MBID: Micro-Blockchain-Based Geographical Dynamic Intrusion Detection for V2X

Haoran Liang, Jun Wu, Shahid Mumtaz, Jianhua Li, Xi Lin, and Miaowen Wen

Abstract

Vehicle-to-everything (V2X) aims to make transportation system more intelligent through linking everything with the moving vehicles, but it brings geographical dynamic intrusions. However, existing intrusion detection systems (IDSs) of vehicles just deploy the preset statics strategies. As a novel security technology, blockchain can realize decentralized tamper- resistance. However, it has not been used for IDSs because of its rigid structure. In this article, we propose Micro-Blockchain based geographical dynamic Intrusion Detection, MBID, for V2X. A novel nested micro-blockchain structure is proposed, where each micro-blockchain deployed in a small region can construct local intrusion detection strategies for vehicles with tamper-resistance. When a vehicle moves to another region, spatial-temporal dynamic IDSs strategies are constructed through the proposed repeatedly nested scheme for micro-blockchains. Moreover, the control plane is proposed to dynamically configure IDSs strategies into the micro-blockchain. Simulation results show the accuracy of MBID.

Introduction

Vehicle-to-everything (V2X) communication is a technology that aims to connect every entity to vehicles [1]. By linking roadside infrastructures, devices, pedestrians, grids, and nearby vehicles to moving vehicles, V2X has become the backbone of the intelligent transportation system (ITS), which tries to make the driving process safer and smarter. V2X has a huge economic impact: the global market size of V2X is expected to reach US$26.72 billion by 2025 [2].

The vision of V2X is built on highly connected vehicles that collect valuable data through diverse communication methods (vehicle-to-vehicle, vehicle-to-infrastructure, etc.) to guide driving. However, a large number of entities connected to vehicles bring not only useful information for driving but also unprecedented risks to these vehicles. The threat model for intrusion detection in V2X is given as follows. The vehicles in V2X have to face intrusions from diverse entities connected to it. These intrusions are featured with diversity and dynamic geographic properties. Specifically, rich communication methods and a large number of untrusted devices in V2X lead to a dramatic increase in the types of intrusions faced by the vehicles. Diverse intrusions against in-vehicle and inter-vehicle networks can cooperate to destroy the vehicles. Moreover, the frequent movement of vehicles results in intrusions that against vehicles will vary by location and time slot, which means that these intrusions feature high temporal-spatial dynamics. For instance, attackers in one area might focus on attacking the controller area network (CAN) bus, while attackers in another area are interested in using a Sybil attack [3].

Recently, a large number of traditional intrusion detection systems (IDSs) have been proposed for intelligent vehicles. Specifically, technologies such as recurrent neural networks (RNNs), convolutional neural networks (CNNs), statistical techniques, and long short-term memory (LSTM) have been employed as models for detecting intrusions against vehicles [4, 5]. For instance, RNN and LSTM were combined to generate the strategy to identify denial-of-service attacks, malware attacks, and command injection attacks against robotic vehicles [6]. Statistical techniques were employed to construct a strategy to detect false information attacks and Sybil attacks against vehicular ad hoc networks [7]. Recursive least-square filter was utilized to build a strategy for identifying intrusion against sensors on vehicles [8]. However, traditional IDSs have three drawbacks. First, due to a lack of reliable local intrusion samples, each traditional IDS typically can only detect particular attacks (e. g., spoof attack, replay attack) for a specific part of in-vehicle and inter-vehicle networks (e. g., CAN bus, telematics unit) rather than intrusion methods that are popular in a specific region. Second, traditional IDSs are generally built on one or two specific models (e.g., CNNs, RNNs). Moreover, the structure of traditional IDSs is static, which indicates that the detection strategy deployed in the system node is static and cannot vary along with changing intrusion methods [9]. Therefore, how to effectively detect the numerous and dynamic intrusions in V2X is still an open problem.

To address the challenges of intrusion detection in V2X, we first conceptualize geographical dynamic intrusion detection (GDID) and illustrate its vision. In particular, GDID aims to dynamically provide on-demand intrusion detection strategies for local vehicles based on reliable local intrusion samples. Recently, blockchain technologies featuring tamper resistance and non-repudiation properties have been employed to handle security problems in the vehicle-to-grid network [10, 11]; thus, we try to build a GDID paradigm with blockchain technologies. However, it is hard to employ traditional blockchain to construct

The authors propose Micro-Blockchain based geographical dynamic Intrusion Detection, named MBID, for V2X. A novel nested micro-blockchain structure is proposed, where each micro-blockchain deployed in a small region can construct local intrusion detection strategies for vehicles with tamper-resistance.

Haoran Liang, Jun Wu (corresponding author), Jianhua Li, and Xi Lin are with Shanghai Jiao Tong University; Shahid Mumtaz is with Instituto de Telecomunicaes; Miaowen Wen is with South China University of Technology.

Digital Object Identifier: 10.1109/MCOM.001.1900143

0163-6804/19/$25.00 © 2019 IEEE

To identify intrusions in V2X communication, we first conceptualize the geographical dynamic intrusion detection (GDID). We define GDID as a secure and distributed system which enables to dynamically deploy intrusion detection strategies on vehicles based on reliable regional intrusion samples.

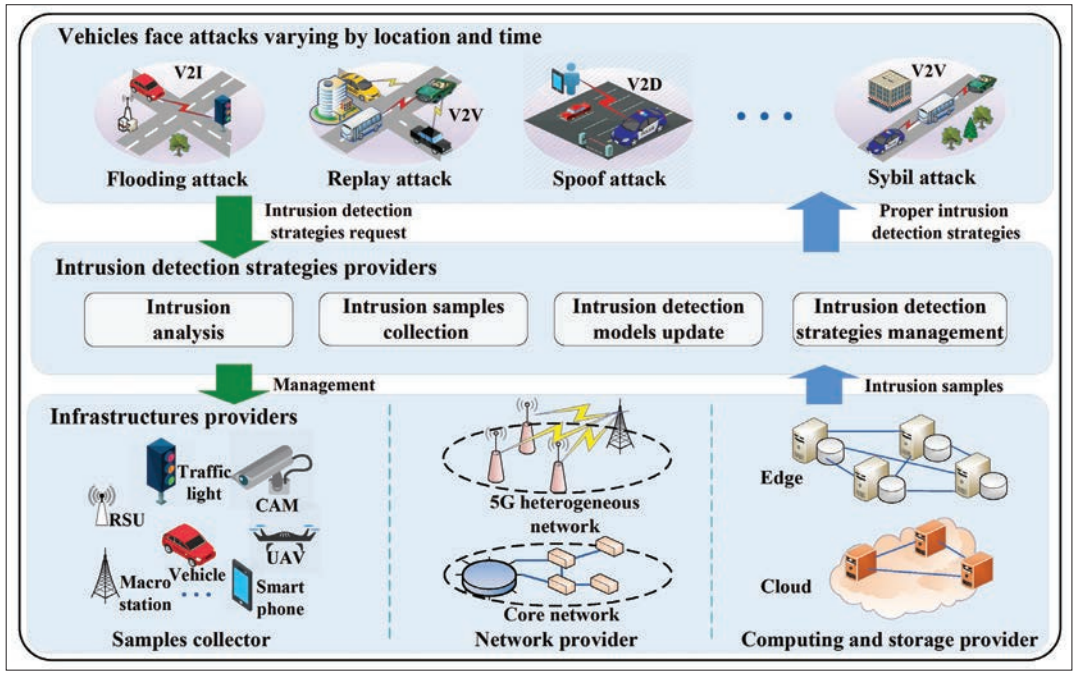

Figure 1. Three entities in geographical dynamic intrusion detection: vehicles, intrusion detection strategy providers, and infrastructure providers.

a GDID paradigm because it indiscriminately stores data belonging to different regions and needs a high time cost to store the data on the blockchain [12]. Thus, we propose a micro-blockchain architecture to build reliable intrusion strategies for the GDID paradigm. Also, the architecture contains one macro-blockchain and several micro-blockchains. Local intrusion samples and intrusion detection strategies can be quickly stored, prepaid, and disseminated through the micro-blockchain architecture deployed and run in a specific region. Moreover, several micro-blockchains can construct a larger micro-blockchain, which enables spatial-temporal dynamic intrusion detection strategies to be provided for vehicles moving around a large region. All the data collected by micro-blockchains will be stored in the macro-blockchain for verifying the legality of the collected data and producing cryptocurrency for the data providers. The construction of the GDID paradigm needs not only reliable local datasets but also the dynamic deployment of intrusion strategies. Hence, we propose a distributed and hierarchical control plane over the micro-blockchain architecture to build a GDID paradigm.

Envisioning Geographical Dynamic Intrusion Detection

To identify intrusions in V2X communication, we first conceptualize the GDID. We define GDID as a secure and distributed system that enables dynamically deployment of intrusion detection strategies on vehicles based on reliable regional intrusion samples.

As shown in Fig. 1, three entities are abstracted from GDID: authorized vehicles, intrusion detection strategy providers (IDSPs), and infrastructure providers. Authorized vehicles in GDID can request proper intrusion detection strategies from IDSPs based on their current state. With data collected from a global view, IDSPs can reliably provide services including intrusion samples collection, intrusion analysis, intrusion detection models update, and intrusion detection strategy management. Infrastructure providers provide computation, communication, and storage resources to support IDSPs and vehicles. The benefits of GDID are summarized as follows. First, authorized vehicles can dynamically obtain reliable intrusion detection strategies when intrusions vary along with environments. Second, for GDID, the collected reliable local datasets not only provide intelligence about local intrusions but also materials to build specialized and reliable intrusion detection strategies. Third, tasks in infrastructure providers are placed and orchestrated by the IDSPs; thus, infrastructures can provide more reliable services. Last but not least, since GDID mainly tries to construct diverse reliable intrusion detection strategies fit the local environment, traditional intrusion detection models can be reused in GDID.

Micro-Blockchain-Based Geographical Dynamic Intrusion Detection Paradigm

Overview of the Architecture

As shown in Fig. 2, the micro-blockchain-based geographical dynamic intrusion detection (MBID) paradigm contains four planes: the micro-blockchain plane, virtualization plane, control plane, and application and management plane.

- The *micro-blockchain plane* provides reliability and incentives for data collection and intrusion detection strategy deployment in MBID.
- The *virtualization plane* aims to improve the efficiency and flexibility of deploying micro-blockchain.
- The *control plane* provides micro-blockchain management service, intrusion detection statistical service, intrusion detection model uploading service, and intrusion model deployment service.

- The *application and management plane* contains application and management interfaces of the proposed MBID.

Micro-Blockchain Plane

MBID requires a mechanism that not only provides incentives to encourage users to share more intrusion detection strategies, intrusion samples, and intrusion models but also enables the reliability of these data to be ensured. Thus, we attempt to propose a blockchain plane to provide reliability and incentives for the data collection and deployment in MBID.

Traditional blockchain cannot be directly deployed in MBID for the following reasons. First, in MBID, intrusion samples and intrusion detection strategies related to a specific region and time slot need to be stored locally without introducing irrelevant data. However, a traditional blockchain node contains all the data collected by the blockchain. Second, data collected in different regions and time slots requires to be correlated easily to construct intrusion detection strategies suitable for a large region. However, deploying an independent traditional blockchain for each region leads to breaking the correlation of datasets. Third, in MBID, the data provider should be paid quickly to keep their enthusiasm for sharing reliable intrusion samples and intrusion detection strategies. However, traditional blockchain needs lots of time to confirm a transaction.

The structure of micro-blockchain architecture: Micro-blockchain architecture aims to accelerate the speed of intrusion sample collection and intrusion detection strategy deployment in small regions while keeping these data reliable. To reduce the number of blocks waiting to be confirmed and the time used to do proof of work (PoW), micro-blockchain architecture is designed as a blockchain consisting of one macro-blockchain and a large number of micro-blockchains. The region with the smallest size that needs to be analyzed is called the basic region. For micro-blockchain, it is constructed for collecting data and deploying intrusion detection strategies for users in a region that consists of several basic regions. Micro-blockchains can be nested repeatedly to form a bigger micro-blockchain to provide spatial-temporal dynamic intrusion detection service for vehicles moving from one region to another. Since micro-blockchain is responsible for efficiently collecting local data and quickly prepaying for the data, its consensus mechanism should be light. For a practical Byzantine fault tolerance (PBFT)-based consensus mechanism micro-blockchain, the following proactive mechanisms can be employed to mitigate the interfering of the voting process caused by malicious nodes. First, since the attack can only be realized by colluding more than 1/3 of the nodes in the PBFT-based blockchain, the interference can be mitigated by adding more nodes to participate in the consensus process. Moreover, increasing the cost of running the consensus process can also mitigate the interference of malicious nodes. For instance, we can require nodes who participate in the consensus process to provide a PoW. The benefit of becoming a malicious node can be smaller than the benefit of becoming a normal node when the cost of PoW is large enough. The macro-blockchain in micro-blockchain architecture is designed to store all the intrusion samples and intrusion detection strategies distributed in the system; thus, the macro-blockchain needs to be set as a traditional blockchain with a PoW consensus mechanism to keep data stored in it reliable.

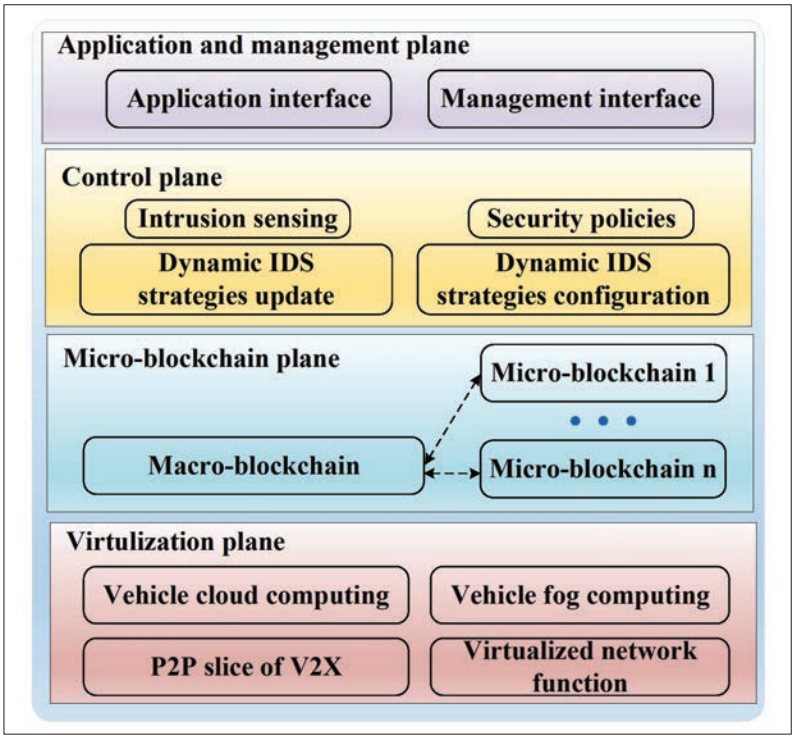

Figure 2. Micro-blockchain-based geographical dynamic intrusion detection.

Intrusion sample and intrusion detection model storage in micro-blockchain: To provide intrusion samples/intrusion detection strategies for a specific micro-blockchain, the identity of data providers needs to be checked by the nodes in the micro-blockchain. Here, the intrusion detection strategies are constructed based on intrusion detection models including RNNs, CNNs, LSTM, random forest, and so on. If the data provider is on the blacklist of a trust authority (TA) for providing fake information, its request for uploading data will be refused. Otherwise, the data provider will sign the data with its digital signature and send it to one of the nodes of the micro-blockchain. Since there are many types of intrusion samples, the intrusion samples require the use of a template to describe their content. For instance, the intrusion samples of denial of service (DoS) attacks should be described with the protocol category, flag, and so on. The nodes will organize the collected intrusion samples to the corresponding micro-blockchain. After checking the signature of the uploaded data, nodes in the micro-blockchain will package the data into a block and broadcast the block to the whole micro-blockchain. When all the nodes are confirmed, the block will be stored in the micro-blockchain. Since the micro-blockchain only stores local data and pays the data providers by themselves, the collected intrusion samples/intrusion detection models should be stored into the macro-blockchain to let the nodes in the micro-blockchain get rewards. With the macro-blockchain, the intrusion intelligence collected in one region can be reached by users in other regions. The data will be signed by every node in the micro-blockchain before being sent to the macro-blockchain. The signed data will be organized as blocks waiting to be confirmed in the macro-blockchain. To confirm a block con-

The control plane focuses on identity authentication, querying and analyzing intrusion samples in micro-blockchain, updating intrusion detection models, deploying intrusion detection strategies for vehicles and managers. To handle intrusions featured with high spatial-temporal dynamics, controllers in the control plane are organized with a distributed and hierarchical architecture.

taining data uploaded by micro-blockchains, macro-blockchain nodes will check every signature and every hash value. Once the data uploaded to the macro-blockchain is confirmed to be legal, the nodes in micro-blockchains will earn some cryptocurrency based on the volume of data uploaded to the macro-blockchain. To get paid by the macro-blockchain, all the micro-blockchain nodes also serve as macro-blockchain nodes. Different from full nodes that store the whole macro-blockchain locally, each micro-blockchain node only stores the headers of the longest macro-blockchain. They can check if they have been paid by using simplified payment verification protocol as other bitcoin-like blockchain nodes do. If the collected data is found to be illegal, the data will be abandoned, and the nodes in that micro-blockchain will be removed from the micro-blockchain. New nodes will be deployed by the TA to run that micro-blockchain by rerolling to the last correct state stored in the macro-blockchain. The newly joining nodes will be authenticated by the TA in the micro-blockchain structure. The TA can employ public key infrastructure (PKI) to provide strict identification and authentication service. The nodes running the micro-blockchain will not get paid if they keep forming blocks on the basis of the block containing illegal data.

Intrusion detection strategy deployment in micro-blockchain: Intrusion detection strategies may be modified by attackers when the strategies involve delivery to users. Hence, how to realize tamper-resistant intrusion detection strategies should be solved. The deployment of intrusion detection strategies should be realized by encrypting and storing the strategies in the micro-blockchain architecture. If a vehicle links to the micro-blockchain and has paid the intrusion strategy provider, it can get the decryption key. The vehicle can ask the TA to remove the strategy provider from the micro-blockchain network when the intrusion detection strategy does not perform as well as it has promised. The non-availability of the micro-blockchain delivery network does not affect the intrusion detection strategies that have been deployed on the vehicle. Hence, mitigations for executing security strategies for non-availability of the micro-blockchain delivery network are given as follows. First, reputation-based strategies, which do not rely on micro-blockchain, need to be embedded as basic strategies in vehicles, although these strategies might cause a large number of false alerts. Then vehicles can protect themselves by refusing to connect to entities with low reputation value. Second, the intrusion detection strategies that have been obtained from micro-blockchain should be executed to secure the vehicle. Moreover, the intrusion detection strategies of the target area need to be pre-downloaded before the vehicle goes on the road. Details on intrusion sample transition and intrusion detection strategy deployment are given in Fig. 3.

Control Plane

The control plane focuses on identity authentication, querying and analyzing intrusion samples in micro-blockchain, updating intrusion detection models, and deploying intrusion detection strategies for vehicles and managers. To handle intrusions featuring high spatial-temporal dynamics, controllers in the control plane are organized with a distributed and hierarchical architecture. Moreover, for controllers that aim to serve users in a small region, they are typically deployed on edge nodes with spatial-temporal awareness [13].

Distributed and Hierarchical Architecture: The controllers in the control plane are organized in distributed and hierarchical architecture based on the region size they dominate. Specifically, in a basic region, multiple controllers rather than a single controller are employed to serve users in this region to prevent a single point of failure. These controllers are organized in a distributed way and deployed in the low level of the control plane architecture. Moreover, to cover the demands of users living in a large region that contains several basic regions, controllers at a higher level in the control plane are required. Similarly, multiple controllers are simultaneously assigned to cover a large region consisting of several basic regions, and they are also organized in a distributed way. Controllers at a higher level manage all the low-level controllers in their large region; thus, they mainly take on the responsibility of providing services that can only be delivered in a large region or across regions.

Dynamic update: Controllers need to periodically sense the popular intrusion methods in their coverage region by analyzing the intrusion samples collected by the micro-blockchain. Following that, the controllers can construct reliable intrusion detection strategies based on the analysis results.

Scalable deployment: Since the distribution of vehicles that request intrusion detection strategies from the MBID system varies from time to time, the burden of controllers belonging to different regions is characterized by scalability. This indicates that the upper-level controllers are required to collect the demand information of low-level controllers in their coverage region in a proactive way. The upper-level controllers need to contain all the configurations on the low-level controllers and deploy low-level controllers to fulfill the demands of users in a scalable way.

Virtualization Plane

As shown in Fig. 4, micro-blockchain is built on the virtualization plane. The virtualization plane is proposed to support the reliable running of the micro-blockchain plane and control plane by providing a logical view of data collectors, storage resource, computing resource, and network resource.

In the micro-blockchain architecture, many micro-blockchains simultaneously exist in one basic region, in which each micro-blockchain requires independent storage resource, computing resource, and network resource. However, it is impractical to construct static policies of allocating network resource, computing resource, and storage resource for every edge node and a cloud center to run different types of micro-blockchains. For controllers in the control plane, the location and number of controllers in the control plane are dynamic rather than static. Thus, constructing a static resource allocation policy for an edge node or a cloud center to run controllers is impractical. Hence, the micro-blockchain plane and control plane should be constructed based on the virtualization technology.

Network slicing is built on network functions virtualization and software-defined networking techniques [14, 15]. With network slicing, each service can have a specific network that is dedicated to running the service. Thus, network slic-

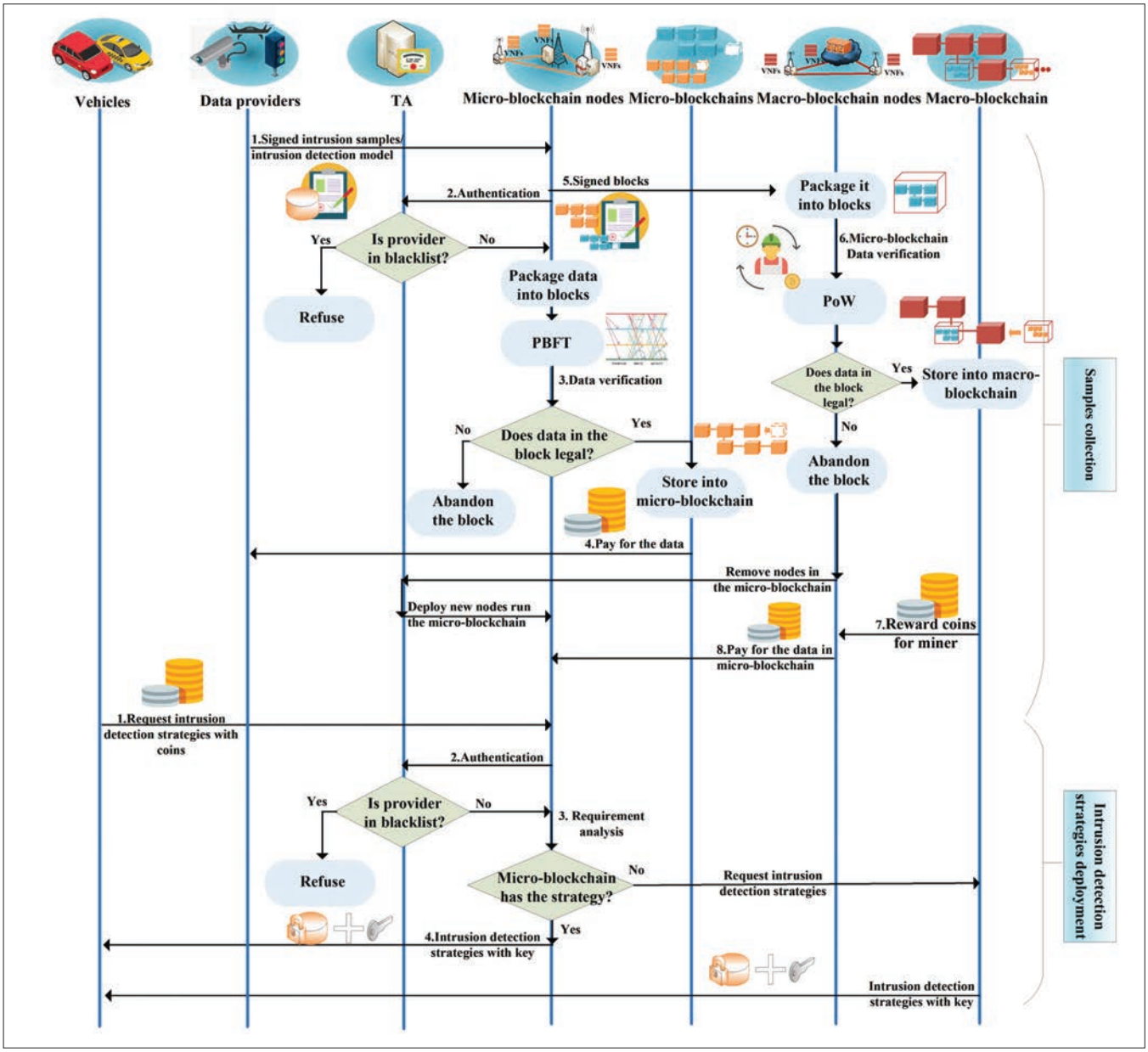

Figure 3. Intrusion sample collection and intrusion detection strategy deployment in micro-blockchain.

ing can be utilized to build peer-to-peer (P2P) networks for micro-blockchains deployed in the same region. In particular, the speed of block broadcasting can be guaranteed by constructing a unique network slice for each micro-blockchain. Moreover, virtual machines can be employed to dynamically provide computing resources for micro-blockchain nodes and controllers. By leveraging the virtual storage technique, which stores data blocks to edge nodes in a distributed manner, the problem of storing micro-blockchains with a large amount of data can be resolved.

Application and Management Plane

The application and management plane serves users with an application interface and a management interface. Specifically, when it receives requests from vehicles, it converts the requests sent by authorized vehicles to services that can be operated by the control plane. Users can obtain intrusion detection related services (e. g., intrusion detection strategies update, intrusion information analysis) and management services (e. g., removing blockchain nodes) from other planes without having to know details on how they work.

Benefit of Micro-Blockchain Architecture

In V2X scenarios, vehicles need to face a variety of attacks, which vary by time and location. Micro-blockchain enhances the security of V2X as follows. First, when the vehicle moves from one region to another, the micro-blockchain can repeatedly be nested to deliver tamper-resistant intrusion detection strategies fit for the real-time location of the vehicle. Second, the micro-blockchain structure can efficiently collect reliable intrusion detection models and intrusion samples in a specific region in a tamper-resistant way. The trusted intrusion detection models and regional intrusion samples can be used to construct reliable intrusion detection strategies for the target region. The micro-blockchain structure provides a

The trusted intrusion detection models and regional intrusion samples can be used to construct reliable intrusion detection strategies for the target region. The micro-blockchain structure provides a decentralized structure to provide intrusion detection service for the vehicles featured with distributed and frequent movement. The micro-blockchain structure eliminates a single point of failure.

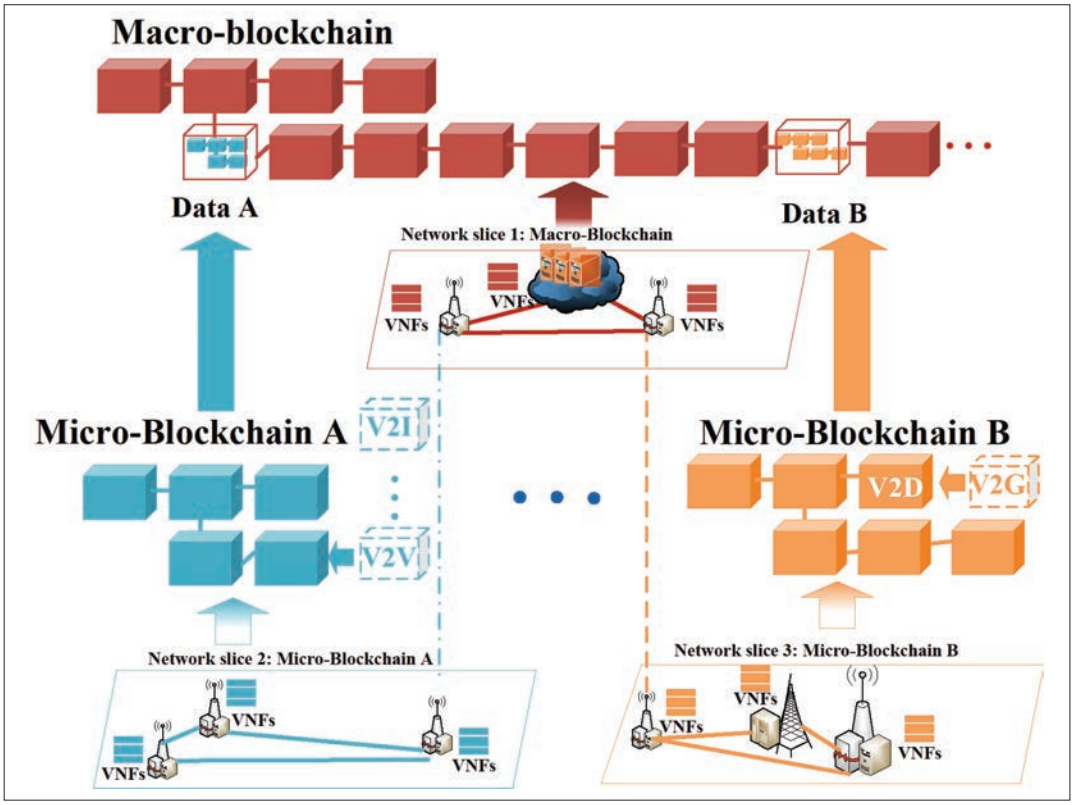

Figure 4. Virtualization-plane-supported micro-blockchain.

decentralized structure to provide intrusion detection service for the vehicles featuring distributed and frequent movement. The micro-blockchain structure eliminates a single point of failure.

Performance Evaluation

To compare the performance of MBID with regular IDS, simulation is carried out on Keras running on a cloud platform with 13,335,276 kb RAM, Tesla K80 GPU, and Intel Xeon 2.3 Ghz CPU.

Compared to regular IDS, micro-blockchain in MBID can ensure intrusion samples, which are collected to construct intrusion detection strategies, are comprehensive, and cannot be modified. Moreover, MBID dynamically deploys intrusion strategies based on location and time slot, while regular IDS deploys them in a static way. To simulate MBID, we train a classical back propagation (BP) neural network based on the original training dataset, where epoch and batch size are set as 12 and 128, respectively. To simulate regular IDS that cannot prevent tampering, we train BP neural network 1 with the same model and parameters in MBID while using modified intrusion samples, where half of the attacks are modified as normal data. To simulate regular IDS that cannot obtain enough training datasets, we train BP neural network 2 based on the incomplete intrusion samples that is half the size of the original intrusion dataset, in which the model and parameters are the same as in the neural network used in MBID. The detection rates of MBID, BP neural network 1, and BP neural network 2 are shown in Fig. 5. It can be seen that, with the same intrusion detection model, intrusion detection strategies provided by MBID are more accurate than the strategies provided by normal IDS. Moreover, MBID has the potential to provide intrusion detection strategies constructed based on other models.

Compared to the traditional public blockchain, the micro-blockchain structure is more efficient in auditing a newly gathered data block. Specifically, a public blockchain node announces for auditing a block by verifying the signatures, finding a PoW of the block, and signing the verified data. The micro-blockchain announces it by verifying the signature, creating a hash about the block and the previous block, and signing the verified data. We simulate the micro-blockchain and public blockchains using Java, in which difficulty levels of public blockchain 1, public blockchain 2, and public blockchain 3 are set as 5, 6, and 10, respectively. A difficulty level is an integer from 0 to 255, and a public blockchain with higher difficulty level requires more time to find PoW. Assume that users can get one cryptocurrency when one data block is audited by the blockchain; the relationship between the number of cryptocurrencies received by users and the time cost of one node to announce for verifying these blocks is given in Fig. 6. It can be seen that micro-blockchain spends less time in announcing a block for verifying. Moreover, users who upload data related to intrusion detection to blockchain can get more cryptocurrencies in a limited time using the micro-blockchain.

Conclusion

In V2X, the moving vehicles face geographical dynamic intrusions. In this article, we propose micro-blockchain-based intrusion detection to dynamically configure intrusion detection strategies for vehicles based on their location variation. In particular, in MBID, a micro-blockchain architecture was proposed to collect local intrusion samples that can be used to construct intrusion detection strategies fit for the current state. A control plane was proposed over the micro-blockchain architecture to dynamical-

ly deploy intrusion detection strategies for vehicles based on local intrusion information. By repeatedly nesting different micro-blockchains, micro-blockchain architecture can provide geographical dynamic intrusion detection strategies for vehicles moving from one place to another. Simulations were carried out to demonstrate that the proposed intrusion detection approach is more accurate than traditional IDS. This novel approach is significant to enhance the security of V2X.

Acknowledgement

This work was supported in part by the National Natural Science Foundation of China under Grants 61431008 and 61972255.

References

[1] J. E. Siegel, D. C. Erb, and S. E. Sarma, "A Survey of the Connected Vehicle Landscape — Architectures, Enabling Technologies, Applications, and Development Areas," *IEEE Trans. Intelligent Transportation Systems*, vol. 19, no. 8, Aug. 2018, pp. 2391–406.
[2] "Grand View Research"; https://www.grandviewresearch.com/press-release/global-automotive-vehicle-to-everything-v2x-market, 2019, accessed 15 Mar. 2019.
[3] H. Ji *et al.*, "Comparative Performance Evaluation of Intrusion Detection Methods for In-Vehicle Networks," *IEEE Access*, vol. 6, 2018, pp. 37,523–32.
[4] A. Diro and N. Chilamkurti, "Leveraging LSTM Networks for Attack Detection in Fog-to-Things Communications," *IEEE Commun. Mag.*, vol. 56, no. 9, Sept. 2018, pp. 124–30.
[5] K. Wu, Z. Chen, and W. Li, "A Novel Intrusion Detection Model for a Massive Network Using Convolutional Neural Networks," *IEEE Access*, vol. 6, 2018, pp. 50,850–59.
[6] G. Loukas *et al.*, "Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning," *IEEE Access*, vol. 6, 2018, pp. 3491–1508.
[7] K. Zaidi *et al.*, "Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection," *IEEE Trans. Vehic. Tech.*, vol. 65, no. 8, Aug. 2016, pp. 6703–14.
[8] S. Boumiza and R. Braham, "Intrusion Threats and Security Solutions for Autonomous Vehicle Networks," *2017 IEEE/ACS 14th Int'l. Conf. Computer Systems and Applications*, Hammamet, Tunisia, 2017, pp. 120–27.
[9] J. Hong and C.-C. Liu, "Intelligent Electronic Devices With Collaborative Intrusion Detection Systems," *IEEE Trans. Smart Grid*, vol. 10, no. 1, Jan. 2019, pp. 271–81.
[10] L. Li *et al.*, "CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles," *IEEE Trans. Intelligent Transportation Systems*, vol. 19, no. 7, July 2018, pp. 2204–20.
[11] H. Liu, Y. Zhang, and T. Yang, "Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing," *IEEE Network*, vol. 32, no. 3, May 2018, pp. 78–83.
[12] Z. Li *et al.*, "13.Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things," *IEEE Trans. Industrial Informatics*, vol. 14, no. 8, Aug. 2018 , pp. 3690–3700.
[13] C. Zhang and Z. Zheng, "Task Migration for Mobile Edge Computing Using Deep Reinforcement Learning," *Future Generation Computer Systems*, vol. 96, July 2019, pp. 111–18.
[14] J. Wu *et al.*, "NLES: A Novel Lifetime Extension Scheme for Safety-Critical Cyber-Physical Systems Using SDN and NFV," *IEEE Internet of Things J.*, vol. 6, no. 2, Apr. 2019, pp. 2463–75.
[15] S. Al-Rubaye *et al.*, "Enabling Digital Grid for Industrial Revolution: Self-Healing Cyber Resilient Platform," *IEEE Network*. DOI: 10.1109/MNET.2019.1800312.

Biographies

Haoran Liang received his B.S., and M.S., degrees from Jiangxi Normal University, Nanchang, China, in 2011 and 2017, respectively. Now, he is pursuing a Ph.D. degree in the School of Cyber Security, Shanghai Jiao Tong University, Shanghai, China.

Jun Wu (junwuhn@sjtu.edu.cn) received his Ph.D. degree in information and telecommunication studies from Waseda University, Japan, in 2011. He was a visiting researcher at Muroran Institute of Technology, Japan, from January 2019 to February 2019. He is currently an associate professor in the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University.

Shahid Mumtaz received his Ph.D. degree in information and telecommunication studies from Waseda University, Japan, in 2011. He was a visiting researcher at Muroran Institute of Technology, Japan, from January 2019 to February 2019. He is currently an associate professor in the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University.

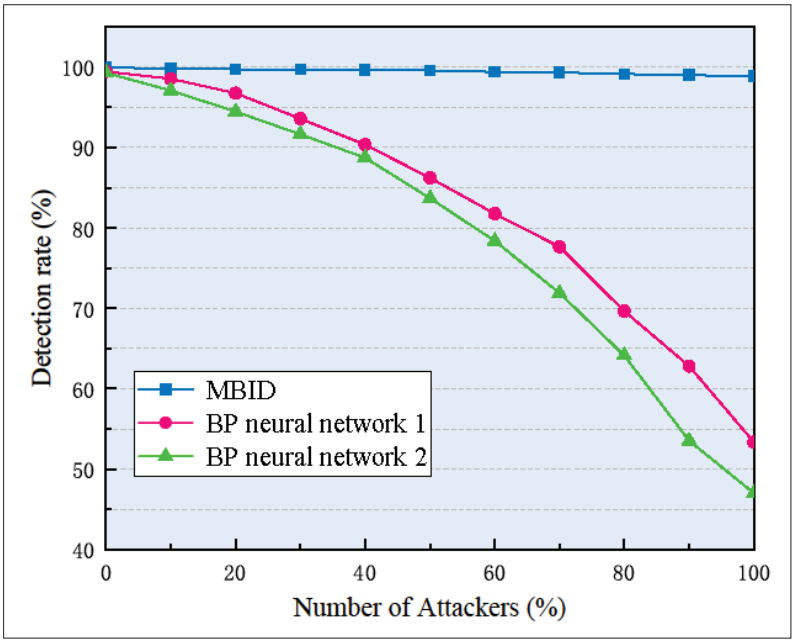

Figure 5. The detection rates of MBID, BP neural network1, and BP neural network 2.

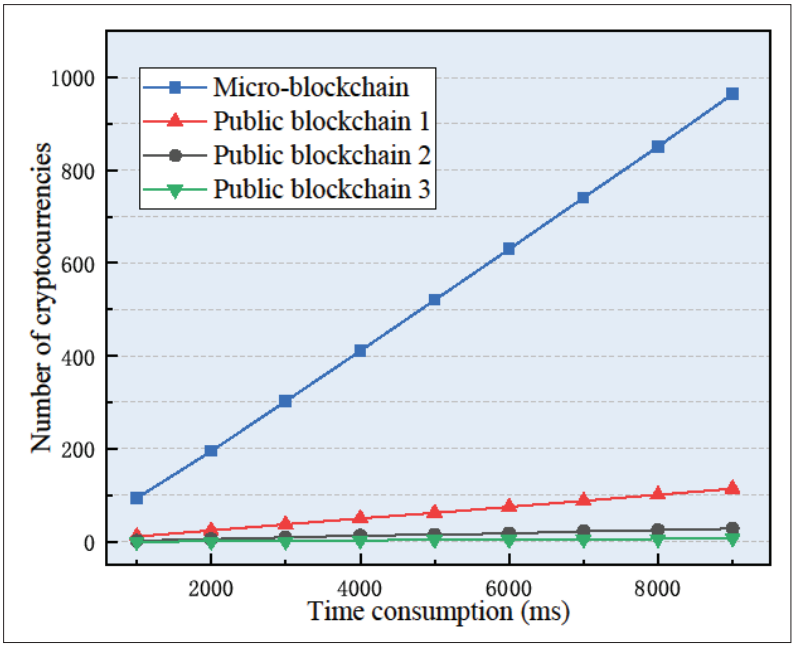

Figure 6. The relationship between the number of cryptocurrencies got by users and the time cost used to announce for verifying blocks.

Jianhua Li received his B.S., M.S., and Ph.D. degrees from Shanghai Jiao Tong University in 1986, 1991, and 1998, respectively. He is currently a professor in the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University. He got the Second Prize of the National Technology Progress Award of China.

Xi Lin received his B.S. degree from the School of Precision Instrument and Opto-Electronics Engineering, Tianjin University, China, in 2016. He is currently pursuing a Ph.D. degree with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University.

Miaowen Wen received his Ph.D. degree from Peking University, China, in 2014. From 2012 to 2013, he was a visiting student research collaborator at Princeton University. He is currently an associate professor at South China University of Technology and a postdoctoral fellow at the University of Hong Kong, China.