Intelligent Intrusion Detection System in Internal Communication Systems for Driverless Cars

Nuha Abd
Computer Sciences Department, College of Computer and Information Technology, University of Anbar, Anbar, Iraq.

Khattab M Ali Alheeti
Computer Networking Systems Department, College of Computer and Information Technology, University of Anbar, Anbar-Iraq. E-mail: co.khattab.alheeti@uoanbar.edu.iq

Salah Sleibi Al-Rawi
Information Systems Department, College of Computer and Information Technology, University of Anbar, Anbar-Iraq. E-mail: dr_salah_rawi@yahoo.com

Received July 02, 2020; Accepted September 05, 2020
ISSN: 1735-188X
DOI: 10.14704/WEB/V17I2/WEB17039

Abstract

The modern car is a complicated system consisting of Electronic Control Units (ECUs) with engines, detectors and wired and wireless communication protocols, that communicate through different types of intra-car networks. The cyber-physical design relies on this ECU network that has been susceptible to several kinds of attacks using wireless, internal and external access. The internal network contains several security vulnerabilities that make it possible to launch attacks via buses and propagation over the entire ECU network, therefore anomaly detection technology, which represents the security protection, can efficiently reduce security threats. So, this paper proposes new Intrusion Detection System (IDS) using the Artificial Neural Network (ANN) to monitor the state of the car by information collected from internal buses and to achieve security, safety of the internal network The parameters building the ANN structure are trained CAN packet information to devise the fundamental statistical attribute of normal and attacking packets and in defense, extracted the related attribute to classify the attack. Experimental evaluation on Open Car Test-Bed and Network Experiments (OCTANE) show that the proposed IDS achieves acceptable performance in terms of intrusions detection. Results show its capability to detect attacks with false-positive rate of 1.7 %, false-negative rate 24.6 %, and average accuracy of 92.10 %.

Keywords

Intrusion Detection, Security, Self-driving Cars, CAN, Internal Communication.

Introduction

Recently, the integration of a number of computing devices called the ECU has made significant progress in an automotive environment. ECU is used to control and monitor a vehicle subsystem to reduce noise, vibration and to improve performance. The ECU replaces the traditional mechanical control parts [1]. Recently, computing devices are used in vehicle networking services to perform inter communication between vehicles and intra-vehicular communication [2] [3].

In [4] [5] efficient fuel consumption is taken into account when calculating the speeds or distances of the connected cars. Tang et al. suggest using the communications to recognize driving habits such as fuel consumption and speed of each vehicle [6][7]. Another researcher showed strong Vehicle-to-Vehicle (V2V) connections based on traffic flow [8]. Also in the communication, a new message transit through the scheme was developed [9]. In addition, through wireless communications that enabled the collaborative platooning used to obtain better traffic flow [10]. The best performing results of the Grand Cooperative Driving Challenge (GCDC) Explore recent developments in the area of practical cooperative driving [11][12]. Consequently, the computing devices' performance in a car increases dramatically. To promote communications, various communication protocols have been developed [13]. One of most important protocols used is the basis of a network connection which Controller Area Network (CAN). It is a multi-master serial bus designed to support connecting sensors and actuators to ECU and the acceptance of the CAN simplifies the emergence of applications in the automotive sector [14]. Often significant information such as diagnostic and data control is transmitting via a CAN bus to support car services such as driverless cars (Figure 1). However, the increase in networking ability is followed by significant security challenges, and the in-vehicle network contains a number of security vulnerabilities [15][16]. ECUs can obtain broadcasting messages from ECU to other ECU in the same bus, and they are unable to diagnose a sender [15]. Several research studies have been conducted to address safety issues in inter-and intra-vehicular communications [17][18]. Specifically, an intrusion detection system (IDS) receives considerable interest due to the reliability and simplicity of detecting attacks. [17][19]. A collection of anomaly detection sensors is implemented that enable the identification of attacks during vehicle service without triggering false positives [19]. Proposed a security protocol for CAN as a counter-measure built in compliance with existing CAN requirements. It is more efficient than existing security protocols in terms of delays in authentication and communication loads [18]. A novel vehicle safety system presented that supports two features; shared authentication of ECUs, users with various access rights. Such features can make for a more distributed security architecture and prevent several attacks [20].

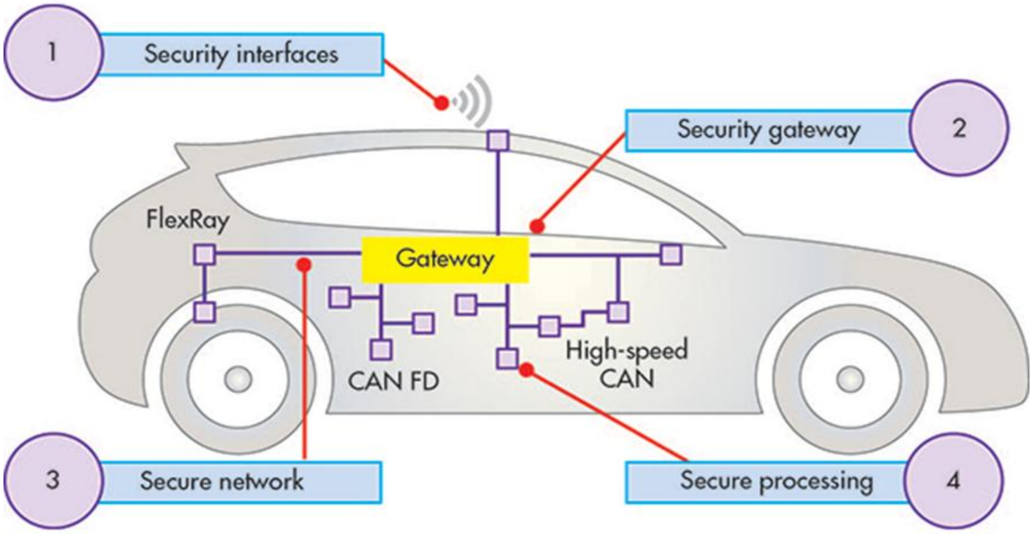


Figure 1 Shows a basic internal network structure of self-driving vehicles [21]

Previous methods of intrusion detection can only be efficient for specific attack systems already considered in design phases [22] [23]. Machine learning-based IDS strategies are used mainly for conventional communication networks in order to deal with the problem [24]. The aim is to collect the basic features of the data and use them to detect any hacking attacks [25]. Methods for detecting intrusions have been developed by using the ANN [26] [27] and support vector machine to classify Type of attacks [28]. In this paper, the anomaly detection system is proposed to secure internal communication systems for self-driving and semi self-driving vehicles. However, it is heavily based on ANN. Thus, intelligent detection scheme plays a vital role to protect information/ control data between ECUs. In addition, the suggested methodology trains CAN packet information in order to work out the fundamental statistical properties of normal packets and attack packets and, in defense, extracts the related attribute to classify the attack. ANN has been shown to be effective in the classification of statistical patterns, security as well as in intelligent vehicular systems [26] [27].

The rest of the paper is constructed as follows. Section 2 gives some related work and gives details about Internal Communication and attack. Section3 (Methodology) includes information on data collection and feature sets, intrusion detection systems, machine learning techniques. Section 4 Presents realistic verification results for the efficiency of the detection system. Section 5 concludes.

Related Works

Although there have been many efforts to build develop effective detection systems, there is still an open area due to various aspects in this area such as a highly dynamic environment, large traffic data size, ambiguous boundaries between normal and abnormal behavior. IDS have been studied and developed to protect against malicious attacks. Using these techniques, the activity of the system is monitored and classified depending on specific rules, methods, and algorithms. This part offers an account of past research on overall intrusion detection systems using different techniques.

Hoppe et al. suggested the technique of intrusion identification through the use of different proxy attack methods previously identified in a database [29]. Additionally, Larson et al. compare the behavior of existing system properties to the selected style to develop the pattern depends on the characteristics [30].

Khattab M. et al. discussed an Intrusion Detection System Against Malicious Assaults in Self-driving cars. Misuse and anomaly two kind of IDSs have been used to detect attacks. The performance of IDS is assessed using a trace file that contains features used in analysis. Trains and Test IDS with all these features in order to distinguish between normal and abnormal behavior. This work can be developed by using a fuzzy data set to reduce the error rate that occurs in the system [31].

Kamran Zaidi. et al. suggested intrusion detection and prevention systems for cars. This system is one of the best ways in the safety of the network as well as the use of automated learning algorithms to detect anomalies. This system is used to detect types of attacks by simulating rogue nodes that can carry out multiple attacks. Data are collected using statistical techniques to determine if the data is wrong and analyzed to be accepted or rejected based on hypothesis testing. The goal of rogue nodes is to destroy the network by quickly dropping or raising its value parameters. This work is developed to detect other attacks in VANET by modifying IDS and using rogue nodes refuse service or reporting the wrong location [32].

Kang M-J, Kang J-W used intrusion detection by methods of a Deep Neural Network for the safety of the vehicle network. (DNN) was shown to bee efficient in the classification of statistical patterns. The parameter train efficiently by initializing the deep neural network depend on the extraction of feature vehicular network packet used in training and testing in order to reach a good rating through the unsupervised pre-training of Deep

Belief Networks (DBN), to detect normal and hacking packets, and therefore identify a malicious attack on the car [33].

Progress becomes important in the automotive field. John Rowley. et al. presented Examining the Driverless Future: An Analysis of Human-Caused Vehicle Accidents and Development of an Autonomous Vehicle Communication Testbed. In recent years has been relying on the Vehicle-to-Vehicle (V2V) model. For communication between vehicles and for safety and mobility but limited to the present. To reduce casualties and eliminate accidents, self-driving cars are used that have proven to be capable of doing so. In this paper, communication protocols were tested to determine the tradeoffs between communication algorithms using powerful tools and the presence of sensors used in various ways [34].

Q. Wang, Z. Lu et al. focused on CAN security, which is an ECU communication standard. Suggested IDS based on CAN messages entropy of identifier bits. CAN injection assaults want to change the CAN ID bits and analyzing such bits' entropy can be an efficient approach to detect attacks. System limited the injection of amount of malicious messages with larger priority IDs by attackers. The experimental findings showed that entropy-based IDS is capable of effectively detecting all the injection assaults without interrupting CAN communication [35].

Moayad Aloqailya. et al Suggested a new hybrid method called D2H-IDS to detect intrusion in intelligent vehicle network environments. A deep belief method is used for data dimensional reduction and the decision tree machine learning technique is used for the selection and classification of features. The efficiency of the proposed model has been illustrated by the actual cyber-security attack. [36].

In this paper, anomaly the intrusion detection system is used to achieve a more security and reliable internal communication of car.

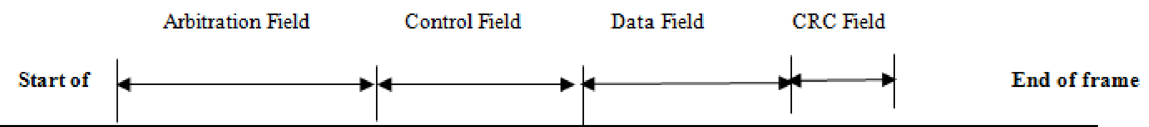
Internal Communication of Self-driving Car

A typical new car integrates a number of networked parts including sensors, actuators, ECUs and devices for communication [37]. ECU is an embedded system that controls one or more car subsystems. With several amount of ECU in cars, connecting two electronic control units directly (point-to-point) is hard because of the increase in the cost and weight of the car and made maintenance more difficult. They can be interlinked through a bus and send messages to all associated nodes. Needed several protocols to correlate them. As a result, vehicles made up of several sub-networks continue to operate among themselves through an electronic control unit. These networks are Control Area Network (CAN), Local Interconnect Network (LIN), Flex Ray and Media Oriented Systems Transport (MOST) [38]. Usually, ECUs communicate through CAN, which is used for in-vehicle communication.

1) Control Area Network (CAN)

Is the most established automotive communication system protocol for the internal vehicle network, intended for a high-speed, semi-directional transmission in the vehicle network and provides a connection rate of up to 1 Mbps. CAN be used to transmit messages as packets of data through the ECU to the network. The low cost, relatively high reliability, reasonable performance in noise-resistance and fault-tolerance properties of CAN motivate its use as a standard for intra-vehicle communication. Nevertheless, CAN is susceptible to potential threats [37] [39].

The standard CAN data frame format is shown in Figure 2[40].



SOF	Identifier	RTR	IDE	r	DLC	0-8 bytes	CRC	ACK	EOF
1 bit	11 bit		6 bit			0-64 bit	16 bit	1 bit	1 bit

Figure 2 CAN frame format

The arbitration field contains 11-bit ID field where each ID matches a specific ECU. The ID numbers also check message priority on the CAN bus, with lower ID numbers taking priority over higher numbers. After the node ID is the Remote Transmission Request (RTR) bit, which is controlling for data frames and recessive for remote requests. The next bits are the Data Length Code (DLC), which described bytes the following DATA field will be (up to 8). The data field includes 8 bytes' information as a maximum to be transmitted in a message. The Cyclic Redundancy Checks (CRC) field to test data integrity and detects mistake in the information packet. The acknowledgment field emphasizes the reception of a correct CAN packet.

However, there are details on a number of mechanisms for detecting possible intrusion into the CAN bus that have been proposed. One of these mechanisms known identifier filtering, The intrusion detection system can use the frame identifier to create a list of permitted and prohibited identifiers on the basis of which it can determine which frames to filter [41]. Other detection mechanism that uses identifiers is timing analysis which is a so common mechanism that uses identifiers and works fully with periodical messages. It consists of setting the time-window of acceptance for each periodic message. The system shall consider as an intrusion whether the same message is received outside the time window so that the message is filtered out. [42][19]. In addition to the message identifier, the data length code (DLC) can also be used to discover bad behavior.

Internal Communication Attacks

An intruder may no longer need to have physical access to the aimed vehicle due to the modern wireless communication capabilities of cars. Attacks of self-driving cars' internal communication system have been categorized in Figure 3:

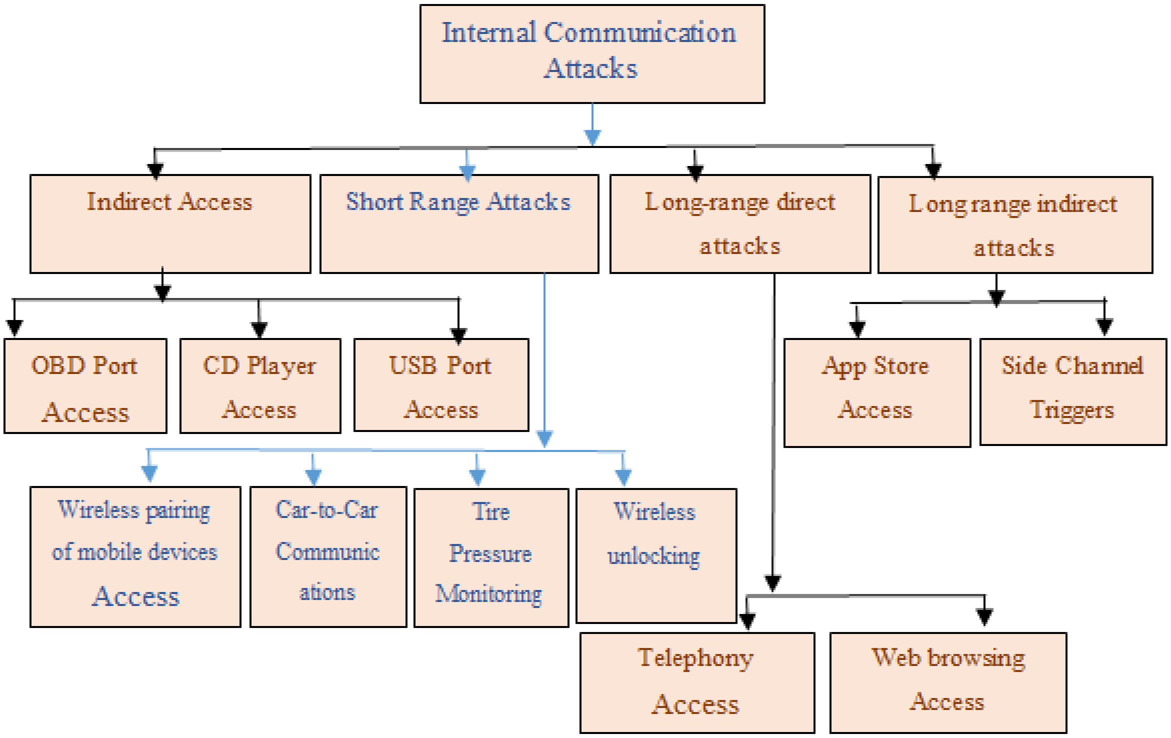


Figure 3 Internal Communication Attacks

Indirect Access concentrate on third-party threats that will be able to attack the car at a later time such as On-Board Diagnostics (OBD) Port, CD Player, and USB Port. As for short-range attacks, these attacks are based on short-range wireless networks. It is possible that this attack would have a direct attack by directly attacking the car's communication, or indirectly through smartphones. Other attacks are from remote locations such as telephony and web browsing. The last type of attack is long-range indirect attacks, this is from a remote and indirect location [43].

In this paper, focus on an attacker who has indirect location over ECU (Figure 4):

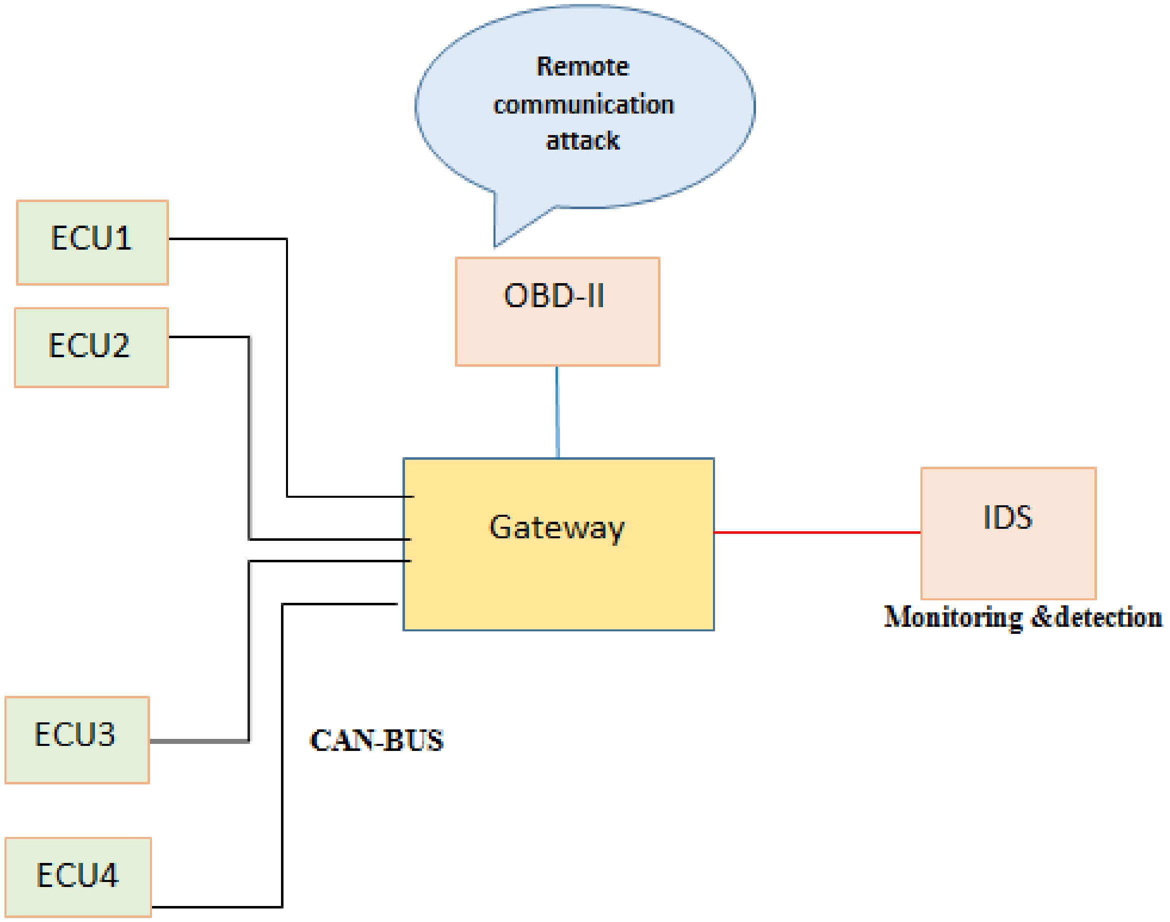


Figure 4 Indirect access of the CAN-Bus

Methodology

We propose an IDS based on a dataset collected from a simulator that created using Open Car Test-Bed and Network (OCTANE) simulation to model the car's internal networks and its environment. This system is capable of providing sufficient internal communication safety for self-driving and semi-self-driving cars. Figure 5 explains the steps of methodology:

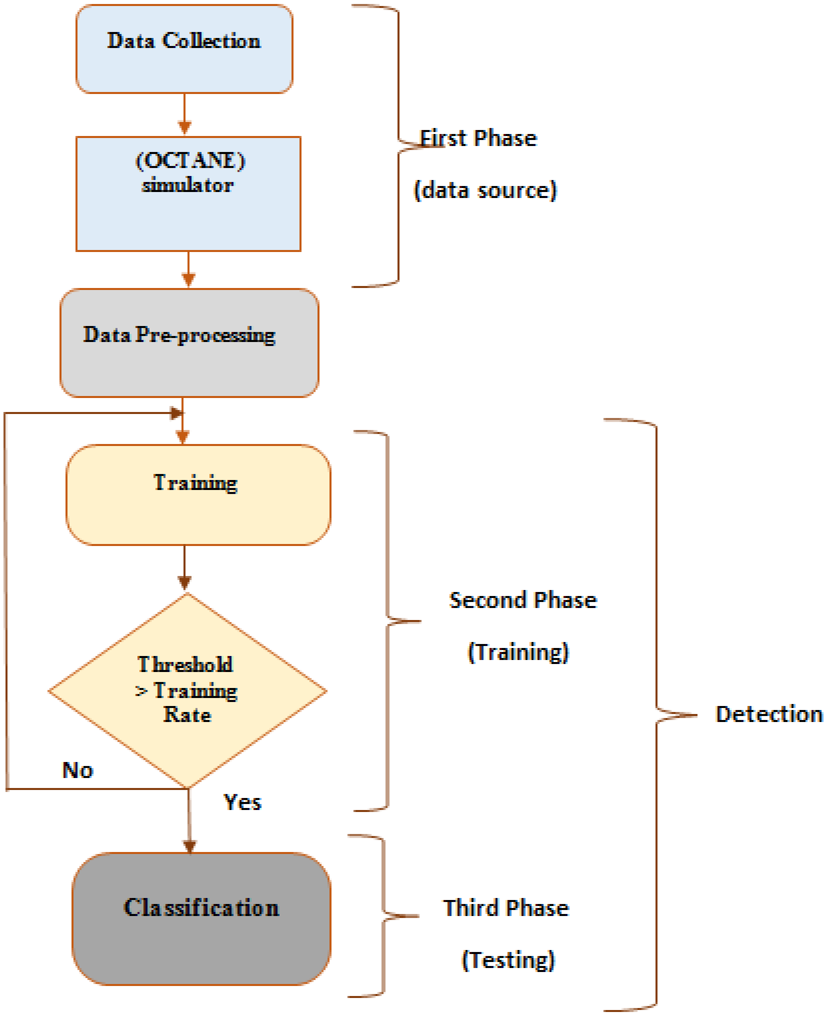


Figure 5 Architecture design of IDS

A. Simulation Environment

The proposed system is tested to measure its performance detection under a certain condition. The initial parameters are one of the important elements of the simulation that determined efficiency and behavior in OCTANE. The suggested security system simulator is Open Car Test-bed and Network to realistically simulated environment for natural and malicious behavior in internal networks of cars.

B. Feature Sets

The IDS is based on features that describe events in the car. extracted the behavior from the simulator because it consists mainly a number of different features that can be used for analysis. Characteristics identify behaviors that are normal or abnormal and used to measure the effectiveness of the suggested IDS. The type and number of features of the IDS are very significant that affect the number of alarms and detection rates. With all the features that define natural and malicious behavior, train and test the IDS. The features set are shown in Table 1.

Table 1 Feature type of CAN

Features	Type
ID	Discrete
ECU-ID	Discrete
Priority	Discrete
DLC	Discrete
Flags	Discrete
Data	Continuous
Time	Continuous
Class	Discrete

C. Data Preprocessing Stage

Network traffic includes numerous types of data (continuous, symbolic and discrete) that vary considerably in ranges. The pre-processing stage of data is important. This stage is based on the following two steps:

Step_1: Convert symbolic attributes to numeric values. The transformation is done by assigning each symbol encoding number. The encoding begins at 1 and increases one within each feature for each symbol.

Step_2: Normalize numerical values. The features of the data are scaled within the [0, 1] range. The main advantage is to prevent attributing those in greater ranges that have broader ranges from dominate those in smaller ranges. The scaling is achieved using the equation 1 [44]:

$$A = \frac{a - min_{old}}{max_{old} - min_{old}}(max\ new - min\ new) + min\ new \quad (1)$$

Where A and a are old and new data values. Min old and Max old are the old range confines while Min new and Max new are the new range confines. Normalizing data also allows the detection rate to be increased and the performance of ANN to be improved.

D. Intelligent Detection System

An Artificial Neural Network (ANN) is used by the intelligent detection system to classify malicious attacks. Current self-driving car studies confirm that ANN is effective and easy in designing the internal systems for these cars. ANN used includes three layers, input, hidden, and output. The input layer is made up of 7 neurons equal to the number of features. Used two hidden layers to reduce the number of false alarms and improve the accuracy of the detection system. The first hidden layer contains three neurons, while the second hidden layer contains 7 neurons.

In the output layer, there are two neurons (normal and abnormal). However, the classifier divides the datasets into ordinary packets and attack packets. It should decide to classify the new packet in which group the packet belongs to. IDS design includes two primary phases the training phase and the detection phase. During the training phase, a CAN packet is processed to extract a feature that represents the statistical behavior of the network. Every CAN packet is either a normal packet or an attack packet. In Figure 6 implemented the ANN structure in order to train the features. In final stage test ANN with data attributes that define behavior that is normal and abnormal. Once the ANN train is secure, the protection can be tracked by detecting network control messages and data packets and automatically generate an alert if malicious behavior occurs.

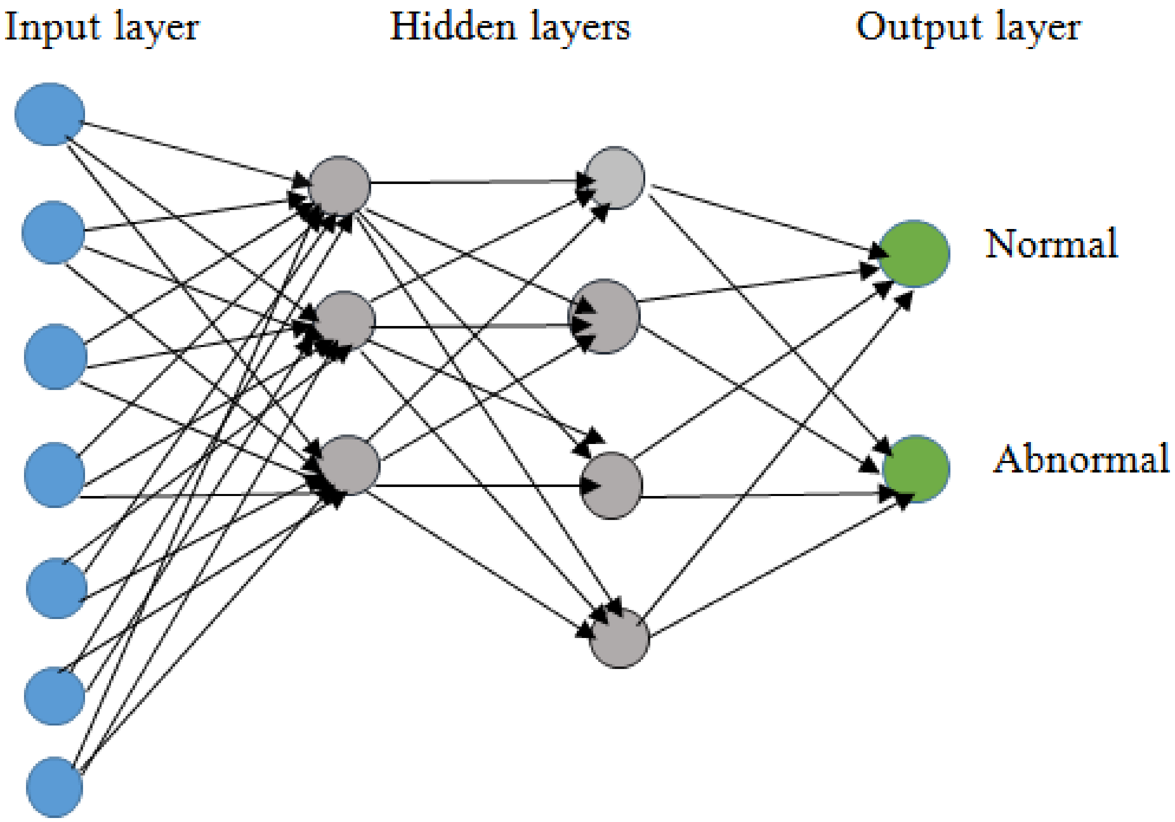


Figure 6 Structure of the Artificial Neural Network (ANN)

The problem is formulating as a supervised machine learning problem Follows in detail. Assume set of input-output pairs: ***C= {(vi, wi)}*** $_{i\in [1,\ N]}$ C is the data set collected, N is the number of examples found. **(vi)**$_{\mathbf{i\in [1,\ N]}}$ training input is a d-dimensional vector of elements perform features $(ai^{(1)}, ai^{(2)} \ldots ai^{(d)})$ contained in the M matrix **(N × d)**. output (wi)$_{i\in [1,\ N]}$ is contained in a 1-dimensional vector **w** and reflects a categorical value that we want to forecast. The purpose of supervised machine learning in equation1 is to assume the presence of some unknown function < ***f*** >, inputs maps to outputs.

$$f\,(v) = w,\ \forall (v, w) \in C. \quad (1)$$

The function estimation **<*f*>** is the main purpose of the learning process; *given* a classified training set and then make the guesses about unknown information $\mathbf{v_k}$ used of the estimated function $\mathbf{w\hat{}=}\boldsymbol{f}\ \mathbf{(}\boldsymbol{v_k}\mathbf{).}$ The input vector $\boldsymbol{v_k}$ and set of training data ***Ctrain***, we indicate the likelihood distribution over possible labels by $\boldsymbol{P\ (w|v_k,\ C_{train})}$. This likelihood is depending on the $\boldsymbol{C_{train}}$ training set and the $\boldsymbol{v_k}$ input vector**.** Used the machine learning model ***R*θ** when approximating the function**<*f*>**, ***R*** is representing the model, and the parameters of model has been indicated by ***θ***. The distribution of probability over possible labels is also determined by selection model, $\boldsymbol{p\ (w= \hat{}w|v_k,\ C_{train},}$ ***Rθ*** use classification parametric systems where the output is one out of the D classes the likelihood of potential labels is a system with a categorical distribution. Let $\boldsymbol{w_{ij}}$ = I ($\boldsymbol{w}_{\mathrm{i}}$ = j) be the one- encoding of $\boldsymbol{w}_{\mathrm{i}}$:

$$p\ (w= \hat{}w|v_k,\ C_{train},\ R\theta) = \Pi^{D}_{j=1}\, \mathrm{M}\theta, j\ (v_k)^{I(w=j)}\ (2)$$

We use the maximum probability method that maximizes $\boldsymbol{p\ (C_{train},\ R\theta) = \Pi^{N}_{i=1}\ p\ (w_i= v_i,}$ ***θ*) to estimate the model parameters <θ>.**

For each hidden input vector vk, make an estimate in favor of the class that has the highest probability distribution when we have the optimal model parameters $\boldsymbol{\theta}^{\wedge}$. As soon as best parameters $\boldsymbol{\theta}^{\wedge}$ are estimated, the outputs of the prognosis model produce an expected signal estimation for a hidden input vector $\boldsymbol{v_k}$. The value w obtained is then compared to the expected value of the signal. An alarm shall be given if the two signals are not the same ***Alert*=1 ↔ wˆ≠w.**

The initial parameters have an important role in the performance of ANN and have a direct impact on performance. The training phase parameters used in the ANN are shown in Table 2 below:

Table 2 Artificial Neural Networks (ANN) Parameters

Parameters	Value
Train Parameters Epoch	41
Train Parameters learn	10^{-7}
Train Parameters goal	0
Train Parameters min-grad	10^{-8}
Time	0.4s

Experimental Results

The performance of the suggested IDS model will be verified using the data set. The data set comprises of 7 features, which reflect the basic properties of the network, as shown in table (1) Such combined properties help to determine the network traffic attacks.

Two different behaviors can classify the security system: ordinary or attack malicious via IDS. This section demonstrated the detection system performance. The accuracy is specified as the level of data detected correctly among all data detected. In other words, the correctly observed data indicates that the true positive and true-negative values are high, while the accuracy indicates that the error rate is low. To determine the feasibility of the proposed system involves using the accuracy metric equation 1[45]:

$$Accuracy = \frac{Number\ of\ correctly\ classified}{\text{Total number of patterns}} * 100\%\ (1)$$

The measurements will also be computed as follows:
True-positive (TP): normal connection record classified as normal
True-negative (TN): attack connection record classified as attack
False-positive (FP): normal connection classified as attack
False-negative (FN): attack connection record classified as normal
Then:

$$TP\ Rate(sensitivity) = \frac{\text{TP}}{\text{TP+FN}} \qquad (2)$$

$$TN\ Rate\ (specificity)\ = \frac{TN}{\text{TN+FP}} \qquad (3)$$

$$FN\ Rate(1 - sensitivity) = \frac{FN}{\text{FN+TP}} \qquad (4)$$

$$FP\ Rate\ (1 - specificity) = \frac{\text{FP}}{\text{FP+TN}} \qquad (5)$$

during the learning and evaluation phase, the data set used in the training phase varies from the data set used in the test phase. performance of the IDS is determining by calculating the total accuracy.

In this case, an anomaly detection is capable of detecting novel attacks. Table 3 indicates the classification accuracy and number of records used in the proposed system.

Table 3 Accuracy of Classification

Attack Class	**IDS**				
	Real Record	**ANN**	**Match Records**	**Miss Records**	**Accuracy**
Normal	209	256	193	63	92.34%
Abnormal	791	741	728	13	92.01 7%
Unknown	0	3	0	3	NaN

The system computed classification rate and created four types of alarms shown in Table (4).

Table 4 Recognition Rate

Alarm Type Accuracy		**Numbers of Connections**
True positive	75.39 %	193
True negative	98.24%	728
False-negative	24.60 %	13
False-positive	1.75 %	63

Discussion

The primary motivation of used intelligent intrusion detection against attacks is that security technologies, such as encryption and digital signatures, which are unable to safeguard the system against unidentified assaults and cannot protect the internal communication of self-driving cars. Resulting in an interest in using intrusion detection systems to supply effective flexibility in protect these kind of networks. In this paper, developed and validated a method of detection of anomaly intrusion.

The proposed was applied in three phases: data collection and preprocessing phase, training phase, and testing phase. Experimental results showed that the normality and abnormality of the car network could be defined with highly accurate and a small false positive alarm rate with error rate 7.90 %.

In order to evaluate the proposed model performance, that is the key factor for any IDS performance evaluation, so we compared the rates accomplished with those given in [33].

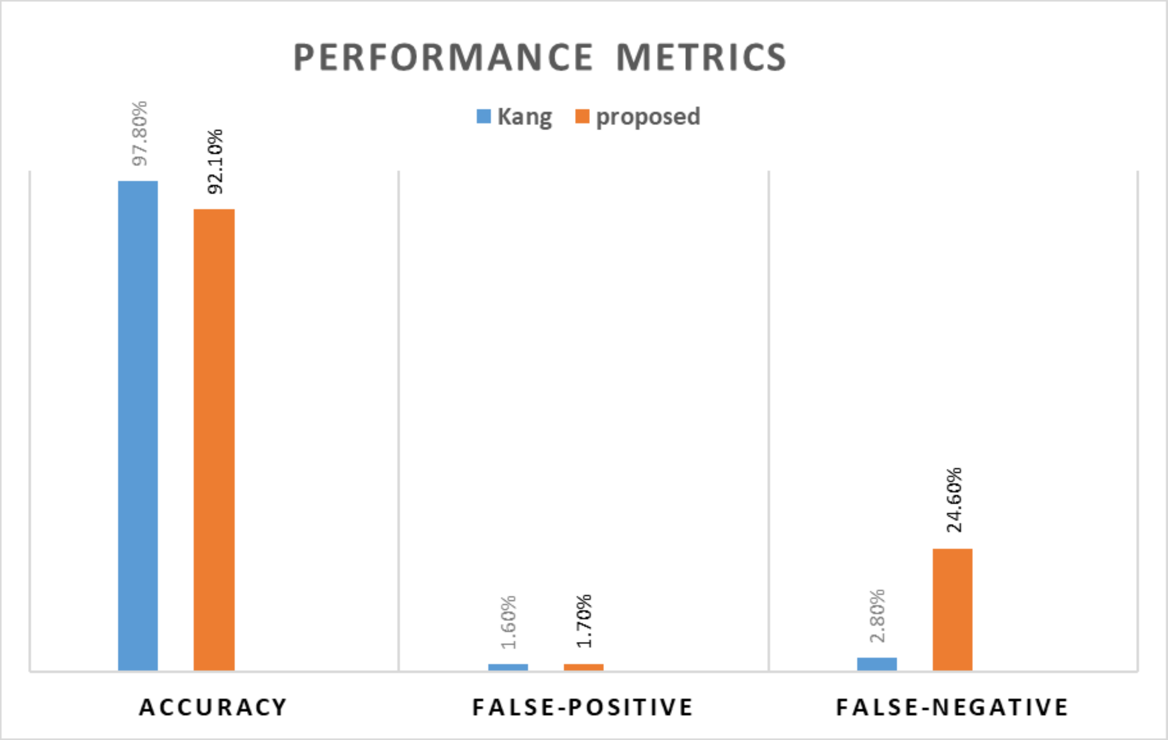


Figure 7 Performance metrics

Conclusion

In this paper we presented novel IDS based on ANN for internal communication of car which capable to detect attack through control on internal communication network. The system was designed with ANN to train and test the parameters with the feature extracted from the in-vehicle network packets. The ANN gives each class the likelihood of distinguished against normal and abnormal packets and show the effectiveness of detection the attack. Although the error rate of our proposed system is 7.90 %, false-positive alarm rate 1.7% and the false negative alarm rate was acceptable, but there is still a need for improvement. For this reason, this study will be advanced by using of a fuzzy data set to reduce the rate of error and false-negative generated in the system.

References

Park, T.J., Han, C.S., & Lee, S.H. (2005). Development of the electronic control unit for the rack-actuating steer-by-wire using the hardware-in-the-loop simulation system. *Mechatronics*, *15*(8), 899–918.

Biswas, S., Tatchikou, R., & Dion, F. (2006). Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety. *IEEE Communications Magazine*, *44*(1), 74–82.

Tuohy, S., Glavin, M., Hughes, C., Jones, E., Trivedi, M., & Kilmartin, L. (2014). Intra-vehicle networks: A review. *IEEE Transactions on Intelligent Transportation Systems*, *16*(2), 534–545.

Yu, S., & Shi, Z. (2015). Fuel consumptions and exhaust emissions induced by cooperative adaptive cruise control strategies. *International Journal of Modern Physics B*, *29*(14), 1550084.

Yu, S., & Shi, Z. (2015). Dynamics of connected cruise control systems considering velocity changes with memory feedback. *Measurement, 64*, 34–48.

Tang, T., Shi, W., Shang, H., & Wang, Y. (2014). A new car-following model with consideration of inter-vehicle communication. *Nonlinear Dynamics*, *76*(4), 2017–2023.

Tang, T.Q., Shi, W.F., Shang, H.Y., & Wang, Y.P. (2014). An extended car-following model with consideration of the reliability of inter-vehicle communication. *Measurement, 58*, 286–293.

Jin, W.L., & Recker, W.W. (2006). Instantaneous information propagation in a traffic stream through inter-vehicle communication. *Transportation Research Part B: Methodological*, *40*(3), 230–250.

Kesting, A., Treiber, M., & Helbing, D. (2010). Connectivity statistics of store-and-forward intervehicle communication. *IEEE Transactions on Intelligent Transportation Systems, 11*(1), 172–181.

Yu, S., & Shi, Z. (2014). An extended car-following model at signalized intersections. *Physica A: Statistical Mechanics and its Applications*, *407,* 152–159.

Van Nunen, E., Kwakkernaat, M.R., Ploeg, J., & Netten, B.D. (2012). Cooperative competition for future mobility. *IEEE Transactions on Intelligent Transportation Systems, 13*(3), 1018–1025.

Lidstrom, K. (2012). A modular CACC system integration and design. *IEEE Transactions on Intelligent Transportation Systems, 13*(3), 1050–1061.

Yu, F., Li, D.F., & Crolla, D.A. (2008). Integrated vehicle dynamics control—State-of-the art review. *In IEEE Vehicle Power and Propulsion Conference*, 1–6.

Hristu-Varsakelis, Dimitrios, Levine, William S. (2005). Handbook of networked and embedded control systems. *Control Engineering, 43*(4), 377-394.

Koscher, K. (2010). Experimental security analysis of a modern automobile. *In IEEE Symposium on Security and Privacy*, 447–462.

Kleberger, P., Olovsson, T., & Jonsson, E. (2011). Security aspects of the in-vehicle network in the connected car. *In IEEE Intelligent Vehicles Symposium (IV)*, 528–533.

Kemmerer, R.A., & Vigna, G. (2002). Intrusion detection: a brief history and overview. *Computer (Long. Beach. Calif), 35*(4), 27-30.

Woo, S., Jo, H.J., & Lee, D.H. (2014). A practical wireless attack on the connected car and security protocol for in-vehicle CAN. *IEEE Transactions on Intelligent Transportation Systems*, *16*(2), 993–1006.

Müter, M., Groll, A., & Freiling, F.C. (2010). A structured approach to anomaly detection for in-vehicle networks. *In Sixth International Conference on Information Assurance and Security*, 92–98.

Patsakis, C., Dellios, K., & Bouroche, M. (2014). Towards a distributed secure in-vehicle communication architecture for modern vehicles. *Computers Security*, *40*, 60–74.

Birnie, A., & Van Roermund, T. (2016). Electronic Design.com. https://www.electronicdesign.com/markets/automotive/article/21801792/4-layers-of-automotive-security.

Tyagi, P., & Dembla, D. (2014). Investigating the security threats in vehicular ad hoc networks (VANETs): towards security engineering for safer on-road transportation. *In International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2084–2090.

Sun, X., Yan, B., Zhang, X., & Rong, C. (2015). An integrated intrusion detection model of cluster-based wireless sensor network. *PLoS One*, *10*(10), e0139513.

Deepa, A.J., & Kavitha, V. (2012). A comprehensive survey on approaches to intrusion detection system. *Procedia Engineering*, *38*, 2063–2069.

Chae, H., Jo, B., Choi, S.H., & Park, T. (2013). Feature selection for intrusion detection using nsl-kdd. *Recent Advances in Computer Science*, 184–187.

Golovko, V., & Kochurko, P. (2005). Intrusion recognition using neural networks. *In IEEE Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, 108-111.

Zhang, Z., Li, J., Manikopoulos, C.N., Jorgenson, J., & Ucles, J. (2001). HIDE: a hierarchical network intrusion detection system using statistical preprocessing and neural network classification. *In Proceedings on IEEE Workshop on Information Assurance and Security*, 85–90.

Hu, W., Liao, Y., & Vemuri, V.R. (2003). Robust anomaly detection using support vector machines. *In Proceedings of the international conference on machine learning*, 282–289.

Hoppe, T., Kiltz, S., & Dittmann, J. (2008). Security threats to automotive CAN networks--practical examples and selected short-term countermeasures. *In International Conference on Computer Safety, Reliability, and Security*, 235–248.

Larson, U.E., Nilsson, D.K., & Jonsson, E. (2008). An approach to specification-based attack detection for in-vehicle networks. *In IEEE Intelligent Vehicles Symposium*, 220–225.

Alheeti, K.M.A., Gruebler, A., & Mc Donald-Maier, K.D. (2015). An intrusion detection system against malicious attacks on the communication network of driverless cars. *In 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, 916–921.

Zaidi, K., Milojevic, M.B., Rakocevic, V., Nallanathan, A., & Rajarajan, M. (2015). Host-based intrusion detection for vanets: a statistical approach to rogue node detection. *IEEE Transactions on Vehicular Technology*, *65*(8), 6703–6714.

Kang, M.J., & Kang, J.W. (2016). Intrusion detection system using deep neural network for in-vehicle network security. *PLoS One*, *11*(6), e0155781.

Rowley, J. (2018). Examining the driverless future: An analysis of human-caused vehicle accidents and development of an autonomous vehicle communication testbed. *In Systems and Information Engineering Design Symposium (SIEDS)*, 58–63.

Wang, Q., Lu, Z., & Qu, G. (2018). An entropy analysis based intrusion detection system for controller area network in vehicles. *In 31st IEEE International System-on-Chip Conference (SOCC)*, 90–95.

Aloqaily, M., Otoum, S., Al Ridhawi, I., & Jararweh, Y. (2019). An intrusion detection system for connected vehicles in smart cities. *Ad Hoc Networks*, *90*, 101842.

Al-Jarrah, O.Y., Maple, C., Dianati, M., Oxtoby, D., & Mouzakitis, A. (2019). Intrusion Detection Systems for Intra-Vehicle Networks: A Review. *IEEE Access*, *7*, 21266–21289.

Studnia, I., Nicomette, V., Alata, E., Deswarte, Y., Kaâniche, M., & Laarouchi, Y. (2013). Survey on security threats and protection mechanisms in embedded automotive networks. *In 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W)*, 1–12.

Zeng, W., Khalid, M.A.S., & Chowdhury, S. (2016). In-vehicle networks outlook: Achievements and challenges. *IEEE Communications Surveys & Tutorials*, *18*(3), 1552–1571.

Wang, C., Zhao, Z., Gong, L., Zhu, L., Liu, Z., & Cheng, X. (2018). A distributed anomaly detection system for in-vehicle network using HTM. *IEEE Access*, *6*, 9091–9098.

Miller, C., & Valasek, C. (2015). *Remote exploitation of an unaltered passenger vehicle.* Black Hat USA, *91*.

Cho, K.T., & Shin, K.G. (2016). Fingerprinting electronic control units for vehicle intrusion detection. In *25th ${$USENIX$}$ Security Symposium (${$USENIX$}$ Security 16)*, 911–927.

Ali, K.M. (2017). *An intelligent intrusion detection system for external communications in autonomous vehicles.* University of Essex.

Duda, R.O., Hart, P.E., & Stork, D.G. (2012). *Pattern classification.* John Wiley & Sons.

Han, M.L., Il Kwak, B., & Kim, H.K. (2018). Anomaly intrusion detection method for vehicular networks based on survival analysis. *Vehicular Communications*, *14*, 52–63.