IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 23, 2020, accepted December 21, 2020, date of publication December 23, 2020,
date of current version January 6, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3046862

Clock-Based Sender Identification and Attack Detection for Automotive CAN Network

JIA ZHOU[1,2], GUOQI XIE[1,2], (Senior Member, IEEE), SIYANG YU[3], AND RENFA LI[1,2], (Senior Member, IEEE)

[1]Key Laboratory for Embedded and Network Computing of Hunan Province, Changsha 410082, China
[2]College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China
[3]College of Information Technology and Management, Hunan University of Finance and Economics, Changsha 410000, China

Corresponding author: Renfa Li (lirenfa@hnu.edu.cn) and Guoqi Xie (xgqman@hnu.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61932010, Grant 61672217, Grant 61702172, and Grant 61972139.

ABSTRACT Building the security mechanism for Controller Area Network (CAN) to defend against attack has drawn substantial attention recently. Fingerprinting ECUs to provide the ability of authentication based on the physical characteristics can protect the CAN network effectively. The clock skew which is unique and stable can be exploited to pinpoint the attacker and detect intrusion. However, a common downside of existing clock-skew-based approaches is that the estimation process can be affected by the message scheduling or arbitration. In our work, a novel intrusion detection system (IDS) that exploits the inherent difference in the clock of devices for automotive CAN network is designed. The estimation process of clock skew in our approach relies only on the time measurement of a single CAN frame. Thus, the disturbance from the data-link layer can be avoided. Since the performance of our IDS depends heavily on the accuracy of estimated clock skew, our approach is evaluated on CAN networks with different settings to simulate cases in which the sampling rate is sufficient or not. The feasibility as well as the limitation of our approach are presented in our work. The evaluation shows that our IDS can identify the sender and detect attacks with an average identification rate of more than 99.7% when the sampling rate is sufficient. Besides, the performance degradation as low sampling accuracy is shown and feasible measures for improvement are also discussed.

INDEX TERMS Attack identification, automotive security, controller area network, intrusion detection.

I. INTRODUCTION

Nowadays, the vehicles are gradually becoming an mobile computing platform with various external connection channels. The increasingly number of communication techniques applied to vehicles, such as Wifi, Bluetooth, 5G, on-board diagnostics ports and so on, has made the vehicle no longer a closed unit. However, the internal communication systems of vehicles fail to adapt to the challenges brought by the connected vehicles. More and more automotive networks have been the target of security attack as reported. The malicious adversaries can manipulate the vehicle's behaviors and even control the safety-critical function via intruding the automotive network. Miller and Valasek [1] have successfully demonstrated how to compromise the internal communication systems on a production vehicle of Jeep Cherokee and make it stop regardless of driver's input while running on a highway. This has made an recall of 1.4 million cars by Chrysler. For the sake of safety and cost, there is no significant update of internal communication systems of vehicle so far particularly the CAN network. CAN is still the most popular communication protocol for in-vehicle network which bears important role for safety-critical functions such as power train and transmission. Researchers [2] have evaluated the security and explored the vulnerabilities of CAN bus of a production vehicle. The Tencent Keen Security Lab [3] has demonstrated that it is feasible to compromise the Electronic Control Units (ECUs) on the CAN network over a wireless connection. Once any ECU on the CAN network has been infiltrated, it is enough for attackers to manipulate the safety-critical functions [4]. It is very important to design defense mechanism for CAN to protect vehicles.

CAN is a well-developed communication protocol which have been proven effective and in use over 30 years.

The associate editor coordinating the review of this manuscript and approving it for publication was Wen Chen.

Many important topics about CAN such as real-time analysis [5]–[7] and task scheduling [8] are well studied. Nowadays, there are much research which focus on the security concerns of CAN network. The intrinsic shortcomings of CAN protocol, such as lacking of mechanism for authenticity verifying, low available bandwidth and short data payload of CAN frames, limit the traditional security mechanism such as message authentication and encryption [9]–[11] to be applied on automotive CAN network. Intrusion Detection System (IDS) is an popular alternative [12], [13]. Our work focuses on the IDSs which utilize the unique difference between physical characteristics in devices to provide the ability of intrusion detection and attacker identification. The IDSs of this kind can defend some sophisticated attacks such as masquerade attack [14] effectively while another popular IDS called frequency-based IDS [15]–[17] cannot handle.

Constructing fingerprints for identifying ECUs and detecting attacks based on the differences of signal characteristics has been successfully demonstrated in [18] firstly. Work done by Choi *et al.* [19] measures the voltage level of signal to design the IDS for automotive CAN network. However, it is required to measure an predefined bit string located in the identifier of extended frames which makes the approach practically difficult for real vehicles. As an optimization, the signal shape as well as the voltages are combined to provide more comprehensive characteristics for constructing fingerprint [20], [21]. In [20], an oscilloscope with sampling rate of 2.5 GS/s is adopted to collect data.

Besides voltage, the timing of signal is another physical characteristic which can be exploited for automotive IDS. The fundamental of approaches [14], [22]–[24] is based on the fact that the clock skew exists in the clocks of different ECUs which is unique and stable thus can be exploited as fingerprint to detect attack and pinpoint the source sender in automotive networks. The clock skew represents the difference in frequency among different ECUs. Due to lack of built-in mechanism to synchronize clocks of devices on CAN bus, the behavior of timing of ECU on the bus depends only on local clock, which shall result in difference of time of signal transmitted on the bus. The clock skew can be estimated by calculating the difference between actual arrival time and expected value of periodic CAN frames [14], [22]. However, the actual arrival time of CAN frames can be affected by scheduling, queuing and arbitration delay [22] which might result in wrong computed clock skews. As pointed out in [22], the skews of frames with different period sent by the same ECU computed by the original approach [14] could be different which is incorrect. Besides, the computing process cannot be applied to aperiodic CAN frames.

To address the limitations discussed above, a novel approach to estimate the clock skew is proposed. It measures the duration of CAN frames directly to compute the skew. The estimation process only relies on the measurement of single CAN frame, thus it can avoid the impact introduced by message arbitration, queuing or scheduling. The IDS then extracts statistical features from measurements to construct the fingerprint for ECUs. Two detection methods, single-feature detection and multi-features detection respectively, which are responsible for cases with different settings are proposed to pinpoint the transmitter of frames and detect intrusion in our work. For intrusion detection, dynamic threshold approach [25] is applied for improving the performance. To evaluate our method, four kinds of classification algorithms are employed to compare with each other. From our evaluation, it shows that our approach can detect the attack and identify the sender effectively when the sampling rate of data collector is enough. Since our approach relies heavily on the measurement of clock skew which depends on the sampling rate, the performance of our method might be degraded with low sampling rate. To compensate for this, the limitation and feasible measures for improvement are also discussed in our paper. Our contributions can be summarized as below:

- An novel IDS based on the clock skew of devices is proposed to identify the sender and detect intrusion. The process of clock skew estimation is effective and robust, which can avoid the disturbance from data-link layer such as message queuing or arbitration.
- Two detection methods which can be applied to CAN networks with different settings are proposed in our work.
- Evaluation on a set of experiments with different settings have demonstrated the feasibility of our approach.
- The limitation of our approach that the decreased accuracy might result in the degradation of performance is pointed out and evaluated in our work. Related discussion and feasible measures for improvement are also presented in our work.

The organization of my paper is as follows. Section II introduces the automotive CAN protocol and related work on IDS which exploits the signal characteristics. In Section III, we give an overview of the system model where our approach can be applied and what kind of adversaries we can defend. In Section IV, it describes how our IDS is designed and how it works. In the next Section V, the results of our approach on sender identification and intrusion detection are evaluated and discussed. Finally, our work is concluded in the Section VI.

II. BACKGROUND AND RELATED WORK

In this section, the CAN protocol is briefly introduced firstly. Next, the related work about intrusion detection system based on the signal characteristics for automotive CAN bus is discussed.

A. PRIMER ON CAN

1) AUTOMOTIVE CAN BUS

CAN is critical for in-vehicle communication system, particularly the powertrain system [26]. Nowadays, the CAN communication system is implemented on every production

vehicle as required [21]. There are usually several CAN bus employed in a single vehicle, which can be used for different function such as powertrain, body control and infotainment. The bit rates of different CAN bus can be customized (typical settings such as 500 kbps, 125 kbps or 33 kbps) according to its function and requirement for data transmission. Multiple CAN bus can be interconnected via a central node like gateway. The internal communication system can be accessed by a Standardized interface called OBD-II.

2) CAN FRAME FORMAT

The CAN bus utilizes two signals, which are CAN high and CAN low, to generate the differential signal to transmit data. The logical 1 transmitted on CAN bus is called recessive bit, while the logic 0 is called dominant bit. Data in CAN is transmitted in the unit of frames. The format of the CAN data frame is as follows: SOF (Start of Frame); Arbitration field; Control; Data, in which the payload can only be 1 to 8 bytes; CRC (Cyclic Redundancy Check), ACK (Acknowledgement) and EOF (End of Frame), which is depicted in Figure 1. The identifier is included in the arbitration field of data frame. There are two kinds of data frame according to the length of identifier. The standard frames is equipped with a identifier of 11-bit, while the extended frames are with a identifier of 29-bit.

FIGURE 1. CAN data frame format [23].

3) MESSAGE-ORIENTED PROTOCOL AND BROADCAST NATURE

In the CAN protocol, the frames do not carry any information about which ECU the frame is come from or sent to. Besides, there is no any mechanisms provided in CAN to verify the authenticity of CAN frames. As CAN is broadcast protocol, the frames sent from one node can be received by all nodes on the bus. The receiver decides whether to further process the received frame or not by checking the identifier only.

4) IDENTIFIER ASSIGNMENTS

The identifier of CAN frame indicates the priority of CAN frame, which is responsible for arbitration process. The lower the value of identifier is, the higher priority the frame is. To eliminate potential error and ambiguity, the identifier is required to be unique which can only be allocated to one and only one ECU on a single CAN bus [26]. Each ECU can be assigned with a set of identifiers and the ECU is regarded as the legitimate sender of these identifiers. In normal case, the ECU can only transmit the data with identifiers which have been assigned to it. The assignment would be finished during design phase.

5) ARBITRATION AND ACKNOWLEDGEMENT

When multiple ECUs try to publish the data to the bus simultaneously, an collision occurs and the arbitration process called bit-wise arbitration starts. During the arbitration field, the frame with the minimum value of identifier (i.e. the frame with the highest priority) shall eventually win the arbitration and is able to keep transmitting the rest of the data until the ACK slot. During the ACK slot, all ECUs but the sender which have correctly received the frame shall transmit a dominant level simultaneously on the bus to notify the sender no error detected.

B. RELATED WORK

It is critical to provide security mechanism to protect automotive network from malicious adversaries. By exploiting the inherent variations of physical characteristics in devices introduced by imperfect production process to provide the ability of authentication has been proved effective for such as PUF (Physical Unclonable Function) [27]–[30] as well as source identification and intrusion detection for automotive networks [31].

To our best knowledge, the study [18] is the first work which exploits the physical characteristics of signal to identify the sender for automotive CAN bus. It has proved that the differences of the signal characteristics can be distinguished among devices and stable for several months which is suitable for fingerprinting electronic devices. Based on the observations, a set of researches which utilize the characteristics of the physical signal in frame bits to construct the intrusion detection system for automotive CAN bus are proposed. Cho and Shin [32] uses the minor intrinsic differences of voltage level of the dominate bits between ECUs for identification of the attacker. Choi *et al.* [19] measures the voltage level of an predefined bit string located in the second part of the identifier of extended frames to source the sender and detect intrusion. To improve performance of IDS, it introduces the machine learning algorithms to determine which ECU the received CAN frames belong to. The sampling rate used is up to 2.5 GSPS, and identification rate can reach to 96.48 %. The approach requires that the predefined bit string shall be identical and embedded to all monitored CAN frames which means that the modification on software of all existing ECUs is needed. Besides, the CAN frames which the identifier B field is already in use cannot apply this approach. These shortcomings greatly limit its application on real vehicles. In order to avoid the burden of modifying the CAN bus protocol and existing ECUs, studies [20], [21] have optimized the approach. The shape, as well as the voltage levels of the signal of dominant bits are taken into consideration together for detection of attacks. In Scission [21], the signal of CAN dominate bits are divided into three parts, which are the rising edge, the falling edge, and the holding edge between the rising and falling edge, to extract more distinct and unique features for improving classification performance. Thus, the signal of any bit sting instead of a predefined and fixed bit string

can be extracted sufficient features for constructing the fingerprint of ECUs. It should be noted that the measurements on arbitration field are discarded since the signal during arbitration field might be the expression of combination with outputs of multiple ECUs. For further improvement, another voltage-based IDS SIMPLE [33] is proposed to mitigate the impact of environmental conditions such as supply voltage and temperature on fingerprint generation by compensating the drifts of extracted features.

In addition to voltage-based IDS, the timing of signal is another characteristics which can be exploited to construct fingerprint for ECUs. The work done by Yang *et al.* [34] employs more comprehensive physical characteristics of signal including both voltage and time. It provides a system ensembled with two kinds of classifier and a total of six classification algorithms to construct stable detector for attacks. However, it makes the system too complicated and increases the computational overhead. The CIDS which exploits the clock skew of electronic devices to fingerprint ECU is proposed in reference [14]. The clock skew is estimated by measuring the difference between expected and actual arrival time of consecutive periodic CAN frames. Ji *et al.* [35] evaluate the performance of clock skew-based detection method compared with information entropy detection algorithm. However, the estimation process of clock skew as discussed above can be easily compromised by modifying the transmission of frames as demonstrated in [24]. Besides, Kulandaivel *et al.* [22] point out that the calculation process of clock skew proposed in [14] can be affected by the period of CAN frames. It might result in incorrect estimated clock skews and therefore cannot identify the sender correctly either. To mitigate the limitation that the estimation process is period-dependent, another time-based IDS called BTMonitor [23] is proposed. The BTMonitor measures the bit time of dominant bits and recessive bits separately and extracts the statistical features to generate the fingerprint of ECUs. The measurements are taken for every single CAN frame. Thus, the BTMonitor can be applied to both periodic and aperiodic CAN frames, while the modification on arrival time of transmitted frame does not affect its performance. Same as voltage-based IDS [20], [21], the measurements on arbitration field are excluded. Similarly, our approach estimate the clock skew based on the measurements from single CAN frame which can overcome the shortcomings of CIDS [14]. Compared with BTMonitor, the process of data collection in our approach is improved which can generate less data and facilitate the deployment on automotive network.

III. SECURITY AND THREAT MODELS

This section provides a description of security and threat models considered by our system. The system model is introduced firstly followed by adversary model to explain which scenarios our system can be applied.

A. SYSTEM MODEL

The deployment of our system on existing automotive network is non-destructive. The fingerprint used by our IDS is constructed from the physical characteristics of signal directly. The connection to CAN bus wires is required for our system. Beyond that, any modification on CAN protocol or existing ECUs' software and hardware is unnecessary for deploying our system on the network, which can significantly reduce the effort for deployment and is critical for application on real vehicles. Thus, our IDS can be added to the monitored CAN network as an additional device, as well as a part integrated into other node such as gateway.

The structure of today's automotive network varies between different manufactures and models. For some car models, the automotive network is more complex which consists of several sub-networks. Each sub-network is usually responsible for different functions, such as powertrain, body control or multimedia, and is possibly connected with others via gateway. Since the fingerprint of ECUs is extracted by analyzing the electrical signal directly, the frames sent from ECUs on another sub-network are indistinguishable and regarded as transmitted by gateway node from the perspective of our system in one sub-network. In this case, our IDS can either be included into the central gateway which can monitor multiple sub-networks simultaneously, or be added to each sub-network that needs to be monitored as an additional node. It is assumed that our system is enhanced by security mechanism from being compromised by adversaries.

B. ADVERSARY MODEL

Any kinds of attack launched by malicious CAN frames that are NOT from their legitimate sender can be defended against by our system. That is, from the perspective of our IDS, if the actual sender of the transmitted CAN frames on the bus is inconsistent with its legitimate sender, an intrusion is reported. The actual sender can be predicted by our system, and the legitimate sender can be derived by its identifier. These kinds of attack are collectively referred as impersonation attack. The adversary model can be seen in Fig. 2. The

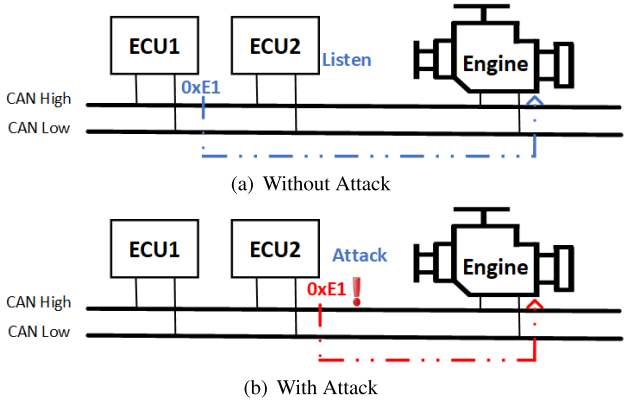

FIGURE 2. Adversary model.

adversary is assumed to be smart that can learn the patterns of network traffic such as timing or voltage to impersonate the victim ECU more accurately. Some state-of-the-art attacks on automotive network such as masquerade attack [14] and cloaking attack [24], [36] can be classified as impersonation attack.

The adversary tries to disguise its identity and impersonate the targeted ECU to manipulate the behavior of vehicle. The impersonation attack can be launched easily after compromising an ECU, while the damage on the automotive network can be fatal. The reasons are explained as follows. The identifiers of CAN frames are pre-assigned to corresponding ECUs during the design phase. It is required that one identifier can only be assigned to one and only one ECU (i.e. the legitimate sender) [26] to eliminate potential conflict and ambiguity during communication process. Hence, our system have the knowledge of which ECU is allowed to transmit which identifiers. Since there is no any mechanisms specified in CAN to verify the authenticity of CAN frames, the bus participant cannot determine whether the received frames are from their legitimate sender. Thus, the adversary can imitate any available identifiers of CAN frames and launch the impersonation attack to cause automotive network malfunction after intrusion. It has been demonstrated that the infiltration of any ECU on the monitored CAN network is enough for the attacker to control the safety-critical functions [4].

Another common type of attack on vehicles is frequency-related attack such as fabrication attack and suspension attack [14]. The adversary aims to cause malfunction on vehicles by injecting extra malicious frames or stopping the transmission of existing frames, by which the frequency of transmitted frames shall be influenced. The frequency-related attack can be detected effectively by existing approaches [14]–[17] considering the frequency of frames under attack shall deviate from their expected behaviors significantly. The DoS Attack on automotive network as discussed in [37], which dominate the CAN bus and paralyze normal communication by injecting a large number of frames with higher priority (smaller identifier), can also be detected easily by monitoring the network traffic. Thus, these kinds of attack are out of the scope of our system.

IV. OUR METHOD

This section describes how our method works.

A. OVERVIEW OF OUR METHOD

In automotive networks, all ECUs are equipped with clocks which consist of a electronic oscillators that runs at a nominal frequency. Due to the imperfection of manufacturing process, subtle deviations from the actual frequency to nominal frequency exists in electronic oscillators, called clock skew. It has been demonstrated that the clock skew can be utilized as fingerprint for identifying automotive ECUs in previous work [14], [22]–[24]. Due to the absence of global clock in CAN protocol, the CAN frame timing is determined only by the the local clock. Thus, the timing of CAN frames will inherit the clock skew of the transmitter node. Our basic idea is to estimate the clock skew from the CAN frame timing and design our IDS for attack detection and sender identification based on the estimated skews.

A clock-skew-based source identification and intrusion detection method is proposed. More specifically, the clock skew of sender ECU is computed by comparing the single CAN frame's actual length with its nominal length. The nominal length is the product of the nominal bit time and the number of bits. And the actual length is measured from the electrical signal of single CAN frame. Compared with previous clock-skew-based work [14], [22], our approach for clock skew estimation is more straightforward, effective and robust by which the disturbance introduced by message scheduling, queuing and arbitration process can be avoided.

A solution consisting of two detection methods is provided to deal with different situations. They are *single-feature detection* and *multi-features detection* respectively. Only one detection method is required during running process. Our system selects an appropriate detection method according to its performance on training datasets and other metrics (such as computing overhead and response time). During the selection process, the single-feature detection is first evaluated. If the detector cannot discriminating different ECUs well due to insufficient sampling rate of ADC or noise like CAN bit jitter [38], the multi-features detection is picked as the detection method for the monitored network. Since our method is based on the physical characteristics of clocks in devices, the selection process can be done as long as the setup of the network to be monitored is ready. The overall process of our method can be seen in Algorithm 1.

Algorithm 1 Overall Process of Our Method

```
for i = msg_1, msg_2, msg_3 ... do        ▷ Data Collection
    Clock Skew Estimation
end for

Call Single-feature Detection             ▷ Selection Process
if Detection Accuracy >= Threshold then
    Select Single-feature Detection
else
    Select Multi-features Detection
end if
```

B. CLOCK SKEW ESTIMATION

This section describes the details of estimation process of clock skew based on single CAN frame. Related concepts is introduced firstly.

Clock Related Concepts Two clocks $\mathbb{C}_1$ and $\mathbb{C}_2$ are discussed as an example.

- ***Clock Offset:*** The difference in time between clocks, i.e., $\mathbb{C}_1(t) - \mathbb{C}_2(t)$ is the clock offset of clock $\mathbb{C}_1$ to $\mathbb{C}_2$ at time t.
- ***Clock Frequency:*** It indicates the speed at which the clock runs, which is denoted by $\mathbb{C}'_1(t)$ for $\mathbb{C}_1$ at time t.

- ***Clock Skew:*** Similar to clock offset, it is the difference in frequency between clocks, i.e., $\mathbb{C}'_1(t) - \mathbb{C}'_2(t)$ is the skew of clock $\mathbb{C}_1$ relative to $\mathbb{C}_2$ at time t.

Bit Timing Related Concepts

- ***Nominal Bit Rate (NBR):*** The bit rate is to indicate the speed of CAN. The NBR is the number of bits sent by an ideal node in one true second. The bit rate is required to be uniform and fixed a one given CAN bus.
- ***Nominal Bit Time (NBT):*** The ideal duration for one bit, defined as the reciprocal of NBR. That is, $NBT = 1/NBR$.

Primer on CAN Transceiver To participate in a CAN network, an ECU is required to be equipped with a CAN protocol controller and a CAN transceiver, as shown in Fig. 3. The CAN controller implements the functions prescribed by the CAN specification. It can work as a standalone device or be integrated into the micro-controller. The CAN transceiver (transceiver stands for transmit and receive) works as an interface between the CAN protocol controller and the bus line and converts the logical level of the CAN controller to electrical representation of the bus [26].

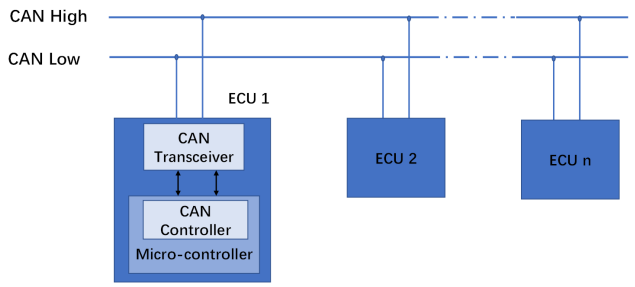

FIGURE 3. Architecture of CAN bus.

1) HIGH-LEVEL IDEA

Due to the effect of hardware characteristics in ECUs such as skew in clock, CAN bit jitter [38] or noise in CAN transceiver, the actual bit time shall deviate from the nominal bit time. Since there is no global clock in CAN network, the actual bit time will inherit the physical characteristics of transmitter node.

The difference between the measured time and true time shall be increased linearly over time since the clock skew is constant. Thereby, the slope of the increase of time difference is the skew of clock. Due to lack of the built-in mechanism for synchronizing the clock, the time duration of CAN frames sent from different ECUs might be different [23]. Based on this, our IDS measures the length of electrical signal of CAN frames and compare the measured length with nominal length (defined as the product of NBT and the number of bits) of CAN frames to estimate the clock skew of the sender ECU. The derived clock skew is then utilized to fingerprint the ECU. It should be noted that our measurement is based on the differential signal (the difference between CAN high and CAN low) which can resist electromagnetic interference and provide a more stable and accurate electrical signal.

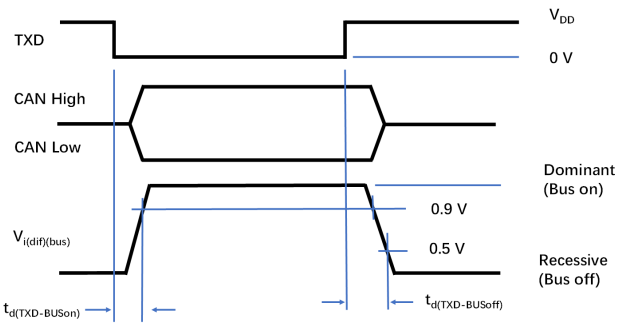

FIGURE 4. Timing diagram of TXD of CAN transceiver.

2) PROCESS OF CLOCK SKEW ESTIMATION

The process of clock skew estimation is as follows. Our IDS first measures the length for one received CAN frame. There are two adjustments in our measurement instead of measuring the whole CAN frame: (i) Our measurement starts from one rising edge and ends at another rising edge instead of from rising edge to falling edge. (ii) The ACK field is excluded from our measurement. That is, our measurement begins from the rising edge of Start-of-frame (SOF) field and ends at the last but one rising edge of one complete frame, as shown in Fig.5.

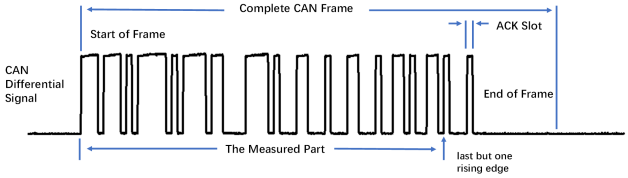

FIGURE 5. An example of the measured length of received frame.

The first adjustment is to ensure more stable and accurate measurement on electrical signal. More specifically, the timing diagram of transmit data (TXD) for CAN transceiver can be seen in Fig.4. It can be seen that the output of electrical signal by CAN transceiver shall reflect the timing characteristics of high-level hardware. The $t_{d(TXD-BUSon)}$ and $t_{d(TXD-BUSoff)}$ refer to delay TXD to bus active and inactive respectively. These two values are not necessarily equal and the difference between them varies on different transceivers. Thus, the measurement of time elapsed in our method is between two rising edges of CAN electrical signal to minimum the effect of these delays. The start and end point of rising edge in our measurement are set as 0.9 V.

The second adjustment is necessary due to the acknowledgement mechanism prescribed by CAN protocol. As discussed in Section II-A, during the ACK slot, the bus is driven by all nodes except the transmitter which have correctly received the frame. Hence, the measurements should exclude

the ACK filed since it does not represent the signal characteristics of the transmitter.

Meanwhile, the number of bits during the duration is counted based on the nominal bit rate of CAN bus. Thus, the nominal length of the received frame is computed as the product of nominal bit time and number of bits. Then, our IDS calculates the difference by subtracting the actual length of the received CAN frame from the nominal length. The estimated clock skew by our method is the ratio of the difference to the measured length (actual length) of the received CAN frame. The estimation of clock skew can be expressed as:

$$Skew = \frac{NBT * n - S}{S}$$

In the equation, NBT, S and n refer to *Nominal Bit Time*, the measured length and the corresponding number of bits respectively.

C. FEATURE EXTRACTION

Firstly, the clock skew for every single received CAN frame is computed. Then, every N calculated results (i.e. clock skews) with same identifier are grouped together as one data sample for further detection. There are two detection methods proposed in our work. They are single-feature detection and multi-features detection which can be applied on different situations. The main difference between these two detection methods is the feature extraction, while the general process of them is similar. The details of feature extraction of these two detection methods are as follows.

1) SINGLE-FEATURE DETECTION

Here only ONE feature, expected value of data sample, is used to construct our intrusion detection system for the automotive network. When the sampling accuracy of ADC is high enough, the clock skew can be estimated accurately and precisely within length of single CAN frame. In this case, our IDS can distinguish which ECU the received CAN frame comes from by only the estimated clock skew. The expected value is taken to reduce the influence of measurement deviation or noise (such as CAN bit jitter [38]).

2) MULTI-FEATURES DETECTION

The performance of our method can be affected by the sampling rate of ADC and relative clock skew between ECUs. The single-feature detection can work well when the sampling rate of ADC is enough to tell the minimum difference of average clock skew between ECUs. The Multi-features detection is called if the detection accuracy of single-feature detection is less than the preset threshold. More features are extracted from calculated clock skews of data sample as fingerprint to represent the sender ECU in multi-features detection. Multiple features can provide more details of sender ECU than single feature. That is, multiple features usually can characterize sender ECUs better. To construct fingerprint for electronic devices based on the statistical features has been proved effective in previous work [19]–[21], [23], [25]. Besides, comparing to previous work [19]–[21] which exploits features on both time and frequency domain, our approach only adopts the features in the time domain and avoids the complexity of frequency domain transformations. For every newly received data sample, the required features are extracted firstly. The selected features which used to construct ECU fingerprint and generate the classification model are shown in table 1.

TABLE 1. Selected features in time domain for constructing the fingerprint. *x* represents the estimated clock skew. *N* indicates the number of the data.

Feature	Description
Mean	$\overline{x} = \frac{1}{N}\sum_{i=1}^{N} x(i)$
Standard Deviation	$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x(i)-\overline{x})^2}$
Variance	$\sigma^2 = \frac{1}{N}\sum_{i=1}^{N}(x(i)-\overline{x})^2$
Skewness	$\gamma = \frac{1}{N}\sum_{i=1}^{N}(\frac{x(i)-\overline{x}}{\sigma})^3$
Kurtosis	$\beta = \frac{1}{N}\sum_{i=1}^{N}(\frac{x(i)-\overline{x}}{\sigma})^4 - 3$
RMS (Root Mean Square)	$A = \sqrt{\frac{1}{N}\sum_{i=1}^{N} x(i)^2}$
Maximum Value	$H = \max(x(i))$
Energy	$en = \frac{1}{N}\sum_{i=1}^{N} x(i)^2$

D. SENDER IDENTIFICATION

The problem of sender identification, as well as intrusion detection, can be regarded as a classification problem, where frames sent from one node on the CAN network can be seen as from one class. Any CAN frames sent by the same ECU shall be considered as from the same class since they inherit the clock skew and variations of the same sender. It is a multinomial classification problem since the number of nodes in an automotive network is usually more than two. In our work, any received frame that its actual sender is inconsistent with its legitimate sender (derived from its identifier) is considered as malicious message, marked as intrusion.

Our IDS uses the supervised learning algorithm to generate the classification model and classify the newly received data to distinguish which ECU the received CAN frame belongs to. There are two phases in this step. In the training phase, the training data with label which indicates the sender ECU is fed into the classifier to generate the classification model firstly. Then the classifier predicts which ECU it comes from for every newly received data sample during the testing phase. The predicted ECU is considered as the actual sender of the received data sample by our system. Specifically, in the testing phase, the classifier first predicts an array of probabilities that indicates how likely the received data sample belongs to for every single class. Then the ECU with the highest probability is selected as the sender for the received data sample. It is important to make sure that the training process is done under a trustworthy environment, such as during production or in authorized workshop. Otherwise, the generated classification model would be corrupted by malicious training data.

E. INTRUSION DETECTION

If the actual sender (i.e. the predicted label) of CAN frame is inconsistent with its claimed sender (derived by identifier), an alarm is triggered and the data sample is marked as intrusion. Instead of selecting the ECU with the highest probability as the actual sender as usual, an intrusion detection approach with dynamic thresholds [25] is introduced in our work to detect intrusion. The process is as follows. Considering the number of malicious CAN frames is significantly lower than the total number of CAN frames in automotive network, our system employ a lower threshold $Thres_{min}$ by which it can reduce the computational overhead and increase the robustness against the electromagnetic interference. Our system computes the probability that the received data sample belongs to the corresponding ECU of the obtained identifier firstly. If the probability is no less than the threshold $Thres_{min}$, the legitimate ECU of the identifier is considered as its actual sender (i.e. the received data sample is considered as normal). Only if the probability is lower than the threshold $Thres_{min}$, our system then computes the probabilities of the remaining ECUs. By this way, unnecessary computation can be avoided thus improve efficiency. The highest probability of the remaining ECUs is selected to compare with another threshold $Thres_{max}$. If it is greater than the threshold $Thres_{max}$, the data sample is marked as intrusion and the corresponding ECU of the highest probability is considered as the source of the malicious CAN frames. If the highest probability is less than the upper threshold $Thres_{max}$, the received data sample is marked as suspicious. In our work, the suspicious messages is regarded as normal messages that the legitimate sender of the identifier is taken as the actual sender instead of the predicted sender (i.e. the computed label with the highest probability). It should be noted that, the further investigation and detection method is needed for suspicious CAN frames. The performance of sender identification and intrusion detection is evaluated in Section V. Several popular classification algorithms are adopted in our work. By introducing the dynamic thresholds detection approach, the false positive (FP, i.e. those normal data samples but incorrectly marked as intrusion) which is a very important criteria for deployment on real vehicles can be reduced. Since as the false positive (FP) decreases, the unnecessary reactions or alarms of automotive protection system can be avoided thus improve the overall driving experience.

V. EVALUATION

A CAN bus prototype which consists of six nodes is set up to evaluate our proposed method. Our experimental settings fix the sampling rate of the ADC and vary the bit rate of CAN bus to simulate different situations that our detection methods can be applied. Three typical kinds of CAN bus bit rate which are widely used in production vehicles are selected to simulate situations in which the sampling rate is sufficient or not to estimate the clock skew directly within length of one CAN frame. These three selected kinds of CAN bus bit rate are 500 kbps, 125 kbps and 33 kbps, which are served as high speed, medium speed and low speed CAN bus respectively in automotive network. In our work, the sampling rate of our data collector is set as 500 MSPS. From our evaluation, it can be found that the detection accuracy of our method shall be affected by the sampling accuracy and relative clock skew between ECUs. By a series of experiments, the results have demonstrated that our proposed method can identify ECUs and detect intrusion well in Controller Area Network. The evaluation shows the promising prospect of our method for deployment on real vehicles.

A. EXPERIMENTAL SETTINGS

1) CAN BUS PROTOTYPE

The CAN bus prototype consists of six nodes (ECUs) to simulate the CAN bus communication. It includes two kinds of CAN development boards produced by different manufacturers. One kind of ECUs is composed by an Arduino UNO board and a CAN bus module designed by Seeed Studio. The CAN controller and transceiver of the CAN module are MCP2515 and MCP2551. The other kind of ECU is developed by MCU STM32F103VET6 which provides CAN interfaces itself (function as CAN controller) and TJA1050 as CAN transceiver. The number of both kinds of ECU is three. In order to simulate application scenarios which our different detection methods can apply, the baud rates of CAN bus prototype are set as 500 kbps, 125kbps, and 33 kbps respectively, which are widely adopted in vehicles as high-speed, medium-speed and low-speed CAN bus. The CAN bus prototype is shown in Figure 6.

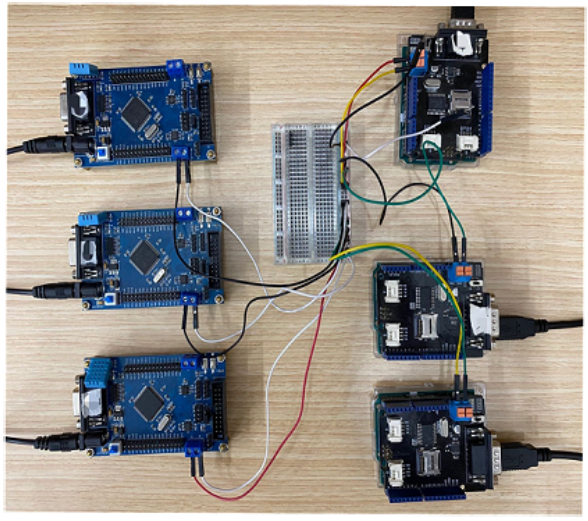

FIGURE 6. CAN Bus prototype.

2) DATA COLLECTOR

In our evaluation, the signals are collected by a PicoScope 5244D at a sampling rate of 500 MS/s and a resolution of 8 bit. The two signals of CAN bus, CAN high and CAN low, are recorded by two oscilloscope probes respectively.

For processing, the two signals are first converted to a differential signal. Then the differential signal is fed into the detector for further processing.

3) CLASSIFICATION ALGORITHM

In our work, we test the performance of four different classification algorithms which are adopted and proved effective in previous work [19], [25]. These classification algorithms we exploited are Support Vector Machine (SVM), Multinomial Logistic Regression (MLR), Naive Bayes (NB) and Bagged Decision Tree (BDT). We performed the default implementations of these classification algorithms provided by MatLab R2017b. For Support Vector Machine, the linear kernel was adopted as kernel function. For Bagged Decision Tree, the number of decision trees was set as 30. To evaluate how well the predictive model trained on particular data set generalizes to an independent data set, the 10-fold cross validation test is performed. In 10-fold cross validation, the initial data set is randomly divided into ten folds equally firstly. Then, nine of the ten folds are utilized as training data set to generate the classification model. The remaining one fold is retained for testing the model as validation data. This process is repeated ten times so that each fold is taken as validation data in turn. Finally, the results are combined to produce a single estimation in our work.

B. SENDER IDENTIFICATION

This section evaluates the ability of our approach for sourcing the sender of CAN frames. For sender identification, the ECU with the highest predicted probabilities is regarded as its actual sender. By comparing the predicted sender with its actual sender based on ground truth, the identification rates for each ECU are computed. The results are shown by confusion matrix. Our work evaluates the ability of the proposed method for sender identification on low-speed CAN bus, medium-speed CAN bus and high-speed CAN bus respectively.

1) LOW-SPEED CAN BUS

The performance of single-feature detection on low-speed CAN bus is evaluated firstly. The speed of CAN bus is 33 kbps. The confusion matrix for the identification rate of different classification algorithms is shown in Table 2. The average, as well as the minimum identification rates of the six ECUs are shown in the table. The results with different size N of data sample are also demonstrated. Our system sets $N = 5$ and $N = 10$ here. It can be seen that, the average identification rates of all four classification algorithms are always higher than 99.8% when $N = 5$. All the minimum identification rates of six ECUs are also higher than 99.7%. When the size of data sample becomes larger, e.g. $N = 10$, the identification rates of Naive Bayes and Bagged Decision Tree even reach 100 percent during our evaluation. It should be noted that the 100% identification rate does not mean that no misclassification can occur. From our evaluation, the performance of single-feature detection on low-speed CAN bus can reach very high even when the size of data sample N is small. Thus, multi-features detection here is unnecessary for low-speed CAN bus.

TABLE 2. Identification rate of single-feature detection on low-speed CAN [Unit:%].

	N=5		N=10	
	Avg	**Min**	**Avg**	**Min**
MLR	99.93	99.78	99.93	99.60
SVM	99.89	99.77	99.71	99.19
NB	99.97	99.80	100	100
BDT	99.93	99.78	100	100

2) MEDIUM-SPEED CAN BUS

The bit rate of medium-speed CAN bus set in our evaluation is 125 kbps. The performance of single-feature detection is evaluated firstly to see if it is effective to identify the sender on medium-speed CAN. The size of data sample is set as 20 and 50, i.e. $N = 20$ and $N = 50$. The results are shown in Table 3.

TABLE 3. Identification rate of single-feature detection on medium-speed CAN [Unit:%].

	N=20		N=50	
	Average	**Min**	**Average**	**Min**
MLR	83.62	49.88	88.15	59.31
SVM	84.21	30.84	84.91	46.36
NB	86.69	47.62	89.12	51.42
BDT	83.03	54.35	85.93	57.61

From the observations, there is a significant decrease of performance on all four classification algorithms. The minimum identification rate of Support Vector Machine (SVM) when $N = 20$ drops to 30.84% which means the single-feature detection on medium-speed CAN bus cannot source the sender correctly. This is because the bit time becomes shorter as the bit rate of CAN bus increase, which makes the length of single CAN frame shorter. The shorter the length of single CAN frame becomes, the less accurate the estimated clock skew is. Thus, our system might not distinguish clock skews from different ECUs by only the expected value of estimated clock skews since the measurement error dominates the differences between ECUs. Here the performance of multi-feature detection is evaluated to see if it can be improved by introducing more features. The results are demonstrated in Table 4.

Compared with single-feature detection, the performance of multi-features detection has increased significantly. When $N = 20$, the average identification rate of Multinomial Logistic Regression increased from 83.62% to 96.64%, while the minimum identification rate increased from less than 50% to over 92%. When $N = 50$, the accuracy on both average and

TABLE 4. Identification rate of multi-features detection on medium-speed CAN [Unit:%].

	N=20		N=50	
	Avg	**Min**	**Avg**	**Min**
MLR	96.64	92.73	99.63	99.11
SVM	97.11	93.86	99.83	99.70
NB	96.48	93.02	99.70	99.26
BDT	96.78	93.20	99.88	99.55

minimum can get a high precision, which both exceed 99%. The results of other algorithms similar to this. It means that more features can provide more details of hardware which favors the problem of sender identification.

3) HIGH-SPEED CAN BUS

The performance of our method on high-speed CAN is evaluated in this section. Only the results of multi-features detection are shown in Table 5. The size of data sample N is set as several different values here to see if the performance can be affected by the size of data sample. That is, $N = \{50, 100, 150, 200, 250, 300\}$. As shown in the results, as the size of data sample N increases, the performance increases steadily. When N is larger than 200, the rate of increase on performance slows down. However, a larger N shall result in a longer response time of intrusion detection. Thus, the size of data sample is not the larger the better. It is suggested that the size of data sample N on high-speed CAN is set as 200 during our evaluation to balance the performance and response time for our system. Besides, it can be seen that the difference in the identification rates among the selected machine learning algorithms is not significant. As shown from the results, there is a performance degradation on high-speed CAN comparing with results on low-speed and medium-speed CAN. However, our approach can still be effective for identifying ECUs in real vehicles. The reasons are discussed in the following section.

4) DISCUSSION ON RESULTS OF HIGH-SPEED CAN

From the results shown in Section V-B3, the average and minimum identification rate for SVM is 90.06% and 69% respectively when $N = 200$. To further analyze the results of high-speed CAN, the confusion matrix of multi-features detection using SVM when $N = 200$ is shown in Table 7. The confusion matrix describes how many CAN frames from a certain ECU are correctly or incorrectly classified. For example, the number on the first row and first column indicates the ratio of CAN frames from ECU0 that are identified correctly, while the number on the first row and third column indicates the ratio of CAN frames from ECU0 that are misclassified to ECU2.

It can be seen that, the drop in overall performance is mainly explained by the ECU0 and ECU2. The CAN frames from other ECUs excluding ECU0 and ECU2 can still be well identified with very high probability. From the perspective of our intrusion detection system, the difference between clock skews of ECU0 and ECU2 is indistinguishable which can be called as birthday paradox [14]. In our work, the birthday paradox is mainly caused by that the clock skew and associated statistical features of different ECUs extracted by our method overlap each other thus the classifier cannot discriminate them. In our evaluation, the ECU0, ECU2 and ECU4 are identical development boards composed of Arduino UNO and CAN bus shield (use Arduino for short below), while the rest of ECUs are the same devices developed by MCU STM32F103VET6 (use STM32 for short below). Due to ECU0 and ECU2 are identical in construction, and their clock skews are near-equivalent to each other, our method cannot distinguish ECU0 from ECU2 well based on currently adopted sampling rate. It leads to the performance degradation. Next, the ways to improve the performance and deployment on real vehicles are discussed.

1) The performance of our evaluation can be improved by upgrading the hardware. In our method, the clock skew is estimated by measuring the length of single CAN frame. As the bit rate of CAN bus increases, the length of single CAN frame becomes shorter. The accumulated clock offset during single CAN frame becomes shorter. Thus, higher sampling rate of ADC is required to tell the minor differences between different ECUs for faster CAN bus. From our evaluation, there is a significant drop in performance of single-feature detection when the bit rate is increased from low-speed (33 kbps) to medium-speed (125 kbps), as well as the performance of multi-features detection from medium-speed (125 kbps) CAN to high-speed (500 kbps). Hence, the performance of high-speed CAN bus shall be further improved when using higher sampling rate, while the performance during our evaluation is limited since the maximum sampling rate of our data collector for two-channel (i.e. CAN high and CAN low) is 500 MSPS.

2) From our observations, the chance for birthday paradox on vehicular CAN bus from the perspective of our intrusion detection system is not strong. The clock skews of our six ECUs by measurements on low-speed CAN bus is shown in Table 6. On low-speed CAN, the measurements by ADC are more accurate and precise, thus the estimated clock skew is closer to the true clock skew. The first row shows the estimated clock skew in unit of ppm (part per million), while the second row shows the difference from the skews of former ECU. The third and fourth row describe the number and base board used by the ECU. It should be noted that the data is listed in ascending order of clock skew instead of from ECU0 to ECU6, by which the minimum difference between clock skews can be easily targeted. It can be seen that the difference of clock skews between ECU0 and ECU2 is around 5.41%. The results are based on the measurements on low-speed CAN. As the bit rate increases, the length of single CAN frame reduce. On high-speed CAN, our data collector cannot get the clock skew precisely. Hence, the estimated clock skews of ECU0 and ECU2 may overlap each other, which leads to a significant drop in identification rate as

TABLE 5. Identification rate of multi-features detection on high-speed CAN [Unit:%].

	N=50		N=100		N=150		N=200		N=250		N=300	
	Avg	**Min**	**Avg**	**Min**	**Avg**	**Min**	**Avg**	**Min**	**Avg**	**Min**	**Avg**	**Min**
MLR	80.74	43.38	84.78	54.91	87.56	63.64	90.07	70.62	90.94	74.07	91.33	72.47
SVM	81.05	43.71	85.22	54.78	87.72	62.22	90.06	68.19	91.06	72.73	91.28	73.28
NB	79.34	37.66	84.33	51.68	87.18	60.40	88.14	64.15	88.54	64.98	90.45	68.02
BDT	79.43	44.32	84.06	54.78	85.50	57.78	89.74	69.27	89.54	69.70	90.93	73.28

TABLE 6. Estimated clock Skews of ECUs on Our CAN bus prototype.

Clock Skew (ppm)	44.1	51.8	54.6	59.9	62.6	68.1
Clock Skew Difference (%)	0	17.46	**5.41**	9.71	**4.51**	8.79
Node Number	ECU3	ECU2	ECU0	ECU4	ECU1	ECU5
Node Construction	STM32	Arduino	Arduino	Arduino	STM32	STM32

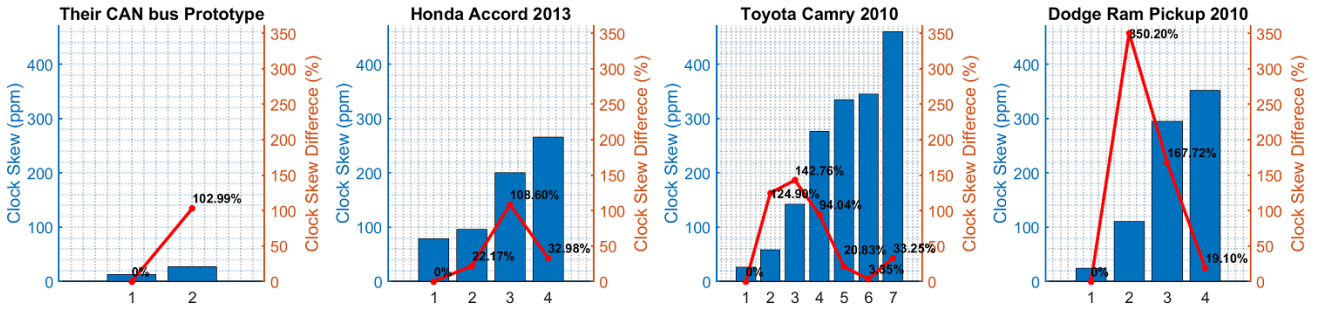

FIGURE 7. The clock skews of one CAN prototype and several car model presented in [14] and difference between skews. In the figure, the bars are clock skews of ECUs presented in ascending order. The value on the polyline represents the difference of skew of current ECU from the skew of the former one.

TABLE 7. Confusion matrix for multi-features detection using SVM when $N = 200$ [Unit:%].

	ECU0	**ECU1**	**ECU2**	**ECU3**	**ECU4**	**ECU5**
ECU0	68.20	0	27.22	0	4.58	0
ECU1	0	100	0	0	0	0
ECU2	24.40	0	75.34	0	0.26	0
ECU3	0	0	0	100	0	0
ECU4	2.94	0	0	0	97.06	0
ECU5	0	0.22	0	0	0	99.78

shown in Table 7. Besides, it can be noticed that the difference of skews between ECU1 and ECU4 is only 4.51% which is the minimum difference on our prototype. However, our IDS can discriminate the ECU4 and ECU1 very well. This is because despite the average estimated clock skew may overlap between ECU1 and ECU4, other extracted statistical features (such as variations of clock skew) may have big difference considering the ECU1 and ECU2 are different in construction and therefore can favor the classification.

Similarly, the nodes on automotive networks are usually produced by different manufacturers and OEMs for real vehicles. The nodes are different in construction, as well as the differences in clocks between ECUs may be more obvious which can be demonstrated by results in [14]. The authors of [14] reveal the clock skews of their CAN bus prototype and several common car models as shown in Fig 7. In the subfigure, the bar graph shows the clock skews in ascending order, while the broken-line graph shows the difference of clock skews between one ECU and its former one. From the results, except for the clock skew of the 6th ECU (The value is 345.3 ppm) in Toyota Camry 2010 which is different from clock skew of the 5th ECU (The value is 334.1 ppm) of only by 3.35%, others are far greater than the minimum difference which our system can identify effectively. Therefore, our method can be a promising and effective way for identifying ECUs on real vehicular CAN bus.

3) The ECUs, which cannot be distinguished by our system, can be regarded as one superclass. Despite the birthday paradox is considered as a rare case as discussed above. However, when it happens, one solution for improving the performance is to increase the sampling rate to get more accurate and precise measurements for calculating clock skews. If it is not feasible by upgrading the hardware, an alternative is to consider these two ECUs with near-equivalent clock skews as one node (superclass). The CAN frames sent from these two ECUs are regarded as one class for model training and predication. When there is any misbehavior found in

CAN frames from the superclass, our system can trigger an alarm and simply treat the two ECUs as one node for further processing. Further investigation and advanced detection can be introduced if necessary.

C. INTRUSION DETECTION

In this section, the performance of the dynamic threshold detection approach for intrusion detection is evaluated. Besides false positive rate (FPR) which indicates the ratio of normal samples but incorrectly marked as malicious, the false negative rate (FNR) is another important criteria for intrusion detection system. The false negative rate is an error rate that indicates the ratio of malicious CAN frames but incorrectly marked as normal. For convenience, our system also adopts the metrics ***sensitivity*** and ***specificity*** to evaluate the performance of intrusion detection of our system. The ***sensitivity*** and ***specificity*** are defined as:

$$Sensitivity = 1 - FNR$$
$$Specificity = 1 - FPR$$

To evaluate false negative rate of our system, only a fraction of collected data samples is handled as malicious CAN frames since the number of malicious CAN frames is significantly lower than the one of normal frames for attacks in automotive network. In our evaluation, 10% of the data samples from the test sets are selected randomly to simulate the attack. The identifiers of those data samples that are selected are modified to those identifiers which are authorized to use by another ECU (i.e. the victim). To better evaluate the effect of attack, the 10% of the CAN frames sent by all six ECU in test sets are handled as attack. The victim ECUs of the attacks are changed to other five ECUs continuously for each attacker. This ensures that each ECU can be the target of attack by every other ECU. In our evaluation, our IDS sets the upper threshold $Thres_{max} = 0.5$ and the lower threshold $Thres_{min}$ as 0.2 for all settings. The results of our evaluation are as follows.

1) LOW-SPEED CAN BUS

The resulting confusion matrices of intrusion detection on low-speed CAN bus is shown in Table 8. It can be seen that, both the false negative rate (FNR) and false positive rate (FPR) can reach very low. That is, our system is able to detect intrusion very accurately and avoid false alarms with a very high probability. For SVM, our approach can achieve an identification rate of on average 99.89% when $N = 5$ and 99.71% when $N = 10$ as shown in Table 2 with a false positive rate of 0.11% and 0.29% respectively, which means that every 1000 and 400 frames a false alarm occurs for $N = 5$ and $N = 10$ respectively. By introducing dynamic threshold approach, the false positive rate (FPR) of SVM is significantly reduced to 0.04% and 0% respectively.

TABLE 8. Confusion matrices of intrusion detection on low-speed CAN for single-feature detection.

N=5				
	Attack	Predicted		Suspicious Frames
		0	1	
MLR	0	99.93	0.07	0
	1	0.96	99.04	0.14
SVM	0	99.96	0.04	0.04
	1	0	100	0
NB	0	99.96	0.04	0
	1	0	100	0
BDT	0	99.92	0.08	0
	1	0	100	0
N=10				
	Attack	Predicted		Suspicious Frames
		0	1	
MLR	0	99.94	0.06	0
	1	0.14	99.86	0
SVM	0	100	0	0.20
	1	0.42	99.58	0.28
NB	0	100	0	0
	1	0	100	0
BDT	0	100	0	0
	1	0	100	0

2) MEDIUM-SPEED CAN BUS

This section evaluates the performance of dynamic threshold approach on medium-speed CAN. The new detection approach is only applied to the data extracted by multi-features detection method since it is proved that the single-feature detection does not work well for medium-speed CAN as demonstrated in Section V-B2. The false positive rates (FPR) of our system on medium-speed CAN without introducing the threshold approach can be calculated by subtracting the identification rate, which can be seen in Table 4, from the total probability 1. Comparing with them, the performance of all four classification algorithms has been improved by applying the threshold detection approach, which can be seen in Table 9. When $N = 20$, the false positive rates (FPR) on average have been decreased by at least 0.64% (which is NB) for all four classification algorithms. For MLR, the false positive rate has been reduced significantly by 2.21%. Except for NB, the false negative rates (FNR) of the other classification algorithms are slightly higher than the false positive rates (FPR). The specificity of NB can reach to 99.15% when $N = 20$. When $N = 50$, although a very high identification rate has been reached in Section V-B2, the overall performance can still be improved by introducing the dynamic threshold detection approach.

3) HIGH-SPEED CAN BUS

For high-speed CAN, the performance of sender identification is not satisfying. It can be explained by that the very

TABLE 9. Confusion matrices of intrusion detection on medium-speed CAN for multi-features detection.

		N=20		
	Attack	Predicted		Suspicious Frames
		0	1	
MLR	0	98.85	1.15	0.02
	1	2.33	97.67	0.30
SVM	0	98.80	1.20	0
	1	1.39	98.61	0.04
NB	0	97.12	2.88	0
	1	0.85	99.15	0
BDT	0	98.76	1.24	0
	1	1.59	98.41	0.16
		N=50		
	Attack	Predicted		Suspicious Frames
		0	1	
MLR	0	99.85	0.15	0
	1	0.45	99.55	0
SVM	0	99.90	0.10	0
	1	0.15	99.85	0.05
NB	0	99.79	0.21	0
	1	0.10	99.90	0
BDT	0	99.95	0.05	0
	1	0.10	99.90	0

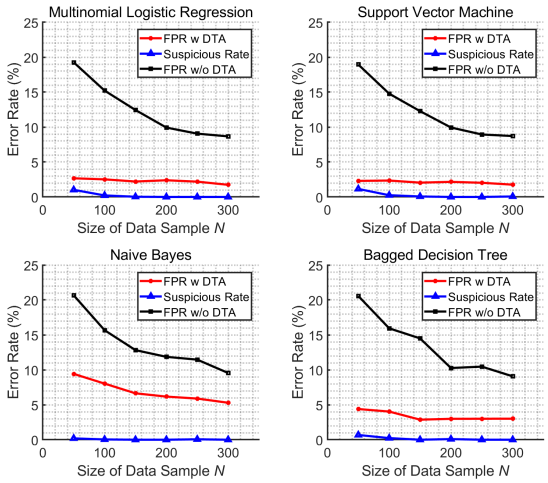

FIGURE 8. The false positive rate (FPR) w and w/o dynamic threshold approach (abbreviated as DTA in figure) and suspicious rate for high-speed CAN.

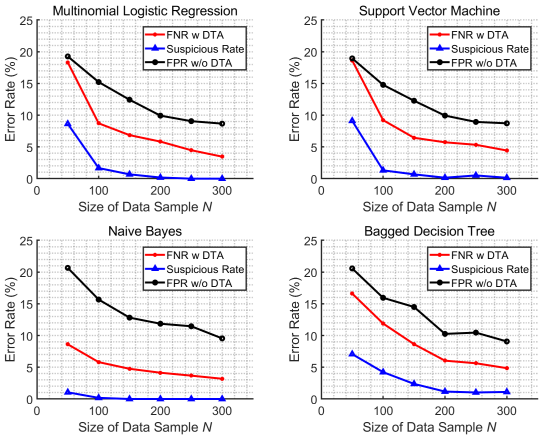

FIGURE 9. The false negative rate (FNR) with dynamic threshold approach (abbreviated as DTA) and suspicious rate comparing with false positive rate (FPR) w/o DTA for high-speed CAN.

tiny difference of skews between ECUs in same construction cannot be distinguished by our current system. The discussion can be referred in Section V-B4. When the size of data sample N is set as 200, the average false positive rate (FPR) of four classification algorithms without applying the threshold detection method is around 10.50%. It means that there would be plenty of false alarms during driving and make a really bad driving experience without further measures. When $N = 50$, the average false positive rate can be up to 19.86%, which is far from acceptable. This section evaluates how much the performance of our system can be improved by introducing the dynamic threshold detection method for high-speed CAN.

The FPR and corresponding suspicious rates when applying dynamic threshold approach comparing with FPR without the threshold approach are shown in Fig 8. As can be seen, there is a significant improvement of FPR for all classification algorithms by introducing the dynamic threshold approach. When $N = 200$, the false positive rate of SVM drops by around 7.78% to 2.16%. When N is set as 50, the false positive rate for SVM can be reduced around 16.59%. Except for NB, the variation of FPR when applying the threshold approach is slight when N varies. That is, these three classification algorithms can reach a stable and low false positive rate even when N is small. For NB, the false positive rate decreases when N increases, and the curve is flatten from $N = 200$. Besides, the suspicious rates of all algorithms stay at a low level and stable.

Similarly, the FNR and corresponding suspicious rates of four classification algorithms are shown in Fig 9. The false positive rate (FPR) without the dynamic threshold approach is also adopted as a reference to compare. From the observations, the performance of all classification algorithms have been improved (The FPRs have been reduced.). Unlike the results shown in Fig 8, the false negative rates (FNR) can be reduced significantly as the size of data sample increases. When N takes a smaller value, the suspicious rates is a little high. From $N = 200$, the suspicious rates are reduced down to a stable and low level.

In summary, from the evaluation shown above, the overall performance of our system can be always improved by applying the dynamic threshold approach. Especially when a high false positive rates appears due to the insufficient sampling accuracy (i.e. the case of high-speed CAN in our evaluation),the overall performance of our system can be improved significantly. From the observations, the false positive rate is

reduced a lot to a low level which can be very helpful for comfortable driving experience.

VI. CONCLUSION

Building security mechanisms for automotive CAN network is urgent and full of challenges. Due to the broadcast nature and no built-in mechanism for verifying the authenticity of frames in CAN, some sophisticated attacks like the impersonation attack which have the ability to manipulate the safety-critical functions of vehicles can be easily launched. Intrusion Detection Systems based on signal characteristics are a promising technology to mitigate the issue. In our paper, a novel IDS which utilizes the inherent difference in clock of devices is proposed for source identification and detection of attacks. Our approach computes the clock skew of devices via a straightforward and effective way. Thus, the computing process can neglect the effect of message queuing or arbitration and reduce the intermediate data which needs to be stored comparing to the state-of-the-art IDSs.

Since the performance of our IDS relies heavily on the measurements of clock skew which depends on the sampling rate, our approach is evaluated on CAN networks with different settings. Our evaluation shows the feasibility and limitation of our method. The results show that the average identification rate on four selected classification algorithms can achieve more than 99.7% when the sampling rate is sufficient. The case when the sampling accuracy is not enough is also discussed and feasible measures for mitigation are proposed. Additionally, our approach is non-destructive which can be well deployed on the automotive CAN network without any modification on the hardware or software of CAN protocol and nodes on the bus. Therefore, it can concluded that our approach is an effective and feasible solution for securing automotive network.

REFERENCES

[1] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, p. 91, Aug. 2015.

[2] C. Urquhart, X. Bellekens, C. Tachtatzis, R. Atkinson, H. Hindy, and A. Seeam, "Cyber-security internals of a skoda octavia vRS: A hands on approach," *IEEE Access*, vol. 7, pp. 146057–146069, 2019.

[3] Z. Cai, A. Wang, W. Zhang, M. Gruffke, and H. Schweppe, "0-days & mitigations: Roadways to exploit and secure connected BMW cars," *Black Hat USA*, vol. 2019, p. 39, Aug. 2019.

[4] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Secur. Privacy*, May 2010, pp. 447–462.

[5] G. Xie, G. Zeng, R. Kurachi, H. Takada, R. Li, and K. Li, "Exact wcrt analysis for message-processing tasks on gateway-integrated in-vehicle can clusters," *ACM Trans. Embedded Comput. Syst.*, vol. 17, no. 6, p. 95, 2018.

[6] M. Di Natale and H. Zeng, "Practical issues with the timing analysis of the controller area network," in *Proc. IEEE Conf. Emerg. Technol. Factory Autom.*, Sep. 2013, pp. 1–8.

[7] H. Zeng, M. Di Natale, P. Giusto, and A. Sangiovanni-Vincentelli, "Stochastic analysis of CAN-based real-time automotive systems," *IEEE Trans. Ind. Informat.*, vol. 5, no. 4, pp. 388–401, Nov. 2009.

[8] G. Xie, G. Zeng, L. Liu, R. Li, and K. Li, "Mixed real-time scheduling of multiple DAGs-based applications on heterogeneous multi-core processors," *Microprocessors Microsyst.*, vol. 47, pp. 93–103, Nov. 2016.

[9] X. Ying, G. Bernieri, M. Conti, and R. Poovendran, "TACAN: Transmitter authentication through covert channels in controller area networks," in *Proc. ACM/IEEE Conf. Cyber-Phys. Syst.*, Apr. 2019, pp. 23–34.

[10] C.-W. Lin and A. Sangiovanni-Vincentelli, "Cyber-security for the controller area network (CAN) communication protocol," in *Proc. IEEE Int. Conf. Cyber Secur.*, Dec. 2012, pp. 1–7.

[11] Y. Xie, L. Liu, R. Li, J. Hu, Y. Han, and X. Peng, "Security-aware signal packing algorithm for CAN-based automotive cyber-physical systems," *IEEE/CAA J. Automatica Sinica*, vol. 2, no. 4, pp. 422–430, Oct. 2015.

[12] W. Wu, R. Li, G. Xie, J. An, Y. Bai, J. Zhou, and K. Li, "A survey of intrusion detection for in-vehicle networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 919–933, Mar. 2020.

[13] Z. Qin and F. Li, "An intrusion defense approach for vehicle electronic control system," in *Proc. Int. Conf. Commun. Electron. Inf. Eng. (CEIE)*, Oct. 2016, pp. 494–499, doi: 10.2991/ceie-16.2017.62.

[14] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *Proc. USENIX Conf. Secur. Symp.*, 2016, pp. 911–927.

[15] M. Muter and N. Asaj, "Entropy-based anomaly detection for in-vehicle networks," in *Proc. IEEE Intell. Vehicles Symp.*, Jun. 2011, pp. 1110–1115.

[16] C. Miller and C. Valasek, "Adventures in automotive networks and control units," *A SANS Whitepaper*, vol. 21, pp. 260–264, Aug. 2013.

[17] M. R. Moore, R. A. Bridges, F. L. Combs, M. S. Starr, and S. J. Prowell, "Modeling inter-signal arrival times for accurate detection of can bus signal injection attacks: A data-driven approach to in-vehicle intrusion detection," in *Proc. ACM Conf. Cyber Inf. Secur. Res.*, 2017, p. 11.

[18] P.-S. Murvay and B. Groza, "Source identification using signal characteristics in controller area networks," *IEEE Signal Process. Lett.*, vol. 21, no. 4, pp. 395–399, Apr. 2014.

[19] 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 Trans. Veh. Technol.*, vol. 67, no. 6, pp. 4757–4770, Jun. 2018.

[20] W. Choi, K. Joo, H. J. Jo, M. C. Park, and D. H. Lee, "VoltageIDS: Low-level communication characteristics for automotive intrusion detection system," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 2114–2129, Aug. 2018.

[21] M. Kneib and C. Huth, "Scission: Signal characteristic-based sender identification and intrusion detection in automotive networks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2018, pp. 787–800.

[22] S. Kulandaivel, T. Goyal, A. K. Agrawal, and V. Sekar, "Canvas: Fast and inexpensive automotive network mapping," in *Proc. 28th USENIX Secur. Symp. USENIX Secur.)*, 2019, pp. 389–405.

[23] J. Zhou, P. Joshi, H. Zeng, and R. Li, "Btmonitor: Bit-time-based intrusion detection and attacker identification in controller area network," *ACM Trans. Embedded Comput. Syst.*, vol. 18, no. 6, pp. 1–23, Jan. 2020.

[24] X. Ying, S. U. Sagong, A. Clark, L. Bushnell, and R. Poovendran, "Shape of the cloak: Formal analysis of clock skew-based intrusion detection system in controller area networks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 9, pp. 2300–2314, Sep. 2019.

[25] M. Kneib, O. Schell, and C. Huth, "EASI: Edge-based sender identification on resource-constrained platforms for automotive networks," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, San Diego, CA, USA, Feb. 2020, pp. 1–16.

[26] M. Di Natale, H. Zeng, P. Giusto, and A. Ghosal, *Understanding and Using the Controller Area Network Communication Protocol: Theory and Practice*. Springer, 2012.

[27] J.-L. Zhang, G. Qu, Y.-Q. Lv, and Q. Zhou, "A survey on silicon PUFs and recent advances in ring oscillator PUFs," *J. Comput. Sci. Technol.*, vol. 29, no. 4, pp. 664–678, Jul. 2014.

[28] J. Zhang, Y. Lin, Y. Lyu, and G. Qu, "A PUF-FSM binding scheme for FPGA IP protection and pay-per-device licensing," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1137–1150, Jun. 2015.

[29] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM/IEEE Design Autom. Conf.*, Jun. 2007, pp. 9–14.

[30] S. Sutar, A. Raha, D. Kulkarni, R. Shorey, J. Tew, and V. Raghunathan, "D-PUF: An intrinsically reconfigurable dram PUF for device authentication and random number generation," *ACM Trans. Embedded Comput. Syst.*, vol. 17, no. 1, p. 17, 2018.

[31] P.-S. Murvay and B. Groza, "TIDAL-CAN: Differential timing based intrusion detection and localization for controller area network," *IEEE Access*, vol. 8, pp. 68895–68912, 2020.

[32] K.-T. Cho and K. G. Shin, "Viden: Attacker identification on in-vehicle networks," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2017, pp. 1109–1123.
[33] M. Foruhandeh, Y. Man, R. Gerdes, M. Li, and T. Chantem, "Simple: Single-frame based physical layer identification for intrusion detection and prevention on in-vehicle networks," in *Proc. 35th Annu. Comput. Secur. Appl. Conf.*, 2019, pp. 229–244.
[34] Y. Yang, L. Wang, Z. Li, P. Shen, X. Guan, and W. Xia, "Anomaly detection for controller area network in braking control system with dynamic ensemble selection," *IEEE Access*, vol. 7, pp. 95418–95429, 2019.
[35] 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. 49375–49384, 2018.
[36] S. U. Sagong, X. Ying, A. Clark, L. Bushnell, and R. Poovendran, "Cloaking the clock: Emulating clock skew in controller area networks," in *Proc. ACM/IEEE Int. Conf. Cyber-Phys. Syst.*, Apr. 2018, pp. 32–42.
[37] H. Lee, S. H. Jeong, and H. K. Kim, "OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame," in *Proc. 15th Annu. Conf. Privacy, Secur. Trust*, Aug. 2017, pp. 57–5709.
[38] *PLL Jitter and Its Effects in the CAN Protocol*, TB078, Microchip Technol. Inc., Chandler, AZ, USA, datasheet, 2004.

JIA ZHOU is currently pursuing the Ph.D. degree in computer science and technology with Hunan University. His research interests include automotive security, cyber-physical systems, and embedded systems.

GUOQI XIE (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from Hunan University, China, in 2014.

From 2014 to 2015, he was a Postdoctoral Research Fellow with Nagoya University, Japan. Since 2017, he has been an Associate Professor with the Department of Computer Engineering, College of Computer Science and Electronic Engineering, Hunan University. His current research interests include embedded and cyber-physical systems, parallel and distributed systems, and software engineering and methodology. He received the Best Paper Award at IEEE ISPA 2016 and the 2018 IEEE TCSC Early Career Researcher Award. He is currently serving on the editorial boards of the *Journal of Systems Architecture*, *Microprocessors and Microsystems*, and the *Journal of Circuits, Systems and Computers*. He is an ACM Senior Member.

SIYANG YU received the Ph.D. degree in computer science and technology from Hunan University, China, in 2017.

He is currently a Teacher with the Hunan University of Finance and Economics. His research interests include industrial Internet of Things, abnormal analysis, and intrusion detection.

RENFA LI (Senior Member, IEEE) is currently a Professor of computer science and electronic engineering with Hunan University, Changsha, China. He is also the Director of the Key Laboratory for Embedded and Network Computing, Hunan, China. His current research interests include computer architectures, embedded computing systems, cyber-physical systems, and the Internet of Things. He is a member of the Council of CCF and a Senior Member of ACM.