Computers, Materials & Continua
DOI:10.32604/cmc.2021.016411
Article

Tech Science Press

Game-Oriented Security Strategy Against Hotspot Attacks for Internet of Vehicles

Juan Guo[1], Yanzhu Liu[2,*], Shan Li[3], Zhi Li[4] and Sonia Kherbachi[5]

[1]Guilin University of Electronic Technology, Beihai, 536000, Guangxi, China
[2]Great Wall Computer Software and Systems Inc., Beijing, 100083, China
[3]Department of Electronics and Communication Engineering, Beijing Electronic Science and Technology Institute, Beijing, 100070, China
[4]State Grid Information & Telecommunication Group Co., Ltd., Beijing, 100031, China
[5]Department of Management, University of Bejaia, Bejaia, 06000, Algeria
[*]Corresponding Author: Yanzhu Liu. Email: lwtxzz2278@163.com
Received: 01 January 2021; Accepted: 23 February 2021

Abstract: With the rapid development of mobile communication technology, the application of internet of vehicles (IoV) services, such as for information services, driving safety, and traffic efficiency, is growing constantly. For businesses with low transmission delay, high data processing capacity and large storage capacity, by deploying edge computing in the IoV, data processing, encryption and decision-making can be completed at the local end, thus providing real-time and highly reliable communication capability. The roadside unit (RSU), as an important part of edge computing in the IoV, fulfils an important data forwarding function and provides an interactive communication channel for vehicles and server providers. Additional computing resources can be configured to accommodate the computing requirements of users. In this study, a virtual traffic defense strategy based on a differential game is proposed to solve the security problem of user-sensitive information leakage when an RSU is attacked. An incentive mechanism encourages service vehicles within the hot range to send virtual traffic to another RSU. By attracting the attention of attackers, it covers the target RSU and protects the system from attack. Simulation results show that the scheme provides the optimal strategy for intelligent vehicles to transmit virtual data, and ensures the maximization of users' interests.

Keywords: Edge computing; internet of vehicles; differential games; security defense

1 Introduction

With the rapid development of internet technology such as network communication and intelligent vehicles, the internet of vehicles (IoV), including the cloud platform, car connection, car-road interconnection, and car service platform, has entered daily life. As an important part of intelligent transportation, the IoV has achieved real-time perception of roads and traffic conditions

by combining the GPS, car/road camera, and other technologies such as sensors, computing, and intelligent processing [1]. Vehicles are increasingly connected to the internet of things (IoT), which enables access to information for drivers and passengers on the move [2]. Through rapid transmission and interaction with multiple traffic signals, the network of cars has implemented real-time analysis and realized control of the vehicle and the road, which improves traffic efficiency and traffic safety, and better serves the user.

By converting a vast amount of data to meaningful, actionable knowledge, the IoV can help to meet challenges to safe, efficient transportation [3]. Owing to the lack of physical resources for data processing, most vehicles must be based on roadside units (RSUs) connected to a cloud data center [4]. Although the cloud computing platform has almost unlimited resources, its centralized architecture has the disadvantages of transmission delay and lack of network stability [5]. Data volume, real-time demand, IoV computing capacity, and demand for communication stability limit the ability of the cloud computing architecture to meet user needs [6]. Edge computing (EC) has become the object of intense research to solve these problems, in the form of the edge computing-based internet of vehicles (ECIoVs) [7].

EC responds to user requests in a timely and efficient manner by distributing processing and memory functions at the network's edge, thereby reducing the time consumed by network operations and service delivery [8]. Compared to cloud computing, EC can provide fast, efficient computing and communication, and can realize the real-time interaction of all kinds of data, which is the new direction of the IoV. To deploy storage and computing at the wireless network edge, including radio access points, the edge information system (EIS), edge caching, EC, and edge AI will play a key role in the IoV [9]. AI-related modules of EC are redesigned to distribute AI functions to the edge [10]. However, the deployment position is closer to the user, which weakens its protection, increasing the likelihood of attack, which will affect user service [11], giving rise to security issues.

The RSU is an important edge node, and an important component in the interaction of the user with edge calculation, network communication, and terminal equipment. This study designs a virtual traffic defense mechanism to avoid the interruption of vehicle communication and the compromise of user privacy from hotspot attacks on an RSU. Game theory is introduced to describe the costs and benefits of sending data to different RSUs. By maximizing the welfare of the system, the optimal strategy for each vehicle to send data to each RSU is obtained, so as to protect RSUs from hotspot attacks while minimizing the impact on network performance caused by virtual traffic.

2 Related Work

A large number of RSUs and vehicles equipped with embedded devices constitute the IoV with data communication, transmission, computing, and other capabilities [12]. Data collected from vehicles include parameters such as a vehicle's speed, location, and direction of movement, while data collected from RSUs can include overall traffic information [13]. EC conducts computing tasks and data caching near end-users [14]. At present, the network of cars utilizes marginal computing to give more computing, data storage, and communication ability to RSUs, so that they can simultaneously store, forward, and process packets [15]. However, this increased functionality compromises user safety, and even the security of the network, due to attack. An attack on an RSU will first interrupt intelligent vehicle services in an area, which affects the user experience. An attacked RSU will not be able to return data to the cloud, which will hamper its resource scheduling. Even more serious is the disclosure of sensitive user information.

Many solutions have been proposed to the privacy and security issues of RSUs. Chen et al. proposed a batch identification game model (BIGM) in wireless mobile networks, enabling nodes to find invalid signatures in a reasonable time in the cases of both complete and incomplete information [16]. Liu et al. [17] designed a method to implement security policies and showed that traffic forwarding rules can illustrate security strategies. Arif et al. [18] suggested that packets sent to service providers from smart vehicles can ensure the safety of interactive data by anonymous processing techniques. Ying et al. [19] suggested that intelligent vehicles in a mixed area will be distributed to the symmetric key used to encrypt communication data between intelligent vehicles and RSUs. Basudan et al. [20] designed a communication protocol for the free adjustment of the fog node RSU, which can realize two-way authentication and protection of data integrity in communication. Wang et al. [21] proposed a scheme of computing, storage and communication with an RSU, so as to realize real-time collection, analysis and uploading of communication information of intelligent vehicles. Hui et al. [22] proposed a method of chaotic secure data transmission, encrypting and decrypting the main data signal by the principle of n-shift encryption.

This article studies a potential attack and the corresponding defense scheme of an RSU in the edge calculation of a car network based on a decision framework. We analyze the dynamic decision-making process of the user in the hot attack of an RSU, and help an intelligent vehicle on the IoV to achieve its maximum income to ensure its privacy and security.

3 Edge Computing Game Security Model

The network game security model based on EC has a cloud layer, edge node layer, and intelligent terminal layer, as shown in Fig. 1. The cloud layer is the data storage and resource scheduling center of the three-layer network model. The cloud data center (CDC) is located in the cloud layer and mainly coordinates the demand for resources of the boundary node layer. The edge nodes of dynamic virtual computing resource (VCR) dynamically provide the allocation and management of virtualization services for the server and RSU edge node layer on demand. The edge node layer in the middle is deployed on the edge server and RSU, and is dispersed in hotspots such as gas stations, parking spaces, and supermarkets. It coordinates between users and service providers, and a vehicle is connected to its recent RSU when it receives the service. As the bottom of the three-tier structure, the intelligent terminal layer is composed of a large number of intelligent vehicles and their generated data. Based on short-distance communication such as Wi-Fi, Bluetooth, and ZigBee, the intelligent vehicle is connected to the edge node, and service is provided by the RSU in the EC node.

Roles fulfill different functions and form an IoV communication environment through cooperation or resistance. The main roles are the security center, RSU, intelligent vehicle, and RSU attacker.

3.1 Safety Center

Deployed in the cloud layer, the security center is the highest security manager in the network, is responsible for the safety of all entities including the vehicle, RSU, and service providers, and is certified as an organization that provides trusted services.

3.2 RSU

RSUs are deployed in dispersed locations such as gas stations, parking lots, and supermarkets, and have computational hardware, such as multifocal cuts, memory, and physical resources,

to process user requests. The RSU creates virtual machines, and dynamically creates, migrates, uninstalls, and destroys resources between them to realize intelligent, efficient, real-time services.

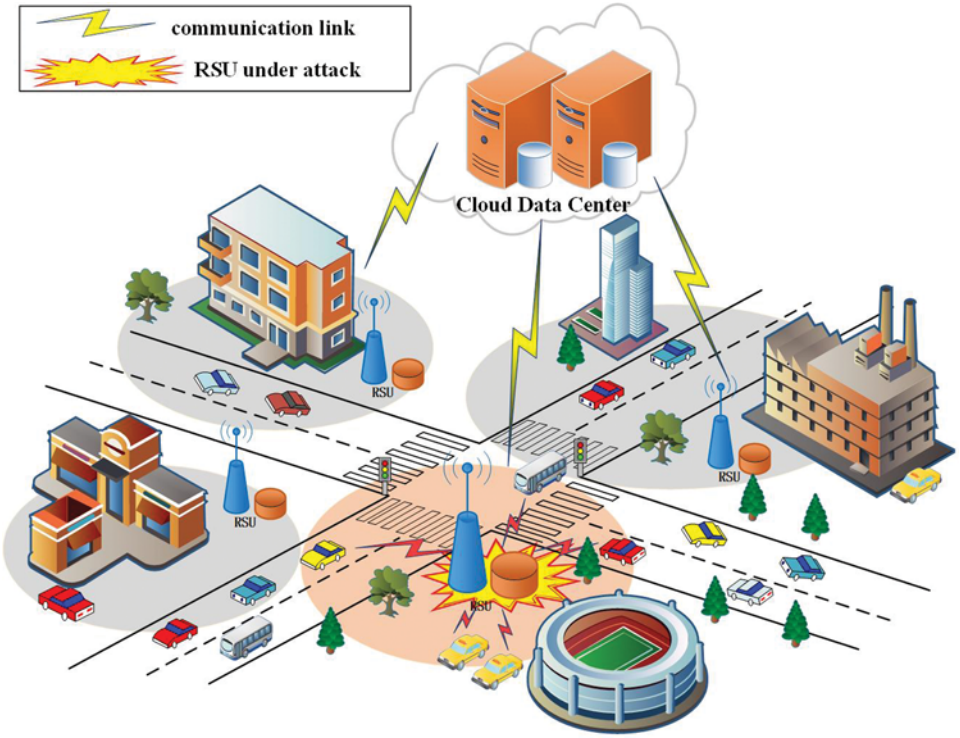

Figure 1: Network model based on edge computing

3.3 Intelligent Vehicle

An intelligent vehicle interacts with an adjacent RSU through the short-distance communication of Wi-Fi, Bluetooth, and ZigBee. It sends a service request to an RSU, which processes it to an edge server. Owing to the close geographical location of the communication parties, the communication effect and user experience will be better.

3.4 RSU Attacker

RSU attacks are monitored at all times. When an RSU interacts frequently with many vehicles and there is a surge in communication data, a hot service phenomenon occurs. The RSU attacker installs a traffic eavesdropping device near each RSU, selects the target RUS with the largest current data traffic through real-time traffic statistics, and attacks it. By attacking the target RSU, it can disrupt or even interrupt the current service.

To ensure the normal operation of the RSU network and provide safe and reliable data interaction, we use virtual traffic to identify the monitoring results of global attackers [23,24]. That is, the intelligent vehicles in the area send the virtual traffic to the non-hot RSU, which can mislead the attacker, thereby successfully resisting the attack.

An incentive mechanism encourages intelligent vehicles to send virtual packets to a specified RSU, which generates virtual traffic. An RSU will develop incentives based on virtual traffic

requirements. At the same time, the utility function of the intelligent vehicle will be obtained by combining the actual cost with the reward scheme to evaluate the degree of participation of the defense scheme. The parameters are shown in Tab. 1. We establish the security model based on the differential game edge.

Table 1: Model parameter

Symbol	Meaning
v_j^i	jth vehicle receiving service in the coverage of the ith RSU
U_j^i	Total income of vehicle v_j^i
$\phi_j^i(t)$	Virtual data volume of vehicle v_j^i transmission in t hours
l_j^i	Incentive for unit virtual traffic
c_j^i	Data transmission cost of a unit virtual packet sent by vehicle v_j^i at time t
θ_j	Size of affected application
τ_j^i	Amount of business data required for vehicle
$\eta_j^i(t)$	Risk coefficient changes as vehicle transfers virtual data
ρ	Parameter used to evaluate the value of user data, $\rho > 0$
E_i	Additional consumption caused by network delays
κ_i	Controls the weight of the network's extra overhead
$x(t)$	Network variable
α	Total cost of applying for network resources
β	System load change parameter

Considering the following scenario, in the IoVs, the set of vehicles that are covered in the ith RSU is denoted as $\mathcal{G}_i$, and the jth vehicle served in the set is given as v_j^i, $v_j^i \in \mathcal{G}_i$. $\phi_j^i(t)$ is the virtual data quantity transmitted by vehicle v_j^i at time t, whose value will directly affect the revenue of vehicles. The excitation obtained by vehicle v_j^i transmitting virtual data $\phi_j^i(t)$ at time t is represented by $l_j^i\phi_j^i(t)$, where l_j^i is the excitation value of unit virtual flow. The transmission cost of vehicle v_j^i transmitting virtual data at time t is $c_j^i\phi_j^i(t)$, where c_j^i is the transmission cost of unit virtual data packets by vehicle v_j^i. During service, the vehicle must bind and transmit the virtual data package with the business packet, and additional virtual data packages will inconvenience the vehicle. To facilitate discussion, we assume $\eta_j^i(t) = \rho_j^i\left(\phi_j^i\right)^2$, and ρ is a parameter greater than zero to evaluate the number of users. Finally, with the transmission of virtual data, the communication link may produce a certain network transport overhead, such as network latency. We describe this as $E_i = \kappa_i x(t)$, where κ_i is a weight parameter to control the extra cost of the network, and a larger value of κ_i indicates a more serious network impact. $x(t)$ is the state variable of the network, which satisfies

$$dx(t) = \left[\alpha_j^i\phi_j^i(t) - \beta x(t)\right]dt, \quad x(t_0) = x_{t_0}, \tag{1}$$

where α and β are positive parameters, α is the total cost parameter generated by applying network resources, and β is the ratio of unexpected load overhead to system load.

According to the above model, the income U_j^i of vehicle v_j^i can be expressed as

$$U_j^i = \left(l_j^i - c_j^i\right)\phi_j^i(t) - \left(\theta_j^i + \rho_j^i\tau_j^i\right)\left(\phi_j^i(t)\right)^2 - \kappa_i x(t). \tag{2}$$

Therefore, based on differential game theory [25], when the game theory time is $(0, T)$, the total cost function of vehicle v_j^i can be expressed as

$$J_j^i = \max_{\phi_i} \int_{t_0}^{T} U_j^i e^{-r(t-t_0)} dt + q[x(T)]. \tag{3}$$

4 Feedback Nash Equilibrium Model Solution

Based on research on the feedback Nash equilibrium solution of the differential game [26] and the above model, for any vehicle v_j^i, there exists a continuously differentiable function $V_t{}^i(t, x) : [0, T] \times R \to R$ satisfying the Isaacs–Bellman equation,

$$\begin{cases} -V_t{}^i(t, x) = \max\limits_{\phi} \left\{ \begin{array}{l} \left(\left(l_j^i - c_j^i\right)\phi_j^{i*}(t) - \left(\theta_j^i + \rho_j^i\tau_j^i\right)\left(\phi_j^{i*}(t)\right)^2 - \kappa_i x(t) \right) e^{-r(t-t_0)} \\ \quad + V_x{}^i(t, x)\left[\sum\limits_{i=1}^{n} \alpha_i \phi_j^{i*}(t) - \beta x(t)\right] \end{array} \right\}. \\ V_T^i(T, x) = q(x(T))\, e^{-r(t-t_0)} \end{cases} \tag{4}$$

Then the strategy set $\phi_j^{i*}(t)$ is the feedback Nash equilibrium solution of the differential game described by Eqs. (1) and (3). For the optimal policy set $\phi_j^{i*}(t)$, we give the following theorem.

Theorem 1: For the differential game of Eqs. (1) and (3) , the feedback Nash equilibrium solution is $\phi_j^i(t) = \dfrac{\alpha_j^i}{2M_j^i}\left(\dfrac{(q(r+\beta)+\kappa_i)\, e^{(t-T)(r+\beta)} - \kappa_i}{r+\beta}\right) + \dfrac{N_j^i}{2M_j^i}$, where $M_j^i = \theta_j + \rho_j^i\tau_j^i$, $N_j^i = l_j^i - c_j^i$.

Proof: The partial derivative of Eq. (4) with respect to x can be obtained as

$$\phi_j^i(t) = \frac{\alpha_j^i V_x{}^i(t, x)}{2M_j^i} e^{r(t-t_0)} + \frac{N_j^i}{2M_j^i}, \tag{5}$$

where $M_j^i = \theta_j + \rho_j^i\tau_j^i$, $N_j^i = l_j^i - c_j^i$.

To facilitate the solution, define

$$V^i(t, x) = [A_i(t)\, x + B_i(t)]\, e^{-r(t-t_0)}. \tag{6}$$

Take the partial derivative of Eq. (6) to obtain

$$V_x(t, x) = A_i(t)\, e^{-r(t-t_0)}. \tag{7}$$

Then

$$-V_t(t,x)=\left(rA_i(t)-\frac{d(A_i(t))}{dt}\right)xe^{-r(t-t_0)}+\left(rB_i(t)-\frac{d(B_i(t))}{dt}\right)e^{-r(t-t_0)}. \tag{8}$$

Substitute Eqs. (6) in (5) to obtain

$$\phi_j^i(t)=\frac{\alpha_j^i}{2M_j^i}A_i(t)+\frac{N_j^i}{2M_j^i}. \tag{9}$$

Substitute Eqs. (7) and (8) in formula Eq. (4) and simplify to obtain

$$\begin{aligned}-V_t{}^i(t,x)&=\max_{\phi}\left\{U_j^ie^{-r(t-t_0)}+V_x{}^i(t,x)\left[\sum_{i=1}^{n}\alpha_i\phi_i(t)-\beta x(t)\right]\right\}\\&=x(t)\,e^{-r(t-t_0)}\left(-\kappa_i-\beta\boldsymbol{\mathcal{A}}_i(t)\right)\\&\quad+e^{-r(t-t_0)}\left(\boldsymbol{\mathcal{N}}_j^i\left(\frac{\alpha_j^i}{2\boldsymbol{\mathcal{M}}_j^i}\boldsymbol{\mathcal{A}}_i(t)+\frac{\boldsymbol{\mathcal{N}}_j^i}{2\boldsymbol{\mathcal{M}}_j^i}\right)-\boldsymbol{\mathcal{M}}_j^i\left(\frac{\alpha_j^i}{2\boldsymbol{\mathcal{M}}_j^i}\boldsymbol{\mathcal{A}}_i(t)+\frac{\boldsymbol{\mathcal{N}}_j^i}{2\boldsymbol{\mathcal{M}}_j^i}\right)^2\right.\\&\quad\left.+\boldsymbol{\mathcal{A}}(t)\sum_{i=1}^{n}\alpha_i\left(\frac{\alpha_j^i}{2\boldsymbol{\mathcal{M}}_j^i}\boldsymbol{\mathcal{A}}_i(t)+\frac{\boldsymbol{\mathcal{N}}_j^i}{2\boldsymbol{\mathcal{M}}_j^i}\right)\right).\end{aligned} \tag{10}$$

Comparing Eqs. (8) and (10), it can be seen that

$$r\boldsymbol{\mathcal{A}}_i(t)-\frac{d(\boldsymbol{\mathcal{A}}_i(t))}{dt}=-\kappa_i-\beta\boldsymbol{\mathcal{A}}_i(t). \tag{11}$$

Therefore, the optimal strategy can be calculated as

$$\phi_j^i(t)=\frac{\alpha_j^i}{2M_j^i}\left(\frac{(q(r+\beta)+\kappa_i)\,e^{(t-T)(r+\beta)}-\kappa_i}{r+\beta}\right)+\frac{N_j^i}{2M_j^i}, \tag{12}$$

where $M_j^i=\theta_j+\rho_j^i\tau_j^i$, $N_j^i=l_j^i-c_j^i$.

Theorem 1 has been proved.

5 Experimental Simulation

We used MATLAB simulation tools to evaluate the performance of the proposed virtual traffic defense strategy based on a differential game. Consider a network of vehicles including five RSUs, each with an effective circular coverage area of radius 300 meters. After entering an RSU-covered area, a vehicle will participate in virtual traffic defense activities according to its initial state, and will protect the system from hotspot attacks. There are five vehicles in the observation range that send data to the RSU. Assume that the system observation time is 5 min, the RSU needs a total of 5 KB of traffic, and the system virtual traffic incentive value is 100 per byte. The values of other system parameters are shown in Tab. 2.

Table 2: Model simulation parameter settings

	θ	α	β	τ	ρ	κ	l	r	t
$i=1$	12	2	0.2	100	10	10	100	0.15	[0, 5] min
$i=2$	13	3	0.3	110					
$i=3$	14	4	0.4	120					
$i=4$	15	5	0.5	130					
$i=5$	16	6	0.6	140					

Fig. 2 depicts the relationship between the optimal amount of transmitted data $\phi_j^i(t)$ and time t, from which it can be seen that $t \in [0, 5]$, and $\phi_j^i(t)$ will be affected by many variables. Because an RSU provides a reasonable incentive strategy, the optimal transmission strategy $\phi_j^i(t)$ of the intelligent vehicle is an increasing function of time t. This means that the vehicle can make more money by continuously increasing the amount of virtual data it transmits. At the same time, because of the different network states, the speed of the vehicle transmission of virtual data can differ, i.e., a relatively poor network environment must transmit more virtual data to maximize the return. At the game's conclusion, the vehicle will stop transmitting virtual data. Vehicle 1, due to its better network environment and less business data, has a relatively stable transmission speed over the whole game, and it continues transferring for 4.8 min. Vehicle 5 suffers from a poor network environment and more business data, which requires more data transmission at greater speeds, and the time required for transmission is shorter.

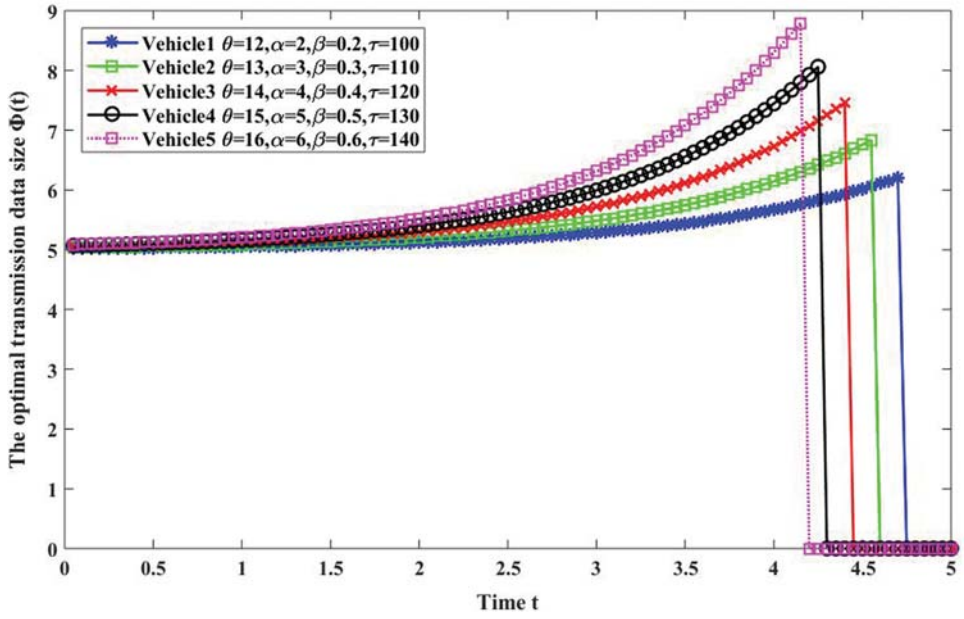

Figure 2: Change of optimal transmission data volume $\phi_j^i(t)$ with time t

The state of the vehicle network channel when the intelligent vehicle transmits virtual data is shown in Fig. 3. It is clear that additional virtual data transmission increases network load,

which harms RSUs and vehicle networks. The more virtual data transmitted, the worse the state of the network channel. When the intelligent vehicle stops transmitting virtual data, the network channel resumes its initial state.

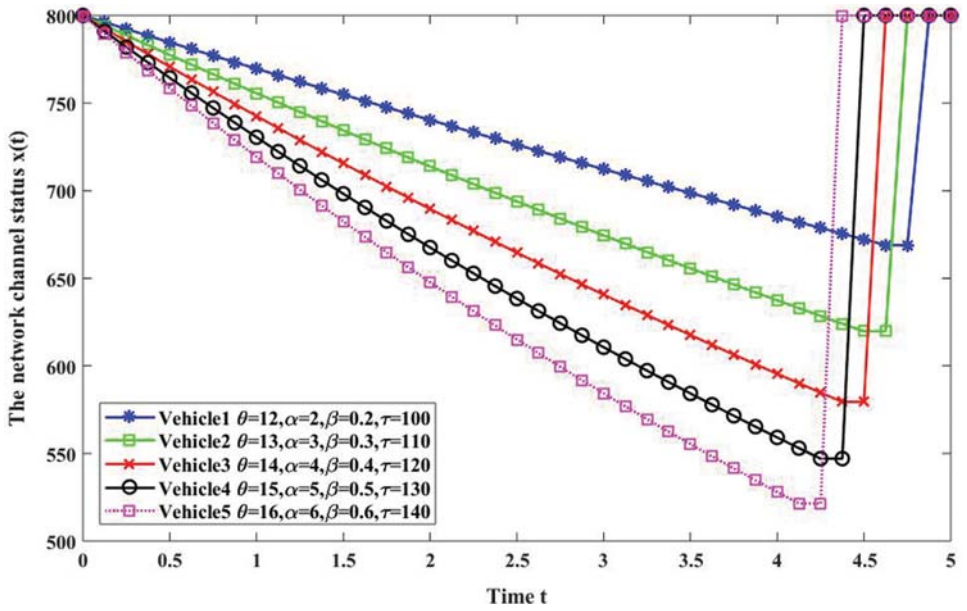

Figure 3: Change of channel state $x(t)$ with time t

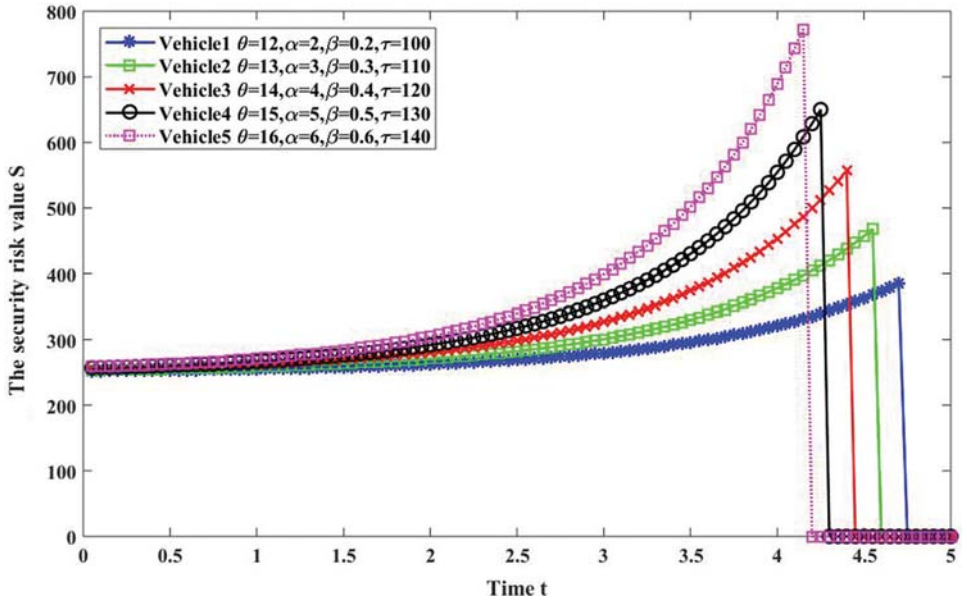

Figure 4: Changes in security risk values over time

The security risks of a vehicle when transmitting virtual data are shown in Fig. 4, from which it can be seen that the transmission of virtual data will bring security risks to the vehicle. With the increase of transmission volume, the security risks suffered by the vehicle increase. The greater the amount of virtual data transmitted, the higher the risk. As the transmission is completed, its security risk will be reduced to the initial state.

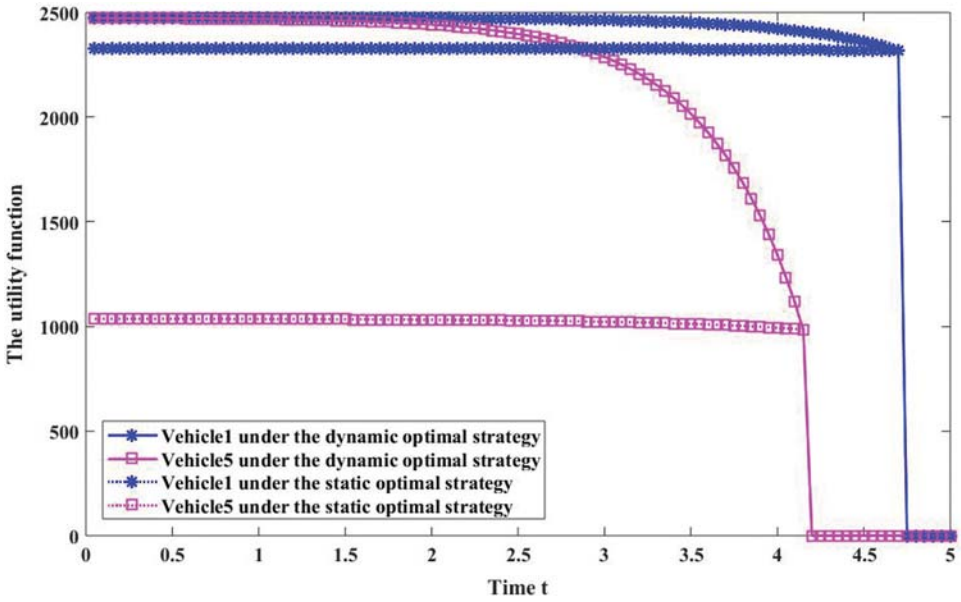

Figure 5: Comparison of dynamic optimal and static optimal game utility functions

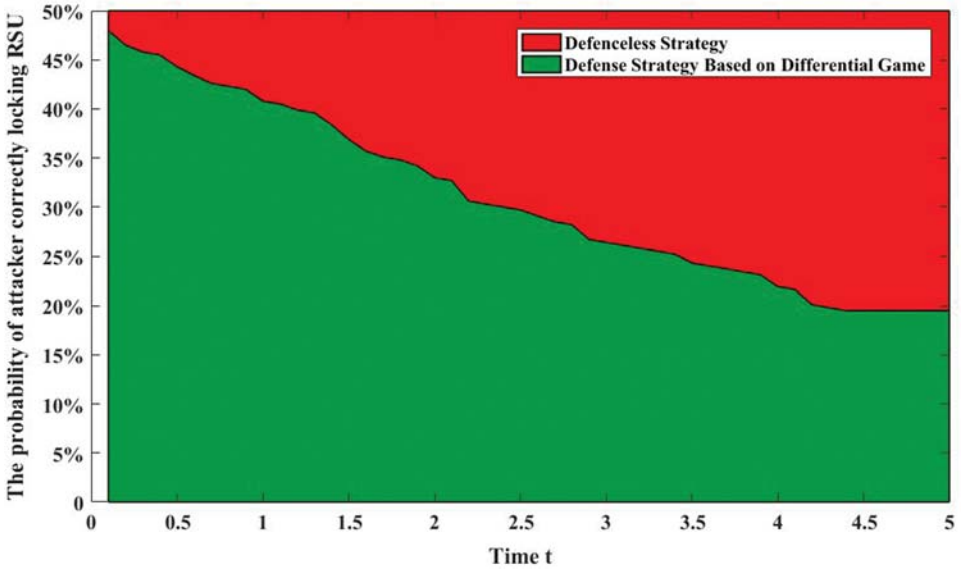

Figure 6: Comparison of probability of a successful hotspot attack

Fig. 5 compares vehicle revenue under the dynamic optimal transmission of the proposed virtual data volume strategy and the static optimal transmission of virtual data volume strategy, from which it can be seen that the benefits of the former are much greater than those of the latter.

Fig. 6 shows the probability of an attacker correctly locking a target RSU with or without a defense plan. Because an RSU misleads attackers by incentivizing vehicles to obtain virtual data, attackers cannot find hotspots, which avoids security threats from hotspot attacks on the RSU. The simulation results in Fig. 6 show that the proposed virtual traffic transmission strategy based on differential games can effectively hide hotspot phenomena, thus protecting the network from RSU hotspot attacks.

From simulation experiments, the quantitative relationship between the amount of data sent by vehicles and the channel state and safety risk can be obtained under the proposed safety model. According to the optimal strategy formed by the game among vehicles, the maximum welfare of the system can be obtained. While protecting the secure communication of the target RSU, the negative influence on the channel state is minimized.

6 Conclusion

Addressing the vulnerability to attack of an RSU in a network of vehicles relying on edge computing, we proposed a security defense scheme using differential game theory. An incentive mechanism was adopted to encourage serviced vehicles within a hotspot to send virtual traffic to another RSU. By attracting the attacker's attention, the target RSU is protected from attack. Additional virtual traffic will increase the network load. Therefore, the system model was established through a differential game, and the optimal virtual data strategy was obtained, so as to balance communication security and network performance. Simulation results showed that the proposed scheme can effectively defend an RSU from hotspot attacks, provide the optimal strategy for the transmission of virtual data volume for intelligent vehicles, and avoid significant degradation of network performance.

In future work, the opportunity interval of vehicle communication will be further considered. By analyzing its statistical model, the virtual data can be made closer to the distribution of real network traffic, so as to hide and protect key RSUs.

Acknowledgement: We gratefully acknowledge the anonymous reviewers who read drafts and made many helpful suggestions.

Funding Statement: This work is supported by Guangxi Vocational Education Teaching Reform Research Project (GXGZJG2020B149), J. G. (Juan Guo).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] W. Han, M. Cheng, M. Lei, H. Xu, Y. Yang *et al.,* "Privacy protection algorithm for the internet of vehicles based on local differential privacy and game model," *Computers, Materials & Continua*, vol. 64, no. 2, pp. 1025–1038, 2020.

[2] J. Contreras-Castillo, S. Zeadally and J. A. Guerrero-Ibañez, "Internet of vehicles: Architecture, protocols, and security," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3701–3709, 2018.

[3] W. Xu, C. Yan, W. Jia, X. Ji and J. Liu, "Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 5015–5029, 2018.

[4] B. Mohammed and D. Naouel, "An efficient greedy traffic aware routing scheme for internet of vehicles," *Computers, Materials & Continua*, vol. 60, no. 3, pp. 959–972, 2019.

[5] X. Wang, W. Wang, L. T. Yang, S. Liao, D. Yin *et al.,* "A distributed HOSVD method with its incremental computation for big data in cyber-physical-social systems," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 2, pp. 481–492, 2018.

[6] L. Zhang, W. Cao, X. Zhang and H. Xu, "MAC2: Enabling multicasting and congestion control with multichannel transmission for intelligent vehicle terminal in internet of vehicles," *International Journal of Distributed Sensor Networks*, vol. 14, no. 8, pp. 1–20, 2018.

[7] X. Huang, R. Yu, M. Pan and L. Shu, "Secure roadside unit hotspot against eavesdropping based traffic analysis in edge computing based internet of vehicles," *IEEE Access*, vol. 6, pp. 62371–62383, 2018.

[8] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, 2017.

[9] J. Zhang and K. B. Letaief, "Mobile edge intelligence and computing for the internet of vehicles," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 246–261, 2020.

[10] C. Gong, F. Lin, X. Gong and Y. Lu, "Intelligent cooperative edge computing in internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9372–9382, 2020.

[11] Z. Li, X. Zhou, Y. Liu, H. Xu and L. Miao, "A non-cooperative differential game-based security model in fog computing," *China Communications*, vol. 14, no. 1, pp. 180–189, 2017.

[12] S. Yang, "A task offloading solution for internet of vehicles using combination auction matching model based on mobile edge computing," *IEEE Access*, vol. 8, pp. 53261–53273, 2020.

[13] A. Nanda, D. Puthal, J. J. P. C. Rodrigues and S. A. Kozlov, "Internet of autonomous vehicles communications security: Overview, issues, and directions," *IEEE Wireless Communications*, vol. 26, no. 4, pp. 60–65, 2019.

[14] C. Wu, X. Chen, T. Yoshinaga, Y. Ji and Y. Zhang, "Integrating licensed and unlicensed spectrum in the internet of vehicles with mobile edge computing," *IEEE Network*, vol. 33, no. 4, pp. 48–53, 2019.

[15] S. Oussama, S. Harous and Z. Aliouat, "A new heuristic clustering algorithm based on RSU for internet of vehicles," *Arabian Journal for Science and Engineering*, vol. 44, no. 11, pp. 9735–9753, 2019.

[16] J. Chen, K. He, Q. Yuan, G. Xue, R. Du *et al.,* "Batch identification game model for invalid signatures in wireless mobile networks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 6, pp. 1530–1543, 2017.

[17] J. Liu, Y. Li, H. Wang, D. Jin, L. Su *et al.,* "Leveraging software-defined networking for security policy enforcement," *Information Sciences*, vol. 327, no. C, pp. 288–299, 2015.

[18] M. Arif, G. Wang and V. Balas, "Secure VANETs: Trusted communication scheme between vehicles and infrastructure based on fog computing," *Studies in Informatics & Control*, vol. 16, no. 6, pp. 235–246, 2018.

[19] B. Ying, D. Makrakis and H. T. Mouftah, "Dynamic mix-zone for location privacy in vehicular networks," *IEEE Communications Letters*, vol. 17, no. 8, pp. 1524–1527, 2013.

[20] S. Basudan, X. Lin and K. Sankaranarayanan, "A privacy-preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing," *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 772–782, 2017.

[21] L. Wang, G. Liu and L. Sun, "A secure and privacy-preserving navigation scheme using spatial crowdsourcing in fog-based VANETs," *Sensors*, vol. 17, no. 4, pp. 668–683, 2018.

[22] H. Hui, C. Zhou, S. Xu and F. Lin, "A novel secure data transmission scheme in industrial internet of things," *China Communications*, vol. 17, no. 1, pp. 73–88, 2020.

[23] H. Li, Y. Yang, Y. Dai, S. Yu and Y. Xiang, "Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data," *IEEE Transactions on Cloud Computing*, vol. 8, no. 2, pp. 484–494, 2020.

[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 Transactions on Parallel and Distributed Systems*, vol. 23, no. 10, pp. 1805–1818, 2012.

[25] T. Mylvaganam, M. Sassano and A. Astolfi, "A differential game approach to multi-agent collision avoidance," *IEEE Transactions on Automatic Control*, vol. 62, no. 8, pp. 4229–4235, 2017.

[26] D. Yeung, "Dynamically consistent cooperative solution in a differential game of transboundary industrial pollution," *Journal of Optimization Theory and Applications*, vol. 134, no. 1, pp. 143–160, 2007.