A Game Theory Based Intrusion Detection Model for Vehicle CAN-Bus Network

Xiang Xu, Fei Li*, Lulu Gao, Yong Liu

School of Cybersecurity, Chengdu University of Information Technology, Chengdu, China

*corresponding author's e-mail: lifei@cuit.edu.cn

Keywords: vehicle CAN bus security; intrusion prevention; game theory; security gateway

Abstract: This paper analyzes the problem of the security defense of in-vehicle electronic information systems. According to the low energy consumption of the intrusion detection system based on game theory and the characteristics of active defense, proposed a CAN bus security gateway based on game theory, which effectively solves the problem of passive defense and energy consumption of existing car security gateways, and proves that it is theoretically feasible.

1. Introduction

With the rapid development of the global automotive industry, the popularity of the information industry, especially the mobile Internet, the comprehensive deployment of the Internet of Vehicles industry has set off a wave of informatization and intelligence in the automotive industry. Major auto companies have increased the intelligence of automobiles through independent research and development or cooperation with IT companies, but with the increase of intelligence, cars have more abundant in-vehicle information functions and applications (such as smart navigation, Intelligent parking), at the same time some security risks to be discovered by hackers, resulting cars to be hacked frequently. The hacker uses the physical interface to access the CAN bus through the OBD(On-Board Diagnostics), and then directly monitors and destroys the CAN bus network; It can also be connected to the car entertainment system through wireless LAN or RF technology, and then eavesdrop on part of the CAN bus information or destroy the CAN bus network through the car entertainment system; Or through the mobile Internet to eavesdrop, intercept, tamper with the information between the car and the remote server, seriously threatening the driver's personal and property safety. Therefore, the safety problem of the in-vehicle electronic information system needs to be solved urgently.

It is not difficult to see from these hacking incidents that people are mainly focused on the car CAN bus network. The in-vehicle electronic information system is composed of a plurality of different types of bus networks (mainly using a CAN bus network), and these bus networks are connected by an in-vehicle gateway. If an attacker wants to monitor or destroy the car CAN bus, it needs to through the car gateway to connect to the car's internal CAN bus network Therefore, the research on the car CAN bus security gateway can not only isolate the data between the bus networks inside the car, but also effectively prevent the hacker through the external network from invading the car power system and ensure the safety of the in-vehicle electronic information system.

2. Related Research

Groza, Murvay used several modified broadcast protocols for authentication, and they verified the protocol [1] [2], they also found that the source of the message can be inferred by using the signal characteristics of the CAN bus [3], which provides a detection method for can bus attack detection.

Zhang Zijian, Zhang Yue et al. analyzed the attack model of CAN bus. An abnormality detection system applied to CAN bus is proposed [4], The system establishes an anomaly detection table and monitors the real-time data of the ECU (Electronic Control Unit) to determine whether the value of the ECU is within a legal range at each moment. It is proved by experiments that the system can

  DOI: 10.25236/isaicn.2019.078

effectively detect abnormal frames.

Qin Gui, Yu He analyzed the safety status of the on-board CAN bus network, summarized the potential security vulnerabilities of the on-board CAN system, for the CAN bus network has the characteristics of periodic determination and stable number of messages [5]. The theoretical analysis method of information entropy of CAN network information system is proposed to deal with the attacks, such as discarding, modifying, reading, spoofing, flooding and replaying. The experimental results show that the method based on information entropy and message relative distance can be used for anomaly detection of vehicle CAN bus network [6].

Although the design of these in-vehicle security gateways meets the requirements of in-vehicle equipment to a certain extent and has certain security protection functions, But these intrusion detection systems have these shortcomings, with a lot of calculations, higher system power consumption and a certain delay. Due to the resource limitations of the car gateway itself, the intrusion detection system needs to share limited resources with other applications, ensuring the real-time forwarding of data while ensuring the normal operation of the intrusion detection system. So we are need involve the choice of different strategy in the process of dealing with issues such as car status and intrusion detection efficiency, In order to make the efficiency of the intrusion detection system as high as possible and reduce the waste of resources as much as possible, it is not only necessary to predict the attack strategy of the attacker when selecting the defense decision, but also to consider the cost of the defense. So as to achieve the optimal balance between the safety and efficiency of the in-vehicle electronic information system, the game theory model is an effective way to solve the problem of intrusion detection and intrusion detection of the in-vehicle electronic information system.

3. Intrusion Detection System Based on Game Theory

Game theory is the study of mathematical models of strategic interaction between rational decision-makers. The parties involved in the game each have different goals or interests. In order to achieve their respective goals and interests, all parties must consider the various possible action plans of their opponents and try to choose the best or most reasonable solution for themselves.

Although game theory has not been applied to the security defense of in-vehicle electronic information systems so far, with the research and expansion of game theory, game theory has gradually been applied to intrusion detection systems.

As early as 1997, Syverson [7] proposed the idea of using a random game theory to rationally analyze normal and malicious nodes in the network. In 2002, Lye and Wing [8] used stochastic games theory to formalize and implement the idea of Syverson, and gave an example of application in the enterprise network, analyzing the Nash equilibrium and the respective optimal actions when both the enterprise and the attacker play the game.

Cao Hui, Wang Qing-qing proposed an attack prediction model based on static Bayesian game [9]. By simulating the offensive and defensive behavior choices of attackers and defenders, the model predicts the probability that rational attackers and defenders will choose to attack and defend, in order to maximize their respective benefits, make Passive detection becomes initiative and targeted defense possible.

Zuo Jun proposed an intrusion detection model based on repeated game theory [10], and established a repeated game model algorithm for detecting malicious communication nodes. Experiments show that the model can effectively suppress malicious node attacks and improve network efficiency.

Xiong Zi-li, Han Lan-sheng proposed a wireless sensor network intrusion detection model based on game theory [11], and proved that the system can not only effectively resist multiple network attacks, but also reduce the energy consumption caused by intrusion detection systems, extends the life of the network.

Through the above literature analysis, the introduction of game theory into the vehicle intrusion detection system can solve the problems of large amount of calculation, energy consumption and delay.

4. Research on Vehicle Security Gateway Based on Game Theory

Internet of Vehicles is a typical application of Internet of Things technology in implementing intelligent transportation. With the development of the Internet of Vehicles, the degree of intelligentization of automobiles has increased, and at the same time, automotive electronic information systems are facing more and more security problems. Existing automotive security gateways have been unable to meet the current automotive information security protection needs. Therefore, this paper proposes a research idea of car safety gateway model based on game theory, as shown in Figure 1. It is designed to balance the resource consumption between the normal communication activity of the gateway and the intrusion detection system, and to maximize the positive detection rate of the intrusion detection system.

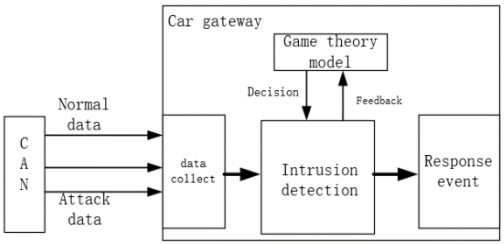

Figure 1. Vehicle Security Gateway Model Based on Game Theory.

The intrusion detection system is an active defense system. According to certain security policies, by monitoring the running status of the network and the system, various attack attempts, attacks, or attack results are discovered as much as possible to ensure the confidentiality of network system resources, Integrity and availability. Due to the resource limitations of the car gateway itself, the intrusion detection system needs to share limited resources with other applications, ensuring the real-time forwarding of data while ensuring the normal operation of the intrusion detection system. Therefore, it is necessary to balance the resource consumption between the gateway normal communication activity and the intrusion detection systems.

4.1 Game Theory Model

This paper introduces the game theory into the intrusion detection system, studies the offensive and defensive equilibrium problem, correctly evaluates the damage caused by the attack behavior, establishes the mathematical model of the decision control process, selects the more correct decision for the defensive behavior, and effectively solves the intrusion detection system Efficiency and energy consumption issues.

In the in-vehicle electronic information system, an attacker attacks the car ECU in order to obtain revenue, attempts to destroy the normal work of the electronic information system, interferes with or controls the vehicle; The intrusion detection system monitors the system in order to make sure the normal work of the system, ensuring that the car is protected from attack. So choose a non-cooperative game theory model. In the process of attack and defense, the attacker and the intrusion detection system repeatedly repeat the offensive and defensive process, so this is a repeated game theory model; However, in each game, there is no fixed sequence of actions between the attacker and the defender, and the latter does not know the strategy adopted by the first actor, which is a static game process; Since the CAN bus is a multi-master broadcast bus, all data in the CAN network is transmitted in plaintext, so it is assumed that both the attacker and the defender have accurate information on the other party's characteristics, policy space, and revenue function, so the game process is in line with a complete information game. Therefore, we choose a non-cooperative complete information static game model.

Definition: The game model expressions for Attack and defense of the vehicle electronic information system can be simply recorded as:

$$G = \{(D, A), (S_{D,} S_A), (U_D, U_A)\} \quad (1)$$

Participant: The first tuple (D, A) defined in (1) represents the player. The D refers to Defender,

the decision maker of the intrusion detection system, The A refers to Attacker.

Strategy space: The second tuple (S_D, S_D) defined in (1) represents the decision space of two participants. Suppose the car has i ECUs, labeled E_1, $E_2 \cdots E_i$, we assume that the attacker can only attack at most one ECU in one attack behavior, and the car defender can only choose to start an ECU intrusion response strategy at a time. Then in each game, for an ECU, the attacker has two strategies: attack (denoted as A_1); no attack (denoted as A_2), $S_A = \{A_1, A_2\}$. For the defender, there are two options for the protection strategy of an ECU: start the ECU intrusion detection (denoted as C_1); do not start the ECU intrusion detection (denoted as C_2), $S_D = \{C_1, C_2\}$. This gives all the policy combinations of the attacker and the defender, as shown in the following matrix T:

$$\mathrm{T} = \begin{bmatrix} (C_1, A_1) & (C_1, A_2) \\ (C_2, A_1) & (C_2, A_2) \end{bmatrix}. \tag{2}$$

Income function: The third tuple (U_D, U_A) defined in (1) represents the income function. Before calculating the income function of both offense and defense, we first define the symbols needed to construct the income function, as shown in Table 1.

TABLE I. Income Function Symbol Definition

Symbol	definition
$U(t)$	income of normal operation of in-vehicle electronic information system at time T
V_{alue}	Average value of each ECU in the system
DC_i	The cost of the intrusion detection system launching a defense strategy for the i-th ECU
U_a	Attack node utility function
AC_i	The cost of attacking the i-th ECU
L_i	The income of the attacker attacking the i-th ECU
E	The income from the attacker listening to the data of the i-th ECU

In the above definition,$L_i = \sum V_{alue}$,the attacker's income is equal to the sum of all the losses of the attack node and the associated node. $V_{alue} \gg DC_i$,The cost of the node being attacked is much higher than the cost of launching a defense strategy. Using the symbols defined in Table 1, the attacker's income matrix M and the defender's income matrix N can be calculated.

$$\mathrm{M} = \begin{bmatrix} -U_a & E \\ L_i - AC_i & E \end{bmatrix} \tag{3}$$

$$N = \begin{bmatrix} U(t) - DC_i & U(t) - DC_i \\ U(t) - \mathrm{V}_{alue} & U(t) \end{bmatrix} \tag{4}$$

In the intrusion detection attack and defense game model, each node can independently determine the action strategy., and the gateway acts in strict accordance with the policy. Each node will get the income ($U(t)$) when it runs normally. Each node will have a certain cost (DC_i) when it launches a defense strategy, such as the gateway resource occupancy or energy consumption, At this time, the node incomes is $U(t) - DC_i$. When the node does not launch the defense strategy and is attacked, the cost will be much greater than the consumption of the defense policy. In this case, the node incomes is $(t) - V_{alue}$. If the attacker does not attack, it will listen to the network information and create conditions for future attacks, so the attacker will get the income is E. When the attacker launches an attack and is detected by the intrusion detection system, the gateway temporarily quarantines the data of the ECU node, and the attacker will get the income is $-U_a$.

4.2 Nash Equilibrium Solution

In the intrusion detection attack and defense game model, because $E < L_i - AC_i$, the attacker always tries to launch an attack in order to maximize the incomes. For the attacker, the biggest benefit is that when the attacking node, the attacked node does not initiate the intrusion detection.

However, the attacker must also consider the worst case. When the attacker launches the attack, the defender also activates the intrusion detection system. This means that the more frequently the attack is launched, the greater the probability of being detected. Once detected, the Nodes will be quarantined, and the attacker will lose the most incomes. the defender needs to consume certain resources to start the intrusion detection, if no attack behavior occurs most of the time, the node keeps the detection system open, which consumes a lot of resources and reduces the network life cycle. For the defense node, its biggest benefit is not to start the intrusion detection system, but because it be attacked loss is much greater than the startup intrusion detection system consumption, the defense node must consider the possibility of being attacked, and have necessary to start the intrusion detection system to ensure the security of the in-vehicle electronic information system. In the in-vehicle electronic information system, an attacker can attack any ECU, and the intrusion detection system can also initiate different defense strategies to protect any ECU. Therefore, the following conclusions:

Conclusion: This game theory model does not have a pure strategy Nash equilibrium.

This conclusion is in line with our expectations, because in this game model, neither the attacker nor the defender has an absolute dominant strategy. Assume that the attacker's optimal strategy is to attack ECU A. The defender's optimal defensive strategy is to defend against ECU B. Obviously, when an attacker attacks ECU A, the benefit of defending ECU A will be much greater than that of defending ECU B. This will encourage the defender to defend against ECU A. Similarly, when the defender defends ECU A, the attacker obviously chooses another attack strategy in order to obtain more incomes. Both the offense and the defense cannot be stabilized, so the game model does not have a purely strategic Nash equilibrium.

According to the existence theorem of Nash equilibrium, the game of any finite strategy must have a Nash equilibrium of the hybrid strategy. Constructible hybrid strategy matrix $P = \begin{bmatrix} \alpha & 1-\alpha \\ \beta & 1-\beta \end{bmatrix}$, Use α to indicate the probability of ECU i initiating intrusion detection, and β to indicate the probability of an attacker attacking ECU I, Therefore, the probability of not initiating the intrusion detection is $1-\alpha$, and the probability of not launching the attack is $1-\beta$.

So, the attacker's hybrid strategy yield function is:

$$\begin{aligned} \mathrm{U}_A^1 &= (L_i - AC_i)(1-\alpha)\beta + (-U_a)\alpha\beta + E(1-\alpha) \\ &= (L_i - AC_i)(1-\alpha)\beta - U_a\alpha\beta E(1-\alpha) \end{aligned} \tag{5}$$

The defender's hybrid strategy yield function is:

$$\begin{aligned} \mathrm{U}_D^1 &= (U(t) - DC_i)(1-\alpha)\beta + (U(t) - \mathrm{V}_{alue})\alpha\beta + U(t)(1-\alpha)(1-\beta) \\ &+ (U(t) - \mathrm{V}_{alue})\alpha(1-\beta) \\ &= DC_i\alpha\beta + U(t) - \alpha\mathrm{V}_{alue} - DC_i\beta \end{aligned} \tag{6}$$

It can be seen from the mixed strategy benefit function of the attacker and the defender that the mixed strategy α, β is inverse proportional. When the hybrid strategy starts the intrusion detection system with a large probability α, the probability of the attack being detected will increase accordingly, and the attacker's income will decrease. At this time, the attacker should reduce the attack probability β; If the defense node initiates intrusion detection, no attack behavior is detected, the gateway resources are wasted, and the benefit of the defense node is also reduced. Therefore, the defense node gradually reduces the probability α of initiating the intrusion detection. As α decreases, the attacker gradually increases the attack probability β in order to obtain higher incomes. In the end, a dynamic balance point, the Nash equilibrium, is reached between the attacker and the defender.

Due to the dynamic characteristics of the vehicle, we need to adopt different defense strategies for different ECUs. At the same time, depending on the different state of the car, the required defense strategies are also different. According to the above conclusions, in order to achieve the Nash equilibrium in the process of repeated games between the attacker and defender, it is necessary to formulate a defense strategy (α,1-α) according to the periodic dynamics of the current situation of the

network. makes the defensive strategy of the in-vehicle electronic information system constantly change in the offensive and defensive, achieves dynamic balance, and fully utilizes limited resources to provide effective security protection for the automobile.

5. Simulation

In order to verify the accuracy of the model proposed in this paper, CANoe software was selected to simulate the model, and Matlab was used for data analysis, and real-time data of a pure domestic electric vehicle was used as test data. And the behavior of the intruder is randomly generated in the test data as the abnormal data, and the game theory model is used to analyze the game situation, and the best response decision is obtained. Under the same conditions, we compare the intrusion detection system based on the game theory model with the traditional intrusion detection system. Figure 2 shows the intrusion detection rate of each intrusion detection algorithm under the same conditions.

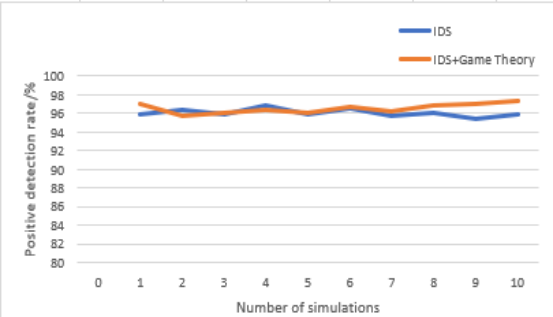

Figure 2. Intrusion Detection Rate Comparison Chart.

It can be seen from Fig. 2 that after using the game theory to model the attack and defense process of the CAN bus network, the detection rate of the system is slightly higher than that of the original intrusion detection system, which satisfies the expected effect.

While conducting the simulation experiment, we evaluate the energy consumption of the intrusion detection system based on the number of detection strategies initiated during the system operation. Assuming that there are N ECUs in the in-vehicle electronic information system, there are N kinds of defense strategies correspondingly, and the game period is T, and in unit time T the energy consumption of the single defense strategy in the system is J.

When all defense policies in the intrusion detection system are started, the energy consumed is W_1, then:

$$W_1 = NTJ \quad (7)$$

When the game theory algorithm is used to analyze and formulate the defense strategy, the starting probability of the defense strategy is $\alpha = \{\alpha_1, \alpha_2, \ldots \ldots \alpha_n\}\ (0 \le \alpha \le 1)$, then the energy consumed at this time is W_2:

$$W_2 = \sum_{i=1}^{N} \alpha JT \quad (8)$$

Energy consumption ratio:

$$\frac{W_1}{W_2} = \frac{NTJ}{\sum_{i=1}^{N} \alpha JT} \quad (9)$$

We substitute the simulation results into equations (7), (8), (9) above to obtain the total energy consumption of the two intrusion detection systems, as shown in Figure 3. The game theory-based intrusion detection system saves nearly 30% energy consumption compared to traditional intrusion detection systems.

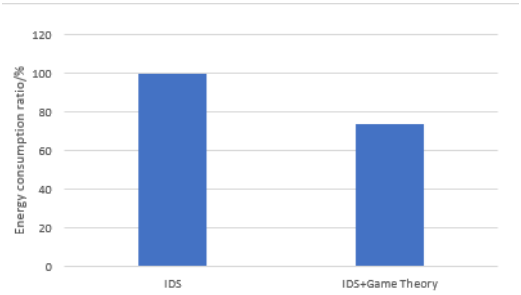

Figure 3. Energy Consumption Ratio.

6. Conclusion

In this paper, the in-vehicle electronic information system is fully researched and analyzed. Proposed a CAN bus security gateway based on game theory , which effectively solves the problem of passive defense and energy consumption of existing car security gateways, and proves that it is theoretically feasible. It provides a new idea for car security gateways. The idea has certain positive significance.

References

[1] B. Groza and P. S. Murvay, “Efficient Protocols for Secure Broadcast in Controller Area Networks.” IEEE Transactions on Industrial Informatics, vol. 9, 2013, pp. 2034-2042.

[2] B. Groza and P. S. Murvay. Broadcast Authentication in a Low Speed Controller Area Network. E-Business and Telecommunications. Springer Berlin Heidelberg, 2012.

[3] P. S. Murvay and B. Groza. "Source Identification Using Signal Characteristics in Controller Area Networks." IEEE Signal Processing Letters, vol. 21, Apr. 2014, pp. 395-399.

[4] ZHANG Zi-jian, ZHANG Yue and WANG Jian, “An Anomaly Detection System Applied to CAN Bus.” Information Security and Communications Privacy, Aug. 2015, pp. 92-96

[5] YU He, QIN Gui-he, SUN Ming-hui, YAN Xin and WANG Xuan-zhe, “Cyber security and anomaly detection method for in-vehicle CAN” Journal of Jilin University(Engineering and Technology Edition), vol. 46, Jul. 2016, pp.1246-1253.

[6] YU he. “Research on Connected Vehicle Cyber Security and Anomaly Detection Technology for In-vehicle CAN Bus.” Diss, 2016

[7] Paul F. Syverson, “A different look at secure distributed computation.” Computer Security Foundations Workshop IEEE, Jun. 1997, pp. 109-115.

[8] Lye K W and Wing J M, “Game strategies in network security.” International Journal of Information Security, vol.4, 2005, pp. 71-86.

[9] CAO Hui, WANG Qingqing, MA Yi-zhong and LUO Ping, “Attack prediction model based on static Bayesian game.” Application Research of Computers, vol. 24, Oct. 2007, pp. 122-124.

[10] ZUO Jun. “Repeated game theory intrusion detection model for the Internet of Things.” Journal of Chongqing University: Natural Science Edition, vol. 37 Jun. 2014, pp. 90-96.

[11] XIONG Zi-li, HAN Lan-sheng, XU Xing-bo, FU Cai and LIU Bu-yu, “Research on Intrusion Detection of Wireless Sensor Networks Based on Game Theory.” Computer Science, vol. 44(s1), 2017, pp. 326-332.