Hindawi
Security and Communication Networks
Volume 2020, Article ID 8834845, 17 pages
https://doi.org/10.1155/2020/8834845

Research Article

Advanced Temperature-Varied ECU Fingerprints for Source Identification and Intrusion Detection in Controller Area Networks

Miaoqing Tian,[1] **Ruobing Jiang**, **Haipeng Qu**, **Qian Lu**,[2] **and Xiaoyun Zhou**[1]

[1]*Department of Computer Science and Technology, Ocean University of China, Qingdao, China*
[2]*College of Computer Science and Technology, Qingdao University, Qingdao, China*

Correspondence should be addressed to Ruobing Jiang; jrb@ouc.edu.cn

Received 14 June 2020; Revised 17 September 2020; Accepted 5 October 2020; Published 30 October 2020

Academic Editor: Bela Genge

External wireless interfaces and the lack of security design of controller area network (CAN) standards make it vulnerable to CAN-targeting attacks. Unfortunately, various defense solutions have been proposed merely to detect CAN intrusion attacks, while only a few works are devoted to intrusion source identification. Demonstrated by our experimental studies, the most advanced IDS with intrusion source identification, which is based on the physical feature fingerprints of the in-vehicle Electronic Control Units (ECUs), will fail when the temperature changes. In this paper, we innovatively propose temperature-varied fingerprinting, called TVF, for CAN intrusion detection and intrusion source identification. Motivated by the remarkable observation that the physical feature of an ECU, i.e., its clock offset, changes linearly with the temperature of ECUs, the concept of temperature-varied fingerprints is proposed. Then, for a severe intrusion case, we provide an advanced TVF for further supplemented and expanded. The proposed advanced temperature-varied fingerprinting is implemented, and extensive performance evaluation experiments are conducted in both CAN bus prototype and real vehicles. The experimental results illustrate the effectiveness and performance of advanced TVF.

1. Introduction

With the development of automobile intelligent control systems, multifunctional Electronic Control Units (ECUs) have been mounted in contemporary vehicles. Typically, ECUs exchange messages via the controller area network (CAN) which is a de facto standard for in-vehicle networks. However, due to the lack of security defense design of CAN protocol, those vulnerable ECUs are easily accessed by adversaries to perform CAN-targeting attacks. The vulnerable ECUs are those noncritical and usually support wireless functions, such as WiFi, Bluetooth, and various V2X communications, which can link with outside terminals, including smartphones, base stations, and other vehicles.

The in-vehicle network intrusion is to inject spoofing messages through a vulnerable ECU to the CAN bus, which will induce those safety-critical ECUs to conduct dangerous operations [1–4]. The safety-critical ECUs are those enabling control critical safety-related types of equipment in the vehicle, e.g., automatic cruise system, antiskid brake system, and airbags. An illustrating example of intrusions on CAN bus is shown in Figure 1. ECU X was wirelessly compromised by adversaries, and its messages are noncritical and pose little threat to the car. ECU Y is a critical controller ECU which is able to send brake commands Msg_y through CAN bus when the vehicle overspeeds. Z is a safety-critical ECU with crucial function, which performs brake operations when receiving brake commands Msg_y from Y. In other words, an intrusion attack can be mounted by adversaries through ECU X by sending forged commands Msg_y to the CAN bus to seduce ECU Z performing unexpected braking. Such kinds of intrusion attacks could completely ignore drivers' input and lead to brake errors, power steering failures, or other severe hazards to passengers' safety.

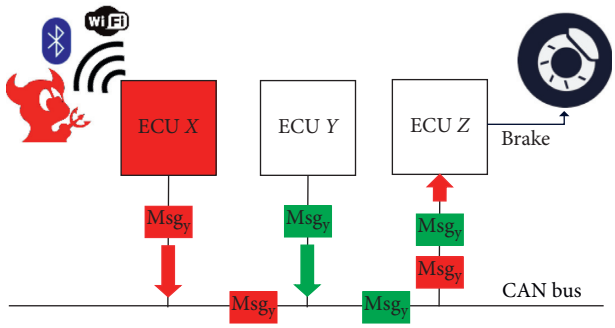

Figure 1: ECU X is wirelessly connected to the outside world and is compromised by an adversary, and the adversary masquerades ECU Y to send forged messages Msg_y to the CAN bus. Consequently, ECU Z conducts the brake when it receives the forged message Msg_y.

Intrusion detection is dedicated to detecting intrusion attacks in in-vehicle networks. It has faced the following challenges. First, it requires high accuracy because any false-positive error may severely affect the safety of drivers. Then, since ECUs inside vehicles have limited computational resources, complex cryptographic algorithms cannot be deployed in vehicles. Last, there are no source or destination addresses in a CAN frame, so it is difficult to trace the attacker ECU even though an intrusion was detected.

Two types of intrusion detection solutions have been proposed for in-vehicle network attacks. One is message-recognition-based intrusion detection systems (IDSs) [1, 5–9] and the other is the source-recognition-based detection solutions [10–16]. In a message-recognition-based detection system, intrusion attacks can be detected by analyzing the message features, e.g., CAN message rate, CAN message time information, and CAN bus entropy. Nevertheless, such message-recognition-based detection solutions cannot recognize which ECU actually mounts the attack, as the CAN frame does not carry any source information. Existing ECU source-recognition-based solutions are typically based on clock skew fingerprint [10, 13] and voltage fingerprint [11, 12, 14–16]. Although these solutions achieve the identification of attack sources, they can only be useful in a temperature-stable environment.

Based on the analysis of the experimental results, we witnessed that the clock skew-based fingerprints are susceptible to the temperature, which leads to the failure of existing clock skew-based fingerprints. According to our observation, only 10 centigrade temperature difference will make the ECU fingerprints fail.

In this paper, we innovatively propose the temperature-varied fingerprinting for intrusion detection and source identification in the in-vehicle CAN network. We utilize the characteristics of clock offsets, which varied with temperature, as fingerprints of each ECU to detect the intrusions and identify the source. Based on the previous work [17], we improve upon the TVF to counter an advanced masquerade attack, in which the adversary delays the transmission by a difference between the target ECU and the compromised ECU on the clock offset. That means the two ECUs have the same clock offset based on the current temperature, yet the previous TVF cannot detect it. The advanced TVF exploits the correlation coefficient of normal and attack messages for detecting. The instantaneous change of the clock offset, which is estimated by messages from one ECU, is impacted by the dynamic temperature. Thus, messages from the same ECU have a high correlation. In contrast, messages from different ECUs are almost irrelevant.

Compared to existing solutions that utilize the information of clock offset for detection and identification, the advanced TVF is more suitable for the interior environment of a vehicle with significant temperature change. The proposed method constructs the fingerprint for each and every ECU within an in-vehicle network according to its temperature-dependent clock offset.

To the best of our knowledge, this is the first work that exploits the temperature-varied clock information to detect and identify the intrusion in in-vehicle networks. This paper has made several contributions as follows:

(i) Based on our observation, we found that the clock offsets of ECUs are varied regularly with the increase in temperature.

(ii) Proposal of TVF, which utilizes temperature-varied fingerprinting for intrusion detection and source identification, and advanced version of TVF is made for further supplemented and expanded.

(iii) The proposed solution is implemented, and extensive experiments are conducted in both CAN bus prototype and real vehicles. The effectiveness of the proposed method has been verified.

The rest of the paper is structured as follows. The related work is provided in Section 2. Section 3 describes the necessary background and the main attack model of the CAN bus. A set of empirical studies of TVF are described in Section 4. In Section 5, we provide an overview of the proposed method, and the details of the proposed method are introduced in Section 6. We evaluated the TVF on the CAN bus prototype and the real vehicle in Section 7. Finally, the paper is concluded in Section 8.

2. Related Work

To resist against in-vehicle network related attacks, researchers come up with two main solutions. One is the message-identification-based intrusion detection systems, and the other is the source-identification-based detection solutions.

2.1. Message-Identification-Based Detection. The message-identification-based IDS is one of the best ways to enhance the security of in-vehicle network, and various IDSs have been proposed to guard against in-vehicle network-related attacks [1, 5, 6, 18–24]. Several message-identification-based IDSs are introduced to detect invasions by analyzing message characteristics, e.g., CAN message frequency, CAN message periods, and CAN bus entropy. In addition,

machine learning is also extensively used in these kinds of intrusion detection systems.

Some of the IDSs are introduced utilizing characteristics and entropy of regular CAN bus to detect attacks. Muter et al. [6] presented a solution to use the features of attack messages to distinguish the intrusions. The solution involves a series of detection sensors that serve as recognition criteria for in-vehicle network intrusions. These detection sensors are constructed with normal properties of the CAN bus network, which are used for distinguishing the abnormal message. However, it cannot detect the attack messages that are entirely in line with the normal behavior of CAN messages. Afterward, an entropy-based attack detection solution is proposed by the author [5], who can successfully distinguish the variations between the normal and abnormal behavior of CAN bus networks.

Several solutions used the time intervals of messages to detect the intrusion. Song et al. [19] proposed an IDS based on the analysis of the feature of CAN message time intervals, and three kinds of injection attacks are performed on the CAN network to evaluate the solution. The result showed the IDS could successfully detect the three attacks within a millisecond. Likewise, Gmiden et al. [25] proposed to use the feature of time intervals of messages with the same ID for intrusion detection, and their solution does not need a modification on CAN standard. Such time-based intrusion solutions are very useful at detecting common intrusion attacks on the CAN bus, e.g., Denial-of-service (DoS) attack. Nevertheless, these solutions seem unable to solve the situation when the attack message has the same time interval with the normal message.

Machine learning was already applied to some solutions for intrusion detection. Seo et al. [7] proposed the GAN-based Intrusion Detection System (GIDS), which used the Generative Adversarial Nets to train only normal data rather than the real attack data for detecting intrusions. GIDS could detect the intrusion attacks without considering the attack types. Kang et al. [8] presented an approach using a deep neural network (DNN) to train the high-dimensional CAN message for detecting. The approach calculates the static characteristics of the inherent properties of normal and attack messages, respectively. Then, the corresponding features are extracted to decide whether the in-vehicle network is being attacked.

However, none of these solutions considered the source ECU of the intrusion message. These IDSs just considered if there was an intrusion on the CAN bus, and no further source identification was made. It is hard to identify the source ECU of the intrusion message because there is no source address in a CAN frame.

2.2. Source-Identification-Based Detection. The source-identification-based detection solutions could track the attack source after they have detected the intrusions. As in-vehicle network such as CAN protocol does not involve any source transmitters information, it is difficult for the above message-identification-based detection solutions to distinguish the exact ECU that launches the attacks. Researchers have proposed solutions that use unique physical features to detect the intrusions and identify the source of the attacks. These unique physical features might be signal voltage, the clock related features, propagation delays, and signal attenuation due to wire lengths [26]. Among these features, clock skew and signal voltage have already been used as fingerprints in the existing ECU source-identification-based approaches.

2.2.1. Voltage Fingerprints. Diverse ECUs had tiny differences in the voltage of electrical signals when they sent the message, which leads by the hardware and production process of the transceiver. Therefore, the unique features of electrical signals could be used as fingerprints for detecting intrusions as well as identifying the source ECU of the intrusion message.

Hoppe et al. [26] proposed a method which utilizes the voltage characteristic of ECUs to detect forged messages. Murvay and Groza [11] also proposed a solution that uses the characteristics of voltage signals of the ID field of the CAN frame to identify the source ECU. The solution used the Mean Squared Error and convolution of voltage signals for fingerprinting ECUs. However, the voltage features on the first few bits of the ID field may not be unique due to the CAN protocol's arbitration rule, so the features on the ID field may not be suitable for fingerprinting ECU.

Choi et al. [27] proposed a source identification detection method. The method chooses to use the voltage features extracted in the extended ID field of an extended CAN frame as fingerprints of ECUs. In their solutions, a supervised learning method is used to classify the statistical voltage features extracted from the extended ID fields. However, the extended CAN frame format has not been widely used in modern in-vehicle networks, and most vehicles are deployed with the standard format on the CAN bus network. Subsequently, the author [15] proposed to use the dominant, positive-slope, and negative-slope portion voltage signals which are extracted from the standard CAN frame as a fingerprint to detect the in-vehicle network attack. The scheme has been verified on real vehicles, and it could discriminate between errors and the bus-off attack on CAN bus [28].

A voltage-based attacker identification (Viden) [12] approach was come up to identify the source ECU of the intrusion message on the CAN bus which used the feature of voltage signals as fingerprints. Viden first learns the ACK threshold from the voltage signals that send from the real source ECU in the ACK slot field of a CAN frame. Then, it selects appropriate voltage signals based on the ACK threshold to derive the voltage instance, which is a set of features of an ECU's voltage output. After that, Viden uses the voltage instance obtained from every new signal to construct and update an ECU's voltage profile as its fingerprint. Finally, the voltage profiles are used to distinguish the source ECU. Viden could ignore the type of frames and the transmission speed to identify the attacker ECU in various conditions. Nevertheless, the voltage signals are

sensitive to temperature, which causes the Viden to be less accurate.

Kneib and Huth [16] proposed an intrusion detection system called Scission. Scission extracts the voltage signal feature for fingerprinting ECUs and thus to detect intrusions and identify the sender ECU. The effectiveness of Scission has been verified in the real vehicle. Besides, the influence of temperature on voltage signals is also considered in the Scission. Scission is proved to be valid in the temperature of 23°C, 25°C, 32°C, and 36°C, respectively. However, there remains a higher and lower temperature under practical conditions.

2.2.2. Clock Skew Fingerprints. The clock frequencies information, which is uniquely determined by the quartz crystal clock in the transmitter ECU, can be utilized to distinguish different ECU. A clock-based IDS (CIDS) solution [10] was proposed to use accumulated clock offset for fingerprinting the transmitter ECU to detect and identify intrusions. Based on the thus-obtained fingerprints, CIDS builds the model of ECUs' clock behaviors to detect the intrusion and identify the source of the intrusion message. Nevertheless, the solution did not adequately consider the temperature, and the solution could be valid only in a temperature-stable environment.

Sagong et al. [13] proposed a cloaking attack which could emulate the clock skew of the ECU on CAN bus. The clocking attack is an intelligent masquerade attack that could deceive CIDS. However, the cloaking attack is designed under the assumption that the clock skew of an ECU is constant. They still did not consider the temperature change in the vehicular environment. The temperature will enable the clock offset to vary, which will make the clock skew not constant.

Existing source-identification-based detection solutions could detect the intrusions and identify the transmitter ECUs well when the temperature is stable. However, these solutions may fail when the temperature of ECUs changed. Moreover, the temperature of an ECU is directly affected by the neighboring environment, especially the engine, which will make some of the ECU's temperature unstable. The features such as voltages and clock offset-based fingerprints are susceptible to the temperature and thus affect the accuracy. Consequently, these solutions will fail because of the unstable temperature of ECUs inside the vehicle.

3. Background

In this section, we describe the background of the CAN bus and the ECUs. And then, the attack model is given.

3.1. CAN Bus. Controller Area Network (CAN) bus is the communication channel between ECUs inside vehicles, which adopts the CAN protocol. CAN protocol provides a broadcast transmission mechanism, and all nodes (ECUs) are connected through one single bus. In other words, the message sent from one ECU is broadcast to all other nodes on the CAN bus. When other ECU receives the broadcast message, it will check and determine whether to receive the message. An example of messages transmission on CAN bus is shown in Figure 2; ECU X sends its prepared message to the CAN bus. ECU Y and ECU Z are both on the bus and receive the message in turn. Then, each node checks the message to make sure if it wants. Finally, ECU Y checks and accepts the message while ECU Z ignores it. Each node only accepts the messages it wants and ignores the others.

There are four kinds of CAN frames on the CAN bus, and they are data frame, remote frame, error frame, and overload frame. Among them, we focus primarily on the data frame as it carries more useful information, such as command and sensor data. There are two kinds of data frames: one is the standard frame with an 11 bit identifier (CAN2.0A), and the other is the extended frame with a 29 bit identifier (CAN2.0B) [29]. We mainly focus on the standard frame in the proposed method, as the standard frame is the most widely used in modern vehicles. In the following, we called the standard data frame the CAN message. As shown in Figure 3, a standard CAN data frame involves fields such as Start of Frame (SOF), identifier (ID), CRC, and ACK. We can see that the standard data frame does not contain the protection measures fields such as encryption or authentication. Moreover, CAN frames do not contain a validation field or any source address identifier field so that the node can send packets indiscriminately to the others. In other words, if the adversaries compromise one ECU, he can inject messages arbitrarily into the CAN bus through this node and thus conduct hazardous operations.

When multiple ECUs send messages to the CAN bus simultaneously, to avoid the collision, each node sends the messages according to the priority depending on the ID. That is to say, messages with lower IDs have a high priority to send. For instance, if two messages are sent on the CAN bus with the ID value of 0×13 and 0×72 at the same time, the message with ID 0×13 is sent first due to the lower value.

We assume that all the ECU and its sending messages are known by default. Moreover, we can get the correspondence between the ECU and its message from the vehicle manufacturers. The other way is to reverse engineer the messages in the CAN bus [1].

3.2. ECU Security Levels. The modern vehicle has approximately 25 ECUs in it, and the number of ECU in some high-end models is even more than 100 [30]. These ECUs have diverse functions, for example, some ECUs control the window and the door, and others may control brake. They are connected with each other via the CAN networks and located in different positions inside vehicles. The position of the ECU varies with the model of the vehicle. We summarized most of the models and obtained the ECU distribution in the vehicle, as shown in Figure 4. The ECUs, which have a high demand for real-time messages, are in the high speed CAN bus (the red line), and most of these ECUs are closely related to the safe driving of the vehicle. As the name suggests, the low speed CAN bus line of the ECUs have a low real-time requirement for messages, and these ECUs have less threat to the safety of the vehicle.

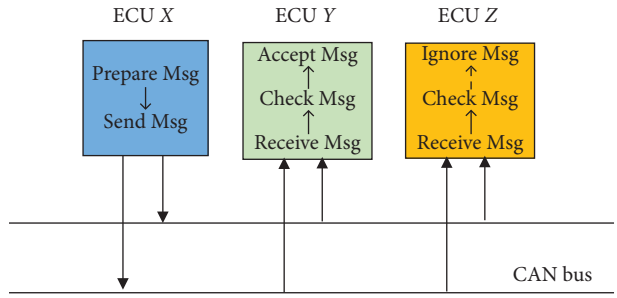

Figure 2: Message transmission on CAN bus.

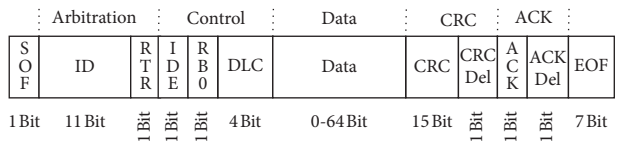

Figure 3: Format of the standard data frame on the CAN bus.

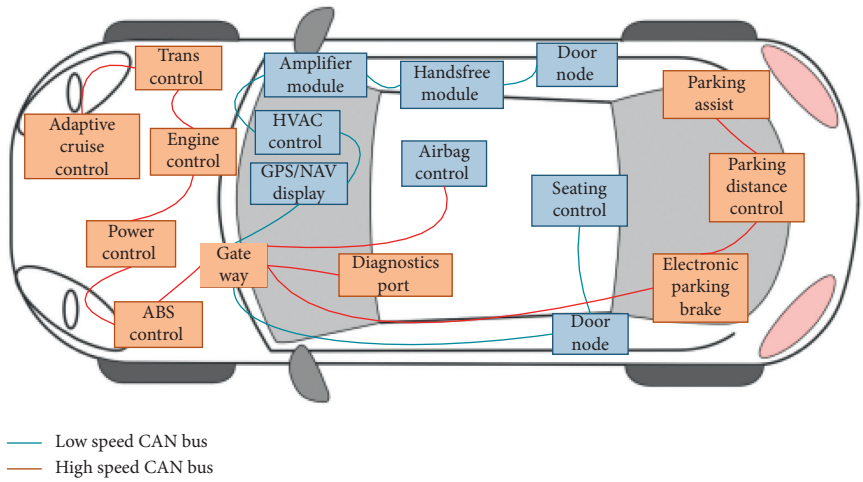

Figure 4: The ECU distribution in a vehicle.

Based on the security requirement, ECUs can be divided into safety-critical ECUs and less critical ECUs. Among the various ECUs, the safety-critical ECUs are generally supposed to be able to control the critical safety-related facilities, e.g., engine ECU, automatic transmission ECU, and antilock brake system ECU. Such critical ECUs are connected to the high speed CAN bus in a wired and secure manner. However, there are some less critical ECUs, such as the Tire Pressure Monitoring System (TPMS) and Gateway ECU, which may have multiple modes of communication in the high speed CAN bus. These kinds of ECUs could communicate with the CAN bus network and the wireless network, and the wireless network can be used as remote access points to attack the in-vehicle network [1–3, 31].

3.3. Attack Models. At present, adversaries have two ways to invade the in-vehicle CAN network. One way is to inject the forged message through the compromised ECUs that are remotely cracked by various wireless attack surfaces [1, 2]. Another way is to inject the forged message into the in-vehicle network via the OBD-II interface inside the vehicle. We mainly focus on the former one since the second one needs physical access to the vehicle and lacks flexibility. The main attack models are discussed below.

3.3.1. Attack Models. The adversary could inject forged messages into the CAN bus network and thus control the vehicle, as long as he compromised one of the ECUs via various wireless or wired attack surfaces. This is because messages are broadcast to all ECUs on a single CAN bus in vehicles, and there is no source address or authentication field on a CAN frame. When ECUs receive the broadcast message, they will check the message and determine whether to receive it or not. So, the forged messages which are sent by the adversary will be executed indiscriminately by the ECU. According to the research [10], the attack models are mainly

classified by three kinds: the *suspension attack*, the *fabrication attack*, and the *masquerade attack*. A suspension attack, just as the name implies, means the compromised ECU is suspended from sending its message by the adversary. The fabrication attack means the ECU is compromised to send any forged messages to the CAN bus. The masquerade attack is a more covert attack that contains the suspension attack and the fabrication attack. It means that two ECUs need to be compromised. Among the two ECUs, the one who sent the target message is imposed on the suspension attack, and the second one is imposed on the fabrication attack to send the target message. It means the second ECU is compromised to send the message with the same ID and period of the suspend ECU. Miller et al. [32] had mounted the masquerade attack on the Jeep Cherokee controlling the ABS collision prevention system. In the proposed method, we primarily focus on the masquerade attack as it can cause more severe damages to vehicles.

3.3.2. Advanced Attack Model. There is an enhanced masquerade attack in which the adversary is able to alter the ECU's temperature and thus change the clock offset. To mount this attack, the adversary could cool down or heat up the compromised ECU to mimic the target ECU's clock offset [10]. Moreover, the enhanced masquerade attack cannot be detected and identified by our previous work [17].

4. Empirical Study

In this section, we first did a simple experiment and observed the influence of temperature on the ECU's clock offset. Then, a further observation of the clock offset is described on distinct ECUs at different temperatures.

4.1. Setup. We discovered that the clock offset changes with temperature, which will cause the clock-based fingerprints to fail by some sample experiments. Inspired by CIDS [10], which utilized the clock offset inherent in the ECU as fingerprints to identify the attacker ECU, we replicated their algorithm with the same experimental setup, e.g., a CAN prototype. Through multiple experiments, we found that the temperature has a significant impact on the clock offset. Then, we carried out the experiments at the temperature of 10°C and 30°C, respectively. We measured the clock offset at the two temperatures and found that the average clock offset of one ECU at 30°C was slightly larger than it at 10°C.

4.2. Observation. In a vehicle, the temperature of ECUs is correspondingly changed with the driving status and the ECU's positions in the car. We have investigated various models of cars and found that most ECUs are distributed in the engine cabin of the car. The engine temperature is the most significant factor that affects the ECU temperature, with the highest temperature of more than 80°C after the car started. As shown in Figure 5, we measure the temperature distribution in the engine cabin of a Volkswagen Polo vehicle after it has been driven for 30 minutes at a speed of

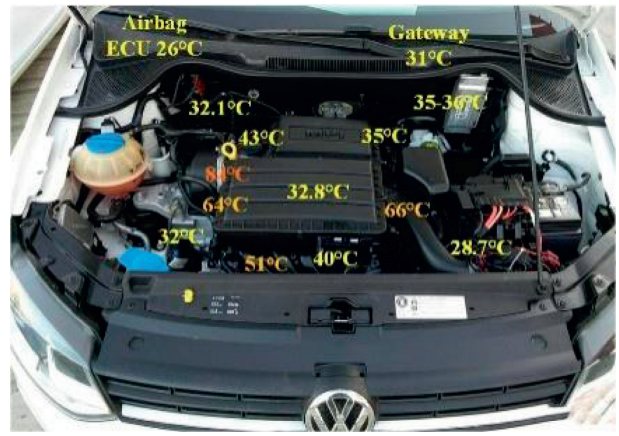

Figure 5: The temperature distribution in the engine compartment of a car after it has been driven for 30 minutes at a speed of 40 km/h.

40 km/h when the ambient air temperature was at 15°C. The temperatures of each part, including the ECUs, are scaled from 26°C to 84°C in the engine cabin of the car, and the temperatures of the ECUs are different with their locations. For instance, the temperature of the ABS ECU is 43°C. While the temperature of gateway ECU and airbag ECU is 31°C and 26°C, respectively.

We observed the intervals of messages with the same ID at two different temperatures and found they are different. The probability mass function of message intervals at different temperatures for the same message is shown in Figure 6. We can clearly see that the message interval of 0×30 is concentrated at 50.675 ms at 20°C, while it is about 50.7 ms at 70°C.

According to the above experimental results, the average clock offset of ECU is susceptible to temperature, and the value of the clock offset increases with the rising of temperature. We measured the clock offset of ECU *A* and ECU *B* from 10°C to 50°C, respectively. The results are shown in Figure 7, and the average clock offset of both ECUs varies about linearly with temperatures from 10°C to 50°C. In addition, according to our observation, if ECU *A* is 10° higher than ECU *B*, they will have the same clock offset. This situation may exist in real vehicles, which can render existing fingerprint-based methods ineffective. To sum up, the influence of temperatures should be considered when using the time information as ECUs' fingerprints.

5. Overview

In this section, we first provide the basic terminology for the problem statement and then explain the basic idea of TVF.

5.1. Problem Statement. The chief problem that TVF solves is to detect the intrusion attack and identify the attack source on the CAN bus, and the essential variables and terminology description are formalized as follows. We follow the definition of the clock offset in Paxson [33]. One additional ECU is used for recording the timestamp when the traffic on the CAN arrived, denoted by ECU U_R. Let U denote the nodes

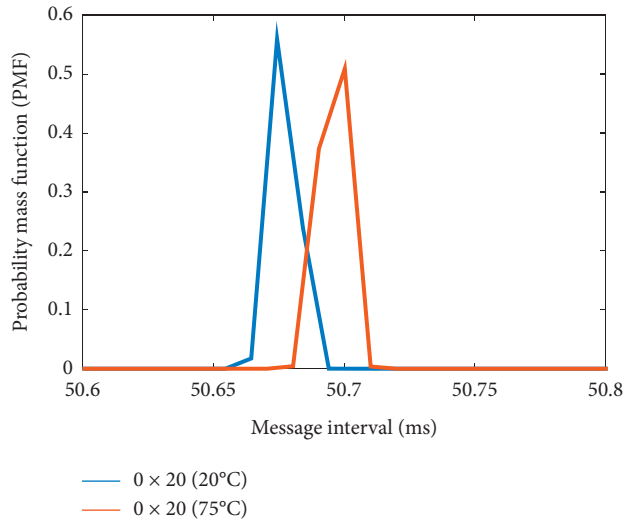

Figure 6: The probability mass function (PMF) of message intervals at different temperatures for the message with the same ID.

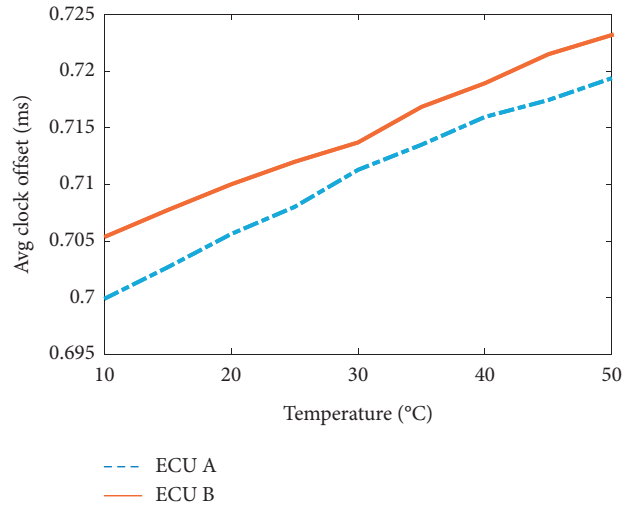

Figure 7: The average clock offset curve of ECUs at different temperatures.

(ECUs) on the CAN bus, $U = \{U_1, U_2, \ldots, U_i, \ldots, U_n\}$, and all these ECUs send periodic messages on the CAN bus. Typically, each ECU can send at least one kind of periodic message. We chose one of the periodic messages to denote the clock information of the ECU, as the messages with multiplied IDs that are sent from the same ECU have the same clock offset. The periodic message M_{iR} that is sent from ECU U_i to ECU U_R at temperature C_t ($0^\circ\text{C} < T_c < 80^\circ\text{C}$) is denoted by the tuple $M_{iR} = \{U_i, U_R, S_{it}, ID_i\}$, where $S_{it} = \{S_{it,1}, S_{it,2}, \ldots, S_{it,j}, \ldots, S_{it,m}\}$ refers to the timestamp sequence of the message M_{iR}. We primarily consider the periodical messages on the CAN bus because most of the messages on the CAN bus are sent periodically. Even in some models of vehicles, all the messages on the CAN bus are periodical [10, 34, 35]. We do not consider the nonperiodic messages in the proposed method.

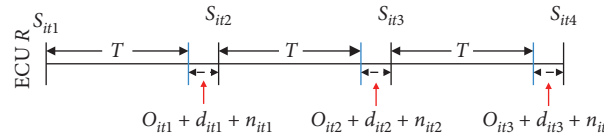

Figure 8: The clock offset of message arrivals.

As shown in Figure 8, ECU U_R is the receiving end, and a series of messages with period T is sent from ECU U_i. The interval of two adjacent timestamps is a bit larger than T, as the hardware quartz crystal clock induces the sending ECU U_i to deviate from the real clock with a small offset from the true clock each time. The timestamp interval of the message with the same ID at C_t is denoted by

$$I_{it,j} = S_{it,(j+1)} - S_{it,j} = T + O_{it,j} + n_{it,j} + d_{it,j}, \quad (1)$$

where $O_{it,j}$ is the relative clock offset between U_i and U_R when U_i sends the jth message at C_t, $d_{it,j}$ is the transmission delay of one message on the CAN bus, and $n_{it,j}$ is the noise generated by the quantization process of the timestamp at the receiver [36]. Later, in this paper, we refer to the clock offset as relative clock offset. $d_{it,j}$ tends to zero and $n_{it,j}$ is a zero-mean Gaussian noise term [36], and both of them are little affected by temperature. It is reasonable to assume $E[d_{it,j}] = 0$ and $E[n_{it,j}] = 0$; then, we have $E[I_{it,j}] \approx T + E[O_{it,j}]$. So, the average clock offset can be calculated as follows:

$$E[O_{it,j}] = E[I_{it,j} - T] = E[S_{it,(j+1)} - S_{it,j} - T]. \quad (2)$$

Let $\Omega_i = \{(C_1, O_{i1}), (C_2, O_{i2}), \ldots, (C_t, O_{it}), \ldots, (C_h, O_{ih})\}$, where O_{it} is the average clock offset that deduce by M_{iR} at C_t. The average clock offset O_{it} of an ECU increases linearly with temperatures that ranged from 0°C to 80°C, which can be described by a linear model, denoted f_i. The uniquely linear model f_i can be used as the fingerprint of an ECU.

Given the message timestamp sequence S_{it} and the temperature C_t, the intrusions can be detected. Intrusion detection can be described as the problem whether the derived vector (C_t, O_{it}) belongs to f_i or not. After the intrusion has been detected, we can get the clock offset of intrusion message O_{ai}. Then, with the cooperation of f_i of each ECU, the intrusion source could be identified.

5.2. Basic Idea. The proposed TVF consists of three phases: fingerprint construction, intrusion detection, and source identification. Figure 9 shows the overview of the proposed method. An ECU clock contains a crystal oscillator that ticks at a nominal frequency and a counter for counting ticks. However, the actual frequency which determines the clock offset of an ECU is affected by the environment, such as the temperature [36, 37]. Based on our observation, the average clock offset of ECU varies regularly with temperatures. Therefore, we chose the average clock offset at different temperatures as the fingerprint, and the basic idea of our method is described below.

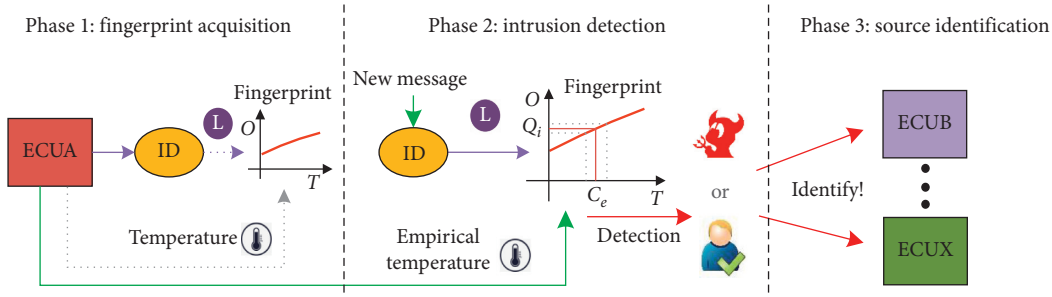

Figure 9: The overview of the proposed method.

5.2.1. Fingerprint Construction. To construct the temperature-varied fingerprint of ECU in a real vehicle, we need to calculate the clock offset of the ECU at different temperatures.

In a vehicle, the temperature of an ECU is influenced by the surroundings, e.g., the position of ECUs, the vehicle's driving status, and the ambient temperature. Among them, the most influential factor is the driving status of a vehicle. By measuring the temperature of the ECU in different driving status, we can roughly know the temperature range of the ECU. Besides, the temperature range of each ECU can be obtained from the vehicle manufactures. To make sure the normal works of ECUs, the automobile manufacturer will measure the temperature range of ECUs during all driving status before an automobile leaves the factory.

5.2.2. Intrusion Detection. We first calculate the average clock offset (O_i) based on the timestamps of the newly obtained messages with the same ID. According to the message ID, the transmitter ECU can be determined. Then, we can estimate the temperature (C_e) (empirical temperature) of the ECU according to the vehicle's current driving status. Finally, whether the vector (C_e, O_i) conforms to the fingerprint model of the ECU U_i can be determined. If this vector does not belong to the model f_i, the message can be judged as the intrusion message.

We refer to the ECU's temperature at different driving status as the empirical temperature of an ECU, denoted as C_e, and refer to the temperature that deduces by the fingerprint model and the timestamps of the message as the real temperature, denoted by C_r. The value of real temperature C_r is correct at the fingerprint construction phase. However, the value of C_r maybe fake in the intrusion detection phase, as another ECU may forge it.

5.2.3. Intrusion Source Identification. The ECU that may mount the attack can be deduced according to the average clock offset of intrusion messages and the fingerprint model. Based on the average clock offset of the intrusion messages and the fingerprints, the attack temperatures C_{ir} of each ECU can be obtained. If the attack temperature C_{ir} is in the error range of the empirical temperature C_{ie}, the ECU can be judged as the intrusion source ECU.

To achieve the basic idea described above, we have to face the following challenges.

5.2.4. Fingerprint Model Acquisition of ECU. The clock offset of ECU at each temperature needs to be obtained within its safe operating temperature range; then, the fingerprint model is constructed through the average clock offset at each temperature.

5.2.5. Intrusion Detection. The average clock offset of newly arrived messages and the ECU's empirical temperature is used to determine whether the messages are normal or not. How to distinguish between normal and abnormal messages is an important issue concerning the accuracy of intrusion detection.

5.2.6. Source Identification. After detecting the intrusions, we need to determine the source ECU of the intrusion messages. Since CAN messages do not contain any source information of transmitter ECU, it is difficult to get the intrusion source directly through the intrusion messages.

6. Proposed Approach

In this section, we describe our method to detect intrusions and identify the source of intrusions. According to our experimental observation, the clock offset of ECUs varied with temperature can be fingerprinted. Then, the thus-obtained fingerprints can be used to detect intrusion messages as well as to identify the source ECU. The flow chart is shown in Figure 10, and we describe the proposed TVF in three steps: the construction of fingerprints, the detection of intrusion messages, and the identification of intrusion source ECU.

6.1. Construction of the Fingerprints. For each ECU, the temperature-varied fingerprints were constructed when there were no intrusions. One can obtain the average clock offset from the periodic message $M_{iR} = \{U_i, U_R, S_{it}, ID_i\}$ of each ECU at a certain temperature from 0°C to 80°C. Through multiexperimental observations, we discovered that the average clock offset of each ECU is grown linear with the temperature at the working range. Hence, the fingerprint can be described as the linear regression model:

$$f_i: O_{it} = k_i C_t + e_i, \tag{3}$$

where O_{it} represents the average clock offset of ECU U_i, C_t is the temperature, k_i is the regression parameter, and e_i is the

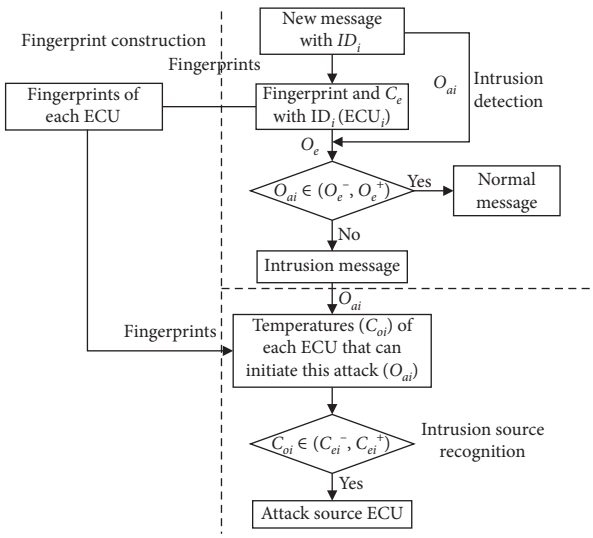

Figure 10: Flow chart of our method.

fingerprint error. The regression parameter k_i represents the slope of the linear fingerprint model. In order to obtain the unknown parameter k_i, we use the Least Square Method (LSE) to calculate the fingerprint model f_i of each ECU. The LSE is used to find the optimal value of the objective function. Here, we use it to find the optimal solution of linear regression. The pseudocode of the fingerprint construction with LSE is illustrated in Algorithm 1.

6.2. Intrusion Detection. In this phase, the timestamps of the newly arrived message and the empirical temperature of the ECU that matched the arrived message is used to determine whether there is an intrusion on the CAN bus. Measure a given ID message for a period of time to get $M_{xR} = \{U_x, U_R, S_{xr}, ID_x\}$, and the clock offset O_{xr} of ECU U_x can be deduced through its timestamp sequence S_{xr}.

In the meantime, the empirical temperature C_{xe} of ECU U_x also can be estimated from the driving status. Once the empirical temperature C_{xe} is obtained, we can get an average offset O_{ex} from the fingerprint. The average clock offset resembles a Gaussian distribution at a specific temperature. Then, if the value of $|O_{xr} - O_{xe}|$ is bigger than $0.8\sigma_{xe}$, where σ_{xe} is the standard deviation of the average offset at the empirical temperature C_{xe}, the message with ID_x will be considered as a masqueraded attack message. If it is a normal message, the real temperature C_r and the empirical temperature C_e should be basically the same, or else it may be considered as an intrusion message. In other words, by judging whether the value of O_{xr} belongs to $[O_{xe} - 0.8\sigma_{xe}, O_{xe} + 0.8\sigma_{xe}]$, we can detect the intrusion message. The pseudocode of the detection of masquerade attacks is illustrated in Algorithm 2.

6.3. Message Source Identification. The masquerade attack has been detected in the previous step, and next TVF will identify the real source ECU that sends the attack message, as the attack message was sent by a different ECU rather than the original one. Firstly, the attacked average clock offset O_{ack} can be obtained through the detected intrusion message, and its value is the clock offset of the ECU that sends the intrusion message. By substituting the clock offset O_{ack} into the fingerprints of each ECU, we can get the possible attack temperature of each ECU, denoted as C_{ir}. At the same time, we empirically get the temperature error range $[u_{ie} - 0.8\sigma_{ie} - e_i/k_i, u_{ie} + 0.8\sigma_{ie} - e_i/k_i]$ of each ECU. If C_{ir} is in the empirical temperature error range, ECU U_i is determined as the source ECU of the intrusion message. The pseudocode of source identification is illustrated in Algorithm 3.

6.4. Advanced Method. There is a situation that can lead to the failure of TVF. When the clock offset of the attacking ECU is exactly the same as that of the attacked ECU, TVF cannot detect the intrusion in this situation. Because the average clock offset of the attacker ECU is almost equivalent to that of the intruded ECU and its value is in the normal range of the clock offset of the intruded ECU, TVF cannot detect it. When the two periodic messages are sent from the same ECU with different IDs, their average clock offsets are almost equal, and the value of the correlation coefficient, ρ, of the two messages is close to 1. While the correlation of periodic messages sent from different ECUs, $\rho \simeq 0$.

For the above situation, we have made an advanced method, which is an advanced supplement based on TVF. We use the correlation coefficient ρ of the average clock offset of the two periodic messages to detect the intrusion and identify the source. The correlation coefficient of the clock offset of periodic messages can be used to judge whether these two messages are sent from the same ECU, especially inside a car. In other words, the advanced masquerade attack can be detected and identified depending on the value of the ρ of two periodic messages, as the temperature changed clock offset of the two messages from the same ECU has a higher correlation coefficient. Figure 11 shows the kernel density plots of the Pearson correlation sets of the periodic messages sent from the same ECU and different ECUs, respectively. The measurements were collected by the CAN prototype shown in Section 7. One can see that the two sets both resemble Gaussian distribution, and the two distributions are distinct from each other. A threshold value of τ is used to distinguish the two sets. TVF determines value $\tau = F_s + F_d/2$, where $F_s = u_s - 3\sigma_s$, μ_s and σ_s are the mean and the standard deviation of the sets from the same ECU, respectively. $F_d = u_d - 3\sigma_d$ is the set that is sent from different ECU, where μ_d and σ_d are the mean and the standard deviation, respectively.

If two messages are sent from the same ECU, their correlation coefficient is higher than τ. Then, the correlation coefficient is lower than τ when two messages are sent from different ECUs. Based on this, the advanced TVF can check the value of ρ to determine whether the two messages are sent from the same ECU or different ECUs. For example, ECU A sends 0×11 and 0×55 periodically, and the value ρ of the two messages may be higher than τ as they are sent from the same ECU. While ECU B

Require: $\{S_{it}\}$: a set of timestamp sequence of messages with ID_i that are sent from ECU U_i at a temperature of C_t;
Ensure: periodic message with the periods of T.

(1) $j = 1$, $m = |S_{it}|$, $N = |C_t|$
(2) **for** $j = 1$ to $m - 1$ **do**
(3) $\quad I_j \longleftarrow S_{it,(j+1)} - S_{it,j}$ ▷ Timestamp interval
(4) $\quad j \longleftarrow j + 1$
(5) **end for**
(6) $O_{it} \longleftarrow (1/m-1)\sum_{j=1}^{m-1}(I_j - T)$ ▷ Average offset at temperature C_t
(7) **function** LSE (O_{it}, C_t)
(8) $\quad k_i = \sum_{t=1}^{N} O_{it}C_t - (1/N)\sum_{t=1}^{N} O_{it}\sum_{t=1}^{N} C_t / \sum_{t=1}^{N} O_{it}^2 - (1/N)\sum_{t=1}^{N} O_{it}\sum_{t=1}^{N} O_{it}$
(9) $\quad e_i = (1/N)\sum_{t=1}^{N} O_{it} - k_i(1/N)\sum_{t=1}^{N} C_t$
(10) **end function**

Algorithm 1: Fingerprint construction with LSE.

Require: $\{S_{xr}\}$: a set of timestamp sequence of new arrival messages with ID_x that are sent from ECU U_x;
C_{xe}: the empirical temperature of ECU U_x at the moment;
O_{xe} the standard deviation of ECU U_x's average clock offset distribution at the temperature of C_{xe}.
Ensure: periodic message with the period of T.

(1) $j = 1$, $m = |S_{xr}|$,
(2) **for** $j = 1$ to $m - 1$ **do**
(3) $\quad I_j \longleftarrow S_{xr,(j+1)} - S_{xr,j}$
(4) $\quad j \longleftarrow j + 1$
(5) **end for**
(6) $O_{xr} \longleftarrow (1/m-1)\sum_{j=1}^{m-1}(I_j - T)$▷Average offset
(7) $O_{xe} \longleftarrow k_x C_{xe} + e_x$
(8) **if** $|O_{xr} - O_{xe}| > 0.8\sigma_{xe}$**then**
(9) $\quad$ **return** 1 ▷ Intrusion message
(10) **else**
(11) $\quad$ return 0
(12) end if

Algorithm 2: Masquerade attack detection.

Require: $\{O_{\text{ack}}\}$: the average clock offset of intrusion message;
μ_{ie}, σ_{ie}: the mean and standard deviation of ECU U_x's average clock offset at the empirical temperature of C_{ie}
Ensure: periodic message with the period of T.

(1) $C_{ir} \longleftarrow O_{\text{ack}} - e_i/k_i$ ▷ Attack temperature of each ECU
(2) **if** $C_{ir} \in [\mu_{ie} - 0.8\sigma_{ie} - e_i/k_i, \mu_{ie} + 0.8\sigma_{ie} - e_i/k_i]$ **then**
(3) $\quad$ **return** i ▷ Attack source message
(4) **end if**

Algorithm 3: Source identification.

masqueraded ECU A to send the message 0×11, and the value ρ may be lower than τ. Then, the attack on the CAN bus can be detected as well as the source ECU of it depending on the threshold value of ρ.

7. Evaluation

We now evaluate TVF on the CAN bus prototype and a real vehicle. Numerous experiments were carried out to prove the temperature-based clock offset, which can be used as fingerprints of ECUs. Then, based on this, the intrusion message can be detected, and the source can be identified in the CAN bus network.

7.1. Setup. A CAN bus prototype with four Arduino-based ECUs and a desktop thermostatic test chamber is used for the simulation experiment, and a real vehicle is also used in the real-world situation experiment.

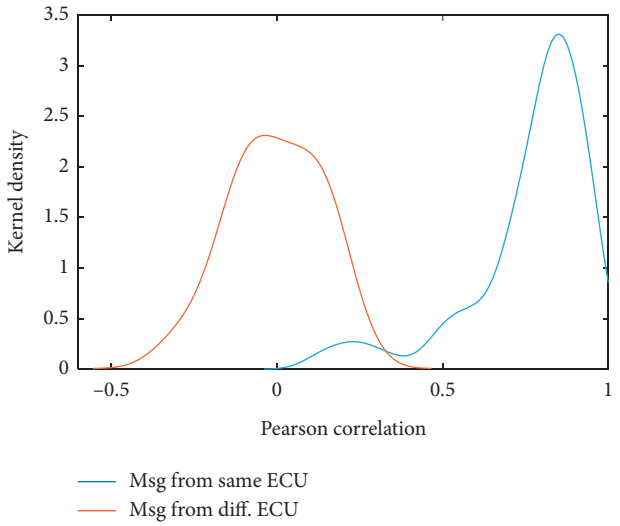

Figure 11: The Pearson Correlation of different messages from different ECU.

7.1.1. CAN Bus Prototype. The CAN bus prototype involves four CAN transceiver nodes, each node consists of a Seeeduino CAN bus shield and an Arduino UNO board [38, 39]. The Seeeduino CAN bus shield is an open-source MCU development board that consists of an MCP2515 CAN controller, an MCP2551 CAN transceiver, and a 120 Ω terminating resistor for the communication of CAN bus. The CAN bus prototype with four CAN nodes was set up to operate with a speed of 500 kbps. We only kept the resistor of two longest-distance nodes, which as the terminating resistor, and removed the resistor from the CAN shield PCBs of the other two notes to prevent signal reflection during communication on the CAN bus. On the CAN bus prototype, the first node A was programmed to send message 0×11, node B to send message 0×33 and 0×55, and node C to send message 0×68 and 0×90. These three nodes were set to send messages at the same frequency, and the sending periods were 50 ms. Node D was programmed as the message receiving node to run TVF.

7.1.2. Desktop Thermostatic Test Chamber. As shown in Figure 12, we used the desktop thermostatic test chamber to simulate the temperature of an ECU in a real vehicle. The model of the desktop thermostatic test chamber is DHTHM-50-20P-SD, and its working temperature ranges from −20°C to 180°C. Nodes A, B, and C were put inside the thermostatic test chamber to send messages. To precise measuring the temperature changed clock offset the former three nodes, we put node D outside the test chamber in a stable temperature as the receiver node. The temperature is set up from 0°C to 80°C according to the operating temperature range of the ECU in the real vehicle.

7.1.3. Real Vehicle. As shown in Figure 13, a Toyota Vios 2017 was used for our experiments in a safe and controllable environment. We used our CAN bus prototype to connect to the On-Board Diagnostics (OBD-II) system port [40] of the

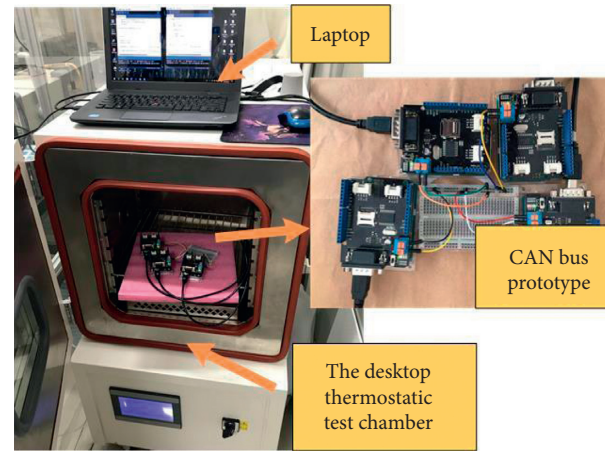

Figure 12: CAN bus prototype and desktop thermostatic test chamber.

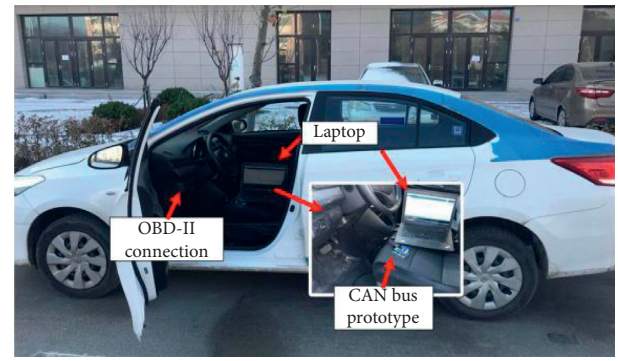

Figure 13: Toyota Vios 2017 used for experiments on real vehicle.

vehicle with a DB9 to OBD2 Cable. The CAN bus prototype was used to capture the traffic from the in-vehicle network. To get the different temperatures environments, we experimented at noon and night during 7 days, and the average temperature was about 12°C at noon and 2°C at night. These experiments were carried out when the vehicle drives at a constant speed of 40 km/h for a trip of approximately 30 minutes. Considering the security problem, we only measured the data of the real vehicle for fingerprinting ECUs.

7.2. Temperature-Varied Clock Offset as a Fingerprint. We verified the utility of TVF and built it on the CAN bus prototype and a real vehicle.

7.2.1. CAN Bus Prototype. We built the TVF of ECUs on the CAN bus prototype. The clock offsets deduced by message series are stable at a constant value at a certain temperature, and the values of each ECU are distinguished from each other. As shown in Figure 14(a), the clock offsets which are deduced by the three ECU's messages on the prototype are stable at 0.7042 ms, 0.6986 ms, and 0.6748 ms at 20°C, respectively. By exploiting the clock feature of ECU, CIDS [10] builds the fingerprint of ECUs to detect the intrusions and

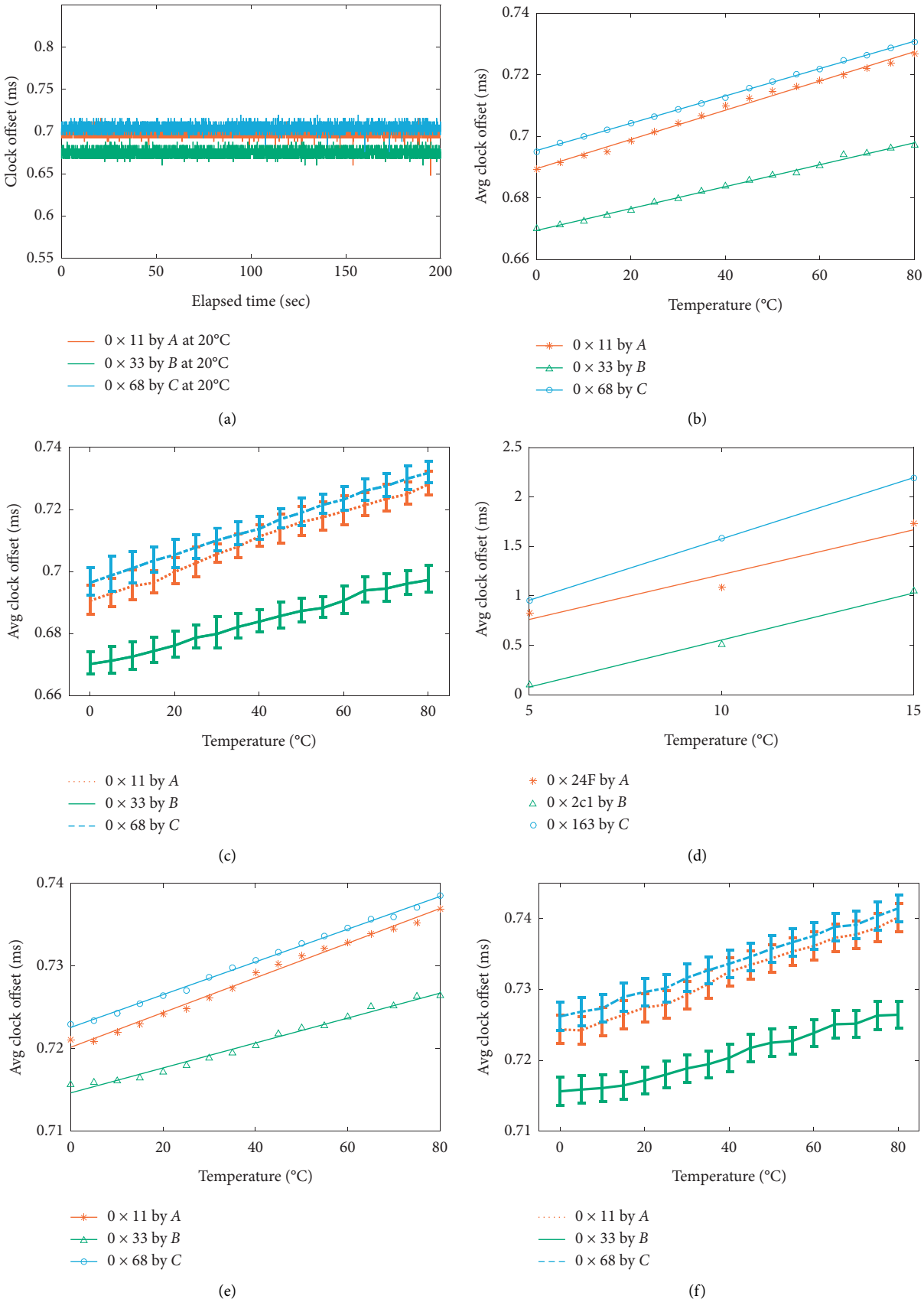

FIGURE 14: The clock offset and fingerprint of ECU in different evaluation settings. (a) The clock offset of ECUs at 20°C. (b) The fingerprints of ECUs with $T = 50$ ms. (c) The error bar of fingerprints with $T = 50$ ms. (d) The fingerprints of the real vehicle. (e) The fingerprints of ECUs with $T = 20$ ms. (f) The error bar of fingerprints with $T = 20$ ms.

identify the actual transmitter ECU. Nevertheless, we found that the clock offsets of the ECU varied with the temperature. Then, we built the temperature-varied fingerprint for detecting and identifying.

The temperature-varied clock fingerprints of the CAN bus prototype are shown in Figure 14(b). The average clock offsets were calculated every five degrees with the rise of temperature. All the deduced averaged clock offsets are linear with the temperature grows, and we use the LSE to build the fingerprint of each ECU. We can see the linear models of the three ECUs are separated from each other with the growth of the temperature, which can be used as the fingerprint to distinguish ECUs. The error bar graph of the average clock offset is shown in Figure 14(c). The clock offset fluctuates between up and down errors of 0.005 ms centered the average value. Still, clock offsets of different ECUs can be distinguished from each other. The average clock offset of node A was 0.6964 ms at 0°C, while it increased to 0.7318 ms at 80°C. To obtain the average clock offset at different temperatures, we put nodes A, B, and C in the thermostatic test chamber at different temperatures, and node D was put outside the test chamber as the receiver end. The range of temperatures was set from 0°C to 80°C, and the messages were measured every 5° increase in temperature. Figures 14(e) and 14(f) plot the fingerprints and the error bar of the average offset under different message periods. The result shows that the temperature-varied clock fingerprint will not be affected by message periods, and different ECU can be distinguished in the CAN bus prototype.

7.2.2. Real Vehicle. A real vehicle (Toyota Vios 2017) was also used to validate TVF. The temperature-varied clock fingerprint can be constructed by the CAN traffic data which were logged by our CAN prototype. Because the temperature of ECUs in the engine cabin will gradually increase after the car starts, we logged the traffic data at different temperatures, and the TVF of ECUs on a real vehicle could be constructed. The data were logged in the static state of the vehicle at an ambient temperature of 5°C and 15°C, respectively. Since the temperature was stable at about 5°C when collecting the initial data, we can distinguish whether the message is from the same ECU by using the clock-based fingerprint method [10]. Then, we found messages 0×24F, 0×2C1, and 0×163 were transmitted from three ECUs, respectively. The TVF of ECUs on a real vehicle is shown in Figure 14(d). The results show that the temperature clock fingerprint can be used in real vehicles.

7.3. The Detection of Masquerade Attack. To estimate the detection capability of TVF against the masquerade attack, we first implemented the attack on the CAN bus prototype, and then we detected it with the proposed method.

We mounted a masquerade attack on the CAN bus prototype. On the CAN bus prototype, node A was programmed to send 0×11, B was programmed to send the target message 0×33 and 0×55, and C was programmed to send 0×68. Now, we set note A to mount the masquerade attack on B; then, note A was compromised to send 0×33 and 0×11 and B was compromised to stop sending the message 0×33. To keep the instant total numbers of messages on the CAN bus constant, we let A continue sending messages 0×11. Figure 15(a) shows the masquerade attack that is mounted by A on B at 20°C. The clock offset of the 0×33 suddenly increased by about 30 μs when the masquerade attack was mounted at 75 s.

We then detected the masquerade attack on the CAN bus by the proposed method. Node D was programmed to run the proposed TVF. We set the masquerade attack that was mounted by A at 10°C, 40°C, and 60°C, respectively. As shown in Figure 15(b), the orange and the blue line are the fingerprint of A and B. The red circles are the clock offsets of attack messages that were mounted by A at three temperatures, and the values were 0.6940 μs, 0.7103 μs, and 0.7266 μs, respectively. Nevertheless, the empirical temperature of B was 20°C and the average clock offset of the normal message of B was 0.6748 μs. It can be clearly seen that the normal average clock offset is significantly lower than that of the attack messages, and then the masquerade attacks at three temperatures were surely detected by TVF.

7.4. The Identification of Source ECU. We estimated the feasibility of the intrusion source identification of TVF on a CAN bus prototype. We detected the masquerade attack in the intrusion detection phase, yet we still did not recognize which was the attacker ECU that launched the intrusion. Considering that note A and note C were compromised by the adversary. Note C was programmed to mount a masquerade attack on A, and the empirical temperatures of A, B, and C were 20°C, 40°C, and 30°C, respectively. As the clock offset of C at 30°C was higher than that of A at 20°C, the masquerade attack which was mounted by C was easily detected by TVF. Moreover, the attack source note C could also be identified by analyzing the possible temperature and empirical temperature of C. As shown in Figure 15(c), the red circle indicates the average clock offset of the intrusion message (send by C), and the value of it is about 0.71 ms. The orange circle on the fingerprint corresponds to the possible attack temperature. From the figure, the average clock offset of intrusion message exceeds the fingerprint of B so that B can be excluded from the source of intrusion first. The nodes that can mount the attack were A and C, and their possible attack temperatures were 30°C and 40°C, respectively. The empirical temperature of A was 20°C, so it cannot send the attack message. The empirical temperature of C was 30°C and the temperature of the attack was close to 30°C. So, it can be determined that C was the source of the attack.

7.5. Computational Time. We evaluated the computational time required of the proposed TVF. TVF consists of three phases. We only evaluated the computational time required for the intrusion detection phase, which was mainly implemented on the ECU, and intrusion detection is the main phase that affects the computational overhead compared to other phases. The fingerprint construction phase was analyzed using the MATLAB codes, which were conducted on an Intel i5 3.4 GHz dual-core processor with 8 GB

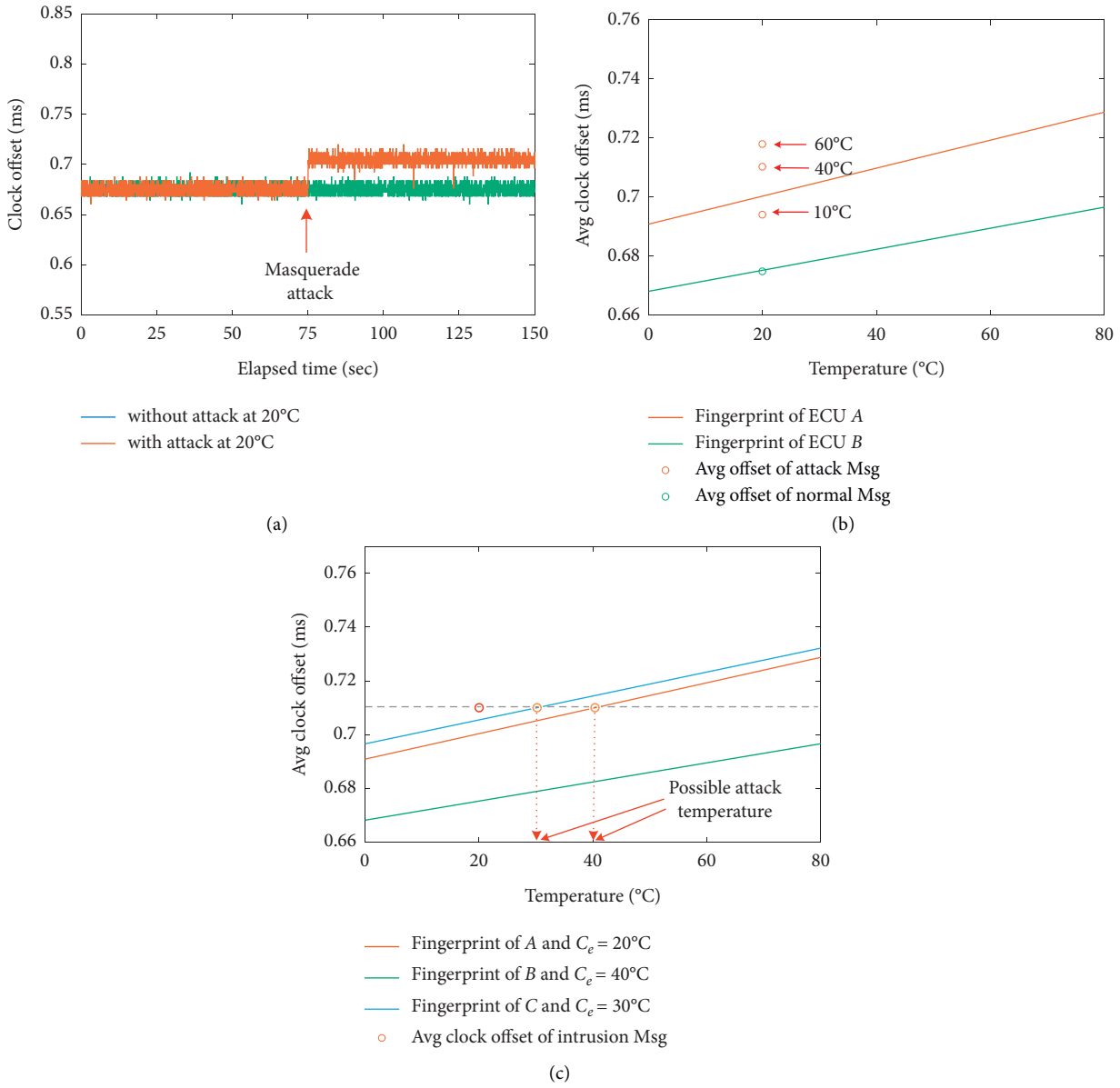

Figure 15: Intrusion detection and identification. (a) Masquerade attack at 20°C. (b) The fingerprint and the average offset of attack message. (c) The recognition of source ECU.

of RAM. Moreover, the intrusion detection phase and source identification phase were programmed on the CAN prototype by C. In the CAN prototype, TVF only detected the messages sent by the three ECUs, and its program's global variables use 32% of dynamic memory. Table 1 shows the computational time for TVF to conduct one correct detection of intrusion under different message periods. The computational time is largely dependent on the period of messages according to the value of m in Algorithm 2.

In addition, the Arduino-based ECU seems insufficient to analyze all CAN messages in real-time for detection, due to the large CAN traffic with high frequency and limited computing capability of the ECU. However, we can handle this problem by deploying TVF to devices with a strong computing capability, such as adding a Raspberry Pi to run the proposed solution. We will try to implement TVF on this kind of devices with high computing capability in future work.

Table 1: The computational time for intrusion detection.

Msg periods (ms)	The required time (s)
30	0.3045
50	0.5048
70	0.7052

7.6. Performance. We illustrated the detection rate and false alarm rate of TVF and compared it with state-of-the-art IDS, and we also examined the performance of advanced TVF on the advanced masquerade attack.

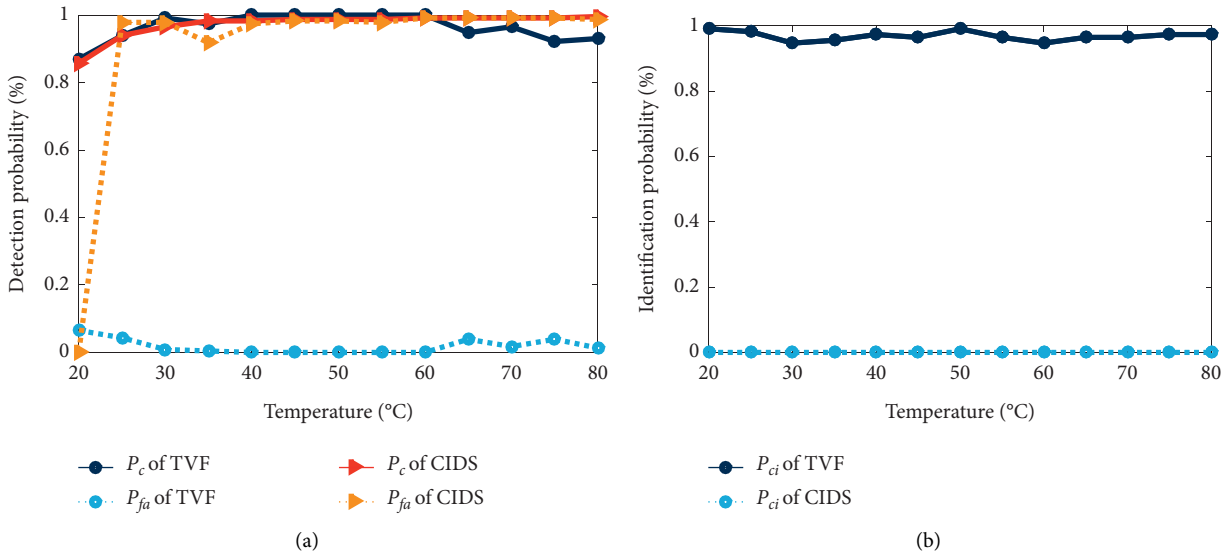

Figure 16: Detection rate and false alarm rate. (a) Detection rate and false alarm rate of TVF and CIDS under different temperatures. (b) Identification rate of TVF and CIDS under different temperatures.

We used two performance metrics of P_c and P_{fa} to evaluate the proposed method. The metric P_c is the probability of correctly detect the attack. The metric P_{fa} is a false alarm, which means a normal CAN message is identified as an attack one. An excellent in-vehicle network IDS may have a high P_c and a low P_{fa}. In a vehicle, a high P_c may help the driver quickly identify the existence of the attack and take action accordingly. Meanwhile, the low P_{fa} reduces the driver's distraction and thus ensure driving safety.

We demonstrated the detection rate P_c and false alarm rate P_{fa} of TVF and compared the proposed detection method with CIDS. Considering the scenario, node A mounted a masquerade attack on node C. We first built the fingerprints of A, B, and C with CIDS at 10°C. We chose a certain temperature to build the fingerprints because CIDS did not consider the temperature in their solutions. At the same time, we built the fingerprints by the TVF at a temperature of range from 0°C to 80°C, as shown in Figure 14(b). Then, we examined TVF and CIDS with messages which were sent at different temperatures, e.g., 20°C, 55°C, and 80°C. The results of TVF and CIDS are shown in Figure 16(a). The detection rate P_c of CIDS at 20°C is close to 0% because the clock offset of A at 20°C is the same with C at 10°C. Although the detection rate P_c of CIDS rises to about 98% after 25°C, the false alarm rate P_{fa} is up to as high as 98% because CIDS considers its legitimate high-temperature clock offsets as attacks. The detection rate of TVF is stable at about 96.4%, and the false alarm rate is below 1.8%. At the same time, the proposed method also can identify the source of the intrusion message, and the result is shown in Figure 16(b). The correct identification rate P_{ci} of the proposed method is 97.2%, and the P_{ci} of CIDS is about 0%. When the temperature is at 20°C, the clock offset of A is equal with C, so the masquerade attacks mount by A is identified sending from C; then, the P_{ci} is 0%. Then, with the temperature increase, the accumulated clock offset does not match any of the fingerprints of CIDS, so the P_{ci} is 0%. Accordingly, the proposed method can detect the masquerade attack at various temperatures with a stable rate. Moreover, the proposed method could identify the source of the intrusion message accurately.

We also evaluated the advanced TVF against the advanced masquerade attack. A more serious situation, which the above two solutions did not consider, is that the adversaries used the same clock offset as the target ECU to launch the masquerade attack. In other words, the adversaries launch an advanced masquerade attack that the TVF and CIDS can not detect and identify. For the advanced attack, advanced TVF has an average detection rate of 85% and a source identification rate of 80%, while the previous version of TVF and CIDS are both about 0%. On the whole, the advanced proposed method is a significant supplement that can detect the advanced masquerade attack.

8. Conclusion

Existing ECU physical-based fingerprinting methods are susceptible to the impacts of temperature, which could result in the failure of detection and identification based on our multiply empirical studies. To counter this situation, we proposed TVF, a temperature-varied fingerprint, which exploits the fact that the clock offset of the ECU change linearly with the temperature for intrusion detection and source ECU identification. Based on this, an advanced version of TVF is made for further supplemented and expanded, which can counter more serious intrusion cases. As far as we know, we are the first to introduce temperature as a vector to build the fingerprint and achieved excellent results on the detection and identification of intrusions. The proposed method has been verified on a CAN bus prototype and a real vehicle, and the results show that it can accurately detect the intrusion messages and identify the source ECU in

the in-vehicle network. Therefore, we believe that the proposed method can effectively enhance the security and safety of the vehicle.

Data Availability

The data were collected from the CAN bus prototype with the Arduino, which have mentioned in the paper. Moreover, the real vehicle data were collected from the OBD port with a DB9 to OBD2 Cable. Later, we will put the data on the Internet.

Conflicts of Interest

The authors declare that they have no conflicts of interest .

Acknowledgments

The work was partly supported by the China Postdoctoral Science Foundation (Grant no. 2019M652475) and Fundamental Research Funds for the Central Universities (Grant no. 201813021).

References

[1] C. Miller and C. Valasek, "Adventures in automotive networks and control units," in *Proceedings of the Defcon*, vol. 21, pp. 260–264, Las Vegas, NV, USA, 2013.

[2] S. Nie, L. Liu, and Y. Du, "Free-fall: hacking tesla from wireless to can CAN bus," in *Proceedings of the Black Hat USA*, pp. 1–16, Las Vegas, NV, USA, 2017.

[3] A. Greenberg, "Hackers remotely kill a jeep on the highway-with me in it," *Wired*, vol. 7, p. 21, 2015.

[4] M. D. Pese, T. Stacer, C. A. Campos, E. Newberry, D. Chen, and K. G. Shin, "Librecan: automated can message translator," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2283–2300, London, UK, November 2019.

[5] M. Muter and N. Asaj, "Entropy-based anomaly detection for in-vehicle networks," in *Proceedings of the Intelligent Vehicles Symposium (IV)*, pp. 1110–1115, IEEE, Dearborn, MI, USA, June 2011.

[6] M. Muter, A. Groll, and F. C. Freiling, "A structured approach to¨ anomaly detection for in-vehicle networks," in *Proceedings of the 2010 Sixth International Conference on Information Assurance and Security (IAS)*, pp. 92–98, Atlanta, GA, USA, November 2010.

[7] E. Seo, H. M. Song, and H. K. Kim, "Gids: Gan based intrusion detection system for in-vehicle network," in *Proceedings of the 2018 16th Annual Conference on Privacy, Security and Trust (PST)*, Belfast, Ireland, August 2018.

[8] M. J. Kang and J. W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PLoS One*, vol. 11, no. 6, Article ID e0155781, 2016.

[9] B. Groza and P.-S. Murvay, "Efficient intrusion detection with bloom filtering in controller area networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 1037–1051, 2018.

[10] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *Proceedings of the USENIX Security Symposium*, pp. 911–927, Austin, TX, USA, August 2016.

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

[12] K.-T. Cho and K. G. Shin, "Viden: attacker identification on in-vehicle networks," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1109–1123, Dallas, TX USA, October 2017.

[13] S. U. Sagong, X. Ying, A. Clark, L. Bushnell, and R. Poovendran, "Cloaking the clock: emulating clock skew in controller area networks," in *Proceedings of the 9th ACM/IEEE International Conference on Cyber-Physical Systems*, pp. 32–42, Porto, Portugal, April 2018.

[14] M. Kneib and C. Huth, "On the fingerprinting of electronic control units using physical characteristics in controller area networks," *Informatik*, vol. 2017, 2017.

[15] 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 Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2114–2129, 2018.

[16] M. Kneib and C. Huth, "Scission: signal characteristic-based sender identification and intrusion detection in automotive networks," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 787–800, Toronto, ON, Canada, October 2018.

[17] M. Tian, R. Jiang, C. Xing, H. Qu, Q. Lu, and X. Zhou, "Exploiting temperature-varied ecu fingerprints for source identification in in-vehicle network intrusion detection," in *Proceedings of the 2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC)*, pp. 1–8, London, UK, 2019.

[18] U. E. Larson and D. K. Nilsson, "Securing vehicles against cyber attacks," in *Proceedings of the 4th Annual Workshop on Cyber security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead*, New York, NY, USA, 2008.

[19] H. M. Song, H. R. Kim, and H. K. Kim, "Intrusion detection system based on the analysis of time intervals of can messages for in-vehicle network," in *Proceedings of the 2016 International Conference on Information Networking (ICOIN)*, pp. 63–68, Kota Kinabalu, Malaysia, 2016.

[20] G. Brindusescu, "Darpa hacked a chevy impala through its onstar system," 2015, https://www.autoevolution.com/news/%20darpa-hacked-a-chevy-impala-through-its-onstar-system-video-92194.html.

[21] S. Checkoway, D. Mccoy, D. Anderson, B. Kantor, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *Proceedings of the USENIX Security Symposium*, San Francisco, CA, USA, August 2011.

[22] R. Currie, "Hacking the can Bus: Basic Manipulation of a Modern Automobile through CAN Bus Reverse Engineering," SANS Institute InfoSec Reading Room, Bethesda, MA, USA, 2017.

[23] J. Pagliery, "Tesla car doors can be hacked," 2014, https://money.cnn.com/2014/03/31/technology/security/tesla-hack/.

[24] M. Marchetti and D. Stabili, "Read: reverse engineering of automotive data frames," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 1083–1097, 2019.

[25] M. Gmiden, M. H. Gmiden, and H. Trabelsi, "An intrusion detection method for securing in-vehicle can bus," in *Proceedings of the 2016 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, pp. 176–180, Sousse, Tunisia, December 2016.

[26] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive can networks–practical examples and selected

short-term countermeasures," in *Proceedings of the International Conference on Computer Safety, Reliability, and Security*, pp. 235–248, Newcastle, UK, September 2008.

[27] W. Choi, H. J. Jo, S. Woo, J. Y. Chun, J. Park, and D. H. Lee, "Identifying ecus using inimitable characteristics of signals in controller area networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 4757–4770, 2018.

[28] K.-T. Cho and K. G. Shin, "Error handling of in-vehicle networks makes them vulnerable," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1044–1055, Vienna, Austria, October 2016.

[29] R. B. GmbH, "Can specification version 2.0," Tech. Rep. 300240, Rober Bousch GmbH (Postfach), Gerlingen, Germany, p. 72, 1991, 1991.

[30] I. Foster and K. Koscher, "Exploring controller area networks," *USENIX Association*, vol. 40, no. 6, 2015.

[31] R. M. IshtiaqRoufaH. Mustafaa et al., "Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study," in *Proceedings of the 19th USENIX Security Symposium*, pp. 11–13, Washington, DC, USA, 2010.

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

[33] V. Paxson, "On calibrating measurements of packet transit times," *ACM SIGMETRICS Performance Evaluation Review*, vol. 26, no. 1, pp. 11–21, 1998.

[34] J. Daily, "Analysis of critical speed yaw scuffs using spiral curves," *SAE Technical Papers*, vol. 1, 2012.

[35] R. Ruth, W. Bartlett, and J. Daily, "Accuracy of event data in the 2010 and 2011 Toyota Camry during steady state and braking conditions," *SAE International Journal of Passenger Cars-Electronic and Electrical Systems*, vol. 5, no. 1, pp. 358–372, 2012.

[36] S. Zander and S. J. Murdoch, "An improved clock-skew measurement technique for revealing hidden services," in *Proceedings of the USENIX Security Symposium*, pp. 211–226, San Jose, CA, USA, 2008.

[37] S. Mohalik, A. C. Rajeev, M. G. Dixit, S. Ramesh, and S. Jiang, "Model checking based analysis of end-to-end latency in embedded, real-time systems with clock drifts," in *Proceedings of the 2008 45th ACM/IEEE Design Automation Conference*, Anaheim, CA, USA, June 2008.

[38] Arduino Uno Rev3., https://store.arduino.cc/usa/arduino-uno-rev3.

[39] CAN-BUS Shield V2., https://www.seeedstudio.com/CAN-BUS-ShieldV2-p-2921.html.

[40] On-Board Diagnostic System, http://www.obdii.com/.