Classification Approach for Intrusion Detection in Vehicle Systems

Abdulaziz Alshammari, M. A. Zohdy, George Corser
Department of Electrical and Computer Engineering, Oakland University, Rochester, MI, USA 2
Email: aaalshammari@oakland.edu, zohdyma@oakland.edu , gpcorser@svsu.edu

Abstract
Vehicular ad hoc networks (VANETs) enable wireless communication among Vehicles and Infrastructures. Connected vehicles are promising in Intelligent Transportation Systems (ITSs) and smart cities. The main objective of VANET is to improve the safety, comfort, driving efficiency and waiting time on the road. VANET is unlike other ad hoc networks due to its unique characteristics and high mobility. However, it is vulnerable to various security attack due to the lack of centralized infrastructure. This is a serious threat to the safety of road traffic. In Vehicle Systems. The Controller Area Network (CAN) is a bus communication protocol which defines a standard for reliable and efficient transmission between in-vehicle parts simultaneously. The message moves through CAN bus from one node to another node, but it does not have information about the source and destination address for authentication. Thus, the attacker can easily inject any message to lead to system faults. In this paper, we present machine learning techniques to cluster and classify the intrusions in VANET by KNN and SVM algorithms. The intrusion detection technique relies on the analysis of the offset ratio and time interval between the messages request and the response in the CAN.

Keywords
CAN-Bus, IDS, KNN, SVM, Machine Learning, DoS Attack, Fuzzy attack

I. INTRODUCTION

Advancement in technology in has brought about the concept of intelligent vehicles which are considered to more efficient and safer for the users. Intelligent vehicles tend to be connected to other vehicles, roadside infrastructure such as the traffic management system and the internet, hence making them to be among the Internet of Things. However, such high levels of connectivity have meant that intelligent vehicles are at risks of cyber-attacks which might interfere with different aspects of the vehicle such as its communication systems, endangering the security and privacy of the vehicle as well as putting the lives of its passengers at risk [5,6,7, 29].

Connected vehicle technology has always been aimed at solving the challenges that are occasionally experienced with intelligent transport systems. An Intelligent Transport System usually allows intelligent vehicles to be in a position to communicate with the roadside infrastructure, other vehicles on the road and other road users. The communication system of an intelligent vehicle is usually referred to as Vehicle-to-Everything (V2X) or it is also referred to as the VANET, an abbreviation for Vehicular Ad hoc Networks [30]. An ordinary VANET communication system is usually responsible for three main types of communication to be considered a smart automotive. Those types of communication are Vehicle-to- Infrastructure(V2I), Vehicle-to-Vehicle (V2V), and Vehicle-to-Pedestrian (V2P). V2I involves the vehicle communicating with the roadside infrastructures such as location sensors and other traffic monitoring systems. V2V involves a smart automobile being able to share information with other vehicles on the road. V2P involves the communication between the vehicle and pedestrians on the road. A cyber-attack on this communication system of a specific car or the ITS system is likely to result in endangering the security and privacy of the vehicle as well as put the lives of its passengers at risk [31,35].

There have been numerous concerns about the privacy and security of intelligent vehicles and the intelligent transport systems with various attacker models for smart vehicles being experienced. Among these concerns are cyber security threats on the VANET communication system where cyber attackers may exploit any potential weaknesses within the system to jam and spoof its signal. This would result in the whole V2X system being affected through deceptive signaling and delaying of the signal so as to ensure that the message transmitted is distorted and does not achieve its intended purposes [32,33].

Other security threats faced by smart automotive may include hacking through the internet, as connected vehicles have access to the internet, or physical access to the vehicle intelligence system [34]. For example, in 2016 Charlie Miller and Chris Valasek, who are security experts, wirelessly hacked the intelligence system of the Jeep Cherokee. Miller and Valasek were able to demonstrate that the Jeep Cherokee intelligence system had security vulnerability when they were able to compromise its entertainment system, steering and brakes, and its air conditioning system while the driver of the car was still driving[36]. Another example is with the Nissan Leaf, where its companion application became exploited by hackers using its identity number that is usually printed on the vehicles windows. This vulnerability allowed the hackers to take control of the heating and air conditioning system.

Tesla Motors is considered to have the best cyber security on its intelligent vehicle system due to the amount of resources and time that is continually spent on improving it. However, researchers were able to gain control of the Tesla Model S where they discovered a security vulnerability that would allow an attacker to open the doors as well as start and drive away with the car. However, the attackers would require having physical access to this car if they were to execute such a plan. For this reason, the risk was impractical, though Tesla addressed this vulnerability immediately.

CAN Bus

Controller Area Network (CAN) is a bus communication protocol that can be utilized as a standard for reliable and efficient transmission between vehicle nodes in real time. In such network, broadcast messages must transmit from one node to another on the bus and there is no information about the source and the destination address for the validation. This security hole leads to inject any message by an attacker that can course to system malfunction.

ECU is an embedded system which used in today’s vehicles to control the engine and other components’ functions. It is a computer with inside pre-programmed and programmable computer chips that is almost like a personal computer. The car’s engine computer ECU makes the engine function the engine using sensors to control all engine functions [38,39]. The engine ECU is the most vehicles is contacted to onboard diagnostic connector and then report all diagnostic information to all other ECUs. This technique is helping in reducing the amount of wire that is needed or not needed to go to every ECU in order to test them [40]. Tuohy et al. [41] stated in their analysis research that intra-vehicle networks demonstrate that each electronic sensor in a vehicle requires a new ECU device and subsystem and calls for standardization of automotive networks in intra-vehicular networks. There are many V2V wireless communication protocols like vehicular collision warning communication protocol, direction-aware broadcast forwarding routing protocol, etc. [42]. The study [43] introduced a comprehensive state of the art survey on Integrated Vehicle Dynamics Control (IVDC) where they discuss several methodologies of IVDC and control strategies of coordination between ECU subsystems. Inter-vehicle communications through media like infrared and microwave using various kinds of protocols, enable vehicles to obtain data to deliver road traffic safety and efficiency, which is otherwise impossible to measure with on-board sensors [44]. Reliability of inter-vehicle communication is one of the main aspects to ensuring wide range deployment of cooperative vehicle systems. The inter-vehicle communication allows vehicles to exchange message within a short broadcast range [45,46]. There are different communication protocols are established to support the communication. The most important protocol is Controller Area Network (CAN). It is a serial-bus communication protocol that supporting to connect sensors and actors with ECUs [47]. ECUs can be attacked and intruded. Bypassing network security protections in vehicular systems, and embedding malicious code are instances of attacks that can avoid a large number of safety-critical systems. An attacker can get remote code execution of ECU in automotive vehicles through interfaces like Bluetooth. The attacker can influence the behavior of vehicles such as steering braking, acceleration and display, etc.

As we mentioned earlier, due to the weakness of in-vehicle, attackers will be strongly motivated to exploit the vulnerabilities of CAN Bus. In this work, we investigated two types of attacks that occurs in-vehicle: DoS and Fuzzy attacks. We proposed a classification method to detect these kinds of attacks.

DoS attack

In DOS attacks the server of the network is flooded with too many requests. As VANETs are using wireless technologies, it is easy to launch a DOS attack very easily. As a result of it, VANET service receivers may not receive, requested services at real time and lead to catastrophic results. [01, 02]

In DOS attacks, the attacker can inject high priority messages in a very short period of time into the bus. Not only that, it is easy to gain control of a node in the network by the attacker. Therefore, it is easy to send the highest priority identifiers. Thus, the network is flooded very quickly and eventually will lead to accidents and on.

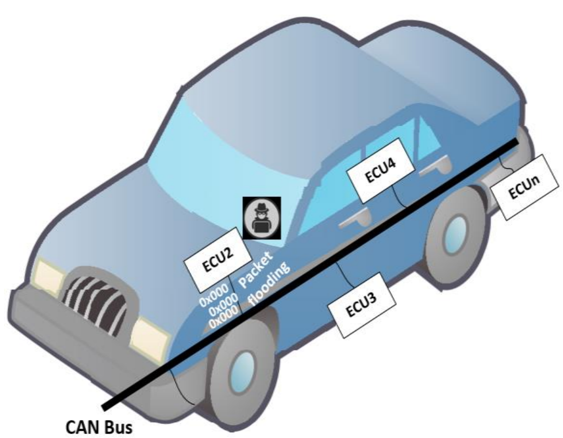

Fig. 1 DoS attack scenarios on in-vehicle network

Fuzzy attack
In a fuzzy attack the attacker injects messages of randomly spoofed identifiers with arbitrary data. As the result of it, all nodes of the network receive lots of functional messages and it may lead to malfunction of the network. This may lead to mal behavior in vehicles.
To launch a fuzzy attack, the attacker observed in vehicle messages and select the target identifier/s. This may course to unexpected behaviors. Following the figure shows the possible damages to the CAN in such attack

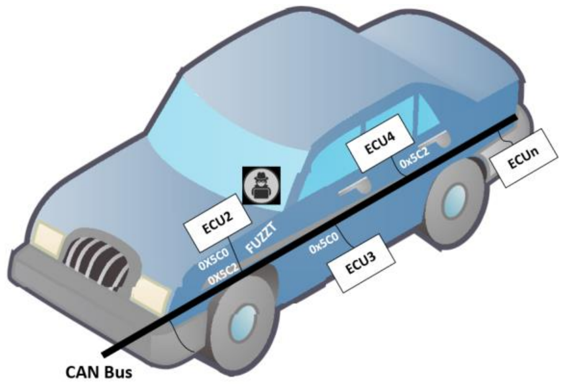

Fig. 2 DoS attack scenarios on in-vehicle network

The paper is organized as follows: Section 2 related works in CAN Bus and IDS in machine learning, while the proposed detection model is illustrated in Section 3. Then in Section 4, results and performance and evaluation are presented and discussed to demonstrate the effectiveness of the proposed technique. Finally, the conclusions and future work are provided in Section 5

I. RELATED WORKS

A. CAN Bus

Recently, the research into CAN bus security has grown because of some demonstrations of the vulnerabilities of in-vehicle networks. Previous approaches to detecting attacks on the CAN bus have mainly been based on timing information. CAN packets are normally transmitted at a regular frequency, so controlling frequency detection to defense against most attacks [11,19,21]. There are several approaches have been provided to be a very effective at detecting inserted and missing packets [20,8,17,9,10].

There are many of researchers have been proposed anomaly detection methods for connected vehicles. The most of these methods and proposes were related to Controller Area Network (CAN Bus). They are based on characteristics of in-vehicle architectures and networks. Manufacturers must pay attention to CAN Bus standard weakness that might impact the security of vehicles. CAN is a standard that allows communication between numerous mechanisms in modern automobiles.

Corey Thuen, senior security consultant at IOActive, explained the attackers can exploit many vulnerabilities in the technology systems of modern vehicles and 27% of these weaknesses due to exploit the CAN protocol. Exploit the CAN is lead to control the connected car.

The goal of designing CAN is for half-duplex and high-speed transmission bus inter vehicle network. It delivers up to 1Mbps communication rate [12]. The automotive manufactures are commonly used CAN protocol. In CAN, each Electronics Control Unit (ECU) send a message to the vehicle network using a data packet. There is no clear destination for CAC packet. Therefore, ECU send the message alone with its ID number and then the ECU on the destination retrieves the message by sender ID.

The are four mains frames inside in the communication inside CAN: the data frame, the remote frame, the error frame and the overload frame. Most of the communication comes over data frames which creates of the data field, acknowledge field, arbitration field, and Cyclic Redundancy Check (CRC) field. Also, the arbitration field comprises an 11-bit identifier field and a Remote Transmission Request (RTR) field, that is used in arbitration and must be set to a foremost bit of a data frame. It will follow by 8-byte, then the cycle redundancy check field. The figure[***] shows the structure of the data frame.

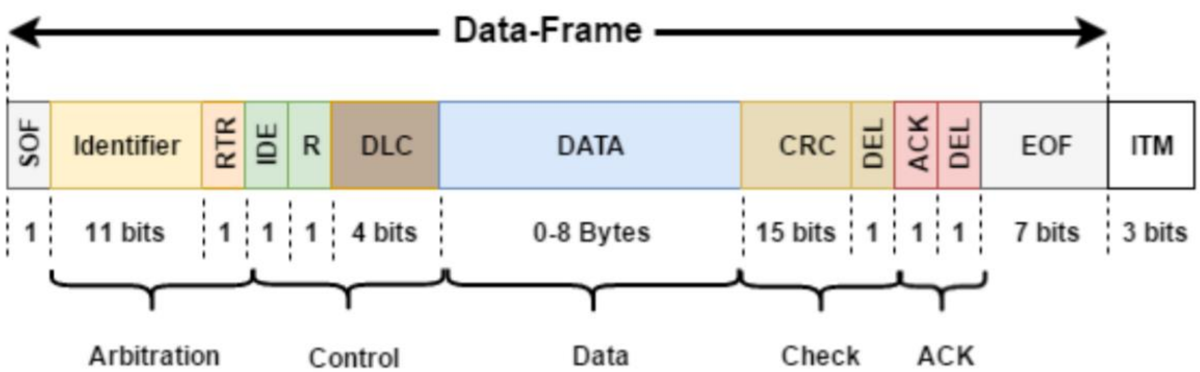

Fig. 3 CAN data frame structure

There are many researches have introduced to solve the vulnerabilities of CAN-Bus. Cho and Shin [14] proposed a Clock-based IDS (CIDS) based Intrusion Detection system to protect in-vehicle Electronic Control Units (ECUs) and mitigate attacks in-vehicle network. The CIDS is able to extract clock skews from message intervals, fingerprints the transmitter ECUs, and models their clock behaviors using Recursive Least Squares (RLS). Then, CIDS could detect intrusions by

CUSUM analysis based on the thus-constructed model. They clarify that the experiment applied on real vehicles and CIDS is able to detect various types of in vehicle network intrusions.

Wand and Sanjay [24] proposed VeCure applied security method for vehicle systems, which is able to solve the message authentication vulnerability of the CAN Bus. The characteristics of VeCure method are. It’s compatible with the modern connected vehicle systems. Besides, it can provide a trust structure. It is considered a novel message authentication method with offline computation ability to decrease the delay and cost of online message processing. VeCure provides a message authentication on the CAN in order to isolate the spoofed messaged injected from a targeted or compromised ECU and OBD-II port

B. Intrusion Detection with Machine Learning

Intrusion detection methods have been deliberate to help the network prevent malicious attacks. Machine learning has been studied extensively in intrusion detection in VANET. In literature quite number of effective intrusion detection techniques are developed based on machine learning techniques, based on the statement that the forms of the attack packets differ from those the normal packets like other ad hoc network types.

Cho at el. [13] proposed an anomaly-based intrusion detection system (IDS), they called it Clock-based IDS (CIDS). This scheme measures and exploits the intervals of periodic in vehicle message for fingerprinting ECUs. So, they use clock skew to confirm ECUs. There are a lot of attack come from an unusual source: it could be a Foreign ECU or a compromised source that typically sends difference message. In case the ECU sending malicious packets can identified due to its clock skew is skew is unlike the authentic ECU. The adversary, however, able to match clock skews and overcome this method. When the attacks compromised ECU and it could not detect anything, is regular system of the IDs of the malicious packets.

Other approaches have discussed detection attack with packet data. Detection insertion attacks by using packet message entropy [15]. The drawback of this method was not estimated against attacks that influence only the message contents of a packet. Markovitz at el. [16] introduced a novel domain-aware anomaly detection system for in-car CAN bus traffic. They discovered the presence of semantically-meaningful content field, Multi-Value field and counter or sensor fields through inspection of real CAN bus communication. This method could not have assessed with attack situations. Another approached done by Taylor al el. [18] proposed an anomaly detector based on a Long Short-Term Memory neural network to detect CAN-bus attacks. They system work by learning to predict the coming data word from any destination by bus. The bits that highly in the actual next word are flagged as anomalies. Their detection system is increasing in time CAN bus traffic rather than different data stream.

There is not a serious security system need for traditional vehicles because there is no network to communicate with external network. However, Controller Area Network (CAN) connect the parts of vehicle together. Vehicles become computerized and connected to external networks. If the security is achieved, then safety will be achieved as well. It is important to detect and prevent the attacks in order to protect the safety of people. Therefore, there have been many researches are working in detecting and preventing attacks that target vehicles. Hoppe et al. [27] proposed a scheme for in-vehicle intrusion detection based on the investigation of the rate of messages. Due to the number of messages on CAN bus that includes the sum the normal and attacks messages, they analyzed the rates of messages per seconds in order to detect anomalous message rates.

Muter et al. [28] introduced a method for anomaly detection. The proposed technique proved that there is no false-positive error, but if attacker injects messages and could not outcome and break and effect the CAN , then their algorithm cannot detect the attack at all.

Fuad at el. [25] proposed an effective misbehavior detection model based on machine learning techniques. The methods has four phases: data acquisition, data sharing, analysis and decision making. They used Artificial Network (ANN) methods using the feed forward and the back-propagation algorithms. It works by classifying and training based on historical data from both normal or malicious data. They used a real traffic dataset which called(NGSIM), so that's making their model more effective.

Hortelano at el. [26] proposed evaluates the efficacy of watchdog modules for intrusion detection in VANETs. The scheme works by controlling all coming packets so the system could decide if there is attack or not. There are a lot of IDS was proposed based on watchdog module in vehicle systems. They introduced three contributions in their proposed system. First, they stated that this module is compatible protocol and can work with any protocol in ad hoc routing. Second, it is a high detection system and can work with low detection system. Finally, it can promise the prior properties and efficiency reducing the most of false positives and false negatives.

Van Herrewege et al. [22] proposed improve to CAN bus messages by adding a message authentication protocol. They stated that the standard authentication protocol is not appropriate to CAN bus. Also, they presented a CAN bus protocol "CANAuth" which is compatible lightweight message authentication protocol, but a pre-shared key need to be known by all the nodes that could making verify messages.

Matsumoto et al. [23] introduced a technique of preventing unauthorized data transmission in CAN. All data on the bus is monitored by a protected ECU. It broadcasts an error message when identifying a spoofed message, and that occurred before the unauthorized transmission is finalized. Most of previous researches investigate about message rate-based intrusion detection on CAN bus, so they need to gather a huge amount of CAN bus messages and the goal is to compute the distribution of a message. Therefore, the modern vehicles have limited computer pow for their devices in order to detect and response immediately. To solve this problem Song el al [11] suggest a light-weight intrusion detection scheme. The main contribution is simplifying detection algorithm to respond faster and reduce the usage of computing power.

II. The Proposed Intrusion Detection System

We propose an intrusion detection system that determines the intrusions in vehicles. We use two algorithms based on KNN and SVM to detect the DoS and Fuzzy attacks. Through the analysis, we use two car-hacking datasets: "DoS dataset" and "fuzzy dataset," which are provided by the Hacking and Countermeasure Research Lab (HCRL). These datasets came from real vehicles by connecting CAN traffic by the OBD-II port. Then, they got the performing of the message injection attacks. Each dataset has 300 intrusions of message injections and each intrusion achieved from 3 to 5 seconds. Each dataset needs from 30-40 minutes of the CAN traffic.
The DoS data set has 3,665,771 numbers of the messages, 3,078,250 messages are normal while 587,521 injected messages. It has 12 columns. Fuzzy dataset contains 3,838,860 rows of messages and 12 columns. It has 2,759,492 normal messages and 1,079,368 injected messages. In DoS attacks the injecting message occurs of '0x000' CAN ID, while in fuzzy attack Injecting messages are spoofed random CAN ID and DATA values. The 12 attributes are: Timestamp, CAN ID, DLC, DATA[0], DATA[1], DATA[2], DATA[3], DATA[4], DATA[5], DATA[6], DATA[7], flag. Table [1] shows the explaining of some attributes.

Table 1 Data attributes of CAN

Attributes	Recorded times
Timestamp	Data value by byte.
Data [0 – 7]	Data value by byte.
CAN ID	CAN ID message in HEX
DLC	# of data bytes
Flag	T or R T denotes injected message R denotes normal message

The structure of the tow datasets is similar, though they represent different types of attacks. The DoS dataset represents DoS attacks, where it involves injecting message of '0000' CAN ID every 0.3 millisecond, we note that '0000' is the most dominant. However, fuzzy attack dataset represents injecting messages of totally random CAN ID and Data vales every 0.0 milliseconds.

We mentioned before that both datasets are similar, so we applied the same preprocess on to both of them. First, we added appropriate header names to each dataset as they are unmarked with headers. Then, we removed unnecessary columns, which were the Timestamp as we do not have a time-series analysis. We removed the missing data as well. We also converted hexadecimal data into decimal format. Finally, we marked the normal messages with 1 and the injected messages with 0.

For classification, we used two algorithms of the most well-known classification techniques: Support Vector Machine and K-Nearest Neighbor. First, we made a preprocessing for data as we mentioned above. Then, we extracted the features of each dataset. After that, we implemented KNN and SVM, and we will explain how they work in the next step. The following figure shows our proposed model:

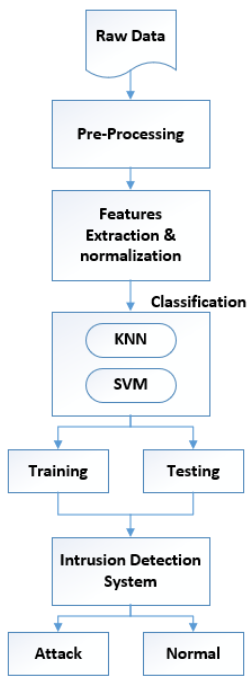

Fig. 4 Intrusion Detection Classification Model

A. K-Nearest Neighbor

There are various analysis algorithms used in machine learning. KNN is a non-parametric algorithm intended for classification and regression. It has various advantages over other machine learning algorithms: ease of interpreting algorithm's output, low calculation, and high predictive power [1]. It is a simple algorithm that stores all existing case and classifies new cases by a same measure such as distance functions. Any case in this algorithm is classified based on a majority vote of its neighbors, with the case being allotted to the class most common between its K-nearest measured by a distance function. For example, if K is an integer K = 1, then K is assigned to the class of its nearest neighbor [2]. Look at table [2].

Table 2 KNN

KNN algorithm
K-Nearest Neighbor
X: training data
Y: class label of X
X: unknown sample
Classify(X, Y, x)
For i= 1 to n:
Calculate the distance $d(X_i, x)$
End for
Calculate set I having indices for the k smallest distances
Return the majority label for {Yi, where i ϵ I }

B. Support Vector Machine (SVM)

SVM is a supervised machine learning algorithm, and it can be used for either classification or regression challenges [3,4]. However, it is mostly used in classification problems. Therefore, there are many applications of SVM like in E-commerce, Stock marketing, etc. Not like other machine learning algorithms, SVM is based on the concept of decision planes that defines decision boundaries. It is a type of graphical approach. Table 3 the explains of how SVM works.

Table 3 SVM

SVM algorithm
*
*

III. PRFORMANCE EVALUATION AND DISCUSSION

Through this analysis, we used Python, and the main reason we used python is because it has a free library for the Python programming language called Scikit-learn which helps a lot with machine learning. It delivers a range of supervised and unsupervised learning algorithms by a consistent interface in Python. It features various classification, regression and clustering algorithms including SVM, KNN, linear regression, etc. Actually, Scikitis is designed to interoperate with the Python numerical and scientific libraries like NumPy and SciPy. This library is focused on modeling data but not on loading, manipulating, and summarizing data. In order to detect the intrusive data, we planned to use clustering techniques like using K-means and K-medoids to detect the outlier sample and isolate it from the original data, but we received the data so we used the classification algorithms. Therefore, there is no signal processing and no noise, so we do not need to use a filter like Kalman.

The performance of any binary classifier can be evaluated based on four kinds of alarms:

- True Positive rate (T_p): correctly identified samples
- True Negative rate (T_n): correctly rejected samples
- False Positive rate (F_p): incorrectly identified samples

- False Negative rate (F_n): incorrectly rejected samples

These criteria are used to calculate some metrics as shown in the following equations (1) through (4):

The following equations (1) to (4) are used to calculate some matrices:

$$Accuracy = \frac{T_P + T_n}{T_P + T_n + F_P + F_n} \qquad (1)$$

$$F - score = \frac{2T_P}{2T_P + F_P + F_P} \qquad (2)$$

$$Percision = \frac{T_P}{T_P + F_P} \qquad (3)$$

$$Recall = \frac{T_P}{T_P + T_n} \qquad (4)$$

We split the data into two parts: 70% for training of dataset and 30% of dataset for testing. The following is the result of comparison between KNN and SVM for the four metrics in the fuzzy data set.

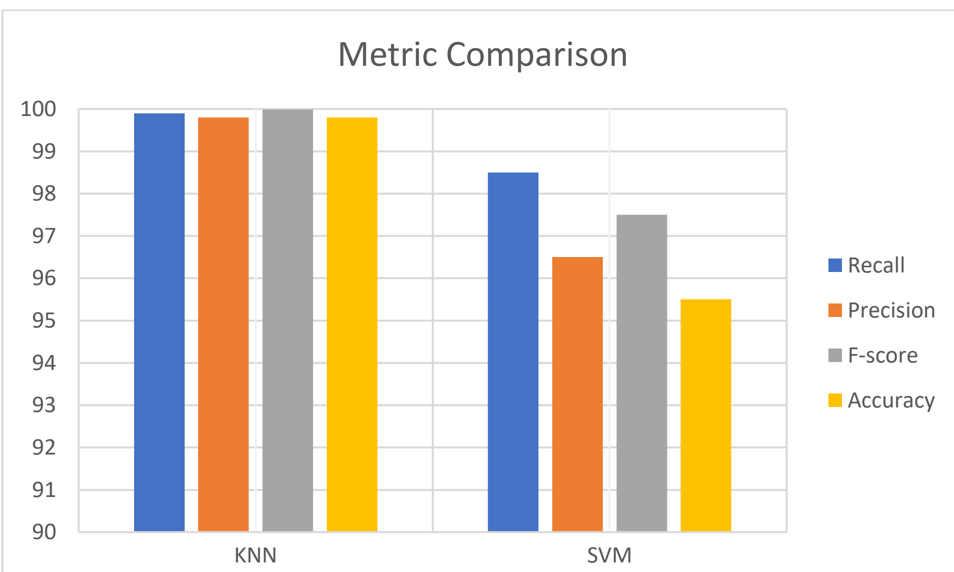

Fig. 5 Comparison between metrics for fuzzy dataset

The following figure represents the comparison between KNN and SVM for the DoS dataset

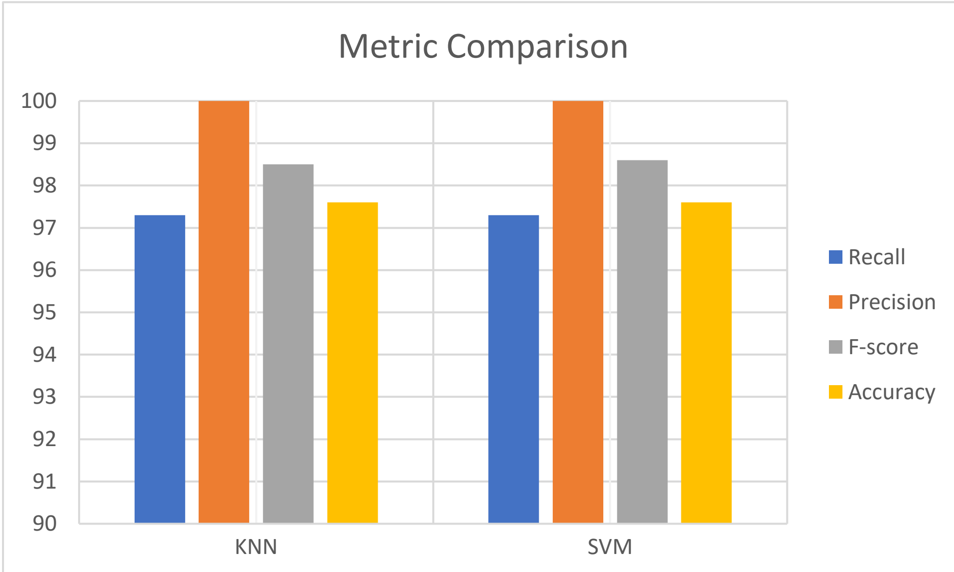

Fig 6 Comparison between metrics for DoS data set

The other significant factor we calculated is the time consumption. Figure 7 illustrates the time measures for KNN and SVM models. The x-axes represent the difference of the spilt of data set between training and testing, we splitted them as the following: 70% for training and 30% for testing, 80% for training and 20% for testing, and 90% for training and 10% for testing. The KNN model is left out because it need more than two hours to be completed. Unlike training, the testing time is almost the same for both.

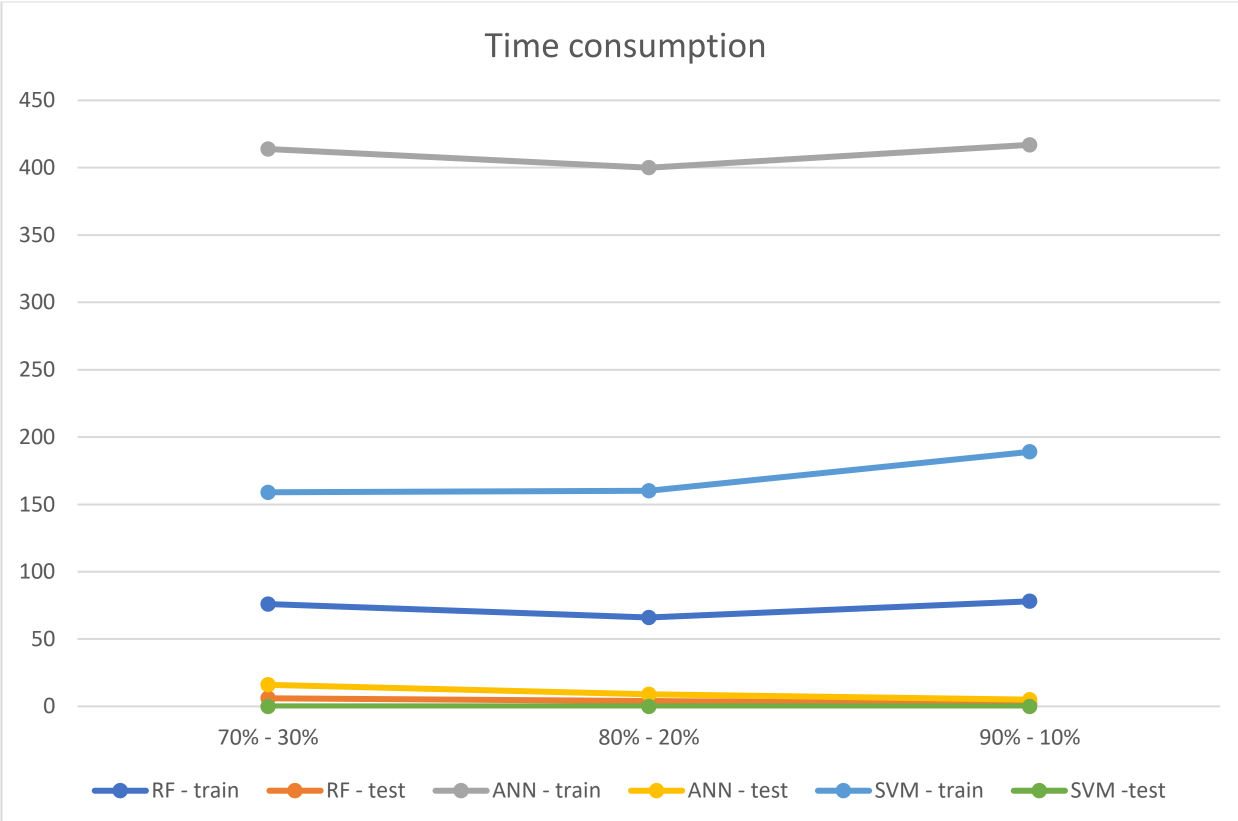

Fig. 7 Time consumption

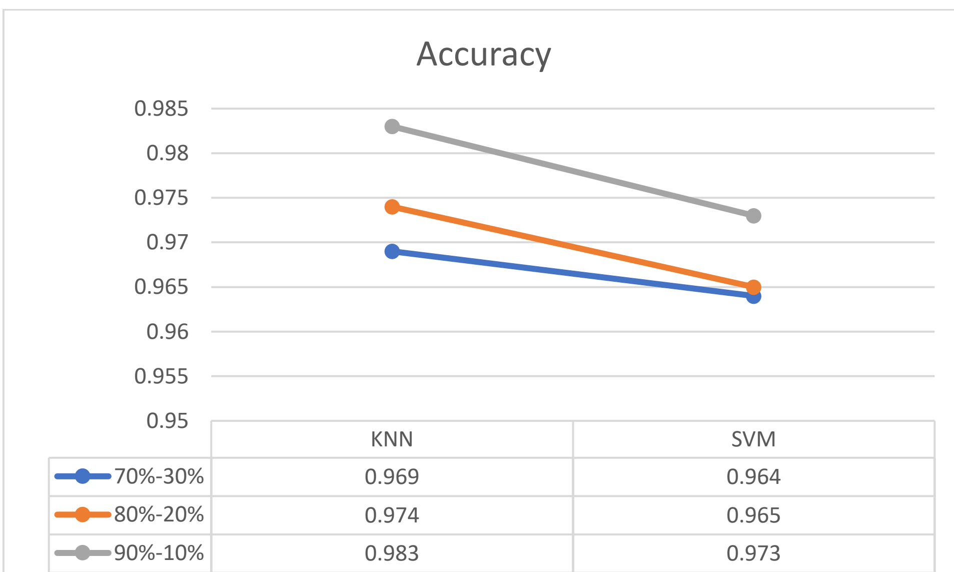

Fig 8 Accuracy

In the above figure, the accuracy of KNN and SVM for both data sets. It is clear that both of them have a high accuracy of more than 96%, however, KNN gave much better accuracy. We note that when we increase the percent of training in the data sets, the accuracy is much better.

The last factor is F-score, and it is almost similar to the accuracy. However, the accuracy situation is a little bit better than what we got in F-score. KNN is better than SVM, but the difference is not big. In general, they have almost the same, about 93%.

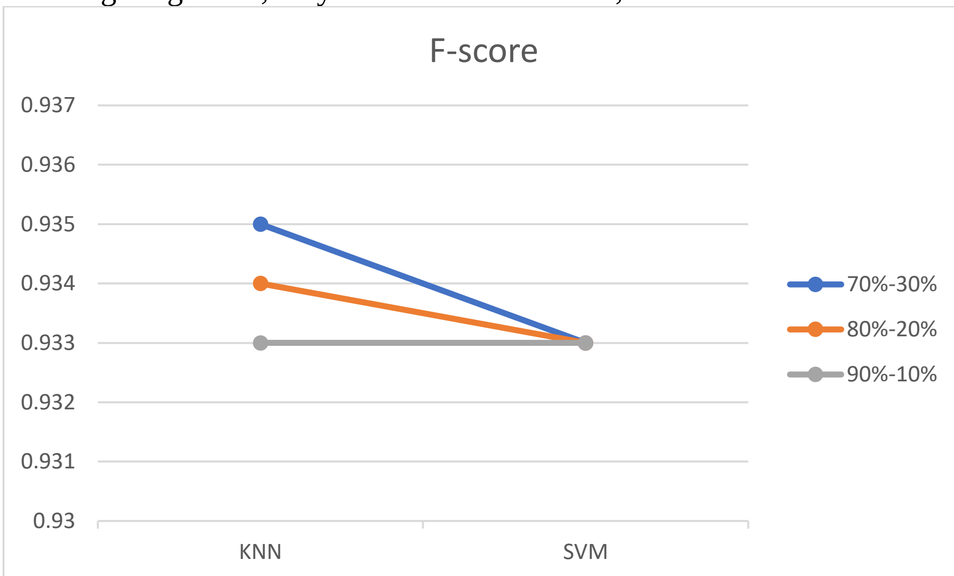

Fig. 9 F-score

IV. Conclusion

In modern systems such as connected vehicles, intelligent intrusion detection systems have become a vital security application. These vehicles are targeted to different type of attacks which lead to effects on the vehicles' performance, threats to public and private property and road safety. In this work, we propose an intrusion detection method for CAN bus IDS in vehicles. It has the ability to detect DoS and the Fuzzy attacks which occur on CAN Bus. We use two data sets, one for DoS Attack and other one for Fuzzy attack which is created by HCRL. We preprocessed the data and, then implemented the KNN and SVM algorithms. Both of them provided great results, however, KNN gives better performance than SVM. In future work, we will use some other classification algorithms and make the comparison to get the best one for IDS in vehicles. Besides, we will work to come up with a new method to prevent some attacks on CAN Bus.

References

[1] Peterson, L. E. (2009). K-nearest neighbor. Scholarpedia, 4(2), 1883.
[2]Bhatia, N. (2010). Survey of nearest neighbor techniques. arXiv preprint arXiv:1007.0085.
[3] Joachims, T. (2002). Learning to classify text using support vector machines: Methods, theory and algorithms (Vol. 186). Norwell: Kluwer Academic Publishers.
[4] Ben-Hur, A., & Weston, J. (2010). A user’s guide to support vector machines. In Data mining techniques for the life sciences (pp. 223-239). Humana Press.
[5] Fengzhong Qu, Zhihui Wu, Fei-Yue Wang, and Woong Cho, ”A security and privacy review of VANETs”, IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985-2996, Dec., 2015
[6] Razzaque M.A., S. A.S., Cheraghi S.M. (2013) Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the Road Ahead. In: Khan S., Khan Pathan AS. (eds) Wireless Networks and Security. Signals and Communication Technology. Springer, Berlin, Heidelberg
[7] Rivas, D. A., Barceló-Ordinas, J. M., Zapata, M. G., & Morillo-Pozo, J. D. (2011). Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation. Journal of Network and Computer Applications, 34(6), 1942-1955.
[8] A. Taylor, N. Japkowicz, and S. Leblanc, “Frequency-based anomaly detection for the automotive CAN bus,” in Proc. 2015 World Congress on Industrial Control Systems Security (WCICSS), pp. 45–49, Dec. 2015.
[9] H. M. Song, H. R. Kim, and H. K. Kim, “Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network,” in Proc. 2016 International Conference on Information Networking (ICOIN), pp. 63–68, Jan. 2016.
[10] M. Brooks, “Anomaly Detection on Vehicle Networks,” in Presented at the 11th ESCAR Embedded Security in Cars Conference, 2013.
[11] H. M. Song, H. R. Kim, H. K. Kim, "Intrusion detection system based on the analysis of time intervals of can messages for in-vehicle network", Information Networking (ICOIN) 2016 International Conference on. IEEE, 2016.
[12] Farsi M, Ratcliff K, Barbosa M. An overview of Controller Area Network. Computing and Control Engineering Journal 1999; 10
[13] K.-T. Cho and K. G. Shin, “Fingerprinting Electronic Control Units for Vehicle Intrusion Detection,” in Proc. 25th USENIX Security Symposium, (Austin, TX, USA), Aug. 2016.
[14] Cho, Kyong-Tak, and Kang G. Shin. "Fingerprinting electronic control units for vehicle intrusion detection." 25th USENIX Security Symposium (USENIX Security 16). USENIX Association, 2016.
[14] Cho, Kyong-Tak, and Kang G. Shin. "Fingerprinting electronic control units for vehicle intrusion detection." 25th USENIX Security Symposium (USENIX Security 16). USENIX Association, 2016.
[15] M. Muter and N. Asaj, “Entropy-based anomaly detection for in-vehicle networks,” in Proc. 2011 IEEE Intelligent Vehicles Symposium (IV), pp. 1110–1115, June 2011
[16] M. Markovitz and A. Wool, “Field Classification, Modeling and Anomaly Detection in Unknown CAN Bus Networks,” in escar Europe 2015, 2015.
[17] U. E. Larson, D. K. Nilsson, E. Jonsson, "An Approach to Specification-based Attack Detection for In-Vehicle Networks", the IEEE Intelligent Vehicles Symposium, pp. 220-225, 2008.

[18] A. Taylor, S. Leblanc, and N. Japckowicz, “Anomaly Detection in Automobile Control Network Data with Long Short-Term Memory Networks,” in Proc. 2016 IEEE International Conference on Data Science and Advanced Analytics, (Montreal, Canada), IEEE Computational Intelligence Society, Oct. 2016
[19] C. Miller and C. Valasek, “Adventures in Automotive Networks and Control Units,” tech. rep., IOActive Labs Research, Aug. 2013.
[20] M. Muter, N. Asaj, "Entropy-based anomaly detection for in-vehicle networks", Intelligent Vehicles Symposium (IV), pp. 1110-1115, 2011.
[21] C. Miller and C. Valasek, “A Survey of Remote Automotive Attack Surfaces,” tech. rep., IOActive Labs Research, 2014.
[22] A. Van Herrewege, D. Singelee, and I. Verbauwhede. Canauth-a simple, backward compatible broadcast authentication protocol for can bus. In ECRYPT Workshop on Lightweight Cryptography 2011, 2011.
[23] T. Matsumoto, M. Hata, M. Tanabe, K. Yoshioka, and K. Oishi. A method of preventing unauthorized data transmission in controller area network. In Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th, pages 1–5, May 2012.
[24] Q. Wang and S. Sawhney, "VeCure: A practical security framework to protect the CAN bus of vehicles," 2014 International Conference on the Internet of Things (IOT), Cambridge, MA, 2014, pp.13-18.doi: 10.1109/IOT.2014.7030108
[25] Ghaleb, F. A., Zainal, A., Rassam, M. A., & Mohammed, F. (2017, November). An effective misbehavior detection model using artificial neural network for vehicular ad hoc network applications. In Application, Information and Network Security (AINS), 2017 IEEE Conference on (pp. 13-18). IEEE.
[26] J. Hortelano, J.C. Ruiz, P. Manzoni. “Evaluating the Usefulness of Watchdogs for Intrusion Detection in VANETs,” in IEEE Int. Conf. Commun. Workshops (ICC), 2010
[27] T. Hoppe, S. Kiltz, and J. Dittmann. Security threats to automotive CAN networks - practical examples and selected short-term countermeasures. In SAFECOMP, 2008.
[28] M. Muter, A. Groll, and F. C. Freiling, "A structured approach to anomaly detection for in-vehicle networks, " in 6th Int, Conf. Information Assurance and Security (lAS). Atlanta, GA: IEEE, 2010, pp. 92-98.
[29] Sakiz, F., & Sen, S. (2017). A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. Ad Hoc Networks, 61, 33-50.
[30] Abboud, K., Omar, H. A., & Zhuang, W. (2016). Interworking of DSRC and cellular network technologies for V2X communications: A survey. *IEEE transactions on vehicular technology*, *65*(12), 9457-9470.
[31] Engoulou, R. G., Bellaïche, M., Pierre, S., & Quintero, A. (2014). VANET security surveys. Computer Communications, 44, 1-13.
[32] Wedel, J. W., Schünemann, B., & Radusch, I. (2009, December). V2X-based traffic congestion recognition and avoidance. In Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 10th International Symposium on (pp. 637-641). IEEE.
[33] Hong, J. (2016). Cyber Security Issues in Connected Vehicle of Intelligent Transport System. Indian Journal of Science and Technology, 9(24).
[34] Kleberger P, Olovsson T, Jonsson E. Security aspects of the In-vehicle network in the connected car. Proceedings of IEEE IV; Germany. 2011. p. 528–33.
[35] Knapik P, Schoch E, Kargl F. Electronic decal: A security function based on V2X communication. Proceedings of VTC; Canada. 2014. p. 1–14.

[36] Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. Black Hat USA, 2015.
[37] Kelion, L. (2016). Nissan Leaf electric cars hack vulnerability disclosed. BBC News. Np, 24.
[38] Kong, F., Zhang, L., Zeng, J., & Zhang, Y. (2007, August). Automatic measurement and control system for vehicle ECU based on CAN bus. In Automation and Logistics, 2007 IEEE International Conference on (pp. 964-968). IEEE.
[39] Lawrenz, W. (1997). CAN system engineering. From theory to practical applications, New York.
[40] Cebi, A., Guvenc, L., Demirci, M., Karadeniz, C. K., Kanar, K., & Guraslan, E. (2005, June). A low cost, portable engine electronic control unit hardware-in-the-loop test system. In Industrial Electronics, 2005. ISIE 2005. Proceedings of the IEEE International Symposium on (Vol. 1, pp. 293-298). IEEE.
[41] Tuohy S, Glavin M, Hughes C, Jones E, Trivedi M, Kilmartin L. Intra-Vehicle Networks: a review. IEEE Trans. on Intelligent Transportation Systems 2015; 2: 534–54
[42] Torrent-Moreno, M., Mittag, J., Santi, P., & Hartenstein, H. (2009). Vehicle-to-vehicle communication: fair transmit power control for safety-critical information. IEEE Transactions on Vehicular Technology, 58(7), 3684-3703.
[43] Tchamna, R., & Youn, I. (2013). Yaw rate and side-slip control considering vehicle longitudinal dynamics. International Journal of Automotive Technology, 14(1), 53-60.
[44] Tsugawa S. Inter-vehicle communications and their applications to intelligent vehicles: an overview. IEEE Intell. Veh. Symp. 2002.
[45] Jin WL, Recker WW. Instantaneous information propagation in a traffic stream through inter-vehicle communication. Transp. Res. B 2006; 3.
[46] Kesting A, Treiber M, Helbing D. Connectivity Statistics of Store-and-forward Intervehicle Communication. IEEE Transactions on Intelligent Transportation System 2010.
[47] Johansson KH, Aurngren M, Nielsen L. Vehicle applications of controller area network. Handbook of Networked and Embedded Control Systems 2005.