Journal of Combinatorial Mathematics
and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Research on the Construction of Evolutionary Stabilization and Signaling Game Model for IoT Privacy Protection

He Jiang[1], Xiaoru Li[1,]✉

[1] *Taiyuan University, Taiyuan, Shanxi, 030012, China*

ABSTRACT

In this paper, we understand the shortcomings of the current mainstream IoT privacy protection methods through analysis, and in this way, we propose an evolutionary and signaling game model for IoT privacy protection. The model analyzes the stabilization trend of IoT platform penalty coefficients on privacy protection and provides protection strategies. Combining the implications of the signaling game model, the degree of IoT privacy protection is measured using the Bayesian equilibrium solving algorithm. Simulation experiments are conducted to evaluate the specific effect of the model on IoT privacy protection. The increase in the detection rate of the model accelerates the convergence of the probability of malicious nodes, e.g., when the detection rate increases from 0.7 to 0.9, the convergence time is reduced by about two stages. The larger the penalty amount of the IoT platform, the model recommends more aggressive protection strategies, and the probability increases from 0.16 to about 0.4. The game parameters of the model reflect the malicious behavior in IoT, and the trust level affects the game parameters. The model in this paper reduces the attack gain by 4% to 10% compared with the comparison model when the fixed defense gain is 1500, which can better reflect the influence of protection signals on the attacker's actions.

Keywords: Evolutionary game, signaling game, Bayesian equilibrium solving, privacy protection

1. Introduction

Game theory is the study of the decision-making behavior of players with conflicting interests, in which two or more players must make choices that may affect the interests of other players, and each player in the game increases his or her own benefits through competition [1]. From the definition of game theory, the process of interaction between the two parties involved in the game is similar to the process of interaction between the attacking and defending parties in privacy protection, so game theory is suitable for analyzing and modeling the IoT privacy protection problem, so as to study the decision-making process of the participants, and it has different characteristics from those in the classical

✉ Corresponding author.
E-mail address: lixiaorucomputer@163.com (X. Li).
Received 10 January 2024; Revised 15 February 2024; Accepted 25 December 2024; Published Online 15 April 2025.
DOI: 10.61091/jcmcc127a-232

optimization problem, which is conducive to the study of the generalization of the privacy problem [2-3].

Evolutionary stabilization is that the game parties continuously improve their strategies until they reach a dynamic equilibrium, which ultimately makes the system in a stable state [4]. The process of evolutionary game has two main types of actions, selection and mutation, the strategy with high adaptability in the population will be selected by more individuals, and become more and more popular until the population strategy reaches a stable state, and a few individuals may randomly select a strategy, and this mutation may lead to a higher return or a lower return, the strategy with a better return will be selected by the individuals, and the strategy with a low return generated by the mutation will be extinguished, the population is stabilized through this continuous selection and mutation, and the strategy with a lower return will become extinct. Through this constant selection and mutation, the population finally reaches the evolutionary stable strategy [5-7]. The signaling game is a kind of dynamic game with incomplete information, and the participants in the signaling game know their own utility function explicitly, but they cannot know the utility function of their opponents exactly [8-10]. Signal senders and receivers are the players in a signaling game, which explores the possibility that an action by a signal sender may deliver a particular message to a signal receiver who subsequently participates in the game.

Currently, most of the IoT applications are connected through wireless communication, so the miscreants can obtain the information sent by each node by eavesdropping on the wireless signals [11-13]. Like traditional networks, IoT also needs to be protected to authenticate nodes, prevent misuse, detect anomalies and protect node privacy [14-16]. Privacy protection in IoT mainly includes data privacy protection and location privacy protection. Among them, data privacy protection is mainly aimed at such attacks, i.e., the attacker attacks the private data transmitted by the node to achieve the purpose of stealing or tampering with the information, or the attacker directly captures the node and modifies it for his own use, and privacy protection techniques such as cryptographic security, data anonymization, etc., are mainly adopted to deal with this type of attack [17-18]. Location privacy protection techniques are mainly used such as authentication and multiple pseudonyms [19-20].

Therefore, constructing models for IoT privacy protection using evolutionary stabilization and signaling games can optimize IoT privacy strategies.

The first section of the study provides an overview of the architecture of the Internet of Things (IoT) and privacy protection methods, on the basis of which a novel IoT privacy protection method is proposed. The method integrates the evolutionary stability and signaling game models, and the evolutionary game model can determine the stability of the equilibrium point to provide the best strategy for privacy protection. The signaling game model seeks the optimal node detection strategy and attack strategy through Bayesian principle. Both of them interact with each other to effectively reduce the harm of malicious nodes and maximize the degree of privacy protection.

2. Overview

IoT privacy security involves the privacy protection of people's food, clothing, housing, and transportation, and scholars have used game theory to simulate the evolution of these privacy security problems in order to find a suitable protection strategy. Literature [21] then plays a signaling game with edge nodes and IoT nodes to optimize the IoT trust management strategy. Similarly, literature [22] plays a game with IoT devices and edge nodes and derives an evolutionary stable strategy to maximize the revenue, and shows that the IoT data sharing privacy protection scheme is effective and correct after performing the final simulation.

For the social networks that we often come into contact with in our life, literature [23] proposes a game theoretic framework and successfully constructs a model for user relationship and privacy protection decision-making in community networks, which helps social network administrators to design reasonable charging mechanisms and management strategies on the one hand, and encourages

community users to implement privacy protection measures on the other hand. In personal social networks, personality privacy is also a focus area, so literature [24] uses game theory and data encryption to construct a personality privacy protection framework, and simulation results show that this framework effectively balances the backward problem between crowdsourcing services and privacy policies in mobile crowdsourcing for better protection of personality privacy. Vehicles are also intelligent in life, and game theory is also applied to in-vehicle autonomous networks [25], and vehicle whereabouts data also involves privacy and security issues. Literature [26] has done research on reputation management of vehicle networking, using evolutionary game to construct an exercise model for dynamic attack strategies, and simulation experiments show that the final result of evolution can be quantified in reputation management of vehicle networking. Whereas, literature [27] utilized a game between vehicle data holders and requesters to enable them to find a balance between privacy concessions and incentive motivations to protect privacy security. Also.

Furthermore, literature [28] provides a framework that synthesizes interpretable artificial intelligence, federated learning, game theory, and social psychology to deal with IoT cyber-attacks. Attacks are a major aspect that threatens IoT privacy, as they are often attacked with malicious intent. Therefore, literature [29] uses two-layer game theory among advanced persistent threat attackers, IoT defenders, and cyber insurance to prove that welfare-optimal cyber insurance can cover half of the defender's loss. Whereas there must exist a defense for the attack, the signaling game is to use the two as the two sides of the game. For example, literature [30] constructs a moving target defense of signaling game for the defense strategy under attacking behavior, focusing on the defender. And literature [31] constructs a two-way signaling game model focusing on both attacking and defending parties, and the results show that the deception defense strategy is the most available strategy for the defending party in cybersecurity. However, there are various types of defensive deception for online privacy security, and literature [32] uses game theory to conceptualize their classification and provide a systematic basis for their understanding.

3. Key knowledge and technologies

3.1. Research on Privacy Protection in the Internet of Things

3.1.1. IoT architecture. The Internet of Things, as a rather complicated but well-organized system of division of labor, is characterized by close association with enterprises, long industrial chain, multiple links, multiple terminals, multiple devices, and strong interaction. The upper layer is a platform hub, distributed with data storage centers and cloud servers, the role of the middle layer is to carry out preliminary processing and transmission of data, and the bottom layer is a large number of terminal devices, so it seems that the Internet of Things is actually a typical “end-pipe-cloud” structure. In this way, IoT is actually a typical “end-pipe-cloud” structure. This section organizes several most representative architectures proposed at home and abroad, in order to provide theoretical guidance for subsequent research and application implementation.

1) Basic Architecture. When defining a generic architecture for IoT, early researchers and organizations mainly considered the development of the industry and the urgent needs of the growing number of devices, and therefore proposed a simple three-layer structure, consisting of a perception layer, a network layer, and an application layer from the bottom up.

Subsequent practice has proven that the three-layer structure does not meet the actual IoT environment, because the “network layer” does not cover all the underlying technologies for transmitting data to the IoT platform.

2) SOA-based architecture. Service Oriented Architecture (SOA), as a key technology for integrating heterogeneous systems or devices, can support IOT based on SOA. SOA-based IOT architecture is a five-layer structure: perception layer, object abstraction layer, middleware layer, application layer, and management layer. The middleware layer pairs services with their requesters based on address and

name, enabling IOT applications to handle heterogeneous objects without regard to specific hardware platforms. The management layer monitors and manages the underlying four layers.SOA is considered as an architecture that supports multiple ways to achieve interoperability between heterogeneous devices.

3) Cloud-based edge computing architecture. In recent years, IoT infrastructure has also been integrated with some emerging technologies such as cloud computing and fog computing All sensors and actuators are connected to the cloud, and the information generated by the sensors is processed in the cloud, and the results of the calculations are returned to the actuators. This is actually an ideal model from an information flow perspective: the cloud can be easily updated with control functions, and big data technologies can be used to analyze the datasets generated by the sensors and feed back to the control algorithms to optimize productivity.

4) Information-centric (ICN) architecture. With the popularization of 4G and 5G, multimedia-based content distribution services have gradually become the core business of the Internet.The core idea of ICN is to cache copies of popular content through inter-network caching and routing mechanisms to reduce the waste of resources caused by repeated transmissions in the network. At the same time, information-centered, content and host are unbundled, breaking the host-centered naming rules of TCP/IP protocol, and data exchange between nodes is based on the name of the content rather than the address of the target.

3.1.2. IoT Privacy Protection Methods. In order to protect IoT privacy, especially in the release and use of data, some privacy-preserving approaches have been proposed.

1) k-anonymization [33] makes information about a particular data indistinguishable from at least k-1 other information by removing some of the key information. However, the privacy-preserving ability of k-anonymity is often unsatisfactory; on the one hand, it is itself vulnerable to table linking attacks, and on the other hand, k-anonymity itself is a center-based privacy-preserving data dissemination method, where the center of information processing is able to see all of the user's information when privacy-preserving the user's information is processed.

2) Differential Privacy Protection [34] Its mainly discusses the problem of personal data leakage caused by multiple overall data releases. And differential privacy is inevitably brought about by the lack of data accuracy, in the use of big data environment, the use of differential privacy is still very reliable, but to some of the data volume is not too large, or the data accuracy requirements are very high environment, such as smart health care, smart home, etc., may cause huge deviation and make the data can not be used.

3) Federated Learning [35] is a privacy preserving technique in a machine learning environment. Its aim is not to deliver user data to data centers for processing, but to process the data locally. The result is that on the one hand, it ensures that the user has complete ownership of his data. On the other hand, it is able to resist curiosity from the data center about the user's data. Federated learning in practice needs to be complemented by privacy-preserving data aggregation due to its vulnerability to reverse analytics attacks.

After understanding the shortcomings of common methods for IoT privacy protection, this paper constructs an evolutionary stabilization and signaling game model for IoT privacy protection. The specific design process is described below.

3.2. Evolutionary Stability Game Modeling in Privacy Protection

Classical game theory assumes complete rationality as a prerequisite, however, this assumption is difficult to meet in the actual adversarial game. Evolutionary game theory suggests that each participant in the game system is not completely rational, and needs to improve the existing strategies through continuous trial and error, learning and improvement, so that each party tends to a certain balance of interests, and at this time the strategy is no longer changed, and the system presents a stable

state.

3.2.1. Model bases. Evolutionary game [36] mainly contains the following basic elements:
1) Participant space, also known as the game party, contains all the decision makers in the game process, and there are at least two participants, who are finite rationality, they will make their own decisions based on the limited information, and adjust their own strategies according to the results of the game.
2) Game strategy space in each game process the game will be based on the current state of the system, the situation of the participants and so on to choose a guiding program, the set of strategy choices of each game is the strategy space.
3) The set of game benefit function game benefit function is the benefit obtained by the game party adopting a certain strategy.
4) Game belief space game belief is the probability of the game party to take a certain strategy, representing the game party's tendency to choose the degree of strategy.

Evolutionary game theory of stable strategy and replication dynamic equation solution process is as follows:

Suppose that for a certain practical problem, there are multiple groups playing the game at this time, and each group possesses a sufficient number of individuals, and each individual is free to choose its own strategy behavior. The set of groups is denoted as $N = \{1, 2, \ldots, a, u\}$, where a denotes one of the groups in the game, and each individual in the group can randomly choose n kinds of strategies, noting that the combination of strategies in a is $M_a = \{m_{a1}, m_{a2}, \ldots, m_{ai}, \ldots, m_{an}\}$, $i \in \{1, 2 \ldots n\}$, and setting t moments in a the number of groups choosing strategy m_{ai} as $x_{ai}(t)$, accounting for the proportion of $p_{ai}(t)$, and a the group choosing strategy m_{ai} with the expected payoff of $U_{ai}(t)$, and t moments in the average payoff of $\overline{U_a}(t)$. Therefore, we get the basic equations as follows:

$$\sum_{i=1}^{n} p_{ai}(t) = 1 \tag{1}$$

$$p_{ai}(t) = \frac{x_{ai}(t)}{\sum_{i=1}^{n} x_{ai}(t)} \tag{2}$$

$$\overline{U_k^A}(t) = \sum_{i=1}^{n} p_{ki}(t) U_{ki}^A(t) \tag{3}$$

As the game continues, the number of individuals in the a group choosing the m_{ai} strategy changes, and the essence of this change is that the outcome of the game is passed from group to group causing individuals to improve their strategies. The rate of change is actually affected by factors such as the expected payoff of the strategy, the number of individuals choosing m_{ai} and so on. i.e:

$$x_{ai}'(t) = x_{ai}(t) \cdot U_{ai}(t) \tag{4}$$

The replication dynamics equation for the choice m_{ai} strategy can be reasoned as follows:

$$
\begin{aligned}
p_{ai}'(t) &= \frac{x_{ai}'(t)\sum_{i=1}^{n} x_{ai}(t) - x_{ai}(t)\sum_{i=1}^{n} x_{ai}'(t)}{\left[\sum_{i=1}^{n} x_{ai}(t)\right]^2} \\
&= \frac{x_{ai}(t)}{\sum_{i=1}^{n} x_{ai}(t)}\left[\frac{x_{ai}'(t)}{x_{ai}(t)} - \frac{\sum_{i=1}^{n} x_{ai}'(t)}{\sum_{i=1}^{n} x_{ai}(t)}\right] \\
&= p_{ai}(t)\left[\frac{x_{ai}(t)\cdot U_{ai}(t)}{x_{ai}(t)} - \frac{\sum_{i=1}^{n} x_{ai}(t)\cdot U_{ai}(t)}{\sum_{i=1}^{n} x_{ai}(t)}\right] \\
&= p_{ai}(t)\left[U_{ai}(t) - \overline{U_a}(t)\right]
\end{aligned}
\tag{5}
$$

Therefore, it is concluded as follows, when replicating the dynamic equations for evolutionary game analysis, "replicating dynamics" is to carry out a strategy adjustment dynamic mechanism. It is expressed by equation $\frac{dp_{ai}(t)}{dt} = p_{ai}(t)\left[U_{ai}(t) - \overline{U_a}(t)\right]$, where: $\frac{dp_{ai}(t)}{dt}$ indicates the rate of change p in the proportion of a groups adopting the i strategy. $p_{ai}(t)$ indicates the proportion of a groups adopting the i strategy. $U_{ai}(t)$ denotes the expected return for the a group adopting the i strategy. $\overline{U_a}(t)$ denotes the average expected return of all strategies for the a group.

Similarly, the replication dynamics under multiple groups can be introduced:

$$
\begin{cases}
\frac{dp_{1i}(t)}{dt} = p_{1i}(t)\left[U_{1i}(t) - \overline{U_1}(t)\right] \\
\frac{dp_{2i}(t)}{dt} = p_{2i}(t)\left[U_{2i}(t) - \overline{U_2}(t)\right] \\
\frac{dp_{ni}(t)}{dt} = p_{ni}(t)\left[U_{ni}(t) - \overline{U_n}(t)\right]
\end{cases}
\tag{6}
$$

The replication dynamics equation is labeled with ratio $F_a(t) = \frac{dp_{ai}(t)}{dt}$. Calculation $F_a(t) = 0$ then yields the equilibrium solution, the equilibrium point of the replication dynamics equation, that is, the point at which the proportion of players adopting a particular strategy choice is in a steady state throughout the change in replication dynamics.

3.2.2. Stability analysis. The Lyapunov system stability discrimination method is as follows: the replicated dynamic equations of all game parties are associated to construct the replicated dynamical system equation (6), and the Jacobi determinant $J = \left(J_{ij}\right)_{n\times n}$ is computed as follows:

$$
J = \begin{bmatrix}
J_{11} & J_{12} & \cdots & J_{1n} \\
J_{21} & J_{22} & \cdots & J_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
J_{n1} & J_{n2} & \cdots & J_{nn}
\end{bmatrix}
\tag{7}
$$

After the equilibrium point is calculated, the stability of the equilibrium point is determined by analyzing the positivity and negativity of the characteristic root.

3.3. Signaling game based privacy protection model for IoT

The main work of signaling game [37] includes:
1) Based on the consideration of detection rate and false alarm rate, trust degree and attack lethality are introduced to construct the IoT privacy protection model based on signaling game.
2) Firstly, the static signal game is analyzed, then the static game is expanded into a multi-stage dynamic game, and the beliefs of the nodes are updated using Bayesian principle, which proves the existence of multi-stage dynamic equilibrium in the model, and the degree of privacy protection of IoT is measured using information entropy, which provides optimal strategies for the nodes, and also provides suggestions for the IoT to take privacy protection measures.

Table 1 shows the symbols used in the following and their representative meanings.

Table 1. Symbol definition

Symbol	Meaning
α	The lethal degree of attack
β	Test rate
θ	False rate
TD	Trust
σ	The probability of an attack by a malicious node of the internet of things
γ	The probability of testing by a malicious node of the internet of things
g_a	Object network malicious node attack benefit
g_b	The benefits of collaborative interaction with the internet of things
g_c	The iot detection node detects the benefit of the attack
c_a	The cost of attack on the internet of things
c_b	Cost of cooperation between the internet of things
c_e	The cost of detecting the detection node of the internet of things
c_d	The malicious node of the internet of things is cheated
m_c	The internet detection node is missing the loss

3.3.1. IoT privacy-preserving signaling game models. The privacy protection game model can be represented as a seven-tuple $\left[N,K,S,p,\overline{p},U,T\right]$ with the following implications:

1) N is the set of participants in the game, $N=\{\text{IoT detection node, IoT node}\}$.

2) K represents the set of participant types in the signaling game, $K=K_D\cup K_z$, where $K_D=\{k_D\}$ is the set of IoT detection node types, k_D represents detection nodes: $K_z=\{k_z=0,k_z=1\}$ is the set of IoT node types, $k_z=0$ represents normal nodes, and $k_i=1$ represents malicious nodes.

3) S is the set of strategies of the game participants, $S=S_D\cup S_z$ where $S_D=\{Detect,Idle\}$ is the set of strategies of the detecting nodes, Detect stands for Detect and Idle stands for Idle. $S_z\left(k_z=0\right)=\{Cooperate\}$ is the set of strategies for normal nodes, Cooperate represents cooperation, and $S_z\left(k_z=1\right)=\{Cooperate,Attack\}$ is the set of strategies for malicious nodes, Attack represents attack.

4) p is the a priori concept that represents the initial probability that an IoT node belongs to a malicious node.

5) $\overline{p}$ is the posterior probability, which represents the probability that the IoT node belongs to the malicious node as updated by the detection node through observation and detection using Bayesian formula.

6) U is the set of payoffs for the participants of the game, and $U=U_D\cup U_z$, represents the set of payments corresponding to the different strategies chosen by the detection node, and the IoT node,

respectively.

7) $T=\{t_1,t_2,\ldots,t_n\}$ represents the stage of the game.

When a malicious node tries to attack the IoT so as to waste its resources and affect the normal operation of the network, this attack will bring a benefit to the malicious node g_a, and at the same time the malicious node adopts the attack will incur a corresponding cost c_a, βg_c represents the loss of the malicious node being detected. When the malicious node takes cooperation, this camouflage cooperation process will bring gain g_b and gain trust gain TD, and also will incur resource cost c_b as well as a deception loss c_d. For the detection node, when it takes detection behavior and the node chooses to attack, it will incur detection gain βg_c and detection cost c_e, while α is introduced to represent the lethality of the attack of the malicious node, and the loss caused by node's attack is $\alpha(1-\beta)g_a$, β and θ denote the detection rate and false alarm rate, respectively, where false alarm rate is the probability that the detecting node will misreport the node taking cooperation as an attack, and m_c denotes the false alarm loss. Based on the above analysis, the payment matrix is obtained as shown in Table 2.

Table 2. The payment matrix of the privacy protection signal game

S_p \ S_z	Detect	Idle
The node is a malicious node		
Attack	$(1-\beta)g_a-c_a-\beta g_c$ $\beta g_c-c_e-\alpha(1-\beta)g_a$	g_a-c_a $-g_a$
Cooperate	$g_b-c_b-c_d+TD$ $-c_e-\theta m_c$	$g_b-c_b-c_d+TD$ 0
The node is a normal node		
Cooperate	$g_b-c_b-c_d+TD$ $-c_e-\theta m_c$	$g_b-c_b-c_d+TD$ 0

In this paper, we adopt strategy entropy to measure the degree of privacy protection, noting P as the probability of nodes adopting cooperation, and H as the uncertainty of information, the smaller the value of H means that the uncertainty of the variables is getting smaller and smaller, the larger the amount of information available, and the smaller the corresponding degree of privacy protection. Then by the information entropy theory, for one game can be obtained:

$$H = P\log_2 P-(1-P)\log_2(1-P) \tag{8}$$

where P is equal to the probability of a normal node plus the probability of a malicious node multiplied by the probability of cooperation, viz:

$$P=1-p+p(1-\sigma)=1-p\sigma \tag{9}$$

For finitely repeated games can be obtained:

$$H=-\sum_{s\in S_i(k-1)}P^t(s)\log_2 P^t(s)+\left(1-P^t(s)\right)\log_2\left(1-P^t(s)\right) \tag{10}$$

where P^t denotes the probability that node t takes cooperation in the game phase.

3.3.2. Bayesian Equilibrium Solving for the Internet of Things Privacy Signaling Game:

1) Multi-stage game equilibrium. Assuming, stage games t_n and t_{n-1} have the same payoff matrix, i.e., in this paper, we do not consider the discounting of payoffs in the multi-stage signaling game, $h_s(t_n)$ is the history of node k_z's actions, $S_z(t_n)$ denotes node $(k_z=1)$'s actions in t_n, and

$p\left(k_z=1 \mid S_z\left(t_n\right), h_s\left(t_n\right)\right)$ is the posteriori inference, which denotes the probability that the node is a malicious node in stage t_n. It is obtained by Bayes' law:

$$\begin{aligned} & p\left(k_z=1 \mid S_z\left(t_n\right), h_s\left(t_n\right)\right) \\ & =\frac{p\left(k_z=1 \mid h_s\left(t_n\right)\right) p\left(S_z\left(t_n\right) \mid k_z=1, h_s\left(t_n\right)\right)}{\sum_{k_z \in K_z} p\left(k_z \mid h_s\left(t_n\right)\right) p\left(S_z\left(t_n\right) \mid k_z', h_s\left(t_n\right)\right)} \end{aligned} \tag{11}$$

Since there is a detection rate β and a false alarm rate θ for IoT detection nodes in detecting other nodes, the effect of β and θ will be taken into account in the calculation of $p\left(S_z\left(t_n\right) \mid k_z, h_s\left(t_n\right)\right)$, which can be obtained:

$$p\left(Attack \mid k_z=1, h_s\left(t_n\right)\right)=\beta \sigma+\theta(1-\sigma) \tag{12}$$

$$p\left(Cooperate \mid k_z=1, h_s\left(t_n\right)\right)=(1-\beta) \sigma+(1-\theta)(1-\sigma) \tag{13}$$

$$p\left(Attack \mid k_z=0, h_s\left(t_n\right)\right)=\theta \tag{14}$$

$$p\left(Cooperate \mid k_z=0, h_s\left(t_n\right)\right)=1-\theta \tag{15}$$

Malicious node in phase t_n with strategy $\omega_{z_n}=\left(\sigma_n, 1-\sigma_n\right)$, Detecting node in phase t_n with strategy $\omega_{D_n}=\left(\gamma_n, 1-\gamma_n\right)$, and for Detecting node to take Detect in phase t_n, the expected gains of Idle are respectively:

$$\begin{aligned} E_{U_D}(Idle) & =-\sigma_n p\left(k_z=1 \mid h_s\left(t_n\right)\right) g_a \\ & +\left(1-\sigma_n\right) p\left(k_z=1 \mid h_s\left(t_n\right)\right) * 0 \\ & +\left(1-p\left(k_z=1 \mid h_s\left(t_n\right)\right)\right) * 0 \\ & =-\sigma_n p\left(k_z=1 \mid h_s\left(t_n\right)\right) g_a \end{aligned} \tag{16}$$

$$\begin{aligned} E_{U_p}(Detect) & =\sigma_n p\left(k_z=1 \mid h_s\left(t_n\right)\right)\left(\beta g_c-c_e-\alpha(1-\beta) g_a\right) \\ & +\left(1-\sigma_n\right) p\left(k_z=1 \mid h_s\left(t_n\right)\right)\left(-c_e-\theta m_c\right) \\ & +\left(1-p\left(k_z=1 \mid h_s\left(t_n\right)\right)\right)\left(-c_e-\theta m_c\right) \end{aligned} \tag{17}$$

In the case where the malicious node $\left(k_z=1\right)$ adopts the optimal policy $\omega_{z_n}^*$, the nondifferentiability can be obtained from the detection node k_D taking the actions Detect and Idle:

$$E_{U_D}(Detect)=E_{U_D}(Idle) \tag{18}$$

Therefore, the optimal attack probability of malicious node $\left(k_z=1\right)$ is:

$$\sigma_n^*=\frac{\left(c_e+\theta m_c\right)}{p\left(k_z=1 \mid h_s\left(t_n\right)\right)\left(\beta g_c-\alpha(1-\beta) g_a+g_a+\theta m_c\right)} \tag{19}$$

For malicious node $\left(k_z=1\right)$, the expected gains from taking actions Attack and Cooperate are respectively:

$$\begin{aligned} E_{U_z}(Attack) & =\gamma_n p\left(k_z=1 \mid h_s\left(t_n\right)\right)\left((1-\beta) g_a-c_a-\beta g_c\right) \\ & +\left(1-\gamma_n\right) p\left(k_z=1 \mid h_s\left(t_n\right)\right)\left(g_a-c_a\right) \end{aligned} \tag{20}$$

$$\begin{aligned} E_{U_s}\left(Cooperate\right) &= \gamma_n p\left(k_z=1\mid h_s\left(t_n\right)\right)\left(g_b-c_b-c_d+TD\right) \\ &+\left(1-\gamma_n\right)p\left(k_z=1\mid h_s\left(t_n\right)\right)*\left(g_b-c_b-c_d+TD\right) \\ &+\gamma_n\left(1-p\left(k_z=1\mid h_s\left(t_n\right)\right)\right)\left(g_b-c_b-c_d+TD\right) \\ &+\left(1-\gamma_n\right)\left(1-p\left(k_z=11h_s\left(t_n\right)\right)\right)\left(g_b-c_b-c_d+TD\right) \end{aligned} \tag{21}$$

In the case of detecting node k_D adopting the optimal policy $\omega_{D_n}^*$, the nondifferentiability of Attack and Cooperate can be obtained by malicious node $\left(k_z=1\right)$ adopting Attack and Cooperate:

$$E_{U_z}\left(Attack\right)=E_{U_z}\left(Cooperate\right) \tag{22}$$

Therefore, the optimal detection probability for detecting node k_D is:

$$\gamma_n^*=\frac{g_b-c_b-c_d+TD-p\left(k_z=1\mid h_s\left(t_n\right)\right)\left(g_a-c_a\right)}{-\beta\, p\left(k_z=1\mid h_s\left(t_n\right)\right)\left(g_a+g_c\right)} \tag{23}$$

Therefore, there exists a mixed-strategy perfect Bayesian equilibrium $\left(\sigma_n^*,\gamma_n^*\right)$ in the multi-stage game t_n, related to α,β, θ,TD, and posterior inference $p\left(k_z=1\mid h_s\left(t_n\right)\right)$, respectively.

2) IoT privacy protection degree measure. From the above equation:

$$\begin{aligned} p\left(k_z=1\mid S_z\left(t_n\right),h_s\left(t_n\right)\right) &= \frac{p\left(k_z=1\mid h_s\left(t_n\right)\right)\left(\beta\sigma+\theta(1-\sigma)\right)}{\left(1-p\left(k_z=1\mid h_s\left(t_n\right)\right)\right)\theta+p\left(k_z=1\mid h_s\left(t_n\right)\right)} \\ &*\frac{1}{\left(\beta\sigma+\theta(1-\sigma)\right)} \\ &=\frac{p\left(k_z=1\mid h_s\left(t_n\right)\right)\left(\beta\sigma+\theta(1-\sigma)\right)}{p\left(k_z=1\mid h_s\left(t_n\right)\right)\left(\beta\sigma+\theta\sigma\right)+\theta} \end{aligned} \tag{24}$$

can be obtained from equations (9) and (24):

$$P=1-\frac{p\left(k_z=1\mid h_s\left(t_n\right)\right)\left(\beta\sigma+\theta(1-\sigma)\right)}{p\left(k_z=1\mid h_s\left(t_n\right)\right)\left(\beta\sigma+\theta\sigma\right)+\theta}\sigma \tag{25}$$

For the multi-stage signal repetition game, it is obtained from Eqs. (10) and (25):

$$\begin{aligned} H=-\sum_{s_z\in S_z}&\left(\left(1-\frac{p\left(k_z=1\mid h_s\left(t_n\right)\right)\left(\beta\sigma+\theta(1-\sigma)\right)}{p\left(k_z=1\mid h_s\left(t_n\right)\right)\left(\beta\sigma+\theta\sigma\right)+\theta}\sigma\right)^t\right. \\ &*\log_2\left(1-\frac{p\left(k_z=1\mid h_s\left(t_n\right)\right)\left(\beta\sigma+\theta(1-\sigma)\right)}{p\left(k_z=1\mid h_s\left(t_n\right)\right)\left(\beta\sigma+\theta\sigma\right)+\theta}\sigma\right)^t \\ &+\left(1-\left(1-\frac{p\left(k_z=1\mid h_s\left(t_n\right)\right)\left(\beta\sigma+\theta(1-\sigma)\right)}{p\left(k_z=1\mid h_s\left(t_n\right)\right)\left(\beta\sigma+\theta\sigma\right)+\theta}\sigma\right)^t\right) \\ &\left.*\log_2\left(1-\left(1-\frac{p\left(k_z=1\mid h_s\left(t_n\right)\right)\left(\beta\sigma+\theta(1-\sigma)\right)}{p\left(k_z=1\mid h_s\left(t_n\right)\right)\left(\beta\sigma+\theta\sigma\right)+\theta}\sigma\right)^t\right) \end{aligned} \tag{26}$$

So far, the formula for the degree of privacy protection in IoT as shown in equation (26) is obtained, and its value is related to the detection rate β, the false alarm rate θ, and the posterior probability

$p\left(k_z=1 \mid h_s\left(t_n\right)\right)$ of a malicious node in IoT.

3.4. Experimental setup and data set

This section introduces the development environment as well as hardware and software used in the development of this system according to the actual situation, as shown below:

Processor: Intel(R) Core (TM) i7-7700K CPU @ 4.20GHz
Main Frequency: 4.20GHz
RAM: 16.0GB
Operating System: Windows 10
Experimental tools: Python 3.8 and TensorFlow 2.3.0

The KDD CUP99 dataset provides a unified benchmark for evaluating the strengths and weaknesses of intrusion detection algorithms, where each network connection is labeled as either normal or anomalous, and the types of anomalies are categorized into four categories: DoS, R2L, U2R, and Probing.In order to better apply the gaming model to the KDD Cup99 dataset, the NSL_KDD dataset is created, which contains the KDD Cup99 dataset's data features and anomaly types, and duplicate records were eliminated to reduce the amount of data for a more effective and accurate assessment of IoT privacy protection technologies.

4. Results and analysis

4.1. Effect of detection rate and false alarm rate on a posteriori probability of malicious node

In this section, MATLAB 2022 is used to describe the multi-stage signaling game model and conduct the corresponding experiments. First, the results of each game stage are observed, including the a posteriori probability of the malicious node p, the optimal attack probability taken by the malicious node σ_n^* and the optimal detection probability of the detecting node γ_n^*, as well as the degree of privacy protection, and then the effects of different parameters on the results are investigated and analyzed, from which it can be determined which aspects of the node need to be improved to better protect IoT privacy.

In our experiments, we set the basic game parameters such as trust TD = 15, malicious node attack gain g_a = 100, node cooperation gain g_b = 60, detecting node detection gain g_c = 80, malicious node attack cost c_a = 40, node cooperation cost c_b = 15, node detection cost c_c = 15, spoofing loss c_d = 10, and false alarm loss m_c = 10.

In the experiment, the a posteriori probabilities need to be constantly updated based on different stages. The faster the a posteriori probability converges, the faster the detecting node can detect the malicious node, thus stopping the malicious node's attack at the source and protecting IoT privacy. The experiment is given an initial value such that the malicious node probability p = 0.5, which represents the same probability of normal and malicious nodes in the initial phase.

Figure 1 demonstrates the convergence speed of the probability of malicious node p as the detection rate β varies. From the data in the figure, it can be seen that the larger the detection rate, the greater the convergence speed p and the faster it converges to 1, i.e., the detecting node can more quickly determine whether the node is malicious or not. For example, when β = 0.9, it goes through roughly 3 stages to reach the convergence point, while when β = 0.7, it goes through roughly 5 stages to reach the convergence point.

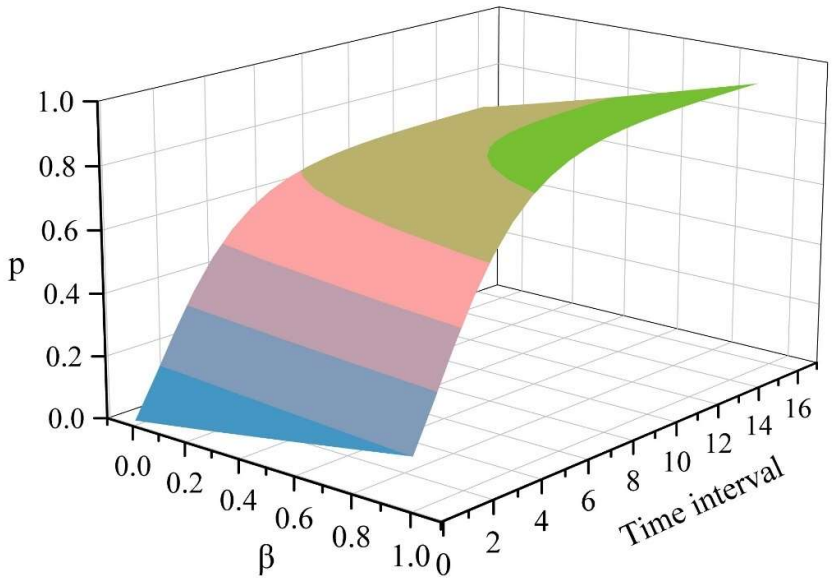

Fig. 1. The trend of p with the variation of the detection rate

4.2. Stabilizing Trends in Privacy Protection Evolution with Different Penalty Coefficients and Amounts

In order to simulate the evolutionary path of privacy protection strategy selection between the IoT platform and the task publisher, the parameters of the model are assigned values according to the actual operation of the IoT platform and the design of rules.

In this section, while keeping the reward coefficient unchanged, i.e., the task publisher's strategy behavior will not affect the reward it receives, and exploring how increasing the penalty coefficient of the IoT platform affects the evolutionary stability of the two sides of the game, the trend of the stability of the two sides' strategy evolution under different penalty coefficients is shown in Fig. 2.

According to the evolution results in the figure, it can be concluded that when the penalty value coefficient of the IoT platform is 0.2, 0.4, and 0.8, the final privacy protection strategy choices of the task publisher and the IoT platform also change, and the trend of the model in the process of evolution gradually converges to the point 1. The simulation results show that when the IoT platform raises the penalty coefficient, i.e., the same behavior in the IoT platform's rules gets a punishment of strength is greater, the whole model converges to the ideal state more quickly after continuous game rounds, which can better protect IoT privacy.

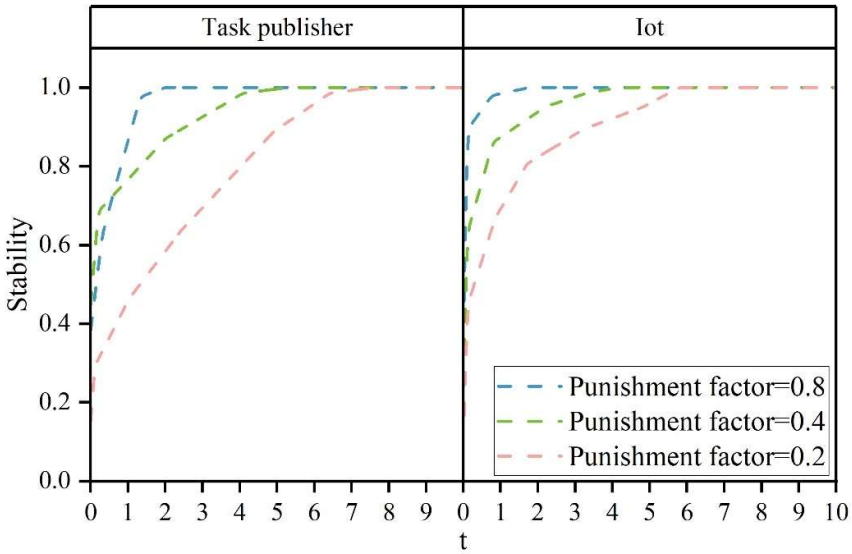

Fig. 2. Strategic evolution stability trend of the two sides of the penalty coefficient

In addition, in this section, based on the statistical data of the IoT platform, MATLAB2022 is used to perform the simulation analysis of protection strategy selection, which is a numerical study to simulate the behaviors of participants under different mechanisms. The IoT platform is set to choose the proportion of positive protection strategy x = 0.2, the proportion of incentive constraint strategy y = 0.8, and the running time is [0, 10]. Changes in the game model are discussed by varying the values of the regulatory fees and the reward and penalty amounts. The penalty amount is set to 14 versus 18.

Figure 3 shows the effect of penalty amount on the probability of IoT platforms actively choosing privacy positive protection strategies with incentive constraints. The data in the figure shows that the larger the penalty amount is, the higher the cost for IoT platforms to choose privacy positive protection strategies and tend to positive protection strategies, while the proportion of incentive constraint strategies will be reduced accordingly, i.e., the larger the penalty amount is, the larger the value of x tends to be stabilized, and the smaller the value of y tends to be stabilized.

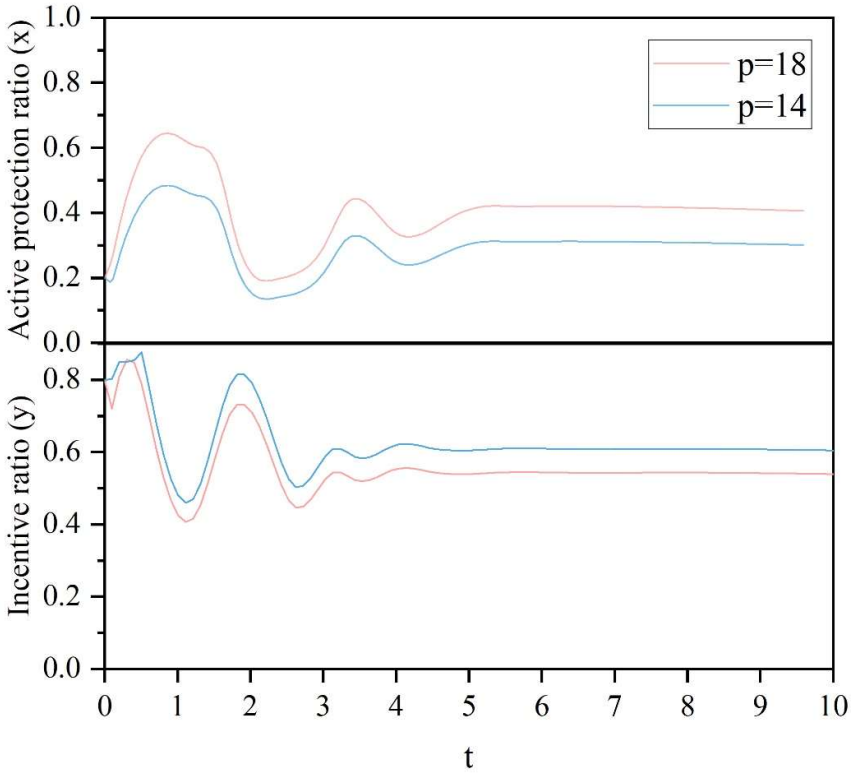

Fig. 3. The impact of the protection strategy of the Internet platform

4.3. Impact of IoT Behavioral Levels on Privacy Protection

This section assumes that there are five levels of IoT behavioral trust: very trusting (trust level 1), trusting (trust level 2), basic trusting (trust level 3), suspicious (trust level 4), and distrusting (trust level 5). Two experiments were conducted on this basis:

Experiment 1: The parametric factors a1, a2, a3, a4, and a5 of the game analysis are 0.96, 0.92, 0.60, 0.64, and 0.70, respectively.

Experiment 2: If the parametric factors a1, a2, a3, a4, and a5 of the game analysis are 0.95, 0.93, 0.60, 0.70, and 0.64, respectively.

The values of Einc2 (the income obtained by the assessee from the malicious behavior) and Sinc (which is a constant, representing the fixed income of the normal operation of the cloud environment system) are fixed at 400 and 500 respectively, and the parameters r and p are magnified by 100 times

The value of the cost paid by IoT Platform), Sloss (the loss of IoT Platform when malicious information is not detected), and Ecost (the opportunity cost of the "normal" of the assessee).

$$\begin{aligned} Epun &= a_1^k Einc \\ Einc &= a_2^k Einc_2 \\ E\cos t &= a_3^k Einc \\ Sloss &= a_4^k Einc \\ S\cos t &= a_5^k Einc \\ p &= \frac{1-a_2^{2k}+a_3^{2k}}{a_1^{2k}+a_3^{2k}} \\ r &= \frac{a_5^{2k}}{a_4^{2k}+a_5^{2k}} \end{aligned} \tag{27}$$

Figures 4 and 5 show the values of the game parameters obtained in the two sets of experiments, respectively, and the analysis shows that:

1) When the gain Einc2 of the appraisee from the malicious behavior is fixed, the gain of the appraisee from the normal behavior $Einc = a_2^k Einc_2$, the punishment of the malicious appraisee when the malicious behavior is detected $Epun = a_1^k Einc$, the opportunity cost of the appraisee's “normal” $E\cos t = a_3^k Einc$ decreases with the decrease of the appraisee's trust level.

2) While the cost paid by the IoT platform when it is normal $S\cos t = a_5^k Einc$ and the loss of the IoT platform when it is maliciously unchecked $Sloss = a_4^k Einc$ decreases as the trust level of the appraisee decreases.

3) The probability p of real-time monitoring of IoT intrusion attacks increases as the trust level of the appraisee decreases.

4) When the value of a4 is smaller than the value of a5, the tendency of the appraisee to have malicious behavior increases with the decrease of the trust level, and when the value of a4 is larger than the value of a5, the tendency of the appraisee to have malicious behavior decreases with the decrease of the trust level, which is caused by the IoT platform to improve the probability of real-time monitoring of intrusion attacks.

The above experimental analysis shows that: on the basis of the user and the IoT to provide behavioral trust to prevent, it is necessary to increase the effective monitoring and prevention strategy of abnormal behavior, only a reasonable combination of prevention and monitoring can be better for the user to provide IoT privacy protection strategy.

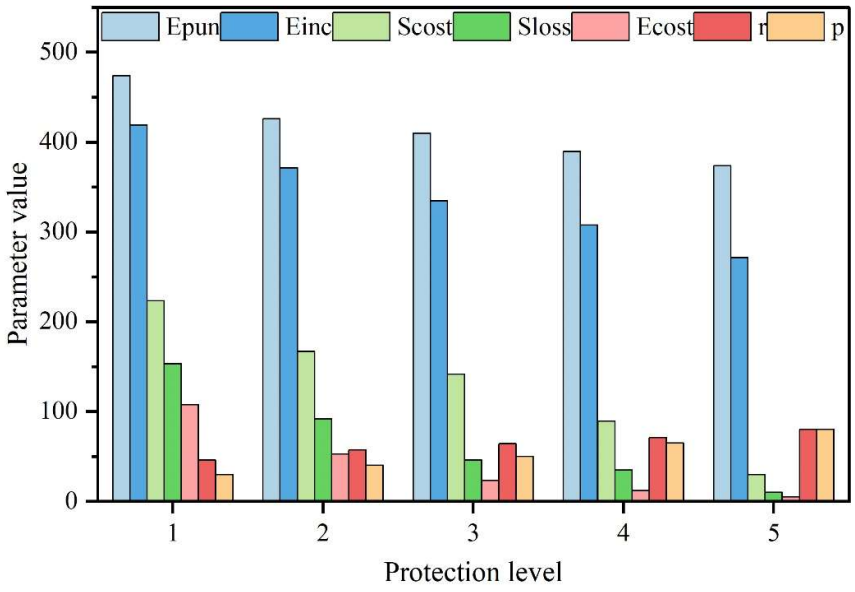

Fig. 4. Experiment 1 game parameter trend

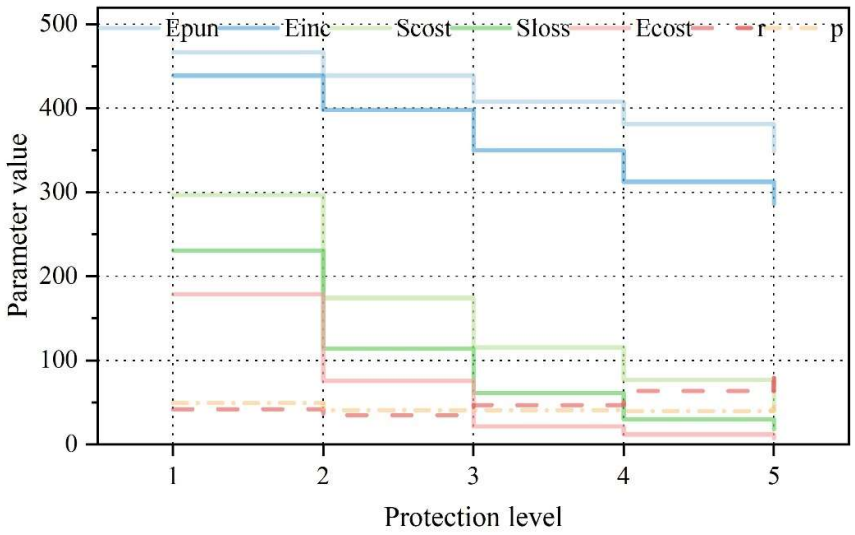

Fig. 5. Experiment 2 game parameter trend

4.4. Evaluating the effectiveness of IoT privacy protection based on attack and defense gains

In order to verify the feasibility and effectiveness of the models and algorithms proposed in this paper, a simulation system consisting of network defense equipment, Web server, client, FTP server and DB server is constructed and experimented.

Markov, Fliplt and the method proposed in this paper belong to the same multi-stage decision-making algorithm, comparing the privacy protection effect of the three models, which can show the superiority of this paper's method. Figures 6 and 7 show the comparison results of the attack and defense gains in each stage and the comparison of the attack gains in each stage, respectively. The horizontal coordinate of Fig. 6 indicates the defense gain and the vertical coordinate indicates the attack gain; the horizontal coordinate of Fig. 7 indicates the number of attack and defense stages and the vertical coordinate indicates the attack gain. As can be seen from Fig. 6, looking at each stage, in the case of the same privacy protection gain, the attack gain of this paper has a significant reduction in value, such as when the defense gain is 1500, the attack gain of this paper's model compared to the comparative model is reduced by 4%~10%. This is because this paper considers the attacker in the

defender to release the signal to induce the role of confusion, there will be a misjudgment of the type of defense, so there will be an additional loss of revenue, the reduction of the attack revenue in Figure 7 has a more intuitive display, this paper's model in the selected eight attack and defense phases of the attack revenue are lower than the comparison algorithm. By considering the miscalculation situation in the attack and defense decisions, the gain quantification is more precise and more in line with the attack and defense reality that the participants are imperfect.

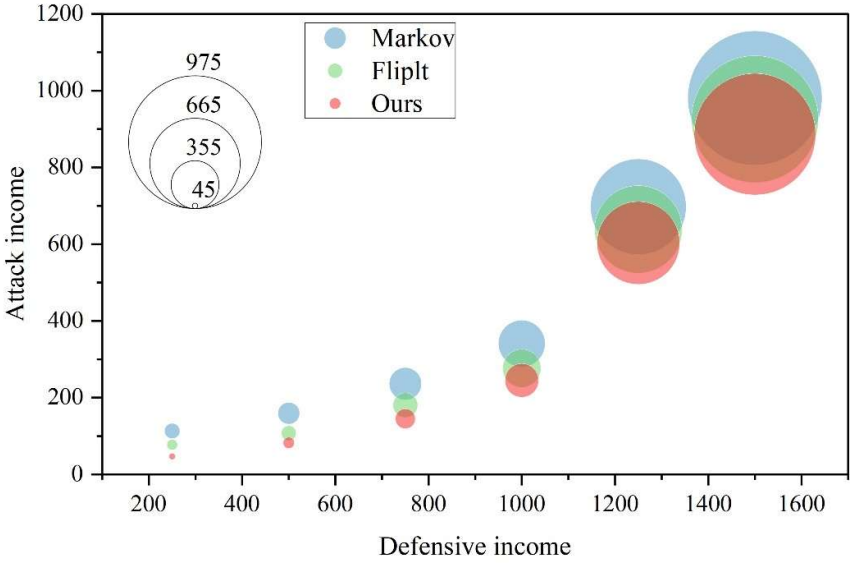

Fig. 6. Comparison of attack-defense benefit in each stage

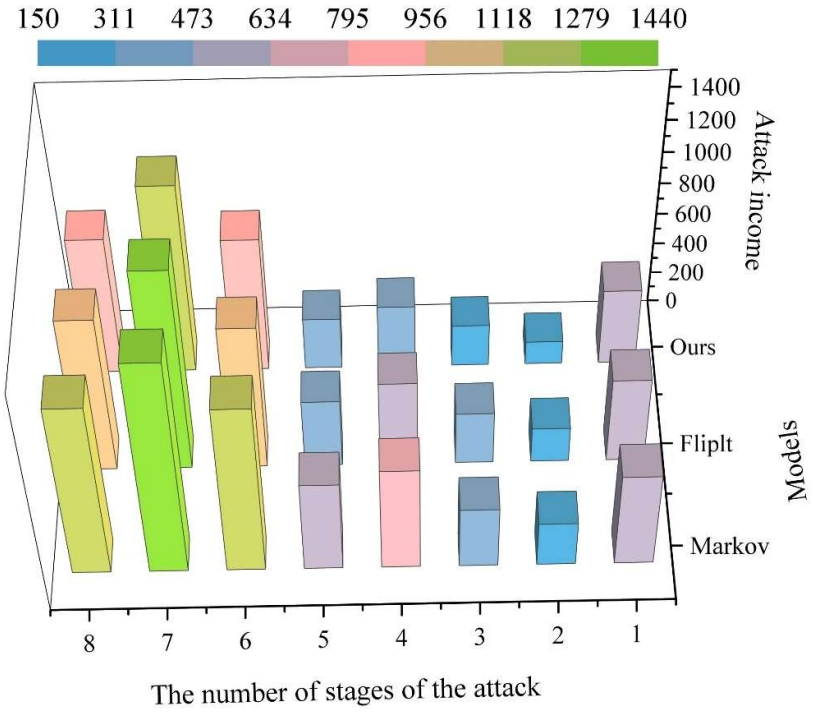

Fig. 7. Comparison of attack benefit in each stage

In order to more directly illustrate the reduction rate of attack gain of this paper's algorithm compared to the other two algorithms, the formula for the reduction rate of attack gain is introduced:

$$\sigma = \frac{U_A' - U_A}{U_A} \tag{28}$$

U_A denotes the attack gain in this paper's algorithm, U_A' denotes the attack gain of the comparison algorithm in this paper's experimental environment, and σ denotes the attack gain reduction rate of this paper's privacy-preserving decision-making optimization algorithm compared with the comparison literature. Table 3 shows the comparison results of the attack gain reduction rate, which shows that compared with the comparison model, the average attack gain reduction rate of this paper ranges from 23.82% to 47.47%, which indicates that the privacy-preserving decision-making algorithm of this paper better reflects the influence of the protection signal on the attacker's action, and it can effectively frustrate the attacking action and realize the active protection.

Table 3. Attack benefit reduction rate

Attack income reduction rate(%)	Markov	Fliplt
Min	15.83	8.07
Max	93.41	51.92
Average	47.47	23.82

5. Conclusion

The article introduces the IoT conventional system and specifically analyzes the shortcomings of the current commonly used IoT privacy protection methods, which provides the main research direction for this paper. The research focuses on establishing new IoT privacy protection models from two perspectives: evolutionary stability and signaling game. The effectiveness of these two sets of models for IoT privacy protection models is verified through simulation experiments. The detection rate of this paper's model is 0.9, the probability of IoT malicious node can converge to 1 after 3 stages. The IoT improves the penalty coefficients and the fine amount, which can better protect the IoT privacy. The detection probability of IoT intrusion attack increases with the decrease of trust level, which can effectively reduce the malicious behavior of the examiner. The attack gains of this paper's model are 23.82% to 47.47% lower than the comparison model, which indicates that this paper's model can have an impact on the attackers of IoT privacy and achieve privacy protection.

Project Fund

1) Project of the 14th Five Year Plan for Education Science in Shanxi Province: Research on the Application of Sensor Technology System in the Smart Transformation of University Libraries (Fund No. GH-220170).
2) 2023 Shanxi Province Higher Education Teaching Reform and Innovation Project: "Research and Practice on the Achievement oriented Education Model of 'Specialized Innovation Integration' - Taking the Course of 'Sensor Technology' as an Example (Fund No. J20231425)".
3) “Supported by Open Project Foundation of Key Laboratory of Computation Intelligence and Chinese Information Processing of Ministry of Education and Key Laboratory of Data Intelligence and Cognitive Computing of Shanxi Province”.
4) National Computer Education Research Project for Higher Education Institutions: OBE Driven Blended Learning Model for IoT Technology Courses: Innovative Practice of Applied Undergraduate Education (Fund No. SXCF202411).
5) Special Project for Implementing the Spirit of the Third Plenary Session of the 20th Central Committee of the Communist Party of China in the Philosophy and Social Sciences Planning of Shanxi Province in 2024: "Promoting Innovative Research on Emotional Computing and Social Governance -

Group Behavior and Public Opinion Analysis Based on Multimodal Data Analysis (Fund No.: 2024QH061 (YB)).
6) Taiyuan University Project: Application and Research of Internet of Things Technology in Smart Campus (Fund No.: 23TYYB03).

References

[1] Barron, E. N. (2024). Game Theory: An Introduction. John Wiley & Sons.

[2] Do, C. T., Tran, N. H., Hong, C., Kamhoua, C. A., Kwiat, K. A., Blasch, E., ... & Iyengar, S. S. (2017). Game theory for cyber security and privacy. ACM Computing Surveys, 50(2), 30-37.

[3] Oh, S. J., Fritz, M., & Schiele, B. (2017). Adversarial Image Perturbation for Privacy Protection--A Game Theory Perspective. In International Conference on Computer Vision (pp. 1491-1500). IEEE.

[4] Lindgren, K. (2018). Evolutionary dynamics in game-theoretic models. In The economy as an evolving complex system II (pp. 337-367). CRC Press.

[5] Quijano Silva, N., Ocampo-Martínez, C., Barreiro Gómez, J., Obando, G., Pantoja, A., & Mojica Nava, E. (2017). The role of population games and evolutionary dynamics in distributed control systems: the advantages of evolutionary game theory. IEEE control systems magazine, 37, 70-97.

[6] Zhang, S., Wang, C., & Yu, C. (2019). The evolutionary game analysis and simulation with system dynamics of manufacturer's emissions abatement behavior under cap-and-trade regulation. Applied Mathematics and Computation, 355(C), 343-355.

[7] Yiqing, L. I. U., Yang, T. A. N. G., Yanru, L. I. A. N. G., & Chundong, X. U. (2023). Evolutionary game and stability analysis of mining heritage tourism development supervision. Operations Research and Management Science, 32(2), 83.

[8] Zhu, Q., Zhao, X., & Wu, M. (2024). Third-party certification: how to effectively prevent greenwash in green bond market?–analysis based on signalling game. Environment, Development & Sustainability, 26(6).

[9] Fudenberg, D., & Vespa, E. (2019). Learning theory and heterogeneous play in a signaling-game experiment. American Economic Journal: Microeconomics, 11(4), 186-215.

[10] Zhang, T., Huang, L., Pawlick, J., & Zhu, Q. (2020). Game-Theoretic Analysis of Cyber Deception: Evidence-Based Strategies and Dynamic Risk Mitigation. Modeling and Design of secure Internet of Things, 27-58.

[11] Qu, Y., Yu, S., Zhou, W., Peng, S., Wang, G., & Xiao, K. (2018). Privacy of Things: Emerging Challenges and Opportunities in Wireless Internet of Things. IEEE Wireless Communications.

[12] Ding, X., Zou, Y., Ding, F., Zhang, D., & Zhang, G. (2019). Opportunistic relaying against eavesdropping for Internet-of-Things: A security-reliability tradeoff perspective. IEEE Internet of Things Journal, 6(5), 8727-8738.

[13] Illi, E., Qaraqe, M., Althunibat, S., Alhasanat, A., Alsafasfeh, M., de Ree, M., ... & Al-Kuwari, S. (2023). Physical layer security for authentication, confidentiality, and malicious node detection: a paradigm shift in securing IoT networks. IEEE Communications Surveys and Tutorials, 1-1.

[14] Yu, M., Zhang, J., Wang, J., Gao, J., Xu, T., Deng, R., ... & Yu, R. (2018). Internet of Things security and privacy-preserving method through nodes differentiation, concrete cluster centers, multi-signature, and blockchain. International Journal of Distributed Sensor Networks, 14(12).

[15] Kumar, N., Madhuri, J., & ChanneGowda, M. (2017, May). Review on security and privacy concerns in Internet of Things. In 2017 International Conference on IoT and Application (ICIOT) (pp. 1-5). IEEE.

[16] Wachter, S. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. Computer Law and Security Review, 34(3).

[17] Barbosa, M., Mokhtar, S. B., Felber, P., Maia, F., Matos, M., Oliveira, R., ... & Voulgaris, S. (2017, September). SAFETHINGS: Data Security by Design in the IoT. In 2017 13th European Dependable Computing Conference (EDCC).

[18] Khadam, U., Iqbal, M. M., Alruily, M., Al Ghamdi, M. A., Ramzan, M., & Almotiri, S. H. (2020). Text data security and privacy in the internet of things: threats, challenges, and future directions. Wireless Communications and Mobile Computing, 2020(1), 7105625.

[19] Sun, G., Chang, V., Ramachandran, M., Sun, Z., Li, G., Yu, H., & Liao, D. (2017). Efficient location privacy algorithm for Internet of Things (IoT) services and applications. Journal of Network and Computer Applications, 89(1), 3-13.

[20] Vijayakumar, P., Obaidat, M. S., Azees, M., Islam, S. H., & Kumar, N. (2019). Efficient and secure anonymous authentication with location privacy for IoT-based WBANs. IEEE Transactions on Industrial Informatics, 16(4), 2603-2611.

[21] Esposito, C., Tamburis, O., Xin, S., & Choi, C. (2020). Robust Decentralised Trust Management for the Internet of Things by Using Game Theory. INFORMATION PROCESSING & MANAGEMENT, 57(6), 1-16.

[22] Shen, Y., Shen, S., Li, Q., Zhou, H., Wu, Z., & Qu, Y. (2023). Evolutionary privacy-preserving learning strategies for edge-based IoT data sharing schemes. Digital Communications and Networks, 9(4), 906-919.

[23] Du, J., Jiang, C., Chen, K. C., Ren, Y., & Poor, H. V. (2018). Community-Structured Evolutionary Game for Privacy Protection in Social Networks. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 13(3).

[24] Xiong, J., Ma, R., Chen, L., Tian, Y., Li, Q., Liu, X., & Yao, Z. (2019). A personalized privacy protection framework for mobile crowdsensing in IIoT. IEEE Transactions on Industrial Informatics, 16(6), 4231-4241.

[25] Khan, A. A., Abolhasan, M., & Ni, W. (2018). An evolutionary game theoretic approach for stable and optimized clustering in vanets. IEEE Transactions on Vehicular Technology.

[26] Tian, Z., Gao, X., Su, S., Qiu, J., Du, X., & Guizani, M. (2019). Evaluating Reputation Management Schemes of Internet of Vehicles Based on Evolutionary Game Theory. IEEE Transactions on Vehicular Technology, 68(6).

[27] Sfar, A. R., Challal, Y., Moyal, P., & Natalizio, E. (2019). A Game Theoretic Approach for Privacy Preserving Model in IoT-Based Transportation. IEEE Transactions on Intelligent Transportation Systems, 20(12).

[28] Arisdakessian, S., Wahab, O. A., Mourad, A., Otrok, H., & Guizani, M. (2022). A Survey on IoT Intrusion Detection: Federated Learning, Game Theory, Social Psychology and Explainable AI as Future Directions. IEEE Internet of Things Journal, 1.

[29] Zhang, R., & Zhu, Q. (2020). $\mathtt {FlipIn} $: A Game-Theoretic Cyber Insurance Framework for Incentive-Compatible Cyber Risk Management of Internet of Things. IEEE Transactions on Information Forensics and Security, 15.

[30] Sun, Y., Ji, W., Weng, J., Zhao, B., Li, Y., & Wu, X. (2020, December). Selection of optimal strategy for moving target defense based on signal game. In Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies (pp. 28-32).

[31] Hu, Y., Zhang, H., Guo, Y., Li, T., & Ma, J. (2020). A Novel Attack-and-Defense Signaling Game for Optimal Deceptive Defense Strategy Choice. Wireless Communications and Mobile Computing, 2020(1), 8850356.

[32] Pawlick, J., Colbert, E., & Zhu, Q. (2019). A Game-theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy. ACM Computing Surveys, 52(4).

[33] Nanlan Jiang,Yinan Zhai,Yujun Wang,Xuesong Yin,Sai Yang & Pingping Xu. (2024). Location Privacy Protection for the Internet of Things with Edge Computing Based on Clustering K-Anonymity. Sensors (Basel, Switzerland)(18),6153-6153.

[34] Muhammad Kashif & Kubra Kalkan. (2024). Differential privacy preserving based framework using blockchain for internet-of-things. Peer-to-Peer Networking and Applications(1),1-23.

[35] Syed Abdul Moeed,Ramesh Karnati,G. Ashmitha,Gouse Baig Mohammad & Sachi Nandan Mohanty. (2024). A Novel Enhanced Approach for Security and Privacy Preserving in IoT Devices with Federal Learning Technique. SN Computer Science(6),750-750.

[36] Pu hao Guo,Xiang qian Wang & Xiang rui Meng. (2024). Evolutionary game study and empirical analysis of the adoption of green coal mining technology: A case study of ITMDB. Energy134019-134019.

[37] Zhao Yue,Shen Yang & Yan Jiaqi. (2021). Design and Application of Genetic Algorithm Based on Signal Game and Newsboy Model for Optimizing Supply Chain. Discrete Dynamics in Nature and Society