Aiden: Association-Learning-Based Attack Identification on the Edge of V2X Communication Networks

Yuanfang Chen, *Member, IEEE*, Muhammad Alam, *Senior Member, IEEE*, Shahid Mumtaz, *Senior Member, IEEE*

***Abstract*—In vehicle security, attack identification has been proposed to identify the compromised electronic control units (ECUs) of a vehicle. Fingerprinting methods using a variety of features have been widely applied to identify attacks. However, these methods only consider the features of an individual ECU, and ignore the logical association among different ECUs. This condition leads to high requirements in terms of feature measurements, and a great deal of useful information is lost to achieve identification. In this paper, an association-learning-based model, designated Aiden, is proposed to identify the compromised ECUs on the edge of V2X communication networks and without feature measurements. Experiments on a real vehicle show the effectiveness of the proposed model.**

***Index Terms*—Association Learning, Attack Identification, Automotive Security, Edge Intelligence, V2X Communication Networks.**

I. Introduction

In modern vehicles, the adoption of sensors and electronic control units (ECUs) brings intelligence and convenience to driving and makes autonomous driving possible [1]–[3]. However, successful attacks targeting these modern vehicles via intelligent electronics have been demonstrated [4]–[7]. These attacks inject attack messages into a vehicle through wireless channels, and enter into the controller area network (CAN) bus of the vehicle. This way, an attacker can control the vehicle and cause deviations from a safe operational regime (as shown in Fig. 1). As a typical example, Miller *et al.* [8] showed an attack in which the multimedia system, power system, and braking system of a vehicle could be controlled without requiring any physical access. This led to the recall of millions of vehicles.

No matter how accurately an attack can be detected in a vehicle, if one cannot know which ECU is mounting the attack and, hence, which one must be isolated/patched, the vehicle remains insecure and unsafe. Attack identification has been proposed to determine which ECUs are actually mounting attacks. Moreover, it is much more economical to isolate/patch the compromised ECUs than to blindly consider all the ECUs as compromised. Kyong-Tak Cho *et al.* proposed a clock-based intrusion detection system (CIDS) [9] to identify which ECU mounted an attack. The CIDS exploits the intervals of in-vehicle messages to estimate the clock skews of ECUs, and the estimated clock skews are used to fingerprint the ECUs. Based on the fingerprints of ECUs, the CIDS constructs a model of ECU clock behaviors using the recursive least-squares (RLS) algorithm. The fingerprinting capability of the CIDS enables the identification of the compromised ECU. However, if attack messages are injected aperiodically, the CIDS cannot be used in attack identification. This is called the periodic dependence problem. Viden (Voltage-based attacker identification) was designed to avoid the problem of periodic dependence [10]. It fingerprints ECUs on the CAN bus via voltage measurements, allowing Viden to identify the compromised ECU irrespective of how and when an attacker injects its messages. In more recent work, Kneib *et al.* [11] designed a system to identify the ECUs sending particular CAN frames by using the fingerprints extracted from the CAN frames. The proposed system uses the physical characteristics of CAN frames to assess whether the frames are sent by legitimate ECUs. To improve this system, Liu *et al.* [12] proposed a local–outlier–factor-based method to distinguish voltage waveforms, fingerprint ECUs, and further identify the compromised ECUs.

However, these previous methods need complex and ac-

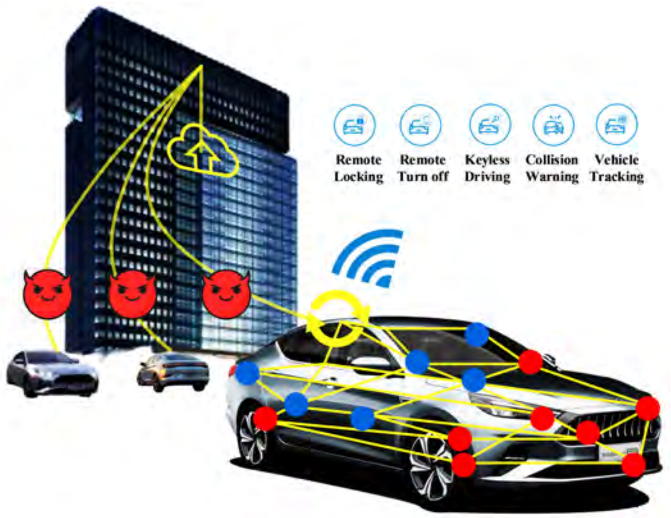


Fig. 1. An attack enters into the CAN bus of a modern/autonomous vehicle through wireless channels, and the in-vehicle ECUs connected by the CAN bus are compromised. Because of the intrinsic associations among different ECUs to take actions, the attack from the compromised ECUs easily causes cascading failure to make the vehicle deviate from a safe operational regime.

Yuanfang Chen is with School of Cyberspace, Hangzhou Dianzi University, Muhammad Alam is with School of Engineering, London South Bank University, and Shahid Mumtaz is with Instituto de Telecomunicações, Universidade de Aveiro.

Manuscript received xxxx xx, 2021; revised xxxx xx, 2022. Corresponding author: Yuanfang Chen (email: yuanfang.chen.tina@gmail.com).

curate measurements; that is, they have high requirements in terms of feature measurements. Moreover, they are centralized, which means that there is a third-party data center to which vehicle users are required to upload their private data. This means that these methods completely rely on the computational resources of the data center to process data, but fail to efficiently utilize the resources in vehicles. To conquer the challenges that exist in the above methods, an association-mining model, designated Aiden, is proposed to identify the compromised ECUs directly on the edge of V2X communication networks[1].

Aiden learns the association of different ECUs and infers the logical relationship among these ECUs. On this inference basis, if any illogical relationship exists during a driving action, Aiden then considers that an attack has occurred and can identify which ECU is compromised.

The contributions of this paper are as follows.

1) Model Design. Aiden is designed to avoid high requirements in feature measurements, such as the avoidance of the periodic dependence problem and the need for complex and accurate voltage measurements. It only analyzes the intrinsic logical association of different ECUs when an operation is performed during driving. It exploits the logical association to identify the compromised ECUs and does not need to consider whether the message sending is periodic or aperiodic.
2) Model Implementation. Aiden is implemented as a part of OBD-II to act as an edge device to achieve edge intelligence. It is deployed to the edge of V2X communication networks to obtain improvements of real-time communication and privacy [14]. Moreover, it does not require additional special equipment to support its deployment, so it is cost effective and easily accepted by users as well as easily deployed to vehicles.
3) Model Evaluation. Aiden is evaluated on the CAN bus prototype and on a real vehicle.

The rest of this paper is organized as follows. In section II, the background of this paper is provided, and, in section III, related work is reviewed. In section IV, the problem studied in this paper is detailed, while the design of the Aiden model is evaluated in section V on a CAN bus prototype system. Further discussion of Aiden is given in section VI, including its limitations. The paper is concluded in section VII.

II. Background

In a vehicle, ECUs broadcast their retrieved sensor data via messages on the CAN bus, and the data are recorded by the vehicle's event data recorder (EDR). The EDR is a device installed in a vehicle to record the information related to the vehicle driving. In addition, the message used to carry the data contains a unique identifier (ID) that represents the function of the message. For example, the ID of a message from a 2011 Toyota Camry is 398 (Hex); according to the ID number, by the parse file available from the manufacturer, one can parse that this message comes from the "Fuel" functional area of the vehicle. Different vehicles have different numbering standards for the messages from different ECUs, and the quantity and type of ECUs are also different for different types of vehicles. In this study, the data from a 2011 Toyota Camry [15] is used, and the relationship between IDs and corresponding ECUs is listed in Table I.

Table I shows that there are multiple ECUs in the same functional area, and the messages from these ECUs have the same ID. For example, there are four ECUs for the function that controls wheel speed. Two of these ECUs are used to control the speed of the two front wheels (message ID is OB0), while the other two are used to control the speed of the two rear wheels (message ID is OB2). Therefore, the ID of messages used to facilitate the communications among ECUs cannot be used to uniquely identify a particular ECU.

However, it is important to identify the compromised ECUs in a vehicle, as the identification is the foundation of precisely defending against security threats in V2X communication networks. Such networks are proposed and aim to achieve intelligence and even automatic driving of vehicles. The vehicles in the V2X communication ecosystem are equipped with different sensors to collect different types of data [16], as well as ECUs to control different on-board equipment; moreover, these different ECUs can communicate with each other. On this basis, all of the vehicle equipment is connected and further linked with external information networks. Therefore, security threats extend from information networks to in-vehicle networks, and security becomes important, as any system failure of a vehicle directly affects driving safety.

III. Related Work

Fingerprinting ECUs has been attempted for attack identification. In existing methods, there are two types of ways to fingerprint ECUs: message timing and voltage measurements.

Message Timing. In [9], the CIDS was proposed to detect attacks by fingerprinting the ECUs on the CAN bus. The CIDS extracts the ECUs' clock skews from message arrival times. Clock skew (also called timing skew) is a phenomenon for a signal transmitter and can be represented as the slope of the accumulated clock offset[2]. Owing to the use of accumulated clock offsets as the fingerprints of ECUs, only when attack messages are injected periodically can the CIDS be used for attack identification. In other words, if a compromised ECU injects messages aperiodically, the CIDS cannot identify it. In a real scenario, some ECUs' message sending is aperiodic. Instead of fingerprinting ECUs with message timings, some researchers have proposed the use of voltage measurements, which avoids the constraint on the periodicity of message injection.

Voltage Measurements. In [17], the mean-square error (MSE) of voltage measurements was used as the ECU fingerprint. However, this scheme was shown to be valid only for the

[1] V2X (vehicle-to-everything) is communication between a vehicle and any entity that may affect or may be affected by the vehicle. It is a vehicular communication system that incorporates other specific types of communication as V2I (vehicle-to-infrastructure), V2N (vehicle-to-network), V2V (vehicle-to-vehicle), V2P (vehicle-to-pedestrian), and V2D (vehicle-to-device) [13].

[2] The accumulated clock offset is the sum of the absolute values of average clock offsets for every N received messages. Moreover, the clock offset is the difference in the time reported by the clock C_i and the clock C_{i+1}.

TABLE I
RELATIONSHIP BETWEEN DATA FRAMES AND ECUS

ECU	CAN ID (Decimalism)	CAN ID (Hex)	Periodicity (ms)	Data Length (bytes)
Vehicle speed	1552	610	500	8
Odometer	1553	611	1000	8
Engine speed	708	2C4	30	8
Fuel	920	398	Aperiodic	2
Throttle pedal	705	2C1	30	8
Brake pedal	548	224	30	8
Throttle	947	3B3	500	3
PRND (Gearbox)	948	3B4	1000	8
WSPD1: Wheel speed (front right)	176	0B0	10	6
WSPD2: Wheel speed (front left)	176	0B0	10	6
WSPD3: Wheel speed (rear right)	178	0B2	10	6
WSPD4: Wheel speed (rear left)	178	0B2	10	6
Steering Angle	37	025	10	8
Aircon	896	380	1000	8

voltages that were measured during the transmission of CAN messages and on a low-speed (10-kbps) CAN bus. Modern vehicles, however, usually operate on a 500-kbps CAN bus. To overcome these challenges, researchers have proposed to further extract the features of the time and frequency domains of voltage measurements and use them as inputs for classification ([18]). This way, successful fingerprinting ECUs on high-speed CAN buses is facilitated. However, this type of method requires not only a high sampling rate (2.5 Gsamples/s) but also the use of an extended CAN frame. Moreover, because the modeling process uses batch learning, unpredictable changes occur in the CAN bus (e.g., battery-consumption level). In [10], Viden was proposed, which fingerprints ECUs through a different way of using voltage measurements. Viden has no restrictions on the type of CAN messages or the speed of CAN buses to be used. However, voltage-measurement-based methods require many complicated measurements and a substantial amount of processing.

IV. AIDEN

To avoid the abovementioned problems in the existing methods, this paper proposes Aiden, which learns the association of different ECUs in a vehicle to deduce the compromised ECUs.

A. Problem Formulation

Attack identification is used to identify compromised ECUs in vehicle security. In this section, the attack identification issue is formulated and described.

If there is a tree that can be used to visually show the paths of message transmission among ECUs, for an attacker, the optimal policy for compromising ECUs on the vehicle's CAN bus is to keep as many legitimate ECUs (victims) as possible inside the subtrees of the compromised ECUs. Meanwhile, the attacker does not desire the compromised ECUs to be easily detected and identified by any defense strategy.

First, the overall gain of attacks from an attacker is formulated: $G_{attack} = (1 - P_{detect})\frac{number\ of\ victims}{number\ of\ total\ nodes}$, where P_{detect} denotes the possibility that attacks are detected. Then, to maximize the gain, the attacker's goal becomes to find an optimal tree level (h) for the compromised ECUs and try to put them in the message transmission tree as sparsely as possible. Thus, the solution of this optimization problem is that all the compromised ECUs are at the same optimal height (h), and there is no compromised ECU that is placed within the subtree of another. Otherwise, the number of victim ECUs will be reduced without increasing the overall gain (G_{attack}). In the rest of this paper, the optimal policy of an attacker is always considered the worst case so as to guarantee a lower bound for the effectiveness of any defense scheme.

In this study, an attack in a dynamic environment is identified, and in this dynamic environment ECUs have different running times; an aging factor $0 < \beta \leq 1$ is used to reflect such life cycles; that is, $p_f^{(r)}[i] = \beta^{(r)} \cdot (1 - (1 - p_f^{r-1}[i]) \cdot (1 - f(i)))$ ($\beta^{(0)} = 1, \beta^{(r)} = 0.5\beta^{(r-1)}$, and $p_f^{(0)}[i] = 0$), where $p_f^{(r)}[i]$ denotes the probability of the suspicious level on the compromise of ECU i during the r^{th} round, and $f(i)$ is the suspicion level that the ECU i has been compromised. For example, if $p_f[i] = 1$, it is considered that ECU i is compromised. Moreover, this equation guarantees that a legitimate ECU that is occasionally suspected of being compromised will not be eventually identified as an illegal one.

B. System and Attack Models

In the proposed system model, the vehicle's CAN bus is considered to have been equipped with an identification system by which to detect attacks and identify compromised ECUs. This system model consists of two parts: adversaries and compromised ECUs. The adversaries attack the in-vehicle ECUs that work on the CAN bus protocol. For example, an adversary controls the on/off operation of ECUs and injects attack messages through the compromised ECUs. The compromised devices cause serious damage to the target that the adversary intends to attack, such as the brake system of an autonomous vehicle. The proposed system complements the attack detection system via attack identification.

For the proposed attack model, because an unauthorized ECU cannot join in-vehicle networks without a valid credential, only the authorized internal ECUs are considered [19]. It is assumed that a compromised ECU controlled by an attacker launches an attack on the other ECUs in its subtree. Moreover, it is further assumed that an intelligent attacker knows defense strategies and the tree topology of message transmission, and can place the compromised ECUs into the positions of its choice.

Fingerprinting-based identification methods can only handle the attacks that cause a change of an ECU. The improvement achieved in the proposed method can not only process the attacks causing the change of an ECU but also process the attacks causing the change of the logical association among related ECUs.

C. Aiden

Aiden is used to overcome the challenges of fingerprinting-based methods, namely that they need complex and accurate measurements and have high requirements in feature measurements. Moreover, Aiden has edge-computing ability. Unlike the high requirements in feature measurements of fingerprinting-based methods, Aiden does not use any feature to fingerprint ECUs. It learns the association of different ECUs and infers the logical relationship among these ECUs. Regarding its edge computing ability, Aiden federates edge devices, such as in-vehicle devices connected with OBD-II, to conduct distributed data processing, and coordinates the learning behaviors of these edge devices. Eventually, Aiden achieves attack identification on the edge of V2X networks [20].

Aiden includes the following three steps.

Step 1: Data Pre-processing. Two kinds of states for all ECUs are marked by state flags in the dataset, that is, rise and decline, and each state record is a state change [3]. The final pre-processed dataset is made up of these elements: ECU IDs, state flags of ECUs, and time stamps. Take, for example, the following records: 223U: 1, 0.09998; 223D: 2, 0.11956; 0B0U: 3, 0.12996; 0B0D: 4, 0.15902; 0B0U: 3, 0.19057, where 223 and 0B0 are ECU IDs, U/D denotes the rising/falling state, and these states are numbered 1,2,3 ... If the same ECU appears in the same state, the state number is the same (e.g., they are two records at different times: 0B0U: 3, 0.12996, and 0B0U: 3, 0.19057, but they have the same state number, that is, 3). Moreover, in this example, 0.09998,0.11956,... are time stamps, and the time stamp is recorded as the offset from the start time in seconds.

Step 2: Sequence Extraction. The pre-processed dataset without attacks is denoted A. During each ECU state change, the full permutation is performed for the normal behavior data in the dataset A, and the occurrence number of each permutation is counted, according to the support degree[4]. Then, permutations with occurrence numbers less than the support degree are removed. The remaining permutations are the pattern sequences that are desirable to obtain.

Step 3: Attack Identification. Data traversal is performed on all of the pre-processed data that accompany attacks, and the data are pre-processed in the data pre-processing step. During any ECU state change, in the pattern sequences extracted from normal behavior data, whether other ECU state changes that are related to it are consistent to the pattern sequences is checked. If there is no consistent sequence, the corresponding ECU is marked as having been compromised.

In each time slot of length T_{slot}, Aiden can be trained to achieve a desirable performance, by running an iteration of following phases:

Phase 1: An edge-computing center receives and distributes the pattern sequences extracted from the normal behavior data of each vehicle.

Phase 2: Each vehicle updates its local pattern sequences with a referral to the distributed pattern sequences from the edge-computing center.

In this iteration, each vehicle transmits its updated pattern sequences to the edge-computing center, which aggregates its received pattern sequences to improve the performance of the Aiden model.

V. Prototype System and Evaluation

A. Prototype System and Evaluation Setups

The prototype system designed to evaluate Aiden is shown in Fig. 2, and the evaluation was deployed under four attack scenarios, which are shown in Figs. 4 ~ 7.

In the prototype system, the edge-computing center illustrated in Fig. 3 is used to gather driving data and inject attacks by

[3] A state change is the point of the state change from the rising (falling) state to the falling (rising) state.

[4] The support degree which is described in the sequence extraction step is a specific number of occurrences. Its calculation is as follows: first, count the number of occurrences of each ECU in the dataset A, and then arrange them in ascending order, de-duplicate them, and remove zeros, $C = a_0, a_1, ..., a_i$ (i =the number of elements in the dataset C). The support degree is set to a_j, and $j = 0.05 * i$. The reason one sets the value of the support degree is to compare the following values: $j = 0.05 * i, j = 0.1 * i, j = 0.2 * i$, and $j = 0.5 * i$. The accuracy of attack identification for these values is 0.9308, 0.9270, 0.9256, and 0.9256, respectively. According to the comparison result, the accuracy is the highest when $j = 0 and 05 * i$.

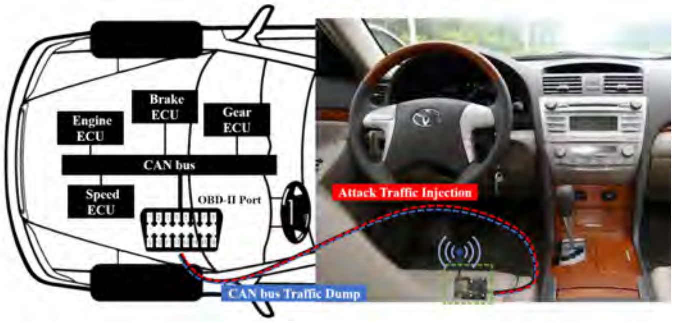
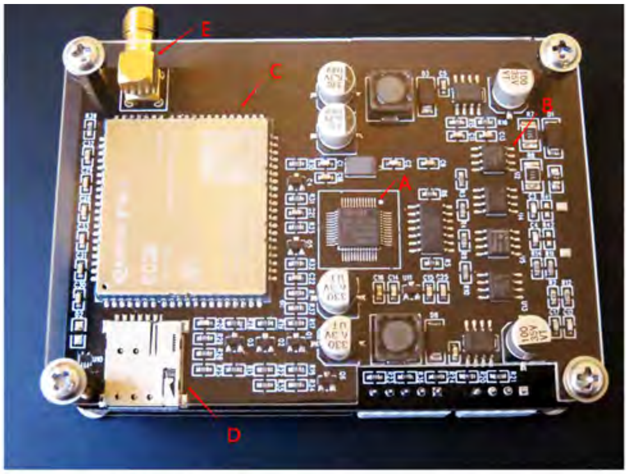


Fig. 2. Components of prototype system designed to evaluate Aiden. The system can inject attacks through the OBD-II interface. The injection process can be done in either of two communication modes: wired or wireless.

the wired/wireless communication mode. Moreover, the center is responsible for implementing edge computing to distribute the pattern sequences to multiple vehicles and achieve the training of the proposed model Aiden.



A. MCU,model STM32F103CBT6,is the main control chip.
B. OBD module, includes two sets of CAN line transceivers (CAN High and CAN Low),one set of K line transceivers, and one set of L line transceivers.
C. EC20 module, is used for 4G communication.
D. NANO(U)SIM card slot,is used to insert SIM card.
E. LTE 4G antenna interface.

Fig. 3. Edge-computing center used to realize edge computing so as to achieve distributed model training.

Based on the abovementioned prototype system, an evaluation was conducted under the four attack scenarios of diagnosis attack, fuzzy attack, replay attack, and spoofing attack, as these attacks can immediately and severely impair in-vehicle functions or cause extensive vehicle damage. Detailed descriptions of the proposed attack scenarios follow.

1) **Diagnosis attack**. The automobile diagnosis instrument is a vehicle fault-detection terminal. During the diagnosis process, it sends diagnosis frames to the vehicle CAN bus, and vehicle ECUs execute instructions after receiving the diagnosis frames. In this study, a custom-designed development board is used to send diagnosis frames to a vehicle to achieve attack operations. This is called a diagnosis attack. An example is shown in Fig. 4.

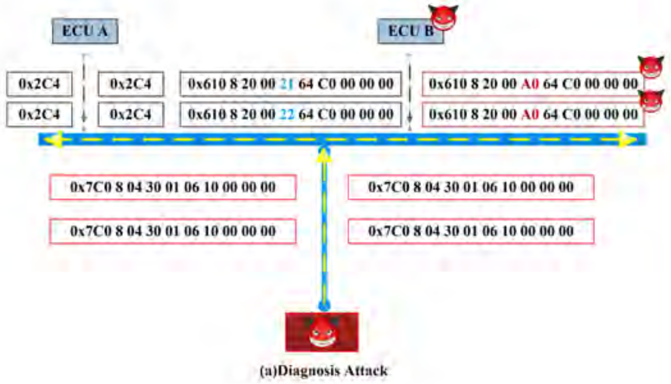

ECU A
ECU B
0x2C4
0x2C4
0x2C4
0x2C4
0x610 8 20 00 21 64 C0 00 00 00
0x610 8 20 00 22 64 C0 00 00 00
0x610 8 20 00 A0 64 C0 00 00 00
0x610 8 20 00 A0 64 C0 00 00 00
0x7C0 8 04 30 01 06 10 00 00 00
0x7C0 8 04 30 01 06 10 00 00 00
0x7C0 8 04 30 01 06 10 00 00 00
0x7C0 8 04 30 01 06 10 00 00 00
(a)Diagnosis Attack

Fig. 4. Example of a diagnosis attack in the proposed prototype system.

In this example (Fig. 4), experiments were conducted on the aforementioned 2011 Toyota Camry at 33 and $34 km/h$ driving speeds, and the diagnosis attack was carried out with a diagnosis frame ($7C0$ 8 04 30 01 06 10 00 00 00) to change the speed shown on the dashboard to $160 km/h$. This type of attack greatly interferes with the driver to understand the current vehicle driving speed.

2) **Fuzzy attack**. Fuzzing is a software-testing technique that inputs invalid or random data called FUZZ into the software system to discover vulnerabilities [21]. As an attack scenario, the fuzzy attacker performs indiscriminate attacks by an iterative injection of random CAN frames with the "randint" function, which is a module that generates random integer numbers within a specified range. In this attack, an attacker directly and randomly injects any frame on the CAN bus, and determines the corresponding relations between CAN frame IDs and ECUs by observing the correspondence between vehicle behavior changes and ECUs. Based on these corresponding relations, the attacker knows which ECUs can be attacked. According to the content of the injected frame, the fuzzy attack can be divided into two categories: fuzzy ID attacks and fuzzy payload attacks. Fuzzy ID attacks refer to the random change of the CAN frame ID, after which the attack injects the ID-changed frame into the CAN bus. Fuzzy payload attacks refer to the random change of the payload of the CAN frame after selecting the CAN frame ID, after which the attack injects the payload-changed frame into the CAN bus. An example is shown in Fig. 5.
In the example shown in Fig. 5, for the fuzzy ID attack, CAN frame IDs $0x100$ and $0x123$ are random numbers, and for the fuzzy payload attack, the payloads of the CAN frame $0x610$ are randomly changed to FF FF FF FF FF FF FF FF and 01 23 45 67 89 AB CD EF.

3) **Replay attack**. An attacker monitors the vehicle CAN bus to obtain the information of the data frames ap-

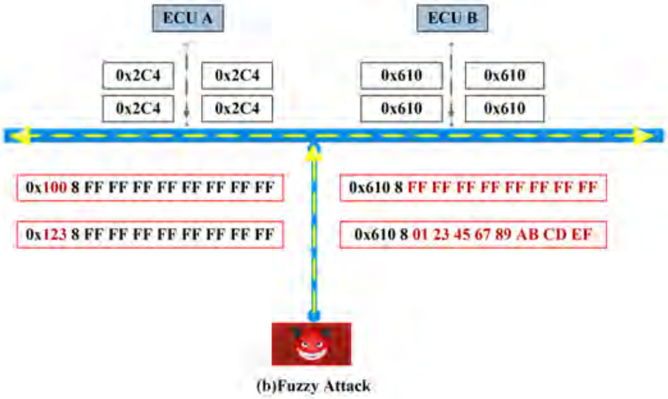

ECU A
ECU B
0x2C4
0x2C4
0x2C4
0x2C4
0x610
0x610
0x610
0x610
0x100 8 FF FF FF FF FF FF FF FF
0x123 8 FF FF FF FF FF FF FF FF
0x610 8 FF FF FF FF FF FF FF FF
0x610 8 01 23 45 67 89 AB CD EF
(b)Fuzzy Attack

Fig. 5. Example of a fuzzy attack in the proposed prototype system.

pearing on the CAN bus, and copies the data-stream fragments that occur during the monitoring period. The attacker injects these copied data frames into the CAN bus to interfere with the normal actions of the vehicle. This is called a replay attack. An example of a replay attack is shown in Fig. 6.

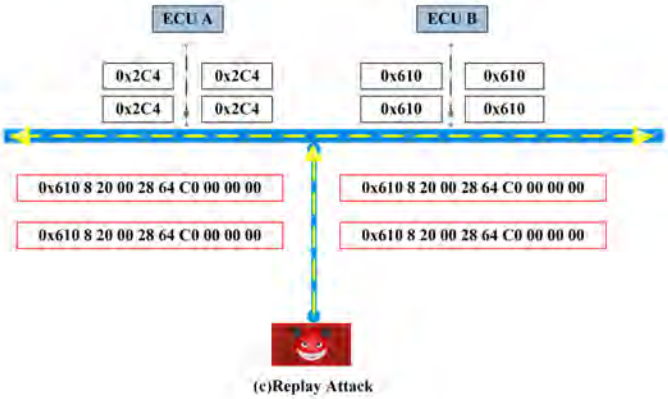

ECU A
ECU B
0x2C4
0x2C4
0x2C4
0x2C4
0x610
0x610
0x610
0x610
0x610 8 20 00 28 64 C0 00 00 00
0x610 8 20 00 28 64 C0 00 00 00
0x610 8 20 00 28 64 C0 00 00 00
0x610 8 20 00 28 64 C0 00 00 00
(c)Replay Attack

Fig. 6. Example of a replay attack in the proposed prototype system.

In the example shown in Fig. 6, an attacker copies and replays the data frames with the frame ID 0x610.

4) **Spoofing attack**. In this attack, after cracking the semantics of the CAN frame payload, the attack injects the modified and recomposed data frames into the CAN bus to carry out an attack. The attack frames of the spoofing attack are sent at the same frequency as the normal ECU, so the compromised ECU can pretend to be a normal ECU, and the compromised ECU cannot be easily identified.

The example shown in Fig. 7 explains the experiment carried on the 2011 Toyota Camry. The frames with the CAN ID 610 are related to the vehicle speed shown on the dashboard, and the time period of normal ECUs to send frames is 500ms.

If the vehicle is stopped, the third byte of the frame is 00, indicating that the vehicle speed is 0km/h. An attack modifies the third byte of four frames to 14, 28, 3C, and 50, which correspond to vehicle speeds of 20, 40, 60, and 80km/h, respectively. Then, the attack sends the modified frames to the CAN bus at a time interval of 500ms. As the vehicle has an automatic door lock function, when the vehicle shows the fake speed under the attack, the ECU of the door lock controls signals to automatically lock the doors, even though the true speed of the vehicle is 0km/h.

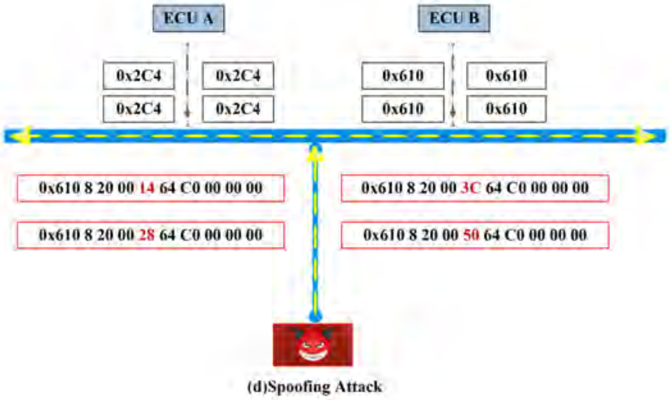

ECU A
ECU B
0x2C4
0x2C4
0x2C4
0x2C4
0x610
0x610
0x610
0x610
0x610 8 20 00 14 64 C0 00 00 00
0x610 8 20 00 28 64 C0 00 00 00
0x610 8 20 00 3C 64 C0 00 00 00
0x610 8 20 00 50 64 C0 00 00 00
(d)Spoofing Attack

Fig. 7. Example of a spoofing attack in the proposed prototype system.

To substantiate attack identification against the four attack scenarios, two different kinds of datasets: normal driving data and abnormal driving data, are used. The data are the CAN messages obtained through the in-vehicle OBD-II port of a real vehicle (the aforementioned 2011 Toyota Camry) [7]. The normal driving data without attacks measure the ground-truth value of the vehicle's normal operation. The abnormal driving data are those containing attacks.

The equipment setup used for the extraction of the two kinds of driving datasets is as follows. A development board with the main control chip STM32 is used to obtain the data from the in-vehicle OBD-II port and analyze/transmit data. The data acquisition and transmission rates are both 500$kbps$, and the data transmission employs 4G standards. Moreover, the board supports multiple diagnosis protocols, such as ISO15765, ISO14230, and SAEJ1939. On this basis, in the same experimental environment, the computation time is at the millisecond level for Aiden and the approach (it is used for comparison) and can almost be ignored.

B. Evaluation Results and Analysis

To demonstrate the performance of the proposed model for attack identification, in this section the comparative results of the overall performance evaluation are presented and analyzed; the comparison is made with an approach that previously proposed by Cho *et al.* [9].

1) Evaluation Results: In this study, the accuracy of attack identification is measured by considering the four attack scenarios described in section V-A. Accuracy is defined as the ratio of the correctly identified data for a specific attack scenario and the four defined attack scenarios, and is formulated as $Accuracy = TP + TN/(TP + FP + TN + FN)$, where TP denotes an attack packet classified as **attack**, and the corresponding compromised ECU is identified. FP

indicates that a normal packet is classified as **attack**, and the corresponding compromised ECU is identified falsely. FN means that an attack packet is classified as **normal**, and the corresponding compromised ECU is not identified. TN shows that a normal packet is classified as **normal**, and there are no ECUs to be identified as compromised.

To demonstrate the applicability and scalability of the proposed model, an evaluation experiment was conducted under five speeds: 0, 20, 40, 60, and $80km/h$. The results are shown in Fig. 8. Moreover, Aiden's performance is compared with that of the existing method using the CIDS under four defined attack scenarios. Figure 9 illustrates the comparative results.

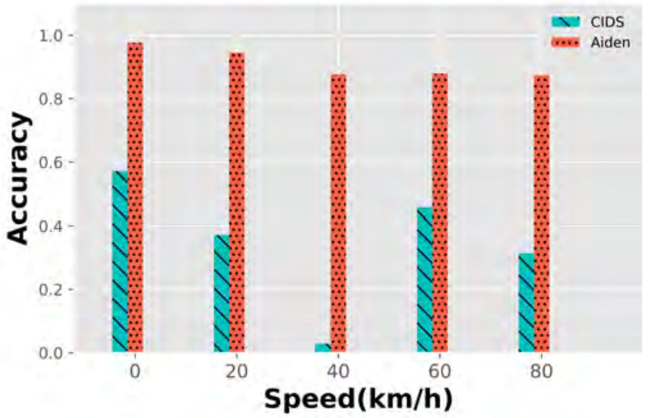


Fig. 8. Average accuracy of attack identification in four types of attack scenarios under five vehicle speeds.

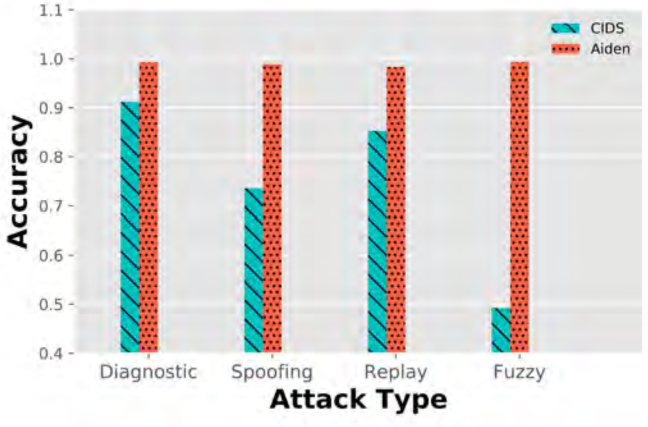


Fig. 9. Comparative results of Aiden and CIDS under four types of attack scenarios.

2) Result Analysis: The identification performance of the proposed model is evaluated by "accuracy". The evaluation of the identification accuracy is done using four types of attack scenarios, with two kinds of datasets and under five vehicle speeds.

Figure 8 illustrates the identification accuracy under five speeds, that is, 0, 20, 40, 60, and $80km/h$, and each accuracy value is calculated as the average in four defined attack scenarios at a certain speed. In all of the speed cases, Aiden performs better than the CIDS: The accuracy is improved by 41.5% for a speed of $0km/h$, 60.7% for $20km/h$, 96.7% for $40km/h$, 48.0% for $60km/h$, and 64.1% for $80km/h$. The values of identification accuracy for the five speed scenarios are listed in Table II.

TABLE II
IDENTIFICATION ACCURACY VALUES FOR FIVE SPEED SCENARIOS

	CIDS	Aiden
0	0.571429	0.976463
20	0.371429	0.944714
40	0.028571	0.876691
60	0.457143	0.878607
80	0.314286	0.874445

Figure 9 provides the identification accuracy evaluated using four defined attack scenarios for the 2011 Toyota Camry, and the comparative results are presented as the mean values of the attack-identification accuracy from multiple experiments. In all of the attack scenarios, for the identification accuracy, Aiden obtains higher values than the CIDS regardless of the defined speeds. The accuracy is improved by 8.2% for the diagnosis attack, 50.4% for the fuzzy attack, 13.3% for the replay attack, and 25.6% for the spoofing attack. The values of identification accuracy for the four defined attack scenarios are listed in Table III.

TABLE III
IDENTIFICATION ACCURACY VALUES FOR FOUR ATTACK SCENARIOS

	CIDS	Aiden
Diagnosis attack	0.911765	0.992849
Fuzzy attack	0.492307	0.993416
Replay attack	0.852941	0.983284
Spoofing attack	0.735294	0.988703

VI. DISCUSSION

In this study, a cost-effective model for attack identification is proposed and evaluated. The proposed model only analyzes the CAN messages from real vehicles. It performs association learning to learn the logical association among different ECUs, without using any feature to fingerprint ECUs. Moreover, the model does not need to know the content inside CAN messages. Therefore, the model can be applied to any type of vehicle without parsing the CAN messages.

Most importantly, because the loss of information content is reduced by considering the association of CAN messages from different ECUs, the proposed model can provide higher accuracy in attack identification.

The processing procedure of the proposed model abides by the principle of integrity for digital evidence [22], and ensures that the collected data are not forged or modified. Similar to the data transmitted over a general network, the CAN message is a form of volatile data that temporarily exists on the CAN bus that disappears after completing its function. For this reason, the CAN messages on the CAN bus should be saved with metadata when an attack occurs.

With the association learning of CAN messages, volatile data constitute valuable information with which to better understand events happening to the CAN bus. Additionally, they can provide a clue for determining the source of and thereby solving the problems caused by an attack. Therefore, it is important to ensure the authenticity and integrity of data in the detection and identification processes. The proposed model strengthens the case for CAN messages of the CAN bus to be accepted as legally significant digital evidence.

VII. Conclusion

In this study, a model is developed for attack identification by learning the ECUs' association in the driving behaviors. Through such learning, pattern sequences are obtained to represent the association of different ECUs. Moreover, the proposed model, Aiden, does not have to consider vehicle models.

The performance of the proposed model is evaluated by measuring the identification accuracy in four specific attack scenarios. To cover a wide range of internal running status of a vehicle, five different vehicle speeds are used to evaluate the identification accuracy by applying statistical values. From the perspective of ensuring performance, Aiden preserves the association of different ECUs, ensuring the information integrity of CAN messages.

In the future, given the association property of volatile data on the CAN bus, research concerning digital forensics will be conducted by using the model Aiden [22]–[24]. In the digital forensics of vehicles, to ensure the information integrity from different ECUs and trace the information flow on the in-vehicle CAN bus, information should be retrieved and ascertained from the traces left by the various devices connected to the CAN bus.

In summary, the results of this study contribute to secure data management on the edge of V2X communication networks.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (Grant No. 61802097), the Project of Qianjiang Talent (Grant No. QJD1802020), and the Key Research & Development Plan of Zhejiang Province (Grant No. 2019C01012).

References

[1] J. E. Siegel, D. C. Erb, and S. E. Sarma, "A survey of the connected vehicle landscapeąłarchitectures, enabling technologies, applications, and development areas," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2391–2406, 2017.

[2] J. Z. Varghese, R. G. Boone *et al.*, "Overview of autonomous vehicle sensors and systems," in *International Conference on Operations Excellence and Service Engineering*, 2015, pp. 178–191.

[3] K. Kant, "Advanced persistent threats in autonomous driving," *ACM SIGMETRICS Performance Evaluation Review*, vol. 47, no. 4, pp. 25–28, 2020.

[4] Y. Li, Q. Luo, J. Liu, H. Guo, and N. Kato, "Tsp security in intelligent and connected vehicles: Challenges and solutions," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 125–131, 2019.

[5] Y. Xun, J. Liu, N. Kato, Y. Fang, and Y. Zhang, "Automobile driver fingerprinting: A new machine learning based authentication scheme," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1417–1426, 2019.

[6] S. Nie, L. Liu, and Y. Du, "Free-fall: Hacking tesla from wireless to can bus," *Briefing, Black Hat USA*, vol. 25, pp. 1–16, 2017.

[7] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno *et al.*, "Comprehensive experimental analyses of automotive attack surfaces," in *USENIX Security Symposium*, vol. 4. San Francisco, 2011, pp. 447–462.

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

[9] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*, 2016, pp. 911–927.

[10] ——, "Viden: Attacker identification on in-vehicle networks," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1109–1123.

[11] 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*, 2018, pp. 787–800.

[12] J. Ning, J. Wang, J. Liu, and N. Kato, "Attacker identification and intrusion detection for in-vehicle networks," *IEEE Communications Letters*, vol. 23, no. 11, pp. 1927–1930, 2019.

[13] Wikipedia. Vehicle-to-Everything (V2X). [Online]. Available: https://en.wikipedia.org/wiki/Vehicle-to-everything

[14] L. Song, G. Sun, H. Yu, X. Du, and M. Guizani, "Fbia: A fog-based identity authentication scheme for privacy preservation in internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5403–5415, 2020.

[15] 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. 2012-01-0999, pp. 358–372, 2012.

[16] X. Lin, J. Wu, S. Mumtaz, S. Garg, J. Li, and M. Guizani, "Blockchain-based on-demand computing resource trading in iov-assisted smart city," *IEEE Transactions on Emerging Topics in Computing*, 2020.

[17] 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.

[18] 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.

[19] T. Alladi, S. Chakravarty, V. Chamola, and M. Guizani, "A lightweight authentication and attestation scheme for in-transit vehicles in iov scenario," *IEEE Transactions on Vehicular Technology*, 2020.

[20] J. Gao, K. O.-B. O. Agyekum, E. B. Sifah, K. N. Acheampong, Q. Xia, X. Du, M. Guizani, and H. Xia, "A blockchain-sdn-enabled internet of vehicles environment for fog computing and 5g networks," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4278–4291, 2019.

[21] S. Dinesh, N. Burow, D. Xu, and M. Payer, "Retrowrite: Statically instrumenting cots binaries for fuzzing and sanitization," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 1497–1511.

[22] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, "Block-def: A secure digital evidence framework using blockchain," *Information Sciences*, vol. 491, pp. 151–165, 2019.

[23] N.-A. Le-Khac, D. Jacobs, J. Nijhoff, K. Bertens, and K.-K. R. Choo, "Smart vehicle forensics: Challenges and case study," *Future Generation Computer Systems*, vol. 109, pp. 500–510, 2020.

[24] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (iot) forensics: Challenges, approaches and open issues," *IEEE Communications Surveys & Tutorials*, 2020.

Yuanfang Chen (S'09-M'16) received the M.S. and first Ph.D. degrees from Dalian University of Technology, China, and the second Ph.D. degree from University Pierre and Marie Curie, France. From 2009 to 2010, she was an Assistant Researcher with Illinois Institute of Technology, USA, with Prof. Xiangyang Li. She is currently a Professor with Hangzhou Dianzi University, China, and she is a Professor with Shanghai Jiaotong University, China. Her research interests include Artificial Intelligence of Things, Artificial Intelligence Security, and Algorithm Design.

Muhammad Alam (S'10-M'14-SM'17) received Ph.D. degree in Computer Science from University of Aveiro, Portugal (2009-2014). In 2009, he joined the Instituto de Telecomunicações-Aveiro (Portugal) as a senior Researcher. In 2017, he joined Xi'an Jiaotong-Liverpool University (XJTLU), Suzhou as an Assistant Professor in Computer Science. Currently, he is working as Senior Lecturer in smart cities and secure systems (IoT) at London South Bank University, UK. His research interests include Vehicle Communication, Internet of Things Security, and Algorithm Design.

Shahid Mumtaz is an IET Fellow, IEEE ComSoc, IAS and ACM Distinguished speaker, recipient of IEEE ComSoC Young Researcher Award (2020), founder and EiC of IET "Journal of Quantum Communication", Vice-Chair: Europe/Africa Region-IEEE ComSoc: Green Communications & Computing Society and Vice-Chair for IEEE standard on P1932.1: Standard for Licensed/Unlicensed Spectrum Interoperability in Wireless Mobile Networks. He is the author of 4 technical books, 12 book chapters, 300+ technical papers (200+ IEEE Journals/Transactions, 100+ Conferences, 2 IEEE Best Paper Awards-in the area of mobile communications. Most of his publication is in the field of Wireless Communication. He is serving as Scientific Expert and Evaluator for various Research Funding Agencies. He was awarded an "Alain Bensoussan Fellowship" in 2012. He is the recipient of the NSFC Researcher Fund for Young Scientist in 2017 from China.