Received July 13, 2018, accepted August 19, 2018, date of publication September 3, 2018, date of current version November 14, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2868002

Secure Roadside Unit Hotspot Against Eavesdropping Based Traffic Analysis in Edge Computing Based Internet of Vehicles

XUMIN HUANG[1], RONG YU[1], (Member, IEEE), MIAO PAN[2], (Senior Member, IEEE), AND LEI SHU[3,4], (Senior Member, IEEE)

[1]School of Automation, Guangdong University of Technology, Guangzhou 510006, China
[2]Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77204, USA
[3]College of Engineering, Nanjing Agricultural University, Nanjing 210095, China
[4]School of Engineering, University of Lincoln, Lincoln LN67TS, U.K.

Corresponding author: Rong Yu (yurong@ieee.org)

This work was supported in part by programs of NSFC under Grant 61379115, Grant 61422201, Grant 61501127, Grant 61370159, Grant 61503083, Grant U1301255, and Grant U1501251, in part by the Science and Technology Program of Guangdong Province under Grant 2015B010129001, Grant 2015B010106010, Grant 2016A030313705, Grant 2014B090907010, and Grant 2015B010131014, in part by the Special-Support Project of Guangdong Province under Grant 2014TQ01X100, in part by the Science and Technology Program of Guangzhou under Grant 2014J2200097, and in part by the U.S. National Science Foundation under Grant US CNS-1343361, Grant CNS-1350230 (CAREER), Grant CNS-1646607, Grant CNS-1702850, and Grant CNS-1801925.

ABSTRACT Edge computing-based Internet of Vehicles (EC-IoV) has emerged when computing environment is extended to vehicular network edge for supporting compute-intensive applications. To implement EC-IoV, roadside units (RSUs) are enhanced and upgraded toward edge computing infrastructures with hardware improvements. RSU is a crucial component to communicate with and serve vehicles in EC-IoV. However, RSUs easily suffer from potential network attacks. The attacks lower the quality of user experience, disrupt RSU workload scheduling and even result in user information leakage. Due to the open deployment environment, network traffic among all RSUs may be eavesdropped by a global adversary. When a hotspot phenomenon causes heavy traffic to an RSU, the adversary could take advantage of traffic statistics to locate the RSU. After that, the adversary may concentrate to attack the RSU and try to interrupt on-going services. As a consequence, *RSU hotspot attack* with traffic eavesdropping is launched. In this paper, we focus on such a new adversary model in EC-IoV and discuss the attack and its defence. To prevent from the attack, we propose a proactive scheme by generating dummy traffic delivery. The local vehicles are collaborative and encouraged to send dummy packets to specified RSUs. This dummy traffic will mislead the traffic statistics and protect hospot RSUs. Stackelberg game approach is used to build an incentive mechanism in the scheme. Numerical results demonstrate that our scheme is effective and efficient to secure EC-IoV against RSU hotspot attack.

INDEX TERMS Edge computing, network security, vehicular and wireless technologies, collaborative work.

I. INTRODUCTION

As a vital branch of Internet of Things, Internet of Vehicles (IoV) has been developed as an open and integrated platform to enable great information interactions among humans, vehicles, things and environment for improving network intelligence and sustainability. IoV promotes safety and efficiency of transportation, improves user experience and enriches vehicular services in smart cities [1]. However, with the increasing number of global vehicles that act as data consumers/producers simultaneously, huge quantities of data is generated and needs to be processed with strict requirements, e.g., low latency and bandwidth consumption. This highly requires more functionalities at the network edge of IoV. To cope with the issues, recent work focus on integrating edge computing technologies into IoV for extending computing environment to the network edge, and thus leading to a new paradigm named Edge Computing based IoV (EC-IoV). In EC-IoV, localized data processing can be achieved to improve overall performance during service provision. Compute-intensive applications are facilitated well with ultra-low service latency, pervasive network connectivity and diverse awareness support. Nowadays, EC-IoV has been widely applied to support a variety of key services, e.g., autonomous driving [2], augmented reality [3] and computation offloading [4].

Roadside unit (RSU) is an essential component to facilitate network functionalities of EC-IoV. RSUs are enhanced by adding extra processing capabilities and upgraded toward accessible edge computing infrastructures in EC-IoV [5], [6]. After that, RSUs are able to handle packet forwarding and localized data processing. Then RSU plays a critical role in EC-IoV. RSUs are deployed in hotspot regions to act as gateways to the backbone network. RSUs establish communication channels between service providers and mobile vehicles. Moreover, enhanced RSUs are capable of directly processing some user requests instead of forwarding all of them to the network core.

In fact, RSUs easily suffer from potential network attacks. First, when an RSU is destructed, on-going services are procrastinated. Local vehicles have to travel to other RSUs for services. This significantly lowers quality of experience for users. Second, unexpected service requests are transferred to nearby RSUs. Load imbalance among the RSUs will be further worse and worse [7]. Then, original workload scheduling of RSUs will be disrupted. It may have cascading impact on the following up service provision as well. Last but not least, RSUs are used for collecting status information of vehicles [8], e.g., safety messages. If RSU is compromised, sensitive information is leaked out. However, security protection of RSUs is seldom investigated in existing researches. Previous work mainly focus on how to minimize the number, and optimize deployment locations and scheduling of RSUs.

The security threats for RSUs have the following key features:

- *Continuous Eavesdropping:* Vehicles communicate with RSUs via license-free wireless spectrum when they are within the valid transmission range [9]. In the open environment, an adversary is convenient to passively eavesdrop the communications [10]. Traffic information of RSUs can be acquired as prior knowledge for assisting in making decisions.
- *Distinguishable Target:* For the adversary, a target RSU should have distinguishable characteristics to be located. It is not feasible for the adversary to launch attacks for all the RSUs regardless of the cost.
- *Concentrated Efforts:* Due to the constrained capabilities, it is reasonable for the adversary to attack a limited number of RSUs. Limited efforts are concentrated to cause interference even interruptions to on-going services.

Based on these simple but typical features, we propose a new adversary model, called RSU hotspot attack, in which a global adversary eavesdrops wireless communications and records network traffic to monitor, locate and attack a target RSU. The adversary uses traffic statistics to locate the target RSU with the maximum amount of receiving packets. As a consequence, the adversary may concentrate to destroy the normal communications of the target RSU. To prevent from the attack, we design a proactive defense scheme by generating dummy traffic delivery. Taking the advantage of dummy traffic, the scheme aims to obfuscate the statistics in the traffic pattern, and thus the target RSU can be effectively hidden. To do so, local vehicles are collaborative to send dummy packets to corresponding RSUs, leading to dummy traffic in the defense scheme. Besides, an incentive mechanism is used to encourage vehicles to participate. We present Stackelberg game approach to formulate the interactions between RSUs and participating vehicles. Each RSU not only acts a leader to minimize its overall cost but also considers utility maximization for participating vehicles. The main contributions of this paper are summarized as follows.

- Considering the features of EC-IoV, we introduce a novel RSU hotspot attack with traffic eavesdropping and emphasize the severe damages to EC-IoV.
- In RSU hotspot attack, an adversary model with a multiphase attack procedure is presented to illustrate the attack.
- Stackelberg game approach is employed to optimize the incentive mechanism for participating vehicles with respect to the collaborative dummy traffic delivery scheme. Stackelberg equilibrium analysis is also provided.
- Extensive simulations show that the proposed scheme with the Stackelberg game approach is effective and efficient to secure EC-IoV against RSU hotspot attack.

The rest of this paper is organized as follows. Section II presents the related work. The system model of EC-IoV is introduced in Section III. We present RSU hotspot attack with the adversary model and attack procedure in Section IV. We employ the Stackelberg game to develop the incentive mechanism for our proposed collaborative dummy traffic delivery scheme in Section V. Numerical results and analysis are provided in Section VI. Finally, we draw the conclusion in Section VII.

II. RELATED WORK

A. SECURITY THREATS FOR RSUS IN EC-IoV

The increasing risk of RSUs is resulted in EC-IoV when the new networking paradigm is emerged and applied widely. Recently, EC-IoV has been proposed by integrating edge computing technologies into existing IoV. To realize EC-IoV, enabling technologies mainly consist of mobile edge computing and fog computing. In particular, with the help of fog computing technology, RSUs are upgraded towards available edge computing infrastructures for facilitating EC-IoV.

The detailed concept, applications and key technologies of mobile edge computing are found in the white paper published by the standards organization European Telecommunications Standards Institute (ETSI) [11]. Owing to significant advantages, mobile edge computing has been introduced for improving compute-intensive and time-sensitive vehicular services. For example, mobile edge computing is regarded as the ideal solution to assist in road safety services so that ultralow-latency (below 1 ms) traffic alerts can be supported [12]. Besides, mobile edge computing servers enable localized data processing in vehicular networks. According to previous work, the servers can execute tasks in computation offloading [13], realize distributed reputation management [14] and promote electric vehicle discharging/charging management [15].

Fog computing is also a prominent technology for achieving EC-IoV. Hou *et al.* [16] introduced the concept of vehicular fog computing. They considered vehicles as near-user infrastructures to carry out a certain amount of communication and computation tasks. Vehicular fog computing is proposed to make the best utilization of these vehicular resources by optimizing collaboration among special vehicles, i.e., slow-moving and parked vehicles. In addition, the work in [5] and [6] considered that existing network infrastructures, e.g., common router (including RSU), can also be upgraded to become edge computing infrastructures with adequate hardware improvements. Then RSUs are enhanced with extra processing capabilities to offer sufficient computation resources for localized data processing when necessary. Local requests are able to be directly processed with fleet response and lower latency. Hence, RSUs exhibit significant potentialities to act as a vital enabler for the implementation of EC-IoV.

However, RSUs tend to suffer from security challenges in EC-IoV environment as they are assigned with two-fold responsibilities, consisting of packet forwarding and data processing simultaneously. RSU is a crucial component for the wide application of EC-IoV and generally deployed in the open environment. So it naturally becomes a target of an adversary and faces with potential security threats. Compared with current work, our work focus on identifying a new security challenge regarding RSUs in EC-IoV. We introduce RSU hotspot attack with traffic eavesdropping, wherein the adversary utilizes traffic statistics to locate a target RSU and concentrates to attack it. The adversary tries to interrupt on-going services in EC-IoV.

B. SEVERE DAMAGES CAUSED BY RSU ATTACKS TO EC-IoV

At the network edge, computing environment around mobile vehicles will be influenced due to RSU attacks in EC-IoV. When an RSU is destructed, local requests cannot be processed and normal service provision has to be terminated. This clearly leads to low-level quality of user experience. RSU workload scheduling is also disrupted as unexpected and external user requests are transferred from the RSU to nearby RSUs. Besides, the compromised RSU may reveal sensitive information of users when the RSU is employed to monitor passing vehicles in EC-IoV.

Moreover, existing work have considered that RSUs are crucial for ensuring network performances and different RSU optimizations are studied. Nowadays, the researchers pay attention to RSU optimizations in deployment and scheduling scenarios. One one hand, due to the critical roles of RSUs, the appropriate distribution of RSUs is of paramount importance. So a certain number of RSUs should be deployed at considerate locations for overall performance. The work in [17] and [18] considered the optimal RSU deployment in highways and hybrid VANET-sensor networks. Besides, RSU scheduling is optimized when RSUs play various roles in vehicular networks. For example, RSUs can be used for data dissemination in [19]. The authors proposed an improved cooperative load balancing approach among the RSUs to lower overall request drop rates for vehicles. Many RSU-aided schemes have also been proposed to provide security guarantee for mobile vehicles as RSUs are exploited for message authentication [20], key generation [21] and certificate revocation [22]. The corresponding scheduling optimizations were introduced for efficient utilizations of RSUs. Once there exist launched attacks for RSUs, the above RSU optimizations are greatly weaken. Finally, inevitable performance degradation is caused in the network.

C. GLOBAL ADVERSARY IN RSU HOTSPOT ATTACK

In this paper, we consider that RSU hotspot attack derives from a global adversary. Based on the descriptions in [10], a global adversary has a complete view of the monitored network and is perhaps the most popular threat model for resulting in network vulnerability.

Similarly, the adversary in RSU hotspot attack is such a global adversary. It holds the remarkable capability of global traffic analysis by observing the traffic patterns of different RSUs over the whole network. In vehicular environment, the global adversary only passively eavesdrops all the communications. Sufficient monitoring devices are necessarily deployed at fixed locations. For eavesdropping, this consumes an accepted amount of energy in regular operations. The global adversary is also aware of the locations of all the RSUs. Then the global adversary detects coexisting communication channels and may correlate a sender and receiver of each packet [23]. It cannot interpret the encrypted packets but is able to acquire traffic information between RSUs and local vehicles as prior knowledge via continuous eavesdropping.

The prior knowledge is easily utilized by the global adversary to locate a target RSU staying busy. In the presence of the global adversary, traffic statistics about various RSUs are known. At the same time, status information of all the RSUs corresponding to traffic density is revealed to the global adversary. The global adversary would like to concentrate to attack the RSU with the busiest state for causing interference even interruptions to on-going services.

III. SYSTEM MODEL

A. NETWORK COMPONENTS

Figure 1 illustrates a typical network of implementing EC-IoV, which a global adversary draws attention to. As a crucial network component, RSU plays a key role in facilitating network functionalities. On one hand, RSUs are deployed at hotspot regions, e.g., gas stations, parking

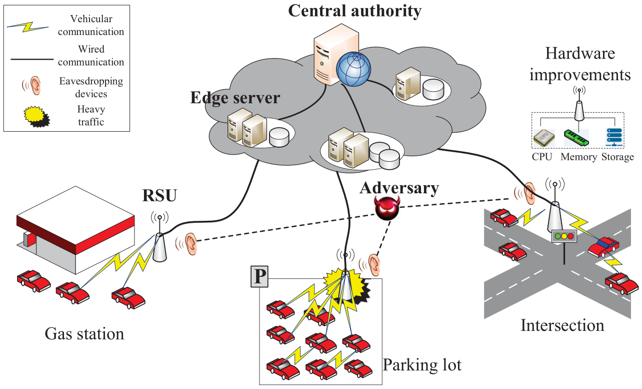


FIGURE 1. Edge computing based IoV.

lots and intersections. They act as pivotal coordinators during service provision. Vehicles transmit requests to and receive packets from the nearest RSUs via existing vehicular communications. RSUs upload them to corresponding service providers via wired communications. In turn, service providers respond to vehicles with the help of RSUs. In EC-IoV environment, service providers directly process user requests by employing edge servers in EC-IoV, whose decision-making capabilities benefits from hardware improvements of RSUs. Besides, there exists a central authority acting as the top security manager to ensure network-wide security protection. In the meantime, a global adversary distributes eavesdropping devices near each RSU and thus, communication channels between local vehicles and RSUs are detected. More details about the network components of EC-IoV are described as follows.

- *RSU:* With the increasing edge responsibilities, RSUs are enhanced with processing capabilities based on generic application purposes, in addition to just forwarding packets. In EC-IoV, RSUs are configured with hardware equipment, e.g., CPU, a number of cores, memory size, storage capacity and so on. In this way, enhanced RSUs are of extra and sufficient physical resources. Then edge servers are emerged and co-locate in the RSUs by further virtualizing these physical resources.
- *Edge Server:* Advanced network function virtualization technology can be utilized for manipulating the edge servers. The virtualization technology provides administrators with the ability to manually establish virtual machines for computing instances. Software defined networking technology is also exploited to schedule available resources among the virtual machines dynamically. Thus, creating, migration, offloading and destroying of virtual machines are optimized according to different network states. In short, the comprehensive technologies enable that service providers are capable of localized data processing for proximal users with a higher efficiency.
- *Central Authority:* The central authority is a public and authentic organization trusted by all the other entities, including vehicles, RSUs and service providers. All the entities should register with it to acquire legal identities. In particular, the central authority employs a part of dedicated edge servers to execute regular operations for facilitating network management. For example, for secure communications, the central authority delegates multiple edge servers to locally generate and distribute public/private keys, a set of pseudonyms, digital signatures and certificates for the legal entities.
- *Vehicle:* By using vehicle-to-vehicle and vehicle-to-infrastructure communications, vehicles interact with nearby RSUs within the valid communication range. The requests are directly processed by the edge servers in EC-IoV. Owing to proximal communications and prompt processing, a wide range of compute-intensive services can be provisioned well in EC-IoV. Moreover, local vehicles may send numerous requests to an RSU simultaneously when popular events stimulate the common interests.
- *Global Adversary:* A mass of vehicles are served by an RSU in a hotspot phenomenon. The RSU will receive much more packets from local vehicles in a certain time period. This gives rise to an obvious inconsistency in the network traffic pattern among all the RSUs. By monitoring network traffic, the adversary utilizes traffic statistics to locate and attack the RSU with heavy traffic. From the viewpoint of the adversary, more receiving packets demonstrates that there exist more on-going services connecting to the RSU. Based on concentrated efforts, the interference, or even interruptions can be maximized for current services.

B. HOTSPOT PHENOMENON IN EC-IoV

For an RSU, it may become a target RSU of the adversary when local popular events lead to a large number of simultaneous requests. We take an example to clarify the existence of such a hotspot phenomenon. When there exists a sale promotion of a supermarket in the weekend, a location-based service provider appoints edge servers in an RSU to issue and announce this activity to passing vehicles. Most of nearby vehicles are exactly attracted to request for more details on the sale promotion. A lot of requests are sent to the RSU. During service provision, the RSU clearly communicates with requesting vehicles for further enriching user satisfaction. The frequent requests result in continuous communications between the RSU and local vehicles. The RSU receives much more packets than other normal RSUs within the same time interval. As a consequence, the hotspot phenomenon causes heavy traffic to the RSU. For the adversary, a target RSU also appears after realizing the obvious traffic inconsistency among all the RSUs.

In this paper, we consider that many complex factors are mixed together to induce a hotspot phenomenon in EC-IoV, and the subsequent advent of the target RSU. The typical factors consist of time frame, traffic density and user profiles. In general, all the factors can be divided into dynamic and static, regular and random, and external and internal. They are triggered and at work to form a hotspot RSU that ceaselessly interacts with most of local vehicles in the following time slots. Hence, any RSU in a region may become the target RSU in RSU hotspot attack as popular events make a great impact on the network traffic in EC-IoV.

IV. RSU HOTSPOT ATTACK

In RSU hotspot attack, a global adversary aims to locate a target RSU by making use of traffic statistics in a hotspot phenomenon. RSU hotspot attack is speculative and the procedure is comprised of several phases: initialization, monitoring, analysis and attack. As shown in Fig.2, we provide more details about flow chart of the phases as follows.

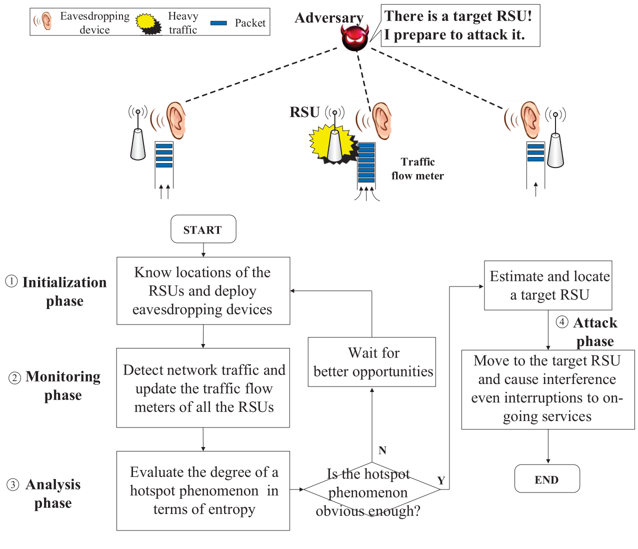

Eavesdropping device
Heavy traffic
Packet
Adversary
There is a target RSU! I prepare to attack it.
RSU
Traffic flow meter
START
① Initialization phase
Know locations of the RSUs and deploy eavesdropping devices
② Monitoring phase
Detect network traffic and update the traffic flow meters of all the RSUs
③ Analysis phase
Evaluate the degree of a hotspot phenomenon in terms of entropy
Is the hotspot phenomenon obvious enough?
N
Y
Wait for better opportunities
Estimate and locate a target RSU
④ Attack phase
Move to the target RSU and cause interference even interruptions to on-going services
END

FIGURE 2. Adversary model in RSU hotspot attack.

A. INITIALIZATION PHASE: DEVICE DEPLOYMENT

In the initialization phase, locations of all the RSUs are known to the adversary in advance. To acquire traffic information, the adversary deploys plenty of eavesdropping devices near the RSUs to detect communication channels in real time. Then a network-wide traffic monitoring is achieved.

B. MONITORING PHASE: TRAFFIC EAVESDROPPING

In the phase, the adversary needs to monitor the network traffic continuously to hold sufficient prior knowledge. As mentioned above, the complex factors for the advent of a target RSU in the hotspot phenomenon consist of predictable and unpredictable factors. It is a tough task for the adversary to forecast the hotspot phenomenon. Locating a target RSU by prediction tends to be much more infeasible. Thus, the adversary should eavesdrop on network traffic over time to cumulative the knowledge. The procedure of knowledge cumulation refers to update traffic flow meters of every RSU. In other words, for an RSU, the amount of receiving packets is recorded.

Here, each eavesdropping device is enhanced by being equipped with antenna, spectrum analyzers and decision-making module. The eavesdropping device realizes vehicles in the proximity of an RSU, and intercepts appeared packets in the monitoring area. Once a packet is transmitted, both the angle of packet arrival and the strength of the transmission signal are extracted well. So the eavesdropping device can determine the location of the source vehicle [24]. Then all the entities including nearby vehicles and the RSU within the estimated transmission range become the potential receiver. Furthermore, the eavesdropping device exploits time correlations proposed in [25] to infer whether the packet is uploaded to the RSU. Ultimately, the eavesdropping device measures traffic statistics about the RSU in a feasible way. At the end of an observing time period, real-time network traffic information of all the RSUs is transmitted to and gathered by the adversary.

C. ANALYSIS PHASE: DECISION MAKING

The adversary makes a decision on whether to launch the attack in the analysis phase. With rationality, the adversary always determines whether to launch the attack by evaluating the degree of hotspot phenomenon. Only when there exists an obvious hotspot phenomenon, the adversary is willing to attack. We consider that the adversary uses entropy to quantify the degree of hotspot phenomenon. Entropy is an information-theoretic metric, which has been used widely in previous studies about security and privacy issues. According to the theory in [26], with the lower entropy, the hotspot phenomenon is easier to be observed. Traffic inconsistency is more apparent to be realized. The adversary is also convenient to identify the existence of the target RSU and locate it.

For all the RSUs, the various amounts of receiving packets are detected in real time. In a given observing time period t, there exists a hotspot phenomenon in the network. At the end of the time period, for RSU i, its detected amount of receiving packets is denoted as σ_i^t. The adversary regards the RSU as a target RSU based on the probability $p_i = \sigma_i^t / \sum \sigma_i^t$. Then the degree of the hotspot phenomenon is calculated in terms of entropy, $H = -\sum p_i \log p_i$. The entropy is to indicate traffic distribution among all the RSUs. If the entropy is lower enough at that time, the adversary will realize an obvious hotspot phenomenon and determine to take actions subsequently. Then the RSU with the maximum amount of receiving packets becomes a target. Otherwise, the adversary keeps monitoring and waits for better opportunities.

D. ATTACK PHASE: INTERFERENCE CREATION

Because of the constrained capabilities, the adversary prefers to launch a concentrated attack for RSUs in the network. The adversary may have the proposed time-and-budget limitations in [27]. Hence, it may be intellectual for the adversary to concentrate to attack one specified RSU instead of several RSUs in the network. Clearly, the adversary tries to choose the above target RSU for maximizing the interference for on-going services. By distinguishing the amounts of receiving packets in a time period, the target RSU is identified and located. At the beginning of the next time period, the adversary moves to the target RSU and tries to impede its norm operations. The adversary does some severe damages, e.g., interfering communication channels of the target RSU. This aims to cause frequent interference, or even interruptions to current services provisioned by the RSU.

V. PROACTIVE DEFENSE BY GENERATING DUMMY TRAFFIC DELIVERY

To prevent from RSU hotspot attack, a proactive defense scheme is designed to ensure security protection for EC-IoV. A global adversary eavesdrops on the entire network traffic and exploits traffic statistics to instruct the actions, including realizing the existence of and locating a target RSU. To mislead the adversary, we propose collaborative dummy traffic delivery (CDTD) scheme to obfuscate traffic statistics in the traffic pattern. Similar technique has been used in [24]. Hence, the target RSU can be effectively hidden owing to the CDTD scheme.

A. BASIC PRINCIPLE

According to the adversary model, the adversary determines whether to take actions and locate a target RSU assisted by traffic statistics in real time. By evaluating the degree of a hotspot phenomenon, the adversary judges whether there exists obvious traffic inconsistency among all the RSUs. If there exists, the adversary locates the target RSU with the maximum amount of receiving packets. Based on the consideration, it is a great way to throw dummy traffic in the adversary's eyes on observing network traffic. By introducing dummy traffic into the network, traffic statistics about the RSUs will be obfuscated in the created disguise. The degree of hostpot phenomenon is ''modified'' and the adversary has no valid motivations to launch the RSU hotspot attack. Finally, the target RSU is hidden to avoid security threats.

The CDTD scheme is executed by RSUs when the scheme is triggered to secure EC-IoV against potential RSU hotspot attack. In particular, the central authority employs specialized edge servers to perform regular operations in the defense scheme. The central authority assigns the edge servers in the RSUs to record traffic information in each presetting time period. At the end of a time period, all the traffic information is gathered to calculate the observing entropy. The central authority also judges whether there exists an obvious phenomenon resulting in that the entropy is lower than a specified threshold value. If there exists, the central authority will also know which RSU becomes a target RSU by comparing with the various amounts of receiving packets. Then residual RSUs are allocated to generate dummy traffic.

More specially, each RSU except the target RSU schedules local vehicles to send dummy packets to it. Within the valid transmission range, local vehicles communicate with the RSU during service provision. As the defense scheme is active, they should be collaborative to send a specified amount of dummy packets along with transmitting normal packets. To accomplish the high-workload dummy packet transmission task, a single vehicle is largely insufficient so the collaboration among the local vehicles is required. Besides, dummy packets can also be bound with normal packets to transmit. All the dummy packets will be attached with a special identification to differ from norm packets. Then the RSU identifies dummy packets and ignores processing them. At this point, on-demand dummy traffic is able to be generated via collaboration of local vehicles for misleading the adversary, and avoiding minor disturbance to current services. But dummy packet transmission gives rise to energy consumption and unnecessary inconvenience for local vehicles. Thus, a considerate incentive mechanism is required to encourage vehicles to participate and guarantee the feasibility of the scheme. We list the notations that will be used in the rest of this paper in Table 1.

TABLE 1. Summary of key notations.

Notation	Description
$\mathcal{G}_i$	A group of vehicles served by RSU i.
$\vert\mathcal{G}_i\vert$	Group size of $\mathcal{G}_i$.
v_j^i	The j^{th} member belonging to $\mathcal{G}_i$.
x_j^i	The amount of dummy packets sent by v_j^i.
U_j^i	Utility function of v_j^i for participating in the CDTD scheme.
R_i	The total rewards offered by RSU i for all the participating vehicles in $\mathcal{G}_i$.
c_j	Data transmission cost of v_j^i for sending one-unit dummy packet.
θ_j	Inconvenience parameter of v_j^i to send dummy packets when running applications.
d_i	The maximum amount of dummy packets required by RSU i.
r_i	Risk parameter of RSU i to indicate degradation for the CDTD scheme caused by receiving insufficient dummy packets.
C_i	Cost function of RSU i in the CDTD scheme.

B. STACKELBERG GAME APPROACH

In the incentive mechanism, reward policy should be set for stimulating local vehicles to participate in our defense scheme. After the defense scheme is triggered, an RSU encourages local vehicles to send dummy packets to it, resulting in dummy traffic. Facing with various reward policies, vehicles response with different participation levels in the scheme according to their acquired utilities. Next, we formulate a utility function of one participating vehicle in the CDTD scheme.

In the coverage of RSU i (RSU i is not a target RSU), there exist a group of served vehicles. The group is denoted as $\mathcal{G}_i$ and a member in the group is v_j^i, $j \in \mathcal{G}_i$, becomes a participating vehicle in the CDTD scheme. For v_j^i, its participation level is optimized to maximize the individual utility. The participation level is to indicate the amount of sending dummy packets, x_j^i. x_i^j is a vital decision variable to influence the final utility in the scheme. Clearly, the utility is related with acquired rewards and data transmission cost when sending dummy packets to the RSU. On one hand, for fairness, the individual rewards are linear with the percentage about x_i^j in the summation of x_i^j. For dummy packet transmission, the vehicles should consume some energy corresponding to the amount of transmitted dummy packets. Let c_j represent the data transmission cost for sending one-unit dummy packet. Then the data transmission cost is $c_j x_j^i$. Meanwhile, during the service provision, the vehicle needs to bind the dummy packets with normal packets for simultaneous transmission. As a consequence, extra packet processing gives rise to unnecessary inconvenience on carrying out private service of the vehicle. We consider that such a temporary participation has a negative effect for regular service provision. Similar assumption can be found in [28]. The negative effect causes incurred inconvenience to the vehicle, which is modeled as $\theta_j x_j^{i2}$. θ_j is an inconvenience parameter to formulate the impact for running applications due to the participation. Based on the overall considerations, the utility function U_j^i is equal to the external economic benefits minus the internal inconvenience and expressed by

$$U_j^i = \frac{x_j^i}{\sum\limits_{j\in\mathcal{G}_i} x_j^i} R_i - c_j x_j^i - \theta_j x_j^{i2}. \tag{1}$$

Here, R_i is the total rewards offered by RSU i for all the participating vehicles in $\mathcal{G}_i$. In particular, local RSU i collects all the responses (i.e., $\sum\limits_{j\in\mathcal{G}_i} x_j^i$) from participating vehicles in the CDTD scheme. Then the gathered responses are transferred to each of them for assisting in making decisions.

As for the RSU, its utility function is mainly represented by the overall cost after getting $\sum\limits_{j\in\mathcal{G}_i} x_j^i$ dummy packets via the collaboration of all the participating vehicles. The overall cost C_i is divided into two aspects in the scheme. A part of C_i is directly related with monetary expense of assigning the participating vehicles, R_i. Besides, when the given total rewards R_i is not attractive, this gives rise to a lower value of $\sum\limits_{j\in\mathcal{G}_i} x_j^i$. Plenty of dummy traffic is not satisfied well and this consequently results in a lower efficiency of the scheme. So there exists a risk level when total amount of dummy packets cannot be matched with respect to d_i. Here, if the defense scheme is triggered at the end of a time period t, for RSU i, the required amount of dummy packets is limited by $d_i = \max\ (\sigma_i^t) - \sigma_i^t$. d_i is to avoid too many dummy packets in the CDTD scheme. The bigger difference between $\sum\limits_{j\in\mathcal{G}_i} x_j^i$ and d_i degrades the defense scheme and leads to a higher risk level in the network. Then the risk level is formulated by $r_i(d_i - \sum\limits_{j\in\mathcal{G}_i} x_j^i)$, where r_i is a risk parameter to point out the negative impact caused by insufficient dummy packets of an RSU when trying to improve the observing entropy H. According to the theory of entropy, the great improvement of H depends highly on whether those RSUs with lower values of σ_i^t can achieve many enough dummy packets in time. This means that for those RSUs with lower values of σ_i^t, their risk levels are higher when the related amounts of dummy packets are deficient. Thus, r_i can be calculated by

$$r_i = \alpha e^{\beta(\max(\sigma_i^t)-\sigma_i^t)}, \tag{2}$$

where α and β are two presetting constants for adjustment. The RSU prefers to avoid inefficiency and reduce monetary expense of the scheme jointly. To summarize, the overall cost C_i is shown by

$$C_i = r_i(d_i - \sum_{j\in\mathcal{G}_i} x_j^i) + R_i. \tag{3}$$

To perform the incentive mechanism well, Stackelberg game approach is utilized in this paper. For RSU i, it aims to minimize its overall cost by acquiring the optimal solution of the crucial reward parameter R_i, which has a positive effect on the total participation levels of vehicles $\sum\limits_{j\in G_i} x_j^i$. In turn, participating vehicle v_j^i responses with the participation level x_j^i to maximize its utility. Based on all the gathered responses, the RSU adjusts R_i when necessary. This means that in the incentive mechanism, the RSU is naturally fit for acting a leader to determine the final reward policy while the participating vehicles become followers responding to the RSU with respect to given rewards. Hence, the interaction between the RSU and all the participating vehicles can be formulated as a typical two-stage leader-follower game in the scheme. According to the work in [29], a Stackelberg game model is a convenient analytical model to study the above scenario.

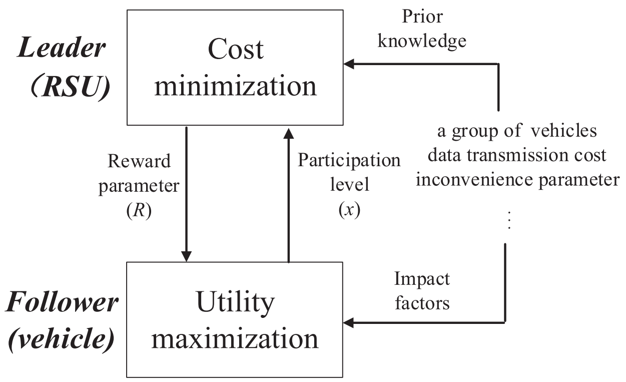


FIGURE 3. **A Stackelberge Game model for the incentive mechanism.**

As shown in Fig. 3, the RSU acts as a leader while all the participating vehicles are multiple followers in the Stackelberg game model. For cost minimization, the leader determines the optimal reward parameter R_i^* based on prior knowledge about the impacts of the decision on behavior of the followers. In the CDTD scheme, the impacts derive from group construction, data transmission cost and inconvenience parameter. Each follower is stimulated to react to the leader and put forward the best participation level x_j^{i*} for utility maximization. Next, we exploit the Stackelberg game theory approach to analyse the best responses of the leader and followers, respectively.

C. STACKELBERG EQUILIBRIUM ANALYSIS

The objective of the proposed Stackelberg game between an RSU (e.g., RSU i) and a participating vehicle (e.g., $v_j * i$) is to find the unique Stackelberg equilibrium where both the RSU and vehicle have no motivations to unilaterally change their decisions. For the game, we define the Stackelberg equilibrium as follows:

Definition 1: A set of strategies (R_i^*, x_j^{i*}) can be regarded as the Stackelberge equilibrium, if and only if it satisfies the following set of inequalities:

$$\begin{aligned} \forall R_i, \quad & C_i(R_i^*, x_j^{i*}) \leq C_i(R_i, x_j^{i*}) \\ \forall x_j^i, \quad & U_j^i(R_i^*, x_j^{i*}) \geq U_j^i(R_i^*, x_j^i). \end{aligned}$$

We firstly analyse the best response of a follower in the game. For v_j^i, differentiating U_j^i with respect to x_j^i, we obtain

$$\begin{aligned} \frac{\partial U_j^i}{\partial x_j^i} &= \frac{\sum\limits_{k \neq j, k \in \mathcal{G}_i} x_k^i}{(\sum\limits_{j \in \mathcal{G}_i} x_j^i)^2} R_i - c_j - 2\theta_j x_j^i \\ \frac{\partial^2 U_j^i}{\partial x_j^{i2}} &= -2 \frac{\sum\limits_{k \neq j, k \in \mathcal{G}_i} x_k^i \sum\limits_{j \in \mathcal{G}_i} x_j^i}{(\sum\limits_{j \in \mathcal{G}_i} x_j^i)^4} R_i - 2\theta_j < 0 \end{aligned} \tag{4}$$

Clearly, the utility function of v_j^i is concave, which indicates that the maximal value of U_j^i exists. Therefore, using the first-order optimality condition $\partial U_j^i / \partial x_j^i = 0$, we have

$$\frac{\sum\limits_{k \neq j, k \in \mathcal{G}_i} x_k^i}{(\sum\limits_{j \in \mathcal{G}_i} x_j^i)^2} R_i - 2\theta_j x_j^i = c_j. \tag{5}$$

Summing up Eqn. (5) over all the vehicles in the group $\mathcal{G}_i$, we easily get

$$\frac{(|\mathcal{G}_i| - 1)}{\sum\limits_{j \in \mathcal{G}_i} x_j^i} R_i - 2 \sum_{j \in \mathcal{G}_i} \theta_j x_j^i = \sum_{j \in \mathcal{G}_i} c_j. \tag{6}$$

Here, $|\mathcal{G}_i|$ is the group size. Besides, we consider that the value of an inconvenience parameter is small enough in practice. Then the difference value of any two inconvenience parameters can be neglected. Hence, $\sum\limits_{j \in \mathcal{G}_i} \theta_j x_j^i$ is approximatively replaced with $\bar{\theta} \sum\limits_{j \in \mathcal{G}_i} x_j^i$, where $\bar{\theta}$ represents the mean value of θ. We simplify Eqn. (6) as follows

$$\frac{(|\mathcal{G}_i| - 1)}{\sum\limits_{j \in \mathcal{G}_i} x_j^i} R_i - 2\bar{\theta} \sum_{j \in \mathcal{G}_i} x_j^i = \sum_{j \in \mathcal{G}_i} c_j. \tag{7}$$

To solve the above equation, we can acquire the final solution of $\sum\limits_{j \in \mathcal{G}_i} x_j^i$ as follows

$$\begin{aligned} \sum_{j \in \mathcal{G}_i} x_j^i &= \frac{\sqrt{(\sum\limits_{j \in \mathcal{G}_i} c_j)^2 + 8\bar{\theta}\,(|\mathcal{G}_i| - 1) R_i} - \sum\limits_{j \in \mathcal{G}_i} c_j}{4\bar{\theta}} \\ &= \phi\sqrt{\eta + \lambda R_i} + \kappa \end{aligned} \tag{8}$$

And $\phi = 1/4\bar{\theta}$, $\eta = (\sum\limits_{j \in \mathcal{G}_i} c_j)^2$, $\lambda = 2(|\mathcal{G}_i| - 1)/\phi$ and $\kappa = -\phi \sum\limits_{j \in \mathcal{G}_i} c_j$. There exists a constraint for $\sum\limits_{j \in \mathcal{G}_i} x_j^i$, namely, $\sum\limits_{j \in \mathcal{G}_i} x_j^i \leqslant d_i$. To sum up, $\sum\limits_{j \in \mathcal{G}_i} x_j^i$ is finally determined by

$$\sum_{j \in \mathcal{G}_i} x_j^i = \begin{cases} \phi\sqrt{\eta + \lambda R_i} + \kappa, & \phi\sqrt{\eta + \lambda R_i} + \kappa \leqslant d_i \\ d_i, & \phi\sqrt{\eta + \lambda R_i} + \kappa > d_i \end{cases} \tag{9}$$

By substituting $\sum\limits_{j \in \mathcal{G}_i} x_j^i$ into Eqn. (5), we solve the optimal solution of x_j^i (denoted as x_j^{i*}) as follows:

$$x_j^{i*} = \begin{cases} \dfrac{R_i/(\phi\sqrt{\eta + \lambda R_i} + \kappa) - c_j}{R_i/(\phi\sqrt{\eta + \lambda R_i} + \kappa)^2 + 2\theta_j}, & \phi\sqrt{\eta + \lambda R_i} + \kappa \leqslant d_i \\ \dfrac{R_i d_i - c_j d_i^2}{R_i + 2\theta_j d_i^2}, & \phi\sqrt{\eta + \lambda R_i} + \kappa > d_i \end{cases} \tag{10}$$

x_j^{i*} is called the best response of vehicle v_j^i in determining the participation level for sending dummy packets to RSU i, which maximizes individual utility under the condition of given reward parameter R_i.

As a leader in the game, RSU i can know x_j^{i*} after hold the knowledge about the impacts of the decision on behavior of the followers. We consider that due to attractive incentives, the vehicles would like to upload status information (including c_j and θ_j) via secure encryptions as scheduled by the RSU. Subsequently, x_j^{i*} is able to be solved and known by the RSU. We substitute $\sum\limits_{j \in \mathcal{G}_i} x_j^i$ into the utility function of the RSU. Considering that $\phi\sqrt{\eta + \lambda R_i} + \kappa \leqslant d_i$, we get

$$C_i = r_i(d_i - \phi\sqrt{\eta + \lambda R_i} - \kappa) + R_i. \tag{11}$$

We take the first and second derivatives of C_i with respect to R_i, and find

$$\begin{aligned} \frac{\partial C_i}{\partial R_i} &= -\frac{r_i \phi \lambda}{2\sqrt{\eta + \lambda R_i}} + 1 \\ \frac{\partial^2 C_i}{\partial R_i^2} &= \frac{r_i \phi \lambda^2}{4\sqrt{(\eta + \lambda R_i)^3}} > 0 \end{aligned} \tag{12}$$

The above equation indicates that the utility function is convex. Similarly, we use the first-order optimality condition $\partial C_i / \partial R_i = 0$ to obtain R_i^*, which is calculated by

$$R_i^* = \frac{r_i^2 \phi^2 \lambda}{4} - \frac{\eta}{\lambda}. \tag{13}$$

As for when $\phi\sqrt{\eta + \lambda R_i} + \kappa > d_i$, $C_i = R_i$. We substitute $\sum\limits_{j \in \mathcal{G}_i} x_j^i = d_i$ into Eqn. (7) to solve R_i. In the case, we get

$$R_i^* = \frac{d_i(\sum\limits_{j \in \mathcal{G}_i} c_j + 2\bar{\theta} d_i)}{|\mathcal{G}_i| - 1}. \tag{14}$$

By combining with the above two cases, R_i^* is finally determined by

$$R_i^* = \begin{cases} \dfrac{r_i^2\phi^2\lambda}{4} - \dfrac{\eta}{\lambda}, & \phi\sqrt{\eta+\lambda R_i}+\kappa \leqslant d_i \\ \dfrac{d_i(\sum\limits_{j\in\mathcal{G}_i} c_j + 2\bar{\theta} d_i)}{|\mathcal{G}_i|-1}, & \phi\sqrt{\eta+\lambda R_i}+\kappa > d_i \end{cases} \tag{15}$$

Theorem 1: A unique Stackelberg Equilibrium exists between the RSU and all the participating vehicles in the proposed Stackelberg game approach.

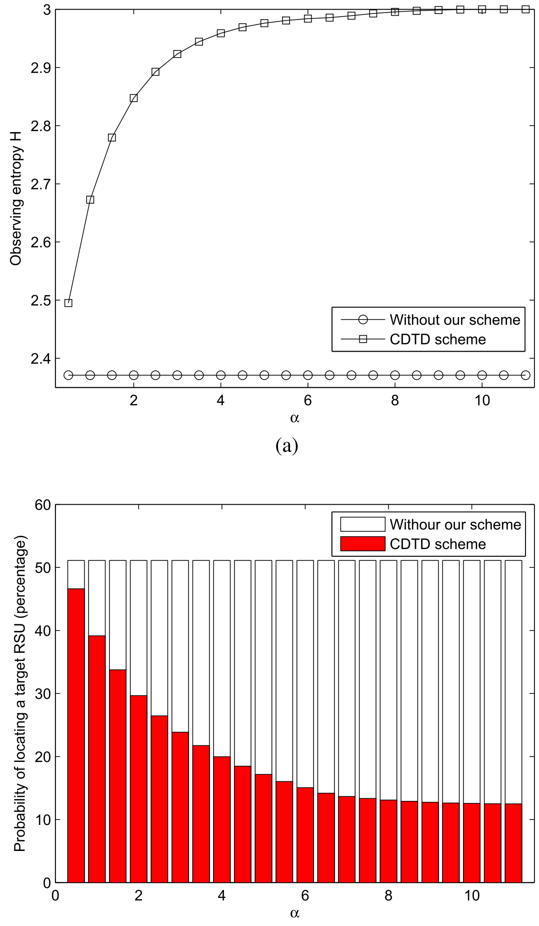
Proof: In the coverage of RSU i, according to the given reward parameter R_i, each participating vehicle acts as a follower and always has its own best response x_j^{i*}. x_j^{i*} is unique due to the concave character of the utility function, namely, $\partial^2 U_j^i/\partial x_j^{i2} < 0$, as shown in Eqn. (4). By having insight into all the best responses $\forall j \in \mathcal{G}_i, x_j^{i*}$, the cost function of the leader is formulated accordingly. After that, to minimize the overall cost, R_i^* is solved, as shown in Eqn. (15). At the same time, we can demonstrate that the RSU has a unique optimal strategy under given the best strategies of all the participating vehicles, by using $\partial^2 C_i/\partial R_i^2 > 0$. Ultimately, in the game model, both the leader and followers are fully satisfied because that their decisions (R_i^*, x_j^{i*}) make that their utilities have been maximized simultaneously. Moreover, when all the players, including each participating vehicle and the RSU, have their optimized payoff and cost, respectively, considering the strategies chosen by other players in the game. They have no incentives to change the decisions and take other actions. Thus, (R_i^*, x_j^{i*}) is obtained to guarantee that the unique Stackelberg equilibrium is reached finally. ■

VI. NUMERICAL RESULTS

In this section, we evaluate significant performance of the proposed scheme for securing EC-IoV against RSU hotspot attack with traffic eavesdropping. We consider a general EC-IoV network consisting of 8 RSUs uniformly deployed in a square area of $1.75 \times 1.75\ km^2$. Transmission range of each RSU is generally 350 m. In EC-IoV environment, local vehicles directly transmit packets to enhanced RSUs for proximal data processing. For an RSU, its packet receiving rate ranges from 0.2 to 2 per second according to different workload states. The number of connecting vehicles is distributed over [15, 25]. Besides, on average, data size of each packet is 128 bytes. The observing time period is set as 30 minutes. For a participating vehicle, data transmission cost for sending per kilobyte of dummy packets c ranges from 0.1 to 3. As for the inconvenience parameter θ, the value is randomly distributed between 0.01 to 0.09.

A. PERFORMANCE EVALUATION OF THE DEFENSE SCHEME

Here, we consider there exists a scenario that one RSU stays busy so the packet receiving rate ranges from 1.6 to 2 per second while other RSUs tend to be idle and their packet receiving rates are only from 0.2 to 0.4 per second. Without any valid defense scheme, the RSU with maximum amount of receiving packets becomes a target RSU of the adversary. To prevent from RSU hotspot attack, we propose a collaborative dummy traffic delivery scheme wherein dummy traffic is introduced to mislead traffic statistics in the traffic pattern via the collaboration of local vehicles when necessary. In this way, the observing entropy H for describing traffic distribution in a hotspot phenomenon can be improved finally.



(a)

(b)

FIGURE 4. Performance comparison with and without our scheme. (a) Observing entropy *H*. (b) Probability of locating a target RSU.

As shown in Fig. 4, we compare the performances between the proposed CDTD scheme and without our scheme. As mentioned above, efficiency of the scheme is strictly related with the considerate setting of risk level parameter r. The value of r is generally set by the central authority, which is responsible for security protection of the entire network. With the value of r increasing, participating RSUs will be expected by the central authority to generate more dummy traffic even with larger payments for participating vehicles. According to Eqn. (2), α and β are two adjustment parameters of r and we set β with fixed value 10^{-6}. The increase of α has a positive effect on increasing the value of r for all the participating RSUs. When the value of α is increased, the central authority pays more attention to the achievement

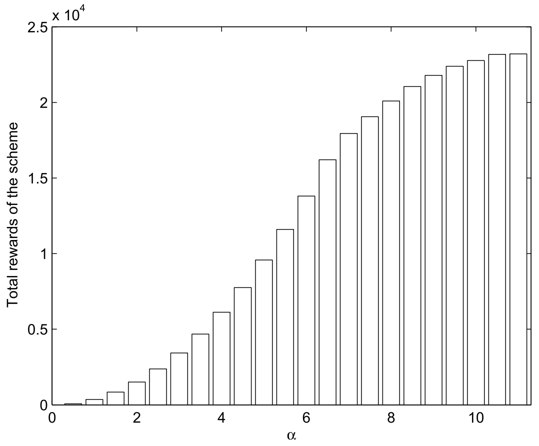


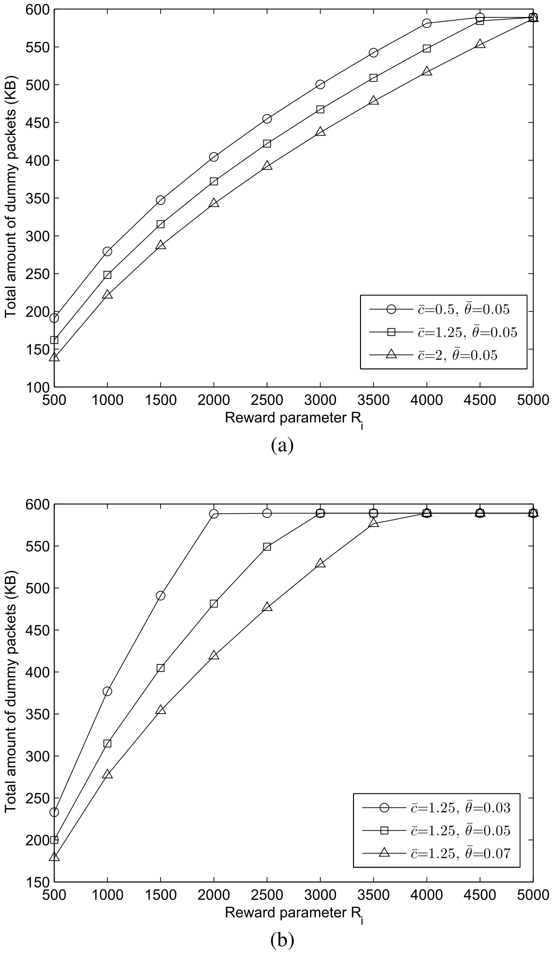
FIGURE 5. Total rewards of the scheme with respect to different values of α.

and efficiency of the scheme and considers monetary expense less. Total rewards are increased to stimulate participating vehicles to send more dummy packets, as shown in Fig. 5. When dummy traffic is generated more, traffic inconsistency is easily restrained and the observing entropy H is improved as well in Fig. 4(a). The observing entropy H approaches to, and ultimately is equal to the maximal value. At this time, each RSU is of the same traffic so the maximal value of the observing entropy H is $\log 8 = 3$.

When the entropy is improved, the adversary cannot locate a target RSU with convenience. In our scheme, the probability of locating a target RSU is decreased due to the degradation of traffic inconsistency. As shown in Fig. 4(b), we find that the probability of locating a target RSU in our scheme is decreased as the central authority sets higher value of α. For example, the decreasing percentage of the probability reaches to about 25% when the value of α is improved from 4 to 6. Meanwhile, the probability in our scheme when $\alpha = 6$ is only about 30% of that without the scheme. Finally, owing to sufficient enough dummy traffic, the probability of locating a target RSU is decreased to the minimal value. There exist 8 RSUs in the network. When each RSU is of the same traffic, the minimal probability of locating a target RSU is 12.5%. In the scheme, once the traffic is balanced among all the RSUs, the originally low observing entropy can be significantly improved to mislead the adversary. Due to the obfuscated traffic statistics in the traffic pattern, the adversary cannot realize the real existence of a hotpsot phenomenon after observing a higher entropy. As a consequence, the adversary has no valid motivations to launch the RSU hotspot attack. Potential security threats are avoided in the network. To summarize, numerical results show that the proposed CDTD scheme is effective to hide a target RSU and secure EC-IoV against RSU hotspot attack.

B. IMPACTS OF DIFFERENT SYSTEM PARAMETERS

To further demonstrate the Stackelberg game, we select randomly an RSU (denoted as RSU i) for observations in the CDTD scheme. The best responses of the RSU and participating vehicles are discussed with respect to different system parameters. In the Stackelberg game approach, the parameters mainly consist of data transmission cost c, inconvenience parameter θ and reward parameter R_i.



(a)

(b)

FIGURE 6. Performance comparison of total amount of dummy packets with respect to different R_i, $\bar{c}$ and $\bar{\theta}$. (a) Different values of average data transmission cost ($\bar{c}$). (b) Different values of average inconvenience parameter ($\bar{\theta}$).

Clearly, for participating vehicles, the total amount of dummy packets in the incentive mechanism is stimulated well by the reward parameter R_i. So the scheme is greatly promoted with the increasing value of R_i. Besides, the total amount of dummy packets is limited to a threshold value indicated by d_i in Section V-B. d_i is to avoid too many dummy packets in the CDTD scheme. Moreover, when participating vehicles are of lower data transmission cost and inconvenience parameter, they would like to send more dummy packets, under the same condition of R_i, as shown in Fig. 6. In Fig.6(a), mean value of c (denoted as $\bar{c}$) is set by three values: [0.5, 1.25, 2]. Higher values of $\bar{c}$ give rise to more additional participating cost for local vehicles. Given the same R_i, participating vehicles prefer to decrease their own amounts of sending dummy packets to maximize the utilities, according to Eqn. (1). We take an example that $R_i = 2500$.

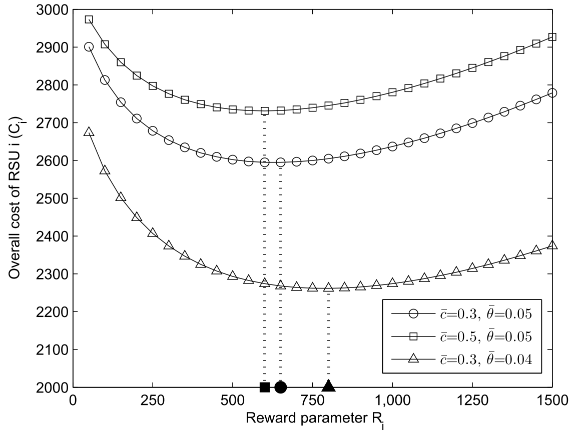


FIGURE 7. Comparison of overall cost of RSU *i* with respect to different R_i, $\bar{c}$ and $\bar{\theta}$.

When $\bar{c}$ is increased from 0.5 to 2, the total amount of dummy packets is reduced from 454 KB to 391 KB. This leads to more than 14% decreasing percentage. Similar results can be found in Fig. 6(b). Thus, the reward parameter R_i are beneficial to increase the total amount of dummy packets while both average data transmission cost $\bar{c}$ and average inconvenience parameter $\bar{\theta}$ have a negative impact for the execution of the incentive mechanism.

As for RSU i, its overall cost C_i is determined by reward parameter R_i and also influenced by state parameters of all the participating vehicles, $\bar{c}$ and $\bar{\theta}$. In the Stackelberg game, C_i is compromised of two aspects: risk level and monetary expense, namely total payments for all the participating vehicles R_i. In Fig. 7, the overall cost of RSU i is changed over the dynamic reward parameter R_i. C_i is increased when the increasing values of $\bar{c}$ and $\bar{\theta}$ bring negative effects for the efficiency of the proposed scheme. This is resulted by insufficient amount of dummy packets under the same condition of R_i. Then the overall cost of the RSU is increased along with the increasing risk level due to the inadequate dummy traffic. Moreover, optimal solution of R_i (denoted as R_i^*) can be also found in the figure and indicated by the markers of solid round, square and triangle. As shown in Fig. 7, R_i^* will be decreased with the increasing values of $\bar{c}$ and $\bar{\theta}$. For the RSU, when participating vehicles are inconvenient to undertake dummy traffic generation tasks, excessive rewards become inefficient and may be invalid. Thus, at the moment, the optimal strategy of the RSU is to take actions for lessening R_i^*. For example, the value of R_i^* is decreased about 25% when $\bar{c} = 0.3$ and $\bar{\theta} = 0.04$ are increased to $\bar{c} = 0.5$ and $\bar{\theta} = 0.05$. In summary, through the above numerical results, we have illustrated that the Stackelberg game approach is efficient for executing the CDTD scheme.

VII. CONCLUSION

In this paper, we consider the features of EC-IoV, and introduce RSU hotspot attack with traffic eavesdropping and corresponding defense in EC-IoV. RSU is a key enabler for EC-IoV but it also suffers from potential attacks due to the open deployment environment. Any attacks for RSUs will cause severe damages to EC-IoV. We propose RSU hotspot attack, in which a global adversary eavesdrops wireless communications and records network traffic to monitor, locate and attack a target RSU with heavy traffic. By utilizing traffic statistics about the RSUs, the adversary is easy to locate the target RSU in case of an obvious hotspot phenomenon. Thus, we are motivated to design a proactive scheme by generating dummy traffic delivery. In the defense scheme, local vehicles should be collaborative and encouraged well to send dummy packets to specified RSUs. This leads to dummy traffic for misleading the traffic statistics. Then the target RSU can be effectively hidden. Stackelberg game approach is used to build an incentive mechanism in the scheme. Meanwhile, the unique Stackelberg equilibrium is analysed via a theoretical method. Finally, extensive simulations show that the scheme with the Stackelberg game approach is effective and efficient to secure EC-IoV against RSU hotspot attack.

We will further consider to study the potential approaches for effectively protecting general RSUs in EC-IoV environment. When an adversary becomes strong enough, it may choose an arbitrary number of RSUs to launch large-scale attacks. We explore how to ensure security guarantee for those RSUs even without hotspot phenomena. In this paper, the adversary tries to identify target RSUs after traffic eavesdropping and analysis. Under the circumstance, for mitigating the attacks timely, we may pay attention to integrate with existing traffic eavesdropping detection techniques, e.g., those proposed in [30] and [31]. In this way, comprehensive defense scheme is performed to overcome eavesdropping based security threats for RSUs in EC-IoV, reacting to the capability enhancement of the adversary. Besides, open issues of the proposed defense scheme need also to be considered well. For example, current practical simulation platforms can be directly utilized for convenient and advanced performance evaluation in different scenarios, e.g, 3GPP V2X deployment scenario. Furthermore, in the Stackelberg game model, some of participating vehicles may prefer not to reveal private information to local RSUs. Here, existing estimation methods, e.g., Bayesian estimation, are great alternatives.

REFERENCES

[1] Y. Fangchun, W. Shangguang, L. Jinglin, L. Zhihan, and S. Qibo, "An overview of Internet of vehicles," *China Commun.*, vol. 11, no. 10, pp. 1–15, Oct. 2014.

[2] Q. Yuan, H. Zhou, J. Li, Z. Liu, F. Yang, and X. S. Shen, "Toward efficient content delivery for automated driving services: An edge computing solution," *IEEE Netw.*, vol. 32, no. 1, pp. 80–86, Jan. 2018.

[3] W. Zhang, B. Han, and P. Hui, "On the networking challenges of mobile augmented reality," in *Proc. Workshop Virtual Reality Augmented Netw.*, 2017, pp. 24–29.

[4] K. Zhang, Y. Mao, S. Leng, Y. He, and Y. Zhang, "Mobile-edge computing for vehicular networks: A promising network paradigm with predictive off-loading," *IEEE Veh. Technol. Mag.*, vol. 12, no. 2, pp. 36–44, Jun. 2017.

[5] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwälder, and B. Koldehofe, "Mobile fog: A programming model for large-scale applications on the Internet of Things," in *Proc. 2nd ACM SIGCOMM Workshop Mobile Cloud Comput.*, 2013, pp. 15–20.

[6] N. B. Truong, G. M. Lee, and Y. Ghamri-Doudane, "Software defined networking-based vehicular adhoc network with fog computing," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, May 2015, pp. 1202–1207.

[7] G. G. M. N. Ali, E. Chan, and W. Li, "On scheduling data access with cooperative load balancing in vehicular ad hoc networks (VANETs)," *J. Supercomput.*, vol. 67, pp. 438–468, Feb. 2014.

[8] L. Le, A. Festag, R. Baldessari, and W. Zhang, "Vehicular wireless short-range communication for improving intersection safety," *IEEE Commun. Mag.*, vol. 47, no. 11, pp. 104–110, Nov. 2009.

[9] E. Uhlemann, "Introducing connected vehicles [connected vehicles]," *IEEE Veh. Technol. Mag.*, vol. 10, no. 1, pp. 23–31, Mar. 2015.

[10] M. A. Moharrum and A. A. Al-Daraiseh, "Toward secure vehicular ad-hoc networks: A survey," *IETE Tech. Rev.*, vol. 29, no. 1, pp. 80–89, 2012.

[11] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computing—A key technology towards 5G," *ETSI White Paper*, vol. 11, no. 11, pp. 1–16, 2015.

[12] D. Sabella, A. Vaillant, P. Kuure, U. Rauschenbach, and F. Giust, "Mobile-edge computing architecture: The role of MEC in the Internet of Things," *IEEE Consum. Electron. Mag.*, vol. 5, no. 4, pp. 84–91, Oct. 2016.

[13] K. Zhang, Y. Mao, S. Leng, S. Maharjan, and Y. Zhang, "Optimal delay constrained offloading for vehicular edge computing networks," in *Proc. IEEE 17th Int. Conf. Communs. (ICC)*, Paris, France, May 2017, pp. 1–6.

[14] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25408–25420, 2017.

[15] Y. Cao *et al.*, "Mobile edge computing for big-data-enabled electric vehicle charging," *IEEE Commun. Mag.*, vol. 56, no. 3, pp. 150–156, Mar. 2018.

[16] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, and S. Chen, "Vehicular fog computing: A viewpoint of vehicles as the infrastructures," *IEEE Trans. Veh. Technol.*, vol. 65, no. 6, pp. 3860–3873, Jun. 2016.

[17] C. Liu, H. Huang, and H. Du, "Optimal RSUs deployment with delay bound along highways in VANET," *J. Combinat. Optim.*, vol. 33, no. 4, pp. 1168–1182, 2016.

[18] C.-C. Lin and D.-J. Deng, "Optimal two-lane placement for hybrid vanet-sensor networks," *IEEE Trans. Ind. Electron.*, vol. 62, no. 12, pp. 7883–7891, Dec. 2015.

[19] G. M. N. Ali, P. H. J. Chong, S. K. Samantha, and E. Chan, "Efficient data dissemination in cooperative multi-rsu vehicular ad hoc networks (VANETs)," *J. Syst. Softw.*, vol. 117, pp. 508–527, Jul. 2016.

[20] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, "Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response," *IEEE Trans. Comput.*, vol. 65, no. 8, pp. 2562–2574, Aug. 2016.

[21] M. Wang, D. Liu, L. Zhu, Y. Xu, and F. Wang, "LESPP: Lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication," *Computing*, vol. 98, no. 7, pp. 685–708, 2016.

[22] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3589–3603, Sep. 2010.

[23] K. Mehta, D. Liu, and M. Wright, "Protecting location privacy in sensor networks against a global eavesdropper," *IEEE Trans. Mobile Comput.*, vol. 11, no. 2, pp. 320–336, Feb. 2012.

[24] M. M. E. A. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 10, pp. 1805–1818, Oct. 2012.

[25] J. Deng, R. Han, and S. Mishra, "Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks," *Pervasive Mobile Comput.*, vol. 2, no. 2, pp. 159–186, 2006.

[26] A. Rényi, "On measures of entropy and information," in *Proc. 4th Berkeley Symp. Math. Statist. Probab.*, vol. 1, 1961, pp. 547–561.

[27] S. N. Premnath and Z. J. Haas, "Security and privacy in the Internet-of-Things under time-and-budget-limited adversary model," *IEEE Wireless Commun. Lett.*, vol. 4, no. 3, pp. 277–280, Jun. 2015.

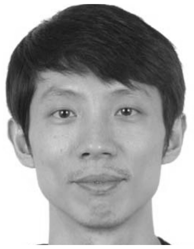
[28] X. Wang, X. Chen, W. Wu, N. An, and L. Wang, "Cooperative application execution in mobile cloud computing: A Stackelberg game approach," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 946–949, May 2016.

[29] J. Cruz, Jr., "Survey of Nash and Stackelberg equilibrim strategies in dynamic games," *Ann. Econ. Social Meas.*, vol. 4, no. 2, pp. 339–344, 1975.

[30] S. Chakravarty, G. Portokalidis, M. Polychronakis, and A. D. Keromytis, "Detection and analysis of eavesdropping in anonymous communication networks," *Int. J. Inf. Secur.*, vol. 14, no. 3, pp. 205–220, 2015.

[31] A. Proano, L. Lazos, and M. Krunz, "Traffic decorrelation techniques for countering a global eavesdropper in WSNs," *IEEE Trans. Mobile Comput.*, vol. 16, no. 3, pp. 857–871, Mar. 2017.

XUMIN HUANG is currently pursuing the Ph.D. degree in networked control systems with the Guangdong University of Technology, China. His research interests mainly focus on network performance analysis, simulation and enhancement in wireless communications and networking.



RONG YU (M'08) received the Ph.D. degree from Tsinghua University, China, in 2007. After that, he was with the School of Electronic and Information Engineering, South China University of Technology. In 2010, he joined the Institute of Intelligent Information Processing, Guangdong University of Technology, where he is currently a Full Professor. He is the co-inventor of over 30 patents and author or co-author of over 100 international journals and conference papers. His research interests include wireless networking and mobile computing in featured environments, such as edge cloud, connected vehicles, smart grid, and Internet of Things. He was a member of the Home Networking Standard Committee in China, where he led the standardization work of three standards.

MIAO PAN (S'07–M'12–SM'18) received the B.Sc. degree in electrical engineering from the Dalian University of Technology, China, in 2004, the M.A.Sc. degree in electrical and computer engineering from the Beijing University of Posts and Telecommunications, China, in 2007, and the Ph.D. degree in electrical and computer engineering from the University of Florida in 2012. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, University of Houston. He was an Assistant Professor in computer science with Texas Southern University from 2012 to 2015. His research interests include cognitive radio networks, wireless big data privacy, deep learning with differential privacy, and cyber-physical systems. His work received the Best Paper Awards from GLOBECOM 2015 and GLOBECOM 2017. He is currently an Associate Editor of the IEEE Internet of Things Journal from 2015 to 2018.

LEI SHU (M'07–SM'15) received the B.Sc. degree in computer science from South Central University for Nationalities, China, in 2002, and the M.Sc. degree in computer engineering from Kyung Hee University, South Korea, in 2005, and the Ph.D. degree from the Digital Enterprise Research Institute, National University of Ireland, Galway, Ireland, in 2010. Until 2012, he was a Specially Assigned Researcher with the Department of Multimedia Engineering, Graduate School of Information Science and Technology, Osaka University, Japan. He is currently a Distinguished Professor with Nanjing Agricultural University, China, and a Lincoln Professor with the University of Lincoln, U.K. He is also the Director of the NAU-Lincoln Joint Research Center of Intelligent Engineering. His main research fields are wireless sensor networks and Internet of Things. He has published over 380 papers in related conferences, journals, and books in the areas of sensor networks. His current H-index is 42 and i10-index is 153 in Google Scholar Citation. He was a recipient of GLOBECOM 2010, ICC 2013, ComManTel 2014, 2014 Top Level Talents in Sailing Plan of Guangdong Province, China, the 2015 Outstanding Young Professor of Guangdong Province, WICON 2016, and the SigTelCom 2017 Best Paper Awards, the 2017 and 2018 IEEE Systems Journal Best Paper Awards, and the Outstanding Associate Editor Award of 2017 IEEE Access. He has been serving as an Associate Editor for the IEEE Transactions on Industrial informatics, the *IEEE Communications Magazine*, the *IEEE Network Magazine*, the IEEE Systems Journal, the IEEE Access, the IEEE/CAA Journal of Automatic Sinica, and *Sensors*. He has served over 50 various Co-Chair for international conferences/workshops, such as IWCMC, ICC, ISCC, ICNC, Chinacom, especially the Symposium Co-Chair for IWCMC 2012, ICC 2012, the General Co-Chair for Chinacom 2014, Qshine 2015, Collaboratecom 2017, DependSys 2018, and SCI 2019, the TPC Chair for InisCom 2015, NCCA 2015, WICON 2016, NCCA 2016, Chinacom 2017, InisCom 2017, WMNC 2017, and NCCA 2018; TPC member of over 150 conferences, such as ICDCS, DCOSS, MASS, ICC, GLOBECOM, ICCCN, WCNC, and ISCC.