STSIR: An individual-group game-based model for disclosing virus spread in social internet of things

Guowen Wu, Lanlan Xie, Hong Zhang, Jianhua Wang, Shigen Shen, Shui Yu

PII: S1084-8045(23)00027-9

DOI: https://doi.org/10.1016/j.jnca.2023.103608

Reference: YJNCA 103608

To appear in: *Journal of Network and Computer Applications*

Received Date: 24 March 2022

Revised Date: 3 January 2023

Accepted Date: 23 February 2023

Please cite this article as: Wu, G., Xie, L., Zhang, H., Wang, J., Shen, S., Yu, S., STSIR: An individual-group game-based model for disclosing virus spread in social internet of things, *Journal of Network and Computer Applications* (2023), doi: https://doi.org/10.1016/j.jnca.2023.103608.

CRediT author statement

Guowen Wu: Conceptualization, Methodology, Software.

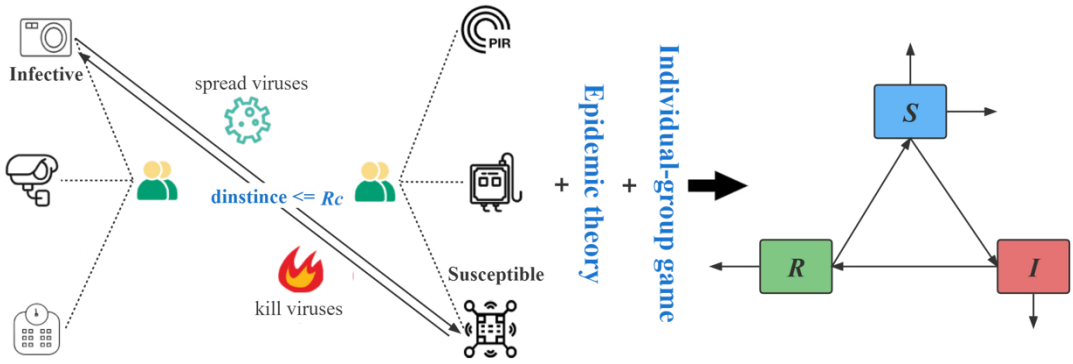
Lanlan Xie: Methodology, Software, Writing- Original draft preparation.

Hong Zhang: Validation, Writing- Reviewing and Editing.

Jianhua Wang: Investigation, Resources.

Shigen Shen: Supervision, Data curation.

Shui Yu: Project administration.



STSIR: An individual-group game-based model for disclosing virus spread in Social Internet of Things

Guowen Wu [a], Lanlan Xie [a], Hong Zhang [a], Jianhua Wang [b], Shigen Shen [c,*], Shui Yu [d]

[a] School of Computer Science and Technology, Donghua University, Shanghai 201620, China

[b] School of Engineering, Huzhou University, Huzhou 313000, Zhejiang, China

[c] Department of Computer Science and Engineering, Shaoxing University, Shaoxing 312000, Zhejiang, China

[d] School of Computer Science, University of Technology Sydney, NSW, Australia

Abstract: Social Internet of Things (SIoT) with deep integration of Internet of Things and social networks has become a target of a large number of hackers who attempt to spread viruses for breaching data confidentiality and service reliability. Therefore, exposing the law of virus spread with social characteristics and addressing historical dependence of infection and recovery rates in an SIoT are urgent problems to be solved at present. To this end, we propose a novel virus spread model (STSIR) based on an epidemic theory's analysis framework and individual-group game theory, which more reasonably describes viruses spread among devices considering people behavior. Aiming at the characteristics of SIoTs including limited social distance and dynamic number variation of people and devices, we adopt and improve the traditional epidemic model SIR to reveal the form of viruses continuously spreading to neighbor nodes. We then introduce an individual-group game to establish the attack and defense model between infected SIoT nodes and susceptible SIoT nodes, in order to not only obtain the mixed Nash equilibrium solution by using a payoff matrix but also solve the dependence of the infection and recovery rates on historical experience. Further, we establish differential equations to represent the model STSIR, which are the basis of proving the existence of model equilibrium points and analyzing stability mathematically. Finally, the effectiveness of the model STSIR in curbing virus spread is verified by simulating two equilibrium points. Under the same conditions in an SIoT, the model STSIR reduce viruses by ~45% more than the model SIS, and saves stabilization time cost by ~66.7% compared with the model SIR, which proves that the model STSIR is obviously more effective.

Keywords: Social Internet of things; Virus spread; Individual-group game; Epidemic theory; Stability; Equilibrium points

1 Introduction

Social Internet of Things (SIoT) is a new paradigm (Cai et al., 2022; Jiang et al., 2020), where Internet of Things (IoT) merges with social networks, providing a network platform for objects (i.e. people and devices) to share information and socialize with other objects by utilizing comprehensive relationships among objects (Chung and Liang, 2020; Wang et al., 2022), making the world more convenient and more efficient (Qiu et al., 2020). SIoT enables objects to communicate with each other automatically, nevertheless, it is not reliable when objects are vulnerable to attack (Zhu et al., 2020). Especially viruses spread is a major threat to the security of cyber activities (Signes-Pont et al., 2018). Once an SIoT node is infected, the virus will quickly spread to the neighboring nodes along the SIoT network. It can monitor, illegally access, steal and tamper with data, causing serious property losses and privacy violations. It is our bounden responsibility and mission to reduce the harm of SIoT virus attacks on social economy and privacy leakage in the background of Internet, and to curb the spread of virus in a short time by studying the law of virus spread in SIoTs, which motivates us to carry out the current research. At present, researches on SIoT viruses pay popular attention to two aspects: one is to detect SIoT viruses, and the

* Corresponding author.
E-mail address: gwwu@dhu.edu.cn (G. Wu), xielan0052@163.com (L. Xie), zhanghong@dhu.edu.cn (H. Zhang), jianhua026637@163.com (J. Wang), shigens@usx.edu.cn (S. Shen), shui.yu@uts.edu.au (S. Yu)

other is to study the spread law and containment measures of viruses in an SIoT. This paper mainly focuses on the latter rather than discussing virus detection in detail.

Game theory is a mathematical tool and method that studies the nature of struggle or competition, which has been broadly used in network security (Shen et al., 2022; Rasool et al., 2022; Shen et al., 2017; Sun, 2021). Specially, the individual-group game, where both parties participate in with only one individual on one side and multiple individuals on the other side, is a process in which both parties decide their own actions based on the strategies the other party may adopt in order to maximize its returns. When neither party can improve returns by unilaterally changing its own strategy, the game reaches the Nash equilibrium that maximizes gains for all parties (Wu and Wang, 2018; Liu et al., 2021). The normal nodes and viruses in an SIoT are regarded as the two sides in the game, and both sides will consider the actual actions of the other side in the spread process in order to reach the Nash equilibrium. As a common virus activity monitoring method, intrusion detection system (IDS) (Louk and Tama, 2023) is used in SIoT to detect viruses and kill them in time, which will hinder the spread of viruses to normal nodes. When an infected SIoT node sends viruses to nearby susceptible ones, susceptible SIoT nodes need to consider whether the infected SIoT node sends viruses to themselves. It also needs to consider whether the susceptible SIoT nodes call IDS or not due to energy consumption, indicating that the intrusion detection process in an SIoT is an individual-group game (Ariful and Jun, 2020; Shakya et al., 2019; Tavanpour et al., 2020). Therefore, the individual-group game is herein used to analyze the process of virus spread in an SIoT.

Mathematical modeling of infectious diseases has a long history (Castellano et al., 2015; Giordano et al., 2020; Hethcote, 2000; Hota et al., 2021; Leonardo Stella, 2021). Epidemiology-based models describing infectious disease spread can be employed to study the dynamics of virus spread in an SIoT (Chen et al., 2016; Mahboubi et al., 2017) because of the high similarity between infectious diseases and viruses in the SIoT. Existing epidemic models include Susceptible-Infected (SI), Susceptible-Infected-Susceptible (SIS) (Punzo, 2022), Susceptible-Infected-Recovered (SIR) (Chen et al., 2016; Mei et al., 2017) etc. In particular, the model SIR has great application to numerous scenarios of virus spread (Hota, et al., 2021; Pagliara and Leonard, 2021). In an SIoT, nodes that have never been infected by viruses are considered susceptible ones and are susceptible to viruses. When susceptible nodes are infected by viruses, they will become infected nodes. Some of infected nodes will become recovered nodes after killing the viruses and have certain ability to resist virus reinfection. Since the model SIS tends to describe scenarios where nodes are still susceptible to viruses after killing them, it is not suitable for SIoTs. Therefore, this paper is mainly based on the model SIR rather than the model SIS.

Herein, we propose a novel model called STSIR by extending the model SIR using epidemiology theory. Compared with the traditional model SIR, we combine the characteristics including limited social distance and number of users changing dynamically in an SIoT. For the social distance, objects and people in an SIoT are defined as social units, which can exchange normal information or send viruses according to their social distance. Then we proposed a social distance criterion based on the six degrees of separation (Ke, 2010), in order to specifically describe the network influence degree of social units with different social distances in the SIoT. In addition, in order to realistically depict the dynamics of both sides in the process of attack and defense between viruses and nodes, we introduce an individual-group game to obtain the mixed Nash equilibrium solution of the payoff matrix, realizing a function of automatic acquisition of the infection and recovery rates of the model STSIR and avoiding their dependence on historical experience. Finally, the effectiveness of the model STSIR is proved by lots of simulation experiments.

Our contributions are summarized as follows:

- We propose a model STSIR that is innovatively defined a social distance criterion and improved to describe the spread of infected SIoT nodes in an SIoT, which not only considers a situation that infected SIoT nodes lose

infectivity to external nodes after spreading along the limited social distance, but also describes the influence of dynamic changes of user traffic in the network, making the model STSIR more universal to an SIoT.

- We first construct an individual-group game where the game type is based on an SIoT attack and defense process between infected SIoT nodes and susceptible SIoT nodes, which is the reason why the infection and recovery rates in STSIR are automatically obtained by calculating the return matrix of the game, naturally solving an important issue of lack of the infection and recovery rates in the spread of new viruses.
- We prove the existence and stability of equilibrium points of the model STSIR while the threshold of viruses diffusion or extinction is calculated. Moreover, three initial state parameters, three game parameters and two spatial parameters affecting viruses spread are studied, respectively. A series of simulation experiments show that an excellent performance of STSIR in viruses spread, which contributes to further studies of virus spread in the SIoT.

The rest of this paper is organized as follows. In Section 2, we review the work on virus spread models and present issues to be addressed regarding a practical situation of virus spread in an SIoT. In Section 3, we describe the state transfer process and the game process of the infection and recovery rates in detail when viruses spread around, and work out a mixed Nash equilibrium solution through the payoff matrix of an individual-group game. In Section 4, we obtain differential equations of STSIR, mathematically obtain two equilibrium points of the model STSIR and prove their stability. In Section 5, We analyze an application framework and present a calculation algorithm of the model STSIR. In Section 6, we conduct lots of simulation experiments on STSIR, and analyze the effects of eight parameters, including initial states, game parameters, distribution density and social distance, on viruses spread, which all prove clear validity of the model. Finally, we summarize the whole paper.

To clearly examine symbols and parameters covered in this paper, we list them in Table 1.

Table 1

Symbols and parameters covered in this article.

Symbol	Explanation
N	Total number of SIoT nodes
σ	Average distribution density of SIoT nodes
R_c	Social radius of SIoT nodes (Spread radius of infected SIoT nodes)
$S(t)$	Proportion of SIoT nodes in state S at time t
$I(t)$	Proportion of SIoT nodes in state I at time t
$R(t)$	Proportion of SIoT nodes in state R at time t
$I(t)^*$	Number of infected SIoT nodes capable of infecting susceptible SIoT nodes in the SIoT at time t
$r(t)$	Distribution radius of infected SIoT nodes in the SIoT at time t
θ	Birth rate of SIoT nodes
ψ	Conversion rate of SIoT nodes from state R to state S
ω	Death rate of SIoT nodes
β	Infection rate of SIoT nodes in state I
γ	Recovery rate of SIoT nodes from state I to state R
η	Number of nodes that an infected SIoT node can infect
m	Average number of susceptible SIoT nodes infected by a virus
a	Rewards obtained by susceptible SIoT nodes calling IDS to detect and kill viruses successfully
ma	Loss caused by failure of infected SIoT nodes spreading virus
b	Cost of susceptible SIoT nodes calling IDS to detect and kill virus
c	Loss of susceptible SIoT nodes caused by virus infection
mc	Rewards of infected SIoT nodes spreading virus successfully
d	Energy cost of receiving normal information
e	Cost of energy consumed by infected SIoT nodes in sending virus or normal information
x	Probability of infected SIoT nodes sending virus
y	Probability of susceptible SIoT nodes calling IDS to detect and kill virus

R_0	Basic reproduction number
P^i	The i-th equilibrium of SIoT's model STSIR
$J(P^i)$	Jacobi matrix of the i-th equilibrium point of SIoT's model STSIR
P^*	Arbitrary equilibrium of SIoT's model STSIR
$J(P^*)$	Jacobi matrix of any equilibrium point of SIoT's model STSIR
λ_i	The i-th eigenvalue of the matrix
I	Identity matrix

2 Related work

At present, studies of virus spread in an SIoT, which pay close attention to online social networks (OSNs) (Alemany et al., 2023), wireless sensor networks (WSNs) (Álvarez et al., 2023), and complex networks, are still in a preliminary stage. In addition, some studies have introduced game theory to disclose the mechanism of virus spread. In an SIoT, some researchers first noticed that enormous impact of social attributes in IoT cannot be ignored (An et al., 2013; Radanliev et al., 2020; Ahmed et al., 2018). Then, Yi et al. (2021) proposed a cloud edge auxiliary information diffusion model in an SIoT by taking advantage of the advantages of timely processing and feedback of cloud edge computing technology (Alamouti et al., 2022). Al Kindi et al. (2019) developed a simulator to simulate malware spread in an SIoT and found that adding more relationships or increasing the number of owned objects per user has increased the malware spreading rate. Jiang et al. (2016) measured the correlation between the global spreading influence and the local connections of users in OSNs through the two measurement criteria of degree and assortativity, making contributions to the research on the influence ability of nodes. In order to accurately identify offensive and defensive sides in multiple social networks, Qu et al. (2018) proposed a weighted Friendship learning-Based Identification (FBI) method by considering personal profile, network structure and historical friends in the network, and used machine learning algorithms to optimize the weights. Meanwhile, in terms of anomaly identification in IoTs, Cui et al. (2022) proposed a blockchain-empowered decentralized and asynchronous federated learning (FL) (Nguyen et al., 2023; Qu et al., 2023) framework to improve the efficiency of anomaly identification in the Internet of Things. In addition, other models of SIoTs such as trust models are discussed in (Cai, et al., 2022) and (Magdich et al., 2022).

In the studies of curbing the spread of viruses in social networks, tree and graph theory (Zhang and Zhu, 2018; Peng et al., 2019) are introduced in part of them to represent the spread relationships affected by users' social interactions. From the perspective of spread purpose, Zhou et al. (2021) also proposed an advanced persistent threat (APT) (Chen et al., 2023) model with a specific target to improve a hit ratio by sacrificing spread speed. Lin et al. (2021) proposed a dynamic model of fraud threat diffusion in social networks that analyzed its diffusion trends and stability, which could accelerate and suppress the spread of fraud threats. Methods for identifying and reducing the spread of misinformation in social networks are reviewed and classified by (Zareie and Sakellariou, 2021).

Researches on virus spread in WSN is approaching maturity. Shen et al. (2014) proposed differential game (Li and Hu, 2022) based strategies to control the spread of malware at the lowest cost. Zhang et al. (2020) considering that WSNs are prone to loss of data confidentiality, proposed a model called Malware Diffusion Based on Cellular Automaton (MDBCA) that was more suitable for WSN than Markov chain (Kirkby, 2023). Shen et al. (2019) proposed the HSIRD model based on epidemiology to describe the spread dynamics of malware in heterogeneous WSNs, where dynamic differential equations and equilibrium points were obtained, and the stability of equilibrium points were proved. For special unattended WSN, Bahi et al. (2014) and Aliberti et al. (2017) improved an epidemic model to simulate data survivability under attacks.

In terms of virus spread issues in complex networks, a large amount of spread models on arbitrarily weighted, directed, and heterogeneous complex networks (Hu et al., 2018), networks with special carrier devices (Hernández Guillén and

Martín Del Rey, 2018), multiplex networks (Zhao et al., 2019), cloud environment (Abazari et al., 2016) and other networks have been mentioned in previous work in detail. Under Software Defined Networks (SDN) (Xing et al., 2022) emerging in 5G networks (Lefoane et al., 2023), Guan et al. (2018) designed a placement strategy of Network Security Functions (NSFs) (Jiang et al., 2021) with antivirus and devices. As advanced malware attacks on random complex networks, Martín Del Rey et al. (2021) introduced a new model of advanced malware simulated by cellular automata. In addition, massive novel technologies such as machine learning (Gibert et al., 2020; Han et al., 2019; AL-Hawawreh et al., 2018) are being used to contain the spread of viruses in complex networks.

Using game theory as a basis for simulating the real spread dynamics for computer viruses in an SIoT is a viable approach demonstrated in previous studies. The wide applicability of this approach is proofed by a number of related papers that use different games not only for anti-jamming data spread (Liu et al., 2018; Wang et al., 2018; Liu et al., 2022) and preventing privacy leakage (Shen et al., 2018), but also do a good job of containing viruses spread. Jakóbik et al. (2018) built a model based on a general Security Stackelberg games (SSGs) (Bucarey et al., 2021) scenario in cloud environment that enables the automatic selection of provider-level security decisions. Zhou et al. (2020) established an attack-defense game model to analyze a microscopic mechanism of malware spread, and worked out the mixed Nash equilibrium solution of the game model. According to the mixed Nash equilibrium strategy of both sides of the game, the infection probability of malware is determined, and a virus spread model based on game theory is proposed (Li and Li, 2020; Sheryl et al., 2020). The introduction of game theory vividly described an attack and defense process among malware (Razak et al., 2016; Xiao et al., 2017), DDoS attacks (Liu et al., 2021) and normal device nodes invoking defense means such as IDS, which improved the reliability of network services (Nosouhi et al., 2021; Liu et al., 2015; Shen et al., 2022) and data security (Liu et al., 2018).

Table 2

Comparisons of representative related works on spread models in SIoTs.

Paper	States	Advantages	Weaknesses	Key contributions
(Yi, et al., 2021)	SIR	general model; edge computing	none of special characteristics of SIoTs	blockchain-based cloud-edge SIoT architecture
(Zareie and Sakellariou, 2021)	-	survey	none of special characteristics of SIoTs	Social networks; misinformation spread minimization
(Al Kindi, et al., 2019)	SIR	general model; dynamic social relationship	none of special characteristics of SIoTs	a simulator; establishing dynamic social relationship
(Peng, et al., 2019)	SIR	general model; influence spreading tree	none of special characteristics of SIoTs	social interaction graph based on big data sets
(Zhang and Zhu, 2018)	SIR	general model; user relationship graph	none of special characteristics of SIoTs	user relationship graph; partition areas
(Lin, et al., 2021)	SWIR	general model	none of special characteristics of SIoTs	fraud information; optimal control
(Zhang, et al., 2020)	SEIRD	general model	none of special characteristics of SIoTs	WSNs; malware diffusion based on cellular automaton
(Shen, et al., 2019)	SIRD	general model	none of special characteristics of SIoTs	heterogeneous WSNs; diffusion model
(Hu, et al., 2018)	SIS	general model	none of special characteristics of SIoTs	heterogeneous complex networks; optimal weight adaptation
(Hernández Guillén and Martín Del Rey, 2018)	SICR	general model	none of special characteristics of SIoTs	carrier devices; compartmental model
(Zhao, et al., 2019)	US-UI-PV-DV	general model	none of special characteristics of SIoTs	patch distribution; multiplex networks
(Martín Del Rey, et al., 2021)	SIAR	general model	none of special characteristics of SIoTs	complex random networks; cellular automaton
(Zhou, et al., 2020)	SISD	general model	none of special characteristics of SIoTs	attack–defense game model; steady-state infection ratio
(Li and Li, 2020)	SIS	general model	none of special characteristics of SIoTs	evolutionary game theory; vaccination

(Liu, et al., 2021)	s^I-s^e-s	general model;	none of special characteristics of SIoTs	denial-of-service (DDoS) attacks; bayesian game; Q-learning algorithm
this paper	SIR(D)	infectivity decays with social distance; dynamic changes of user traffic	special model for SIoTs	individual-group game-based model; virus spread dynamics in SIoTs

However, aforementioned studies either didn't consider the characteristics of an SIoT network, or the given models were dependent on historical experience of the spread parameters, which were not suitable to describe the dynamics of virus spread in the SIoT and could not provide guidance for effectively containing the spread of viruses in the SIoT. In summary, previous studies still have not addressed three issues of virus spread in the SIoT. The first problem is how to quantify the impact of social relationship, user birth and death, device updates and obsolescence on the spread of viruses in an SIoT. The second problem is how to solve dependence of the infection and recovery rates on historical experience in a virus spread model. The third question is how to determine a threshold that represents whether viruses will diffuse or die out in the SIoT. In this paper, we solve the first problem by defining the social distance R_c, birth rate θ and death rate ω of network nodes. The second problem is solved by using individual-group game theory to describe an attack and defense process among infected SIoT nodes and susceptible ones, and the infection and recovery rates of the model are obtained automatically. Finally, in order to solve the third problem, we investigate two equilibrium points of the model STSIR and verify correctness of the conclusion from a mathematical perspective. Table 2 compares representative related works that have explored virus spread for SIoTs, in order to quickly clarify the existing works and show the value of this paper.

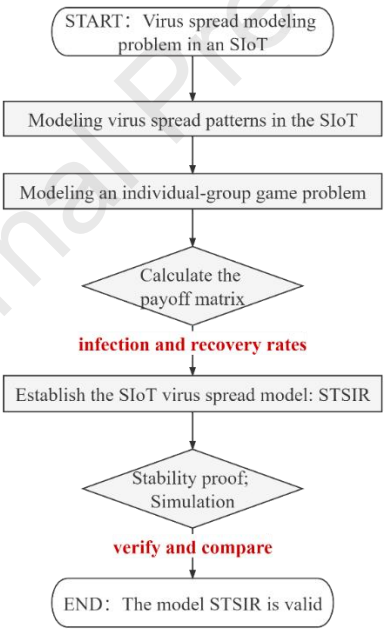


Fig. 1. Flow diagram of the entire approach proposed.

In order to evaluate the effectiveness of the existing models and the proposed model in preventing the spread of viruses more normatively, three evaluation criteria are introduced in this paper: 1) accuracy of the model stability conditions; 2) degree to which the model quantifies the unique characteristics of the SIoT networks; and 3) virus spreading scale and time cost in the process of reaching equilibrium in the SIoT. In general, one of the important ways to evaluate the reliability of a new model is to observe whether the actual stability conditions of the model are consistent with the theoretical conditions, which is the first criterion satisfied by all the existing models and the proposed model STSIR. More important is the second criterion whether a model takes into account characteristics of an SIoT network, such as the limited spread radius of SIoT nodes defined as the SIoT social distance, and the dynamic user traffic change of the network. However, the above studies

fail to consider the two characteristics of the SIoT networks. Therefore, this paper quantifies and integrates them well in the process of proposing the model STSIR. The last criterion is presented to evaluate the effect of the model on containing the spread of the virus in an SIoT. In fact, the ultimate purposes of all studies on virus spread models are to explore how to reduce the maximum spread scale of viruses and compress the time from the beginning of the epidemic to the stabilization, which are proposed as two completeness indicators. The model STSIR proposed in this paper is compared with the existing models SIS and SIR, and it is found that the model STSIR performs ~45% better than the model SIS in terms of virus spreading scale. At the same time, the model STSIR saves ~66.7% of the time cost of reaching stability than the model SIR. Obviously, the model STSIR performs well both in reducing the proportion of infected nodes and in time cost, fully satisfying the third criterion. To clearly understand our methods, we illustrate the entire approach proposed in this paper as shown in Fig. 1.

3 Mechanism of virus spread in the SIoT

3.1 Virus spread patterns in the SIoT

The spread of viruses in an SIoT is a complex process that considers not only viruses spread, but also virus detection and antivirus operations that can restore infected SIoT nodes to recovered ones. It is worth noting that one of the breakthrough characteristics of an SIoT is to build corresponding virtual objects who interact each other based on social relations. Therefore, we define social distance R_c to quantify the impact of social relations on the spread of viruses in an SIoT.

***Definition 1*:** Social distance of an SIoT is represented by character R_c, whose unit is an entity such as a person or an object.

Definition 1 is our specific definition of social distance in an SIoT. Moreover, Small World Theory (Ke, 2010) suggests that each person can contact anyone in the world with up to six people. Therefore, in this paper, the social distance $R_c = 6$ is defined as the social distance that an SIoT node spreads to the whole network at a standard speed. The smaller the R_c, the simpler the social relationship of the person or object in the real world, and the slower the viruses will spread to the whole network. On the contrary, the larger the R_c, the more complex the social relationship of the person or object in the real world, and the faster the viruses will spread to the whole network.

We suppose that there are N nodes in an SIoT, which are randomly and statically distributed in a region. The distribution density of nodes is σ, and each node communicates with neighbor nodes according to its social distance R_c. Initially, only individual SIoT nodes in the center of the region became infected, and then viruses spread to neighbor nodes by sending information. The infected SIoT nodes can send messages with or without viruses, so that neighbor nodes need to decide whether to detect and eliminate possible viruses after receiving a message. In this process, each node chooses its own action. This paper focuses on the case where the basic devices call remote IDS for virus detection and elimination since multitudinous devices such as sensors and digital cameras in an SIoT are simple, basic single-function devices without local antivirus services. Generally, one of the markers of infected SIoT nodes is whether the device contains virus code fragments (Rabbani et al., 2020), and whether the node is under virus attack is judged by whether the received information contains virus code fragments. In addition, IDS technology can also identify viruses from the perspective of virus behavior (Gibert, et al., 2020; De La Torre Parra et al., 2020), which is based on whether the request is an illegal authorization request that will damage the device system, loss data and do other harmful things. In STSIR, we detect and eliminate viruses by calling IDS on messages received by the SIoT devices. If the messages contain virus code snippets, we consider the attack as a virus attack, and the node can choose to eliminate or not to eliminate it, which determines whether it was a

recovery SIoT node or a virus node.

Fig. 2 shows that spread of viruses in the SIoT at time t, where black square blocks represent infected SIoT nodes that are not infectious, white squares represent nodes that are recovered or cannot be infected due to lack of energy, black dots represent infected SIoT nodes, and white dots represent susceptible SIoT nodes. From Fig. 3, infected SIoT nodes in the inner ring will further infect susceptible SIoT nodes outside the ring at the next time $t+1$.

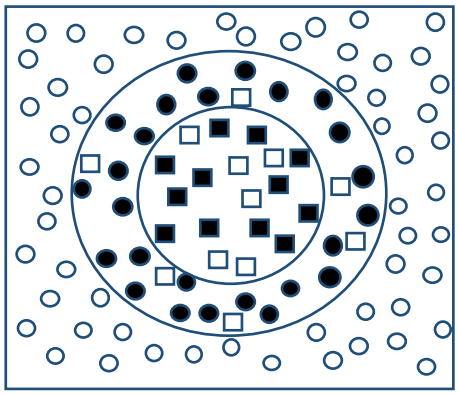


Fig. 2. Virus spread at time t.

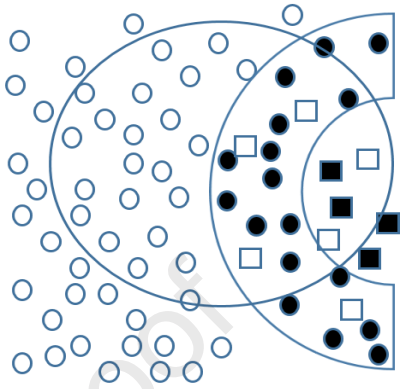


Fig. 3. Virus spread at time $t+1$.

At time t, let $S(t)$ be the number of susceptible SIoT nodes outside the ring that can be infected. Since infected SIoT nodes can only infect susceptible SIoT nodes within the surrounding radius circle R_c, susceptible SIoT nodes are contained within a ring which is distance R_c from the outer edge of the ring in Fig. 3. The number of infected SIoT nodes in the ring is set to $I(t)$, which represents the number of black dots in the ring in Fig. 3, while the number of white squares in the ring is $R(t)$ detected by IDS and sterilized.

At time 0, infected SIoT nodes at the center begin to spread around, and they're going to be distributed in a circle of radius $R(t)$ at time t. Then the number of infected SIoT nodes in the circle is

$$I(t) = \sigma\pi r(t)^2 - R(t). \tag{1}$$

Due to a limited social distance, infected SIoT nodes in the dotted circle can no longer affect susceptible SIoT nodes, and only infected SIoT nodes in the ring outside have the ability to infect. Therefore, the number of infected SIoT nodes in the ring can be calculated as

$$I(t)^* = I(t) - \sigma\pi(r(t) - R_c)^2 - R(t)^*, \tag{2}$$

where $R(t)^*$ is the number of recovered nodes in the ring. Further $R(t)^* = \gamma I(t)^* - \psi R(t)^* - \omega R(t)^*$ where γ is the recovery rate of infected SIoT nodes. Considering $\gamma \gg \psi, \omega$, and it is obvious that $r(t) >> R_c$, so formula (2) can be simplified as

$$I(t)^* = 2\sigma\pi r(t) R_c - \gamma I(t)^*. \tag{3}$$

By combining formulas (1) and (3), we can obtain

$$I(t)^* = \frac{2R_c\sqrt{\sigma\pi\big(I(t) + R(t)\big)}}{(1+\gamma)}. \tag{4}$$

The number η of nodes that an infected SIoT node can infect is

$$\eta = \sigma\pi {R_c}^2. \tag{5}$$

In these η susceptible SIoT nodes, some ones will not be re-infected because IDS was called before. Therefore, we need to multiply η by the density of susceptible SIoT nodes when we want to calculate the total number of nodes that a virus can infect, and finally we can get an average number of susceptible SIoT nodes infected by a virus is

$$m = \frac{S(t)}{N}\eta. \tag{6}$$

3.2 Game model of virus spread in an SIoT

3.2.1 Individual-group game

In an SIoT, viruses spread is a process of spreading outward from central infected SIoT nodes. The infected SIoT nodes will gain benefits when spreading viruses, otherwise, failure to spread viruses will cause a certain loss due to increased exposure of the infected SIoT nodes. On the other hand, in order to prevent viruses from invading the network, susceptible SIoT nodes around the infected SIoT nodes can call IDS installed in a base station for detection according to a certain probability when receiving information. If viruses are detected, an antivirus function is enabled to check and kill viruses. The susceptible SIoT nodes need to spend a certain cost when calling IDS, and will gain a certain benefit when viruses is successfully removed. Obviously, the process of virus spread, detection and killing is an adversarial game, and there is no possibility of cooperation between viruses and IDS, so that we can choose a non-cooperative game model. Fig. 3 shows the specific process of viruses, the viruses in the ring spread out of the ring, and each virus will spread to multiple susceptible SIoT nodes outside the ring, which can be defined as an individual-group game (Ariful et al., 2020).

***Definition 2*:** The individual-group game in an SIoT with viruses spread is a 4-tuple $\{P, S, \theta, U\}$, where

- P ={susceptible SIoT nodes s, infected SIoT nodes i } is a set of players.
- $S = S_s \times S_i$ where S_s ={*call*, *not call*} is the strategy set of player s, and S_i ={*send*, *not send*} is the strategy set of player i.
- $\theta = \theta_t(S_s) \times \theta_t(S_i)$, where $\theta_t(S_s)$ is the proportion vector of player s adopting pure strategy S_s at time t in the whole population, and $\theta_t(S_i)$ is the proportion vector of player i adopting pure strategy S_i at time t in the whole population.
- U is the payoff matrix, and the value of each player is shown in Table 3.

Table 3

Game payoff matrix for a susceptible SIoT node and an infected SIoT node.

virus \ IDS		susceptible SIoT nodes	
		call	*call*
Infected SIoT nodes	*send*	$-ma-e, a-b-d$	$mc-e, -c-d$
	not send	$-e, -b-d$	$-e, -d$

In this paper, an individual-group game model is similar to the Stackelberg model is adopted. The process of virus spread in an SIoT is a game between an infected SIoT node and several susceptible SIoT nodes. Virus designers are familiar with sending and receiving characteristics of each node in the SIoT. Before viruses spread, susceptible SIoT nodes have already carried out a potential evolutionary game, which makes viruses tend to be stable in the way of policy selection and need to pay a price to change this state. Next, the infected SIoT node selects its own response strategy based on the strategy adopted by susceptible SIoT nodes in the SIoT. Thus, the game process is divided into two stages.

In the first stage, the behavior of susceptible SIoT nodes can be described by a replicator dynamic model in evolutionary game. The policy of a susceptible SIoT node is "call IDS" or "not call IDS". According to evolutionary game theory, due to the cost of changing strategies, most participants in susceptible SIoT nodes will keep some pure strategies unchanged, and only a few participants will adopt strategies with higher returns based on imitation behavior. The pure policy space of susceptible SIoT nodes is $S_s(s_1, s_2)$, where s_1 is "call IDS" and s_2 is "do not call IDS". Let $\theta_t(S_s)$ be a proportion vector of nodes in the whole group that adopt the pure strategy $s_i(i = 1, 2)$ in the t stage. Suppose $\theta_t(s_1) = y(0 \le y \le 1)$, then $\theta_t(s_2) = 1 - y$. In the second stage, the policy of an infected SIoT node (individual participant) is "send virus" or "not send

virus", where pure policy space is $S_i(s_1', s_2')$. The infected SIoT node determines its own response function $U_t(S_i) = \sum_s \theta_t(S_s)u(S_i, S_s)$ according to proportional distribution $\theta_t(S_i)$ of different strategies $s_i(i = 1, 2)$ adopted by the susceptible SIoT nodes, which is an expected revenue of the infected SIoT node.

3.2.2 Analyses of the game payoff function

The process of virus spread in an SIoT can be regarded as an attack and defense process between infected SIoT nodes and susceptible SIoT nodes. Table 3 shows a game payoff matrix of attack and defense between infected SIoT nodes and susceptible SIoT nodes. When an infected SIoT node sends a message to another node, it will consume energy at cost e. When a susceptible SIoT node receives information, it is necessary to determine whether to call IDS residing in a base station for detection. If detection is called, energy at cost b is consumed, while energy at cost d is consumed to receive information when a susceptible SIoT node doesn't call IDS. When an infected SIoT node attacks a susceptible SIoT node and the susceptible SIoT node calls IDS, the susceptible SIoT node will gain a reward a for successfully detecting viruses. Since the attack process is a game between an infected SIoT node and m susceptible SIoT nodes, the infected SIoT node will lose ma due to failure of attacks. Similarly, when an infected SIoT node launches attacks and susceptible SIoT nodes don't call IDS, the infected SIoT node will gain reward mc for successfully spreading viruses. In this case, each susceptible SIoT node will be infected by viruses, resulting in a loss c.

3.2.3 Analyses of the game equilibrium

From Table 3, we can see that $a - b > 0$ always true, otherwise IDS will not be called, so $a - b - d > -c - d$ is satisfied. Therefore, a susceptible SIoT node will call IDS if an infected SIoT node sends viruses. Conversely, if an infected SIoT node does not send viruses, we can see from benefits that a susceptible SIoT node will not call IDS. Similarly, an infected SIoT node will not send viruses if a susceptible SIoT node calls IDS. Conversely, an infected SIoT node will send viruses if a susceptible SIoT node does not call IDS. We can see that there is no pure strategy equilibrium solution in the game, but only a mixed strategy equilibrium solution.

The reaction function in the second stage of the game is also an expected revenue function of an infected SIoT node. Then we can calculate the expected revenue of an infected SIoT node. Since the probability of an infected SIoT node sending viruses is x while the probability of not sending viruses is $1 - x$, and the probability of a susceptible SIoT node calling IDS is y while the probability of not calling IDS is $1 - y$. Thus, the expected revenue of an infected SIoT node can be expressed as

$$E_v = xy(-ma - e) + x(1 - y)(mc - e) + (1 - x)y(-e) + (1 - y)(1 - x)(-e). \quad (7)$$

In formula (7), m, a, e, c etc. are all constants at time t.

Simplify (7), we can obtain

$$E_v = -xyma + xmc - xymc - e. \quad (8)$$

We can also get the expected revenue of susceptible SIoT nodes as

$$E_s = xy(a - b - d) + x(1 - y)(-c - d) + (1 - x)y(-b - d) + (1 - x)(1 - y)(-d). \quad (9)$$

Simplify (9), we can obtain

$$E_s = xya - xc + xyc - by - d. \quad (10)$$

According to the definition of equilibrium solution, where an expected revenue of each party reaches maximum value, an extreme value method can be used to find the strategy when E_v and E_s reach their maximum values. For this reason, the partial derivative of x can be obtained for E_v, and then set to 0, so that x can be obtained to maximize E_v. We thus obtain

$$\frac{\partial E_v}{\partial x} = -yma + mc - ymc = 0,$$

and achieve

$$y^* = c/(a + c). \tag{11}$$

Similarly, we find the partial derivative of y for E_S and set it to 0 as

$$\frac{\partial E_s}{\partial y} = xa + xc - b = 0,$$

and achieve

$$x^* = b/(a + c). \tag{12}$$

Therefore, (x^*, y^*) is a mixed equilibrium solution of the game. According to semantics of game equilibrium solution, $x^* \times y^*$ is a probability that an infected SIoT node sends viruses and a susceptible SIoT node calls IDS, which indicates that the susceptible SIoT node is infected with viruses, but viruses are detected and killed by calling IDS, and then the susceptible SIoT node become a recovered one. So, this probability is also called the recovery rate γ, which can be obtained by formulas (11) and (12) as

$$\gamma = bc/(a + c)^2. \tag{13}$$

And $x^* \times (1 - y^*)$ is a probability that an infected SIoT node sends viruses, but a susceptible SIoT node does not call IDS, indicating that the susceptible SIoT node is successfully infected. Therefore, the probability is also called the infection rate β, which can be obtained by formulas (11) and (12) as

$$\beta = ab/(a + c)^2. \tag{14}$$

4 SIoT virus spread model and dynamics analyses

4.1 SIoT virus spread model

Kermack and McKendrick established an epidemic warehouse model in 1927 with a dynamic method, including basic models SI, SIS and SIR. This paper uses SIR for research, which divides nodes into three states: susceptible $S(t)$, infective $I(t)$, and recovered $R(t)$. The ratio of the number of susceptible SIoT nodes infected by an infected SIoT node to the total number of susceptible persons per unit time is the infectivity rate. The recovery rate is the ratio of the number of infected SIoT nodes converted to recovery SIoT nodes to the total number of infected SIoT nodes in unit time (Ariful and Jun, 2020; Shakya, et al., 2019).

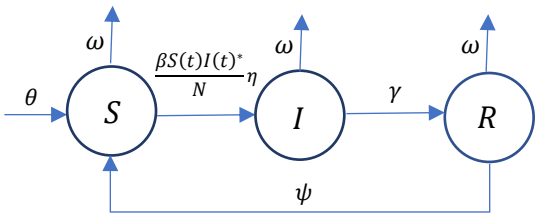


Fig. 4. State transition in STSIR.

Fig. 4 shows the state transition process during viruses spread in the model STSIR. Considering the infection rate β automatically calculated through the individual-group game, which represents a probability that an infected SIoT node sends message with viruses to many susceptible SIoT nodes within a radius of R_c in the case of attack-defense, we determine that susceptible SIoT nodes within this range are infected when they don't call IDS with a probability of $1 - \gamma$. In addition, the birth, death, and iteration of the user social networks in the SIoT, as well as production, maintenance, and obsolescence of devices, are the reasons why the birth rate θ and death rate ω are added to STSIR. Thus, the differential

system dynamics equations of STSIR can be obtained as

$$\begin{cases} \frac{\partial S(t)}{\partial t} = \theta + \psi R(t) - \frac{2ab\sigma\pi {R_c}^3 S(t)}{N} \times \frac{\sqrt{\sigma\pi\left(I(t)+R(t)\right)}}{(a+c)^2+bc} - \omega S(t) \\ \frac{\partial I(t)}{\partial t} = \frac{2ab\sigma\pi {R_c}^3 S(t)}{N} \times \frac{\sqrt{\sigma\pi\left(I(t)+R(t)\right)}}{(a+c)^2+bc} - \frac{bcI(t)}{(a+c)^2} - \omega I(t) \\ \frac{\partial R(t)}{\partial t} = \frac{bcI(t)}{(a+c)^2} - \psi R(t) - \omega R(t) \end{cases} \tag{15}$$

4.2 Equilibrium points and basic reproduction number of the model STSIR

In order to study whether a system is stable or not, we need to analyze stability of differential equations of the system. It is possible for a system to reach equilibrium when one or more equilibrium points exist. In addition, finding equilibrium points of the model can quickly help us determine a threshold at which viruses spread or die during the spread cycle. Therefore, using a mathematical method to calculate equilibrium points of the model STSIR is of a great significance to study the spread rules of viruses and discover countermeasures in an SIoT.

Theorem 1. The model STSIR of formula (15) has two equilibrium points.

Proof. Obviously, with continuous passage of time t, the number of susceptible SIoT nodes $S(t)$, infected SIoT nodes $I(t)$ and recovery SIoT nodes $R(t)$ present continuous curve form. According to the Existence Theorem of Zero in the field of mathematics, for a continuous function $f(x)$, there is zero when $f(x) = 0$. Therefore, we learn that equilibrium points of the model STSIR can exist only when $\frac{\partial S(t)}{\partial t} = 0$, $\frac{\partial I(t)}{\partial t} = 0$, and $\frac{\partial R(t)}{\partial t} = 0$.

Let $\frac{\partial S(t)}{\partial t} = 0$, $\frac{\partial I(t)}{\partial t} = 0$, and $\frac{\partial R(t)}{\partial t} = 0$ in formula (15), the malware-free equilibrium point $P^0(S^0, I^0, R^0)$ is calculated as

$$P^0(S^0, I^0, R^0) = (\frac{\theta}{\omega}, 0, 0). \tag{16}$$

Another endemic equilibrium point $P^1(S^1, I^1, R^1)$ of network can be obtained by formula (15) as

$$P^1(S^1, I^1, R^1) = \left(\frac{N[bc + \omega(a+c)^2]}{2ab\sigma\pi {R_c}^3 (a+c)^2}, I^1, \frac{bc}{(a+c)^2(\psi+\omega)} I^1 \right), \tag{17}$$

where

$$I^1 = \frac{[2\theta ab\sigma\pi {R_c}^3 (a+c)^2 - \omega N[bc + \omega(a+c)^2]](\psi+\omega)}{2ab\sigma\pi {R_c}^3 \omega[bc + (a+c)^2(\psi+\omega)]}. \tag{18}$$

Thus, Theorem 1 is proved.

We use the next-generation matrix method to calculate the basic reproduction number R_0 (Fisman et al., 2020), which indicates whether viruses can spread. Mathematically, $R_0 = \rho(FV^{-1})$ is the spectral radius of the next-generation matrix, where F represents the appearance rate matrix of the new viruses in an SIoT, and V^{-1} represents the inverse matrix of the transfer rate matrix between any states. We calculate that

$$F = \frac{2\theta ab\sigma\pi {R_c}^3}{\omega N}, \tag{19}$$

$$V = r + \omega. \tag{20}$$

Finally, we get the basic reproduction number R_0 as

$$R_0 = \rho(FV^{-1}) = \frac{2\theta ab\sigma\pi {R_c}^3 (a+c)^2}{\omega N[bc + \omega(a+c)^2]} \tag{21}$$

The basic reproduction number is an important index to describe an infectivity of initial viruses in an average disease

period. When $R_0 \le 1$, the infectivity of infected SIoT nodes is weak, and viruses will eventually die out over time, that is $I(t) = 0$. At this point, only the malware-free equilibrium P^0 exists. When $R_0 > 1$, the infected SIoT node will continue to exist in the SIoT, and achieve mutual restriction and balance with susceptible SIoT nodes and recovered nodes. At this point, only the endemic equilibrium P^1 exists.

4.3 Stability analysis of equilibrium point of the model STSIR

If equilibrium points of the model STSIR are stable, the state near equilibrium states will keep approaching to the latter until the whole system stays in a relatively stable state for a relatively long time. The state is each of both equilibrium points, and behavior of nearby states that keep tightening one equilibrium state reflects the stability of equilibrium points.

Theorem 2. When $R_0 \le 1$, the malware-free equilibrium $P^0(S^0, I^0, R^0)$ is locally asymptotically stable.

Proof. It is proved that since $N = S(t) + I(t) + R(t) + \theta$, formula (15) can be rewritten as

$$\begin{cases} \dfrac{\partial S(t)}{\partial t} = \theta + \psi R(t) - \dfrac{2ab\sigma\pi {R_c}^3 S(t)}{N} \times \dfrac{\sqrt{\sigma\pi(N - S(t) - \theta)}}{(a+c)^2 + bc} - \omega S(t) \\ \dfrac{\partial I(t)}{\partial t} = \dfrac{2ab\sigma\pi {R_c}^3 S(t)}{N} \times \dfrac{\sqrt{\sigma\pi(N - S(t) - \theta)}}{(a+c)^2 + bc} - \dfrac{bcI(t)}{(a+c)^2} - \omega I(t) \\ \dfrac{\partial R(t)}{\partial t} = \dfrac{bcI(t)}{(a+c)^2} - \psi R(t) - \omega R(t) \end{cases} \tag{22}$$

Let any equilibrium point be P^*, and the Jacobi matrix $J(P^*)$ of P^* can be obtained according to formula (15) as

$$J(P^*) = \begin{bmatrix} -\dfrac{2ab\sigma^{\frac{3}{2}}\pi^{\frac{3}{2}}{R_c}^3}{N[(a+c)^2 + bc]}\left[\sqrt{N - S(t) - \theta} - \dfrac{S(t)}{2\sqrt{N - S(t) - \theta}}\right] - \omega & 0 & \psi \\ \dfrac{2ab\sigma^{\frac{3}{2}}\pi^{\frac{3}{2}}{R_c}^3}{N[(a+c)^2 + bc]}\left[\sqrt{N - S(t) - \theta} - \dfrac{S(t)}{2\sqrt{N - S(t) - \theta}}\right] & -\dfrac{bc}{(a+c)^2} - \omega & 0 \\ 0 & \dfrac{bc}{(a+c)^2} & -\psi - \omega \end{bmatrix}. \tag{23}$$

The Jacobi matrix $J(P^0)$ corresponding to the equilibrium point P^0 is

$$J(P^0) = \begin{bmatrix} -\dfrac{2ab\sigma^{\frac{3}{2}}\pi^{\frac{3}{2}}{R_c}^3}{N[(a+c)^2 + bc]}\left[\sqrt{N - \dfrac{\theta}{\omega} - \theta} - \dfrac{\theta}{2\omega\sqrt{N - S(t) - \theta}}\right] - \omega & 0 & \psi \\ \dfrac{2ab\sigma^{\frac{3}{2}}\pi^{\frac{3}{2}}{R_c}^3}{N[(a+c)^2 + bc]}\left[\sqrt{N - \dfrac{\theta}{\omega} - \theta} - \dfrac{\theta}{2\omega\sqrt{N - S(t) - \theta}}\right] & -\dfrac{bc}{(a+c)^2} - \omega & 0 \\ 0 & \dfrac{bc}{(a+c)^2} & -\psi - \omega \end{bmatrix}. \tag{24}$$

Let $A = \frac{2ab\sigma^{\frac{3}{2}}\pi^{\frac{3}{2}}{R_c}^3}{N[(a+c)^2+bc]}\left[\sqrt{N - \frac{\theta}{\omega} - \theta} - \frac{\theta}{2\omega\sqrt{N-S(t)-\theta}}\right]$ and $B = \frac{bc}{(a+c)^2}$. After simplification and transformation, formula (24) can be written as

$$J(P^0) = \begin{bmatrix} -A - \omega & 0 & \psi \\ 0 & -B - \omega & \dfrac{\psi A}{A + \omega} \\ 0 & B & -\psi - \omega \end{bmatrix}. \tag{25}$$

I is introduced to represent the identity matrix, and λ is the eigenvalue of the matrix $J(P^0)$. The eigenmatrix of $J(P^0)$ is

$$|\lambda I - J(P^0)| = \begin{vmatrix} \lambda + A + \omega & 0 & -\psi \\ 0 & \lambda + B + \omega & -\frac{\psi A}{A+\omega} \\ 0 & -B & \lambda + \psi + \omega \end{vmatrix}. \tag{26}$$

Formula (24) is computed to obtain the three eigenvalues of $J(P^0)$, where $\lambda_1 = -(A+\omega) < 0, \lambda_2 + \lambda_3 = -(B+2\omega+\psi) < 0$, and $\lambda_2\lambda_3 = (B+\omega)(\omega+\psi) - \frac{\psi AB}{A+\omega} > 0$. Therefore, the eigenvalues $\lambda_2, \lambda_3 < 0$ are all negative values. In this manner, the model STSIR is locally asymptotically stable at equilibrium $P^0(S^0, I^0, R^0)$ if $R_0 \leq 1$, while the equilibrium $P^0(S^0, I^0, R^0)$ is unstable if $R_0 > 1$. This completes the proof.

Theorem 2 shows that when average infection ability of infected SIoT nodes is weaker than defense and recovery ability of an SIoT, infected SIoT nodes will appear and spread over a period of time and then disappear completely, and recovered nodes will be transformed into susceptible SIoT nodes or natural extinction. At this point, only susceptible SIoT nodes exist in the SIoT.

Theorem 3. When $R_0 > 1$, the endemic equilibrium $P^1(S^1, I^1, R^1)$ is locally asymptotically stable.

Proof. According to formula (15), the Jacobi matrix $J(P^*)$ with any equilibrium point of P^* can be written as

$$J(P^*) = \begin{bmatrix} -2\tau\sqrt{I(t)+R(t)} - \omega & -\frac{\tau S(t)}{\sqrt{I(t)+R(t)}} & -\frac{\tau S(t)}{\sqrt{I(t)+R(t)}} + \psi \\ 2\tau\sqrt{I(t)+R(t)} & \frac{\tau S(t)}{\sqrt{I(t)+R(t)}} - \frac{bc}{(a+c)^2} - \omega & \frac{\tau S(t)}{\sqrt{I(t)+R(t)}} \\ 0 & \frac{bc}{(a+c)^2} & -\psi - \omega \end{bmatrix} \tag{27}$$

where $\tau = \frac{ab\sigma^{\frac{3}{2}}\pi^{\frac{3}{2}}{R_c}^3}{N[(a+c)^2+bc]}$. Let $X = \frac{bc}{(a+c)^2} - \omega$ and $Y = \frac{R^1}{I^1}$. The Jacobi matrix $J(P^1)$ corresponding to the equilibrium point $P^1(S^1, I^1, R^1)$ is

$$J(P^1) = \begin{bmatrix} -\omega & -X & \psi \\ 0 & \frac{X}{2(1+Y)} - X - \frac{X^2 I^1}{\omega S^1} + \left(\frac{1}{2(1+Y)} + \frac{\psi I^1}{\omega S^1}\right)\frac{Xbc}{(a+c)^2(\psi+\omega)} & \frac{X}{2(1+Y)} + \frac{\psi X I^1}{\omega S^1} \\ 0 & 0 & -\psi - \omega \end{bmatrix}. \tag{28}$$

The eigenmatrix of $J(P^1)$ is

$$|\lambda I - J(P^1)| = \begin{vmatrix} \lambda+\omega & X & -\psi \\ 0 & \lambda - \left[\frac{X}{2(1+Y)} - X - \frac{X^2 I^1}{\omega S^1} + \left(\frac{1}{2(1+Y)} + \frac{\psi I^1}{\omega S^1}\right)\frac{Xbc}{(a+c)^2(\psi+\omega)}\right] & -\frac{X}{2(1+Y)} - \frac{\psi X I^1}{\omega S^1} \\ 0 & 0 & \lambda+\psi+\omega \end{vmatrix}. \tag{29}$$

Correspondingly, the characteristic polynomial of $J(P^1)$ is

$$(\lambda+\omega)[\lambda + \frac{bc}{2(a+c)^2} + \frac{\omega}{2} + \frac{2ab\sigma\pi{R_c}^3 I^1}{N} + \frac{2ab^2c\sigma\pi{R_c}^3 I^1}{(a+c)^2(\psi+\omega)N}](\lambda+\psi+\omega) = 0. \tag{30}$$

We obviously obtain $\lambda_1 = -\omega < 0, \lambda_3 = -(\omega+\psi) < 0$ and $\lambda_2 = -\frac{bc}{2(a+c)^2} - \frac{\omega}{2} - \frac{2ab\sigma\pi{R_c}^3}{N} I^1 - \frac{2ab^2c\sigma\pi{R_c}^3}{(a+c)^2(\psi+\omega)N} I^1 < 0$. Therefore, the three eigenvalues are all negative. According to the Routh–Hurwitz stability criterion, the model is locally asymptotically stable at the endemic equilibrium point $P^1(S^1, I^1, R^1)$. This completes the proof.

Theorem 3 shows that when average infection capacity of infected SIoT nodes exceeds normal defense and recovery capacity of an SIoT, viruses will rapidly spread to other areas with a high-frequency operation of millions of users, and the number of infected SIoT nodes show a rapid outbreak trend. After a period of spread, the growth rate of infected SIoT nodes will decrease to 0. At this point, infected, susceptible, and recovered SIoT nodes reach a relatively stable state, and infected SIoT nodes will exist in the SIoT for a long time.

5 Application framework

This paper introduces a novel model of virus spread into an SIoT through an epidemiologically theoretical model and

game theory. In Fig. 5, the application framework of model STSIR includes data layer, network layer, platform layer and application layer. Due to the strong social attribute of an SIoT, each virtual entity corresponding to the real entity in the SIoT needs to rely on social relationship spread, which requires a large number of basic devices for data collection. These basic devices usually have simple structure and single function, so that viruses designed by hackers can quickly spread to the surrounding networks through Bluetooth, 2G, 3G, 4G, 5G and other communication means along the network of users and devices in a short time. When basic devices that are not equipped to run antivirus programs locally are attacked, they can call remote IDS to detect and kill viruses. Through cloud services, big data and other platforms, SIoT contributes super-intelligent services such as smart home, smart infrastructure construction, smart warehousing and logistics, smart industry and smart agriculture and forestry to the society, facilitating people's production and life. Discovering and containing the spread of viruses in an SIoT has always been a hot security issue, which will cause serious consequences including user privacy disclosure, device damage and network damage once a device is infected. STSIR analyzes virus spread behavior to suppress viruses spread in the SIoT, which improves the hit rate of devices using lower energy to detect and kill viruses through the proposed game, and obtains several effective ways for network administrators to improve the SIoT network defense ability by analyzing the different effects of multiple parameters on the threshold of virus diffusion or extinction.

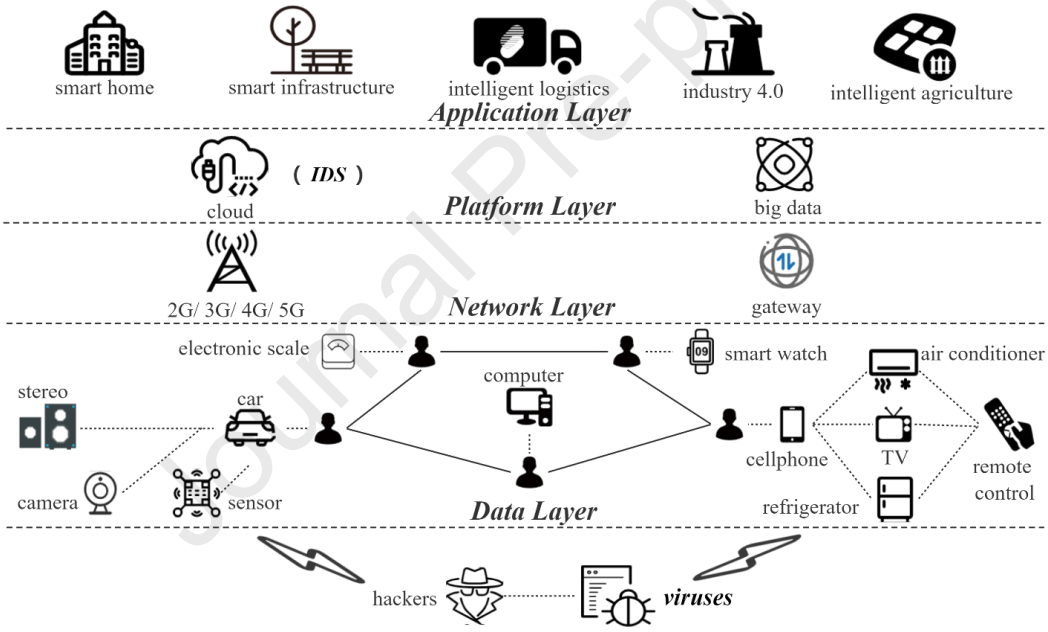


Fig. 5. STSIR application framework.

Algorithm 1 shows the code implementation of the model STSIR, and the effectiveness of the model is verified by the experimental results of the algorithm. According to Algorithm 1, numerous simulation experiments are conducted on this model in Section 6, and the stability of malware-free and endemic equilibriums of STSIR is verified through multidimensional comparison.

Algorithm 1 Calculation algorithm of STSIR model in SIoT.

Inputs: $N, \sigma, R_c, \theta, \psi, \omega, a, b, c$
Outputs: $S(t), I(t), R(t)$
1: initialize conditions: $N, \sigma, R_c, \theta, \psi, \omega, a, b, c$
2: different initial value: $I(0) = x,\ S(0) = 1 - x,\ R(0) = 0$
3: $i = 0, step = 200$

4: **while** $i < step$
5: $S(i+1) = \theta + \psi R(i) - 2ab\sigma^{\frac{3}{2}}\pi^{\frac{3}{2}}R_c{}^3 S(i)\sqrt{I(i)+R(i)}/N((a+c)^2+bc) - \omega S(i)$
6: $I(i+1) = 2ab\sigma^{\frac{3}{2}}\pi^{\frac{3}{2}}R_c{}^3 S(i)\sqrt{I(i)+R(i)}/N((a+c)^2+bc) - bcI(i)/(a+c)^2 - \omega I(i)$
7: $R(i+1) = bcI(i)/(a+c)^2 - \psi R(i) - \omega R(i)$
8: $i = i+1$
9: **end while**
10: **return** $S(i), I(i), R(i)$

6 Experimental analyses

In this section, Wolfram Mathematica 11 is used to simulate the model STSIR in an SIoT. No special configuration is required when we write the simulation programs using Wolfram Programming Language. According to formula (15), differential equations are established, and model parameters are adjusted to control the value of R_0, which can be obtained according to formula (21). Then, correctness of Theorems 2 and 3 is verified by observing the change trend of $S(t)$, $I(t)$, and $R(t)$ over time and analyzing the influence of various parameters on infected SIoT nodes.

6.1 Verify the malware-free equilibrium of the model STSIR

In order to verify Theorem 2 of the malware-free equilibrium point of the model STSIR, we set parameters of the model STSIR according to Table 4, which are referred to the parameter values of the virus spread models in SIoTs (Yi, et al., 2021; Al Kindi, et al., 2019) and WSNs (Zhang, et al., 2020; Shen, et al., 2019; Zhou, et al., 2020). Further, we set the value of R_c in simulations to study its influence on virus spread in an SIoT according to the definition of social distance R_c in Section 3.1 and its standard value $R_c = 6$ entities (Ke, 2010). In terms of game parameters a, b, and c, we set their values depending on game theoretic evaluation (Li et al., 2022; Molinero and Riquelme, 2021) and IDS parameters (Wang and Chang, 2022; Lee et al., 2021; Yungaicela-Naula et al., 2022) articles, focusing here on their relative sizes to explore relevant strategies for containing viruses spread. Thus, according to formula (21), $R_0 = 0.00013$ can be calculated, and the condition $R_0 < 1$ of Theorem 2 is valid.

Table 4

Initial parameters of the model STSIR.

Symbol	Explanation	Value
N	Total number of SIoT nodes	10000000
σ	Average distribution density of SIoT nodes	0.5
R_c	Social radius of SIoT nodes (Spread radius of infected SIoT nodes)	2.5
θ	Birth rate of SIoT nodes	0.1
ψ	Conversion rate of SIoT nodes from state R to state S	0.05
ω	Death rate of SIoT nodes	0.1
a	Rewards of susceptible SIoT nodes calling IDS to detect and kill viruses successfully	5
b	Cost of susceptible SIoT nodes calling IDS to detect and kill virus	1
c	Loss of susceptible SIoT nodes caused by virus infection	3

Fig. 6 shows changeable ratio trends of $S(t), I(t)$, and $R(t)$ in the model STSIR within 200 time steps when $R_0 < 1$. According to formula (16), we can calculate $S^0 = 1$, $I^0 = 0$, and $R^0 = 0$ when the system reaches malware-free equilibrium. From Fig. 6, the ratio of susceptible SIoT nodes gradually increases from the initial 0.5 and finally stabilizes at 1.0; the ratio of infected SIoT nodes gradually decreases from the initial 0.4 to 0 and becomes stable; and the ratio of recovered nodes gradually decreases from the initial 0.1 to the position of 0.

Figs. 7–9 show changing trends of the ratio of node numbers of $S(t), I(t)$ and $R(t)$ in the SIoT within 200 time steps when different $I(0), R(0)$, and $S(0)$ are set in the initial state of the system. From Fig. 7, when $I(0) = 0.2$, the ratio of

infected SIoT nodes gradually stabilizes from 0.2 to 0; when $I(0) = 0.5$, the ratio of infected SIoT nodes gradually stabilizes from 0.5 to 0; and when $I(0) = 0.9$, the ratio of infected SIoT nodes gradually stabilizes from 0.5 to 0. Different initial values of $I(0)$ will not affect the convergence time of $I(t)$, and finally $I(t)$ will stabilize to the position of 0 after ~50 time steps. From Fig. 8, when $R(0)$ is set as 0.3, 0.5, and 0.8 respectively, the final ratio of recovery SIoT nodes will gradually stabilize to 0 after ~50 time steps. From Fig. 9 when $S(0)$ is set as 0.2, 0.6, and 0.8 respectively, the final ratio of susceptible SIoT nodes will gradually stabilize to 1 after ~50 time steps. At this point, only susceptible SIoT nodes exist in the SIoT.

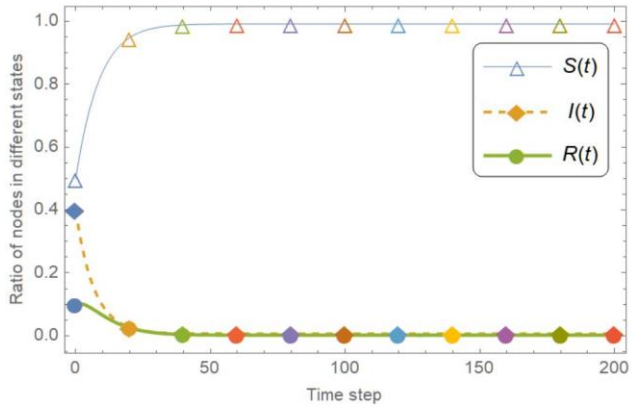


Fig. 6. Ratio changing trends of $S(t)$, $I(t)$, $R(t)$ of model STSIR when $R_0 < 1$.

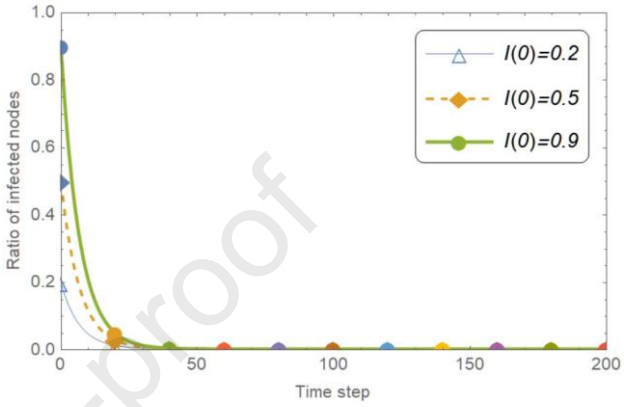


Fig. 7. Ratio changing trends of $I(t)$ of model STSIR at different initial values when $R_0 < 1$.

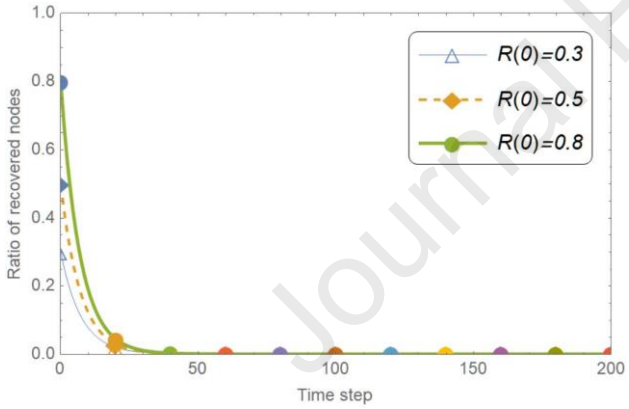


Fig. 8. Ratio changing trends of $R(t)$ of model STSIR at different initial values when $R_0 < 1$.

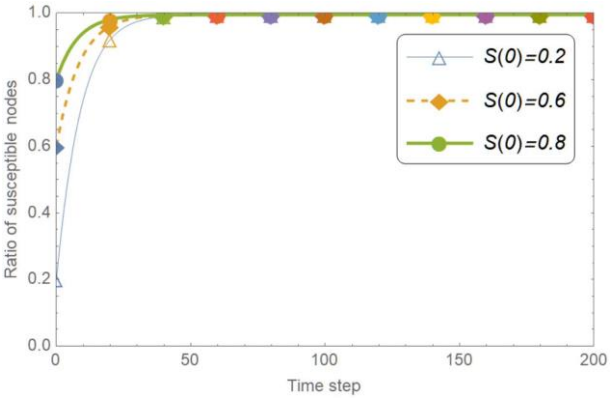


Fig. 9. Ratio changing trends of $S(t)$ of model STSIR at different initial values when $R_0 < 1$.

According to the simulation experiment results of the model STSIR in Figs. 6–9, we can conduct that when $R_0 < 1$, no matter what $S(t)$, $I(t)$, and $R(t)$ of the system are, they will converge to malware-free equilibrium after a certain period of time. Obviously, the defense and recovery thresholds of an SIoT are higher than the attack capability of viruses at this point. Viruses will eventually cease to exist after spreading in the SIoT over a period of time, while susceptible SIoT nodes will occupy an absolutely dominant position. Therefore, Theorem 2 is verified experimentally.

6.2 Verify the endemic equilibrium of the model STSIR

In order to verify the endemic equilibrium of the model STSIR in an SIoT, Theorem 3 of the model STSIR will be verified from the following three dimensions: 1) different initial values of $S(t)$, $I(t)$, and $R(t)$, 2) different game parameters a, b, and c, and 3) different social distance R_c.

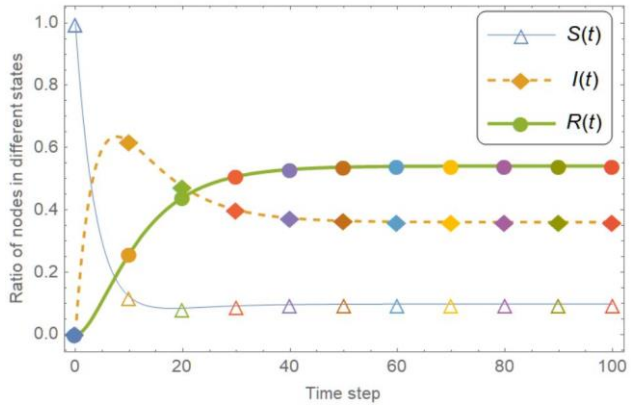


Fig. 10. Ratio changing trends of $S(t)$, $I(t)$, $R(t)$ of the model STSIR when $R_0 > 1$.

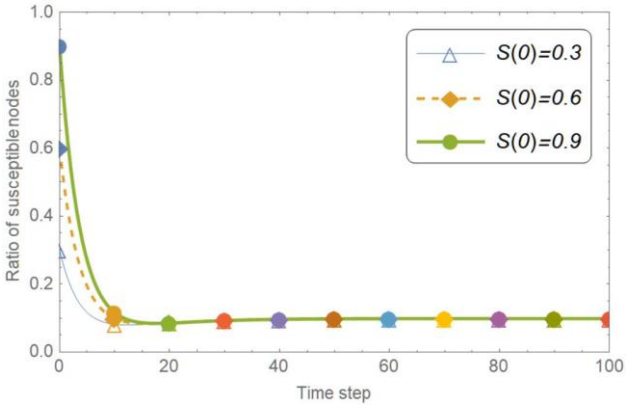


Fig. 11. Ratio changing trends of $S(t)$ of the model STSIR at different initial values when $R_0 > 1$.

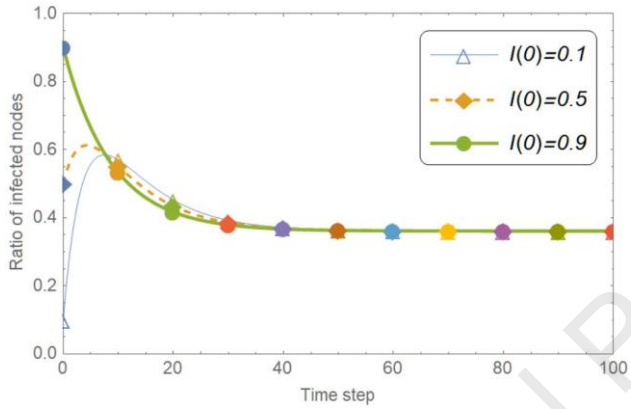


Fig. 12. Ratio changing trend of $I(t)$ of the model STSIR at different initial values when $R_0 > 1$.

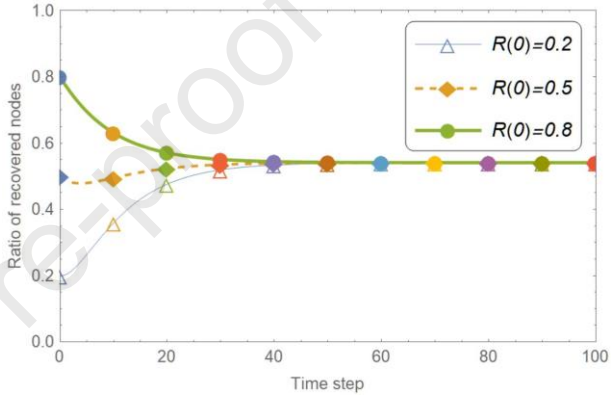


Fig. 13. Ratio changing trend of $R(t)$ of the model STSIR at different initial values when $R_0 > 1$.

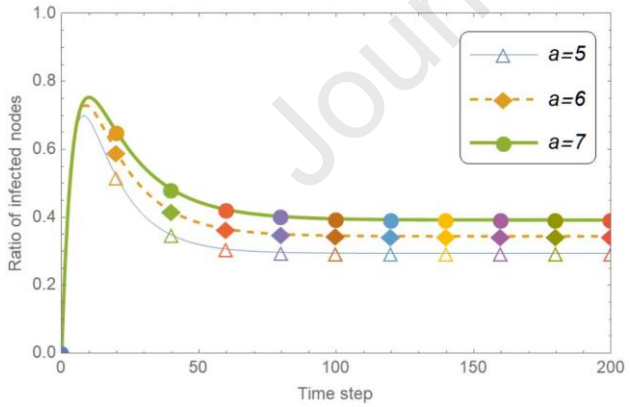


Fig. 14. Ratio changing trend of $I(t)$ of model the STSIR at $a = 5, a = 6, a = 7$ when $R_0 > 1$.

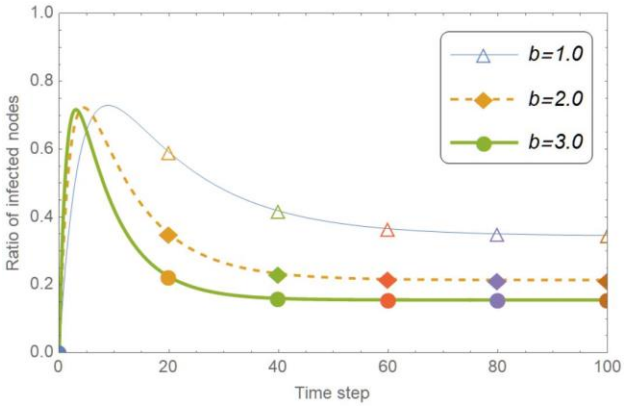


Fig. 15. Ratio changing trend of $I(t)$ of the model STSIR at $b = 1, b = 2, b = 3$ when $R_0 > 1$.

6.2.1 Dimension 1: different initial values of $S(t), I(t), R(t)$

Based on the parameters in Table 4, we set $N = 1000$, $a = 7$, $b = 2$ and $\sigma = 0.5$. According to formula (21), $R_0 = 9.82$ is obtained, and the condition $R_0 > 1$ in Theorem 3 is valid. According to formula (17), an endemic equilibrium $P^1(S^1, I^1, R^1) = (0.102, 0.359, 0.539)$ can be obtained. Fig. 9 shows the changeable ratio trends of $S(t)$, $I(t)$, $R(t)$ in the model STSIR within 100 time steps when $R_0 > 1$. The ratio of susceptible SIoT nodes remains at 0.102 after ~40 time steps, and both infected and recovered SIoT nodes are stable at 0.359 and 0.539 respectively after ~60 time steps. At this point, the

system reaches the endemic equilibrium P^1.

Figs. 11–13 show the changing trends of the ratio of node number of $S(t)$, $I(t)$, $R(t)$ in an SIoT under different initial conditions of $S(0)$, $I(0)$, and $R(0)$ after 100 time steps when $R_0 > 1$. From Fig. 11, when $S(0) = 0.3$, the ratio of susceptible SIoT nodes gradually decreases from 0.3 and stabilizes to 0.1; when $S(0) = 0.6$, the ratio of susceptible SIoT nodes gradually decreases from 0.6 and stabilizes to 0.102; when S(0)=0.9, the ratio of susceptible SIoT nodes gradually decreases from 0.9 and stabilizes to 0.102. The system will eventually stabilize to the position of 0.102 after ~40 time steps, no matter what $S(0)$ is. From Fig. 12, when $I(0)$ is set to 0.1, 0.5 and 0.9 respectively, the final ratio of infected SIoT nodes will gradually decrease and stabilize to 0.359 after ~50 time steps. From Fig. 13, when $R(0)$ is set as 0.2, 0.6 and 0.8 respectively, the final ratio of recovery SIoT nodes will gradually stabilize to 0.539 after ~50 time steps. At this point, infected SIoT nodes will exist in the SIoT for a long time.

According to Figs. 10–13, we can conduct that when $R_0 > 1$, no matter what $S(t)$, $I(t)$, and $R(t)$ of the system are, they will converge to the endemic equilibrium point P^1 after a period of time which is always the same equilibrium because changing the initial values of $S(t)$, $I(t)$, and $R(t)$ will not affect the infection rate of viruses or the recovery rate of the SIoT. In this case, the attack capability of viruses is stronger than the defense threshold of the network. As a result, the network cannot destroy viruses by itself and will coexist with viruses for a long time.

6.2.2 Dimension 2: different game parameters a, b, c

Figs. 14–16 reveal the ratio changing trends of infected SIoT nodes under different values of a, b, and c in model STSIR. From Fig. 14, when $a = 5$, we can calculate that $R_0 = 12.60$ and $P^1(S^1, I^1, R^1) = (0.079, 0.285, 0.636)$ according to formulas (17) and (21). $I(t)$ gradually rises from the initial 0 to the peak and then decreases and stabilizes at 0.285. When $a = 6$, we can calculate that $R_0 = 19.03$ and $P^1(S^1, I^1, R^1) = (0.052, 0.343, 0.605)$, and $I(t)$ finally stabilizes at 0.343. When $a = 7$, we can calculate that $R_0 = 27.24$ and $P^1(S^1, I^1, R^1) = (0.037, 0.397, 0.566)$, and $I(t)$ finally stabilizes at 0.397. From Fig. 15, when $b = 1, R_0 = 19.03$ and $P^1(S^1, I^1, R^1) = (0.052, 0.343, 0.605)$ can be calculated. When $b = 2$, we get $R_0 = 19.28$ and $P^1(S^1, I^1, R^1) = (0.052, 0.209, 0.739)$. When $b = 3$, we have $R_0 = 19.37$ and $P^1(S^1, I^1, R^1) = (0.052, 0.151, 0.797)$. All three cases where $c = I(0)$ are stabilized around the corresponding I^1. From Fig. 16, when $c = 3$ we can calculate that $R_0 = 31.72$ and $P^1(S^1, I^1, R^1) = (0.032, 0.350, 0.618)$. When $c = 6$, we get $R_0 = 28.27$ and $P^1(S^1, I^1, R^1) = (0.035, 0.323, 0.642)$, and $I(t)$ finally stabilizes at 0.343. When $c = 9$, we know that $R_0 = 29.42$ and $P^1(S^1, I^1, R^1) = (0.034, 0.333, 0.633)$. $I(t)$ goes up and then goes down, finally it stabilizes at the corresponding I^1.

Figs. 17-18 show the influence of size relationship between a, b, and c on changing trends of the ratio of infected SIoT nodes in model STSIR when $R_0 > 1$. From Fig. 17, when a is larger than c, the number of infected SIoT nodes will be less when an endemic equilibrium is reached. We know that a is a profit of successful virus detection and elimination, while c is a loss of failure of virus detection and elimination. It means that susceptible SIoT nodes tend to call IDS during the game satisfying $a > c$, thus reducing the ratio of infected SIoT nodes. Conversely, when $a < c$, the number of infected SIoT nodes will increase. From Fig. 18, the number of infected SIoT nodes increases gradually according to different cases $c > b$, $c = b$, and $c < b$. The smaller b is, the lower cost of susceptible SIoT nodes to call IDS is, and the large c is, the greater infection loss of susceptible SIoT nodes is. It means that susceptible SIoT nodes are more inclined to call IDS in the game when $c > b$, whereas frequency of calling IDS will decrease accordingly when $c < b$.

According to Figs. 14–18 we can conduct that when $R_0 > 1$, adjusting game parameters a, b, and c can change the state of endemic equilibrium. However, no matter how a, b, and c change, the system will eventually approach and stabilize at different endemic equilibriums, which inspire us to reduce a cost of energy consumed by normal nodes to call IDS and

increase a reward for successful virus detection to curb the spread of viruses in an SIoT through lots of modern technological means.

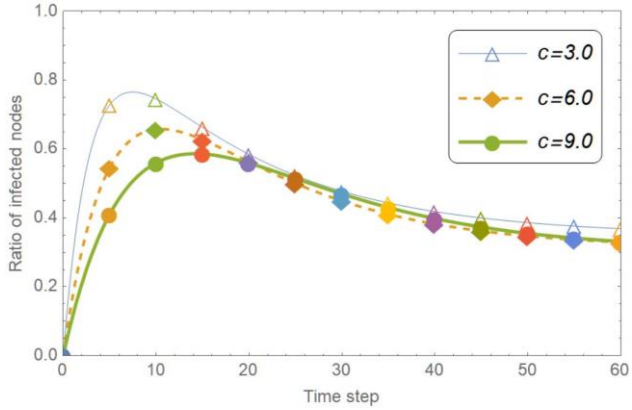


Fig. 16. Ratio changing trend of $I(t)$ of the model STSIR at $c = 3, c = 6$, and $c = 9$ when $R_0 > 1$.

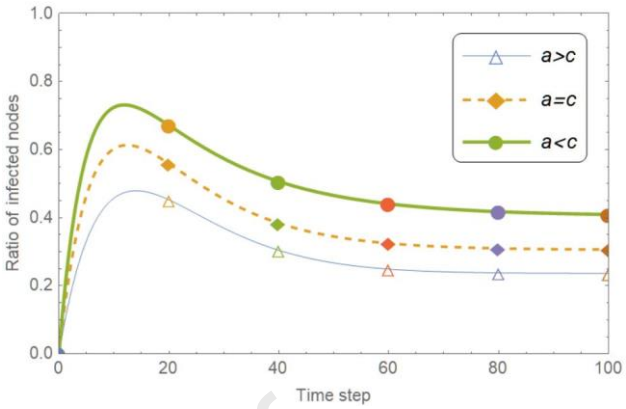


Fig. 17. Ratio changing trend of $I(t)$ of the model STSIR at $a > c, a = c$, and $a < c$ when $R_0 > 1$.

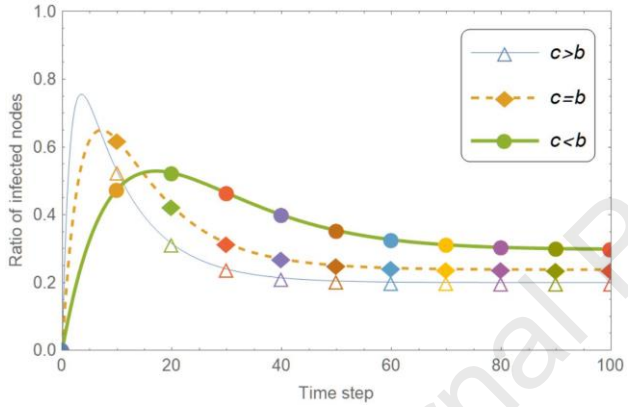


Fig. 18. Ratio changing trend of $I(t)$ of the model STSIR at $c > b, c = b$, and $c < b$ when $R_0 > 1$.

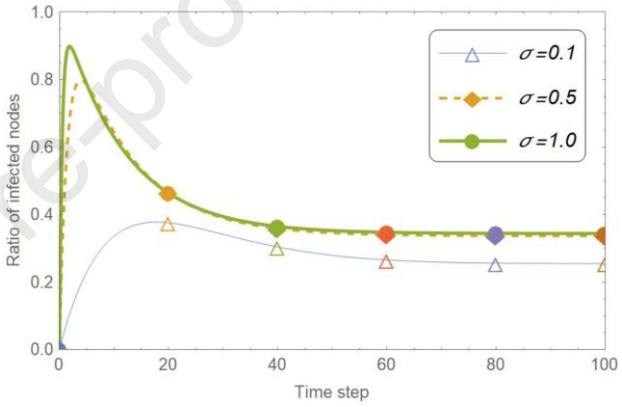


Fig. 19. Ratio changing trend of $I(t)$ of the model STSIR at $\sigma = 0.1, \sigma = 0.5$, and $\sigma = 1.0$ when $R_0 > 1$.

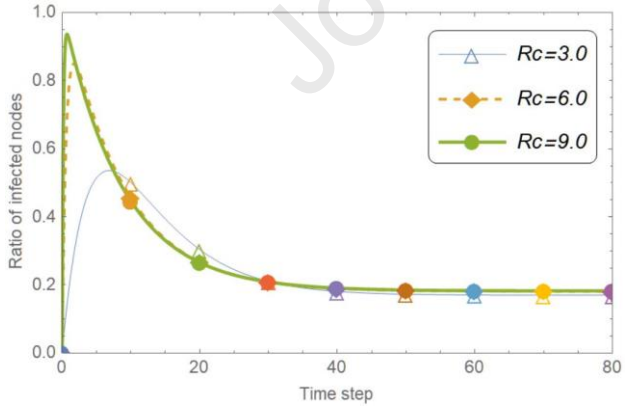


Fig. 20. Ratio changing trend of $I(t)$ of the model STSIR at $R_c = 3$, $R_c = 6$, and $R_c = 9$ when $R_0 > 1$.

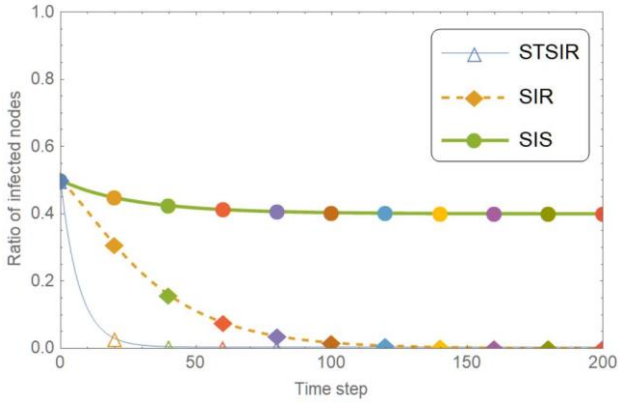


Fig. 21. Comparison the ratio changing trends of $I(t)$ among models STSIR, SIR, and SIS.

6.2.3 Dimension 3: different distribution densities σ and different social distance R_c

Fig. 19 shows the changeable trend of $I(t)$ in model STSIR under different values of node distribution density σ. When $\sigma = 0.1$, we can get $R_0 = 3.64$ and $P^1(S^1, I^1, R^1) = (0.275, 0.252, 0.473)$ according to formulas (17) and (21). Similarly, when $\sigma = 0.5$, we can calculate $R_0 = 36.42$ and $P^1(S^1, I^1, R^1) = (0.055, 0.329, 0.616)$. When σ = 1.0, we have $R_0 = 36.42$

and $P^1(S^1, I^1, R^1) = (0.028, 0.338, 0.634)$. Different density values will affect the number of infected SIoT nodes on the system equilibrium point. The larger node distribution density is, the stronger infectivity of infected SIoT nodes is. But when density exceeds a certain limit, the influence of density on the equilibrium point is negligible.

Fig. 20 shows the changing trend of $I(t)$ under different values of R_c. When $R_c = 3$, we can get $R_0 = 5.37$ and $P^1(S^1, I^1, R^1) = (0.186, 0.149, 0.665)$. When $R_c = 6$, we get $R_0 = 42.97$ and $P^1(S^1, I^1, R^1) = (0.023, 0.179, 0.798)$. When $R_c = 9$, we know that $R_0 = 145.03$ and $P^1(S^1, I^1, R^1) = (0.007, 0.182, 0.811)$. With an increase of R_c, the ratio curve of infected SIoT nodes reaches the peak rapidly, and the peak of infected SIoT nodes increases with an increase of node social distance. After the peak, the number of infected SIoT nodes gradually decreases to 0.18, which means that the greater distance between nodes is, the faster viruses spread and the higher the spread rate is. But eventually, the number of infected SIoT nodes will stabilize at the endemic equilibrium.

According to the simulation experiment analysis of the three dimensions in Figs. 6–20, we can conduct that an SIoT will eventually stabilize at the endemic equilibrium as long as $R_0 > 1$ is satisfied, no matter under conditions of different initial values of $S(t)$, $I(t)$, and $R(t)$, different game parameters a, b, and c or different distribution densities σ and social distances of nodes R_c. The experiment shows that Theorem 3 is reasonable.

6.3 Comparison with traditional models

According to Sections 6.1 and 6.2, when the model STSIR is stable, both the conditions and the ratio of SIoT nodes of S, I, and R are consistent with the theorems and formulas, which can prove the accuracy of the model STSIR. Therefore, here we mainly focus on the advantages of model STSIR compared with models SIS and SIR in curbing virus spread. Under the premise of the same infection and recovery rates, the traditional models SIR and SIS are compared horizontally to verify the efficiency of model STSIR. We set the same ratio of susceptible, infected and recovered SIoT nodes for models SIR, SIS and STSIR. By observing changes in the ratio of infected SIoT nodes of the three models, we can judge which model has the best effect in containing the spread of viruses in an SIoT.

In reality, we study the virus spread model with two ultimate goals: 1) minimize the ratio of infected SIoT nodes; 2) control viruses spread in the shortest time. From Fig. 21, it can be observed that the ratio of infected SIoT nodes in model SIS is stable at ~0.45 after a slow decline, while the ratio of infected SIoT nodes decreases to 0 when model STSIR reaches stability, which reduces the ratio of infected SIoT nodes by ~45% more than that in model SIS. Meanwhile, the model SIR takes ~150 time steps to reach the malware-free equilibrium point, while the model STSIR only takes ~50 time steps to optimize ~66.7% compared with the model SIR, in terms of controlling the speed of virus spread. Obviously, by comparing with models SIS and SIR, STSIR has excellent performance in terms of reducing the ratio of infected SIoT nodes and time cost.

7 Conclusion

Based on an epidemic theory's analysis framework, a novel epidemic model STSIR has been proposed in this paper, which defines the social radius R_c, network traffic inflow θ and outflow ω to reflect characteristics of an SIoT such as limited communication range of people and devices, constant iteration of interpersonal network, and continuous update and elimination of devices. We have introduced an individual-group game to describe the dynamics of virus spread and established the payoff matrix of the game in an SIoT according to an actual attack and defense scenarios of infected SIoT nodes and susceptible SIoT nodes, so that the infection and recovery rates of nodes can be expressed by game parameters, which cuts off dependence of the infection and recovery rates on historical experience. The dynamic equations of STSIR have been proposed, and we have proved that the model STSIR has a malware-free equilibrium point and an endemic

equilibrium point. When the infected SIoT nodes are at the malware-free equilibrium point, they will eventually die out. However, at the endemic equilibrium point, they will continue to spread and eventually exist in the SIoT stably with a certain proportion, which depends on the costs a, b, and c of participating in the game, the social radius R_c, and the distribution density σ of nodes. By controlling game parameters, node social distance and node distribution density, we can adjust the size of the basic reproduction number to determine which equilibrium point the SIoT is in. Especially in the case of the endemic equilibrium point, we can also change a ratio of infected SIoT nodes when the SIoT reaches stability. Compared with models SIR and SIS, the excellent contribution of STSIR to curbing viruses spread in the SIoT is verified. In real life, we can install the virus detection and killing service as long as SIoT devices' conditions are allowed, so as to reduce the cost b of virus detection and killing, and appropriately increase the reward of virus detection and killing service every time to increase a to curb the spread of viruses in the SIoT.

In the future, we will consider repeated game and deep reinforcement learning to carry out further studies. The model presented in this paper provides guidance for the study of virus spread in an SIoT. This paper focuses on an individual-group game in the process of modeling the spread mechanism without considering the repeated behavior between viruses and SIoT nodes, but more realistic situation is that viruses are likely to attack SIoT nodes that fail to infect them again and again. The susceptible SIoT nodes that have been attacked many times will reconsider whether to call the antivirus service for detection and antivirus, which will involve a repeated game. Consequently, the individual-group game discussed in this paper will be repeated, which will lead to more realistic infection and recovery rates affected by the payoff matrix, further optimize the expression of the basic reproduction number R_0, and ultimately determine the accuracy of the experimental conclusion. At the same time, expanding the cost of different device antivirus methods helps to further improve the applicability of the model STSIR to an SIoT, which is caused by the fact that there are some advanced intelligent devices in an SIoT. Such devices have a local antivirus program and often call it locally, thus resulting in less cost. In addition, the first stage of our research on curbing the spread of viruses is to build a model to describe the law of virus spread. Next, in the second stage, we will consider using the spread model optimized by a repeated game and device costs, and explore the optimal control strategy for SIoT node virus detection and killing. This part will use deep reinforcement learning algorithms such as double deep Q-network to conduct optimization experiments to improve the rate of convergence and further reduce the scale of infection.

Acknowledgments

This work was supported in part by Zhejiang Provincial Natural Science Foundation of China under Grant no. LZ22F020002, Humanities and Social Sciences Planning Foundation of Ministry of Education of China under Grant No. 22YJAZH090, and National Natural Science Foundation of China under Grant no. 61772018.

References

Cai B , Li X , Kong W , Yuan J, Yu S, 2022. A reliable and lightweight trust inference model for service recommendation in SIoT. IEEE Internet Things J. 9(13), 10988–11003. https://doi.org/10.1109/JIOT.2021.3125347.

Jiang N , Chen J , Zhou R , Wu C , Chen H , Zheng J, Wan T, 2020. PAN: Pipeline assisted neural networks model for data-to-text generation in Social Internet of Things. Inform. Sciences. 530, 167–179. https://doi.org/10.1016/j.ins.2020.03.080.

Chung KC, Liang SW, 2020. An empirical study of social network activities via Social Internet of Things (SIoT). IEEE Access. 8, 48652–48659. https://doi.org/10.1109/ACCESS.2020.2978151.

Wang J , Xiong Z , Han Q , Han X, Yang D, 2022. Top-k socially constrained spatial keyword search in large SIoT networks. IEEE Internet Things J. 9(12), 9280–9289. https://doi.org/10.1109/JIOT.2021.3114155.

Qiu J , Tian Z , Du C , Zuo Q , Su S, Fang B, 2020. A survey on access control in the age of internet of things. IEEE Internet Things J. 7(6), 4682–4696. https://doi.org/10.1109/JIOT.2020.2969326.

Zhu X , Wen S , Jolfaei A , Haghighi MS , Camtepe S, Xiang Y, 2020. Vulnerability detection in SIoT paplications: A fuzzing method

on their binaries. IEEE Trans. Netw. Sci. Eng., Early Access. https://doi.org/10.1109/TNSE.2020.3038142.
Signes-Pont MT , Cortés-Castillo A , Mora-Mora H, Szymanski J, 2018. Modelling the malware propagation in mobile computer devices. Comput. Secur. 79, 80–93. https://doi.org/10.1016/j.cose.2018.08.004.
Shen Y , Shen S , Li Q , Zhou H , Wu Z, Qu Y, 2022. Evolutionary privacy-preserving learning strategies for edge-based IoT data sharing schemes. Digit. Commun. Netw., Early Access. https://doi.org/https://doi.org/10.1016/j.dcan.2022.05.004.
Rasool RU , Ahmad HF , Rafique W , Qayyum A, Qadir J, 2022. Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML. J. Netw. Comput. Appl. 201, 103332. https://doi.org/10.1016/j.jnca.2022.103332.
Shen S , Ma H , Fan E , Hu K , Yu S , Liu J, Cao Q, 2017. A non-cooperative non-zero-sum game-based dependability assessment of heterogeneous WSNs with malware diffusion. J. Netw. Comput. Appl. 91, 26–35. https://doi.org/10.1016/j.jnca.2017.05.003.
Sun P, 2021. A trust game model of service cooperation in cloud computing. J. Netw. Comput. Appl. 173, 102864. https://doi.org/10.1016/j.jnca.2020.102864.
Wu H, Wang Z, 2018. Multi-source fusion-based security detection method for heterogeneous networks. Comput. Secur. 74, 55–70. https://doi.org/10.1016/j.cose.2018.01.003.
Liu X , Zhang H , Dong S, Zhang Y, 2021. Network defense decision-making based on a stochastic game system and a deep recurrent Q-network. Comput. Secur. 111, 102480. https://doi.org/10.1016/j.cose.2021.102480.
Louk MHL, Tama BA, 2023. Dual-IDS: A bagging-based gradient boosting decision tree model for network anomaly intrusion detection system. Expert Syst. Appl. 213, 119030. https://doi.org/https://doi.org/10.1016/j.eswa.2022.119030.
Ariful K, Jun T, 2020. The role of advanced and late provisions in a co-evolutionary epidemic game model for assessing the social triple-dilemma aspect. J. Theor. Biol. 503, 110399. https://doi.org/10.1016/j.jtbi.2020.110399.
Shakya RK , Rana K , Gaurav A , Mamoria P, Srivastava PK, 2019. Stability analysis of epidemic modeling based on spatial correlation for Wireless Sensor Networks. Wirel. Pers. Commun. 108(3), 1363–1377. https://doi.org/10.1007/s11277-019-06473-0.
Tavanpour M , Kazi BU, Wainer G, 2020. Discrete event systems specifications modelling and simulation of wireless networking applications. J. Simul.(6), 1–25. https://doi.org/10.1080/17477778.2020.1750313.
Castellano C , Van Mieghem P , Vespignani A, Pastor-Satorras R, 2015. Epidemic processes in complex networks. Rev. Mod. Phys. 87(3), 925–979. https://doi.org/10.1103/RevModPhys.87.925.
Giordano G , Blanchini F , Bruno R , Colaneri P , Di Filippo A , Di Matteo A, Colaneri M, 2020. Modelling the COVID-19 epidemic and implementation of population-wide interventions in Italy. Nat. Med. 26(6), 855–860. https://doi.org/10.1038/s41591-020-0883-7.
Hethcote HW, 2000. The mathematics of infectious diseases. SIAM Rev. 42(4), 599–653. https://doi.org/10.1137/S0036144500371907.
Hota AR , Godbole J, Paré PE, 2021. A closed-loop framework for inference, prediction, and control of SIR epidemics on networks. IEEE Trans. Netw. Sci. Eng. 8(3), 2262–2278. https://doi.org/10.1109/TNSE.2021.3085866.
Leonardo Stella APMD, 2021. The role of asymptomatic infections in the COVID-19 epidemic via complex networks and stability analysis. SIAM J. Control Optim. 0(0), S119–S144. https://doi.org/10.1137/20M1373335.
Chen P , Lin C , Cheng S , Hsiao H, Huang C, 2016. Decapitation via digital epidemics: A bio-inspired transmissive attack. IEEE Commun. Mag. 54(6), 75–81. https://doi.org/10.1109/MCOM.2016.7497770.
Mahboubi A , Camtepe S, Morarji H, 2017. A study on formal methods to generalize heterogeneous mobile malware propagation and their impacts. IEEE Access. 5, 27740–27756. https://doi.org/10.1109/ACCESS.2017.2772787.
Punzo G, 2022. An SIS network model with flow driven infection rates. Automatica. 137, 107–110. https://doi.org/10.1016/j.automatica.2021.110107.
Chen Z , Zhu K, Ying L, 2016. Detecting multiple information sources in networks under the SIR model. IEEE Trans. Netw. Sci. Eng. 3(1), 17–31. https://doi.org/10.1109/TNSE.2016.2523804.
Mei W , Mohagheghi S , Zampieri S, Bullo F, 2017. On the dynamics of deterministic epidemic propagation over networks. Annu. Rev. Control. 44, 116–128. https://doi.org/10.1016/j.arcontrol.2017.09.002.
Pagliara R, Leonard NE, 2021. Adaptive susceptibility and heterogeneity in contagion models on networks. IEEE Trans. Autom. Control. 66(2), 581–594. https://doi.org/10.1109/TAC.2020.2985300.
Ke X, 2010. A social networking services system based on the “six degrees of separation” theory and damping factors, 438–441.
Alemany J , Val ED, García-Fornes A, 2023. A review of privacy decision-making mechanisms in online social networks. ACM Comput. Surv. 55(2), 31–37. https://doi.org/10.1145/3494067.
Álvarez R , Díez-González J , Verde P , Ferrero-Guillén R, Perez H, 2023. Combined sensor selection and node location optimization for reducing the localization uncertainties in wireless sensor networks. Ad Hoc Netw. 139, 103036. https://doi.org/https://doi.org/10.1016/j.adhoc.2022.103036.
An J , Gui X , Zhang W , Jiang J, Yang J, 2013. Research on social relations cognitive model of mobile nodes in Internet of Things. J. Netw. Comput. Appl. 36(2), 799–810. https://doi.org/10.1016/j.jnca.2012.12.004.
Radanliev P , De Roure D , Walton R , Van Kleek M , Montalvo RM , Santos O , Maddox LT, Cannady S, 2020. COVID-19 what have we learned? The rise of social machines and connected devices in pandemic management following the concepts of predictive, preventive and personalized medicine. EPMA Journal. 11(3), 311–332. https://doi.org/10.1007/s13167-020-00218-x.
Ahmed M , Li Y , Waqas M , Sheraz M , Jin D, Han Z, 2018. A survey on socially aware device-to-device communications. IEEE Commun. Surv. Tut. 20(3), 2169–2197. https://doi.org/10.1109/COMST.2018.2820069.
Yi Y , Zhang Z , Yang LT , Deng X , Yi L, Wang X, 2021. Social interaction and information diffusion in Social Internet of Things: dynamics, cloud-edge, traceability. IEEE Internet Things J. 8(4), 2177–2192. https://doi.org/10.1109/JIOT.2020.3026995.
Zareie A, Sakellariou R, 2021. Minimizing the spread of misinformation in online social networks: A survey. J. Netw. Comput. Appl. 186, 103094. https://doi.org/10.1016/j.jnca.2021.103094.
Alamouti SM , Arjomandi F, Burger M, 2022. Hybrid edge cloud: A pragmatic approach for decentralized cloud computing. IEEE Commun. Mag. 60(9), 16–29. https://doi.org/10.1109/MCOM.001.2200251.
Al Kindi A , Al Abri D , Al Maashri A, Bait-Shiginah F, 2019. Analysis of malware propagation behavior in Social Internet of Things.

Int. J. Commun. Syst. 32(15), 4102. https://doi.org/10.1002/dac.4102.
Jiang JJ , Qu Y , Yu S , Zhou W, Wu W, 2016. Studying the global spreading influence and local connections of users in online social networks., 431–435. https://doi.org/10.1109/CIT.2016.15.
Qu Y , Yu S , Zhou W, Niu J, 2018. FBI: Friendship learning-based user identification in multiple social networks., 1–6. https://doi.org/10.1109/GLOCOM.2018.8647771.
Cui L , Qu Y , Xie G , Zeng D , Li R , Shen S, Yu S, 2022. Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures. IEEE Trans. Ind. Informatics. 18(5), 3492–3500. https://doi.org/10.1109/TII.2021.3107783.
Nguyen DC , Pham Q , Pathirana PN , Ding M , Seneviratne A , Lin Z , Dobre OA, Hwang W, 2023. Federated learning for smart healthcare: A survey. ACM Comput. Surv. 55(3), 60–61. https://doi.org/10.1145/3501296.
Qu Y , Uddin MP , Gan C , Xiang Y , Gao L, Yearwood J, 2023. Blockchain-enabled federated learning: A survey. ACM Comput. Surv. 55(4), 70–71. https://doi.org/10.1145/3524104.
Magdich R , Jemal H, Ayed MB, 2022. A resilient trust management framework towards trust related attacks in the Social Internet of Things. Comput. Commun. 191, 92–107. https://doi.org/https://doi.org/10.1016/j.comcom.2022.04.019.
Zhang Z, Zhu Z, 2018. A Worm containment approach towards online social networks, 1–8. https://doi.org/10.1109/NAS.2018.8515718.
Peng S , Wang G , Zhou Y , Wan C , Wang C , Yu S, Niu J, 2019. An immunization framework for social networks through big data based influence modeling. IEEE Trans. Dependable Secur. Comput. 16(6), 984–995. https://doi.org/10.1109/TDSC.2017.2731844.
Zhou P , Gu X , Nepal S, Zhou J, 2021. Modeling social worm propagation for advanced persistent threats. Comput. Secur. 108, 102321. https://doi.org/10.1016/j.cose.2021.102321.
Chen Z , Liu J , Shen Y , Simsek M , Kantarci B , Mouftah HT, Djukic P, 2023. Machine learning-enabled IoT security: Open issues and challenges under advanced persistent threats. ACM Comput. Surv. 55(5), 101–105. https://doi.org/10.1145/3530812.
Lin Y , Wang X , Hao F , Jiang Y , Wu Y , Min G , He D , Zhu S, Zhao W, 2021. Dynamic control of fraud information spreading in Mobile Social Networks. IEEE Trans. Syst. Man Cybern. Syst. 51(6), 3725–3738. https://doi.org/10.1109/TSMC.2019.2930908.
Shen S , Li H , Han R , Vasilakos AV , Wang Y, Cao Q, 2014. Differential game-based strategies for preventing malware propagation in Wireless Sensor Networks. IEEE Trans. Inf. Forensic Secur. 9(11), 1962–1973. https://doi.org/10.1109/TIFS.2014.2359333.
Li Y, Hu X, 2022. A differential game approach to intrinsic formation control. Automatica. 136, 110077. https://doi.org/10.1016/j.automatica.2021.110077.
Zhang H , Shen S , Cao Q , Wu X, Liu S, 2020. Modeling and analyzing malware diffusion in wireless sensor networks based on cellular automaton. Int. J. Distrib. Sens. Netw. 16(11), 465433968. https://doi.org/10.1177/1550147720972944.
Kirkby JL, 2023. Hybrid equity swap, cap, and floor pricing under stochastic interest by Markov chain approximation. Eur. J. Oper. Res. 305(2), 961–978. https://doi.org/10.1016/j.ejor.2022.05.044.
Shen S , Zhou H , Feng S , Huang L , Liu J , Yu S, Cao Q, 2019. HSIRD: A model for characterizing dynamics of malware diffusion in heterogeneous WSNs. J. Netw. Comput. Appl. 146, 102420. https://doi.org/10.1016/j.jnca.2019.102420.
Bahi JM , Guyeux C , Hakem M, Makhoul A, 2014. Epidemiological approach for data survivability in unattended wireless sensor networks. J. Netw. Comput. Appl. 46, 374–383. https://doi.org/10.1016/j.jnca.2014.09.011.
Aliberti G , Di Pietro R, Guarino S, 2017. Epidemic data survivability in unattended Wireless Sensor Networks: New models and results. J. Netw. Comput. Appl. 99, 146–165. https://doi.org/10.1016/j.jnca.2017.09.008.
Hu P , Ding L, Hadzibeganovic T, 2018. Individual-based optimal weight adaptation for heterogeneous epidemic spreading networks. Commun. Nonlinear Sci. Numer. Simul. 63, 339–355. https://doi.org/10.1016/j.cnsns.2018.04.003.
Hernández Guillén JD, Martín Del Rey A, 2018. Modeling malware propagation using a carrier compartment. Commun. Nonlinear Sci. Numer. Simul. 56, 217–226. https://doi.org/10.1016/j.cnsns.2017.08.011.
Zhao D , Wang L , Wang Z, Xiao G, 2019. Virus propagation and patch distribution in multiplex networks: Modeling, analysis, and optimal allocation. IEEE Trans. Inf. Forensic Secur. 14(7), 1755–1767. https://doi.org/10.1109/TIFS.2018.2885254.
Abazari F , Analoui M, Takabi H, 2016. Effect of anti-malware software on infectious nodes in cloud environment. Comput. Secur. 58, 139–148. https://doi.org/10.1016/j.cose.2015.12.002.
Xing J , Wu C , Zhou H , Cheng Q , Yu D, Carrasco MAM, 2022. Efficient middlebox scaling for virtualized intrusion prevention systems in software-defined networks. Sci. China Inf. Sci. 65(8), 1–3. https://doi.org/10.1007/s11432-019-2731-7.
Lefoane M , Ghafir I , Kabir S, Awan I, 2023. Unsupervised learning for feature selection: A proposed solution for Botnet detection in 5G Networks. IEEE Trans. Ind. Informatics. 19(1), 921–929. https://doi.org/10.1109/TII.2022.3192044.
Guan J , Wei Z, You I, 2018. GRBC-based network security functions placement scheme in SDS for 5G security. J. Netw. Comput. Appl. 114, 48–56. https://doi.org/10.1016/j.jnca.2018.03.013.
Jiang P , Wang Q , Huang M , Wang C , Li Q , Shen C, Ren K, 2021. Building in-the-cloud network functions: Security and privacy challenges. Proc. IEEE. 109(12), 1888–1919. https://doi.org/10.1109/JPROC.2021.3127277.
Martín Del Rey A , Hernández G , Bustos Tabernero A, Queiruga Dios A, 2021. Advanced malware propagation on random complex networks. Neurocomputing. 423, 689–696. https://doi.org/10.1016/j.neucom.2020.03.115.
Gibert D , Mateu C, Planes J, 2020. The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. J. Netw. Comput. Appl. 153, 102526. https://doi.org/10.1016/j.jnca.2019.102526.
Han W , Xue J , Wang Y , Liu Z, Kong Z, 2019. MalInsight: A systematic profiling based malware detection framework. J. Netw. Comput. Appl. 125, 236–250. https://doi.org/10.1016/j.jnca.2018.10.022.
AL-Hawawreh M , Moustafa N, Sitnikova E, 2018. Identification of malicious activities in industrial internet of things based on deep learning models. J. Inf. Secur. Appl. 41, 1–11. https://doi.org/10.1016/j.jisa.2018.05.002.
Liu J , Wang X , Yue G, Shen S, 2018. Data sharing in VANETs based on evolutionary fuzzy game. Future Gener. Comput. Syst. 81, 141–155. https://doi.org/10.1016/j.future.2017.10.037.
Wang K , Yuan L , Miyazaki T , Chen Y, Zhang Y, 2018. Jamming and eavesdropping defense in green cyber-physical transportation systems using a Stackelberg game. IEEE Trans. Industr. Inform. 14(9), 4232–4242. https://doi.org/10.1109/TII.2018.2841033.
Liu J , Wang X , Shen S , Fang Z , Yu S , Yue G, Li M, 2022. Intelligent jamming defense using DNN Stackelberg game in Sensor Edge Cloud. IEEE Internet Things J. 9(6), 4356–4370. https://doi.org/10.1109/JIOT.2021.3103196.

Shen S , Huang L , H Z , Yu S , Fan E, Cao Q, 2018. Multistage signaling game-based optimal detection strategies for suppressing malware diffusion in Fog-Cloud-Based IoT networks. IEEE Internet Things J. 5(2), 1043–1054. https://doi.org/10.1109/JIOT.2018.2795549.

Jakóbik A , Palmieri F, Kołodziej J, 2018. Stackelberg games for modeling defense scenarios against cloud security threats. J. Netw. Comput. Appl. 110, 99–107. https://doi.org/10.1016/j.jnca.2018.02.015.

Bucarey V , Casorrán C , Labbé M , Ordóñez F, Figueroa Ó, 2021. Coordinating resources in Stackelberg security games. Eur. J. Oper. Res. 291(3), 846–861. https://doi.org/10.1016/j.ejor.2019.11.002.

Zhou H , Shen S, Liu J, 2020. Malware propagation model in wireless sensor networks under attack–defense confrontation. Comput. Commun. 162, 51–58. https://doi.org/10.1016/j.comcom.2020.08.009.

Li X, Li X, 2020. Perception effect in evolutionary vaccination game under prospect-theoretic approach. IEEE Trans. Comput. Soc. Syst. 7(2), 329–338. https://doi.org/10.1109/TCSS.2019.2960818.

Sheryl LC , Mahendra P , Philippa P, Mikhail P, 2020. Game theoretic modelling of infectious disease dynamics and intervention methods: A review. J. Biol. Dynam. 0(0), 1–33. https://doi.org/10.1080/17513758.2020.1720322.

Razak MFA , Anuar NB , Salleh R, Firdaus A, 2016. The rise of "malware": Bibliometric analysis of malware study. J. Netw. Comput. Appl. 75, 58–76. https://doi.org/10.1016/j.jnca.2016.08.022.

Xiao L , Li Y , Huang X, Du X, 2017. Cloud-based malware detection game for mobile devices with offloading. IEEE Trans. Mob. Comput. 16(10), 2742–2750. https://doi.org/10.1109/TMC.2017.2687918.

Liu J , Wang X , Shen S , Yue G , Yu S, Li M, 2021. A Bayesian Q-learning game for dependable task offloading against DDoS attacks in Sensor Edge Cloud. IEEE Internet Things J. 8(9), 7546–7561. https://doi.org/10.1109/JIOT.2020.3038554.

Nosouhi MR , Yu S , Sood K , Grobler M , Jurdak R , Dorri A, Shen S, 2021. UCoin: An efficient privacy preserving scheme for cryptocurrencies. IEEE Trans. Dependable Secur. Comput., Early Access. https://doi.org/10.1109/TDSC.2021.3130952.

Liu J , Shen S , Yue G , Han R, Li H, 2015. A stochastic evolutionary coalition game model of secure and dependable virtual service in Sensor-Cloud. Appl. Soft. Comput. 30, 123–135. https://doi.org/10.1016/j.asoc.2015.01.038.

Shen Y , Shen S , Wu Z , Zhou H, Yu S, 2022. Signaling game-based availability assessment for edge computing-assisted IoT systems with malware dissemination. J. Inf. Secur. Appl. 66, 103140. https://doi.org/https://doi.org/10.1016/j.jisa.2022.103140.

Liu J , Yu J, Shen S, 2018. Energy-efficient two-layer cooperative defense scheme to secure Sensor-Clouds. IEEE Trans. Inf. Forensic Secur. 13(2), 408–420. https://doi.org/10.1109/TIFS.2017.2756344.

Rabbani M , Wang YL , Khoshkangini R , Jelodar H , Zhao R, Hu P, 2020. A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing. J. Netw. Comput. Appl. 151, 102507. https://doi.org/https://doi.org/10.1016/j.jnca.2019.102507.

De La Torre Parra G , Rad P , Choo KR, Beebe N, 2020. Detecting Internet of Things attacks using distributed deep learning. J. Netw. Comput. Appl. 163, 102662. https://doi.org/https://doi.org/10.1016/j.jnca.2020.102662.

Ariful K , Kazuki K, Jun T, 2020. The impact of information spreading on epidemic vaccination game dynamics in a heterogeneous complex network- A theoretical approach. Chaos, Solitons & Fractals. 132, 109548. https://doi.org/10.1016/j.chaos.2019.109548.

Fisman DN , Greer AL, Tuite AR, 2020. Bidirectional impact of imperfect mask use on reproduction number of COVID-19: A next generation matrix approach. Infe. Dis. Mod. 5, 405–408. https://doi.org/10.1016/j.idm.2020.06.004.

Li Q , Zeng C , Xu W, Xiao Y, 2022. A social rumor and anti-rumor game diffusion model based on sparse representation and tensor completion. J. Netw. Comput. Appl. 201, 103343. https://doi.org/https://doi.org/10.1016/j.jnca.2022.103343.

Molinero X, Riquelme F, 2021. Influence decision models: From cooperative game theory to social network analysis. Comp. Sci. Rev. 39, 100343. https://doi.org/https://doi.org/10.1016/j.cosrev.2020.100343.

Wang S, Chang J, 2022. Design and implementation of an intrusion detection system by using extended BPF in the linux kernel. J. Netw. Comput. Appl. 198, 103283. https://doi.org/https://doi.org/10.1016/j.jnca.2021.103283.

Lee S , Mohammed Sidqi H , Mohammadi M , Rashidi S , Rahmani AM , Masdari M, Hosseinzadeh M, 2021. Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review. J. Netw. Comput. Appl. 187, 103111. https://doi.org/https://doi.org/10.1016/j.jnca.2021.103111.

Yungaicela-Naula NM , Vargas-Rosales C , Pérez-Díaz JA, Carrera DF, 2022. A flexible SDN-based framework for slow-rate DDoS attack mitigation by using deep reinforcement learning. J. Netw. Comput. Appl. 205, 103444. https://doi.org/https://doi.org/10.1016/j.jnca.2022.103444.

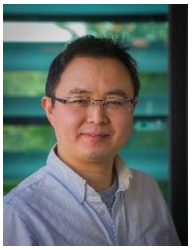
Guowen Wu received the M.S. degree in applied mathematics from Shanghai University, Shanghai, China, in 1996, and the Ph.D. degree in computer software and theory from Fudan University, Shanghai, China, in 2001. From 2002 to 2004, he was engaged in postdoctoral research in Changjiang Computer (Group) Company, and from 2011 to 2012 he was a visiting scholar at Victoria University in Canada. He is an associate professor with the School of Computer Science and Technology, Donghua University, Shanghai, China. His current research interests include Internet of Things, edge computing, game theory, and machine learning.

Lanlan Xie, a postgraduate student of Donghua University, received her bachelor's degree from China West Normal University, Nanchong, China, in 2021. Her research interests include Internet of Things, game theory, and deep reinforcement learning.

Hong Zhang received the B.S. degree in computer science and technology from Shandong Agricultural University, Tai'an, China, in 2007, the M.S. degree in computer software and theory from Donghua University, Shanghai, China, in 2010. She is currently an Experimental Teacher with the College of Computer Science and Technology, Donghua University, Shanghai, China. Her current research interests include Internet of Things, cyber security, edge computing, and game theory.

Jianhua Wang received the B.S. degree in electronic science and technology from Henan Institute of Engineering, Zhengzhou, China, in 2014, the M.S. degree in control engineering from University of Shanghai for Science and Technology, Shanghai, China, in 2017, and the Ph.D. degree in control science and engineering from University of Shanghai for Science and Technology, Shanghai, China, in 2020. He is currently an associate Professor with the School of Engineering, Huzhou University, Huzhou, Zhejiang, China. His current research interests include predictive model control, robust control, security control, and networked control systems.

Shigen Shen received the B.S. degree in fundamental mathematics from Zhejiang Normal University, Jinhua, China, in 1995, the M.S. degree in computer science and technology from Zhejiang University, Hangzhou, China, in 2005, and the Ph.D. degree in pattern recognition and intelligent systems from Donghua University, Shanghai, China, in 2013. He is a Professor with the Department of Computer Science and Engineering, Shaoxing University, Shaoxing, China. He is currently serving as a member of the editorial review board of Journal of Organizational and End User Computing. His current research interests include Internet of Things, cyber security, edge computing, and game theory.



Shui Yu is a Professor of School of Computer Science, University of Technology Sydney, Australia. Dr Yu's research interest includes Big Data, Security and Privacy, Networking, and Mathematical Modelling. He has published three monographs and edited two books, more than 500 technical papers, including top journals and top conferences, such as IEEE TPDS, TC, TIFS, TMC, TKDE, TETC, ToN, and INFOCOM. His h-index is 48. Dr Yu initiated the research field of networking for big data in 2013, and his research outputs have been adopted by industrial systems. He is currently serving a number of prestigious editorial boards, including IEEE Communications Surveys and Tutorials (Area Editor), IEEE Communications Magazine, IEEE Transactions on Computational Social Systems, IEEE Internet of Things Journal, Journal of Network and Computer Applications, and Digital Communications and Networks. He is a Senior Member of IEEE, a member of AAAS and ACM, and a Distinguished Lecturer of IEEE Communication Society.

Declaration of interests

☒ 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.

☐ The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: