

Access to this work was provided by the University of Maryland, Baltimore County (UMBC) ScholarWorks@UMBC digital repository on the Maryland Shared Open Access (MD-SOAR) platform.

Please provide feedback Please support the ScholarWorks@UMBC repository by emailing scholarworks-group@umbc.edu and telling us what having access to this work means to you and why it's important to you. Thank you.

Graph-Based Intrusion Detection System for Controller Area Networks

Riadul Islam, *Member, IEEE*, Rafi Ud Daula Refat, *Student Member, IEEE*, Sai Manikanta Yerram, and Hafiz Malik, *Senior Member, IEEE*

Abstract—The controller area network (CAN) is the most widely used intra-vehicular communication network in the automotive industry. Because of its simplicity in design, it lacks most of the requirements needed for a security-proven communication protocol. However, a safe and secured environment is imperative for autonomous as well as connected vehicles. Therefore CAN security is considered one of the important topics in the automotive research community. In this paper, we propose a four-stage intrusion detection system that uses the chi-squared method and can detect any kind of strong and weak cyber attacks in a CAN. This work is the first-ever graph-based defense system proposed for the CAN. Our experimental results show that we have a very low 5.26% misclassification for denial of service (DoS) attack, 10% misclassification for fuzzy attack, 4.76% misclassification for replay attack, and no misclassification for spoofing attack. In addition, the proposed methodology exhibits up to 13.73% better accuracy compared to existing ID sequence-based methods.

Index Terms—Controller area network, security, intra-vehicular communication, chi-squared test, graph-theory.

I. INTRODUCTION

Autonomous or self-driving vehicles are cars or trucks for which human interaction is not needed in driving. Also known as driverless vehicles, they are equipped with various types of sensors, actuators, a high-performance computing system, and software. Although a fully autonomous car is still not a reality, the demand

for partially autonomous cars with various levels of self-automation is very high. It seems that the successful development of a fully autonomous vehicle will change the world's overall transportation system and economy. Hypothetically, it will provide more safety and reduce the accident rate, as every year many accidents occur only because of mistakes made by the human driver. In addition, an autonomous vehicle can be considered a blessing for the disabled person. To turn the dream into a reality, all the original equipment manufacturers (OEMs) are working on this technology, and it is hoped that we will experience the highest level of autonomous features within the next several years.

However, the key consideration for autonomous vehicles should be providing protection against cyber attackers. As the autonomous vehicle will totally depend on the software, sensors, and third-party signals to operate, one can expect that it will catch the attention of hackers. The impact of cyber or physical attacks performed by intruders can include the disclosure of vehicle or driver information like location, gender, number of passengers currently riding, etc. In order to provide safety, it is important to establish a strong protection mechanism not only in vehicle-to-vehicle communication but also in intra-vehicle communication. For an autonomous vehicle, both the inter-vehicle and intra-vehicle communications are controlled by electronic control units (ECUs). ECUs are called the brain of the self-driving car and are responsible for taking real-time decisions, so it is important that they exchange information among themselves over a secured communication channel.

For the intra-vehicle communication channel, controller area network (CAN) technology is considered the *de facto* standard among the car embedded systems [1]. However, the CAN protocol has some serious security breaches in its core. The protocol actually works similarly to a broadcasting system, in that contains no mechanism for checking the identity of the sender. Several researchers have tried to provide solutions to increase the security of the CAN bus [2]–[5]. Most of them work for a certain type of attack situation. Currently, the increasing amount of research work on autonomous vehicles has

R Islam and S M Yerram are with the Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, Baltimore, 21250 USA e-mail: {riadul, ty16571}@umbc.edu.

R Refat and H Malik are with the Department of Electrical and Computer Engineering, University of Michigan, MI, 48128 USA e-mail: {rerafi, hafiz}@umich.edu

This work was supported in part by the UMBC startup grant and by the Ministry of Education in Saudi Arabia under the grant DRI-KSU-934.

Copyright (c) 2020 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending an email to pubpermissions@ieee.org.

inspired us to work on detecting anomalies in the CAN bus for autonomous vehicles.

Several researchers have proposed different solutions for defending against cyber attacks in a vehicular system. An attack can be performed through either a weak or a strong agent [6]. A weak agent can spoof the CAN bus by injecting messages with high priority (ID 0000, denial of service (DoS) attack [7]) or with any arbitration ID (spoofing [8] or Fuzzy attack [3], [9]). On the other hand, a strong agent uses two attackers at the same time to perform attacks. In that case, one attacker tries to suspend the targeted ECU's communication and the other attacker sends a CAN bus message with the targeted ECU's arbitration ID [3], [7]. Unlike conventional methodologies, we try to find complex relationships about CAN bus data using graph theory.

Graph-based anomaly detection techniques are used widely in industries like finance, fraud detection, computer and social networking, data center monitoring, etc. [10], [11]. The unusual substructure of a graph can be used as a flag or sign of an anomaly. First, we construct a set of graphs from CAN bus data and then search for unusual behavior to flag as an anomaly. Our experimental results showed significant success in detecting anomalies with this approach.

In particular, the major contributions in this work are:

- It is the first-ever graph-based cyber attack defense system for CAN communication.
- It is the first chi-squared distribution implementation for detecting attacks in CAN communication.
- We propose a four-stage intrusion detection system (IDS) for cyber or physical attacks on the CAN bus. Here, we use a graph-based approach to find out patterns in the dataset, and the median test and chi-squared test are used to distinguish two data distributions.
- Our proposed algorithm can detect attacks without any change in the CAN protocol. Therefore, it is applicable to any communication system that uses the CAN protocol.

The rest of the paper is organized as follows: Section II discusses the existing CAN; statistical hypothesis testing, especially the chi-squared test; and graph properties. At the end of this section, we present the related work on anomaly detection in the CAN bus as well as graph-based anomaly detection techniques. Section III describes our proposed solution. Section IV and Section V present details about the experimental results and conclusion, respectively.

II. BACKGROUND AND RELATED WORKS

The broadcasting nature of a CAN communication system confirms that all the messages that are transmitted in the network are accessible by all the connected ECUs. After receiving a CAN message, each ECU translates the bit sequence and extracts the necessary components like arbitration ID, data, cyclic redundancy check (CRC), etc., and finally the ECU decides whether to receive the CAN message or not based on the arbitration ID. Apart from indicating the sender of a particular CAN message, the arbitration ID of a CAN message is used as a priority during a collision between two or more CAN messages. For conflict resolution between two CAN messages, carrier-sense multiple access with collision avoidance is used in the CAN bus protocol [3]. Although the arbitration ID is used to define the priority and the source to resolve conflict, it is incapable of authenticating the origin of that CAN message. This security flaw can be used by the inside attacker (who already has access to the CAN bus) and the outside attacker (who can gain access using the cellular communication network, etc.) to corrupt the CAN system.

These attackers can initiate different kinds of attacks on the CAN bus, and we can generalize them as follows:

- **Fabrication attack:** Through an in-vehicle ECU compromised by a strong attacker, the adversary fabricates and injects messages with forged ID, data length code, and data. Figure 1(a) shows an example of the fabrication attack. The objective of this attack is to override any periodic messages sent by a legitimate safety-critical ECU so that their receiver ECUs get distracted or become inoperable. DoS [7], spoofing [8], and fuzzy attacks [3] are some examples of fabrication attacks [7].
- **Suspension attack:** To mount a suspension attack, the adversary needs only one weakly compromised ECU, and that becomes a weak attacker. The objective of this attack is to stop/suspend the weakly compromised ECUs message transmission, thus preventing the delivery/propagation to other ECUs of the information it acquired [12]. Figure 1(b) shows an example of the suspension attack, where a weak attacker suspends ECU A's operation. As a result, this attack affects the performance of various ECUs that utilize certain information from other ECUs to function properly. Therefore, the suspension attack can harm not only the (weakly) compromised ECU itself but also other receiver ECUs.
- **Masquerade attack:** To mount a masquerade attack [7], the adversary needs to compromise two

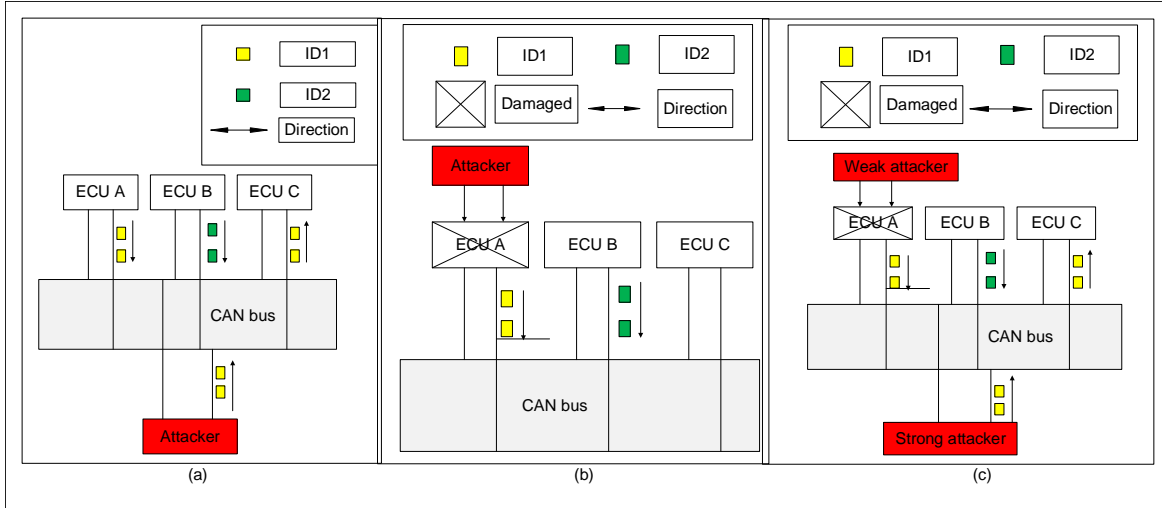


Fig. 1: CAN monitoring-based attack mechanisms: (a) in a fabrication attack, the attacker uses a compromised ECU to inject a message with a forged ID; (b) in a suspension attack, the intruder suspends the communication of a compromised ECU; and (c) in a masquerade attack, the intruder uses a weak attacker to suspend one ECU's data communication and uses a strong attacker to send messages mimicking the suspended ECU's ID and frequency.

ECUs, one as a strong attacker and the other as a weak attacker, as shown in Figure 1(c). The adversary monitors and learns which messages are sent at what frequency by the weakly attacked ECU, and then the strong attacker transmits the message with the ID of the compromised ECU at the same frequency. Examples of this attack are replay or impersonation attacks [13]. Moore

A. Chi-Squared Test

In our proposed methodology, we use the chi-squared test to detect the anomalous CAN data. The chi-squared independence test [14] is a statistical procedure to test if two categorical distributions belong to the same populations or not. It uses the frequency of each category as a factor for distinguishing two distributions. In other words, it is called the chi-square goodness of fit because in this test, the expected frequencies of all the features of one data distribution are extracted and then the findings are compared with the observed frequencies of all the features of the second distribution. If the two distributions are significantly different, we will call it a reject hypothesis; otherwise, we will call it a null hypothesis (if the distributions are the same). The chi-squared test can be described by the following equation,

$$X_{DoF}^2 = \sum_{i=0}^{DoF} \frac{(O_i - E_i)^2}{E_i} \quad (1)$$

where DoF is the degree of freedom, X_{DoF}^2 is the value we will compare against a threshold, O is the observed frequency, and E is the expected frequency. The degree

of freedom in the chi-squared test actually specifies the shape of the distribution. It is a numerical value and can be represented by following equation,

$$DoF = (i - 1) \times (j - 1) \quad (2)$$

where i is the number of categories and j is the number of rows used in that test. The degree of freedom is important for finding out the threshold value from the chi-square table of significance. In general, the chi-squared test works well in a categorical larger data set, which is our primary motivation for using this test for comparing CAN bus-based data distribution.

The chi-squared test is considered one of the most reliable statistical tests now available. Researchers have been relying on the chi-square test for more than a hundred years. Previously, the chi-square test was applied in data correlation [15], experimental and theory-based probability relationship [16], and chiropractic and osteopathic data analysis [14]. In recent years, the chi-squared test has been applied in text classification [17], and in an IDS with a multi-class support vector machine (SVM) [18]. It is a trustable method and has been proven in sectors like medical [19], anomaly-detection [11], and other kinds of data-analysis problems [17]. Other researchers have used the chi-squared test for real-time detection of navigation system soft failures [20]. However, to the best of our knowledge, no previous work used the chi-squared test for anomaly detection in a vehicular network.

B. Graph Properties

A graph is a non-linear data structure consisting of vertices and edges. It actually allows representation of

TABLE I: The proposed methodology uses common graph properties; for example, an edge represents a sequence of CAN messages, while degree represents the number of arbitration IDs sequential with the current ID.

Properties	Significance	In Can bus data
Vertex	Node of the graph	Arbitration ID
Edge	Link between nodes	Arbitration ID sequence
Degree	How many neighbours	How many arbitration IDs are sequential with current ID
Cycle	Loop in the graph	Loop between the sequential arbitration IDs
Root	Starting of the graph	The first CAN message

the relationship between two vertices. We can easily understand the relationship between two vertices from a graph. Over the years, researchers extensively used graph properties to solve various problems in computer science, operating systems, Google maps, social media, etc. Table I presents graph properties and their significance.

C. Related Works

Due to the widespread use of CAN, there has been a significant amount of work on CAN security [2]–[9], [12], [21]–[27]. Researchers incorporate conventional validation techniques to identify invalid CAN ID [21]. To identify anomaly, researchers build a regular model either considering internal CAN messages or vehicle specifications. However, this method can be easily evaded by using existing fabrication attacks. Other researchers proposed a decision tree-based detection system considering eight physical and cyber features [6]. This method uses small-scale robotics vehicle to validate the proposed methodology; however, has high detection latency. Another exciting work introduced an FPGA-based IDS for vehicular systems. Yet, this method is specified for the FPGA platform only, which limits its application to other CPU and GPU-based systems [22].

Other researchers use the periodicity of CAN's message to detect anomaly [2], [26]. Empirically, ECUs generates CAN message at a specific frequency. As a result, it is possible to detect anomalies in inter-arrival time when an external attacker injects messages. Another frequency-based IDS uses a one-class support vector machine to detect anomalies with high accuracy [23]. However, real CAN message prone to variation, and often exhibits inconsistent inter-arrival time, reduces the reliability of these schemes.

Some researchers used information theory and proposed an entropy-based IDS to detect CAN attacks. The basic idea of these systems is normal attack-free CAN messages will have standard or stable entropy. On

the other hand, the attacked CAN messages will have unstable behavior [24], [25]. Another exciting approach and closest to our proposed method is arbitration ID sequencing-based IDS [27]. This method builds a transition matrix using a standard CAN dataset and compares attacked CAN message ID sequence to detect an attack. This method can detect simple impersonate-type attacks; however, it could not detect replay attacks.

III. PROPOSED METHODOLOGY

In this paper, we propose an IDS to secure the CAN bus communication system. The proposed methodology uses statistical analysis as a basis for detecting anomalies and is divided into several steps. The steps are (i) transferring a CAN bus message to a more meaningful graph structure, (ii) extracting graph-based features to import for anomaly characterization, (iii) constructing a hypothesis based on the safe population window, and (iv) comparing the test population window to the base population. This section is organized as follows: Section III-A contains the proposed algorithms and Section III-A2 contains the exploratory data analysis.

A. Proposed Intrusion Detection Methodology

In this section, we will first define two terms used in our proposed algorithm and then detail our proposed methodology. The terms are:

- **Window:** A range of raw CAN bus messages will be called a single window. In our proposed methodology, we consider 200 messages to be window size. In the results section, we will discuss it in detail.
- **Population Window:** A population window is a set of windows. It actually represents a distribution of windows and is used by our methodology to perform hypothesis testing.

1) Constructing a Graph Using CAN Messages:

In [27], the authors propose an IDS based on recurring sequential message IDs, but this model is vulnerable to intelligent attacks. We consider this a starting point for our methodology and incorporate graph theory to build a solid IDS platform. We divide the CAN bus messages into a number of windows and then try to derive the relationships among all the arbitration IDs for each window.

Empirically, graphs are a common method to indicate the relationships among data. Their purpose is to present data that are too complicated to express using simple text or other forms of data structure. For that reason, they have now turned into one of the most popular fields of research. As graph theory can represent complex relationships of data in a very simple manner, we leverage

graph data structure to represent CAN bus data windows in a meaningful structure.

For any given raw CAN dataset, the proposed Algorithm 1 constructs graphs for every 200 messages (to which we refer as a window) and finally returns the overall constructed graph lists. From Line 4 to Line 8, all the necessary variables are initialized. Then we compute the total number of messages in the given CAN dataset in Line 9. In Line 10, a loop is used to iterate over every CAN bus message from the CAN bus dataset. As our methodology considers the arbitration ID as the node of a graph, so we need to extract the arbitration ID from each CAN message in the dataset. From Line 11 to Line 14, we extract the adjacent CAN messages and their corresponding IDs. Then the algorithm constructs an adjacency list from the arbitration IDs extracted from two sequential CAN messages in Line 15.

2) *Extracting Graph-Based Features*: The graph data structure has several basic properties like the number of edges, the number of nodes, the in-degree, the out-degree, etc. In this step, our proposed method will characterize each of the message windows and then will build the population window by extracting graph properties. In order to extract graph properties from a graph constructed using a window of CAN messages, our methodology uses the outcome of step 1 of the proposed Algorithm 1. In Algorithm 1, Line 17 to Line 19 extracts the node number, edge number, and maximum degree from the single constructed graph and stores them in the list of graph properties in Line 20 using the method `fetchGraphProperties()`. After iterating through 200 messages, we initialize the adjacency list and the current graph in Line 21 and Line 22, respectively. In Line 25, we return the whole graph list, which is the population window in our methodology.

3) *Proposed Hypothesis Based on Safe Population Window*: In this step of our proposed intrusion detection methodology, we try to build a hypothesis based on the information of the population window. We have used the popular chi-squared statistical test to build the hypothesis [28]. Using this statistical analysis, we compute a threshold value. The threshold value helps us in the next step to detect the anomalous population. Besides, we introduce a conventional median test to detect a strong replay attack.

Algorithm 2 represents the chi-squared test on our population window. It takes two lists of graphs as inputs and then outputs a boolean value. Out of the two inputs, one is the attack-free graph population and the other is the graph population under test. The boolean value in the output represents whether there is any attack happening or not. In between Line 4 to Line 13 we

Algorithm 1 Graph building algorithm

```

1: Input: CANMessageList[Msg1, Msg2, ..., Msgn] ▷ Raw CAN bus data array
2: Output: GraphList[GP1, GP2, ..., GPn] ▷ Graph array of CAN bus data
3:
4: Initialize: GraphList ← []
5: PreviousID ← -1
6: CurrentGraph ← {} ▷ Start with an empty graph
7: adjacencyList ← {} ▷ A dictionary for adjacency list
8: graphCount ← 1
9: N ← length(CANMessageList[Msg1, Msg2, ..., Msgn])
10: for index in range (0, N - 1) do ▷ Loop through all the CAN messages
11:   CANSingleMsg1 ← CANMessageList[index]
12:   CANSingleMsg2 ← CANMessageList[index + 1]
13:   arbitrationID1 ← ExtractID(CANSingleMsg1)
      ▷ Extraction of Arbitration ID from raw CAN data
14:   arbitrationID2 ← ExtractID(CANSingleMsg2)
15:   adjacencyList ← linkGraphNodes(CANSingleMsg1, CANSingleMsg2)
      ▷ Create link between the two graph Nodes
16:   if (length(adjacencyList) == 200) then ▷ If it true then adjacencyList is a graph built from 200 CAN messages
17:     nodeNumber ← countNodeNumber(adjacencyList) ▷ Count number of nodes in the current graph
18:     edgeNumber ← countEdgeNumber(adjacencyList) ▷ Count number of edges in the current graph
19:     Maxdegree ← countDegree(adjacencyList) ▷ Count maximum degree of each ID from the current graph
20:     currentGraph ← fetchGraphProperties(adjacencyList)
21:     adjacencyList ← {}
22:     currentGraph ← {}
23:   end if
24: end for
25: return GraphList

```

initialize the variables that are needed for our proposed methodology. After that, the algorithm extracts the edges of each graph from the graph list from Line 14 to Line 16 for safe attack-free distribution. Finally, a hypothesis is constructed for the safe edge distribution in Line 20.

4) *Comparing Test Population Window to the Base Population Window*: This step of our proposed intrusion detection methodology consists of two functionalities. The first one is to calculate the chi-square value for the test population window and then compare the value with the threshold. The latter one is to calculate the median value for the test population window and then compare the value with the outlier. By using Equation 3

Algorithm 2 Proposed attack detection algorithm

```

1: Input:  $GrapList_{Base}[GP_1, GP_2, \dots, GP_n]$   $\triangleright$ 
   Graph array of attack free CAN bus data,
    $GrapList_{Test}[GP_1, GP_2, \dots, GP_n]$   $\triangleright$  Graph array of
   test data
2: Output:  $isAttacked$   $\triangleright$  True if the input graph is
   attacked or false otherwise
3:
4: Initialize:  $edgeList_{Base} \leftarrow []$ 
5:  $edgeList_{Test} \leftarrow []$ 
6:  $Chi_{Null} \leftarrow 0$ 
7:  $Chi_{Test} \leftarrow 0$ 
8:  $Median_{Null} \leftarrow 0$ 
9:  $Median_{Test} \leftarrow 0$ 
10:  $\sigma_{Null} \leftarrow 0$ 
11:  $threshold \leftarrow 0$ 
12:  $N_{Base} \leftarrow length(GrapList_{Base}[GP_1, GP_2, \dots, GP_n])$ 
13:  $N_{Test} \leftarrow length(GrapList_{Test}[GP_1, GP_2, \dots, GP_n])$ 
14: for  $index$  in  $range(0, N_{Base})$  do
15:    $edgeList_{Base} \leftarrow$   $fetchEdgeNumbers(GraphList_{Base}[index])$   $\leftarrow$ 
16: end for
17: for  $index$  in  $range(0, N_{Test})$  do
18:    $edgeList_{Test} \leftarrow$   $fetchEdgeNumbers(GraphList_{Test}[index])$   $\leftarrow$ 
19: end for
20:  $Chi_{Null} \leftarrow ExtractDistribution(edgeList_{Base})$   $\triangleright$ 
   Construct hypothesis using attack free graph
21:  $Chi_{Test} \leftarrow ExtractDistribution(edgeList_{Test})$   $\triangleright$ 
   Construct hypothesis using test data
22:  $threshold \leftarrow FindSignificanceLevel(Chi_{Null})$   $\triangleright$ 
   Find threshold using the base distribution
23:  $\{Median_{Null}, \sigma_{Null}\} \leftarrow$   $ExtractDistribution(edgeList_{Base})$   $\triangleright$  Compute
   median and standard deviations using attack free graphs
24:  $Median_{Test} \leftarrow ExtractDistribution(edgeList_{Test})$   $\triangleright$ 
   Compute median using test data
25: if  $(Chi_{Test} \leq threshold)$  then
26:    $isAttacked \leftarrow True$   $\triangleright$  Attack detected
27: else if  $(Median_{Test} > (Median_{Null} + 3\sigma_{Null}))$  then
28:    $isAttacked \leftarrow True$   $\triangleright$  Attack detected
29: else
30:    $isAttacked \leftarrow False$   $\triangleright$  CAN data is safe
31: end if
32: return  $isAttacked$ 

```

and Equation 4 we can detect the anomalous population.

$$Chi_{Test} \leq threshold, [Chi_{Test} = X_c^2]; No \text{ attack} \quad (3)$$

$$Chi_{Test} > threshold, [Chi_{Test} = X_c^2]; Attack \quad (4)$$

In Line 17 to Line 19 of Algorithm 2, we extract the edges from the list of graphs that will be tested. In Line 21, a test hypothesis is made based on the same

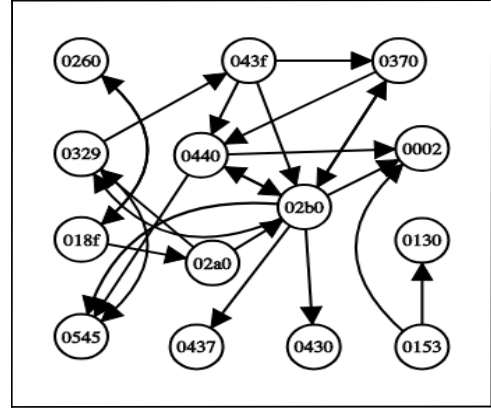


Fig. 2: We use real CAN message data to build a directed graph that represents the sequence of messages.

rules as the attack-free distribution hypothesis or the base hypothesis and the threshold is defined in Line 22 based on the details of the base hypothesis. To detect the replay attack, we incorporate the median test [29]. For this, the Algorithm 2 compute median ($Median_{Null}$) and standard deviation σ_{Null} using attack free data and $Median_{Test}$ of attacked data in Line 23 to Line 24. Finally, the algorithm takes the decision about the test distribution by comparing the test hypothesis with the threshold or our defined outliers ($Median_{Null} + 3\sigma_{Null}$) from Line 25 to Line 31 and returns whether the CAN data is safe or not in Line 32. Our assumed outliers exhibits excellent results and we will discuss in detail in Section III-B and Section IV-A.

B. Exploratory Data Analysis

We have chosen a real vehicle dataset provided by the Hacking and Countermeasure Research Lab [30]. The dataset includes both attack-free and corrupted data with various kinds of attacks. Those attacks include DoS, fuzzy, spoofing, and replay attacks on CAN data.

First, we build graphs using Algorithm 1 with raw CAN bus data. Figure 2 shows an example of a graph generated using the proposed methodology. The nodes of the graph represent arbitration IDs of the CAN bus, and the edge between two nodes indicates CAN bus sequential messages. The direction of the edge indicates the order of the sequence of the messages. For example, if node 043f has an edge with node 0440 and the direction of the edge goes from 043f to 0440, it means arbitration ID 0440 was followed by the message with arbitration ID 043f.

First, we divided the real vehicular CAN bus data into a few windows. The size of each window is 200 messages. However, this number is user-defined, and it is possible to change depending on the design robustness.

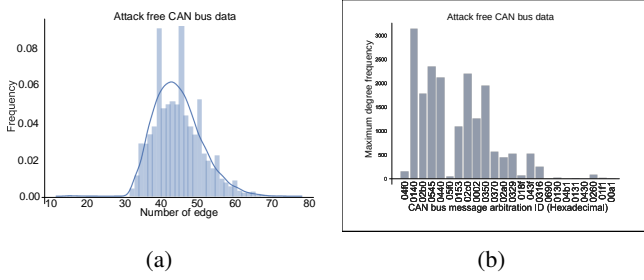


Fig. 3: (a) Attack-free CAN data edge distribution shows a normal distribution, and (b) the attack-free CAN data maximum degree distribution exhibits a regular pattern.

At a 1Mbit/sec speed, a CAN transmits about 8.7K messages/sec. Hence, designers can select how frequently they want to authenticate the CAN. After selecting the window size, we build the graph for each of the windows and derive the common graph properties like edge number and maximum degree distribution for each window. The attack-free CAN data edge distribution shows a normal distribution, as shown in Figure 3(a). Similarly, the attack-free CAN data maximum degree distribution exhibits a regular pattern, as shown in Figure 3(b).

Now we will discuss the graph properties of the dataset with different kinds of attacks. Figure 4(a) represents the distribution of edges for a DoS attack. Unlike attack-free CAN data, the DoS-attacked data do not exhibit a normal distribution. Figure 5(a) shows the situation of the maximum degree for a CAN dataset with a DoS attack. Clearly, a single arbitration ID (0000) dominates the distribution and occupies the CAN network with the highest-priority messages.

Unlike the DoS attack, the graphs with a spoofing-attacked dataset show a bimodal distribution with two distinct peaks, as shown in Figure 4(b). However, similar to a DoS attack, the spoofing-attacked maximum edge distribution has a distinguishable high occurrence of ID 0316 compared to the other IDs, as shown in Figure 5(b).

Similar to the spoofing attack, the graphs with a fuzzy-attacked dataset show a bimodal distribution with two distinct peaks, as shown in Figure 4(c). However, unlike the spoofing attack, the fuzzy-attacked maximum edge distribution has no distinct characteristics compared to the attack-free data as shown in Figure 5(c).

Unlike other attacks, the graphs with a replay-attacked dataset show a normal distribution, as shown in Figure 4(d). In addition, replay-attacked maximum edge distribution has no distinct characteristics compared to the attack-free data, as shown in Figure 5(d).

Apart from impersonation or replay attacks, the data distributions of different attacks are not only different from the attack-free CAN data distribution but also different from each other. We summarize in statistical terms

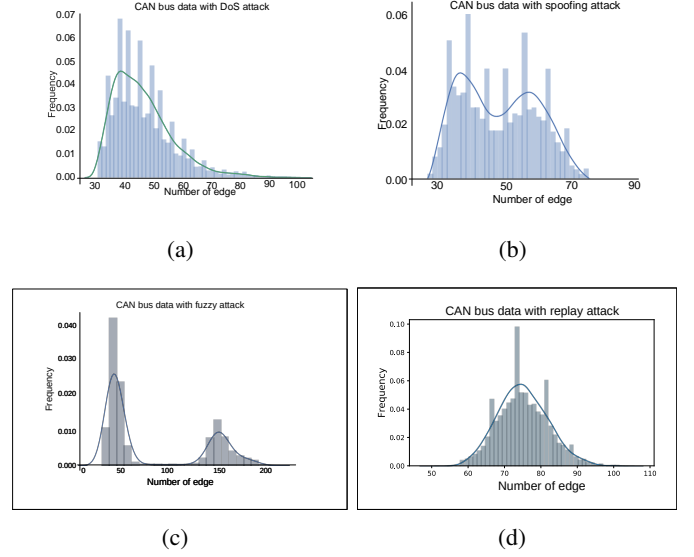


Fig. 4: (a) The DoS-attacked CAN data edge distribution shows a positively skewed distribution, (b) the spoofing-attacked CAN data edge distribution shows a bimodal distribution, (c) similar to spoofing attack, the fuzzy-attacked CAN data edge distribution shows a bimodal distribution, and (d) similar to attack-free CAN data, the edge distribution of replay-attacked data shows a normal distribution.

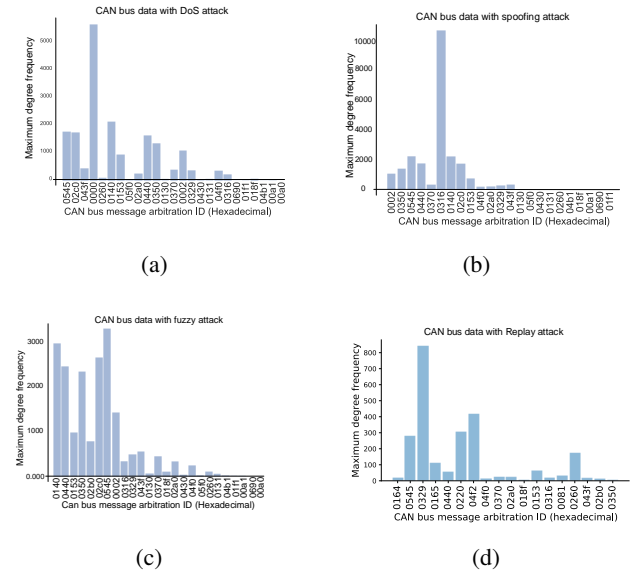


Fig. 5: (a) The DoS-attacked CAN data maximum degree distribution exhibits an irregular pattern with arbitration ID 0000, (b) the spoofing-attacked CAN data maximum degree distribution exhibits an irregular pattern with arbitration ID 0316, (c) The fuzzy-attacked CAN data maximum degree distribution exhibits a regular pattern, and (d) similar to the attack-free CAN data, the replay attacked maximum degree distribution exhibits a regular pattern.

TABLE II: In summary, we can say that among all the attacks, impersonation or replay attack is difficult to detect due to the symmetric edge and maximum degree distributions compared to the attack-free data.

Analysis	Attack free	DoS	Spoofing	Fuzzy	Replay
Mean (edge)	44.6	46.6	49.1	79.8	75.2
Median (edge)	44.0	45.0	49.0	46.0	75.0
Skewness (edge)	Moderate	High	Similar	Moderate	Similar
Max degree ID (%)	0140 (16.9)	0000 (30.8)	0316 (46.4)	0545 (16.8)	0164 (31)

the overall situation of the data distributions in Table II. In the exploratory data analysis, we consider the central tendency or mean of the distribution and the asymmetry of a probabilistic distribution. In our attack-free dataset graph collection, the edge distribution has a mean of 44.6. On the other hand, the DoS, fuzzy, spoofing, and replay attacks have a mean of 46.6, 49.1, 79.8, and 75.17, respectively. In addition, we compute the median of edge distribution which is important for outliers detection, as shown in Table II. The attack free, DoS, fuzzy, spoofing, and replay attacks edge distributions have a median of 44.0, 45.0, 49.0, 46.0, and 75.17, respectively.

Table II also shows the skewness of all the edge distributions for attack-free and attacked datasets. Spoofing and replay attack edge distributions seem symmetric to the attack-free dataset edge distribution. On the other hand, the attack-free and fuzzy attack edge distributions are moderately positive-skewed. Finally, the DoS attack edge distribution is highly skewed. If we look at the maximum degree of CAN arbitration IDs in the graph distribution, it shows that different kinds of attack use different IDs, resulting in dissimilar maximum degrees.

Finally, exploratory analysis proves that the conversion between raw CAN data to the graph gives us a clear indication of an attacked or attack-free CAN bus. Using this technique, we can fetch some extraordinary information from the converted graph. Finally, the graph properties can be used to distinguish different attacked and attack-free situations of the CAN bus system.

IV. EXPERIMENTAL RESULTS AND EVALUATION

In order to verify the proposed methodology, we use a real CAN dataset and performed analysis on an Intel Xeon(R) 3.8 GHz 8-core processor with 32 GB RAM using our proposed algorithm in Python language. For our analysis, we consider about 23K graphs. We divide the result section into three parts: In Section IV-A, we first will discuss the detection methodology for different attacks using the proposed graph-based chi-square test

and median test. Then, in Section IV-B, we will identify the level of significance (LoS).

A. Attack Detection

For detecting an attack using the chi-squared test, we build a base hypothesis using the exploratory attack-free CAN data. We define it as a base distribution. Then, any distribution can be compared with the base hypothesis and differences can be found easily. Figure 6(a) is a visual representation of our chi-squared test on an attack-free distribution. The distribution colored as green represents the safe distribution, and on the other hand, the blue distribution represents the distribution under the test. According to our analysis, any attack-free test data exhibit a similar pattern to our base hypothesis, as shown in Figure 6(a). After that, we built test distributions using DoS-, fuzzy-, spoofing, and replay-attacked datasets. Figure 6(b), Figure 6(c), and Figure 6(d) show the chi-squared test on DoS-, fuzzy-, and spoofing-attacked distributions compared with our base hypothesis, respectively.

Among all the CAN monitoring-based attacks, the replay-attacked edge distribution (i.e., Figure 4(d)) shows no difference from the attack-free distribution (i.e., Figure 3(a)). As a result, the chi-squared test can only achieve up to 66% accuracy. Because of this issue, we incorporate the median test by defining outliers, considering median and $3 \times$ (standard deviation) values. Our prediction accuracy increases significantly using this technique. Clearly, we can easily detect any of those CAN-monitoring-based attacks using the proposed methodology. For this analysis, we consider only edge distributions.

Figure 7 shows the confusion matrix of the proposed methodology. We clearly achieve excellent accuracy in detecting all kinds of attacks described in this section when they are individually tested. The misclassification rate is very low. According to our analysis, the misclassification rate is 5.26%, 10%, 0%, and 4.76% for DoS, fuzzy, spoofing, and replay attacks, as shown in Figure 7(a), Figure 7(b), Figure 7(c), and Figure 7(d), respectively. For fuzzy-, spoofing-, and replay-attacks, we are able to classify all of the test cases successfully. Overall, the proposed methodology has only 4.76% misclassification rate DoS-, spoofing-, fuzzy-, and replay-attacked CAN data.

We also measure the robustness of the proposed methodology when multiple intruders attack the CAN, simultaneously. For this analysis, we consider simultaneous DoS and fuzzy attacks and DoS, fuzzy, and spoofing attacks. The misclassification rate is 13.16% for combined DoS and fuzzy attacks, as shown in Figure 8(a).

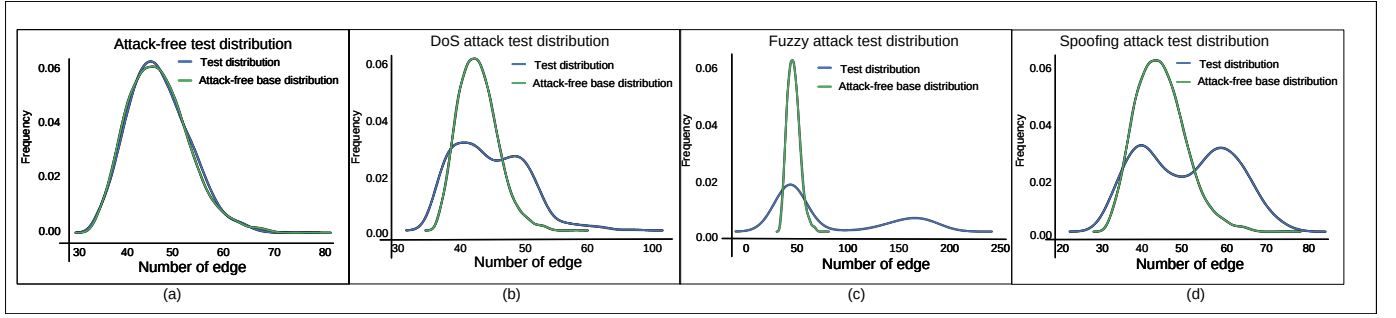


Fig. 6: We used a chi-squared test and built a base-hypothesis using attack-free data: (a) expectedly, the attack-free test distribution and base distributions are identical; (b) chi-squared test easily distinguishes the base normal distribution and bimodal distribution of DoS-attacked data; (c) chi-squared test detects the fuzzy attack compared with the base hypothesis; and (d) chi-squared test easily distinguishes the base normal distribution and bimodal distribution of spoofing-attacked data.

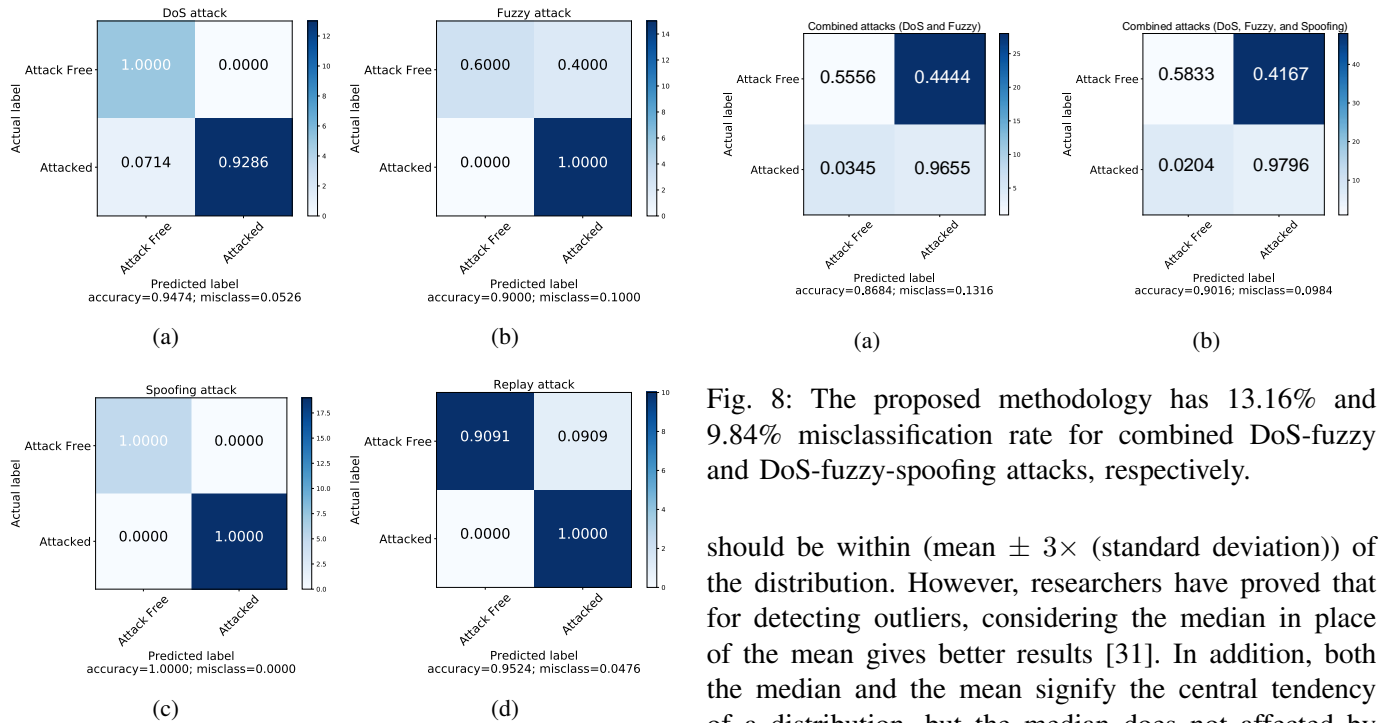


Fig. 7: The proposed methodology has only a 5.26%, 10%, 0%, and 4.76% misclassification rate for DoS, fuzzy, spoofing, and replay attacks, respectively, resulting in only 4.76% overall misclassification rate.

The misclassification rate is 9.84% for combined DoS, fuzzy, and spoofing attacks, as shown in Figure 8(b).

B. Level of Significance Tuning

The LoS is the probability of rejecting a hypothesis. It is critical for any decision, since the threshold value changes depending on the level of significance and DoF . We compute the DoF using Equation 2. In our case, we have two rows, one for the reference distribution and the other for the test distribution. The empirical rule states that in a normal distribution, 99.7% of the data points

Fig. 8: The proposed methodology has 13.16% and 9.84% misclassification rate for combined DoS-fuzzy and DoS-fuzzy-spoofing attacks, respectively.

should be within (mean $\pm 3 \times$ (standard deviation)) of the distribution. However, researchers have proved that for detecting outliers, considering the median in place of the mean gives better results [31]. In addition, both the median and the mean signify the central tendency of a distribution, but the median does not affected by anomalous data. As a result, we considered the median value and divide the reference and test distribution into six regions starting from (mean - $3 \times$ (standard deviation)) to (mean + $3 \times$ (standard deviation)) in a step of one standard deviation. Hence, our column number is 6. Using the chi-square table [32], we can chose the LoS given the threshold and the degree of freedom.

Our test results show the best LoS we should choose corresponding to the threshold value for comparing attack-free or attacked distributions. According to our analysis in Section III-B, the distributions of different attacks have different patterns. Hence, we propose a different level for DoS, fuzzy, spoofing, and replay attacks. Figure 9(a) suggests that a threshold value (15.086) corresponding to a significance level of 0.01 gives us the best prediction accuracy for a DoS attack. In terms of

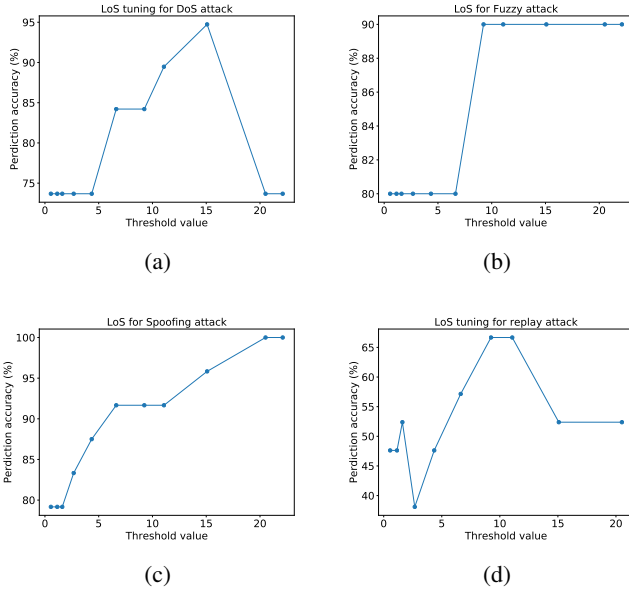


Fig. 9: We identified the best threshold value with level of significance considering the best prediction accuracy.

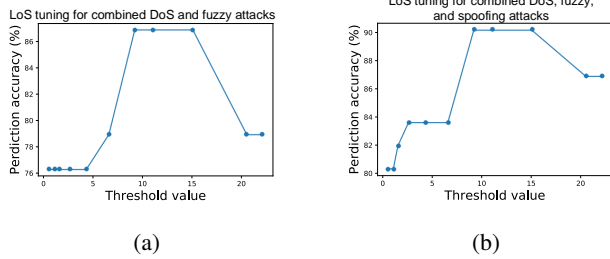


Fig. 10: Similar to individual attacks, we identified the best threshold value with LoS for combined DoS-fuzzy, and DoS-fuzzy-spoofing attacks considering the best prediction accuracy.

spoofing and fuzzy attacks, we propose a significance level of 0.001 (threshold 20.515) and 0.1 (threshold 9.236), as shown in Figure 9(b) and Figure 9(c), respectively. Using a significance level of 0.1 and threshold value of 9.236, the proposed chi-squared test method can achieve up to 66% accuracy, as shown in Figure 9(d). However, when we introduce our proposed median test, the prediction accuracy increases up to 95.24% as shown in Figure 7(d). Figure 10(a) suggests that a threshold value (9.236) corresponding to a significance level of 0.1 gives us the best prediction accuracy of 86.84 for the combined DoS and fuzzy attacks. Using an LoS of 0.1 and threshold value of 9.236, the proposed method can achieve up to 90.16% accuracy for combined DoS, fuzzy, and spoofing attacks, as shown in Figure 10(b).

C. Comparison to Related Work

We evaluated the efficiency of our approach to detect an attack in CAN's message by comparing it to one of the state-of-the-art IDS [27]. To the best of our

TABLE III: The proposed methodology can successfully detect all four (i.e., DoS-, fuzzy-, spoofing-, and replay) kinds of attacks with reasonable accuracy; however, existing ID sequence methodology can not detect any replay attacks.

Type	Method	Accuracy (%)	TPR (%)	FPR (%)	TNR (%)	FNR (%)	Time (μs)
DoS	ID sequence ([27])	100	99.12	100	0.88	0	4.2
	Proposed (LoS = 0.01)	94.74	100	92.86	0	7.14	217.5
Fuzzy	ID sequence ([27])	99.04	98.97	99.39	1.03	0.61	3.2
	Proposed (LoS = 0.1)	100	100	0	100	0	165.7
Spoofing	ID sequence ([27])	86.23	99.3	53.93	46.07	0.7	5
	Proposed (LoS = 0.001)	100	100	0	100	0	258.9
Replay	ID sequence ([27])	–	–	–	–	–	–
	Proposed (LoS = 0.1)	95.24	90.91	100	9.01	0	225.7

knowledge, this is the only methodology that uses CAN bus message sequence to identify CAN attacks. Our method is also constructing a graph to find a pattern among CAN bus message arbitration IDs and using it to detect an attack. Therefore we implemented their approach in the same experimental environment using the same real vehicular CAN message dataset [30] to estimate the effectiveness of our approach.

In the dataset, the attacker targeted the revolutions per minute of an actual vehicle to perform a spoofing attack. When we considered spoofing attack, the proposed methodology has 13.73% better accuracy compared to the existing method, as shown in Table III. When we considered a fuzzy attack, the proposed method exhibits comparable accuracy, however, for DoS attack, the proposed methodology shows 5.26% lower accuracy to the existing ID sequence method. One of the most attractive features of the proposed method is it can detect replay attack with 95.24% accuracy, while the existing method could not detect any replay attacks. Figure 11 shows the misclassification rate of proposed method compared with the state-of-the-art [27]. The current approach requires much lower computation time compared to the proposed method due to the more straightforward implementation. However, the proposed methodology requires only up to 258.9 μs to detect an attack.

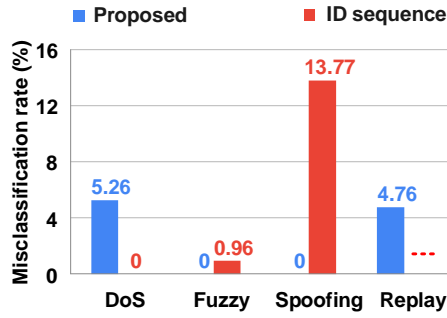


Fig. 11: Considering all four-types of attacks, the proposed IDS has a maximum misclassification rate of 5.26% while the state-of-the-art has 13.77% and not applicable to replay attacks.

V. CONCLUSION

As the involvement of modern technologies in the vehicular industry is increasing the number of cyber threats, we very much need a robust security mechanism to detect them. In this paper, we analyzed the characteristics of all kinds of CAN monitoring-based attacks and proposed a four-stage IDS with the help of graph theory, statistical analysis, and the chi-square method.

To the best of our knowledge, this is the first graph-based IDS for CAN bus communication. Our experimental results show that we have a very low misclassification rate in detecting attacks or attack free data. In terms of DoS, it is only 5.26%; for the fuzzy attack, it is 10%; for replay attack, it is 4.76%; and finally, for a spoofing attack, we were able to detect all the malicious attacks. The proposed methodology exhibits up to 13.73% better accuracy compared to existing ID sequence-based methods [27]. For strong replay attacks, we clearly were not only able to find an attack when it occurred for an infected CAN arbitration ID, but also were able to mark the uninfected arbitration IDs as safe. In this work, we considered only the distribution of the edge and the maximum degree of occurrence of the graph to identify attacks.

In the future, we would like to consider other graph properties such as distribution of nodes, cycles, weighted edges etc. In addition, we will apply different machine learning algorithms in place of the chi-square test to identify anomalies.

REFERENCES

- [1] B. GmbH, "CAN specification version 2.0," 1991.
- [2] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *Proceedings of the USENIX Conference on Security Symposium*. USENIX Association, 2016, pp. 911–927.

- [3] H. Lee, S. H. Jeong, and H. K. Kim, "OTIDS: a novel intrusion detection system for in-vehicle network by using remote frame," in *Annual Conference on Privacy, Security and Trust*, August 2017, pp. 57–5709.
- [4] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 993–1006, April 2015.
- [5] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks—practical examples and selected short-term countermeasures," *Reliability Engineering & System Safety*, vol. 96, no. 1, pp. 11–25, 2008.
- [6] H. Ji, Y. Wang, H. Qin, X. Wu, and G. Yu, "Investigating the effects of attack detection for in-vehicle networks based on clock drift of ECUs," *IEEE Access*, vol. 6, pp. 49 375–49 384, 2018.
- [7] C. Lin and A. Sangiovanni-Vincentelli, "Cyber-security for the controller area network (CAN) communication protocol," in *International Conference on Cyber Security*, December 2012, pp. 1–7.
- [8] K. Iehira, H. Inoue, and K. Ishida, "Spoofing attack using bus-off attacks against a specific ECU of the CAN bus," in *IEEE Annual Consumer Communications Networking Conference*, January 2018, pp. 1–4.
- [9] R. Islam and R. U. D. Refat, "Improving CAN bus security by assigning dynamic arbitration IDs," *Journal of Transportation Security*, April 2020.
- [10] L. Akoglu, H. Tong, and D. Koutra, "Graph based anomaly detection and description: A survey," *Data Mining and Knowledge Discovery*, vol. 29, no. 3, pp. 626–688, May 2015.
- [11] N. Ye and Q. Chen, "An anomaly detection technique based on a Chi-square statistic for detecting intrusions into information systems," *Quality and Reliability Engineering International*, vol. 17, no. 2, pp. 105–112, 2001.
- [12] A. Tomlinson, J. Bryans, and S. Ahmed Shaikh, "Towards viable intrusion detection methods for the automotive controller area network," in *ACM Computer Science in Cars Symposium*, September 2018.
- [13] W. Choi, H. J. Jo, S. Woo, J. Y. Chun, J. Park, and D. H. Lee, "Identifying ECUs using inimitable characteristics of signals in controller area networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 4757–4770, June 2018.
- [14] W. B. Ugoni A., "The Chi square test: an introduction," *COM-SIG Review*, vol. 4, no. 3, pp. 61–64, 1995.
- [15] J. H. Steiger, A. Shapiro, and M. W. Browne, "On the multivariate asymptotic distribution of sequential Chi-square statistics," *Psychometrika*, vol. 50, no. 3, pp. 253–263, Sep 1985.
- [16] R. J. Tallarida and R. B. Murray, *Chi-Square Test*. New York, NY: Springer New York, 1987, pp. 140–142.
- [17] P. Meesad, P. Boonrawd, and V. Nuiplan, "A Chi-square-test for word importance differentiation in text classification," *Proceedings of Computer Science and Information Technology*, vol. 6, 01 2011.
- [18] I. S. Thaseen and C. A. Kumar, "Intrusion detection model using fusion of Chi-square feature selection and multi class SVM," *Journal of King Saud University—Computer and Information Sciences*, vol. 29, no. 4, pp. 462–472, 2017.
- [19] D. Kobayashi, O. Takahashi, H. Arioka, S. Koga, and T. Fukui, "A prediction rule for the development of delirium among patients in medical wards: Chi-square automatic interaction detector (chaid) decision tree analysis model," *The American Journal of Geriatric Psychiatry*, vol. 21, no. 10, pp. 957–962, 2013.
- [20] B. Brumback and M. Srinath, "A chi-square test for fault-detection in kalman filters," *IEEE Transactions on Automatic Control*, vol. 32, no. 6, pp. 552–554, June 1987.

- [21] C. Ling and D. Feng, "An algorithm for detection of malicious messages on CAN buses," in *National Conference on Information Technology and Computer Science*, 2012.
- [22] W. Fu, X. Xin, P. Guo, and Z. Zhou, "A practical intrusion detection system for internet of vehicles," *China Communications*, vol. 13, no. 10, pp. 263–275, October 2016.
- [23] A. Taylor, N. Japkowicz, and S. Leblanc, "Frequency-based anomaly detection for the automotive CAN bus," in *World Congress on Industrial Control Systems Security*, December 2015, pp. 45–49.
- [24] M. Mter and N. Asaj, "Entropy-based anomaly detection for in-vehicle networks," in *IEEE Intelligent Vehicles Symposium (IV)*, 2011, pp. 1110–1115.
- [25] M. Marchetti, D. Stabili, A. Guido, and M. Colajanni, "Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms," in *International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow*, September 2016, pp. 1–6.
- [26] 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 *International Conference on Information Networking*, January 2016, pp. 63–68.
- [27] M. Marchetti and D. Stabili, "Anomaly detection of CAN bus messages through analysis of ID sequences," in *IEEE Intelligent Vehicles Symposium*, June 2017, pp. 1577–1583.
- [28] W. G. Cochran, "The χ^2 test of goodness of fit," *The Annals of Mathematical Statistics*, vol. 23, no. 3, pp. 315–345, September 1952.
- [29] S. Siegel and N. J. J. Castellan, "Nonparametric statistics for the behavioral sciences," *New York: McGrawHill*, 1988.
- [30] H. Lee, S. H. Jeong, and H. K. Kim, "CAN dataset for intrusion detection," in *HCRL*, October 2018.
- [31] C. Leys, C. Ley, O. Klein, P. Bernard, and L. Licata, "Detecting outliers: Do not use standard deviation around the mean, use absolute deviation around the median," *Journal of Experimental Social Psychology*, vol. 49, no. 4, pp. 764 – 766, 2013.
- [32] G. J. Myatt, "Making sense of data: A practical guide to exploratory," *New York: Wiley-Interscience*, 2006.



Rafi Ud Daula Refat received the BSc degree in Computer Science & Engineering from Rajshahi University of Engineering & Technology. He is currently pursuing the Ph. D. degree with the department of Electrical & Computer Engineering, University of Michigan - Dearborn, MI, USA. His research interest focus on cybersecurity and data analysis.



Sai Manikanta Yerram received bachelors degree in Information Technology from Sreenidhi Institute of Science and Technology, Hyderabad, India in 2019. He is a Grad student pursuing Master of Professional Studies in Data Science at the University of Maryland, Baltimore County. His current areas of interest are focused on Machine Learning and their applications.



Riadul Islam is currently an assistant professor in the Department of Computer Science and Electrical Engineering at the University of Maryland, Baltimore County. In his Ph.D. dissertation work at UCSC, Riadul designed the first current-pulsed flip-flop/register that resulted in the first-ever one-to-many current-mode clock distribution networks for high-performance microprocessors. From 2017 to

2019, he was an Assistant Professor with the University of Michigan, Dearborn MI, USA. From 2007 to 2009, he worked as a full-time faculty member in the Department of Electrical and Electronic Engineering of the University of Asia Pacific, Dhaka, Bangladesh. He is a member of the ACM, IEEE, IEEE Circuits and Systems (CAS) society, and IEEE Solid-State Circuits (SSC) Society. He is a member of the Cybersecurity Center for Research, Education, and Outreach at the UM-Dearborn. He holds two US patent and several IEEE/ACM/Springer Nature journal and conference publications in TVLSI, TCAS, JETTA, DAC, ISCAS, MWSCAS, ISQED, and ASICON. His current research interests include digital, analog, and mixed-signal CMOS ICs/SOCs for a variety of applications; verification and testing techniques for analog, digital and mixed-signal ICs; hardware security; CAN network; CAD tools for design and analysis of microprocessors and FPGAs; automobile electronics; and biochips. He is an editorial board member of Semiconductor Science and Information Devices journal.



Hafiz Malik is an Associate Professor in the Electrical and Computer Engineering (ECE) Department at University of Michigan, Dearborn. His research in the areas of automotive cybersecurity, IoT security, sensor security, multimedia forensics, steganography/steganalysis, information hiding, pattern recognition, and information fusion is funded by the National Science Foundation, National

Academies, Ford Motor Company, and other agencies. He has published more than 80 papers in leading journals, conferences, and workshops. He is a founding member of the Cybersecurity Center for Research, Education, and Outreach at the UM-Dearborn. He is also serving a member of Scientific and Industrial Advisory Board (SIAB) of the National Center of Cyber Security Pakistan. He is a member, MCity Working Group on Cybersecurity, since 2015. He is a member of Working Group for IEEE Project 1912–Standard for Privacy and Security Architecture for Consumer Wireless Devices. He is also on the Review Board Committee of IEEE Technical Committee on Multimedia Communications (MMTC).