electronics

MDPI

Article

A Study on Enhancing the Information Security of Urban Traffic Control Systems Using Evolutionary Game Theory

Ke Pan, Li Wang * and Lingyu Zhang

Beijing Key Lab of Urban Intelligent Control Technology, North China University of Technology, Beijing 100144, China; panke@mail.ncut.edu.cn (K.P.); zhlyashin@mail.ncut.edu.cn (L.Z.)
* Correspondence: li.wang@ncut.edu.cn

Abstract: In recent years, there has been significant development in intelligent technologies for urban traffic control, such as smart city and vehicle-to-everything (V2X) communication. These advancements aim to provide more efficient and convenient services to participants in urban transportation. As the urban traffic control (UTC) system integrates with various networks and physical infrastructure, the potential threats of malicious attacks and breaches pose significant risks to the safety of individuals and their properties. To address this issue, this academic paper focuses on studying the network structure of the UTC system. A signal security game model is constructed based on the concepts of evolutionary game theory (EGT), involving three parties: attackers, upper computers (UC), and traffic signal machines (TSM). The model aims to analyze the evolutionary stability of the strategies chosen by each party, and to explore the relationships between various factors and the strategy choices of the three parties. Furthermore, the stability of equilibrium points in the three-party game system is analyzed using the Liapunov method. The conditions in which UC and TSM, dependent on detection rates and defense costs, choose to abandon defense at pure-strategy equilibrium points were obtained. Finally, MATLAB is utilized for simulation analysis to validate the impact of attack costs, defense costs, and detection rates on the information security of UTC systems.

Keywords: evolutionary game theory; urban traffic control; information security

Citation: Pan, K.; Wang, L.; Zhang, L. Enhancing the Information Security of Urban Traffic Control Systems Using Evolutionary Game Theory. *Electronics* **2023**, *12*, 4856. https://doi.org/10.3390/electronics12234856

Academic Editor: Felipe Jiménez

Received: 13 October 2023
Revised: 25 November 2023
Accepted: 27 November 2023
Published: 30 November 2023

1. Introduction

In the past, the communication of urban traffic control (UTC) systems used dedicated networks, which resulted in rare occurrences of attacks on traffic signal networks. As a result, research on the security protection of traffic signal networks has not received widespread attention. Li et al. discovered and proved that the currently deployed connected traffic signal systems in the United States have many security vulnerabilities due to system failures. They proposed a game theory framework that promotes network security and efficient traffic management [1,2]. Haddad et al. proposed an elastic boundary control scheme based on the macroscopic fundamental diagram (MFD) to mitigate the impact of network attacks on traffic signal systems. The developed algorithm can adaptively compensate for the effects of attacks without the need for online fault detection. The stability of closed-loop systems regarding tracking and parameter errors is also demonstrated [3]. Khattak et al. analyzed the security vulnerabilities of active traffic management (ATM) in Virginia, providing a method to determine whether the monitoring system is under attack in real time [4]. Other security researchers have also identified various vulnerabilities in traffic signal systems [5].

Research on UTC system security is relatively scarce. Industrial control systems and UTC systems are both cyber-physical systems that share many similarities. Therefore, research on industrial control system security can provide valuable insights. Nateghi et al. studied the problem of online security state estimation and attack reconstruction to design

a resilient controller for systems. The effectiveness of this technique was validated through attack simulations on a real power system [6]. Wang et al. introduced a Bayesian honeypot game model as a bait system for detecting and collecting attack information in advanced metering infrastructure (AMI) in industrial power control systems. This model overcomes the weakness of traditional honeypot technology in detecting dynamic attacks [7]. However, the construction of precise system mechanism models and attack models is complex and challenging, limiting their practical application. Xu et al. proposed a resilient, memory event-triggered scheme (RMETS) for systems. This scheme effectively balances the security performance required by the system with limited network resources in the event of an attack [8].

Research on the information security issues of UTC systems is valuable and necessary. In the process of information attack and defense in UTC systems, attackers and defenders engage in a clear game relationship, making game theory an appropriate method for modeling and analyzing these issues. There have been numerous studies on information security using game theory. Lye et al. applied stochastic game theory to establish a two-player game model for attackers and defenders, obtaining the optimal strategies for both parties by calculating the Nash equilibrium solutions of the model [9]. Zhu et al. employed multi-player non-zero-sum and stochastic game methods to analyze the adversarial behavior between intrusion detection systems and malicious intruders, optimizing the configuration and cooperation of defense systems [10]. Hewett et al. used a complete and perfect information dynamic game approach to analyze the information security of a power grid SCADA system [11]. Game theory has also been applied to defend against distributed denial of service (DDoS) attacks [12–14]. Information security often involves incomplete information games. Shaolin Tan et al. developed an absolute distance-based consensus protocol for multi-agent systems to help agents reach a consensus point without knowing the relative positions of other agents [15]. Singh et al. designed the learning algorithm for the incomplete information game (LAIIG), which effectively updates participants' information machines [16]. Varga B et al. designed near-potential differential games (NPDG) and applied them to large-scale vehicle control systems, verifying the effectiveness of the algorithm [17].

Ahmad F et al. categorized the research on game theory related to traffic into four groups: traffic management, behavioral interactions, routing operation, and transport safety. They found that classical game theory has various limitations, while evolutionary game theory (EGT) is more suitable for simulating real-world scenarios. They mention that Nash equilibrium (NE) does not necessarily guarantee optimal returns for each participant. In some games, there may be multiple NE states, and evolutionary game theory focuses on the decision-making process, which can effectively solve the problem of multiple equilibria. Some scholars have already applied EGT to information security research [18]. Shi L et al. constructed a three-party evolutionary game model of array honeypots composed of defenders, attackers, and legitimate users. By analyzing the strategies and benefits of participants in the game and establishing a three-party game payoff matrix, they obtained evolutionarily stable strategies by analyzing the replicator dynamic equations of each party [19]. Yang Y et al. proposed a multistage asymmetric information attack and defense model (MAIAD) for Internet of Things (IoT) systems. Under the premise of information asymmetry, MAIAD can determine the optimal defense strategy for IoT systems [20]. Their research only focuses on the information level or IoT as the object, without considering the actual situation in the traffic control environment.

In UTC systems, there are often two control entities, upper computers (UC) and traffic signal machines (TSM), which can respond to the impacts of attackers through coordinated control or individual defense. We use EGT analysis tools to explore the stable strategies and system equilibrium points in this three-party attack–defense game. Evolutionary game theory assumes that players are rational given their preferences, but these preferences may evolve over time. In this study, EGT can be represented as follows: attackers in the traffic environment make attack decisions based on individual profit maximization

(i.e., they respond rationally to the current state of the system), while the system state evolves over time, causing changes in the payoffs for attacking and not attacking, leading UC and TSM to replicate and dynamically adjust their defense strategies. Compared to traditional information security research that only focuses on the game between attackers and defenders, the three-party game introduces more uncertainty factors, making cooperation and coordination between UC and TSM more challenging, especially in situations where false negatives and false positives may occur.

This paper answers the following key questions:

(1) In order to counter attacks, what defense strategies should Upper Computers (UC) and Traffic Signal Machines (TSM) adopt?

(2) What defense strategies should Upper Computers (UC) and Traffic Signal Machines (TSM) adopt to counter attacks? How do detection rates and defense costs affect the decision making of the participants?

(3) Is it possible for both UC and TSM to abandon defense in the end? This would be highly undesirable. What conditions might lead to this, and how can we prevent it from occurring?

The remainder of the paper is organised as follows: Section 2 describes the problem and its corresponding assumptions, and establishes the framework of the basic model. Section 3 analyzes the strategy stability of each participant. Section 4 employs the first Lyapunov method to analyze the stability of pure-strategy equilibria of the replicator dynamic system, obtaining evolutionarily stable strategy combinations under different conditions. Sections 5 and 6 conduct numerical simulations and discuss the impact of parameters. Section 7 concludes the research and provides insights.

2. Evolutionary Game Model

To investigate the security issues of a traffic signal network, it is necessary to first understand the network structure of the UTC system, as shown in Figure 1. Typically, the TSM is located near a corresponding intersection, and is responsible for receiving data information from the UC and various traffic detection devices, as well as controlling the traffic signal lights. The UC is housed in the local public transportation management department and is primarily responsible for the coordination, management, and control of the TSMs at each intersection.

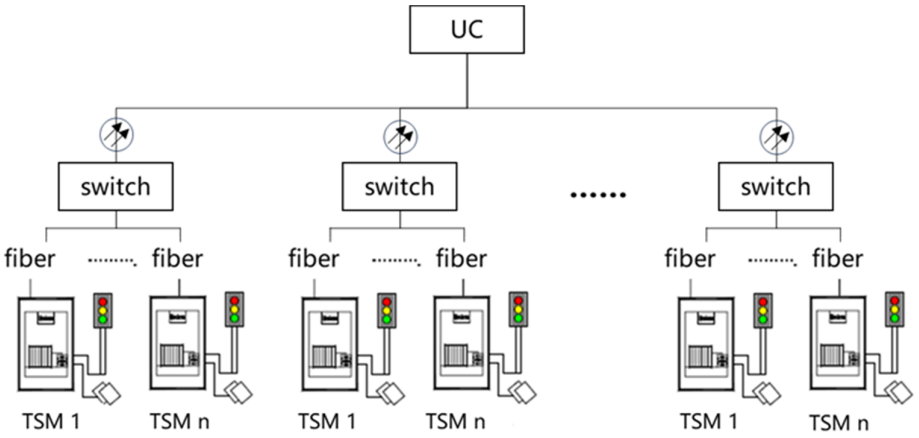

Figure 1. Network structure of the UTC system.

In the UTC system, there are numerous attackers who use various attack methods to disrupt or even paralyze the traffic signal system in order to achieve their own objectives. In response to the malicious behavior of attackers, security personnel in different locations employ various defensive strategies. At the beginning, there is limited knowledge about each other's situation, and through continuous experimentation, they learn about each

other and improve their strategies. Eventually, they find the choices that are most favorable to themselves, leading to a stable state. Therefore, studying these stable states and the conditions for their occurrence is meaningful for ensuring the secure operation of the UTC system. Sometimes, the defense cost may be too high, such as protecting one road smoothly at the expense of causing congestion on others, which is clearly not wise. Finding the conditions under which UC and TSM abandon defense can help security personnel avoid such situations. Similarly, identifying the conditions under which attackers abandon their attacks can effectively reduce security incidents in the UTC system. Therefore, the use of EGT to analyze and study the security game process in the UTC system will be beneficial.

Hypothesis 1. *Let* N_{du} *represent the UC, and its defensive strategy includes selecting defense* (d) *with probability* x *and not defending* (nd) *with probability* $1-x$, $x \in [0,1]$. *Let* N_{ds} *represent the TSM, and its defensive strategy includes selecting defense* (d) *with probability* y *and not defending* (nd) *with probability* $1-y$, $y \in [0,1]$. *Let* N_a *represent the attacker, and its strategy includes selecting attack* (a) *with probability* z *and not attacking* (na) *with probability* $1-z$, $z \in [0,1]$. *Let* α *represent the detection rate of the attack detection system (true positive rate, TPR),* $\alpha \in [0,1]$. β *represents the false alarm rate (false positive rate, FPR),* $\beta \in [0,1]$. S *represents the security value of the traffic network.* Ca *represents the attack cost,* $Ca > 0$. Cdu *represents the individual defense cost of the UC, and* $Cdus$ *represents the UC's defense cost when coordinating with the TSM,* $0 < Cdus < Cdu$. *Let* Cds *represent the individual defense cost of the TSM, and* $Cdsu$ *represent the TSM's defense cost when coordinating with the UC,* $0 < Cdsu < Cds$.

Hypothesis 2. *If both parties in the game are purely rational, the security value of the traffic network S should be greater than any cost. Otherwise, there is no reason for the parties to adopt strategies for the sake of security value [21].*

$$S > max(Ca, Cds, Cdu, Cdsu, Cdus)$$

Next, we discuss the payoffs under various strategies for the attacker when the attacker targets the UC position. When the strategy is (nd, nd, a), the attacker's payoff is $S - Ca$; the payoffs for the two defenders are $-S$. When the strategy is (d, d, a) the UC and TSM engage in coordinated defense; the UC's expected payoff is $\alpha S - (1-\alpha)S - Cdus = (2\alpha - 1)\,S - Cdus$, and the same applies to the TSM. The attacker's payoff is the loss of the defenders' payoff minus the attack cost: $(1-\alpha)S - \alpha S - Ca = (1-2\alpha)\,S - Ca$. When the strategy is (d, nd, a), the UC's payoff for individual defense is $(2\alpha - 1)\,S - Cdu$, the TSM's payoff is $(2\alpha - 1)\,S$, and the attacker's payoff is $(1-2\alpha)\,S - Ca$. When there are no detection errors by the attack detection system, the defenders incur cost: $-\beta Cdx$.

By analyzing the payoffs under various strategies for the participants, we can obtain the evolutionary game payoff matrix of the three-party game, as shown in Table 1. This table reflects the payoff situation of the three parties under various strategy combinations when the attacker chooses a certain attack behavior at a particular moment. If the attacker switches to another attack method, the defensive strategies of the UC and TSM will change accordingly, and the values of the corresponding strategy costs and detection rates will also change.

Table 1. Payoff matrix of the three-party game.

	$N_{du}: d(x)$		$N_{du}: nd(1-x)$	
	$N_{ds}: d(y)$	$N_{ds}: d(1-y)$	$N_{ds}: d(y)$	$N_{ds}: d(1-y)$
$N_a: a(z)$	$(2\alpha-1)S - Cdus$, $(2\alpha-1)S - Cdsu$, $(1-2\alpha)S - Ca$	$(2\alpha-1)S - Cdu$, $(2\alpha-1)S$, $(1-2\alpha)S - Ca$	$(2\alpha-1)S$, $(2\alpha-1)S - Cds$, $(1-2\alpha)S - Ca$	$-S$, $-S$, $S - Ca$
$N_a: na(1-z)$	$-\beta Cdus, -\beta Cdsu, 0$	$-\beta Cdu, 0, 0$	$0, -\beta Cds, 0$	$0, 0, 0$

3. Strategic Stability Analysis

The expected payoff and average expected payoff for the UC when adopting the strategy are

$$\begin{aligned} E_x &= yz\big((2\alpha-1)S - Cdus\big) + (1-y)z\big((2\alpha-1)S - Cdu\big) \\ &\quad + (1-z)y(-\beta Cdus) + (1-z)(1-y)(-\beta Cdu) \\ &= z(2\alpha-1)\,S - yzCdus - (1-y)zCdu \\ &\quad - (1-z)y\beta Cdus - (1-z)(1-y)\beta Cdu \end{aligned} \tag{1}$$

$$E_{1-x} = yz\big((2\alpha-1)S\big) + (1-y)z(-S) \tag{2}$$

$$\overline{E}_x = xE_x + (1-x)E_{1-x} \tag{3}$$

The replicator dynamic equation for the UC, based on the Malthusian equation and combined Equations (1)–(3), is as follows [22,23]:

$$\begin{aligned} F(x) &= \frac{dx}{dt} = x\big(E_x - \overline{E}_x\big) = x(1-x)(E_x - E_{1-x}) \\ &= x(1-x)(z(1-y)2\alpha S - yzCdus - (1-y)zCdu - (1-z)y\beta Cdus - (1-z)(1-y)\beta Cdu) \end{aligned} \tag{4}$$

The expected payoff and average expected payoff for the TSM when adopting the strategy are

$$\begin{aligned} E_y &= xz\big((2\alpha-1)S - Cdsu\big) + (1-x)z\big((2\alpha-1)S - Cds\big) \\ &\quad + (1-z)x(-Cdsu) + (1-z)(1-x)(-Cds) \\ &= z(2\alpha-1)S - xzCdsu - (1-x)zCds \\ &\quad - (1-z)x\beta Cdsu - (1-z)(1-x)\beta Cds \end{aligned} \tag{5}$$

$$E_{1-y} = xz\big((2\alpha-1)S\big) + (1-x)z(-S) \tag{6}$$

$$\overline{E}_y = yE_y + (1-y)E_{1-y} \tag{7}$$

The replicator dynamic equation for the TSM is

$$\begin{aligned} G(y) &= \frac{dy}{dt} = y\big(E_y - yE_y - (1-y)E_{1-y}\big) = y(1-y)(E_y - E_{1-y}) \\ &= y(1-y)(z(1-x)2\alpha S - xzCdsu - (1-x)zCds - (1-z)x\beta Cdsu - (1-z)(1-x)\beta Cds) \end{aligned} \tag{8}$$

The expected payoff and average expected payoff for the attacker when adopting the strategy are

$$\begin{aligned} E_z &= xy\big((1-2\alpha)S - Ca\big) + (1-x)y\big((1-2\alpha)S - Ca\big) \\ &\quad + (1-y)x\big((1-2\alpha)S - Ca\big) + (1-y)(1-x)(S - Ca) \\ &= (y + x - xy)\big((1-2\alpha)S - Ca\big) + (1-y)(1-x)(S - Ca) \end{aligned} \tag{9}$$

$$E_{1-z} = 0 \tag{10}$$

$$\overline{E}_z = zE_z + (1-z)E_{1-z} \tag{11}$$

The replicator dynamic equation for the attacker is

$$\begin{aligned} H(z) &= \frac{dz}{dt} = z\big(E_z - \overline{E}_z\big) = z(1-z)(E_z - E_{1-z}) \\ &= z(1-z)\Big((y + x - xy)\big((1-2\alpha)S - Ca\big) + (1-y)(1-x)(S - Ca)\Big) \end{aligned} \tag{12}$$

Based on the above, the replicator dynamic equation system for the three-party evolutionary game is as follows:

$$\begin{cases} F(x) = x(1-x)(z(1-y)2\alpha S - yzCdus - (1-y)zCdu - (1-z)y\beta Cdus - (1-z)(1-y)\beta Cdu) \\ G(y) = y(1-y)(z(1-x)2\alpha S - xzCdsu - (1-x)zCds - (1-z)x\beta Cdsu - (1-z)(1-x)\beta Cds) \\ H(z) = z(1-z)\left((y+x-xy)\left((1-2\alpha)\,S - Ca\right) + (1-y)(1-x)(S-Ca)\right) \end{cases} \tag{13}$$

According to the principle of evolutionary stability, the probability of strategy choices by participants must satisfy the following conditions to reach evolutionary stability:

$$\begin{cases} F(x) = 0, & dF(x)/dx < 0 \\ G(y) = 0, & dG(y)/dy < 0 \\ H(z) = 0, & dH(z)/dz < 0 \end{cases} \tag{14}$$

First, analyzing the UC by combining Equations (13) and (14):

$$\begin{aligned} z^* &= \frac{y\beta Cdu - y\beta Cdus - \beta Cdu}{2\alpha S - y2\alpha S - yCdus - Cdu + yCdu + y\beta Cdus + \beta Cdu - y\beta Cdu} \\ &= \frac{\beta Cdu + y\beta(Cdus - Cdu)}{(1-\beta)Cdu - 2\alpha S + y((1-\beta)(Cdus - Cdu) + 2\alpha S)} \end{aligned} \tag{15}$$

When $z = z^*$, $F(x) = 0$, the UC's strategy choice remains stable and does not vary over time. When $z > z^*$, $dF(x)/dx|_{x=1} < 0$ and $dF(x)/dx|_{x=0} > 0$. According to Equation (14), we find that $x = 1$ is a stable point, representing the UC's strategy (d) as an evolutionarily stable strategy (ESS). When $z < z^*$, $dF(x)/dx|_{x=0} < 0$ and $dF(x)/dx|_{x=1} > 0$. According to Equation (14), we find that $x = 0$ is an ESS, representing the UC's strategy choice of not defending.

Analyzing the TSM by combining Equations (13) and (14):

$$\begin{aligned} z^{**} &= \frac{x\beta Cds - x\beta Cdsu - \beta Cds}{2\alpha S - x2\alpha S - xCdsu - Cds + xCds + x\beta Cdsu + \beta Cds - x\beta Cds} \\ &= \frac{\beta Cds + x\beta(Cdsu - Cds)}{(1-\beta)Cds - 2\alpha S + x((1-\beta)(Cdsu - Cds) + 2\alpha S)} \end{aligned} \tag{16}$$

When $z = z^{**}$, $G(y) = 0$, the TSM's strategy choice remains stable and does not vary over time. When $z > z^{**}$, $dG(y)/dy|_{y=1} < 0$ and $dG(y)/dy|_{y=0} > 0$. According to Equation (14), we find that $y = 1$ is an ESS, representing the TSM's strategy choice of defending. When $z < z^{**}$, $dG(y)/dy|_{y=1} > 0$ and $dG(y)/dy|_{y=0} < 0$. According to Equation (14), we find that $y = 0$ is an ESS, representing the TSM's strategy choice of not defending.

Lastly, analyzing the attacker by combining Equations (13) and (14):

$$x^* = \frac{y\left((1-2\alpha)S - Ca\right)}{(1-y)2\alpha S} + \frac{S - Ca}{2\alpha S} \tag{17}$$

When $x = x^*$, $H(z) = 0$, the attacker's strategy choice remains stable and does not vary over time. When $x > x^*$, $dH(z)/dz|_{z=1} > 0$ and $dH(z)/dz|_{z=0} < 0$. According to Equation (14), we find that $z = 0$ is an ESS, representing the attacker's strategy choice of not attacking. When $x < x^*$, $dH(z)/dz|_{z=1} < 0$ and $dH(z)/dz|_{z=0} > 0$. According to Equation (14), we find that $z = 1$ is an ESS, representing the attacker's strategy choice of attacking.

4. Equilibrium Point Stability Analysis

By solving $F(x) = 0, G(y) = 0, H(z) = 0$, we obtain 8 pure-strategy equilibrium points, as shown in Table 2. In this paper, the stability of the evolutionary game system is determined using the Liapunov method. Based on the replicator dynamic equation system (13), the Jacobian matrix is as follows:

$$J = \begin{bmatrix} J_1 & J_2 & J_3 \\ J_4 & J_5 & J_6 \\ J_7 & J_8 & J_9 \end{bmatrix} = \begin{bmatrix} \partial F(x)/\partial x & \partial F(x)/\partial y & \partial F(x)/\partial z \\ \partial G(y)/\partial x & \partial G(y)/\partial y & \partial G(y)/\partial z \\ \partial H(z)/\partial x & \partial H(z)/\partial y & \partial H(z)/\partial z \end{bmatrix}$$

$$J_1 = (1-2x)(z(1-y)2\alpha S - yzCdus - (1-y)zCdu - (1-z)y\beta Cdus - (1-z)(1-y)\beta Cdu)$$

$$J_2 = x(1-x)(-z2\alpha S - zCdus + zCdu - (1-z)\beta Cdus + (1-z)\beta Cdu)$$

$$J_3 = x(1-x)((1-y)2\alpha S - yCdus - (1-y)Cdu + y\beta Cdus + (1-y)\beta Cdu)$$

$$J_4 = y(1-y)(-z2\alpha S - zCdsu + zCds - (1-z)\beta Cdsu + (1-z)\beta Cds)$$

$$J_5 = (1-2y)(z(1-x)2\alpha S - xzCdsu - (1-x)zCds - (1-z)x\beta Cdsu - (1-z)(1-x)\beta Cds)$$

$$J_6 = y(1-y)((1-x)2\alpha S - xCdsu - (1-x)Cds + x\beta Cdsu + (1-x)\beta Cds)$$

$$J_7 = -z(1-z)(1-y)2\alpha S$$

$$J_8 = -z(1-z)(1-x)2\alpha S$$

$$J_9 = (1-2z)\Big((y+x-xy)\big((1-2\alpha)S - Ca\big) + (1-y)(1-x)(S-Ca)\Big)$$

Using the Liapunov first method [24], if all eigenvalues of the Jacobian matrix have negative real parts, the equilibrium points are asymptotically stable. If at least one eigenvalue of the Jacobian matrix has a positive real part, the equilibrium points are unstable. If the Jacobian matrix has eigenvalues with real parts equal to zero, while the remaining eigenvalues have negative real parts, the equilibrium points are in a critical state and their stability cannot be determined solely by the sign of the eigenvalues. The stability of each equilibrium point is analyzed as follows:

Table 2. Stability analysis of equilibrium points.

	$\boldsymbol{\lambda_1}$	$\boldsymbol{\lambda_2}$	$\boldsymbol{\lambda_3}$	**Symbol** [1]	**Stability** [2]
(0,0,0)	$S - Ca$	$-\beta Cds$	$-\beta Cdu$	$(+,-,-)$	no
(1,0,0)	βCdu	$-\beta Cdsu$	$(1-2\alpha)S - Ca$	$(+,-,?)$	no
(0,1,0)	βCds	$-\beta Cdus$	$(1-2\alpha)S - Ca$	$(+,-,?)$	no
(0,0,1)	$2\alpha S - Cds$	$2\alpha S - Cdu$	$Ca - S$	$(?,?,-)$	?
(1,1,0)	$\beta Cdsu$	$\beta Cdus$	$(1-2\alpha)S - Ca$	$(+,+,?)$	no
(1,0,1)	$-Cdsu$	$-2\alpha S + Cdu$	$Ca - (1-2\alpha)S$	$(-,?,?)$	?
(0,1,1)	$-Cdus$	$-2\alpha S + Cds$	$Ca - (1-2\alpha)S$	$(-,?,?)$	?
(1,1,1)	$Cdsu$	$Cdus$	$Ca - (1-2\alpha)S$	$(+,+,?)$	no

[1] The symbol represent the signs of the real parts of the eigenvalues $(\boldsymbol{\lambda_1}, \boldsymbol{\lambda_2}, \boldsymbol{\lambda_3})$, where "+" indicates a positive real part, "−" indicates a negative real part, and "?" indicates an unknown sign, requiring further discussion. [2] Stability indicates whether the equilibrium point is stable, where "?" indicates unknown stability, necessitating further discussion.

For the equilibrium point (0,0,1), when $2\alpha S = Cdu$ or $2\alpha S = Cds$, the equilibrium point is in a critical state and its stability cannot be determined by the sign of the eigenvalues. When $2\alpha S < Cdu$ and $2\alpha S < Cds$, the equilibrium point is asymptotically stable. This indicates that when the detection rate is too low or the defense cost is close to the security value, both the UC and TSM evolve to a stable state of not defending due to their own interests. As a result, the system is vulnerable to attacks, and poses a serious threat

to the safety of urban public transportation. To avoid the situation where the game stabilizes at the strategy combination (nd, nd, a), traffic signal system security workers should strive to increase the detection rate and reduce the defense cost.

For the equilibrium point (1,0,1), by the same analysis, when $2\alpha S = Cdu$ or $Ca = (1-2\alpha)S$, the equilibrium point is in a critical state and its stability cannot be determined by the sign of the eigenvalues. When $2\alpha S > Cdu$ and $Ca < (1-2\alpha)S$, the equilibrium point is asymptotically stable. This indicates that when the detection rate is high or the defense cost of the UC is low, for their own interests, the evolutionary stable strategy combination for the three parties will stabilize at the strategy combination (d, nd, a), indicating that the UC will actively defend against the attacker's attacks.

For the equilibrium point (0,1,1), by the same analysis, when $2\alpha S = Cds$ or $Ca = (1-2\alpha)S$, the equilibrium point is in a critical state and its stability cannot be determined by the sign of the eigenvalues. When $2\alpha S > Cds$ and $Ca < (1-2\alpha)S$, the equilibrium point is asymptotically stable. This indicates that when the detection rate is high or the defense cost of the TSM is low, for their own interests, the evolutionary stable strategy combination for the three parties will stabilize at the strategy combination (nd, d, a), indicating that the TSM will actively defend against the attacker's attacks.

5. Simulation

To verify the effectiveness of the stability analysis, numerical values are assigned to the model and numerical simulations are conducted using MATLAB. The parameters used are as follows:

$$(\alpha = 0.4, \beta = 0.1, S = 100, Cdus = 10, Cdu = 30, Cdsu = 10, Cds = 30, Ca = 10)$$

These parameters satisfy the conditions for the equilibrium points (1,0,1) and (0,1,1) to be asymptotically stable. To analyze the impact of different initial strategy probabilities for each participant on the overall evolutionary path, initial strategy probability combinations (x, y, z) are randomly selected within [0,1]. The evolutionary results are shown in Figure 2. Although different initial strategy probabilities lead to different evolutionary rates, they all converge to (1,0,1) and (0,1,1), confirming the correctness of the theoretical derivation.

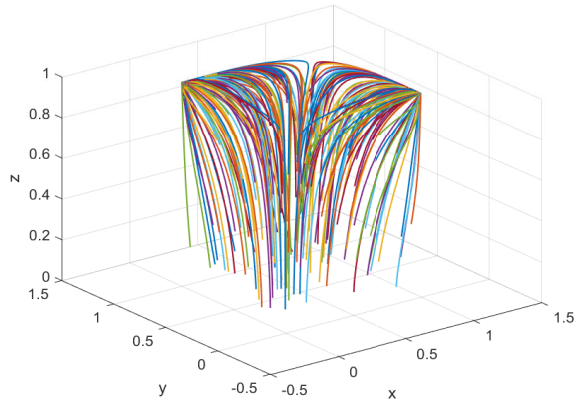

Figure 2. Impact of different initial strategy probabilities.

Next, we conducted a simulation of the attack–defense evolution process of the UTC system based on the data from Case Study I [21]. The system security value (S) was set to 200, and the security requirements were represented by $Ca = Cds = Cdu = 20, Cdsu = Cdus = 10$. The TPR and FPR were set to α = 91.78%, β = 0.25%., respectively. The initial state of the game was set to (0.2,0.2,0.2). After 50 iterations, we obtained the replicating

dynamics of the evolving game, as shown in Figure 3. The trajectory exhibits a spiral convergence, indicating a mixed−strategy equilibrium. At this point (0.286,0.286,0.017), the attacker tends to abandon the attack, while both UC and TSM adopt active defense.

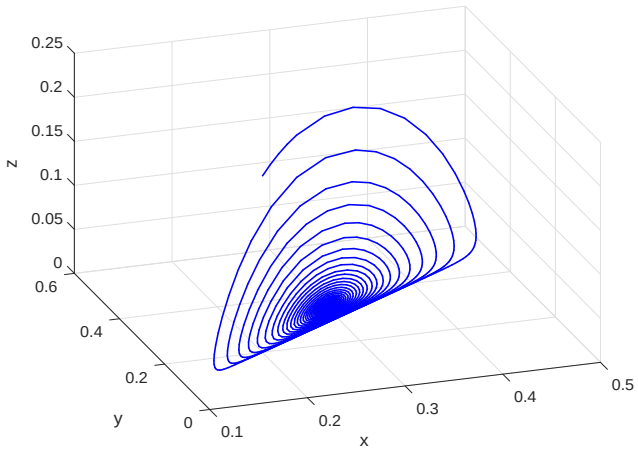

Figure 3. Evolutionary trajectory of mixed-strategy stability.

To compare the security systems of the UC and TSM, we set $Cds = 30, Cdsu = 15$, while keeping the other parameters unchanged. After 50 iterations, we obtained the replicating dynamics of the evolving game, as shown in Figure 4. The trajectory forms a closed loop around the central point, indicating the instability of the three-party game. In this scenario, TSM abandons defense due to its high cost, and the ratio between the attacker and UC remains in constant flux.

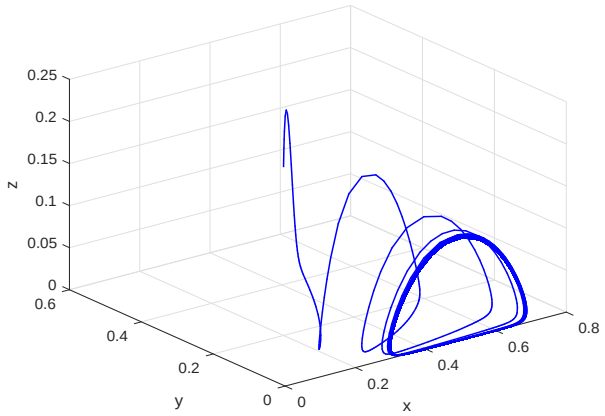

Figure 4. Unstable evolutionary trajectory.

In order to analyze the influence of each parameter on the three-party strategy selection, we set the parameters to satisfy the condition of a pure strategy equilibrium point (1,0,1), with α = 40% and keeping the other parameters unchanged. Then, we varied one of the parameters and observed the changes in the trajectory.

First, we analyze the impact of the detection rate on the evolutionary process and results. Setting the detection rate $\alpha = 0.2,0.3,0.4$, the results after 50 iterations are shown in Figure 5. Decreasing the detection rate accelerates the evolutionary rate of the attacker's

strategy choice of attack. With an increased detection rate, the UC's probability of adopting the defense strategy increases, while the attacker's probability of choosing the attack strategy decreases. Therefore, information security personnel should strengthen the research and development of corresponding attack detection technologies to increase the detection rate and reduce the probability of system attacks.

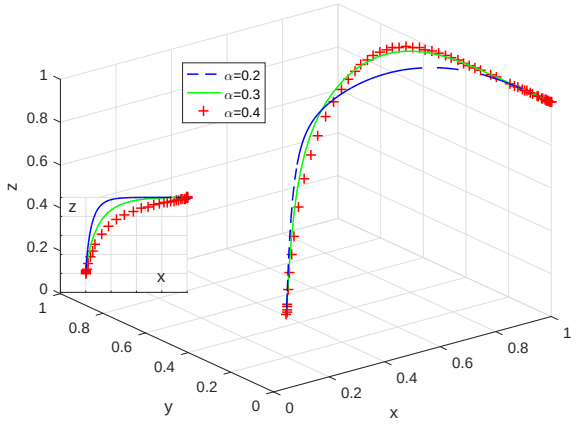

Figure 5. Impact of the detection rate.

Next, we analyze the impact of defense cost on the evolutionary process and results. Setting the defense cost $Cdu = 10,20,30$, the results after 50 iterations are shown in Figure 6. The results show that during the evolutionary process, as the defense cost increases, the UC's probability of adopting the defense strategy decreases, while the attacker's probability of choosing the attack strategy increases. Therefore, reducing the cost of defense strategies is an effective means of ensuring the safe and stable operation of the traffic system.

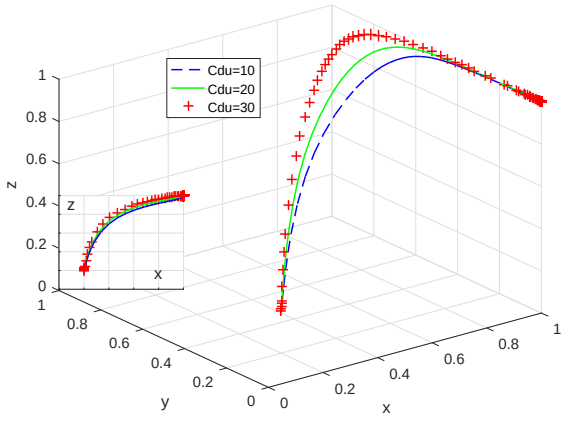

Figure 6. Impact of defense cost.

Lastly, we analyze the impact of the attack cost. Setting the attack cost $Ca = 10,20,30$, the results after 50 iterations are shown in Figure 7. It can be observed that as the attack cost increases, the UC's probability of adopting the defense strategy increases, while the attacker's probability of choosing the attack strategy decreases. From a system design perspective, designers should focus on designing more secure systems, increasing the cost of attacks, and reducing the probability of being attacked.

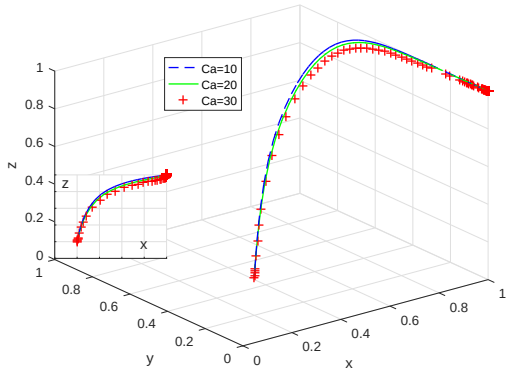

Figure 7. Impact of attack cost.

6. Discussion

The simulated results above reveal the impact of the main parameters on the three-party behavioral strategy evolution and provide different final states of the three-party game evolution under various conditions, which can increase the probability of attackers abandoning their attacks. We found that higher detection rates and comparable attack and defense costs can effectively encourage attackers to abandon their attacks. Lower TPR and higher defense costs can significantly increase the probability of the UTC system being attacked, leading to a tendency for defenders to abandon defense, which is highly dangerous.

The factors influencing the evolutionary dynamics of the UTC system information security can be divided into three priority levels based on their impact. The first priority is TPR, the second priority is defense cost, and the third priority is attack cost. Based on the simulation results, we combined the probabilities of attack and defense to determine the degree of influence of these factors. As shown in Figures 5–7, among all the influencing factors, TPR has the most significant impact, followed by defense cost, while the impact of attack cost is the smallest.

In comparison with the Bayesian game method in [21], the evolutionary game approach allows for a more intuitive understanding of the degree of influence of each parameter on the three-party strategy selection. It helps identify various final evolutionary game states and their corresponding conditions, as well as the evolutionary process from the initial state to the final state. The accuracy of the analysis results of the Bayesian game method is highly dependent on the selection of prior probabilities. Therefore, our approach is more advantageous in assisting researchers in analyzing information security issues in UTC systems.

7. Conclusions

The issue of information security in UTC systems has received relatively little attention. However, as they become increasingly integrated with various information networks, information security concerns are becoming more prominent. In this paper, a three-party evolutionary game model was constructed to analyze the network structure of UTC systems and the interactions between attackers, the UC, and the TSM. The stability of strategy choices for each party, the stability of equilibrium strategy combinations in the game system, and the relationships between various factors were analyzed. The validity of the conclusions was verified through simulation analysis. The main conclusions and insights are as follows.

In situations where the attack detection rate is high and the attack defense costs are unequal, there is no system ESS, and the behavior of the participants exhibits periodic characteristics. However, in situations where the attack detection rate is high and the attack defense costs are equal, the system trajectory converges in a spiral and then stabilizes.

This finding suggests that UTC systems' security personnel can gradually reduce the probability of system attacks by controlling the TPR and costs.

The attack detection rate and defense cost are negatively correlated with the probability of system attacks and positively correlated with the defense rate. These parameters can be further optimized and prioritized based on their impact on the evolutionary dynamics of the system's attack and defense. Therefore, security personnel should focus their efforts on developing strategies that address specific priorities.

Finally, as the attack detection rate decreases and defense costs increase to a certain extent, the system will tend to abandon defense and the probability of being attacked will significantly increase. Therefore, UTC systems' security personnel should continuously monitor new attack methods in the field of information security, and regularly update the system's detection and defense methods.

Author Contributions: Conceptualization, L.W. and K.P.; methodology, K.P.; software, K.P.; validation, K.P.; formal analysis, K.P.; resources, L.W.; data curation, L.Z.; writing—original draft preparation, K.P.; writing—review and editing, K.P.; visualization, L.Z.; supervision, L.Z.; project administration, L.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Beijing Municipal Science and Technology Plan grant number Z221100008122006.

Data Availability Statement: The related authors are willing to provide the data used to support the study's findings upon request, but only for research purposes. Informed consent was obtained from all subjects involved in the study.

Conflicts of Interest: The authors declare that they have no conflict of interest.

Abbreviations

UTC	urban traffic control
UC	upper computers
TSM	traffic signal machines
EGT	evolutionary game theory
ESS	evolutionary stable strategy
TPR	true positive rate
FPR	false positive rate
Variables	
x	the probability of UC adopting a defensive strategy
y	the probability of TSM adopting a defensive strategy
z	the probability of attackers choosing an offensive strategy
Parameters	
α	detection rate of attacks
β	false positive rate of attacks
Cdu	the individual defense cost of the UC
$Cdus$	the UC's defense cost when coordinating with the TSM
Cds	the individual defense cost of the TSM
$Cdsu$	the TSM's defense cost when coordinating with the UC
S	the security value of the traffic network

References

1. Li, Z.Y.; Jin, D.; Hannon, C.; Shahidehpour, M.; Wang, J.H. Assessing and mitigating cybersecurity risks of traffic light systems in smart cities. *IET Cyber-Phys. Syst. Theory Appl.* **2017**, *1*, 60–69.
2. Li, Z.Y.; Shahidehpour, M. Deployment of cybersecurity for managing traffic efficiency and safety in smart cities. *Electr. J.* **2017**, *30*, 52–61.
3. Haddad, J.; Mirkin, B. Resilient perimeter control of macroscopic fundamental diagram networks under cyberattacks. *Transp. Res. Part B Methodol.* **2020**, *132*, 44–59.
4. Khattak, Z.H.; Park, H.; Hong, S. Investigating cybersecurity issues in active traffic management systems. *Transp. Res. Rec. J. Transp. Res. Board* **2018**, *2672*, 79–90.
5. Ghena, B.; Beyer, W.; Hillaker, A. Green lights forever: Analyzing the security of traffic infrastructure. In Proceedings of the 8th USENIX conference on Offensive Technologies, San Diego, CA, USA, 19 August 2014.
6. Nateghi, S.; Shtessel, Y.; Edwards, C. Resilient control of cyber-physical systems using adaptive super-twisting observer. *Asian J. Control* **2023**, *25*, 1775–1790.
7. Wang, K.; Du, M.; Maharjan, S. Strategic honeypot game model for distributed denial of service attacks in the smart grid. *IEEE Trans. Smart Grid* **2017**, *8*, 2474–2482.
8. Xu, Y.; Chai, S.; Shi, P. Resilient and event-triggered control of stochastic jump systems under deception and denial of service attacks. *Int. J. Robust Nonlinear Control* **2023**, *33*, 1821–1837.
9. Lye, K.W.; Wing, J.M. Game strategies in network security. *Int. J. Inf. Secur.* **2005**, *4*, 71–86.
10. Zhu, Q.; Tembine, H.; Tamer, B. Network security configurations: A nonzero-sum stochastic game approach. In Proceedings of the American Control Conference, Baltimore, MD, USA, 30 June–2 July 2010.
11. Hewett, R.; Rudrapattana, S.; Kijsanayothin, P. Cyber-security analysis of smart grid SCADA systems with game models. In Proceedings of the 9th Annual Cyber and Information Security Research Conference, Oak Ridge, TN, USA, 8–10 April 2014; pp. 109–112.
12. Mairaj, A.; Javaid, A.Y. Game theoretic solution for an Unmanned Aerial Vehicle network host under DDoS attack. *Comput. Netw.* **2022**, *211*, 108962.
13. Vetha, S.; Vimala, D.K. A trust-based hypervisor framework for preventing DDoS attacks in cloud. *Concurr. Comput. Pract. Exp.* **2019**, *33*, e5279.
14. Gao, C.; Wang, Y. Reinforcement learning based self-adaptive moving target defense against DDoS attacks. *J. Phys. Conf. Ser.* **2021**, *1812*, 012039.
15. Tan, S.; Wang, Y. A payoff-based learning approach for Nash equilibrium seeking in continuous potential games. *Neurocomputing* **2021**, *468*, 431–440.
16. Singh, M.T.; Borkotokey, S.; Lahcen, R.A.; Mohapatra, R.N. A generic scheme for cyber security in resource constraint network using incomplete information game. *Evol. Intell.* **2022**, *16*, 819–832.
17. Varga, B.; Inga, J.; Hohmann, S. Limited Information Shared Control: A Potential Game Approach. *IEEE Trans. Hum. Mach. Syst.* **2023**, *53*, 282–292.
18. Ahmad, F.; Shah, Z.; Al-Fagih, L. Applications of evolutionary game theory in urban road transport network: A state of the art review. *Sustain. Cities Soc.* **2023**, *98*, 104791.
19. Shi, L.; Wang, X.; Hou, H. Research on Optimization of Array Honeypot Defense Strategies Based on Evolutionary Game Theory. *Mathematics* **2021**, *9*, 805. https://doi.org/10.3390/math9080805.
20. Yang, Y.; Che, B.; Zeng, Y.; Cheng, Y.; Li, C. MAIAD: A Multistage Asymmetric Information Attack and Defense Model Based on Evolutionary Game Theory. *Symmetry* **2019**, *11*, 215. https://doi.org/10.3390/sym11020215.
21. Zhang, J.; Liu, X.; Zhu, P. Cooperation Stimulation and Security in Wireless Ad Hoc Networks—A Power-Efficient Bayesian Game Approach. In Proceedings of the 2016 IEEE 24th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS), London, UK, 19–21 September 2016. https://doi.org/10.1109/MASCOTS.2016.8.
22. Taylor, P.D.; Jonker, L.B. Evolutionary stable strategies and game dynamics. *Math. Biosci.* **1978**, *40*, 145–156.
23. Schuster, P.; Sigmund, K. Replicator dynamics. *J. Theor. Biol.* **1983**, *100*, 533–538.
24. Khalil, H.K. *Nonlinear Systems*; Prentice-Hall: Upper Saddle River, NJ, USA, 1996.