Automotive Intrusion Detection Based on Constant CAN Message Frequencies Across Vehicle Driving Modes

Clinton Young
Iowa State University
Department of Electrical and Computer Engineering
cwyoung@iastate.edu

Habeeb Olufowobi
Howard University
Department of Electrical and Computer Science
habeeb.olufowobi@howard.edu

Gedare Bloom
Howard University
Department of Electrical and Computer Science
gedare.bloom@howard.edu

Joseph Zambreno
Iowa State University
Department of Electrical and Computer Engineering
zambreno@iastate.edu

ABSTRACT

The modern automobile relies on numerous electronic control units communicating over the de facto standard of the controller area network (CAN) bus. This communication network was not developed with cybersecurity in mind. Many methods based on constant time intervals between messages have been proposed to address this lack of security issue with the CAN bus. However, these existing methods may struggle to handle variable time intervals between messages during transitions of vehicle driving modes. This paper proposes a simple and cost-effective method to ensure the security of the CAN bus that is based on constant message frequencies across vehicle driving modes. This proposed method does not require any modifications on the existing CAN bus and it is designed with the intent for efficient execution in platforms with very limited computational resources. Test results with the proposed method against two different vehicles and a frequency domain analysis are also presented in the paper.

CCS CONCEPTS

• **Security and privacy → Intrusion detection systems**;

KEYWORDS

Controller Area Network; Automotive Anomaly Detection; Frequency Detection

ACM Reference Format:
Clinton Young, Habeeb Olufowobi, Gedare Bloom, and Joseph Zambreno. 2019. Automotive Intrusion Detection Based on Constant CAN Message Frequencies Across Vehicle Driving Modes. In *ACM Workshop on Automotive Cybersecurity (AutoSec '19), March 27,2019, Richardson, TX, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3309171.3309179

1 INTRODUCTION

The modern automobile consists of more than 70 electronic control units (ECUs) that communicate and interact with each other over automotive bus systems [2]. Passenger comforts, infotainment features, and connectivity continue to progress through the growth and integration of Internet-of-Things (IoT) technologies. However, the benefits of increased connectivity and features comes with the penalty of vulnerabilities [13], as demonstrated in Figure 1. There is a lack of security preventing attacks against comfort and infotainment features from compromising safety-critical control systems [3]. Cyber attacks on automotive in-vehicle networks have risen [1, 3] and this has driven a need for security in vehicles. Miller and Valasek demonstrated their ability to control a Jeep Cherokee remotely through a cellular network, leading to the recall of over a million vehicles [8].

Most CAN messages are transmitted at fixed time intervals by design, which makes the message traffic predictable. Many methods for anomaly detection rely on this specific characteristic of CAN for intrusion detection. However, as we will demonstrate in Section 3, during transitions of vehicle driving modes, time intervals between messages can change. Therefore, methods based on constant intervals between messages will fail during transitions of vehicle driving modes.

In this paper, we examine the effectiveness of using constant CAN message *frequencies* for anomaly detection. We demonstrate that CAN message frequencies are close to constant, even during transitions of vehicle driving modes. We also perform a frequency analysis to assess the frequency components of CAN messages. We

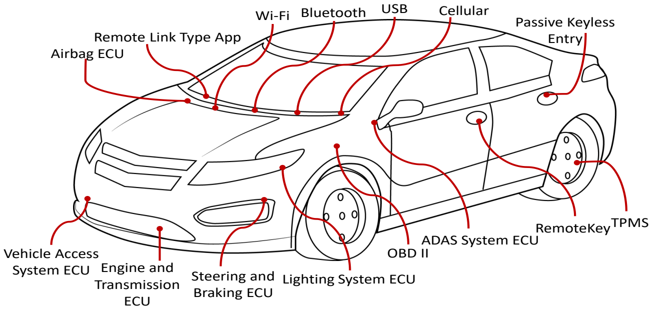

Figure 1: Automotive attack surfaces.

AutoSec '19, March 27, 2019, Richardson, TX, USA
© 2019 Association for Computing Machinery.
ACM ISBN 978-1-4503-6180-4/19/03…$15.00
https://doi.org/10.1145/3309171.3309179

conclude that message frequencies are a better indicator for anomaly detection than time intervals used in many existing methods. Our key contributions are as follows:

- We demonstrate that time intervals between messages can vary during transitions of vehicle driving modes
- We propose a new simple method to ensure the security of the CAN bus that is based on constant message frequencies across vehicle driving modes that does not require any modifications on the existing CAN bus.

The remainder of this paper is organized as follows. In section 2, we discuss automotive intrusion detection systems (IDS). Then, section 3 outlines the method of utilizing constant time interval between messages as the detection feature for automotive intrusion detection and its flaws. In section 4, we present the proposed frequency-based method for intrusion detection and its frequency analysis results with Fourier Transform. In section 5, we outline recent research into the security of CAN bus. In section 6, we summarize the paper and discuss our planned future work.

2 AUTOMOTIVE THREAT AND VULNERABILITY ANALYSIS

We investigate the most common type of attack, message injection, in this paper. This attack can take control of a vehicle's driving operations. The basic idea is that an attacker transmits a packet with the same ID as a legitimate packet as soon as the legitimate packet is transmitted. This will cause other ECUs on the CAN bus to use the data from the attacker's injected message instead of the legitimate one. Even when an attacker is injecting messages, the ECUs still send their messages periodically. Eventually, the rate of messages on the network will be increased by a factor of more than 2 to 100 times, depending on the attacker's injection speed. Miller and Valasek reported that they needed to inject at a rate of at least 20 times faster than normal for their attack to be successful [8]. Because the original ECU is still transmitting its message, an attacker needs to send messages at a fast enough rate to overwrite the normal message with the same ID.

Development of an anomaly-based intrusion detection system (IDS) typically starts with a training or normal model of the monitored system's activity. The IDS compares the current system's activity to the past captured normal model to detect variations in behavior and label those deviations as anomalies. Any deviation not captured in the normal profile could be correctly or mistakenly identified as an intrusion. Having the most complete normal profile is important, so the system does not suffer from high rates of false positives or negatives. The use of anomalies to infer intrusions suffers from a few key challenges:

- Defining a normal model that encompasses all possible expected behavior is extremely difficult. The boundary between normal and anomalous behavior is often blurred.
- Normal continues to evolve, and what is normal currently may not be so in the future.
- Anomalies may not be a result of malicious actions. Data often contains noise which may produce anomalies that can be difficult to distinguish from attacks.
- Attackers try to mask their actions to appear normal, therefore making the task of defining a tight boundary around normal more important, and more difficult.

In the following sections, we will detail how we developed, implemented, and evaluated our IDS to address this threat vector.

3 MESSAGE INTERVAL INTRUSION DETECTION

Numerous works [9, 10, 12] utilize CAN message timing intervals for intrusion detection. The detection process for using CAN message timing intervals is detailed in Figure 2. The anomaly detector usually has two modes - one mode to capture the normal timing intervals for every CAN message and another intrusion detection mode that observes current CAN traffic and compares its message timings to the normal model to detect anomalies. To train the normal model, a few seconds of normal anomaly-free CAN traffic is used to train the IDS. For each CAN ID, the IDS will calculate the interval time, the difference from the previous message time to the current message time, and the average interval time is calculated as shown in Equation (1).

$$\mu = \frac{(\sum_{i=1}^{n} t_i - t_{i-1})}{n} \tag{1}$$

3.1 Message Interval Evaluation

In order to demonstrate the utilization of message intervals as the detection feature, we utilized a traffic capture of normal operation of two vehicles and analyzed the normal message interval timings for all CAN messages. The data set for our first test vehicle is the live vehicle capture data published by Miller and Valasek [8]. This data set contained the CAN traffic of their test vehicle during normal operations. The message injection attacks are simulated by injecting specific messages to create data sets of malicious CAN traffic. During simulations, we can control the rate of injection to allow multi-rate injection attacks and evaluation of the various injection rates. Additionally, we simulated single CAN ID injection along with multiple CAN message ID injection at multiple rates. Figure 3 illustrates the effect message injection has on the message time interval.

To evaluate the IDS based on constant interval timings, the IDS is trained with CAN traffic to build a normal model for all CAN message interval timings. We then applied this IDS against our simulated data sets of message injection attacks. We tested this simple IDS against multiple rates of injection: 2, 5, and 20 times faster than normal values. It was reported that 20 times faster rate

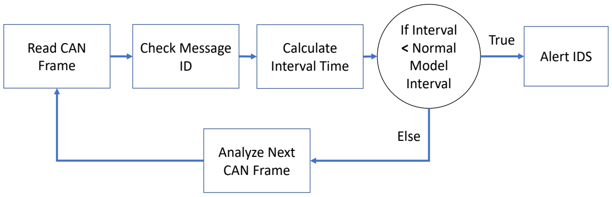

Figure 2: Every CAN message is read and its ID captured. The time interval from current to previous message with the same ID is calculated and compared to the normal model timing interval for that message. If the interval time is less than normal, the IDS will indicate an anomaly and the IDS sends an alert.

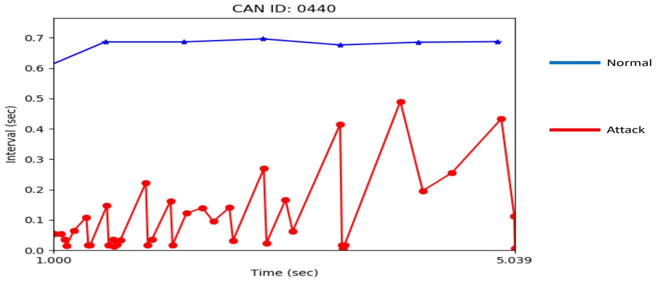

Figure 3: Demonstrating message injection attacks affecting the timings of messages. The simulated attack messages have fluctuating message timings and are shorter than normal depending on rate of injection.

was required for successful attack [8], but we tested for slower rates because we have previously observed a successful attack with a rate of injection of only 2 times faster. Table 1 reports the detection accuracy and false positive rates across the variety of message injection speeds and attacks. Detection accuracy is defined as the number of CAN messages that were correctly identified as having anomalous timings and the false positive rate is the number of incorrectly identified CAN ID messages out of the total messages. Our results show that the faster the rate of injection, the higher the detection rate of anomalies. However, the message timing interval-based IDS also generated increasing false positives when the injection rate increased. Greater injection rate affects the timings of the other CAN messages due to the presence of the additional injected messages.

The data set for our second test was obtained from a vehicle at Oak Ridge National Laboratory. The data set was constructed by logging CAN traffic through the ODB-II port of a real sedan while driving on a dynamometer system, which simulates real road operation. Attacks were performed by injecting malicious messages at high rate to override normal vehicle operations. The malicious messages were constructed by sniffing and spoofing legitimate messages transmitted on the bus. We discovered there were two major issues in the message timing intervals for this second test vehicle.

(1) There were several messages that demonstrated multiple timing intervals. It was assumed that CAN messages have a singular consistent message interval. Numerous previous work stated that all CAN messages have consistent timing intervals [3, 8, 9].
(2) A few CAN messages also had their message timing intervals vary depending on the vehicle's behavior. We expected some variation in the interval but the change that was seen was greater than twice the normal rate.

Table 1: Message Timing Interval Detection Accuracy for Single and Multiple CAN ID Injection Attacks

Attack Type	Message ID	Injection Speed	Detection Accuracy	False Positive
Single Message Injection	0440	2×	75%	0%
		5×	94%	11%
		20×	99%	5%
Multiple Message Injection	0440 and 03D3	2×	0440: 75%	0%
			03D3: 68.75%	0%
		5×	0440: 94%	0%
			03D3: 97.5%	0%
		20×	0440: 99.5%	6.6%
			03D3: 99.4%	6.6%

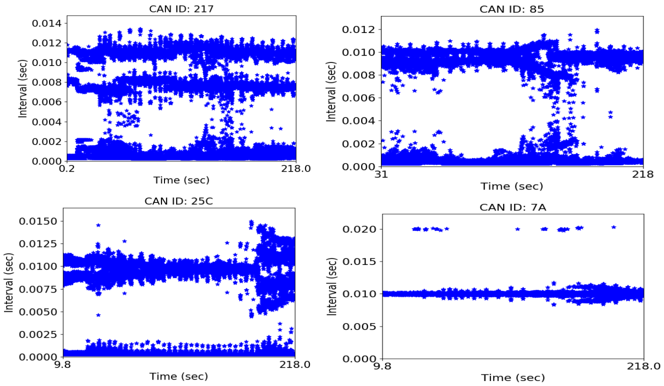

Figure 4: Multiple CAN messages show varying message intervals. Some messages show multiple distinct intervals while some vary due to changes in vehicle operations.

When the IDS was applied to the data set from vehicle 2, it generated 30 percent false positives, with 41 other message IDs detected as anomalous. These poor results were caused by the inconsistencies in the message timing intervals.

For example, in the CAN data set for the second test vehicle, several CAN messages showed non-periodic and multiple timing intervals. Figure 4 illustrates that multiple CAN IDs have varying message intervals. The data set for vehicle 2 had 137 different CAN messages, and about 30 of these messages showed the inconsistencies in the message timing intervals. The differences in CAN message timing behavior and required injection attack rates between the test vehicles may indicate that CAN may differ depending on manufacturer and vehicle. This inconsistent behavior is problematic for anomaly detection algorithms that are based on the assumption of consistent and constant message timing intervals.

4 MESSAGE FREQUENCY DETECTION

We observed that the frequency of the messages remained relatively consistent, even while the CAN message intervals varied. Additionally, we noticed that the number of messages stays consistent even as the vehicle changes modes of operation. Thus, we hypothesize the rate of messages is a better indicator for anomaly detection compared to message interval.

Our proposed anomaly detection method is based on the message frequency: frequency (f) is equal to the rate of messages (m) transmitted in a set time interval (t) - (f=m/t). When the frequency of messages increases by a factor of more than twice the normal value, an anomaly is indicated. As we reported earlier, for an attack to be successful, the rate of injection must be at least twice the normal value. We implemented the frequency-based algorithm in our IDS. Our IDS scans current CAN traffic and calculates the frequency of messages for every CAN ID. If the frequency of messages deviates at a rate of greater than 2 times normal, the IDS will indicate an anomaly for said CAN ID.

It should be noted that this approach is relatively simple in complexity as to be implemented in a simple OBD-II dongle. The dongle is likely connected to the vehicle's OBD port and acts as an additional ECU on the bus. In addition, this proposed method is cost-effective since it does not require any modifications to the native CAN bus.

4.1 Frequency Domain Analysis

We also performed a frequency domain analysis to assess the frequency components of the time series CAN data. If the CAN messages have a constant frequency, it should show a singular peak in the frequency domain. This frequency should change during an attack if it affects the CAN message transmission rates. The time series data for test vehicle 2 was converted into the frequency domain with the Fast Fourier Transform and investigated the effects of different driving modes and message injection attacks. Some data processing was needed to get the discrete CAN time signals into a state which we could apply the Fourier Transform. The CAN time stamps were converted into a square wave. The signal was held high during transmission of the specific CAN message and low when the message was not transmitting. The sampling frequency was (*fs*) as $fs = D/t$ with the number of data points (D) and the time interval (t). In our data sets, the amount of data points varies depending on the CAN message. Typically, we had anywhere from 2000 to 8000 data points depending on CAN message in the logs. With our timing interval, our average sampling frequency for our CAN messages was 200 samples per second. One limitation in using the FFT function is that the number of data points must be a number that is a power of two. Some of our samples were padded with zeros to meet this requirement.

Converting our time series data into square waves allowed us to apply FFT to our data. We chose this representation of our data to simulate the transmission and hold times of each CAN message being transmitted on the bus. However, perfect square waves with equal magnitude correspond to a FFT output with multiple frequency peaks. Figure 5 shows that a square wave decomposes into multiple sine waves at varying magnitudes. Messages that have a single consistent message interval showed this ideal FFT behavior. However, messages that demonstrated multiple timing intervals had more complicated FFT output, as seen in Figure 6. We show that multiple factors of CAN messages may affect the output of our Fourier Transform, including rate of transmission, interval behavior of messages, changes in driving mode, and normal variations in normal timing.

To conduct a frequency analysis against an attack, we used the same injection data from vehicle 2. During a message injection attack, the frequency of messages is increased. However, we observed during an attack, the frequency peaks stayed at the same frequencies while the magnitude of the peaks changed. This result makes sense when understanding that during an attack, the input is now a duplicated square wave to the initial input. Attack traffic is two square waves at the same frequency just offset from each other, hence the FFT plot has the same frequency peaks but at a higher magnitude. These results are reflected in Figure 7.

These results open the possibility that frequency domain analysis is able to discern hidden features that are not present in simple timing analysis. Further investigation is needed to determine the applicability of frequency domain analysis towards intrusion detection.

4.2 Implementation and Evaluation

4.2.1 Vehicle Modes of Operation. We examined the two causes of false positives and message timing irregularities: 1) Vehicle mode of operation and 2) CAN message behavior. CAN message timing intervals were affected by normal changes in the vehicle and generated false positives in anomaly detection. We chose to use message frequency as opposed to message interval to handle these normal behaviors and changes in the model of vehicle and in vehicles themselves.

As the vehicle changed modes of operation, Table 2 shows the rate of messages varies at a rate less than 20 percent. Our vehicle had an average transmission rate of 4402 messages per second through all modes of operation. Figure 8 shows an example CAN message whose timing interval deviated when the vehicle changed modes, hence generating false positives in an interval-based IDS. We demonstrate that the frequency is more consistent as the vehicle changes driving modes and eliminates these false positives. We demonstrated that a successful message injection attack will increase the rate of the injected message by more than a factor of 2. Therefore, the variability in rate of messages during normal operation is negligible when compared to the change caused by injection attacks.

Additionally, we examined the messages that had varying message intervals. As we discussed above, the timing intervals of these

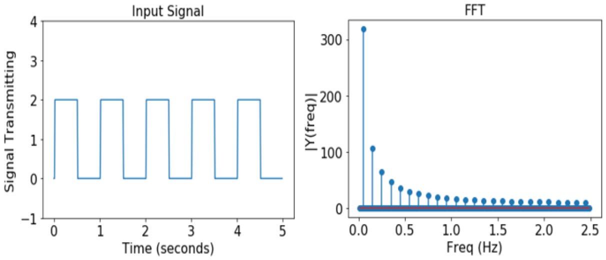

Figure 5: Left plot depicts an ideal square wave, which represents the converted CAN message data. The messages get transmitted at a fixed interval and have a certain transmission time represented by the duty cycle of the wave. The right plot shows the Fourier transform of the square wave.

Table 2: Different Driving Modes Message Count

Driving Mode	Time Duration (Seconds)	Message Rate (Msgs/Sec)
Key ON	10	4448
Key ON to Start	10	4432
Shift to Reverse	15	4356
Accelerate Reverse	10	4351
Decelerate Reverse	10	4353
Shift to Drive	10	4352
Accelerate	15	4413
Maintain Speed	10	4513

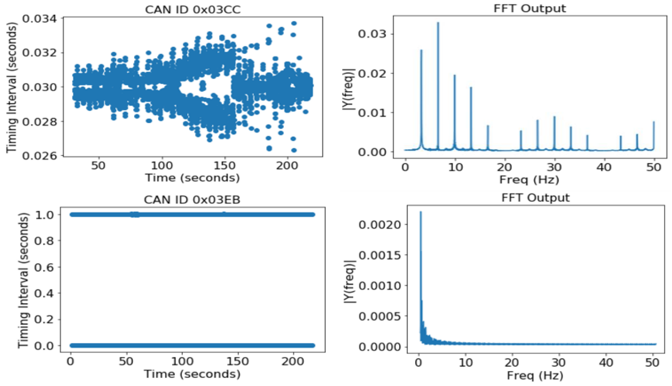

Figure 6: On the left side there are two examples of CAN messages with irregular timing intervals. The right side shows their respective FFT outputs. Variations in the message timings can affect the FFT output.

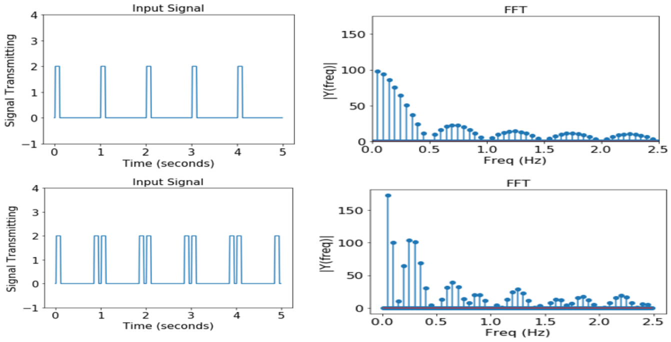

Figure 7: As the message rate doubles during injection attack, the magnitudes of certain frequency peaks will increase.

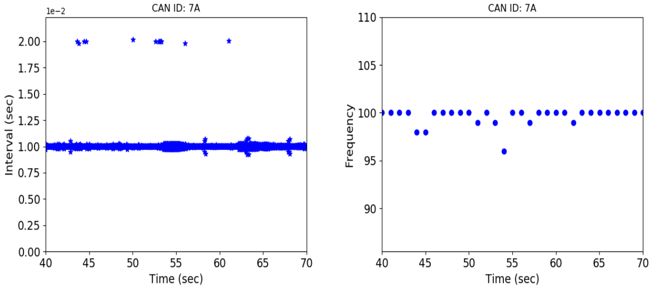

Figure 8: CAN message 0x7A varied when the vehicle shifted driving modes. The timing interval increased by a factor of 2. However, the message frequency of the same message over the same driving transitions, the frequency does not vary more than 5 percent.

messages demonstrate inconsistent behavior. There are certain points where the interval doubles its normal or there are multiple intervals. However, the frequency of these messages never varies more than 20 percent. This variation is within normal parameters.

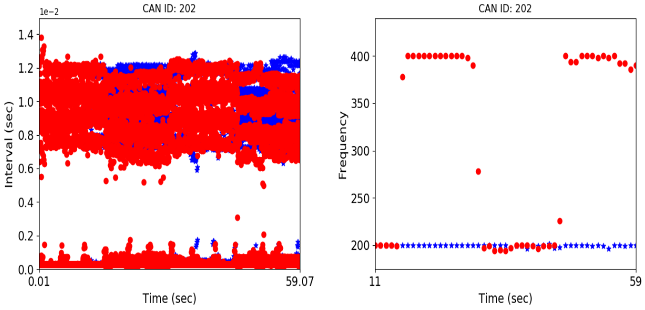

Figure 9: A comparison of the effect message injection attack has on the interval and frequency of CAN ID: 0x202. Left: Message shows multiple variable timing intervals. Injection attack (red) alters the interval of messages by shortening them. Right: By changing timing to frequency, it is clear when message injection attack is occurring, it can be shown that the frequency is consistently at 200 msgs per second normally (blue).

The dips in message rate may be attributed to the delay caused by higher priority messages on the bus as the vehicle is in operation and are not indicative of malicious anomalies.

4.2.2 Message Injection Attack. The number of messages will increase during a message injection attack and therefore the frequency of certain messages will increase. To demonstrate the change in frequency during an injection attack, we simulated an injection attack with the backup light message with ID of 202. The attacks were simulated by injecting malicious messages at a high enough rate to override the normal vehicle operations through the ODB-II port. It required a rate of at least 2 times faster than normal for the desired attack to be successful, as in the backup light turned on. We had 15 seconds of normal traffic, followed by 15 seconds of message injection. This was then repeated for a total of 60 seconds. The frequency doubles in rate during attacks.

Figure 9 shows the captured normal traffic is represented in the blue. The frequency of this particular message was 200 messages per second. The captured message frequency when we injected messages is represented in red. Figure 9 shows that the frequency of messages doubles to 400 message per second when we are injection messages.

We evaluated our message frequency-based IDS against the message injection attack for both test vehicles. Using normal traffic data as the training data, we captured the normal frequency for every CAN ID. The IDS then compared current captured traffic and calculated the frequency for every message. If the frequency increased by 2 times normal, an anomaly was indicated. Similar to interval-based intrusion detection, as the injection rate increased, so did the false positive rate. This is due to the increased amount of malicious packets which at such a high rate will alter the timings of normal messages. The results are summarized in Table 3. It shows that the detection accuracy increased for all injection rates, while decreasing false positives for vehicle 1. While interval detection generated numerous false positives in vehicle 2, frequency-based detection greatly improved detection and false positive rates. We show that frequency-based detection has better detection rates and maintains low rates of false positives compared to current interval-based detection approaches even when applied to different vehicles.

Table 3: Comparison of Intrusion Detection Systems

Vehicle	Detection Type	Detection Accuracy	False Positive
1	Interval	75%	0%
	Frequency	100%	0.7%
2	Interval	96.9%	30%
	Frequency	100%	1.4%
Moore et al. [9]	Interval	99.9%	0.29%
Seo et al. [11]	Generative Adversarial Nets	96.5%	3.8%
Kang et al. [5]	Deep Neural Network	97.8%	1.6%

5 RELATED WORK

Research into CAN bus security has shown the lack of security in automotive systems. Koscher et al. [6] were the first to implement and demonstrate practical attacks on vehicles. They were able to launch attacks by directly interfacing with the OBD-II port. They concluded vehicles should implement a intrusion detection method to detect when a vehicle is being attacked. Checkoway et al. [3] later demonstrated that a vehicle can be exploited remotely. They were able to gain access to the vehicle without having prior physical access, and attack the vehicle over a broad range of attack vectors, including Bluetooth and infotainment systems. The authors concluded that security practices in vehicles should use similar methods as traditional networks to restrict access and improve security.

Hoppe et al. [4] proposed an anomaly-based IDS that is placed on the CAN bus so that it can listen to the network traffic. Their proposed IDS would examine the rate of transmission of specific messages and compares it to what is normal to detect additional or missing messages. Deviations from the expected normal number of messages transmitted are identified as anomalies.

Markovitz et al. [7] proposed a novel domain-aware anomaly detection system for CAN bus traffic. They developed a greedy algorithm to split CAN messages into fields and classify these fields into specific types they observed. Their anomaly detection system uses the classifiers to characterize the fields and build a model for the messages, based on their field types in the learning phase.

Song et al. [12] and Moore et al. [9] both proposed intrusion detection algorithms based on the regularity of CAN message timing intervals. They evaluated how different types of message injection attacks affect the timing intervals of CAN messages. They both determined that an anomaly detection system monitoring the inter-signal wait times of CAN traffic can detect message injection attacks.

Due to limited computational resources in the host platforms, these works proposed simple intrusion detection systems based on message interval timing. However, the effectiveness of an interval-based IDS may degrade significantly due to the changes of time intervals during transitions of vehicle driving modes. Thus, this paper presents a new and simple algorithm that is based on message frequency and is effective across transitions of vehicle driving modes.

6 CONCLUSIONS

In this paper, we demonstrated the basic premise that all CAN messages have consistent timing intervals is not true. Different vehicles and changes in normal driving operation can alter these timing intervals, this makes IDS approaches based on constant timing intervals not reliable. We propose, implemented, and evaluated a frequency-based approach that can resolve the issues encountered by interval-based approaches. Besides just detecting message injection attacks, our approach is able to handle timing variations from normal driving behavior and can be implemented on multiple vehicles. Our method is also light-weight as it does not require changes to the native CAN, this makes our approach applicable to a variety of vehicles.

Future work involves improving the detection and false positive rates of our approaches and applying the IDS on more vehicles. We aim to improve response times by shortening our timing window and we will classify which anomalies are actual intrusions to improve false positive rates. Additionally, we aim to combine the frequency-based approach with a rule-based IDS, similar to hybrid IDSs seen in traditional computing systems. Currently, this detection approach only detects message injection attacks. When used in combination with other detection approaches, we aim to create a more comprehensive automotive intrusion detection system.

ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under Grant No. CNS 1646317 and CNS 1645987.

REFERENCES

[1] Paul Carsten, Todd R Andel, Mark Yampolskiy, and Jeffrey T McDonald. 2015. In-vehicle networks: Attacks, vulnerabilities, and proposed solutions. In *Proc. of the 10th Annual Cyber and Information Security Research Conference.*

[2] Robert Charette. 2009. This car runs on code. *IEEE Spectrum* 46, 3 (2009).

[3] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. 2011. Comprehensive Experimental Analyses of Automotive Attack Surfaces.. In *Proc. of USENIX Security Symposium.*

[4] Tobias Hoppe, Stefan Kiltz, and Jana Dittmann. 2008. Security Threats to Automotive CAN Networks — Practical Examples and Selected Short-Term Countermeasures. In *Proceedings of the 27th International Conference on Computer Safety, Reliability, and Security (SAFECOMP '08).* Springer-Verlag, Berlin, Heidelberg, 235–248. https://doi.org/10.1007/978-3-540-87698-4_21

[5] Min-Joo Kang and Jewon Kang. 2016. Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security. In *PloS one.*

[6] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, and Hovav Shacham. 2010. Experimental security analysis of a modern automobile. In *Proc. of IEEE Symposium on Security and Privacy (SP).*

[7] Moti Markovitz and Avishai Wool. 2017. Field classification, modeling and anomaly detection in unknown CAN bus networks. *Vehicular Communications* 9 (2017), 43–52.

[8] Charlie Miller and Chris Valasek. 2015. Remote exploitation of an unaltered passenger vehicle. BlackHat USA.

[9] Michael R. Moore, Robert A. Bridges, Frank L. Combs, Michael S. Starr, and Stacy J. Prowell. 2017. Modeling Inter-signal Arrival Times for Accurate Detection of CAN Bus Signal Injection Attacks: A Data-driven Approach to In-vehicle Intrusion Detection. In *Proceedings of the 12th Annual Conference on Cyber and Information Security Research (CISRC '17).* ACM, New York, NY, USA, Article 11, 4 pages. https://doi.org/10.1145/3064814.3064816

[10] Habeeb Olufowobi, Gedare Bloom, Clinton Young, and Joseph Zambreno. 2018. Work-in-Progress: Real-Time Modeling for Intrusion Detection in Automotive Controller Area Network. In *Real-Time Systems Symposium (RTSS).* IEEE.

[11] Eunbi Seo, Hyun Min Song, and Huy Kang Kim. 2018. GIDS: GAN based Intrusion Detection System for In-Vehicle Network. *16th Annual Conference on Privacy, Security and Trust (PST)* (2018), 1–6.

[12] Hyun Min Song, Ha Rang Kim, and Huy Kang Kim. 2016. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. In *Proc. of International Conference on Information Networking (ICOIN).*

[13] Bowen Zheng, W. Li, P. Deng, L. Gérardy, Q. Zhu, and N. Shankar. 2015. Design and verification for transportation system security. In *Proc. of Design Automation Conference (DAC).* https://doi.org/10.1145/2744769.2747920