# Game theory in network security for digital twins in industry

Hailin Feng, Dongliang Chen, Haibin Lv, Zhihan Lv

PII: S2352-8648(23)00017-2

DOI: https://doi.org/10.1016/j.dcan.2023.01.004

Reference: DCAN 601

To appear in: *Digital Communications and Networks*

Received Date: 25 June 2021

Revised Date: 24 November 2022

Accepted Date: 12 January 2023

Digital Communications and Networks 7 (2021) 196-200

Contents lists available at Science Direct

Digital Communications and Networks

journal homepage:

# Game theory in network security for digital twins in industry

Hailin Feng [a], Dongliang Chen [b], Haibin Lv [c], Zhihan Lv [d*]

[a] School of Information Engineering, Zhejiang A & F University, Hangzhou, 311300, China

[b] School of Data Science and Software Engineering, Qingdao University, Qingdao, 266000, China

[c] North China Sea Offshore Engineering Survey Institute, Ministry of Natural Resources North Sea Bureau, Qingdao, 266000, China

[d] Department of Game design, Faculty of Arts, Uppsala University, Sweden

*Corresponding Author

ARTICLEINFO

Digital twins
Industrial Internet of Things
Network security
Game theory
Attack and defense

ABSTRACT

To ensure the safe operation of industrial digital twins network and avoid the harm to the system caused by hacker invasion, a series of discussions on network security issues are carried out based on game theory. From the perspective of the life cycle of network vulnerabilities, mining and repairing vulnerabilities are analyzed by applying evolutionary game theory. The evolution process of knowledge sharing among white hats under various conditions is simulated, and a game model of the vulnerability patch cooperative development strategy among manufacturers is constructed. On this basis, the differential evolution is introduced into the update mechanism of the Wolf Colony Algorithm (WCA) to produce better replacement individuals with greater probability from the perspective of both attack and defense. Through the simulation experiment, it is found that the convergence speed of the probability ($X$) of white Hat 1 choosing the knowledge sharing policy is related to the probability ($x_0$) of white Hat 2 choosing the knowledge sharing policy initially, and the probability ($y_0$) of white hat 2 choosing the knowledge sharing policy initially. When $y_0$=0.9, $X$ converges rapidly in a relatively short time. When $y_0$ is constant and $x_0$ is small, the probability curve of the “cooperative development” strategy converges to 0. It is concluded that the higher the trust among the white hat members in the temporary team, the stronger their willingness to share knowledge, which is conducive to the mining of loopholes in the system. The greater the probability of a hacker attacking the vulnerability before it is fully disclosed, the lower the willingness of manufacturers to choose the "cooperative development" of vulnerability patches. Applying the improved wolf colony-co-evolution algorithm can obtain the equilibrium solution of the "attack and defense game model", and allocate the security protection resources according to the importance of nodes. This study can provide an effective solution to protect the network security for digital twins in the industry.

* Corresponding author.

E-mail addresses: hlfeng@zafu.edu.cn (H. Feng), 936418030@qq.com (D. Chen), lvhaibinsoa@gmail.com (H. Lv), lvzhihan@gmail.com (Z. Lv).

https://doi.org/10.1016/j.dcan.2020.07.011

Received 30 November 2019; Received in revised form 12 July 2020; Accepted 30 July 2020

Available online 7 August 2020

## 1. Introduction

Various technologies have emerged in recent years, such as big data analysis, machine learning, and Human Computer Interaction (HCI), all of which help promote the development of intelligent manufacturing and industrial Internet of Things (IoT). The emergence of digital twins will transform the process of industrial manufacturing and provide new methods to reduce costs, monitor assets, optimize maintenance, and create interconnected products [1]. The concept of digital twins was proposed many years ago, and it is a technology that matches digital objects with physical objects developed by researchers from the aerospace administration [2-4]. Based on digital twins, the digital models can be used to manipulate, simulate, and analyze the underlying system controlled by physics. Applying the digital twins technology to the network to create a virtual image of physical network facilities can build a digital twins network platform. Through real-time interaction and mutual influence between the physical network and the twin network, the digital twins network platform can help the network achieve low-cost trial and error, intelligent decision making, and high-efficiency innovation [5]. Currently, digital twins are being widely used in industry, manufacturing, and other industries. Digital twins, as a virtual embodiment of the design, construction, and maintenance of physical entities, are based on the real-time operation process of physical entities and production systems to enhance the accuracy of data analysis and configuration. The reduction of technology costs has accelerated the development of IoT and digital twins technology.

Industrial IoT based on digital twins has profoundly affected the organization, production, and business models of traditional industries, and continuously promoted the intelligent transformation of the global industrial system [6-8]. Digital twins is a cutting-edge technology trend that will play a critical role in deploying industrial Iot applications. The new technology will also help boost industry revenues and reduce the unnecessary overhead associated with equipment and process problems. The development of digital twins technology has also helped reduce repair costs to a large extent. In addition, it improves the consistency of production lines across the organization. In the future, digital twins will be combined with more technologies, such as voice functions, augmented reality, and Artificial Intelligence (AI), to achieve an immersive experience, thereby helping people observe the internal structure of digital twins. Digital twins bring more convenient innovative experiments, lower trial and error costs, finer measurements, more reliable predictions, and easier-to-replicate experiences, and open a window to transform the physical world through the digital world. However, network security has also become prominent with the development and application of digital twins in the industry. Industrial IoT introduces open communication protocols such as Ethernet and Transmission Control Protocol / Internet Protocol (TCP/IP), making industrial control systems increasingly open and standardized, and the connection with the external Internet becomes more frequent [9-10]. The interconnection brought about by the industrial IoT breaks the traditional closed production environment, and exposes the vulnerabilities of the industrial control system to the open network without protection [11]. In cybersecurity, digital twins open new opportunities across the value chain. They extend scalability and efficiency to everything from research, development, testing, and analysis to IP protection and vendor management. Cyber security experts can use digital twins to build online digital copies of each physical asset in a simple form. This digital copy is designed to simulate network attacks, exploits, vulnerabilities, etc., in order to identify possible risks before the original project is attacked.

Industrial IoT security involves the critical infrastructure of water supply, heating, water conservancy, and other systems. Once the network is attacked, it will cause extremely bad effects, so it is very necessary to study the industrial Internet security vulnerabilities to reduce the occurrence of industrial Internet security accidents. Therefore, it is necessary to form a nationally aware intelligent security command platform and promote the high-quality development of a smart society through secure digital twins technology to develop a modern and digital economy. Traditional risk management theories have been difficult to provide effective decision-making guidance for the security protection of digital twins for industrial IoT. In this study, the game theory is adopted to describe the interaction process between attackers and defenders in the network based on the security requirements of the digital twins for industrial IoT. In addition, the security problems in the process of network vulnerabilities are discovered and repaired, the importance of the vulnerability life cycle management to the protection of the digital twins for industrial IoT is clarified, and a targeted allocation strategy for network security protection resources is proposed. The innovation of this study lies in the application of game theory to the analysis of network security risks, which provides new research ideas for the overall perception and effective handling of security vulnerabilities in digital twins networks.

## 2. Related research

### 2.1 Network security of digital twins in industry

Digital twins is an emerging technology in industrial control and automation systems. While this technology has attracted the attention of advanced simulation advantages, the security of its network has also attracted the attention of researchers. Network security assessment is to realize the security risk estimation and control of the network system by identifying the hazard and sensitive points of the security accident. Finding all the hazard and sensitive points is the key to accurate security risk assessment. Gehrmann and Gunnarsson [12] discussed how to use the digital twins model and the corresponding security architecture to realize data sharing and control of safety-critical processes. They identified the drive security design requirements based on digital twins data sharing and conducted high-level design and evaluation of other security components of the architecture. Hassija [13] pointed out that various industrial IoT applications are responsible for automating different tasks and trying to make inanimate physical objects operate without human intervention. Therefore, it is necessary to ensure the high security and privacy of the network in the attack environment during the virtual mapping. The more ways devices are connected to each other, the more ways to intercept threats. Protocols such as Hyper Text Transfer Protocol (HTTP) and Application Ppprogramming Interface (API) are just a few channels that devices in the digital twins network can rely on to intercept hackers. Srivastava et al. [14] proposed ways to protect the digital twins network: guaranteeing port security, disabling port forwarding, and not opening ports when not needed; using anti-malware software, firewalls, and

* Corresponding author.

*E-mail addresses:* hlfeng@zafu.edu.cn (H. Feng), 936418030@qq.com (D. Chen), lvhaibinsoa@gmail.com (H. Lv), lvzhihan@gmail.com (Z. Lv).

https://doi.org/10.1016/j.dcan.2020.07.011

Received 30 November 2019; Received in revised form 12 July 2020; Accepted 30 July 2020

Available online 7 August 2020

intrusion detection systems / intrusion prevention systems; preventing unauthorized Internet protocol addresses; ensuring the system is patched and kept up to date.

### *2.2 Game theory in network security*

In modern society, information and communication technologies have been applied in various fields such as industry and finance, and the security vulnerabilities of traditional information and communication technologies have gradually appeared in industrial IoT systems. Game theory exerts an important role in protecting the network from various attacks. Game theory is a mathematical method for studying phenomena with the nature of struggle or competition, and it can be used to analyze the strategic choice of participants with interdependent behaviors. Lee et al. [15] proposed an attack tree vulnerability quantification method based on game theory, which includes three steps: game strategy modeling, cost impact analysis, and profit calculation. Using game theory, security experts in social IoT systems will be able to respond to security incidents more effectively and provide a reference for building safer industrial IoT systems. Kong et al. [16] proposed a security reputation model based on S-Alex Net Convolutional Neural Network (CNN) and dynamic game theory to solve the inaccurate screening of indicators and lack of scientific verification of evaluation results in industrial IoT. Kiran et al. [17] used non-cooperative game model theory to describe the interaction among different nodes and assist the trust measurement to accurately detect attackers, which greatly reduces the resource consumption.

### *2.3 Summary*

Existing studies mainly focus on the application of game theory in the assessment of IoT security. However, an assessment and solution for digital twins in industry network security is urgently needed as the combination of IoT, and digital twins in industry technology becomes more and more mature. From the perspective of game theory, this study discusses in depth the attack and defense in the digital twins network as well as the vulnerability discovery and repair, and proposes an effective network security protection plan.

## 3. Experimental and computational details

### *3.1 Network key technologies for digital twins in industry*

### *3.1.1 Overall architecture of digital twins.*

Digital twins can be understood as the performance of certain things (processes or services) in reality in a digital virtual environment. In fact, digital twins not only bring automation to various industries, but also increase the value and innovation of different businesses [18]. The digital twins network can be regarded as an organic whole of the network system and become the general structure of the whole life cycle involving the physical network in the future, serving the network planning, construction, maintenance, optimization, and the application of network innovation technologies such as network automatic driving and intent network, and improving the automation and intelligence level of the network. In the architecture of digital twins network (as illustrated in Fig.1), various network management and applications can use digital twins technology to build virtual twins to efficiently analyze, diagnose, simulate, and control the physical network based on data and models. Data is the cornerstone of the digital twins network. Building a unified data sharing warehouse as the single source of truth for the digital twins network provides data support for the digital twins network. The model is the source of the capabilities of the digital twins network and can serve various network applications [19-21]. As a physical network entity, the mapping is presented through the high-fidelity visualization of the network twins, which is the most typical feature of the digital twins network that is different from the network simulation system. The digital twins network spans the network function layer and the application and service layer, and is an important foundation for realizing 6G network data perception, intelligent control, sharing and collaboration.

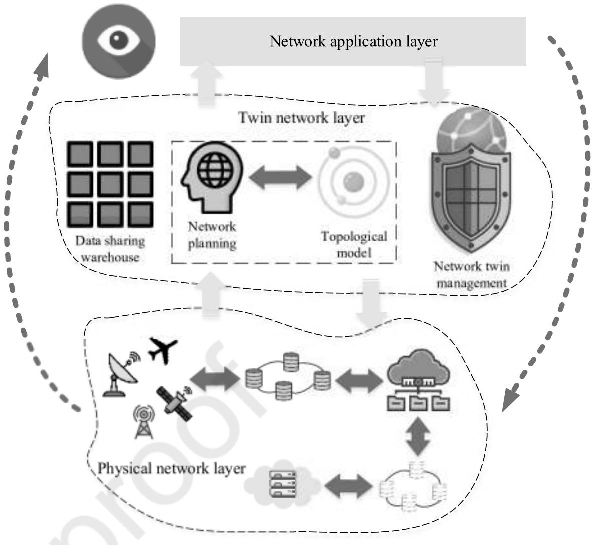


**Fig. 1.** Overall architecture of digital twins.

As the physical object of the network twin, the physical network can be either a cellular access network, a cellular core network, or a data center network, industrial IoT, etc. The twin network layer is the symbol of the digital twins network system, including three key subsystems: data sharing warehouse, service mapping model, and network twin management [22-24]. Among them, the service mapping model completes the data-based modeling and provides data model instances for various network applications, thereby maximizing the agility and programmability of network services. Network applications input requirements to the twin network layer through the twin uplink interface, and deploy services at the twin network layer through modeled examples; and the twin network layer sends control updates to the physical entity network through the downlink interface after full verification. Fig.1 reveals that the digital twins network is not limited to the Software-Defined Network (SDN) architecture, but can realize SDN management and complex network dynamic control and optimization based on virtual layer simulation.

The physical entity is composed of different subsystems that perform specific tasks, providing convenience for different sensors that collect working state parameters [25-26]. Virtual entities are designed to model physical entities with high precision by integrating multiple different types of models (such as geometric models, physical models, behavioral models, and rule models). The service model includes services for physical entities and virtual entities. It optimizes the operation of physical entities and ensures the high reliability of virtual entities by calibrating parameters at runtime. The data model consists of five parts: data from physical entities, data from virtual entities, data from services, domain knowledge, and data fusion module [27-29]. As the cornerstone of the digital twins network, the more complete and accurate the data in the data sharing warehouse, the higher the availability of the data model. The basic and functional models provide services to upper-layer network applications through examples, maximizing the agility and programmability of network services. In addition, the model instance needs to be fully simulated and verified in the virtual twin network element or network topology through the program to complete the prediction, scheduling, configuration, optimization, and other objectives, so as to ensure the effectiveness and reliability of the change control when it is sent to the physical network.

*3.1.2 Key technologies of digital twins.*

At present, the digital twins network system still faces some challenges in terms of compatibility, real-time, and scale. Based on the overall architecture of the digital twins network, this study constructs the digital twins network system using some key technologies, such as network data collection, data storage and services, full life cycle network modeling, interactive visual presentation, and interface protocols.

(1) Network data collection. The key to digital twins technology lies in data. The basic requirements for digital twins data collection are real-time, distributed, and fault-tolerant [30]. The precise control of digital twins replies to the sampled data, so there are higher requirements for the time delay of information processing, and it is necessary to ensure that the time among the multi-sensor units in the system is synchronized. In combination with the digital twins network's requirements for comprehensive and efficient data collection, the use of network telemetry can realize the function of network equipment actively pushing status information, with strong timeliness [31-33]. For different network modeling requirements, the most suitable network telemetry scheme can be selected as needed, including in-band telemetry and out-of-band telemetry. Out-of-band telemetry can effectively improve the incomplete collection and the burden of the Central Processing Unit (CPU), but the detection message of this solution can only go through one forwarding table path, and the probability of finding a network failure is low. The messages of in-band telemetry technology are generated through mirroring, which does not change the forwarding path of the original service messages, nor does it bring a great burden on the CPU. The overall processing architecture of in-band telemetry is shown in Fig.2.

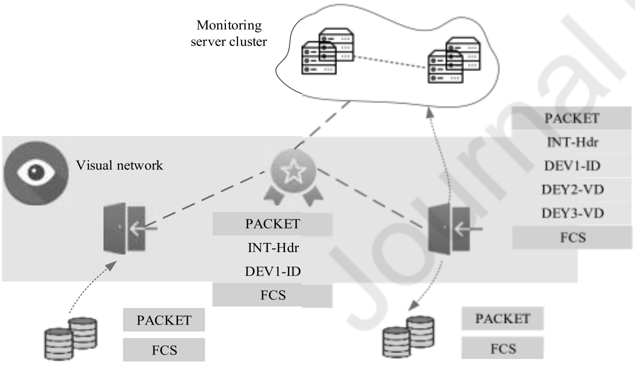


**Fig. 2.** The overall processing architecture of in-band telemetry.

(2) Data storage and services. The design idea of the offline data warehouse is mainly based on the big data technology of Hadoop ecological components, and the calculation is mainly based on distributed computing to improve the operational performance of data. The real-time data warehouse is similar to the offline data warehouse, and its advantage lies in the real-time data [34]. The service mapping model for the digital twins network provides data required for modeling through a unified data service interface, and provides various services such as data search, batch service, and historical rollback.

(3) Full life cycle network modeling: Digital twins will not only help the digital and intelligent transformation of the industry, but will also play a role in the full life cycle management of the live network. Firstly, the visualization capability can solve the problem that customers need to display network performance indicators and operating status intuitively, real-time and three-dimensionally. Secondly, network planning and simulation capabilities can solve the complex and diversified networking and configuration of the industry on-site, resulting in high degree of customization and high cost of networking solutions. Finally, the intelligent operation and maintenance capabilities can solve the problem that the traditional passive failure recovery model cannot quickly respond to requirements. After a failure occurs, the period from complaint to on-site investigation is long, and it is difficult to meet the problem of rapid failure recovery. The industry site network is mainly responsible for connecting various terminals, machines, sensors, and systems at the end of the industry site to meet the diverse business needs of the industry site for sensing, data, positioning, control, and management. The architecture of industry site network system is shown in Fig.3.

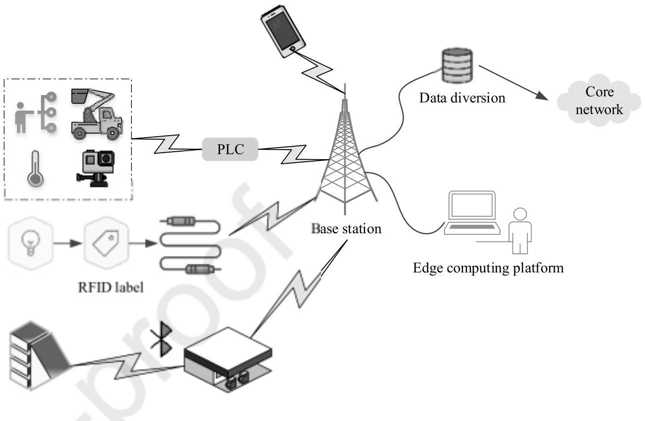


**Fig. 3.** The architecture of industry site network system.

(4) Interactive visual presentation: The digital twins network system has to be able to visualize the data and models in the network twin with high fidelity, and reflect the mapping between the physical entity and the twin. The visualization of the network topology can use the layout algorithm to present the network nodes and links in dots and lines, which clearly and intuitively reflects the network operation status. Functional model visualization is to present model examples, simulation verification, and other processes help users better understand the model [35-37]. In addition, dynamic interactive visualization allows users to have a deeper understanding of data through dialogue and interactive operations with the system.

(5) Interface design and interface protocol system. Standardized interfaces and protocol systems are the basis for meeting the compatibility and scalability of digital twins networks. The data acquisition interface is responsible for completing the data acquisition of the twin network layer data sharing warehouse, and the control issuing interface is responsible for issuing the control instructions after the simulation verification of the service mapping model to the physical network layer. The intent translation interface and capability call interface between the application layer and the network layer can use the HTTP/3.0 protocol. It is a newly developed HTTP based on the Quick UDP Internet Connection (QUIC) protocol. It features fast connection, low latency, forward correction, and adaptive congestion control. With the development of the network scale, there are more and more upper-layer application systems, and the number of lower-layer physical network elements is gradually increasing, resulting in a rapid increase in the actual number of network interfaces. It is necessary to adopt a unified and highly scalable standardized interface in the design of the twin network interface to quickly introduce and integrate new applications and new functions.

### *3.2 Network security vulnerabilities management for digital twins*

*3.2.1 Life cycle of network security vulnerability.*

The integration of digital twins technology and intelligent manufacturing is accelerating, and the transition from a closed system to an open system is an inevitable trend, so that systematic network security risks will be concentrated. Since the equipment and related hardware in the originally closed system environment are relatively simple, the basic equipment and control system will be exposed to unknown network risks. In addition, the data security risks of intelligent manufacturing systems are further increased with the continuous changes in current network attack methods and the in-depth involvement of third-party collaboration services. Based on the current development trend of digital twins network and the security issues it faces, digital twins technology can be incorporated into the network security comprehensive guarantee system, and an overall roadmap to promote its security development can be formulated according to the technical characteristics and application development trends of digital twins.

The security foundation of the digital twins network means that the software, hardware, and cloud data of the networked system are not maliciously tampered with or leaked, and the operating system and network services can continue to operate reliably. The security risks of the digital twins network come from the specific implementation of system hardware, software, and protocols or the loopholes in the security strategy [38]. The attacker can access or damage the system without authorization through these vulnerabilities [39]. The typical life cycle of security vulnerability includes seven stages:

(1) The security vulnerabilities are mined: The exploitable security vulnerabilities in the target system can be mined using some methods such as white box testing, gray box testing, and black box testing.

(2) The code development and testing are permeated: Hackers will develop penetration attack codes while digging for security vulnerabilities to verify whether the security vulnerabilities found actually exist and can be exploited.

(3) The security vulnerabilities and infiltration code are spread: "Black hats" will share secrets in closed small-scale teams to make full use of the attack value brought by the security vulnerabilities and infiltration attack codes; while "white hats" will make the security vulnerability public and inform the manufacturer or unit, so that it can be repaired as soon as possible before it is utilized by the "black hat" hackers.

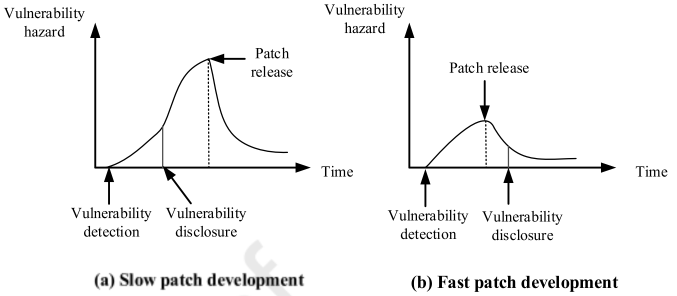
(4) The security vulnerabilities and infiltration code are proliferated: The security vulnerabilities and infiltration code secretly shared in closed teams will eventually be disclosed and published on the Internet. The "black hat" will be quickly grasped and spread in the security community.

(5) Malicious programs appear and begin to spread: "Black hat" further develops malicious programs that are easier to use and more automated spreading capabilities on the basis of mastering security vulnerabilities and penetration codes, and spread them through the social organization structure of hacker communities and the Internet. In this process, the manufacturer completes the patch program development and testing, and releases it.

(6) Infiltration code spreads on a large scale and endangers the network: The release of patches and security alerts by manufacturers will further inform the entire hacker community about the emergence of new security vulnerabilities and corresponding infiltration codes and malicious programs. More "black hats" will obtain and utilize these malicious programs from the Internet or community networks, so that the harm to the Internet has reached its peak at this stage.

(7) The attack code / malicious program gradually disappears: After manufacturer patch programs and detection and removal mechanisms provided by security companies are widely used, the corresponding penetration code and the malicious program will be gradually abandoned by the "black hat" and then disappear.

In the life cycle of security vulnerabilities in digital twins in the industry, patch development and release is the key to bug fixes. If the vulnerability patch development is slow, the vulnerability disclosure will occur before the patch is released. The harm caused by vulnerabilities will increase rapidly before the patch is released, and the vulnerabilities begin to die out quickly after the patch is released. But not all systems will install the vulnerability patch, so the harm of vulnerabilities cannot disappear completely. If the vulnerability patch is developed quickly, the vulnerability will begin to die out due to the release of the patch before it causes major harm. The period from the manufacturer's claim to the vulnerability to its demise belongs to the repair period. The period from manufacturer claim to the patch release is for the vulnerability development. Fig.4 shows the life cycles of vulnerabilities under different patch development speeds.



**(a) Slow patch development** **(b) Fast patch development**

**Fig. 4.** The life cycles of vulnerabilities under different patch development speeds.

### *3.2.2 Vulnerability mining strategy based on evolutionary game.*

The behaviors of "white hat" to identify and report the threats and risks to the system caused by network attacks are very helpful in effectively responding to network attacks and improving the security of information systems [40-42]. However, since most of the white hat groups are formed temporarily, the degree of security knowledge sharing among temporary teams is relatively low. Based on the idea of an evolutionary game, the selection process of the white hat group in the security Knowledge Sharing Strategy (KSS) can be modeled, and finally the evolution process of the white hat mining network security vulnerability strategy can be obtained.

In the temporary team, the white hat individual faces weakness in the quality of knowledge, and the sharing of software vulnerabilities, hackers, viruses, and other information should be in a two-way sharing mode. $K_i$ is supposed to represent the total amount of knowledge inherent in white hats related to digital twins in industry network security. The larger the $K_i$, the stronger the business capabilities of the white hat. When the white hats participate in knowledge sharing, their trust in other members of the team can be expressed as $\omega_i$, and the amount of security knowledge shared by white hats can be expressed as $\omega_i K_i$, When both white hats 1 and 2 choose the strategy {no sharing, no sharing}, then the white hat is performed with a separate penetration test, and the game gain can be written in Eq. (1) below:

$$\{K_1 \cdot \alpha_1 \cdot e, K_2 \cdot \alpha_2 \cdot e\} \tag{1}$$

In the above equation, $e$ is the average revenue of the loopholes, and $\alpha_i$ refers to the loophole conversion rate of security knowledge.

If white hat 1 chooses to share the strategy and white hat 2 chooses not to share the strategy, then white hat 1 can only obtain the vulnerability benefits of its own knowledge of independent penetration testing. During this period, a certain sharing cost will be incurred, but it may also be rewarded by the team. The total revenue of white hat 1 can be calculated with the following equation:

$$K_1 \cdot \alpha_i \cdot e + \left[\left(K_1\omega_1 + K_2\right)\left(1+\gamma\right)\alpha_2 + K_1\alpha_1\right] \cdot \lambda\beta - C_1 \tag{2}$$

In the equation above, $\lambda$ is the vulnerability reward rate of the platform, $\beta$ refers to the probability of the temporary team being rewarded, and $C_i$ represents the cost of knowledge sharing.

The white hat 2 who chooses not to share the strategy will get the loophole benefit generated by the knowledge shared by the white hat 1 and its own inherent knowledge, but cannot get the team reward. The team's total revenue payment is calculated with the following equation:

$$(K_1\omega_1+K_2)(1+\gamma)\alpha_2 e \tag{3}$$

If both white hats 1 and 2 choose the sharing strategy, they will pay the sharing cost and get the sharing benefits. Shared benefits include the increased benefits of synergy after the other party chooses to share knowledge and the incentives provided by the platform's temporary team. At this time, the shared benefits of white hats 1 and 2 are given as Eqs. (4) and (5):

$$(K_2\omega_2+K_1)(1+\gamma)\alpha_1 e+\left[(K_2\omega_2+K_1)(1+\gamma)\alpha_1+(K_1\omega_1+K_2)(1+\gamma)\alpha_2\right]\cdot\lambda\beta-C_1 \tag{4}$$

$$(K_1\omega_1+K_2)(1+\gamma)\alpha_2 e+\left[(K_2\omega_2+K_1)(1+\gamma)\alpha_1+(K_1\omega_1+K_2)(1+\gamma)\alpha_2\right]\cdot\lambda\beta-C_2 \tag{5}$$

It is assumed that the probability of white hat 1 choosing KSS is *x* and the probability of white hat 2 choosing KSS is *y*, and then the corresponding expected benefits are shown as follows when white hat 1 chooses knowledge sharing and non-sharing, respectively:

$$\begin{aligned}U_{1YES}=&(1-y)\cdot\left\{K_1\cdot\alpha_1\cdot e+\left[(K_1\omega_1+K_2)(1+\gamma)\alpha_2+K_1\alpha_1\right]\cdot\lambda\beta-C_1\right\}+\\&y\left\{(K_2\omega_2+K_1)(1+\gamma)\alpha_1 e+\left[(K_2\omega_2+K_1)(1+\gamma)\alpha_1+(K_1\omega_1+K_2)(1+\gamma)\alpha_2\right]\cdot\lambda\beta-C_1\right\}\end{aligned} \tag{6}$$

$$U_{1NO}=y\cdot(K_2\omega_2+K_1)(1+\gamma)\alpha_1 e+(1-y)\cdot K_1\cdot\alpha_1\cdot e \tag{7}$$

Then, the average gain of the white hat 1 can be written as follows:

$$\overline{U_1}=xU_{1YES}+(1-x)U_{1NO} \tag{8}$$

The evolution of game theory suggests that the process of white hat selection strategy change is also learning process. The more the number of white hats in the temporary team that choose to share knowledge, the better the team's total income, and the greater the incentive for white hats to learn. At time *t*, the dynamic change speed equation of the proportion of white hats for knowledge sharing can be expressed as follows:

$$f(x)=\frac{dx}{dt}=x\left(U_{1YES}-\overline{U_1}\right) \tag{9}$$

In the same way, the average gain of white hat 2 and the dynamic change speed equation of selecting knowledge sharing can be obtained, as shown in Eqs. (10) and (11):

$$\overline{U_2}=yU_{2NO}+(1-y)U_{2NO} \tag{10}$$

$$f(y)=\frac{dx}{dt}=y\left(U_{2YES}-\overline{U_2}\right) \tag{11}$$

Before the stable strategy of the dynamic equation is solved, the stable equilibrium points $x^*$ and $y^*$ should be found, and the equilibrium point has to satisfy the following conditions:

$$f(x^*)=f(y^*)=0 \tag{12}$$

$$x^*=\frac{C_2-\left[(K_2\omega_2+K_1)(1+\gamma)\alpha_1+K_2\alpha_2\right]\cdot\lambda\beta}{\alpha_2\lambda\beta\left[(K_1\omega_1+K_2)(1+\gamma)-K_2\right]} \tag{13}$$

$$y^*=\frac{C_1-\left[(K_1\omega_1+K_2)(1+\gamma)\alpha_2+K_1\alpha_1\right]\cdot\lambda\beta}{\alpha_1\lambda\beta\left[(K_2\omega_2+K_1)(1+\gamma)-K_1\right]} \tag{14}$$

Finally, 5 balance points can be obtained, which are O(0,0), A(0,1), B(1,0), C(1,1), and D(x*,y*).

The partial derivatives of *x* and *y* can be solved based on the f(x) and *f(y)*, and the Jacobian matrix *J* can be obtained (equation (15)):

$$J=\begin{bmatrix}\dfrac{\partial f(x)}{\partial x} & \dfrac{\partial f(x)}{\partial y}\\ \dfrac{\partial f(y)}{\partial x} & \dfrac{\partial f(y)}{\partial y}\end{bmatrix}=\begin{bmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix} \tag{15}$$

In terms of shared knowledge, several evolutionary game situations for strategy selection are as follows. (1) In the initial state, neither side of the game white hats share knowledge, but the final stability strategies are all knowledge sharing when they realize that the shared knowledge will obtain additional benefits and team rewards. (2) After the white hat firstly chooses to share knowledge, the other party chooses to share knowledge to obtain team rewards. (3) The white hat chooses to share knowledge, but the party who originally shared the knowledge refuses to continue to share it as the cost of sharing increases. (4) In the initial state, both parties choose to share knowledge, but both parties choose not to share knowledge anymore when the cost of sharing exceeds the sum of the benefits of knowledge sharing.

### *3.2.3 Vulnerability repair strategy based on evolutionary game.*

After the vulnerabilities in the digital twins network are discovered, the ability to repair the vulnerabilities is also different, so that manufacturers can exchange the development progress and related knowledge of the vulnerability patch with each other. $K_A$ and $K_B$ refer to the patch development progresses achieved by the manufacturer A and manufacturer B under the same time and capital consumption, respectively; $\tau$ is the spillover effect brought about by the sharing of patch development information; $\mu_i$ represents the absorption rate of the shared information by the industrial manufacturers. When both A and B choose the strategy {independent development, independent development}, the gain at this time is the phased result brought by the independent development of the manufacturer, which can be expressed as follows:

$$K_A-C_A-\xi D_A\rho-D_A\rho\psi(1-\xi) \tag{16}$$

$$K_B-C_B-\xi D_B\rho-D_B\rho\psi(1-\xi) \tag{17}$$

In the above two equations, *Ci* is the cost during the development of the vulnerability patch, and $D_i$ refers to the maximal loss for the successful hacker attack; $\xi$ represents the probability of a hacker attacking before the vulnerability is disclosed; $\rho$ refers to the probability of a hacker successfully attacking the vulnerability before the vulnerability is disclosed; $\Psi$ is the multiple that the hacker's ability to attack after the vulnerability is disclosed.

If one of the players in the game (party B) chooses the "cooperative development" strategy but manufacturer A chooses the independent development, then manufacturer B can only obtain the results of its own development stage and pay the sharing cost. The total gain of manufacturer B is calculated with following equation:

$$K_B-C_B-C_0-\xi D_B\rho-(1-\xi)D_B\rho\psi \tag{18}$$

And the total gain of manufacturer A is calculated with Eq. (19):

$$(\mu_A K_B+K_A)-C_A-\xi D_A\rho-P-D_A\rho\psi(1-\xi) \tag{19}$$

In the equation above, *P* refers to the potential risk.

If both parties in the game choose the "cooperative development" strategy, they can obtain the other's vulnerability patch development results, and a certain shared cost will also be incurred. In the case of cooperation between the two parties, the development time of the vulnerability patch will be greatly reduced. Usually, the manufacturer has completed the development of the vulnerability patch before the vulnerability is fully disclosed, so the probability of successful hacker intrusion will be greatly reduced. At this time, the total gains of manufacturer A and manufacturer B are expressed as follows:

$$(\mu_A K_B+K_A)(1+\tau)-C_A-D_A\rho \tag{20}$$

$$(\mu_B K_A+K_B)(1+\tau)-C_B-D_B\rho \tag{21}$$

According to the evolutionary game theory, the change process of industrial manufacturers' strategy can also be regarded as a learning process, and the learning speed is related to the number of manufacturers currently choosing "cooperative development" of the vulnerability patch and the benefits brought by the cooperation strategy. In the game, the more manufacturers choosing "cooperative development", the higher their gain, the stronger the motivation of industrial manufacturers to choose "cooperative development". At time *t*, the dynamic change speed of the proportion of manufacturers that choose "cooperative development" can be expressed as follows:

$$f\left(x\right)=\frac{dx}{dt}=x\left(U_{AYES}-\overline{U_A}\right) \tag{22}$$

In the same way, the average gain and the dynamic change speed of choosing "cooperative development" of manufacture B can be obtained, as shown in Eqs. (23) and (24):

$$\overline{U_{B1}}=yU_{BYES}+\left(1-y\right)U_{BNO} \tag{23}$$

$$f\left(y\right)=\frac{dx}{dt}=y\left(U_{BYES}-\overline{U_B}\right) \tag{24}$$

Like the vulnerability mining strategy, the stable equilibrium points $x^*$ and $y^*$ should be required before the stable strategy of the dynamic equation is solved, and the equilibrium points have to satisfy the following conditions:

$$f\left(x^*\right)=f\left(y^*\right)=0 \tag{25}$$

$$x^*=\frac{C_0}{\left(\mu_B K_A+K_B\right)\tau\left(1-\xi\right)\left(\psi-1\right)D_B\rho+P} \tag{26}$$

$$y^*=\frac{C_0}{\left(\mu_A K_B+K_B\right)\tau\left(1-\xi\right)\left(\psi-1\right)D_A\rho+P} \tag{27}$$

Finally, 5 balance points can be obtained, which are O(0,0), A(0,1), B(1,0), C(1,1), and D(x*,y*).

The partial derivatives of *x* and *y* can be solved based on the *f(x)* and *f(y)*, and the Jacobian matrix *I* can be obtained (Eq. (28)):

$$I=\begin{bmatrix}\dfrac{\partial f\left(x\right)}{\partial x} & \dfrac{\partial f\left(x\right)}{\partial y}\\ \dfrac{\partial f\left(y\right)}{\partial x} & \dfrac{\partial f\left(y\right)}{\partial y}\end{bmatrix}=\begin{bmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{bmatrix} \tag{28}$$

### 3.3 *Allocation of security protection resources for digital twins of industrial IoT*

#### *3.3.1 Game model of internet attack and defense.*

Typical industrial IoT security threats include phishing attacks, watering hole attacks, and service vulnerability exploitation. These attacks can usually bypass the corporate network firewall and penetrate the corporate internal network. The attack path of industrial IoT is shown in Fig.5. The attacker firstly obtains access to the factory's internal network through a variety of attack methods, and implants malicious programs into a computer on the factory's internal network. After that, the poisoned machine is undertaken as a springboard to spread through the network through a variety of transmission channels [43-44]. After infecting many devices, malicious programs can not only steal important production data, but also tamper with the control parameters of the control device and disrupt the production process. Once the attacker successfully enters the network, he can launch an attack on the process control and monitoring network. In response to these security threats, defenders can defend against malicious program access attacks by upgrading system vulnerability patches and deploying special industrial firewalls [45]. Defenders can also install specialized industrial anti-virus software to detect and kill malicious programs on devices supported by hardware resources, deploy industrial intrusion detection platforms to audit the internal network of the factory, and resist malicious programs' attacks on the industrial IoT. The attack and defense game for industrial IoT is shown in Fig.6.

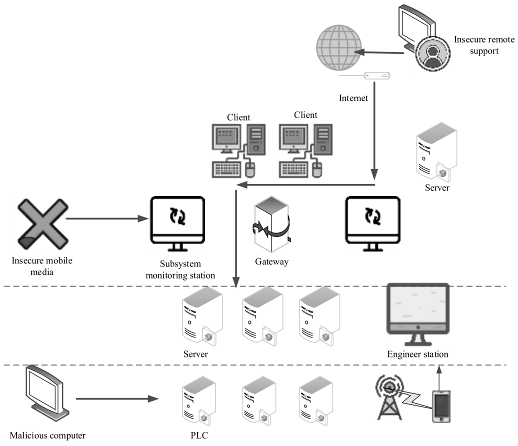


**Fig. 5.** The attack path of industrial IoT.

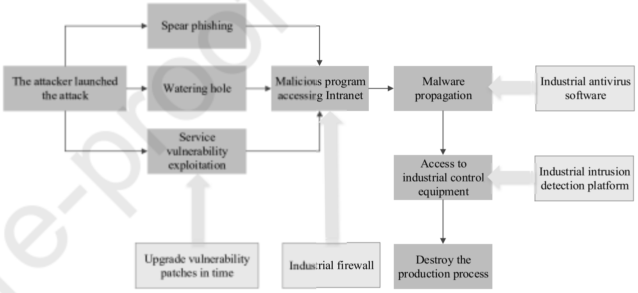

Spear phishing
The attacker launched the attack
Watering hole
Service vulnerability exploitation
Malicious program accessing Intranet
Malware propagation
Industrial antivirus software
Access to industrial control equipment
Industrial intrusion detection platform
Upgrade vulnerability patches in time
Industrial firewall
Destroy the production process

**Fig. 6.** The attack and defense game for industrial IoT.

The computing and bandwidth resources that can be invoked by the security protection measures in the industrial IoT are limited. Compared with traditional computer networks, industrial IoT shows high requirements for real-time and business continuity of industrial production because the network contains many industrial equipment such as Programmable Logic Controller (PLC) and radio frequency identification [46-48]. When industrial Internet security protection strategies are deployed, resource constraints need to be considered, and an optimized security protection effect can be obtained.

It is assumed that there are $n$ devices in a typical industrial IoT, which can be abstractly regarded as a scale-free network composed of $n$ nodes. The amount of defense resources allocated by the defender on node $l$ in the defense strategy $DS^i$ is denoted as $c_l^i$, and the selection state of the attacker on node $l$ in the attack strategy $AS^j$ is denoted as $q_l^j$. $C_D$ is supposed to be the total number of resources that can be used by the defender, and $V_A$ is supposed to be the total number of targets that can be attacked by the attacker synchronously. The conditions that the attack and defense game strategies need to meet are given as follows:

$$\sum_{l=1}^{n} c_l^i \le C_D \tag{29}$$

$$\sum_{l=1}^{n} q_l^j \le V_A \tag{30}$$

The revenue function of both attack and defense can be expressed as Eq. (31) and (32):

$$U_D\left(DS^i, AS^j\right)=-\sum_{l=1}^{n}\theta_l q_l^j\left(1-p_l^i\right)-\sum_{l=1}^{n}c_l^i \tag{31}$$

$$U_A\left(DS^i, AS^j\right)=\sum_{l=1}^{n}\theta_l q_l^j\left(1-p_l^i\right) \tag{32}$$

In the equations above, $\theta_l$ represents the importance of the node, $\sum_{l=1}^{n} c_l^i$ represents the cost of the defense strategy, and $p_l^i$ refers to the probability that the defender can successfully defend against attacks after deploying resources $c_l^i$ on node *l*.

In the attack and defense game, the goal of both parties is to maximize their respective income functions, and their optimal resource allocation strategy needs to satisfy the following equation:

$$\begin{cases} \forall DS^i, U_D\left(DS^*, AS^*\right) \geq U_D\left(DS^i, AS^*\right) \\ \forall AS^j, U_A\left(DS^*, AS^*\right) \geq U_D\left(DS^*, AS^j\right) \end{cases} \tag{33}$$

In the case of limited resource nodes, the equilibrium solution of the attack and defense game model can be transformed into a constrained multi-objective optimization, which can be expressed as equation (34) below:

$$\begin{cases} \max U_D\left(DS^*, AS^*\right) = -\sum_{l=1}^{n} \theta_l q_l^* \left(1 - p_l^*\right) - \sum_{l=1}^{n} c_l^* \\ \max U_A\left(DS^*, AS^*\right) = \sum_{l=1}^{n} \theta_l q_l^* \left(1 - p_l^*\right) \end{cases} \tag{34}$$

### *3.3.2 Balance solution of game model based on improved co-evolution algorithm.*

The game can be solved by co-evolutionary algorithms. This scheme takes into account the conflicts and effects among the populations and between the populations and the environment, and can be better adapted to the antagonism of the game. Weighed Clustering Algorithm (WCA) shows good global convergence and computational robustness, and is especially suitable for solving complex functions with high dimensions and multiple peaks. However, the basic WCA uses a random update mechanism, which greatly affects the performance of the algorithm's rapid convergence. Therefore, differential evolution is introduced into the update mechanism of WCA in this study, which can produce better replacement individuals with greater probability. The specific process of improving WCA is shown in Fig.7. The steps of the wolf colony update mechanism that introduces the idea of differential evolution can be described as follows:

(1) Variation: Two individuals in the head wolf and the wolf detective are selected randomly, which are defined as $X_i^k$ and $X_j^k$, respectively. The vector difference between the two is combined with the individual to be mutated to obtain the mutated individual. The specific mutation operation is shown in Eq. (35):

$$V_R^{k+1} = X_R^k + F \cdot \left(X_i^k - X_j^k\right) \tag{35}$$

In the equation above, $F$ is the scaling factor, and $X_R^k$ represents the individual to be replaced in the *kth* iteration.

(2) Cross: The cross operation is performed between $X_R^k$ and $V_R^{k+1}$ according to Eq. (36):

$$u_{R,d}^{k+1} = \begin{cases} v_{R,d}^{k+1}, & if\ rand \leq crossrate \\ x_{R,d}^{k}, & if\ rand > crossrate \end{cases} \tag{36}$$

In the Eq. (36) above, *crossrate* refers to the cross rate; $u_{R,d}^{k+1}$, $v_{R,d}^{k+1}$, and $x_{R,d}^{k}$ are the d-dimensional components of $U_R^{k+1}$, $V_R^{k+1}$, and $X_R^k$, respectively.

(3) Selection: The individuals with higher fitness are found according to the greedy algorithm of Eq. (37), and then the next-generation population is started:

$$X_{new}^{k+1} = \begin{cases} U_R^{k+1}, & if\ f\left(U_R^{k+1}\right) \geq f\left(X_R^k\right) \\ X_R^k, & if\ f\left(U_R^{k+1}\right) < f\left(X_R^k\right) \end{cases} \tag{37}$$

$f\left(U_R^{k+1}\right)$ and $f\left(X_R^k\right)$ in the above equation refer to the fitness functions of $U_R^{k+1}$ and $X_R^k$, respectively.

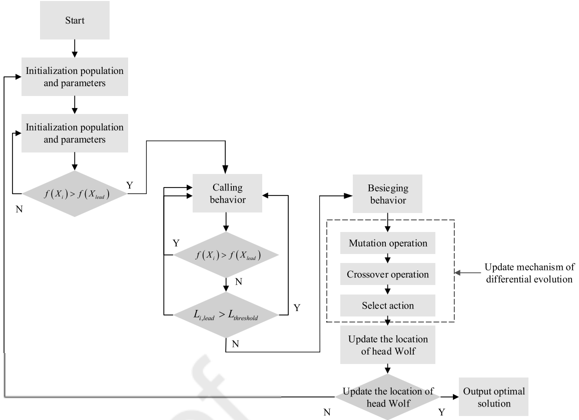

Start
Initialization population and parameters
Initialization population and parameters
$f(X_i) > f(X_{lead})$
Y
N
Calling behavior
Y
$f(X_i) > f(X_{lead})$
N
$L_{i,lead} > L_{threshold}$
Y
N
Besieging behavior
Mutation operation
Crossover operation
Select action
Update mechanism of differential evolution
Update the location of head Wolf
Update the location of head Wolf
N
Y
Output optimal solution

**Fig. 7.** Flow charts of improved WCA.

Defender and attacker strategy sets can construct two competitive populations, respectively. One strategy in the defender strategy set represents an individual in the population, and finally outputs the optimal strategy combination of attack and defense.

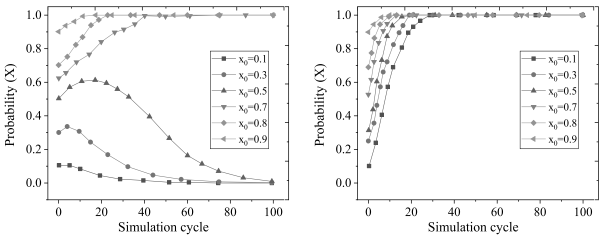
### 3.3.3 *Settings of simulation experiment.*

In the simulation experiment, Python is used to build a simulation program environment, the operating system is Windows 10, and the number of network nodes is set to 25. Wolf population size is set to $N = 50$, wolf detection scale factor is set to $\alpha = 4$, and the update scale factor is $\beta = 6$; in addition, $F = 0.6$, and $crossrate = 0.8$. The total number $C_D$ of defense resources of the defender is the main variable, which is determined as 200, 400, 600, 800, 1000, and 1200 for multiple experiments. The number of targets an attacker can attack at a time is set to $V_A = 5$. The experiment is performed for several times to reduce the influence of random factors. Finally, it is found that after 500 iterations, the co-evolution process will reach a plateau, so the maximum number of iterations is set to 500 in this study.

## **4. Results and discussion**

### *4.1 Analysis of game model of white hat security knowledge sharing*

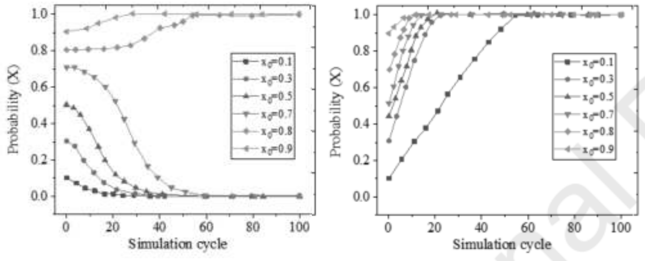
The influences of the initial probability of white hat to choose KSS on the evolution result are analyzed, and the results are shown in Fig.8. The initial probabilities of white hat 1 and white hat 2 to choose the KSS are denoted as *x₀* and *y₀*, respectively. Fig.8(a) illustrates that the convergence rate of the white hat 1 to choose KSS probability (X) is related to the probability *x₀* of choosing the KSS initially. In the evolutionary game, the greater the probability of white hat 1 choosing KSS, the faster the convergence rate. Fig.8(b) reveals that the probability of white hat 1 choosing KSS (X) is also related to the probability *y₀* of white hat 2 choosing KSS (X). When *y₀* = 0.9, X can converge quickly in a short time.



**(a)** $y_0 = 0.3$ **(b)** $y_0 = 0.9$

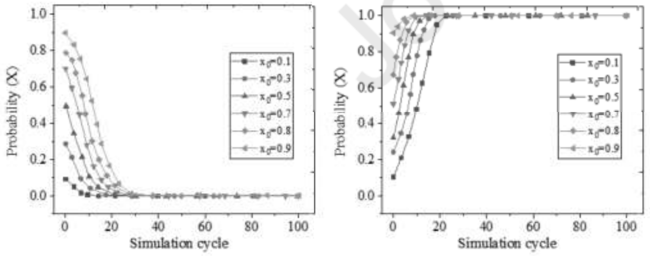
**Fig. 8.** The influence of different initial probabilities on the evolution results

Under the premise of $y_0 = 0.3$, the influence of trust degree $\omega_i$ on the evolution result of white hat to choose KSS is discussed and analyzed. When the value of $\omega_i$ is 0.3 and 0.5, the results obtained are shown in Fig.9. With the increase in trust, the strategy of "not sharing" chosen by the white hat 1 initially has changed into "sharing". This means that the more white hat 1 trusts other members of the team, the stronger its willingness to share knowledge. Under the premise of $y_0 = 0.3$, the influence of the change of the security knowledge value-added rate $\gamma$ on the evolution result of the white hat to choose KSS is analyzed further, and the results when the $\gamma$ is assigned as 0.3 and 0.6 are shown in Fig.10. It illustrates that with the increase of $\gamma$, the knowledge sharing stability strategy of white hat 1 gradually converges from "not sharing" to "sharing".



**(a)** $y_0 = 0.3$ $\omega_1$=0.3 **(b)** $y_0 = 0.3$ $\omega_1$=0.5

**Fig.** 9. The influence of trust degree on the evolution result.

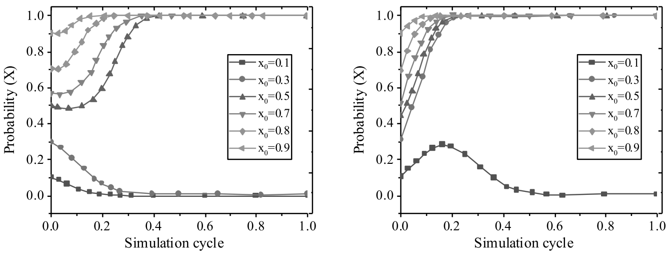


**(a)** $y_0 = 0.3$ $\gamma$=0.3 **(b)** $y_0 = 0.3$ $\gamma$=0.6

**Fig. 10.** The influence of the change of the security knowledge value-added rate on the evolution result.

### 4.2 *Simulation Analysis of Cooperative Game for the Vulnerability Patch Development*

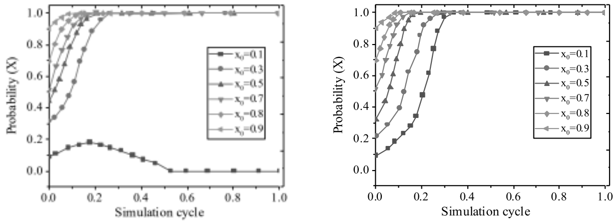
The influence of the initial probability of the manufacturer to choose "cooperative development" of vulnerability patch on the evolution result is analyzed, and the results are illustrated in Fig.11. The initial probabilities of manufacturer A and manufacturer B choosing the "cooperative development" strategy are set as $x_0$ and $y_0$, respectively. Fig.11 reveals that the probability curve of selecting the "cooperative development" strategy converges to zero when the $x_0$ is small and $y_0$ is specified; the probability curve gradually converges to 1 with the increase of $x_0$. The evolution trend and speed of the manufacturer's vulnerability patch development strategy are not only related to the probability of its initial selection of the "cooperative development" strategy, but also affected by the probability of manufacturer B's initial selection on the vulnerability patch development strategy.



**(a)** $y_0 = 0.3$ **(b)** $y_0 = 0.3$

**Fig. 11.** The influence of the initial probability of the manufacturer for vulnerability patch on the evolution result.

Under the premise of $y_0 = 0.3$, the influence of the probability $\rho$ of a successful hacker intrusion on the patch development strategy before the vulnerability is fully disclosed is analyzed, as shown in Fig.12. Since the probability of a hacker's successful intrusion is very low before the vulnerability is fully disclosed, the value of $\rho$ is assigned as 0.1 and 0.01, respectively. With the increase of ρ, the cooperative development strategy of vendor *A* changes from "not sharing" to "sharing". As shown from the sensitivity of changes, a slight increase in the probability of successful hacking before full disclosure will prompt manufacturers to cooperate in developing patches to defend against hacker attacks.



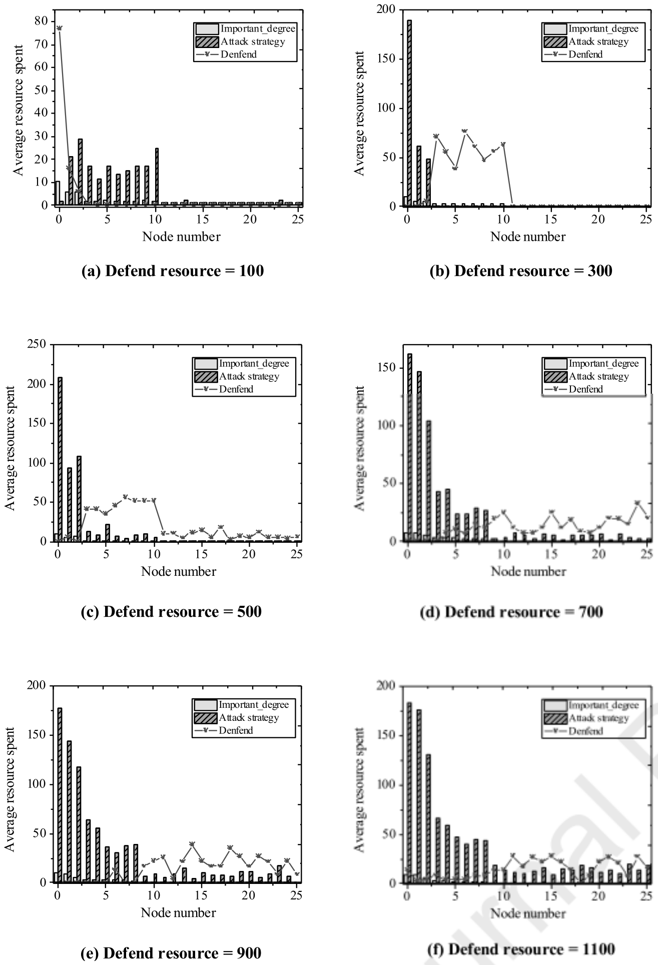
**(a)** $y_0 = 0.3$ $\rho = 0.01$ **(b)** $y_0 = 0.3$ $\rho = 0.1$

**Fig. 12.** The influence of the probability of a successful hacker intrusion on the patch development strategy.

### 4.3 *Solution for optimal strategy to defender*

An improved wolf colony-co-evolution algorithm is adopted to solve the optimal defense strategy under different total security protection resources. Fig.13(a~f) show the attacker's target selection strategy and the defender's resource allocation strategy under different attack coverage conditions. The strategies shown in the figures are the average values obtained after the experiment is repeated 20 times. As given in the figures, when the total amount of security protection resources is small, the defender will allocate all resources to the three most important defense nodes, and the remaining nodes are basically not allocated with defense resources.

In this case, the attacker attacks the nodes that do not have defense resources. As the total number of security defense resources increases, the security defense resources allocated to less important nodes increase, but are still limited. In this case, the attacker will transfer the attack target to a node of lower importance according to the number of security protection resources allocated to each node. Therefore, the optimal resource allocation strategy of the defender should allocate resources according to the importance of the nodes. When the resources are insufficient, the nodes with low importance can be abandoned and the nodes with high importance can be protected.



**(a) Defend resource = 100**

**(b) Defend resource = 300**

**(c) Defend resource = 500**

**(d) Defend resource = 700**

**(e) Defend resource = 900**

**(f) Defend resource = 1100**

**Fig. 13.** Comparison of attack defense strategies under different total security protection resources.

## 5. Conclusions

Facing the multi-dimensional and full-scenario ubiquitous connection that continues to increase in future networks, the digital twins network will become a new direction for future network planning, operation, management, and running, and an important means to realize network intelligence and automation. The holographic presentation of the virtual and real interaction mapping of the network will help users perceive the network status more clearly, mine valuable information on the network more efficiently, and explore innovative network applications with a friendlier immersive interactive interface. With the support of interactive visualization technology, the digital twins network can obviously improve the level of holographic presentation of the network. Not only can various network elements and topology information in the network be dynamically visualized, but the dynamic change process, real-time status, and future evolution direction of the full life cycle of the network can also be presented to users along with the digital twins network model. In the digital twins of industrial networks, many network nodes are involved, so the risk of network attacks is very high. Moreover, the integration of various emerging technologies such as cloud computing and IoT has made network security issues more complex and changeable.

Aiming to protect the industrial Internet security, this study explores the mining and repair of vulnerabilities based on the evolutionary game theory from the perspective of the life cycle of network security vulnerabilities to promote the effective repair of vulnerabilities in the digital twins network. During the vulnerability mining, the KSS among the white hat temporary teams is related to factors such as the amount of knowledge sharing, the cost of knowledge sharing, the rate of knowledge appreciation, and the probability of obtaining team rewards. It is found that with the increase of trust and the increase of knowledge appreciation rate, the probability of white hats choosing KSS is greater. Therefore, establishing trust can reduce the communication cost among white hats and elevate the willingness to share; and training activities can be organized to improve the knowledge sharing ability of white hats. From the perspective of vulnerability repair, whether the manufacturer chooses to cooperate in developing vulnerability patches is related to the probability of successful hacking before the vulnerability is fully disclosed. Before the vulnerability is fully disclosed, a slight increase in the probability of successful hacking will prompt manufacturers to cooperate in developing patches to defend against hacker attacks. Therefore, for the security resource allocation after the game between the attacker and the defender in the digital twins network, an improved algorithm that combines WCA and the co-evolutionary algorithm is proposed in this study, which is verified by simulation experiments to effectively solve the Nash equilibrium of the game model. Based on game theory, this work has made some progress in information security strategy selection of industrial digital twins networks. However, in the actual network environment, there are many random interference factors in the process of attack and defense, such as the change of the system operating environment, which will lead to the change of the game model. In the future research, the stochastic factors should be included to further refine the game model.

## Acknowledgements

## Aheadings in appendices

## References

[1] T. Wang, J. Li, Z. Kong, Digital twin improved via visual question answering for vision-language interactive mode in human–machine collaboration, Journal of Manufacturing Systems, 58 (2021) 261-269.

[2] Y. Fang, C. Peng, P. Lou, Digital-twin-based job shop scheduling toward smart manu facturing, IEEE Transactions on Industrial Informatics, 15(12) (2019) 6425-6435.

[3] Y. Ham, J. Kim, Participatory Sensing and digital twin city: Updating virtual city models for enhanced risk-informed decision-making, Journal of Management in Engineering, 36(3) (2020) 04020005.

[4] H. Guo, M. Chen, K, Mohamed, A digital twin-based flexible cellular manufacturing for optimization of air conditioner line, Journal of Manufacturing Systems, 58 (2021) 65-78.

[5] K. Xia, C. Sacco, M. Kirkpatrick, A digital twin to train deep reinforcement learning agent for smart manufacturing plants: Environment, interfaces and intelligence, Journal of Manufacturing Systems, 58 (2021) 210-230.

[6] Y. He, J. Guo, X. Zheng, From surveillance to digital twin: Challenges and recent advances of signal processing for industrial internet of things, IEEE Signal Processing Magazine, 35(5) (2018) 120-129.

[7] S. Aheleroff, X. Xu, R. Y. Zhong, Digital twin as a service (DTaaS) in industry 4.0: an architecture reference model, Advanced Engineering Informatics, 47 (2021) 101225.

[8] V. Kharchenko, O. Morozova, O. Illiashenko, A Digital Twin for the Logistics System of a Manufacturing Enterprise Using Industrial IoT, Information & Security, 47(1) (2020) 125-134.

[9] M. Wollschlaeger, T. Sauter, J. Jasperneite, The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0, IEEE industrial electronics magazine, 11(1) (2017) 17-27.

[10] F. Tao, J. Cheng, Q. Qi, IIHub: An industrial Internet-of-Things hub toward smart manufacturing based on cyber-physical system, IEEE Transactions on Industrial Informatics, 14(5) (2017) 2271-2280.

[11] T. Gebremichael, L. P. I. Ledwaba, M. H. Eldefrawy, Security and privacy in the industrial internet of things: current standards and future challenges, IEEE Access, 8 (2020) 152351-152366.

[12] C. Gehrmann, M. Gunnarsson, A digital twin based industrial automation and control system security architecture, IEEE Transactions on Industrial Informatics, 16(1) (2019) 669-680.

[13] V. Hassija, V. Chamola, V. Saxena, A survey on IoT security: application areas, security threats, and solution architectures, IEEE Access, 7 (2019) 82721-82743.

[14] G. Srivastava, R. M. Parizi, A, Dehghantanha. The future of blockchain technology in healthcare internet of things security, Blockchain Cybersecurity, Trust and Privacy, (2020) 161-184.

[15] S. Lee, S. Kim, K. Choi, Game theory-based security vulnerability quantification for social internet of things, Future Generation Computer Systems, 82 (2018) 752-760.

[16] F. Kong, Y. Zhou, B. Xia, A security reputation model for IoT health data using S-Alex Net and dynamic game theory in cloud computing Environment, IEEE Access, 7 (2019) 161822-161830.

[17] V. Kiran, S. Rani, P. Singh, Towards a Light Weight Routing Security in IoT Using Non-cooperative Game Models and Dempster–Shaffer Theory, Wireless Personal Communications, 110(4) (2020) 1729-1749.

[18] J. Cheng, H. Zhang, F. Tao, DT-II: Digital twin enhanced Industrial Internet reference framework towards smart manufacturing, Robotics and Computer-Integrated Manufacturing, 62 (2020) 101881.

[19] K. T. Park, Y. W. Nam, H. S. Lee, Design and implementation of a digital twin application for a connected micro smart factory, International Journal of Computer Integrated Manufacturing, 32(6) (2019) 596-614.

[20] S. West, O. Stoll, J. Meierhofer, Digital twin providing new opportunities for value co-creation through supporting decision-making, Applied Sciences, 11(9) (2021) 3750.

[21] R. Rocca, P. Rosa, C. Sassanelli, Integrating virtual reality and digital twin in circular economy practices: a laboratory application case, Sustainability, 12(6) (2020) 2286.

[22] C. Zhuang, J. Liu, H. Xiong, Digital twin-based smart production management and control framework for the complex product assembly shop-floor, The International Journal of Advanced Manufacturing Technology, 96(1) (2018) 1149-1163.

[23] H. Jiang, S. Qin, J. Fu, How to model and implement connections between physical and virtual models for digital twin application, Journal of Manufacturing Systems, 58 (2021) 36-51.

[24] G. Wang, G. Zhang, X. Guo, Digital twin-driven service model and optimal allocation of manufacturing resources in shared manufacturing, Journal of Manufacturing Systems, 59 (2021) 165-179.

[25] T. Kong, T. Hu, T. Zhou, Data construction method for the applications of workshop digital twin system, Journal of Manufacturing Systems, 58 (2021) 323-328.

[26] C. Zhuang, J. Gong, J. Liu, Digital twin-based assembly data management and process traceability for complex products, Journal of manufacturing systems, 58 (2021) 118-131.

[27] D. Jones, C. Snider, A. Nassehi, Characterising the Digital Twin: A systematic literature review, CIRP Journal of Manufacturing Science and Technology, 29 36-52.

[28] C. Wu, Y. Zhou, M. V. P. Pessôa, Conceptual digital twin modeling based on an integrated five-dimensional framework and TRIZ function model, Journal of manufacturing systems, 58 (2021) 79-93.

[29] T. Wang, J. Li, Z. Kong, Digital twin improved via visual question answering for vision-language interactive mode in human–machine collaboration, Journal of Manufacturing Systems, 58 (2021) 261-269.

[30] Y. H. Pan, T. Qu, N. Q Wu, Digital Twin Based Real-time Production Logistics Synchronization System in a Multi-level Computing Architecture, Journal of Manufacturing Systems, 58 (2021) 246-260.

[31] J. A. Marques, M. C. Luizelli, R. Filho, An optimization-based approach for efficient network monitoring using in-band network telemetry, Journal of Internet Services and Applications, 10(1) (2019) 1-20.

[32] S. Tang, D. Li, B. Niu, Sel-INT: A runtime-programmable selective in-band network telemetry system, IEEE transactions on network and service management, 17(2) (2019) 708-721.

[33] J. Hyun, Tu. N. Van, J. H. Yoo, Real−time and fine−grained network monitoring using in−band network telemetry, International Journal of Network Management, 29(6) e2080.

[34] H. Bouali, J. Akaichi, A, Gaaloul. Real-time data warehouse loading methodology and architecture: a healthcare use case, International Journal of Data Analysis Techniques and Strategies, 11(4) (2019) 310-327.

[35] V. Havard, B. Jeanne, M. Lacomblez, Digital twin and virtual reality: a co-simulation environment for design and assessment of industrial workstations, Production & Manufacturing Research, 7(1) (2019) 472-489.

[36] Y. Fan, J. Yang, J. Chen, A digital-twin visualized architecture for Flexible Manufacturing System, Journal of Manufacturing Systems, 60) 176-201.

[37] J. Bao, D. Guo, J. Li, The modelling and operations for the digital twin in the context of manufacturing, Enterprise Information Systems, 13(4) (2019) 534-556.

[38] M. Taddeo, T. McCutcheon, L. Floridi, Trusting artificial intelligence in cybersecurity is a double-edged sword, Nature Machine Intelligence, 1(12) (2019) 557-560.

[39] V. Mullet, P. Sondi, E. Ramat, A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0, IEEE Access, 9 (2021) 23235-23263.

[40] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions, Accident Analysis & Prevention, 148 (2020) 105837.

[41] S. Yamaguchi, White-hat worm to fight malware and its evaluation by agent-oriented Petri nets, Sensors, 20(2) (2020) 556.

[42] C. D. Martin Taking the high road white hat, black hat: the ethics of cybersecurity, ACM Inroads, 8(1) (2017) 33-35.

[43] Y. Xiang, L. Wang, A game-theoretic study of load redistribution attack and defense in power systems, Electric Power Systems Research, 151 (2017) 12-25.

[44] H. Hu, Y. Liu, C. Chen, Optimal decision making approach for cyber security defense using evolutionary game, IEEE Transactions on Network and Service Management, 17(3) (2020) 1683-1700.

[45] Q. Wang, W. Tai, Y. Tang, A two-layer game theoretical attack-defense model for a false data injection attack against power systems,International Journal of Electrical Power & Energy Systems, 104 (2019) 169-177.

[46] S. G. Pease, P. P. Conway, A. A West. Hybrid ToF and RSSI real-time semantic tracking with an adaptive industrial internet of things architecture, Journal of Network and Computer Applications, 99 (2017) 98-109.

[47] S. G. Pease, R. Trueman, C. Davies, An intelligent real-time cyber-physical toolset for energy and process prediction and optimisation in the future industrial Internet of Things, Future Generation Computer Systems, 79 (2018) 815-829.

[48] J. Zhang, X. Qu, A. K. Sangaiah, A study of green development mode and total factor productivity of the food industry based on the industrial internet of things, IEEE Communications Magazine, 56(5) (2018) 72-78.

**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: