Internet of Things, Ad Hoc and Sensor Networks Technical Committee Newsletter

(IoT-AHSN TCN)

Volume 1, No. 17

December, 2022

CONTENTS

PREFACE

The IEEE ComSoc Ad Hoc and Sensor Networks Technical Committee (IoT-AHSN TC) sponsors papers, discussions, and standards on all aspects of IoT, ad hoc and sensor networks. It provides a forum for members to exchange ideas, techniques, and applications, and share experience among researchers. Its areas of interest include systems and algorithmic aspects of sensor and ad hoc networks, networking protocols and architecture, embedded systems, middle-ware and information management, novel applications, flow control and admission control algorithms, network security, reliability, and management. In an attempt to make all the TC members as well as the IoT-AHSN worldwide community aware of what is going on within our main areas of concerns, this newsletter had been set up. The newsletter aims at inviting the authors of successful research projects and experts from all around the world with large vision about IoT-AHSN-related research activities to share their experience and knowledge by contributing in short news.

The seventeenth issue of the IoT-AHSN TC Newsletter focuses on the theme “Internet of Vehicles”. Specifically, this issue includes two news article: i) Side Channel Analysis: A New Perspective for Vehicle Intrusion Detection System; ii) Dependent Application Offloading for Internet of Vehicles. We thank the contributors for their efforts to help make the IoT-AHSN TC Newsletter a success. We hope that the methods/approaches presented in this issue could significantly benefit researchers and application developers who are interested in IoT and ad hoc/sensor networks.

Newsletter Co-Editors
Qiang Ye (Dalhousie University, Canada)
Moez Esseghir (University of Technology of Troyes, France)
Lu Lv (Xidian University, China)

TC OFFICERS AND NEWSLETTER EDITORS

TC Officers

Name	Affiliation	Email
Jiajia Liu (Chair)	Xidian University, China	liujiajia@xidian.edu.cn
Sharief Oteafy (Vice Chair)	DePaul University, USA	soteafy@depaul.edu
Shuai Han (Secretary)	Harbin Institute of Technology, China	hanshuai@hit.edu.cn

Newsletter Editors

Name	Affiliation	Email
Qiang Ye (Editor in Chief)	Dalhousie University, Canada	qye@cs.dal.ca
Moez Esseghir (Technical Editor)	University of Technology of Troyes, France	moez.esseghir@utt.fr
Lu Lv (Technical Editor)	Xidian University, China	lulv@xidian.edu.cn

Side Channel Analysis: A New Perspective for Vehicle Intrusion Detection System

Yijie Xun[*][†], Yuwei Yang[*]
[*]School of Cybersecurity, Northwestern Polytechnical University, Xi'an, Shaanxi, 710072, China
[†]E-mail: xunyijie@nwpu.edu.cn

***Abstract*—While intelligent connected vehicles (ICVs) bring convenience and benefits to people's lives, they also bring vulnerability interfaces that facilitate attacks. Therefore, the experts propose the baseline of two solutions, namely, the protocol-based data encryption/decryption scheme and the intrusion detection system (IDS) based on side channel analysis. Due to the limitation of bandwidth resources and the demand for real-time data transmission, the lightweight data encryption/decryption scheme has made slow progress, and the IDS based on side channel analysis has developed rapidly due to its ability to detect the information about attacks. In this paper, we first study the classification of side channel-based IDS, and then describe the working principles of three existing representative works. Finally, we introduce three new IDSs to compensate for the disadvantages of existing work.**

I. Introduction

With the development of technology, great progress has emerged in intelligent connected vehicles(ICVs), which bring more convenient services and higher life quality to people's lives. However, vulnerability external interfaces are introduced during the progress, which makes the vehicles more vulnerable to attacks. For example, Cai *et al.* [1] revealed the vulnerabilities that existed in vehicle components, which could be exploited by attackers to control the vehicles' external-facing I/O interfaces. In [2], Wang *et al.* proposed an attack on autonomous vehicles using invisible lights to ruin the in-car user experience. Cao *et al.* [3] designed an autonomous driving attack based on lidar that may cause traffic accidents. It is urgent to take appropriate countermeasures in face of security threats in ICVs.

ICVs security has always been a research hotspot in the automotive industry. As a countermeasure against attacks in ICVs, two main lines of defense have been pursued: protocol-based data encryption/decryption scheme and intrusion detection system (IDS) based on side channel analysis. The protocol-based data encryption/decryption scheme protects the vehicle security by encrypting data frames, verifying digital signatures and certificates. Although the protocol-based data encryption/decryption scheme can protect vehicles from being cracked by attackers, its development is hindered due to its large occupation of the bandwidth and computing resources in controller area network (CAN). Although the protocol-based data encryption/decryption scheme protects the vehicles before being cracked by attackers by encrypting data frames, verifying digital signatures and certificates, its development is hindered due to its large occupation of the bandwidth and computing resources in controller area network (CAN). The side channel-based IDSs consist of time-based IDS, voltage-based IDS, and traffic-based IDS, which are developing at high speed respectively.

This paper first studies the classification of side channel-based IDSs, and then illustrates the working principles of three existing representative IDSs. Finally, three new IDSs are introduced to compensate for the disadvantages of the existing work. The experimental results show that the proposed methods can not only detect malicious attacks with high accuracy, but also accurately identify attack sources.

II. IDS Assisted Vehicle Security

A. Time-based IDS

In 2017, Cho and Shin first designed a clock skew-based IDS called CIDS [4]. Next, Sekar Kulandaivel *et al.* [5] developed automotive network mapping tools based on CIDS. CIDS first uses clock skew which means the interval deviation of periodic in-vehicle messages as the fingerprint of each electronic control unit (ECU), so that it can identify the malicious frames in CAN bus. It should be noted that, Work [4] can detect the corresponding attack source ECU only if the transmission period of malicious frame matches the period list of sender ECU. Usually, the message period of the in-vehicle ECU is usually only (0.01, 0.1, 0.2, 0.02) seconds, etc. 6 types, and attackers can easily bypass these periods. To this end, it is necessary to find a new method that can accurately identify the sender ECU of malicious frames within any period. More importantly, CAN frames exchange data between ECUs, and each ECU will send multiple IDs data with different cycles. Whether the clock skew is the same for different ids of the same ECU is not discussed in the work [4].

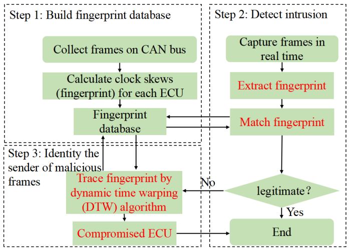
Step 1: Build fingerprint database
Collect frames on CAN bus
Calculate clock skews (fingerprint) for each ECU
Fingerprint database
Step 2: Detect intrusion
Capture frames in real time
Extract fingerprint
Match fingerprint
legitimate?
No
Yes
End
Step 3: Identity the sender of malicious frames
Trace fingerprint by dynamic time warping (DTW) algorithm
Compromised ECU

Fig. 1. ClockIDS

We designed a clock skew-based IDS named ClockIDS [6], which can identify the sender of malicious frames, that is, the controlled ECU. ClockIDS's working principle is as Fig. 1. ClockIDS first builds a fingerprint database by collecting frames in CAN bus and calculating clock skews for each ECU. Then, we use clock skew to achieve the function of intrusion detection and attack source identification by using the empirical rule (ER) algorithm. Since the clock skew caused by different IDs from the same ECU has a similar trend, we use the dynamic time warping (DTW) algorithm to evaluate the similarity of two clock skew IDs. ClockIDS can not only improve the ability of intrusion detection, but also identify the attack source ECU, with an average recognition rate of 96.77%.

B. Voltage-based IDS

In cars, each ECU has its unique voltage signal characteristics. Cho and Shin [7] first discovered this feature and creatively designed a voltage-based IDS named Viden, which can detect malicious frames and locate their senders. Choi *et al.* [8] proposed a voltage-based IDS named VoltageIDS, which use differential signals rather than CAN-H and CAN-L signals directly. Kneib *et al.* [9] designed a voltage-based IDS called Scission requiring lower hardware. However, these voltage-based IDSs are difficult to simultaneously detect malicious frames from internal ECUs and external nodes and require a secret mapping between ECUs and IDs. More than that, they utilize the statistical method and support vector machine to detect abnormal ECUs, while many popular algorithms have not been studied.

To overcome the limitations of previous work, we designed a voltageIDS named VehicleEIDS [10]. The working principle is as Fig. 2. In order to avoid the interference of recessive signal, VehicleEIDS collects and analyzes the dominant signal, that the differential signals higher than 0.5V and lower than 3V. Then, we selected 14 time-domain features as the voltage features. Finally, we use the deep support vector-domain description (deep SVDD) model composed of two convolution layers, a pooling layer, two full connection layers, and a prediction output layer to solve the problem as a binary classification problem with the detection accuracy rate of 98.13%.

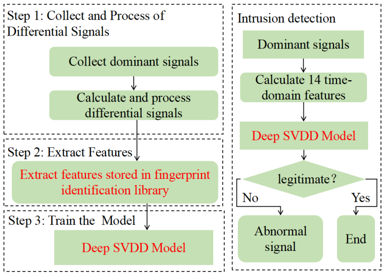
Step 1: Collect and Process of Differential Signals
Collect dominant signals
Calculate and process differential signals
Step 2: Extract Features
Extract features stored in fingerprint identification library
Step 3: Train the Model
Deep SVDD Model
Intrusion detection
Dominant signals
Calculate 14 time-domain features
Deep SVDD Model
legitimate?
No
Yes
Abnormal signal
End

Fig. 2. VehicleEIDS

C. Data frame-based IDS

In addition to time-based IDS and voltage-based IDS, there are traffic-based IDS detecting intrusions based on the traffic data in CAN bus. Although these IDSs can detect various attacks with high accuracy such as spoofing attacks, bus-off attacks, masquerade attacks, none of them can detect the attack that the malicious frames have the same side characteristics, which means the malicious frames and the normal frames both come from the same ECU. Thus, we proposed a data frame-based IDS named GVIDS which can detect the above attacks. After collecting ID frames in CAN bus, GVIDS converts the data fields to images and trains a model based on Generative Adversarial Networks (GAN) to achieve intrusions detection. The average accuracy of GVIDS to detect multiple attacks is 94.66%.

III. Conclusion

This paper first systematically introduced two kinds of security protection methods for the in-vehicle network of ICVs, with a particular focused on side channel-based IDSs. Then three IDSs based on side channel analysis were introduced in detail. It is found that IDSs with different side channel characteristics have their own advantages and disadvantages, it is necessary to use multiple side channel features to enhance in-vehicle network security. More importantly, with the emergence of new technologies such as cloud-vehicle linkage and federated learning, the side channel-based IDS can no longer meet the requirements of in-vehicle network security protection, and new methods need to be constantly explored to protect the security of ICVs.

References

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

[2] W. Wang, Y. Yao, X. Liu, X. Li, P. Hao, and T. Zhu, "I Can See the Light: Attacks on autonomous vehicles using invisible lights," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021, pp. 1930–1944.

[3] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, and Z. M. Mao, "Adversarial sensor attack on lidar-based perception in autonomous driving," in *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2019, pp. 2267–2281.

[4] 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.

[5] S. Kulandaivel, T. Goyal, A. K. Agrawal, and V. Sekar, "CANvas: Fast and inexpensive automotive network mapping," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 389–405.

[6] Y. Zhao, Y. Xun, and J. Liu, "ClockIDS: A real-time vehicle intrusion detection system based on clock skew," *IEEE Internet of Things Journal*, 2022.

[7] 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*, 2017, pp. 1109–1123.

[8] 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.

[9] 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.

[10] Y. Xun, Y. Zhao, and J. Liu, "VehicleEIDS: A novel external intrusion detection system based on vehicle voltage signals," *IEEE Internet of Things Journal*, vol. 9, no. 3, pp. 2124–2133, 2021.

Dependent Application Offloading for Internet of Vehicles

Yixin Fan[1,2], Changle Li[1,2]*, Wenwei Yue[1,2]
[1]State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, Shaanxi, 710071 China
[2]Research Institute of Smart Transportation, Xidian University, Xi'an, Shaanxi, 710071 China
*E-mail: clli@mail.xidian.edu.cn

***Abstract*—With the development of the Internet of Things (IoT) and communication technology, more and more intelligent devices can interact with each other in real time through IoT. Internet of Vehicles (IoV) is a typical application of IoT. In IoV, vehicles interact with the surrounding cooperative vehicles through the communication device and sensing device, and offload onboard applications to the cooperative vehicles with idle computing resources. Offloading dependent applications is a challenging problem in IoV, because the design of offloading strategy is determined by the interaction of multiple factors, including the internal dependency of applications, the high mobility of vehicles, and the collaborative perception of vehicles. In this paper, we propose an onboard dependent application offloading strategy based on Artificial Intelligence (AI) technology, which can effectively reduce offloading latency.**

***Index Terms*—Internet of things (IoT), internet of vehicles (IoV), application offloading, dependent application, artificial intelligence (AI).**

I. Introduction

In recent years, vehicles have become an important component of mobile devices connected to the Internet. The vehicle in IoV integrates sensing, communication and computing technology, and can run new onboard applications with different functions, such as Autonomous Driving, Vehicle Intelligent Assisted Driving and Augmented Reality (AR), Intelligent Navigation, and other applications that serve drivers and passengers [1]. The emergence of such new applications provides users with a variety of services, and greatly improves the driving experience and driving safety.

However, such onboard applications are usually computation-intensive and delay-sensitive, which not only consume huge computing, storage and communication resources, but also require vehicle terminals to make a timely and rapid response. If all these applications are handled locally by the vehicle terminal, the limited local resources seriously restrict the timely processing and response, which poses a significant challenge for the vehicle to ensure the quality of service required [2]. At the same time, computation-intensive onboard applications typically consist of a series of interdependent sub-modules, such as onboard Virtual Augmented Reality and HD maps. The data processing process from raw sensing data to 3D display consists of multiple processing modules, with different module functions and complex dependencies [3].

By combining vehicular edge computing (VEC) technology, vehicles can offload a part of the onboard computing-intensive applications or all of them to edge servers with adequate resources to assist in application processing [4]. Edge servers often combine with Road Side Units (RSU) to cache content or provide computational resources. However, the RSU is often far away from the vehicle, which causes a large transmission delay. The vehicles in IoV are usually equipped with communication units, high-performance computing equipment and sensing equipment. Combined with communication and sensing, vehicle terminals can realize highly efficient collaborative computing, and make full use of the idle resources of nearby collaborative vehicles to alleviate the overload resource demand of the vehicle terminal. Fig. 1 shows the scenario of our dependent application offloading in IoV, in which one vehicle has an application consisting of multiple sub-modules that require the surrounding cooperate vehicles to assist in offloading.

This paper introduces how to design an offloading strategy based on multi-vehicle collaboration for dependent onboard applications in the high mobile IoV that integrates sensing, communication and computing. The main contributions of this paper include analyzing the high mobility of sensing, communication and computing integrated IoV, analyzing the onboard dependent application and modeling methods, and how to utilize multi-vehicle collaborative sensing. At the end of the article, the role of AI in offloading IoV tasks is introduced.

II. Offloading Strategy Design

In this section, we mainly introduce how we consider internal dependency of onboard applications, the high mobility of IoV, and the collaborative sensing between the vehicles when designing the offloading strategies.

A. Internal Dependency of Applications

An IoV application often consists of multiple sub-modules with internal dependencies. When a sub-module is offloading, it often requires information from sub-modules before it. If the dependency is ignored, it may cause the application to obtain the wrong results or exceed the time constraint. However, adding dependency information into the design of the strategy may avoid this problem.

Therefore, we model onboard applications as a Directed Acyclic Graph (DAG) and use DAG to represent the dependence between each sub-module of onboard applications. Each

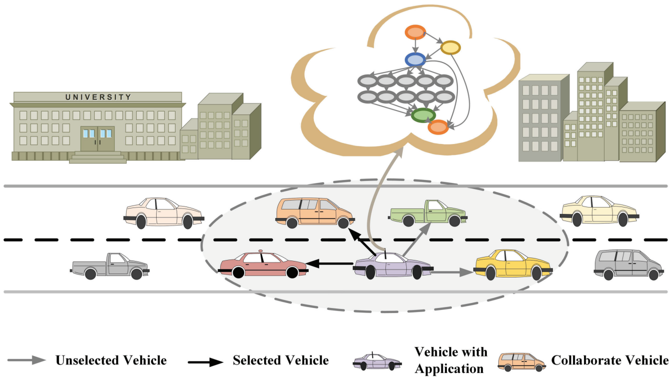

Fig. 1. Multi-Vehicle Assisted dependent application offloading scenario.

node represents a sub-module, and each directed edge represents the sub-module dependency information. By modeling the dependencies, we can determine the offloading sequence of sub-modules.

B. High Mobility of IoV

The high mobility of the vehicle affects the offloading and calculation of the dependent vehicle applications. As the vehicle keeps moving, the distance between the collaborative vehicles varies dramatically over time, which leads to unstable communication connections [5]. In addition, the vehicles with idle computing resources around the vehicle will constantly change. Therefore, the consideration of vehicle mobility is an indispensable part of the design of a multi-vehicle collaborative application offloading strategy.

Since the vehicles are equipped with sensing equipment, the vehicle can obtain the location, speed, acceleration, and resource occupation situation of the surrounding vehicles to determine available collaborative vehicles for offloading in a certain range. Moreover, based on the perceived information, the vehicle can predict the collaborative vehicle companion time using the vehicle mobility prediction algorithm to reduce computational offloading failure.

C. Collaborative Sensing

There are some onboard applications that contain certain sub-modules that often need environmental data as their input, such as onboard Virtual Augmented Reality applications and Autonomous Driving applications [6]. Vehicles are often equipped with multiple sensors with different functions that can collect a variety of environmental information. Therefore, the collaborative vehicle can assist in sensing the environmental information and computing the perceived environmental information.

However, collaborative vehicles at different locations have different perspectives, which requires coordinate transformation of the perceived environmental data. Therefore, the collaborative vehicle does not require providing full environmental information to the task vehicle during dependent application unloading. Collaborative vehicles can perceive a part of environmental information, thus reducing the transmission delay.

To obtain the optimal offloading strategy, we also need the assistance of Artificial Intelligence (AI) techniques. In the part of the vehicle mobility analysis, we need to use Deep Learning (DL) to predict the vehicle companion time. Assigning offloading vehicles to sub-modules of dependent applications requires Deep Reinforcement Learning (DRL) to train neural networks and output offloading decisions with the shortest latency.

III. The Role of AI in IoV Task Offloading

AI is widely used in IoV application offloading. DRL is a branch of artificial intelligence that takes advantage of the perceptual ability of deep learning and the decision-making ability of reinforcement learning [1]. DRL has the ability to abstract many factors affecting the VEC environment into mapping problems and learns optimal offloading strategies from the environment, which makes it become a research focus for solving task unloading problems [4]. Using DRL, appropriate offloading strategies can be obtained without domain-specific knowledge and complex calculation.

IV. Conclusion

This paper mainly introduces how to offload the dependent onboard application in IoV. Firstly, the features of IoV applications and the multi-vehicle collaborative offloading scenario are introduced. Then, we analyze the three factors to consider in designing the offloading strategy, including the internal dependency of onboard applications, the high mobility of IoV, and the collaborative sensing between the vehicles. Furthermore, we consider how to use these three factors combined with AI technology to design offloading strategies for dependent applications.

References

[1] L. Yao, X. Xu, M. Bilal, and H. Wang, “Dynamic Edge Computation Offloading for Internet of Vehicles With Deep Reinforcement Learning,” *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–9, 2022.

[2] G. Liu, F. Dai, B. Huang, Z. Qiang, S. Wang, and L. Li, “Dependency-Aware Task Offloading for Vehicular Edge Computing with End-Edge-Cloud Collaborative Computing,” preprint, In Review, Aug. 2022.

[3] T. Braud, P. Zhou, J. Kangasharju, and P. Hui, “Multipath Computation Offloading for Mobile Augmented Reality,” in *2020 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, (Austin, TX, USA), pp. 1–10, IEEE, Mar. 2020.

[4] Q. Luo, C. Li, T. H. Luan, and W. Shi, “Collaborative Data Scheduling for Vehicular Edge Computing via Deep Reinforcement Learning,” *IEEE Internet of Things Journal*, vol. 7, pp. 9637–9650, Oct. 2020.

[5] N. Cha, C. Wu, T. Yoshinaga, Y. Ji, and K.-L. A. Yau, “Virtual Edge: Exploring Computation Offloading in Collaborative Vehicular Edge Computing,” *IEEE Access*, vol. 9, pp. 37739–37751, 2021.

[6] Y. Qi, Y. Zhou, Y.-F. Liu, L. Liu, and Z. Pan, “Traffic-Aware Task Offloading Based on Convergence of Communication and Sensing in Vehicular Edge Computing,” *IEEE Internet of Things Journal*, vol. 8, pp. 17762–17777, Dec. 2021.