Heliyon 9 (2023) e16590

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

Evolutionary game model based on cumulative prospect theory for information management mechanism in SIoT[☆]

Shuting Liu, Yinghua Ma, Xiuzhen Chen [*]

Institute of Cyber Science and Technology, Shanghai Jiao Tong University, Shanghai 200240, China

ARTICLE INFO

Keywords:
Evolutionary game
Reputation
Social internet of things
Information governance
Conflict control

ABSTRACT

As nodes in Social Internet of Things (SIoT) become more intelligent, malicious information occurs more frequently and spreads more widely. This problem can severely affect the trustworthiness of services and applications in SIoT. Methods to effectively control malicious information spreading in SIoT are essential and necessary. Reputation mechanism provides a powerful tool to tackle this challenge. In this paper, we propose a reputation-based mechanism to activate the self-purification capacity of the SIoT network by balancing information conflicts triggered by reporters and supporters. In order to find the best rewarding and punishment strategy, a bilateral cumulative-prospect-based evolutionary game model of SIoT network information conflict is constructed. Using local stability analysis and numerical simulation, the evolutionary trends of the proposed game model under different theoretical application scenarios are analyzed. The findings indicate that the basic income and deposit of both sides, the popularity of information as well as the importance of the conformity effect all have a significant impact on the system's steady state and evolutionary path. The specific conditions that both participating sides of the game tend to treat conflicts relatively rationally are analyzed. Dynamic evolution analysis and sensitivity analysis of selected parameters show that basic income is positively related to smart object's feedback strategies, while deposit is negatively related to that. While weight of conformity effect or the information popularity goes up, the rising of feedback probability is observed. Based on the above results, suggestions on dynamic reward and punishment strategies are given. The proposed model is a helpful attempt to model the evolution of information spreading in SIoT networks, with the ability to simulate several well-known regularities of message dissemination. Proposed model and suggested quantitative strategies can be helpful to build feasible malicious information control facilities in SIoT networks.

1. Introduction

Internet of Things (IoT) framework allows for the creation of intelligent applications and infrastructures by bridging the gap between the real world and the internet through physical items [1]. The markets of IoT which have steadily evolved over the past few years, cover every facet of human life, encompassing energy, smart houses, smart towns and cities, healthcare, smart traffic management, etc. [2–6]. The Social Internet of Things (SIoT) concept has become increasingly popular in recent years as a result of the

[☆] This article is a part of the "Security and Privacy in IoT Network" Special issue.

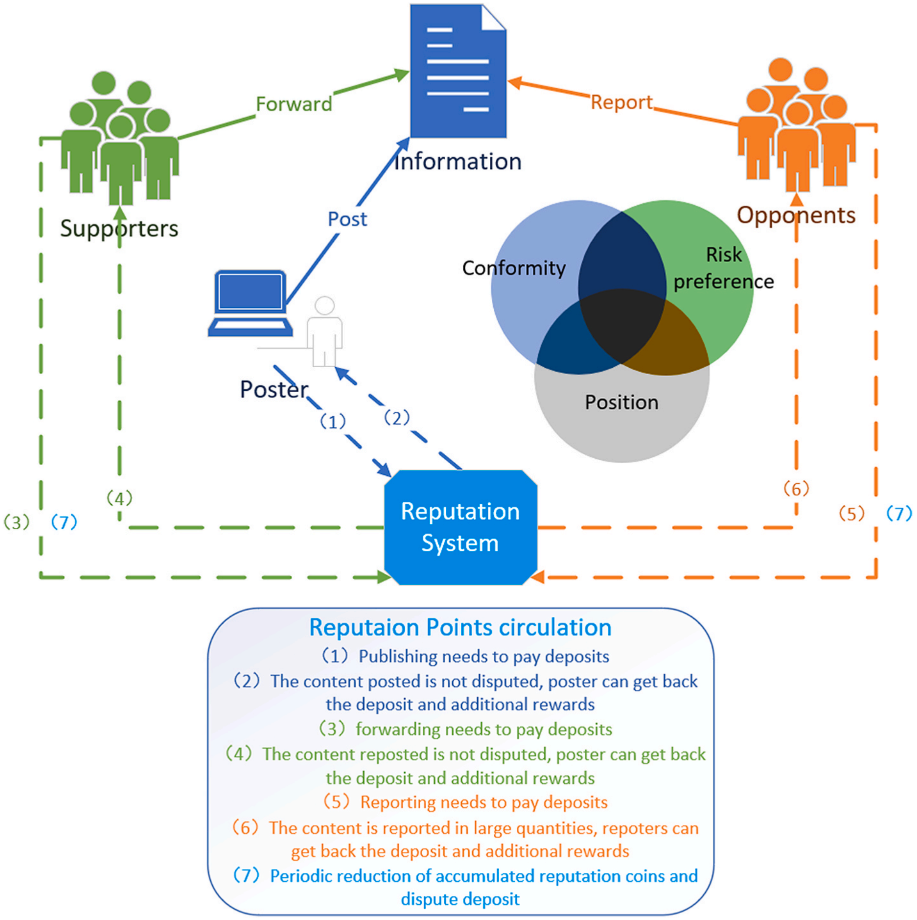
[*] Corresponding author.
E-mail address: chenxz@sjtu.edu.cn (X. Chen).

https://doi.org/10.1016/j.heliyon.2023.e16590
Received 28 February 2023; Received in revised form 2 May 2023; Accepted 22 May 2023
Available online 26 May 2023

indispensable role of devices in people's daily lives. SIoT is equipped with the characteristics of IoT and human society [7–9]. As an integrated network, its purpose is to mold connections of IoT facilities and devices into social interactions in the same way that humans do [10]. Physical objects, the basic constituents of SIoT, are foreseen to think, work and act like humans as Artificial Intelligence (AI) technologies advance [11,12]. We're definitely at the dawn of an automated world powered by SIoT, which is seen to become a ubiquitous and open platform for information dissemination, opinion expression, emotions sharing with smart objects. Inevitable, considerable amount of malicious information travels through SIoT networks, which may cause severe information pollution and misleading. Effective mechanisms to control or reduce the spreading of malicious information and maintain a healthy and rational interaction environment in SIoT are urgently needed in both industries and academia.

Past studies in the field of SIoT have put emphasis on four thrust areas: trust evaluation and management, relationship management, network navigation, and recommendation for service and application. To identify suitable access services in the SIoT network, a recommender system has been put out by Chen et al. [13], in which a node's credibility is assessed based on its present state, historical performance and social connections. A cognitively aware method for the provision of adaptive services in SIoT was created by Hussein et al. [14], which was implemented with subjective and objective context information. The properties of the SIoT network's navigability have been identified by Nitti et al. [15]. In this work, nodes are equipped with information about their neighbors, which can be exchanged in the network to provide global navigation. In order to preserve privacy for message transmission in the social internet of vehicles, an interest-based approach was presented by Zhu et al. [16]. According to Kokoris-Kogias et al.'s [17] suggested trust architecture, which is based on a management system called COSMOS, reputation is calculated with data obtained from the COSMOS platform and friends, while trust is determined by one's personal experiences. Zhou et al. [18] have proposed an integrated scheme for trust evaluation, which not only makes use of personal knowledge and firsthand evidence, but also takes counterparts' ratings into account. The trust platform proposed by Truong et al. [19] for SIoT is based on friend-opinion-based recommendations, feedback-based reputation, and first-hand knowledge.

Mechanisms on friends-oriented or experience-based trust, feedback-based reputation are widely studied. In a feedback-based reputation system, malicious feedback blended with normal feedback are inevitable. Contradictory feedback is called disagreement or conflict. Mild conflict can be helpful to identify malicious information, but serious conflict may lead to system disorder. For example, a large amount of contradictory road-related messages in the Internet of Vehicles not only reduce transportation efficiency,



Reputaion Points circulation
（1）Publishing needs to pay deposits
（2）The content posted is not disputed, poster can get back the deposit and additional rewards
（3）forwarding needs to pay deposits
（4）The content reposted is not disputed, poster can get back the deposit and additional rewards
（5）Reporting needs to pay deposits
（6）The content is reported in large quantities, repoters can get back the deposit and additional rewards
（7）Periodic reduction of accumulated reputation coins and dispute deposit

Fig. 1. Reputation-based dynamic information management mechanism for SIoT.

but also increase the risk of traffic jams and accidents that threaten human life. How to keep feedbacks in a rational and controllable situation is also an important problem.

In this research, a reputation-based dynamic information management mechanism for SIoT, which combines hard (information management mechanism) and soft controls (reputation accumulation mechanism) is studied. Following the rules in this proposed mechanism, contents in system are forwarded (recommended) or reported (identified as malicious) by different nodes. The aim of this research is to design strategy to guide smart objects' behavior to avoid serious information conflicts, for example malicious reports, in the SIoT network.

The proposed mechanism includes reward and punishment strategies and the smart object's reputation calculation. In order to simulate the mechanism, a bilateral evolutionary game model of two parties (information supporters and reporters) in the SIoT network, considering the cumulative prospect theory [20] and the conformity effect [21], is designed and set up. Numerical simulation together with local stability analysis are employed to study both sides' evolutionary stable strategies and validate the related analytical results. Additionally, quantitative suggestions for reward and punishment strategies that satisfy the above-mentioned conditions are given. To the best of our knowledge, this research is the first work to utilize the control of information conflict to address the information governance problem in the SIoT network. In addition, it provides targeted and operational strategies for the reputation system which aims to activate the self-purification capacities of the SIoT network.

The remainder of this essay is structured as follows. The proposed reputation-based dynamic information management mechanism is described in Section 2. The corresponding evolutionary game model is described in Section 3. The evolutionary results are presented and discussed in Section 4. Section 5 analyzes the sensitivity of selected parameters. Section 6 highlights suggestions of strategies for practice. The conclusions and implications are provided in Section 7, along with directions for future work.

2. Theoretical framework

2.1. Reputation-based dynamic information management mechanism

In SIoT, smart objects are acting more independently and with more social behaviors. In order to behave more cooperatively, the reputation mechanism learned from commercial societies is also used in SIoT. A dynamic reputation management mechanism for SIoT is proposed, shown in Fig. 1. Smart objects are asked to use reputation points as a guarantee when sending or forwarding information. This kind of mechanism can motivate smart objects to enhance their decision-making trade-offs, enable SIoT networks to achieve self-purification, and thereby limit the spreading of malicious information.

(1) Information publishing: smart objects deposit reputation points as a guarantee for publishing information. If the information does not cause controversy within some time, the publisher will be rewarded, and conversely, a certain amount of reputation points will be expropriated.

(2) Information forwarding: smart objects who trust information (supporters) may choose to pay a guarantee to forward the message to promote dissemination or make a recommendation. If the message does not cause controversy within some time, smart objects in the supporters' camp will be rewarded, otherwise, they will be punished.

(3) Information reporting: smart objects who consider the information malicious (opponents) may report the information. If the report wins the conflict, smart objects in the opponent's camp are rewarded with reputation points. Otherwise, they are punished with diminished reputation points.

In social network platforms, users with similar interests usually form homogeneous groups [22]. Smart objects in SIoT networks can also be split into two groups: supporters and opponents. For example, when a malicious message is sent, malicious nodes and normal nodes are supporters and opponents, respectively. Under the proposed dynamic information management mechanism, the information dissemination is actually the process in which two groups compete by forwarding and reporting, which is the keystone of this paper.

2.2. Analysis of the subject benefits

In SIoT networks, it is normal that the social identity of a message's supporters can receive both in-system reputation points and out-of-system benefits by forwarding or recommendation. To simplify the modeling, the benefits of these two parts are combined into the basic income of the supporter. Opponents whose report is not designed to be spread thus can only receive the reputation points reward given by the system as their basic income. When many reposts and reports lead to information conflicts, both supporters and opponents will be punished with reputation points reduced by the mechanism. Incentives and penalties for supporters and opponents contribute to a game relationship between the two groups.

Evolutionary game theory is concerned with decision-making problems, which assumes that participants are finitely rational and have the capacity for continuous learning. Using analysis of evolutionary stable strategy (ESS) and numerical simulation, it provides perceptive suggestions for strategies [23,24]. In combination with our research, the interactions between supporters and opponents have a significant influence on how both sides choose their strategies. Decision-makers' actions are the outcome of constant mutual adaptation and adjustment.

Different from expected utility theory (EU) [25], which makes the non-realistic assumption that human beings are completely rational, the cumulative prospect theory [20] provides a more normative and adequate description of individual choice in the face of uncertainty. In social network malicious message spreading, reference-dependent and risk preference of individual behaviors are observed. The risk attitude of smart objects which are controlled by humans, is risk-seeking when facing "gain" and risk-averse when facing “loss”, consistent with cumulative prospect theory.

Under the uncertain environment, conformity effect commonly accompanies whole decision process [21]. Smart objects behave in exactly the same way as group behavioral preferences. As the usability and scientificalness of the conformity effect in SIoT have been examined [26], the conformity effect is taken into account in our model.

In a word, the proposed mechanism is simulated using evolutionary game theory, conformity effect and cumulative prospect theory. To achieve a controllable and balanced condition, the evolutionary trends and stable strategies of participants under various scenarios are investigated. At last a practical policy on quantitative reward and punishment strategies is given, which is helpful in encouraging smart objects to report malicious message and decrease dishonest report.

3. Evolutionary game model of dynamic information management in SIoT networks

3.1. Basic assumptions and analysis of information conflict in SIoT networks

For the convenience of the following analysis, the definitions of some variables and sets related to the strategies of supporters and opponents are given:

B: Set of supporters’ strategies: B_1 denotes feedback (forwarding) and B_2 denotes lurking.

σ_B: The mixed strategy of the supporter, x is the probability that the supporter chooses to feedback (forward) a message, and $1-x$ is the probability that the supporter chooses to lurk.

O: The opponents’ strategy set: O_1 denotes feedback (reporting) and O_2 denotes lurking.

σ_O: The mixed strategy of the opponent, y is the probability that the opponent chooses to feedback (report) the information, $1-y$ is the probability that the opponent chooses to lurk.

S_{ij}: The mixed strategy of supporters and opponents, with supporters choosing strategy B_i and opponents choosing strategy O_j.

Let the reputation points of supporters and opponents be T_1 and T_2. The dispute coefficient is a feature of the message, which indicates the degree of disagreement between two groups. Therefore, the dispute coefficient of supporters is equal to that of opponents, which are respectively denoted by w_1 and w_2, and the calculation method is given by equations (1) and (2).

$$w_1 = w_2 = (|x\theta_1 - y\theta_2| - 1)(x\theta_1 + y\theta_2) \tag{1}$$

$$\left.\begin{aligned}\theta_1 &= T_1/(T_1+T_2)\\ \theta_2 &= T_2/(T_1+T_2)\end{aligned}\right\} \tag{2}$$

Group-related features are transformed into multiple parameters of the system simulation to emulate various situations of the message, which are specified in Table 1.

Assume that supporters can get basic income K_1 by forwarding as a reward for sharing. Similarly, opponents can get basic income K_2 by reporting as a reward for positive feedback.

(1) Under hybrid strategy S_{11}, neither the supporter nor the opponent chooses to lurk, where a conflict of information exists. In addition to the basic income K_1 and K_2, both parties will face the dispute loss L_1 and L_2, which can be calculated as follows. In equation (3), C_1 and C_2 are the deposit of both parties.

$$\left.\begin{aligned}L_1 &= w_1C_1\\ L_2 &= w_2C_2\end{aligned}\right\} \tag{3}$$

(2) Under hybrid strategy S_{12}, supporter chooses to forward, and the opponent chooses to lurk. Thus the supporter can obtain the basic income K_1 , while the opponent has no gain nor loss due to the lack of feedback.

(3) Under hybrid strategy S_{21}, opponents choose to report, while supporters choose to lurk. Thus opponents can get basic income K_2, while supporters have neither gains nor losses.

(4) Under hybrid strategy S_{22}, both supporters and opponents have neither gains nor losses because they choose to lurk.

The payoff matrix of the four hybrid strategies S_{ij} is presented in Table 2, according to the above presumptions and analysis.

Table 1
Description of variables of interest in model.

Variables		Description	Range
Supporters	x	Probability that the supporter chooses to feedback	$0 \le x \le 1$
	T_1	Reputation points of supporters	$T_1 > 0$
	K_1	Basic income of supporters choosing feedback	$K_1 > 0$
	C_1	Deposit of supporters	$C_1 > 0$
Opponents	y	Probability that the opponent chooses to feedback	$0 \le y \le 1$
	T_2	Reputation points of opponents	$T_2 > 0$
	K_2	Basic income of opponents choosing feedback	$K_2 > 0$
	C_2	Deposit of opponents	$C_2 > 0$

Table 2
Payoff matrix of information conflict game for the SIoT network.

Opponents		report (y)	lurk
Supporters	forward (x)	$K_1 + w_1C_1, K_2 + w_2C_2$	K_1, 0
	lurk	0, K_2	0, 0

3.2. Evolutionary game model

3.2.1. The expected utility

Smart objects make decisions toward maximizing individual benefit (that is, making rational judgments regarding the system's present status). Over time, the system's condition changes, and its reward function does as well, which leads to the dynamic adjustment of the behavioral strategies of supporters and opponents. For the forwarding probability x and the reporting probability y, their dynamic rates of change, denoted as $\frac{\partial x}{\partial t}$ and $\frac{\partial y}{\partial t}$, can be defined as equations (4) and (5) in evolutionary game theory.

$$\frac{\partial x}{\partial t} = x(1-x)(U_r - U_d) \tag{4}$$

$$\frac{\partial y}{\partial t} = y(1-y)(N_r - N_d) \tag{5}$$

U_r and U_d in equation (4) present the expected utilities of the supporters who follow the forwarding strategy (B_1) and who adopt the lurking strategy (B_2), respectively. N_r and N_d in equation (5) are the expected utilities of the opponents who adopt the reporting strategy (O_1) and who adopt the lurking strategy (O_2), respectively. According to the payoff matrix in Section 3.1, these utilities can be obtained from equations (6) and (7):

$$\left.\begin{array}{l} U_r = y(K_1 + w_1C_1) + (1-y)(K_1) \\ U_d = y(0) + (1-y)(0) \end{array}\right\} \tag{6}$$

$$\left.\begin{array}{l} N_r = x(K_2 + w_2C_2) + (1-x)(K_2) \\ N_d = x(0) + (1-x)(0) \end{array}\right\} \tag{7}$$

3.2.2. The optimization with the cumulative prospect theory

The reference point, the decision weighting and the value function are important constituents of the cumulative prospect theory framework, which describes the risk attitudes of individual smart objects in terms of "gains" and "losses." [20].

Assume that S is a finite set of states, and its subset A denotes events, X is the set of consequences, also called outcomes. The uncertain prospect f, a mapping from S to X: $f: S \rightarrow X$, assigns to each event a consequence, and the prospect sequence $f = (x_i, A_i), i = 1, 2, \cdots, n$ represents that the consequence x_i will appear after the event A_i occurs. All sequences f are sorted in ascending order of the consequences, and $x_1 \leq x_2 \leq \cdots \leq x_j \leq \cdots \leq x_n$ can be obtained. Select x_j as the reference point, and the value function can be obtained as equation (8), where α and β are the risk attitude coefficients, which reflect diminishing sensitivity of the outcomes away from the reference point x_j. In combination with our research, larger α and β imply greater attention by smart objects to the potential gains and losses of the feedback strategy. λ is the loss aversion coefficient, according to the fact that individuals are more sensitive to losses. The parameters are shown in Table 3.

$$v(x_i) = \begin{cases} (x_i - x_j)^{\alpha}, x_i \geq x_j \\ -\lambda(x_j - x_i)^{\beta}, x_i < x_j \end{cases} \tag{8}$$

If $x_i > x_j$, the outcome is considered as a gain and the value of prospect is positive, denoted by $V(f^+)$. Otherwise, the value of prospect is negative, denoted by $V(f^-)$. The calculation process is given as follows.

Table 3
Variables in cumulative prospect theory.

Variables	Description	Range
α	Risk sensitivity with gains	$0 < \alpha < 1$
β	Risk sensitivity with losses	$0 < \beta < 1$
λ	Loss aversion coefficient	$\lambda > 1$
γ	Weighting function's curvature with gains	$0 \leq \gamma \leq 1$
δ	Weighting function's curvature with losses	$0 \leq \delta \leq 1$

$$\left.\begin{aligned} V(f^+) &= \sum_{i=j}^{n} \pi_i^+ v(x_i) \\ V(f^-) &= \sum_{i=1}^{j} \pi_i^- v(x_i) \end{aligned}\right\} \tag{9}$$

In equation (9), π_i^+ and π_i^- represent the decision weighting functions, which are correlated with the outcomes of gains and losses, respectively. The calculation formulas are as follows.

$$\pi_i^+ = w^+(P(A_i \cup \cdots \cup A_n)) - w^+(P(A_{i+1} \cup \cdots \cup A_n)), j \le i \le n \tag{10}$$

$$\pi_i^- = w^-(P(A_1 \cup \cdots \cup A_i)) - w^-(P(A_1 \cup \cdots \cup A_{i+1})), 1 \le i \le j \tag{11}$$

In equations (10) and (11), $P(A_i)$ is the ideal probability of event A_i occurring. Event A_i represents that supporters make forwarding or lurking decisions, and opponents make reporting or lurking decisions. w^+ and w^- correspond to the capacity function of gains and losses, which are defined as follows.

$$\left.\begin{aligned} w^+(p) = p^\gamma/(p^\gamma + (1-p)^\gamma)^{1/\gamma} \\ w^-(p) = p^\delta/(p^\delta + (1-p)^\delta)^{1/\delta} \end{aligned}\right\} \tag{12}$$

In equation (12), respectively, γ and δ denote the weighting function's curvature in terms of the evaluation of outcomes (gains and losses). Generally, $\alpha = \beta = 0.88$, $\lambda = 2.25$, $\gamma = 0.61$, $\delta = 0.69$. The choices for α, β, λ, γ, δ are based on median estimates given by Tversky & Kahneman [20] and have been used earlier in Ref. [27] for traffic application.

According to the above description, this paper sets the reference point of the supporter's value function as $x_j = K_1$. Thus the expected utilities U_r and U_d of the supporter after the revision of the cumulative prospect theory can be obtained as equation (13).

$$\left.\begin{aligned} U_r &= \pi_{11}^-(y)v(K_1 + w_1C_1) + \pi_{12}^+(1-y)v(K_1) \\ U_d &= \pi_{21}^-(y)v(0) + \pi_{22}^-(1-y)v(0) \end{aligned}\right\} \tag{13}$$

In the same way, set the reference point of the opponent's value function as $x_j = K_2$, and the revised expected utilities N_r and N_d of the opponent can be obtained as equation (14).

$$\left.\begin{aligned} N_r &= \pi_{11}^-(x)v(K_2 + w_2C_2) + \pi_{21}^+(1-x)v(K_2) \\ N_d &= \pi_{12}^-(x)v(0) + \pi_{22}^-(1-x)v(0) \end{aligned}\right\} \tag{14}$$

3.2.3. *The optimization with the conformity effect*

In the SIoT network, smart objects adjust their own strategies when interacting with others. The quantitative equation of the conformity effect [21] is used to correct the expected utilities of supporters and opponents. Here, the conformist value of strategy is denoted by ε, the constant μ determines the strength of conformist bias, and E is the original expected utility. The revised utility $E^{'}$ is given as equation (15).

$$E^{'} = (1-\mu)E + \mu\varepsilon \tag{15}$$

Generally, opponents' reporting behavior is not visible, but the forwarding fervor of the message is visible. Let the proportion of forwarding among supporters be P_{B1} and the proportion of lurking be P_{B2}, $P_{B1} + P_{B2} = 1$. The expected utility of decision makers who choose to forward increases when P_{B1} increases. Thus the conformist value of supporters ε_1 is defined as an increasing function of P_{B1} and the expected utility difference between forwarding and lurking, denoted as $(U_r - U_d)$. With conformism constant μ_1, the modified expected utilities of supporters are presented as equation (16), and the parameter descriptions are shown in Table 4.

$$\left.\begin{aligned} U_r^{'} &= (1-\mu_1)U_r + \mu_1 P_{B1}(U_r - U_d) \\ U_d^{'} &= (1-\mu_1)U_d + \mu_1 P_{B2}(U_r - U_d) \end{aligned}\right\} \tag{16}$$

3.2.4. *Game model construction*

Let $G_1(x,y) = \frac{\partial x}{\partial t}$, $G_2(x,y) = \frac{\partial y}{\partial t}$, and substitute equations 6–16 into equations (4) and (5). We get replication dynamic equations (17) and (18), which present the final evolutionary model of the mixed strategy information game.

Table 4
Variables of interest in conformity effect.

Variables	Description	Range
μ_1	The strength of conformist bias	$0 \le \mu_1 \le 1$
P_{B1}	Forwarding fervor of the message	$0 \le P_{B1} \le 1$

$$G_1(x,y)=x(1-x)(-\lambda)(1-2\mu_1+2\mu_1P_{B1})\left\{\frac{y^\delta}{[y^\delta+(1-y)^\delta]^{\frac{1}{\delta}}}\left[((-w_1)C_1)^\beta-K_1{}^\beta\right]-\frac{[y^\delta+(1-y)^\delta]^{\frac{1}{\delta}}-y^\delta}{[y^\delta+(1-y)^\delta]^{\frac{1}{\delta}}}K_1{}^\beta\right\} \tag{17}$$

$$G_2(x,y)=y(1-y)(-\lambda)\left\{\frac{x^\delta}{[x^\delta+(1-x)^\delta]^{\frac{1}{\delta}}}\left[((-w_2)C_2)^\beta-K_2{}^\beta\right]-\frac{[x^\delta+(1-x)^\delta]^{\frac{1}{\delta}}-x^\delta}{[x^\delta+(1-x)^\delta]^{\frac{1}{\delta}}}K_2{}^\beta\right\} \tag{18}$$

4. Analysis of evolutionary game model

4.1. Solution of equilibrium point

The stability analysis of the above information game evolutionary model is carried out. When the forwarding probability x of supporters and the reporting probability y of opponents no longer change, the income of both sides changing the strategy cannot exceed that of the original strategy, and the system finally reaches an equilibrium state. Let replication dynamic equations (17) and (18) equal 0, shown as equation (19).

$$G=\begin{pmatrix}G_1(x,y)\\G_2(x,y)\end{pmatrix}=f(G,t)=0 \tag{19}$$

Solutions of the above second-order nonlinear differential equations are 5 equilibrium points of the system, namely the silence point $S_1=(0,0)$, the reporting point $S_2=(0,1)$, the forwarding point $S_3=(1,0)$, the conflict point $S_4=(1,1)$ and the center point $S_5=(x^*,y^*)$, where x^* and y^* take values in the open interval from 0 to 1.

But not all equilibrium points are ESS, which may stabilize after a disruption and tolerate mistakes or deviations brought on by finite rationality. In order to assess if the equilibrium point of a system is stable, the method of local asymptotic stability analysis on its Jacobian matrix is proposed by Friedman [28]. The discrimination rule is as follows: J denotes the Jacobian matrix of game model, $tr(J)$ denotes the trace of J, and $\det(J)$ denotes the determinant of J. (1) An equilibrium point is recognized as a saddlepoint if $\det(J)<0$; (2) Under the premise of $\det(J)>0$, we can identify an evolutionary equilibrium point as an unstable center by $tr(J)>0$ and recognize it as a stable center by $tr(J)<0$.

The Jacobian matrix of proposed information game evolutionary model is given by equations (20)–(23), which is composed of derivatives of equations (17) and (18) with respect to x and y, respectively.

$$J=\begin{pmatrix}\dfrac{\partial G_1(x,y)}{\partial x} & \dfrac{\partial G_1(x,y)}{\partial y}\\[2ex] \dfrac{\partial G_2(x,y)}{\partial x} & \dfrac{\partial G_2(x,y)}{\partial y}\end{pmatrix}=\begin{pmatrix}(1-2x)J_{11}+x(1-x)\dfrac{\partial J_{11}}{\partial x} & x(1-x)J_{12}\\[2ex] y(1-y)J_{21} & (1-2y)J_{22}+y(1-y)\dfrac{\partial J_{22}}{\partial y}\end{pmatrix} \tag{20}$$

$$J_{11}=(-\lambda)(1-2\mu_1+2\mu_1P_{B1})\left\{\frac{y^\delta}{[y^\delta+(1-y)^\delta]^{\frac{1}{\delta}}}\left[((-w_1)C_1)^\beta-K_1{}^\beta\right]-\frac{[y^\delta+(1-y)^\delta]^{\frac{1}{\delta}}-y^\delta}{[y^\delta+(1-y)^\delta]^{\frac{1}{\delta}}}K_1{}^\beta\right\} \tag{21}$$

$$J_{22}=(-\lambda)\left\{\frac{x^\delta}{[x^\delta+(1-x)^\delta]^{\frac{1}{\delta}}}\left[((-w_2)C_2)^\beta-K_2{}^\beta\right]-\frac{[x^\delta+(1-x)^\delta]^{\frac{1}{\delta}}-x^\delta}{[x^\delta+(1-x)^\delta]^{\frac{1}{\delta}}}K_2{}^\beta\right\} \tag{22}$$

$$J_{11}{}'=\frac{\partial J_{11}}{\partial x},J_{12}=\frac{\partial J_{11}}{\partial y},J_{21}=\frac{\partial J_{22}}{\partial x},J_{22}{}'=\frac{\partial J_{22}}{\partial y} \tag{23}$$

$$\det(J)=[(1-2x)J_{11}+x(1-x)J_{11}{}']\times[(1-2y)J_{22}+y(1-y)J_{22}{}']-xy(1-x)(1-y)J_{12}J_{21} \tag{24}$$

$$tr(J)=(1-2x)J_{11}+x(1-x)J_{11}{}'+(1-2y)J_{22}+y(1-y)J_{22}{}' \tag{25}$$

$$M=T_2\,/\,(T_1+T_2) \tag{26}$$

$$E_1=1-2\mu_1+2\mu_1P_{B1} \tag{27}$$

$$D_1=(-M(M-1)C_1)^\beta-K_1{}^\beta \tag{28}$$

$$H_1=K_1{}^\beta,H_2=K_2{}^\beta \tag{29}$$

$$I_1=(-(|1-2M|-1)C_1)^\beta-K_1^\beta \tag{30}$$

$$D_2=(-M(M-1)C_2)^\beta-K_2{}^\beta \tag{31}$$

$$I_2 = (-(|1-2M|-1)C_2)^{\beta} - K_2^{\beta} \tag{32}$$

By substituting the 5 sets of equilibrium points into equations (24) and (25) to calculate $\det(J)$ and $tr(J)$, the local stability results are shown in Table 5. The calculation process of the intermediate variables involved, denoted as $M, E_1, D_1, D_2, I_1, I_2, H_1, H_2$, is provided by equations 26–32.

4.2. Stability analysis of evolutionary equilibrium points

From Table 5, variable values of the system payoff matrix, where $H_1 > 0$, $H_2 > 0$, primarily determine the positive and negative of $\det(J)$ and $tr(J)$. Therefore, E_1, D_1, D_2, I_1, I_2 play a major role in determining the state of equilibrium points.

E_1 reflects the influence of conformity effect. When $E_1 > 0$, there are two cases. Case 1: $\mu_1 < 0.5$, which means that the supporters are weakly related to the crowd. Case 2: $\mu_1 > 0.5$, $P_{B1} > 1 - 1/2\mu_1$, which means that the supporters are strongly related to the crowd and the degree of information forwarding is high. When $E_1 < 0$, i.e. $\mu_1 > 0.5$ and $P_{B1} < 1 - 1/2\mu_1$, it means that supporters are strongly correlated with the crowd, and the degree of information forwarding is low. D_1, D_2, I_1, I_2 reflect the risk-taking cost of feedback strategy adopted by supporters and opponents. More specifically, D_1 and I_1 respectively reflect the minimum risk cost and maximum forwarding risk cost of supporters when the reporting probability of opponents is high, $I_1 > D_1$. D_2 and I_2 respectively reflect the minimum risk cost and maximum reporting risk cost of opponents when the forwarding probability of supporters is high, $I_2 > D_2$. D_1, D_2, I_1, I_2 can be combined into 9 conditions. Given the conditions and E_1, the results of local stability analysis, which is applied to the 5 sets of equilibrium points under 18 different information flow scenarios, are shown in Table 6.

According to Table 6, under different initial conditions and scenarios, the evolution results of the system are different. Observing the scenarios with an even label, when supporters are strongly correlated but the message is relatively unpopular, supporters are less sensitive to interests and tend to imitate other supporters, and opponents tend to take the initiative, which ultimately results in either opponents adapting lurking strategy or triggering conflict.

Observing the odd-labeled scenarios, where supporters are weakly correlated and the information has a certain degree of popularity, supporters are prone to risk seeking, and their sensitivity to interests increases.

Fig. 2(a) and (b) present the game evolution process of scenario 9 and scenario 10, respectively. Taking scenario 9 as an example, the system finally converges to 2 center points $S_5 = (1, y^*)$ and $S_5 = (x^*, 1)$.

In scenario 9, when the supporters are stronger than the opponents under the initial strategy conditions, there are more smart objects who resonate with the message. The system converges to $S_5 = (1, y^*)$, which can reduce the probability of the opponent's reporting based on interests through conflict punishment, and avoid malicious reporting in some degree;

When the supporters are weaker than the opponents under the initial strategy conditions, there is a high probability that the information is controversial. The system converges to $S_5 = (x^*, 1)$. The supporters will reduce the forwarding probability under the conflict punishment, reduce the dissemination of disputed information, and avoid the expansion of conflicts.

Scenario 9 is the evolution result under the rational decision of both parties, which should be reached among smart objects through reasonable information management strategies. Therefore, **Condition 5 corresponding to Scenario 9 can be used as a reference for parameter design principles in actual malicious information suppression measures**.

5. Sensitivity analysis and discussion

5.1. System dynamics model and the parameter setting

Using the Vensim software, a system dynamics model of aforementioned game model is established, which is mainly composed of 4 kinds of variables, including 11 external variables, 8 intermediate variables, 2 rate variables, and 4 level variables.

According to Fig. 3, the proportion of two groups of smart objects who adopt feedback strategy and lurking strategy is presented by 4 level variables. The change rate of the percentage of smart objects adopting the feedback strategy is described by 2 rate variables. The 11 external variables come from the subset of variables in Tables 1, 3 and 4.

The flow rate and the intermediate variables involved in the above model are mainly formulated in accordance with the replicator dynamics equations (17) and (18).

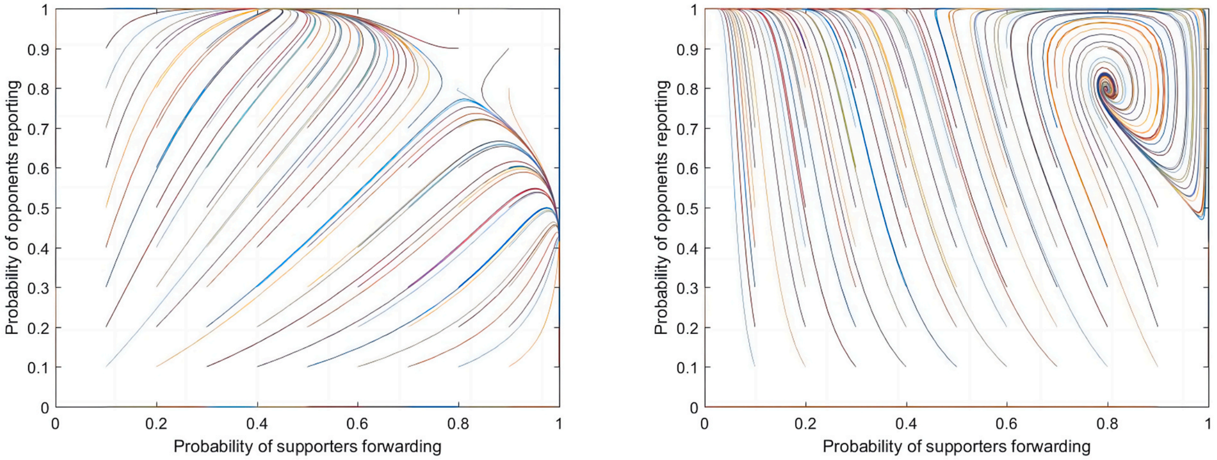
Whether supporters and opponents choose feedback strategy mainly depends on the other party's choice, expected benefits, and risk preference. The factors affecting the final strategy of the participants include basic income, deposit, reputation points, and conformity effect. To further investigate how the above factors influence the implementation of the information conflict suppression

Table 5
Rank and trace of Jacobian matrix corresponding to different equilibrium points.

equilibrium points	$\det(J)$	$tr(J)$
S_1	$\lambda^2 E_1 (K_1 + C_1)^{\beta} (K_2 + C_2)^{\beta}$	$\lambda[E_1 (K_1 + C_1)^{\beta} + (K_2 + C_2)^{\beta}]$
S_2	$\lambda^2 E_1 D_1 H_2$	$-\lambda(E_1 D_1 + H_2)$
S_3	$\lambda^2 E_1 D_2 H_1$	$-\lambda(E_1 H_1 + D_2)$
S_4	$\lambda^2 E_1 I_1 I_2$	$\lambda(E_1 I_1 + I_2)$
S_5	$x^* y^* (1-x^*)(1-y^*)(J_{11}' \vert_{x=x^*} J_{22}' \vert_{y=y^*} - J_{12} \vert_{y=y^*} J_{21} \vert_{x=x^*})$	$x^*(1-x^*) J_{22}' \vert_{y=y^*} + y^*(1-y^*) J_{11}' \vert_{x=x^*}$

Table 6
Stability analysis results of equilibrium points under different information cases.

Condition Index	Condition	Conformity	Scenario Index	S_1	S_2	S_3	S_4	S_5
1	$D_1 > 0, I_1 > 0$	$E_1 > 0$	1		✓	✓		
	$D_2 > 0, I_2 > 0$	$E_1 < 0$	2					✓
2	$D_1 > 0, I_1 > 0$	$E_1 > 0$	3		✓			
	$D_2 < 0, I_2 > 0$	$E_1 < 0$	4					✓
3	$D_1 > 0, I_1 > 0$	$E_1 > 0$	5		✓			
	$D_2 < 0, I_2 < 0$	$E_1 < 0$	6				✓	
4	$D_1 < 0, I_1 > 0$	$E_1 > 0$	7			✓		
	$D_2 > 0, I_2 > 0$	$E_1 < 0$	8		✓			
5	$D_1 < 0, I_1 > 0$	$E_1 > 0$	9					✓
	$D_2 < 0, I_2 > 0$	$E_1 < 0$	10		✓			
6	$D_1 < 0, I_1 > 0$	$E_1 > 0$	11					✓
	$D_2 < 0, I_2 < 0$	$E_1 < 0$	12		✓		✓	
7	$D_1 < 0, I_1 < 0$	$E_1 > 0$	13			✓		
	$D_2 > 0, I_2 > 0$	$E_1 < 0$	14		✓			
8	$D_1 < 0, I_1 < 0$	$E_1 > 0$	15					✓
	$D_2 < 0, I_2 > 0$	$E_1 < 0$	16		✓			
9	$D_1 < 0, I_1 < 0$	$E_1 > 0$	17				✓	
	$D_2 < 0, I_2 < 0$	$E_1 < 0$	18		✓			



(a) scenario 9

(b) scenario 10

Fig. 2. Game evolution process under condition 5.

strategy, a sensitivity analysis of the system dynamics model is performed below, which is based on **Condition 5** and **Scenario 9** founded in Section 4. The parameter settings are as follows.

Based on median estimates given by Refs. [20,29], the risk attitude coefficient β, the decision weighting function's curvature in the loss state δ, and the loss aversion coefficient parameter λ are set to be 0.8798, 0.6891, and 2.2514, respectively. The starting mixed strategy (x, y) of participants during sensitivity analysis is fixed at (0.5, 0.5) and the values of K_1, K_2, T_1, T_2, C_1, C_2 are designed to satisfy **Condition 5**. Specifically, for the analysis involved with basic income and deposit, which is independent of conformity effect, the values of μ_1 and P_{B1} are set to satisfy the constraint of **Scenario 9**.

5.2. *Analysis of evolution influencing factors*

5.2.1. *Impact of basic income on evolution results*

According to equations (33) and (34), the changing rate of the supporter's forwarding probability x with respect to t is related to $(1 - 2\mu_1 + 2\mu_1 P_{B1})$, while the rate of change of the opponent's reporting probability y with respect to t increases as K_2 increases.

$$\frac{\partial G_1(x, y)}{\partial\left(K_1^{\beta}\right)} = \lambda x(1 - x)(1 - 2\mu_1 + 2\mu_1 P_{B1}) \tag{33}$$

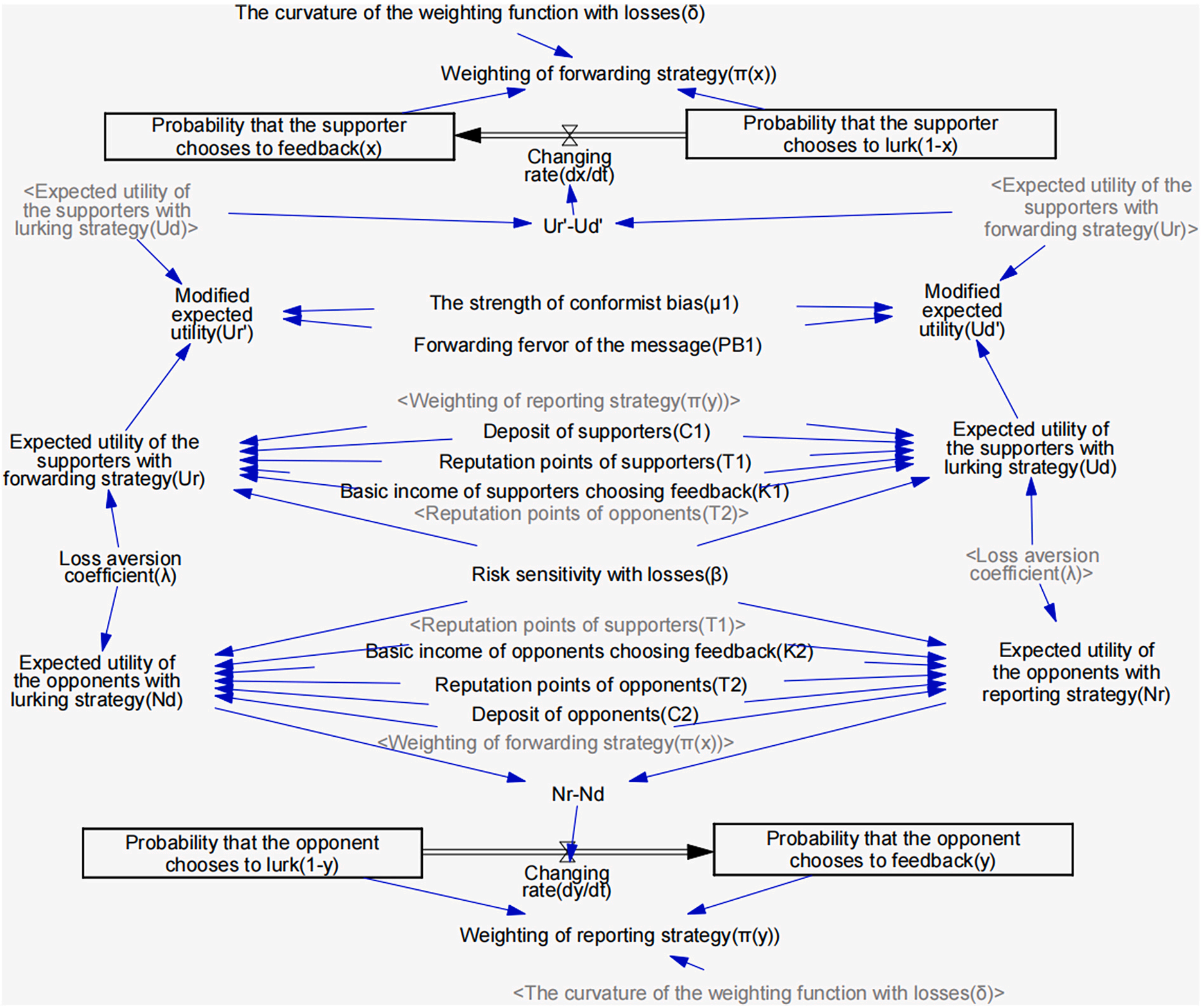
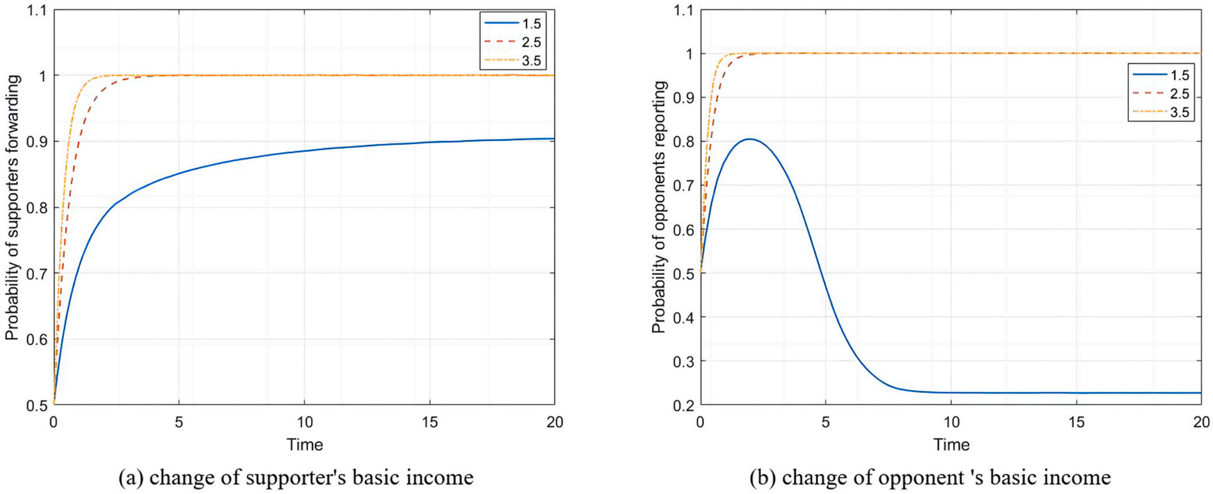

The curvature of the weighting function with losses(δ)
Weighting of forwarding strategy(π(x))
Probability that the supporter chooses to feedback(x)
Probability that the supporter chooses to lurk(1-x)
Changing rate(dx/dt)
<Expected utility of the supporters with lurking strategy(Ud)>
Ur'-Ud'
<Expected utility of the supporters with forwarding strategy(Ur)>
Modified expected utility(Ur')
The strength of conformist bias(μ1)
Forwarding fervor of the message(PB1)
Modified expected utility(Ud')
<Weighting of reporting strategy(π(y))>
Expected utility of the supporters with forwarding strategy(Ur)
Deposit of supporters(C1)
Reputation points of supporters(T1)
Basic income of supporters choosing feedback(K1)
<Reputation points of opponents(T2)>
Expected utility of the supporters with lurking strategy(Ud)
Loss aversion coefficient(λ)
Risk sensitivity with losses(β)
<Loss aversion coefficient(λ)>
<Reputation points of supporters(T1)>
Expected utility of the opponents with lurking strategy(Nd)
Basic income of opponents choosing feedback(K2)
Reputation points of opponents(T2)
Deposit of opponents(C2)
<Weighting of forwarding strategy(π(x))>
Expected utility of the opponents with reporting strategy(Nr)
Nr-Nd
Probability that the opponent chooses to lurk(1-y)
Changing rate(dy/dt)
Probability that the opponent chooses to feedback(y)
Weighting of reporting strategy(π(y))
<The curvature of the weighting function with losses(δ)>

Fig. 3. The system dynamics model of SIoT information conflict.



(a) change of supporter's basic income

(b) change of opponent 's basic income

Fig. 4. The impact of basic income on evolution results.

$$\frac{\partial G_2(x,y)}{\partial\left(K_2^{\beta}\right)} = \lambda y(1-y) \geq 0 \tag{34}$$

(1) Set the parameters as $\mu_1 = 0.3$, $P_{B1} = 0.6$, $C_1 = C_2 = 4$, $T_1 = T_2 = 5$, $K_2 = 2$, and control K_1 as 1.5, 2.5, and 3.5, respectively. Fig. 4(a) presents the evolution trends of supporters' forwarding probability.

(2) Set the parameters as $\mu_1 = 0.3$, $P_{B1} = 0.6$, $C_1 = C_2 = 4$, $T_1 = T_2 = 5$, $K_1 = 2$, and control K_2 to be 1.5, 2.5, and 3.5, respectively. Fig. 4(b) presents the evolution trends of opponents' reporting probability.

As shown in Fig. 4, with other parameters fixed, when the basic income increases, the feedback probability of game party increases and the convergence speed is accelerated. The results show that intentional information with higher basic income, for example malicious message, is more dominant in dissemination in actual social networks [30], which confirms the effectiveness of the proposed model.

5.2.2. *Impact of deposit on evolution results*

For both supporters and opponents, the deposit C_1 and C_2 are their largest estimated risk-taking costs in making feedback decisions. According to equations (35) and (36), the rate of change of the supporter's forwarding probability x with respect to t is related to $(1 - 2\mu_1 + 2\mu_1 P_{B1})$. Whereas as C_2 increases, the rate of change of the report probability y of opponents relative to t decreases with the increase of C_2.

$$\frac{\partial G_1(x,y)}{\partial\left(C_1{}^{\beta}\right)} = x(1-x)(-\lambda)(1-2\mu_1+2\mu_1 P_{B1}) \times \frac{y^{\delta}}{\left[y^{\delta}+(1-y)^{\delta}\right]^{\frac{1}{\delta}}}(-w_1)^{\beta} \tag{35}$$

$$\frac{\partial G_2(x,y)}{\partial\left(C_2{}^{\beta}\right)} = y(1-y)(-\lambda) \times \frac{x^{\delta}}{\left[x^{\delta}+(1-x)^{\delta}\right]^{\frac{1}{\delta}}}(-w_2)^{\beta} \leq 0 \tag{36}$$

(1) Set the parameters as $\mu_1 = 0.3$, $P_{B1} = 0.6$, $K_1 = K_2 = 2$, $T_1 = T_2 = 5$, $C_2 = 4$, and control C_1 as 3.5, 5.5, and 7.5, respectively. Fig. 5(a) displays the evolution results of the changes in supporters' deposit.

(2) Set the parameters as $\mu_1 = 0.3$, $P_{B1} = 0.6$, $K_1 = K_2 = 2$, $T_1 = T_2 = 5$, $C_1 = 4$, and control C_2 as 3.5, 5.5, and 7.5, respectively. Fig. 5(b) displays the evolution results of the changes in opponents' deposit.

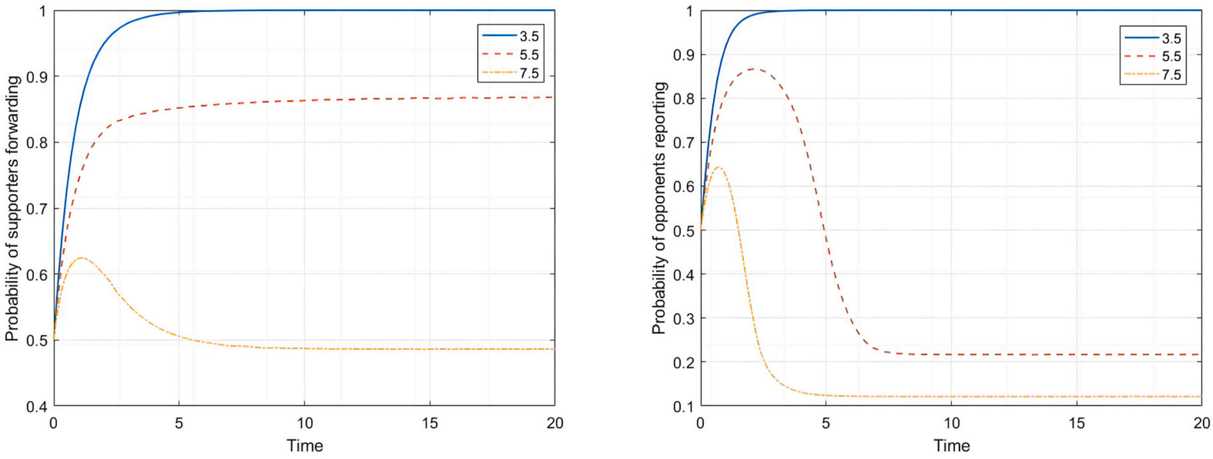
It is clearly seen from Fig. 5 that, with other parameters fixed, when the deposit increases, the feedback probability of game party decreases and the convergence rate slows down.

A proper deposit is important to suppress the dissemination of disagreement of smart objects. To handle malicious message better, the deposit for supporters should be increased to balance their higher basic income.

5.2.3. *Impact of conformity effect on evolution results*

The conformity effect influences the tendency of supporters and opponents to give feedback. To investigate how the two parameters, the strength of conformist bias μ_1 and the forwarding heat P_{B1}, affect the probability of two parties' strategy selection.

The values of μ_1 is changed to 0.3 and 0.7, respectively indicating the weak correlation and strong correlation of supporters. And



(a) change of supporter's deposit

(b) change of opponent 's deposit

Fig. 5. The impact of deposit on evolution results.

the value of P_{B1} is changed to 0.1, 0.5, 0.9, indicating the low, medium and high popularity of information, respectively.

(1) Set the importance of conformity to weak correlation, $\mu_1 = 0.3$, set parameters as $K_1 = K_2 = 2$, $T_1 = T_2 = 5$, $C_1 = C_2 = 4$, control P_{B1} as 0.1, 0.5, 0.9 respectively. Fig. 6(a) depicts the evolution trends of supporters' forwarding probability as P_{B1} changes.

(2) Set the importance of conformity to strong correlation, $\mu_1 = 0.7$, set parameters as $K_1 = K_2 = 2$, $T_1 = T_2 = 5$, $C_1 = C_2 = 4$, control P_{B1} as 0.1, 0.5, 0.9 respectively. Fig. 6(b) depicts the evolution trends of supporters' forwarding probability as P_{B1} changes.

Fig. 6 shows that the increase in popularity of information accelerates the convergence of the supporter's forwarding probability in both cases, and the change range of x increases with the enhancement of conformist bias. Under the influence of the conformity effect, the current state of the two parties and the estimated gains or losses are no longer the main basis for the decision-making of the players. Instead, their behaviors change according to the decision of others in the same camp (such as their circle of friends).

The results show that the model matches the general observed phenomenon that individuals have group adaptive expectations in their judgment [31]. Therefore, in terms of system design, it is suggested to dynamically increase the deposit when the popularity increases, so as to enhance the rationality of decision-making and reduce the degree of group adaptive expectations.

6. Recommended reward and punishment strategies

From the foregoing simulation results and analyses, basic income is positively related to the game party's implementation of feedback strategies, while deposit is negatively related to that. For supporters, the conformity effect and the increase in information popularity will also promote the rise of forwarding probability. And when there is a large gap between the reputation points of the two parties, it plays a facilitating role for the forwarding and reporting strategy, and vice versa, it plays a suppressing role.

Basic income partly acts as an external factor, which is unlikely to be entirely controlled by the reputation system. The only factor that could be fully controlled is the deposit. To achieve good governance, a low deposit for low conflict information would help to encourage sharing, and a high deposit for high conflict information would help to limit the disagreement.

For the mechanism proposed in Section 2.1, a suggestion on how to calculate basic income and deposit is given below.

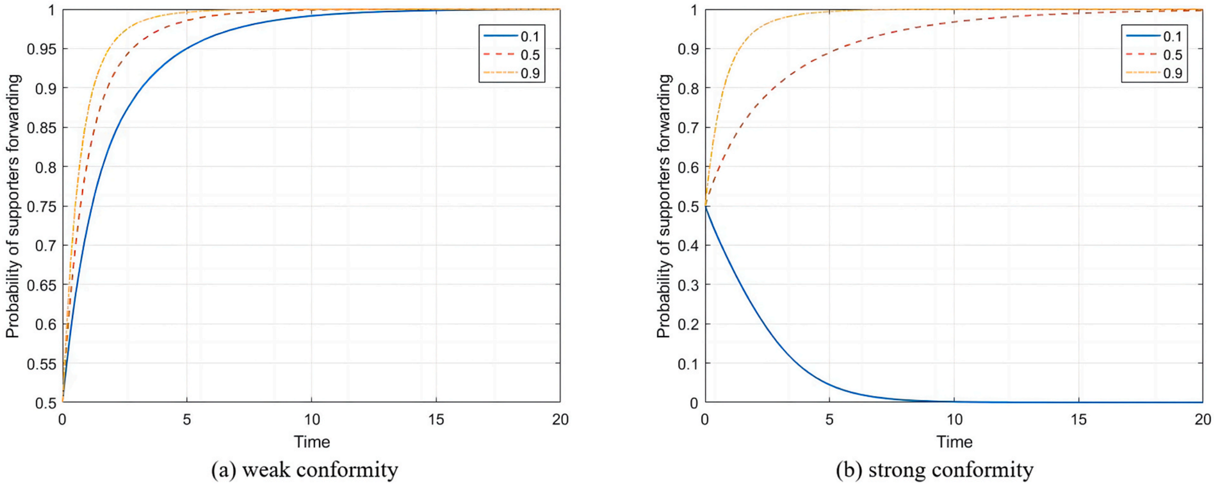
Assume that r_1 and r_2 denote the number of forwarding and reporting, respectively. Then the degree of conflict caused by information can be measured by two parts: the degree of disagreement F_1 and the scope of influence F_2.

$$F_1 = 1 - |r_1 - r_2| \, / \, (r_1 + r_2) \tag{37}$$

$$F_2 = \ln(r_1 + r_2) \tag{38}$$

$$\left.\begin{array}{l} F_m = r_1/(r_1 + r_2) \\ F_n = r_2/(r_1 + r_2) \end{array}\right\} \tag{39}$$

Equations (37) and (38) present the calculation method of F_1 and F_2, respectively. F_1 is between 0 and 1, and a larger F_1 indicates greater disagreements between supporters and the opponents. The larger F_2 means the greater the influence scope of the information. The strengths of forwarding and reporting, denoted as F_m and F_n, are set as equation (39). Information popularity threshold T can be set in different situation. Assuming the reputation points that supporters can obtain by forwarding is K_1, and the reputation points that



(a) weak conformity

(b) strong conformity

Fig. 6. The impact of conformity effect on evolution results.

opponents can obtain by reporting is K_2. According to simulation results, K_2 should be 1.5 to 2 times K_1 in the actual system. The deposits C_1 and C_2 can be calculated using equations 40–42:

$$C_1 = e^{4(F_1 - 0.5)}\left(\frac{2F_2}{F_2 + T}\right)F_m K_1 \tag{40}$$

$$C_2 = e^{4(F_1 - 0.5)}\left(\frac{2F_2}{F_2 + T}\right)F_n K_2 \tag{41}$$

$$K_1 < K_2 \tag{42}$$

The above formula satisfies Condition 5 of Section 4.2. In practical systems, deposit could be dynamically adjusted to achieve good governance in following ways:

(1) When $F_1 < 0.5$, and $F_2 < T$, the disagreement between the supporters and opponents of the information is small, and the influence of the information is also small. The relationship of basic income given by the system and deposit is $C_1 < 0.75K_1$, and $C_2 < 0.75K_2$, so as to ensure that the atmosphere of sharing is not damaged.

(2) When $F_1 > 0.5$, and $F_2 > T$, the information divergence and influence range are large. The relationship of basic income and deposit is $0.75K_1 < C_1 < e^2K_1$, and $0.75K_2 < C_2 < e^2K_2$, which strengthens the rationality of information forwarding and reporting. Bigger deposit can be helpful.

7. Conclusion

In this paper, dynamic reward and punishment strategies are proposed for the reputation-based dynamic information management mechanism in SIoT. The mentality behind the proposed model is that if smart object's awareness of information conflicts enhances, they can judge more precisely about malicious information. We firstly utilized the evolutionary game model for information conflicts in the SIoT network, with cumulative prospect theory and conformity effect. The numerical simulations and sensitivity analysis on the proposed mechanism verified its usefulness in suppressing controversial information. Such model setup and simulation results would motivate the SIoT network developers to design reputation-based information management system as well as to build feasible information conflict control facilities in their own products. The following are the main conclusions and managerial implications.

(1) The basic income and deposit of both sides, the popularity of information as well as the importance of conformity effect all have a significant impact on the system's steady state and evolutionary path. Specific condition which can keep the system in a less-conflict situation is found, and it can be used as a reference for actual measures design to guide the game parties to **rationally treat information conflicts and achieve conflict suppression.**

(2) The proposed game model well simulated the reputation system. Results show that the model matches the general observed phenomenon: individuals have group adaptive expectations in judgment and intentional information is more dominant in dissemination.

(3) A quantitative information management strategy for good governance in SIoT is given at Section 6: the recommendation formula for real-time calculation of deposit (reputation deposit), which can be used and tested in reputation-based information management mechanism proposed for SIoT networks.

In future work, the corresponding malicious information judgment algorithm and blockchain technology will be integrated with information management strategies to achieve an information management system. Taking advantage of security features and intelligent management and manipulation of data, the blockchain based information management system can be used in the SIoT network to effectively suppress malicious information while efficiently sharing information. It can help improve the data flow system in SIoT.

Author contribution statement

Shuting Liu: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper.

Yinghua Ma: Conceived and designed the experiments; Contributed reagents, materials, analysis tools or data; Wrote the paper.

Xiuzhen Chen: Conceived and designed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper.

Funding statement

Support for this work was provided by the Joint Funds of the National Natural Science Foundation of China (U200320075), Action Plan of Science and Technology Innovation of Science and Technology Commission of Shanghai Municipality (No.22511101202).

Data availability statement

Data included in article/supplementary material/referenced in article.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Wazir Zada Khan, Saqib Hakak, Muhammad Khurram Khan, Trust management in social internet of things: architectures, recent advancements, and future challenges, IEEE Internet Things J. 8 (10) (2020) 7768–7788.

[2] Kun Guo, et al., Artificial intelligence-based semantic internet of things in a user-centric smart city, Sensors 18 (5) (2018) 1341.

[3] Pradeep Bedi, et al., Application of AI/IoT for smart renewable energy management in smart cities, in: AI and IoT for Smart City Applications, 2022, pp. 115–138.

[4] Nguyen Binh Truong, et al., Toward a trust evaluation mechanism in the social internet of things, Sensors 17 (6) (2017) 1346.

[5] Ji Eun Kim, Xiangmin Fan, Daniel Mosse, Empowering end users for social internet of things, in: Proceedings of the Second International Conference on Internet-Of-Things Design and Implementation, 2017.

[6] Dina Hussein, et al., Towards a dynamic discovery of smart services in the social internet of things, Comput. Electr. Eng. 58 (2017) 429–443.

[7] A. Khelloufi, et al., A social relationships based service recommendation system for SIoT devices, IEEE Internet Things J. 8 (2020) 1859–1870.

[8] M.S. Roopa, et al., Social Internet of Things (SIoT): foundations, thrust areas, systematic review and future directions, Comput. Commun. 139 (2019) 32–57.

[9] Sana Alam, et al., Trust management in social internet of things (SIoT): a survey, IEEE Access 10 (2022) 108924–108954.

[10] Michele Nitti, et al., A subjective model for trustworthiness evaluation in the social internet of things, in: 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio communications-(PIMRC), IEEE, 2012.

[11] MengChu Zhou, Evolution from AI, IoT and big data analytics to metaverse, IEEE/CAA J. Automat. Sinica 9 (12) (2022) 2041–2042.

[12] Kefa Rabah, Convergence of AI, IoT, big data and blockchain: a review, Lake Inst. J. 1 (1) (2018) 1–18.

[13] Zhikui Chen, et al., A scheme of access service recommendation for the Social Internet of Things, Int. J. Commun. Syst. 29 (4) (2016) 694–706.

[14] Dina Hussein, Soochang Park, Noel Crespi, A cognitive context-aware approach for adaptives services provisioning in Social Internet of Things, in: 2015 IEEE International Conference on Consumer Electronics (ICCE), IEEE, 2015.

[15] Michele Nitti, Luigi Atzori, Irena Pletikosa Cvijikj, Network navigability in the social internet of things, in: 2014 IEEE World Forum on Internet of Things, (WF-IoT). IEEE, 2014.

[16] Liehuang Zhu, et al., PRIF: a privacy-preserving interest-based forwarding scheme for social Internet of Vehicles, IEEE Internet Things J. 5 (4) (2018) 2457–2466.

[17] Eleftherios Kokoris-Kogias, Orfefs Voutyras, Theodora Varvarigou, TRM-SIoT: a scalable hybrid trust & reputation model for the social internet of things, in: 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), IEEE, 2016.

[18] Nguyen B. Truong, et al., From personal experience to global reputation for trust evaluation in the social internet of things, in: GLOBECOM 2017-2017 IEEE Global Communications Conference, IEEE, 2017.

[19] G.M. Lee, N.B. Truong, A Reputation and Knowledge Based Trust Service Platform for Trustworthy Social Internet of Things, 2016.

[20] A. Tversky, D. Kahneman, Advances in prospect theory: cumulative representation of uncertainty, J. Risk Uncertain. 5 (4) (1992) 297–323.

[21] B. Skyrms, Dynamics of conformist bias, Monist 88 (2) (2005) 260–269.

[22] D. Choi, S. Chun, H. Oh, et al., Rumor propagation is amplified by echo chambers in social media, Sci. Rep. 10 (1) (2020) 1–10.

[23] T.L. Vincent, Evolutionary games, J. Optim. Theor. Appl. 46 (1985) 605e12.

[24] H. Gintis, Game Theory Evolving: A Problem-Centered Introduction to Modeling Strategic Behavior, Princeton university press, 2000.

[25] M.J. Machina, "Expected Utility hypothesis." Utility and Probability, Palgrave Macmillan, London, 1990, pp. 79–95.

[26] S.-M. Choi, H. Lee, Y.-S. Han, K.L. Man, W.K. Chong, A recommendation model using the bandwagon effect for E-marketing purposes in IoT, Int. J. Distributed Sens. Netw. 11 (7) (2015).

[27] L.J. Tian, X. Yang, H.J. Huang, et al., The cumulative prospect theory-based travel mode choice model and its empirical verification, Sys. Eng. Theo. Prac. 36 (7) (2016) 1778–1785.

[28] D. Friedman, On economic applications of evolutionary game theory, J. Evol. Econ. (8) (1998) 15–43.

[29] L.H. Xu, Y.Z. Pian, Y.J. Lin, et al., Game analysis of conflicts between pedestrians and vehicular traffic on unsignalized road sections based on cumulative prospect theory, China J. Highw. Transp. 35 (1) (2022) 18.

[30] J.M. Wu, Y. Liu, Governing both Germany and law: dual governance of internet rumors——also on the regulation of "internet rumors" in the securities market, Securit. Law Rev. 18 (2) (2016) 374–393.

[31] G.W. Li, Social mechanism of rumor realization and information governance, Society (4) (2005) 143–155.