This research paper is organized as follows. Section 2, discusses about the vehicular ad hoc network. Section 3, presents the background details and discusses about the different technologies related to machine learning and that are used in VANET from other existing systems. Section 4 discusses about the fuzzy logic techniques in VANETs. Finally, Section V concludes the discussion carried out in the proposed study.

II. INTRUSION DETECTION SYSTEM

Vehicular communication has the main aim to detect various traffic attacks and prevent them by using Intrusion Detection System (IDS), having three main components shown in Figure 1 such as data collection, vectorization and classification engine. IDS also include one main rationale to detect the vehicular attacks of the system, which is known or unknown. Generally IDS depends on some hardware components. Running such hardware components require consistent and robust software [2].

Fig. 1. Main components of IDS

In figure 1, 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 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:

Vehicular communication systems are complex and it has more number of errors.

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 [1].

III. RELATED WORK

Gozde Karatas et. al. [3] proposed the Intrusion Detection System [IDS] 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.

Akash Garg et. al. [4] presented the misuse-based or signature-based IDS that work when data is sent to the network and further the server verifies these data. If any harsh data is obtained, then server discards the packet else carry forward it to the network. Next, the data arrived at the server is examined by using high accuracy tools to detect network packet from the database and then discards the network packet else it will move the data to the system network.

Authorized licensed use limited to: UNICAP - Universidade Católica de Pernambuco. Downloaded on November 12,2024 at 20:12:46 UTC from IEEE Xplore. Restrictions apply.

In [5], 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 [6] 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. [7] 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 [8], 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. [10] 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.

IV. CATEGORIES OF 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 [11].

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.

V. MACHINE LEARNING TECHNIQUES

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.

K- Means Algorithm: The K-mean algorithm can be used to develop an intrusion detection system. [12] This algorithm does not specify the number of clusters and the clusters are created using the optimal value based on fitness function to help identify the type of attack.

Support Vector Machine (SVM): In [14] implemented SVM against network intrusion using MATLAB. KDD dataset is used as bench market dataset for intrusion detection and shows SVM is limited because they need long training time to show the result.

Convolutional Neural Network (CNN): CNN is deep learning algorithm used to classify images and recognize the correct one with high accuracy. This model is made up of neurons with learnable data which is pass from various layers like fully connected layer, pooling, filters and functions. In [15] give the comparison of deep learning CNN with DBN. According to the results the performance of CNN shows that the accuracy and detection of CNN model in intrusion detection is slightly higher than the DBN model.

Long short term memory (LSTM): Long short-term memory network are a recurrent neural network capable of learning order in sequence of prediction problem. LSTM is complex area of deep learning. Supriya P. Shende et. al. [16] conclude that the binary as well as multiclass classification for detection using LSTM in network security. According to author accuracy of LSTM in deep learning network security for binary 99.2% and multiclass 96.9% which is high.

VI. DATA SET USED

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

Authorized licensed use limited to: UNICAP - Universidade Católica de Pernambuco. Downloaded on November 12,2024 at 20:12:46 UTC from IEEE Xplore. Restrictions apply.

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, etc.

VII. PROPOSED ARCHITECTURE

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.

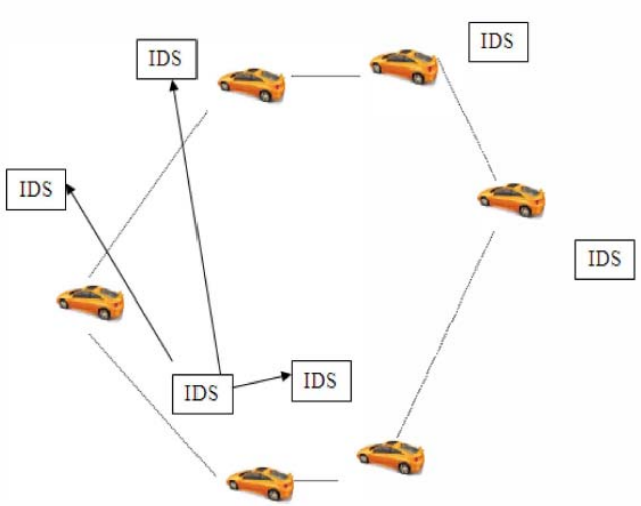

Fig. 2. Intrusion Detection System framework in VANET

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.

TABLE I. SUMMARY OF PREVIOUS RESEARCH OF IDS

Authors	Technique/Methods	Dataset	Attack Type	Contribution	Advantage
M. Ali Aydın et. al. [1]	hybrid IDS (PHAD + NETAD)	IDEVAL	Anomaly	Proposed the hybrid approach for anomaly detection using packet header and network traffic anomaly based on intrusion detection system.	More than 27 type of attack detected. More powerful than signature based IDS. Unknown attack has been detected
Qingqing Zhang et. al. [2]	Data Mining	KDD	Scan Attack DOS	Proposed the hybrid approach for intrusion detection based on data fusion and data mining techniques.	Highly efficient in real time detection False positive rate has been reduced More Flexible
Gozde Karatas et.al. [3]	ANN	KDD Cup'99	Normal DOS R2L U2R	Implemented the intrusion detection system based on the neural network	Minimize the error rate. Great Execution
Tuan A Tang et. al. [6]	DNN	NSL-KDD	DDoS DOS R2L U2R	Proposed the intrusion detection system based on deep learning technique and analyzes the result in NIDS framework	Good detection Rate
John Bellardo et. al. [8]	802.11 MAC layer	--	DOS	Proposed the intrusion detection based on 802.11 MAC layer and analyze the vulnerabilities.	Highly Efficient in detection. Low Overhead

TABLE II. SUMMARY OF VARIOUS TYPES OF IDS TECHNIQUES

IDS	Model	Technique	Method
Watchdog Pathrater	Stand-alone	• Observe the nodes next to each other • To find optimal rout for node it	Monitoring of Router Nodes

Authorized licensed use limited to: UNICAP - Universidade Católica de Pernambuco. Downloaded on November 12,2024 at 20:12:46 UTC from IEEE Xplore. Restrictions apply.

		must synchronize	
Confidant	Distributed Cooperative	• Observe the nodes next to each other • Observe side-by-side nodes • To find optimal rout for node it must synchronize • malicious node must be detected and removed	Reputation
CORE	Distributed Cooperative	• Game Theory • Observe the nodes next to each other • Detecting of optimal rout • malicious node must be detected and removed	Reputation
Zhang et Lee IDS	Distributed Cooperative	• Detection locally and independently • Detect globally and cooperatively by voting	Cooperative Detection
ZBIDS	Clustered	• Markove Chaine	Cooperative Detection
SNORT	Distributed Cooperative	• Pattern Matching	Signature
Jaydip Sen clustered IDS	Clustered	• Detecting the Local Intrusion	Signature
Sterne IDS	Clustered	• Data Fusion/Integration/Reduction	Signature

The table 2 shows the comparative summary of various intrusion detection techniques.

DISCUSSION

In this studying the different intrusion detection techniques proposed in the previous research and finally conclude that most of the existing intrusion detection system have been distributed and are based on various types of anomaly detection. In this studying the different intrusion detection techniques proposed in the previous research and finally conclude that most of the existing intrusion detection system have been distributed and are based on various types of anomaly detection. In addition, machine learning techniques have been used to detect intrusions as these machine learning techniques more efficiently address search and analysis issues with a whole range of resources.

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 their datasets publicly available for review. Intrusion detection systems can create preventive techniques to strengthen network security.

In future, the aim is to design the framework for intrusion detection in VANET. 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] M. Ali. Aydin, A. Halim Zaim and K. Gokhan Celyan, “A hybrid intrusion detection system design for computer network security”, Computer and Electrical Engineering 35(2009) 517-526.

[2] Qingqing Zhang, Hongbian Yang, kai Li and Qian Zhang, “Research on the intrusion detection technology with hybrid model”, 2nd Conference on environmental science and information application technology, IEEE, 2010.

[3] G. Karatas and O. K. Sahingoz, "Neural network based intrusion detection systems with different training functions," 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 2018, pp. 1-6, doi: 10.1109/ISDFS.2018.8355327..

[4] A. Garg and P. Maheshwari, "A hybrid intrusion detection system: A review," 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 2016, pp. 1-5, doi: 10.1109/ISCO.2016.7726909.

[5] F. Gonçalves et al., "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, doi: 10.1109/ICUMT48472.2019.8970942..

[6] 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, doi: 10.1109/WINCOM.2016.7777224.

Authorized licensed use limited to: UNICAP - Universidade Católica de Pernambuco. Downloaded on November 12,2024 at 20:12:46 UTC from IEEE Xplore. Restrictions apply.

[7] K. 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, Second Quarter 2011, doi: 10.1109/SURV.2011.041110.00022.

[8] Bellardo, John & Savage, Stefan. (2003). 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. Proceedings of 12 USENIX Security Symposium. 2-2.

[9] 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, doi: 10.1109/MWC.2004.1269717.

[10] 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, First Quarter 2014, doi: 10.1109/SURV.2013.050113.00191.

[11] Adetunmbi, Adebayo & Adeola, S.Oladele & Abosede, D.O.. (2010). Analysis of KDD '99 Intrusion Detection Dataset for Selection of Relevance Features. Proceedings of the World Congress on Engineering and Computer Science. 1. 20-22.

[12] 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, doi: 10.1109/NANA.2018.8648766..

[13] 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, doi: 10.1109/ICACCI.2018.8554710..

[14] 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.

[15] 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, doi: 10.1109/ITNEC.2019.8729261..

[16] Shende, Supriya. (2020). Long Short-Term Memory (LSTM) Deep Learning Method for Intrusion Detection in Network Security. International Journal of Engineering Research and. V9. 10.17577/IJERTV9IS061016..

Authorized licensed use limited to: UNICAP - Universidade Católica de Pernambuco. Downloaded on November 12,2024 at 20:12:46 UTC from IEEE Xplore. Restrictions apply.