Research on Network Security Situation Awareness and Dynamic Game Based on Deep Q Learning Network

Xian Guo, Jianing Yang, Zhanhui Gang, An Yang*

China Industrial Control Systems Cyber Emergency Response Team, China
gxpaper17@163.com, jn_young90@126.com, gangzhanhui@163.com, whomya@163.com

Abstract

In today's increasingly complex network environment, increasingly severe network attacks, and real-time dynamic changes in offensive and defensive scenarios, network security technology has also evolved from passive security to active security technology, and expanded from analyzing unilateral security elements to comprehensively analyzing overall network security. Aiming at the problem of inaccurate assessment results due to the lack of comprehensive analysis of threat information, protection information and environmental information in existing assessment methods, this paper proposes a defensive random game model. This model analyzes threat propagation and establishes a threat propagation access relationship network, and then establishes a random game model for the game process of threat action and protection strategy implementation to solve the mixed strategy Nash equilibrium. The model comprehensively analyzes the dynamic changes of the security situation elements, ignoring the short-term situation elements that will not change, such as topology structure, service information, etc., and mainly analyzes the dynamic changes of attack information, vulnerability information, and defense measures, and predicts from the host and network levels. The experimental verification shows that the prediction method in this paper can improve the prediction accuracy and is more in line with the offensive and defensive scenarios.

Keywords: NSSA, NSSP, Stochastic game model threat propagation, Deep Q learning, Security situation elements

1 Introduction

Systematic and rational logistics management has become a favorable condition related to computer networks has made the network an indispensable part of people's work and life. With the increasing development of network technology and the increasing complexity of network system structure. Hundreds of millions of Youku information data are sold on the dark web, the "dark cloud" virus has swept back, and the new "worm" ransomware WannaCry swept the world frequently. How to ensure that network users enjoy the fruitful results brought by network technology while avoiding the threat of network security incidents has become an issue of increasing concern to society. The successive promulgation of the "National Cyberspace Security Strategy" and the "Cyber Security Law" mean that the issue of cyber security has risen to the level of national strategy, which has attracted great attention from all parties.

Faced with the severe network security situation, security researchers have conducted in-depth research on attack threats, network vulnerabilities, etc., and already have relatively mature network security technologies, such as antivirus software, protective wall technology, intrusion detection technology, VPN technology, Security scanning technology, etc. A hardware or software program that monitors a network for malicious activity or policy breaches is known as an intrusion detection system (IDS). A network security tool called an intrusion detection system (IDS) was initially developed to identify vulnerability exploits against specific applications or computers. It is software that checks a system or network for malicious activities or policy violations. A security information and event management system are often used to report or gather any harmful activity or violation. A virtual private network (VPN) is a network security technique that establishes a secure and encrypted connection across an insecure network, such as the internet. Through the use of a virtual private network (VPN), a secure and encrypted connection can be established over a less secure network, such the internet. Using a public network like the internet, a virtual private network can be used to extend a private network. A virtual private network (VPN) is a technique of extending a private network across a public network like the internet. Security scanning, often known as vulnerability scanning, is the process of looking for vulnerabilities or undesired file modifications on a website, web-based software, network, or file system. These security technologies solve security problems from different entry points. Each technology and its products can only solve a relatively single network security problem. Its functions are relatively scattered and single, and have specific and limited characteristics. For example, firewall technology is through software The technology combined with hardware isolates direct communication between internal and external networks to achieve access control technology that protects computer network security; intrusion detection realizes active defense network security technology through the discovery of network attacks and intrusions, and discovers through real-time monitoring of computer networks Whether there is a network attack or other suspicious behavior.

Due to the limitations of its own technology, network

*Corresponding Author: Jianing Yang; E-mail: jn_young90@126.com
DOI: 10.53106/160792642023032402030

security technologies with only a single function cannot provide network managers with global information, which affects the managers' ability to respond to the network's global response and decision-making. If you simply aggregate the massive and heterogeneous information generated by these security products, it will not only bring heavy computing and storage burdens, but also drown valuable information in the massive information. How to comprehensively, accurately, and real-timely assess the network security status, make security management change from passive to active, and predict development trends, effectively reduce threats and damages, has become the focus of increasing attention.

Network security situational awareness technology has developed in this context. Network security situational awareness (NSSA) incorporates security monitoring, security visualization, detection methods, data fusion, automation, dynamism, and complexity to attain greater degrees of situation awareness. NSSA is a process of a comprehensive analysis of network security status. NSSA mainly includes four key technologies: situation data acquisition technology. Among them, situation understanding technology and situation prediction technology are key parts. Situation assessment is the main content. NSSA realizes situation analysis and prediction through various security analysis technologies based on historical and current knowledge, providing conditions for improving the network and various equipment functions in the network, and improving the network's own defense capabilities. The required time and the space the security will be used as the environmental threat for both the comprehensive the status for the future. The simulation is all within the structure and the context of the internet and it is managed by the tools which provide the essential information about the network security. Deep Q learning is a regular neural network that helps in the mapping action of the neural networks in the q-network for the maximum output of the deep reinforcement of the Q-learning. It makes the formation of the Q-value function in both the input and the output values which makes the generated output for the q-Value

1.1 Article Contribution

- The dynamic game based on a deep Q learning Network analyzes the changes of the security situation elements.
- the existing situation assessment and prediction technology is achieved by the game-based network.
- The prediction accuracy is improved by the experimental verification with the offensive and defensive scenarios.
- The attack information, vulnerability information, and defense measures were analyzed by the dynamic changes of the model.

1.2 Article Sectional Organization:

The remaining of the article is discussed as follows.

- Section 1 addresses the introduction
- Section 2 addresses the Literature review enumerates the existing methods related to the article
- Section 3 elucidates the Research on Game theory
- Section 4 discuss the experimental result analysis
- Finally, section 5 concludes the research article

2 Literature Review

2.1 Cybersecurity Situational Awareness

In the direction of network security situation assessment technology, Designed and implemented an attack situation assessment software system called SSARE, which is based on questionnaires to realize computer attack detection and NSSE. The real-time situational awareness in distributed networks is integrated with the existing network security systems, and proposed an NSSE model for distributed networks. Further the network system is divided into several levels: system, host, service, etc., and proposed a hierarchical network situation assessment method for situation awareness [1]. After that, based on the analytic hierarchy process, researchers comprehensively used fuzzy the evaluation matrix, game theory, etc. to improve the hierarchical method. The evaluation matrix enables users to compare different ideas and rate them according to a set of criteria in order to find the ones that are the most potential. The amount of difficulty associated with concept execution, as well as the level of value they will provide to the user and the organization, are two common factors. The use of neural networks is proposed to evaluate and predict NSS based on the uncertainty of security factors, and reduce the impact of objective factors [2]. This method first establishes evaluation indicators, and then evaluates NSS based on BP (Back Propagation) neural network. The logs of equipment such as IDS, firewalls, host systems, anti-virus software, etc. were fused through DS evidence theory to obtain potential threats [3-4]. And integrate the CVE vulnerability database information to finally get the real threat information to evaluate the situation. The Common Vulnerabilities and Exposures (CVE) database contains information security problems that have been made public. One vulnerability from the list is identified exclusively by a CVE number. Hidden Markov Model to model the network state and use statistical model characteristics to reduce the impact of the variability of information on the evaluation in response to the misreporting and underreporting of alarm information in massive data [5]. The Hidden Markov Model (HMM) is a straightforward method for modeling sequential data. The term "hidden Markov model" refers to the fact that the Markov Model generating the data is hidden or unknown to the user. More particular, users only have access to observational data, not state-level information.

Figure 1 shows network security situation prediction steps and predicts the level of the situation. Data preparation. Data normalization, Salient asset identification, situation assessment, and prediction are the major steps of prediction and the subprocess takes place in between like alert procurement and alert formatting, etc.,

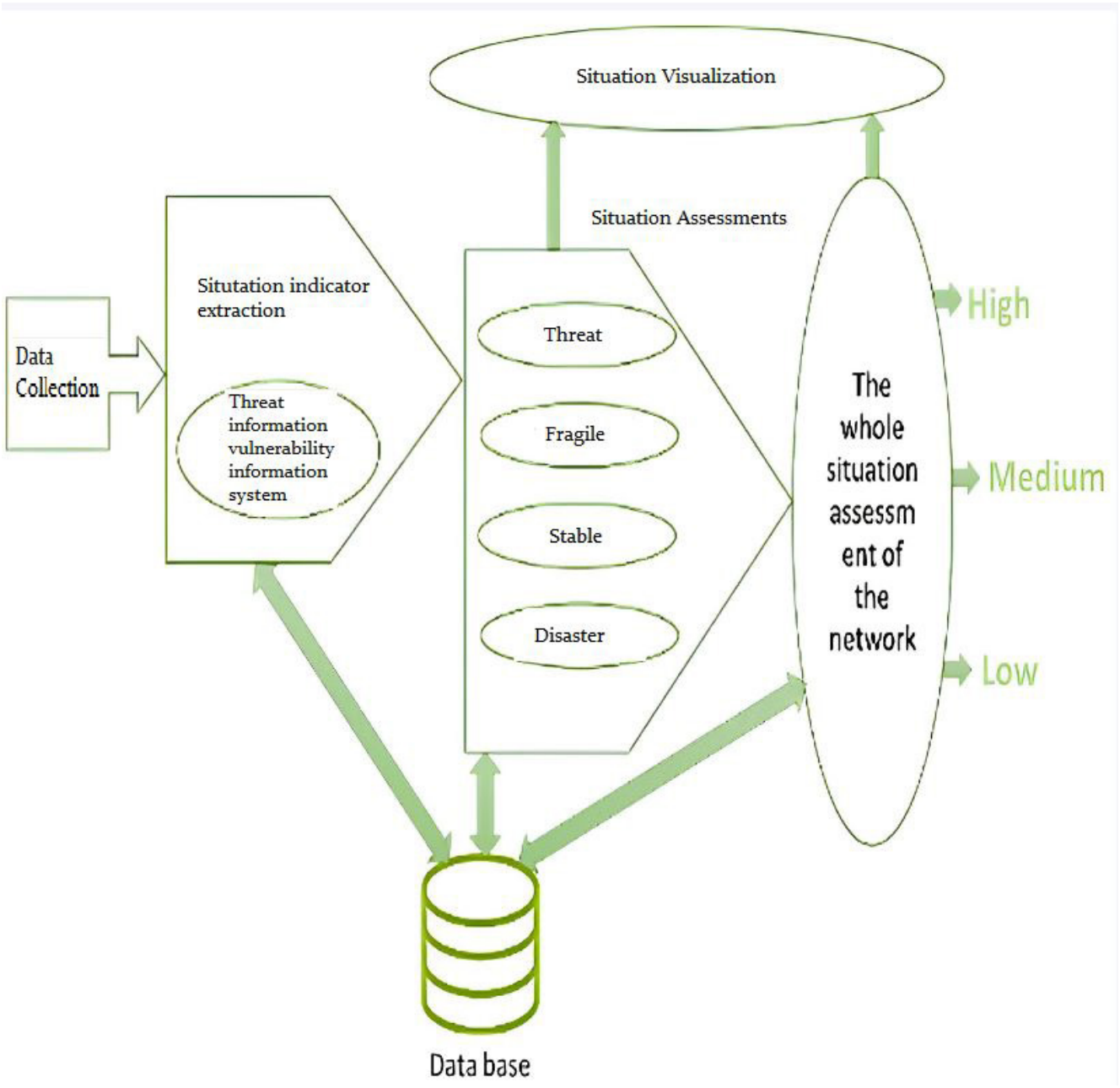


Figure 1. Network security situation prediction

In terms of network security situation prediction (NSSP for short), as early as 1999, the Information Assurance Advisory Council organized the threat assessment and early warning of cyber-attacks. By studying the threat trend analysis process, The model predicts the real-time change flow of network traffic when the network encounters threats [6]. A threat analysis is a procedure used to identify which system components must be safeguarded and the kinds of security dangers (threats) against which they should be protected. The security status of the future network. Uses the autoregressive moving average model (ARMA) to predict the time series generated by the network security situation, but ARMA requires that the target sequence be processed [7]. ARIMA, or autoregressive integrated moving average, is a statistical analysis model that uses time-series data to better recognize the data set or forecast future trends. If a statistical model predicts future values from previous values, it is called autoregressive. Using the Mar Kofu process revises the prediction result. However, the modeling process is quite complicated [8]. The NSSP method is proposed and they pointed out that RBF has a better prediction effect [9]. Based on previous and current security situation data, Network Security Situation Prediction produces quantitative predictions of incoming network security posture. The neural network has the advantages of distribution and self-organizing learning, etc., and it has a high value in dealing with forecasting problems with the characteristics of multi-variable and non-linear forecasting. Proposed a combination of SCGM (1_1) c model and immune principle to realize situation prediction [10]. Realized the real-time prediction, collected IDS alarm log information and network asset information, took the attack sequence as the observation

object, the network security state was the hidden state, and the forward method was used for prediction [11]. An intrusion detection system (IDS) analyzes network traffic for unusual behavior and issues notifications when it is detected. An intrusion detection system (IDS) may be used to assist assess the number and types of attacks. This information may be used by businesses to improve their security systems or adopt more effective controls. In addition, an intrusion detection system may assist businesses in identifying flaws or issues with their network device designs.

Radiofrequency identification technology (English abbreviation, also known as electronic label technology, rose in the century, is currently a relatively advanced non-contact automatic identification technology, its working principle is to use radio frequency signals to achieve non-contact automatic identification through space assistance Target objects and obtain relevant data and deliver relevant information [7-12]. A system called Radio Frequency Identification (RFID) uses radio waves to passively identify tagged objects. It is employed in a variety of commercial and industrial applications, including inventory management and the tracking of library checkouts. A sensor (is a device that can perceive certain information and convert it into other forms of signals according to certain rules. It is a detection device that realizes automatic detection and automatic control. It can achieve the transmission, processing, storage, and storage of information. Display, record and control requirements [13-16]. Figure 2 shows the Endsley situational awareness conceptual model diagram.

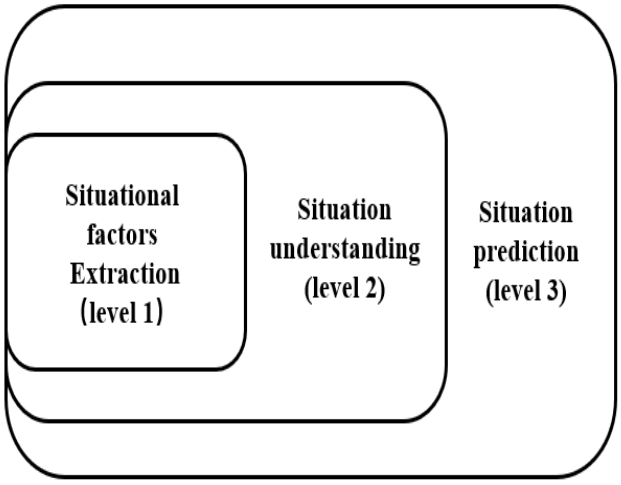


Figure 2. Endsley situational awareness conceptual model diagram

Endsley's situational awareness model depicts three stages or processes in the development of SA states: perception, understanding, and projection. The three hierarchical stages of situational evaluation in Endsley's paradigm each serve as a required (but insufficient) stepping stone to the subsequent, higher level. From perception to interpretation to prediction, this model follows a cycle of information processing. Perceiving the status, qualities, and dynamics of important items in the environment is the initial step toward obtaining SA.

Level 1 Situation Awareness is the perception of the environment's aspects. This is the process of identifying the important parts or «events» that, when taken together, help to describe the scenario. This level semantically marks significant parts of the scenario for later processing at higher levels of abstraction.

Level 2 Situation Awareness has the ability to comprehend the current situation. This is the assemblage of level 1 events into a larger, more holistic pattern, or tactical scenario. This level is used to characterize the present situation in words that are operationally relevant in order to facilitate quick decision-making and action.

Level 3 Situation Awareness entails predicting future events. This is a forecast of the tactical situation based on the current circumstances. When time allows, this level facilitates short-term planning and option evaluation.

2.2 Research on Game Theory in the Security Field

Game theory means that in a certain information environment, the participant chooses a certain strategy to maximize the benefits of itself, and studies the issue of the balance of strategies between different participants. It is also called game theory. Game theory is widely used in economics, mathematics, and other fields, and the application of game theory in the field of network security is becoming more and more extensive [12]. The application in this field can be summarized into two aspects: attack defense analysis and security measurement [13]. A tool employed by analysts in traditional psychoanalysis is the analysis of defenses. In order to comprehend a patient's subconscious mind more fully, it alludes to the study of defense pictures that show up in dreams. Attack models in quantitative analysis reveal information about the underlying security-critical systems. Knowing how such systems behave over time allows us to determine if the chance of a system being penetrated is less than a crucial threshold at any particular moment.

On the one hand, attack defense analysis (quantitative decision-making) refers to constructing a game model based on the game process of the offensive and defensive parties. Offensive behavior is defined as a proactive assault that employs force and hostility, whereas defensive behavior is defined as a reactive action that uses force and aggression to defend oneself from an attack. In games, a defensive strategy seeks to prevent the other side from scoring, whereas an offensive strategy is to score against the opposing team. Game theory solves the problem of competition among multiple participants with opposing goals. On the other hand, security measurement is an important research direction of network security, which is the evaluation of target security attributes and security status. Security measurement based on game theory refers to predicting the strategies of both offensive and defensive parties and evaluating network security on this basis. Network security measurement is a large category, the results of which are affected by the interaction between attackers and defenders. For example, one indicator of risk assessment is the likelihood of a network being attacked.

The NSSA method is proposed, however in the comprehensive analysis of the game, the profit calculation of the participants did not consider the cost issue and only

considered the maximum situation assessment under the minimum strategy lacks the calculation strategy Nash equilibrium, which makes the result accuracy not high [14]. Even if there is no dominating strategy, a game has a Nash equilibrium. It's also feasible for a game to have more than one Nash equilibrium. A subgame perfect equilibrium is a subgame perfect equilibrium in game theory. A Nash equilibrium utilized in dynamic games is a refinement of a Nash equilibrium. The strategy profile provides a Nash equilibrium for every subgame of the original game. Designed a game-theoretical framework based on the attacker, the defender, and the user [15]. Established a random game model with imperfect information describing the game state between users and administrators [12]. Proposed a method in a distributed network attack environment [16]. This method takes advantage of the defender's advantage in obtaining information rights and imitates the attack behavior based on the different capabilities of the offensive and defensive parties to obtain information due to different permissions. The attacker is induced to conduct attacking behaviors so that the defender's benefit is optimized. However, the game model only considers the increase of the defender's income without considering the attacker, which has certain limitations.

The new sensor technology is constantly developing towards miniaturization, multi-functionalization, digitization, intelligence, systemization, and networking. At present, sensors are in a period of transition from traditional to new sensors. After years of technological improvement, sensors are divided into three generations according to their technological advancement: first, structural sensors, which mainly use changes in structural parameters to collect and read and write signals; secondly, solid sensors, which use materials Some characteristics are made, and its characteristic is that the function of the sensor varies according to the different materials used. For example, the use of photosensitive materials to make photosensitive sensors; the last is smart sensors, this type of sensor is composed of micro-processing technology and detection technology, and its main feature is intelligent characteristics [17-20]. After long-term development, sensor technology has become a catalyst for the transformation and upgrading of traditional industries, and it is expected to become an economic growth point for a new type of industry. The time series for the depth network will be in the LTE communication system for the long and the short-term channel occupancy for the authorized historical moments for the guide of the simulations. The speed communication of the long-term railway evaluation is done by the authorization of the channel to find the current formation of the dynamic spectrum of the authorization channels. This study is used in the access of the LSTM network to manage the authorization of the channels. The population growth of the twenty-first century will be managing the food security and the efficiency of the agricultural system of the weather conditions will definitely make the lack of transparency of the multi-network system it manages the decision support system to maintain the deep Q-learning process. This is presented by the filtering and the integration of the network access. This study was used in managing the sustainability of the deep Q learning algorithm.

3 Preliminaries

3.1 Cybersecurity Situational Awareness

According to Endssley's conceptual model of situational awareness, network attack information, network vulnerability data, etc. Data preprocessing is to perform correlation analysis and data fusion after obtaining massive and redundant network security data information to obtain a standardized and standardized data collection. Correlation analysis is used to determine the degree and direction of a link between two variables. Correlation analysis is used in the handling of security events to uncover inter-relationships between security data in order to produce effective security events, analyze these security events, and give technical guidance for network management. The analysis of numerous interconnected datasets that give complementary viewpoints of the same phenomena is known as data fusion. Correlating and fusing data from several sources allows for more accurate inferences than analysing a single dataset alone. Then take the data set as input and use a suitable model to quantitatively analyze the network state. Situation forecasting obtains the development trend of the security state by analyzing historical and existing data and using appropriate models.

Situational awareness technologies are intended to improve operational decision-making from the top down. Decision-makers in a range of businesses have long recognized the importance of situational awareness. Situational awareness technology can be applied in fields such as network security and industrial control. The same framework is applied to different problems, so situational awareness and NSSA are analogous to types and examples. In summary, the following definitions can be given:

Definition 1 Network Security Situation (NSS): refers to obtaining a comprehensive value that can represent its security status based on various related security data in the network system. NSSA technology mainly includes 4 key technologies: situational data acquisition, situational understanding, NSSP technology and visual analysis technology. The network security status prediction (NSSP) examines previous network data and forecasts the network condition in order to warn of potential future network dangers. Predicting network security situations can help with network defense, network security warning, and network resource allocation. Further, the use of sophisticated tools and procedures to evaluate datasets using visual representations of the data is known as visual analytics. Data visualization via graphs, charts, and maps assists users in identifying trends and developing actionable insights. These data-driven insights assist businesses in making better decisions. The key technology of situational understanding technology is NSSE. The complete NSSA process is shown in Figure 3.

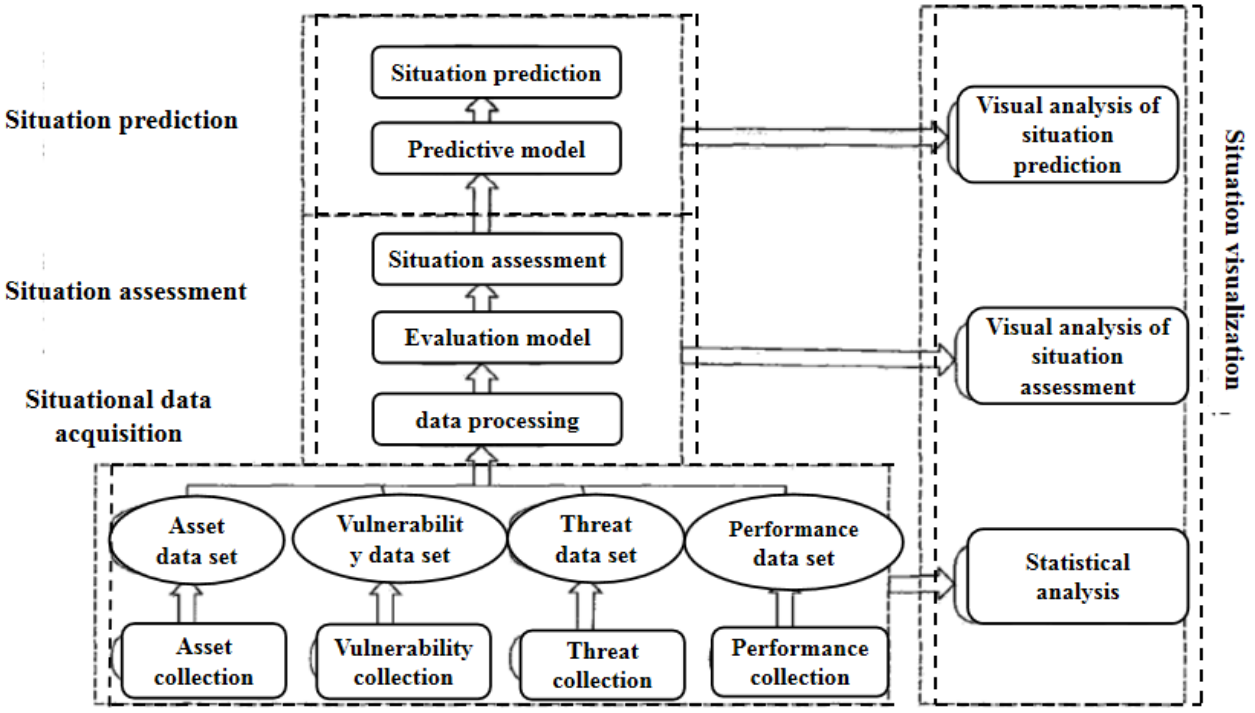


Figure 3. NSSA flow chart

The situation prediction, situation assessment and situational data acquisition are processed for situation visualization in the NSSA flowchart. The process flow of NSSA is shown in the above Figure 3, the process begins with the acquisition of situational data's namely asset, vulnerability, threat and performance these acquired data are processed in the data processing module, then it moves to the evaluation model where the datas are evaluated for security after the evaluation assessment of situation takes place and in the situation prediction phase there are two modules predictive model, situation prediction. In the visualization phase of situation the visual analysis is made for the situation prediction and also for situation assessment, the statistical analysis is considered for the data acquisition phase of NSS.

Definition 2 Asset data: refers to the asset information being evaluated in the network. All asset information in the network constitutes an asset data set S_{asset}. The assets are expressed as:

$Asset = (id_a, name, V_a, type, ser, os, id_r, V_r)$

Use id_a to uniquely identify the asset information; *name* to describe the detailed information of the asset name; the value of the asset V_a represents the importance of the asset, and the value of the asset is quantitatively evaluated by its three security attributes: confidentiality, integrity and availability, and the asset $Va = (val_c, val_i, val_a)$ is expressed as a three-dimensional security attribute The value vector. *type* is the type of assets, including hosts, servers, routers and other network equipment. *ser* Service information for asset operation. *os* is the operating system type. id_r is the identification of the basic operation information of the asset. id_r is the asset operating value obtained according to the basic operating information of the asset, divided into 5 levels.

Definition 3 Basic operating information data: It is the basic operating data corresponding to each asset. The basic operating information identifies the performance of various aspects of the asset. The operating information of a single host is shown as follows:

$Run_h = (id_r, id_a, V_{rh}, \rho_m, \rho_{cpu}, flow)$

Where,

id_r is the basic operation information identification.

id_a is the corresponding asset identification.

V_{rh} is the operating value of host assets.

ρ_m is the memory utilization.

ρ_{cpu} is the CPU utilization.

flow is the flow rate.

The operation information of a single component is shown as follows:

$Run_e = (id_r, id_a, V_{re}, type, \beta, \theta)$

id_r is the basic operation information identification. id_a is the corresponding asset identification. V_{re} is the running value of component assets. *type* is the component type. β is the detection and protection capabilities. θ is the component processing flow.

Definition 4 Vulnerability data: refers to a data set composed of system vulnerability data. The inherent weakness of software or other assets that is used by assaults is known as vulnerability, and will not be harmful when it is not used. Attackers use vulnerabilities to launch attacks. When the network system protection measures are relatively complete or the network system is relatively secure, the difficulty of exploiting the vulnerability will increase, and the threat may not cause security damage. Multiple pieces of vulnerability information form a vulnerable data set S_{vul}. A single vulnerability is expressed as:

$Vul = (id_v, id_a, name, p_t, V_v)$

Where,

id_v is the vulnerability indicator.

id_a is the corresponding asset identification. *name* is the name of vulnerability.

p_t represents the probability of the vulnerability being successfully exploited.

V_v represents the degree of damage after the vulnerability is exploited, which is the same as the asset value and also a three-dimensional value vector. Each aspect is divided into 5 levels.

3.2 Network Security Situation Forecast

The basic process of NSSP refers to combining historical data information and current network security status, using appropriate models or algorithms to qualitatively. NSSP is aware of the security of the overall operation of the network system, real-time perception, and timely detection of dangerous events, providing a basis for timely and accurate network security decision-making or emergency response, and avoiding the occurrence of large-scale network security incidents.

NSSP is an important part of NSSA. It obtains network risk event information and network and node resource information, based on quantitative analysis of network security status, and uses reasonable theoretical models to predict network development trends. At present, methods such as neural network and time series are mainly used to predict the network security status. Forecasting financial data series has been effectively accomplished using neural networks. Time series prediction techniques such as Box-Jenkins and ARIMA presume a linear connection between inputs and outcomes. The ability to approximate nonlinear functions is a benefit of neural networks. The following introduces a commonly used prediction method. The NSSP based on RBF neural network is shown in Figure 4.

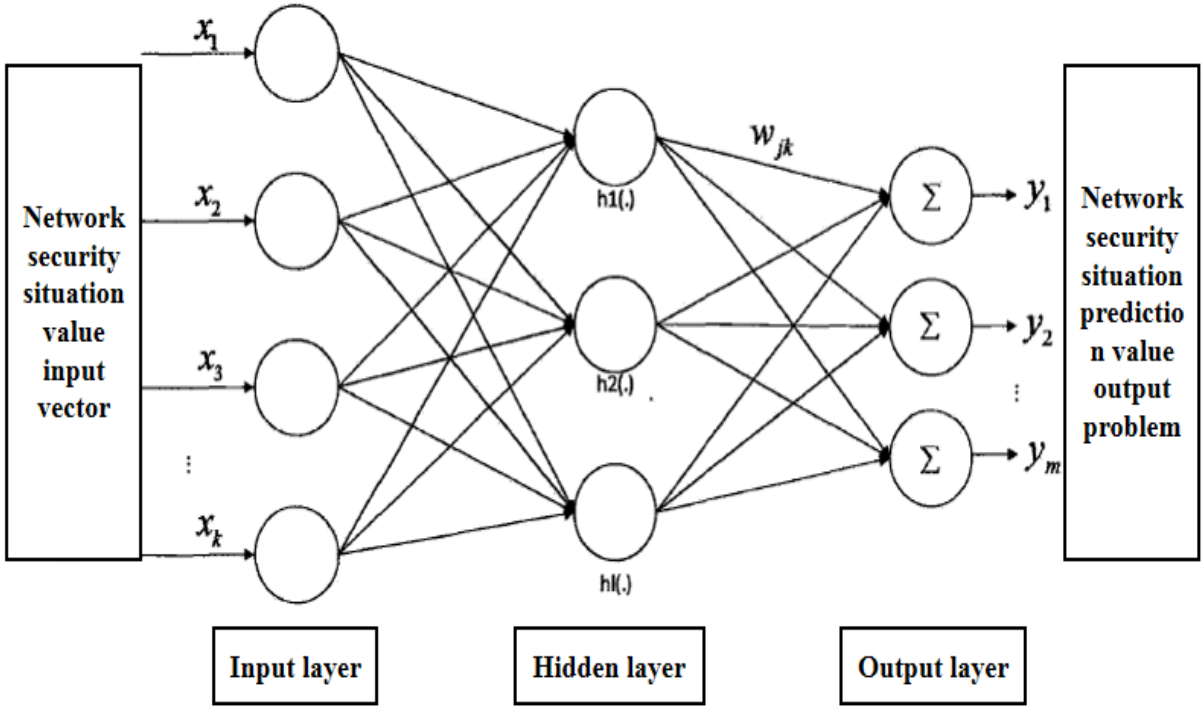


Figure 4. NSSP based on RBF neural network

The input layer main function is to transfer the data source sample information. Each neuron in the hidden layer has an activation function, which completes the mapping from low-dimensional to high-dimensional input data, which is a radial basis function. There is no need for weight connection, which is a non-linear relationship. The output layer is responsible for linearly weighting the results obtained by the hidden layer.

The mapping function is:

$$y_i = \sum_{i=1}^{n} w_{ik} \varphi(\left| X - X^i \right|), i = 1, 2, 3, ..., n$$

Among them, w_{ik} represents the relative weight of the hidden layer and the output layer.

4 Network Security Situation Assessment Model Based on Random Game Model

4.1 Cyber Security Posture Assessment

According to different classification methods, the NSSP method can be summarized into the classification results. There are three participants in the network attack and defense environment: attackers, defenders, and legitimate users. The attacker in the network system to get the best benefit, while the defender takes security measures to prevent the attacker from destroying. The conflicts of interest are antagonistic and will not form a norm of cooperation. Legitimate users will not cooperate with other parties by default, and they always

hope to obtain maximum network resources at a lower cost. In summary, the network security problem can be simplified to a multi-player non-cooperative game process, where each game party pursues the maximization of their own interests. A non-cooperative game, as opposed to a cooperative game, is one in which individual players compete with one another and relationships can only exist if they are self-enforcing. Cooperative game theory focuses on how much people can appropriate given the value each coalition of players can provide, whereas non-cooperative game theory focuses on which movements players should logically perform.

We assume that all players participating in the game process are rational and will choose appropriate strategies to obtain the greatest benefits at the smallest possible cost. The change of any party's strategy may affect the change of the other party's income, which will change the selection strategy, so the influence of the tripartite behavior is integrated. The venerable tripartite model of attitudes remains the most often used measuring paradigm for (explicit) attitudes. The link between a latent attitude and its cognitive, emotional, and behavioral expressions is described by this tripartite model, which is a latent variable model. Under the same circumstances, a rational attacker will choose a strategy that is easy to use and harmful to the attack. On this basis, it will consider reducing costs to increase revenue. Defenders will choose vulnerabilities that have a greater impact on system security to patch, and minimize the impact on system availability. The behavior of legitimate users has a relatively small impact on the outcome of the game, so the impact of legitimate user behavior is not considered in this article. The quantitative analysis of the benefits of each player shows that the benefits of the offensive and defensive parties are not completely equal, and the process is a non-zero-sum game.

The random is represented by the following octet:

Algorithm For Threat Propagation

Require: w, {state}, δ, α

Y ← αD, Y ({state}) ←δ

$Y=\sum w_{ik} y(X\left|x_j\right.=0$

A ←0D×D

repeat

T ← w ⊗ Y T

A ← T − W ◦ AT

Y ←< A,1' >

A ({state}) ←0

Y ({state}) ←δ

until Y has converged

return Y

$ADSGM = (I, S, A, D, \pi, P, R, \delta)$

1. Participant I: The decision-making body, in this article $I = \{ i_a, i_d \}$.

2. State space S: the state of the game system. The transition process of the game state is determined by the simultaneous influence of the actions of both offensive and defensive parties.

3. Attacker action set A, in state S_k, $A_k = (a_1, a_2, ..., a_m)$, $A_k \in A$, represents the attacker's action set in state k. In this article, the attacker's action is defined as the threat propagating to uninfected neighboring nodes, expressed as: $A_k = (a_1, a_2, ..., a_m)$, where $A_k(i) = m$ represents the action of the threat propagating to node m at state k, and the attacker's action at state k according to the threat propagation algorithm.

4. Guardian action set D, in state S_k, $D_k = (d_1, d_2, ..., d_n)$ $D_k \in D$, represents the guardian's action set in state k. In this article, the actions of the defender are divided into: eliminate the vulnerability, cut off the propagation path, $D_k = (d_1, d_2, ..., d_n)$, where $D_k(j) = n$ means to eliminate the vulnerability of node n, $D_k(j) = e(m, n)$ means to cut off the propagation path $e(m, n)$. The set of actions of the defender to spread the current access network according to the threat State and propagation algorithm are obtained.

4.2 Network Security Situation Assessment Analysis

The analysis of network security is the process of analyzing the network to find the vulnerability or attack, by finding the components of network which requires the immediate solution for the security in network and the scanning of vulnerability in the network also helps to determine the security of network. As the complete security of network provides the decreased risk of theft, sabotage and data loss.

The types of security analysis for network is shown above in Figure 5. The analysis are fundamental, finding coverage analysis and the point to point analysis. The fundamental analysis is the process of measuring financial factors and economic factors and produce the intrinsic values to measure the security of a network. Fundamental analysis is a technique for determining a stock's real cost. It incorporates financial information, external factors, events, and industry trends. It's vital to remember that a stock's inherent value or fair value doesn't alter overnight. The finding coverage analysis can be analysed based on the distance that takes to reach the distance in the particular time period is considered for the analysis. An organization can do a coverage analysis to ensure that it is examining all expenses associated with running a clinical trial and that all expenditures are covered. Furthermore, organizations are not blindly funding a research experiment because they did not conduct a thorough investigation. The Point-to-point analysis is used in the routing problem of a network, as it consists of set of points to find the optimal route. Point-by-point analysis is a continuous data analysis approach in which each data point is analyzed separately. Computer-based real-time data capture works well with point-by-point analysis.

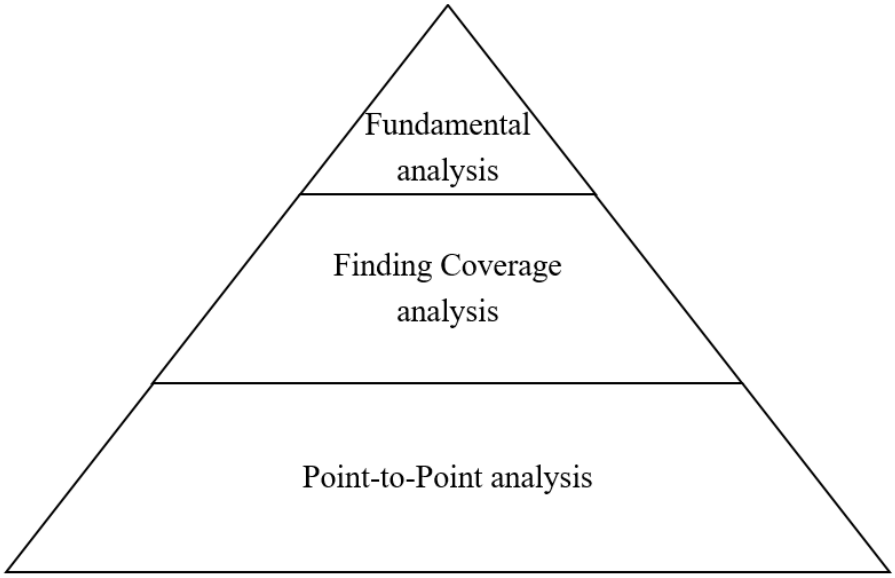


Figure 5. Security analysis for network

4.2.1 Offensive and Defensive Revenue Quantification

In the network attack and defense environment, a rational attacker will choose a strategy that is easy to use and harmful to the attack. On this basis, it will consider reducing costs to increase revenue.

The damage to the system includes damage to assets and related links. The direct benefit of threat t to asset i and related edges in the k state is expressed as:

$ua_i(t, k) = Sdam_i(t) - A\cos t_i(t)$

$Sdam$ means safety damage to the system. $A\cos t$ represents the cost of the attack. The threat benefit value is determined to be 0, otherwise it is ignored.

$$Sdam_i(t) = Vdam_i(t) + \sum_{e \in E} Edam_{ei}(t)$$

E is the set of related path edges. $Vdam$ means the security hazard to the asset. $Edam$ represents the loss caused to the link. The calculation method is as follows:

$Vdam_i(t) = (V_a, V_v)\, p_t p_v$

$Edam_{ei}(t) = (V_e) \bullet \Delta\rho \bullet p_{es}$

When there are multiple vulnerabilities on asset i, take the largest damage vulnerability to express.

Protectors protect asset nodes or links and deploy security strategies to reduce damage caused by attacks. Considering the nodes affected by the defender's protection measures and the affected propagation links, the value of the profit obtained by the defender against the threat t in the state k is expressed as

$$ud_i(t,k) = -Sdam_i(t) + \sum_{i \in N, e \in E} D\cos t_i(t)$$

Protective measures reduce the security damage caused by threats to the system by $Sdam$. $D\cos t$ represents the cost of protective measures. Negative costs include the loss of node service quality caused by the protective strategy. When operating cost When it is very large, the return is assigned a value of 0. The negative cost is expressed as:

$D\cos t_i(t) = \theta_{node}(i,j)\, val_{ai} \bullet V_r + \theta_{edge}(i,j)\, V_e \bullet \rho_e$

$\theta(i,j)$ means adopting a protection strategy j the damage coefficient to the usability caused by the attack i.

4.2.2 Game Matrix Quantification

Since the offensive and defensive random game model is a synthesis, the attack action that the attacker can select is represented, and the defense action that the defender can select is represented by each column in the matrix. Therefore, in each game state S_k, for threat t. The inherent situation is represented by the direct benefits of both offensive and defensive parties, and the potential situation is represented by the situation discount value of the future state. The matrix game elements of the offensive and defensive sides are expressed as $(s_{ij}^a(t,k), s_{ij}^d(t,k))$.

$$S_{ij}^a(t,k) = r_{ij}^a(t,k) + \delta \sum_{i=1}^{K} p_{ij}^{kl}((S_l(t)|S_k(t)), S_k(t), A_k(i), D_k(j)) S_l(t)$$

$$S_{ij}^d(t,k) = r_{ij}^d(t,k) + \delta \sum_{i=1}^{K} p_{ij}^{kl}((S_l(t)|S_k(t)), S_k(t), A_k(i), D_k(j)) S_l(t)$$

$$i = 1, 2, ..., m; j = 1, 2, ..., n;\ p_{ij}^{kl} \geq 0; \forall i, j, k, l, \sum_{i=1}^{K} p_{ij}^{kl} < 1$$

$S_{ij}^a(t,k)$ means that the attacker adopts $A_k(i)$ when the threat t is in the offensive and defensive state S_k. It is composed of two parts. The former $r_{ij}^a(t,k)$ means that the attacker adopts $A_k(j)$ and the defender adopts the attack of $D_k(j)$ o'clock. The direct benefits obtained by the former, and the latter represents the potential benefits.

The game process is shown in Figure 6, S_i represents the game state, and the game matrix is constructed in each game state, and the action choices of the offensive and defensive

parties determine the next moment of the game state.

According to the above formula, the quantification of direct benefits can be considered in two situations. If i is equal to j, that is, the attacker attacks node i and the defender protects node j, then $r_{ij}^{a} = -A\ \text{cost}_i + D\ \text{cost}_j$, $r_{ij}^{d} = D\ \text{cost}_j - A\ \text{cost}_i$. If i is not equal to j, the attacker attacks i, and the defender protects j, then $r_{ij}^{a} = Sdam_i - A\ \text{cost}_i + \delta D\ \text{cost}_i$, $r_{ij}^{d} = -\delta \bullet Sdam_j + \delta D\ \text{cost}_j - A\ \text{cost}_j$.

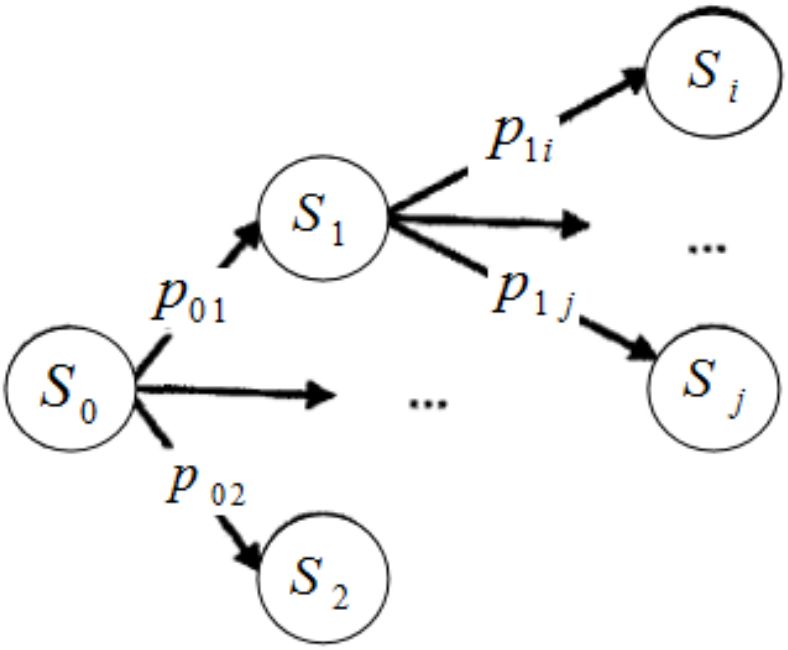


Figure 6. Game process diagram

The process of game theory is shown in the above Figure 4. The game theory is the process of designing strategic interaction (S_0, S_1, S_2, S_j, S_i) between two or more players is given as (P_{01}, P_{02}, P_{1i}, P_{1j}) in the situation contains set of rules and outcomes.

4.2.3 Situation Assessment Algorithm Based on ADSGM

This section introduces the algorithm for implementing NSSE based on the above ADSGM model. The flow chart of the algorithm is shown in Figure 5. The algorithm constructs TPAN.

Based on TPAN to evaluate the NSS of the current state S_0, consider the k-step propagation of the threat, K = 2, 3, 4, 5. Obtain the game state under each step of propagation, denoted as $S_k = (S_{k1}, S_{k2}, ..., S_{kl})$, K = 1, 2, 3, ..., K, for each game state double matrix game, and calculate the expected return and equilibrium strategy. According to the value iteration algorithm, the calculation results of k steps are substituted into $k-1$ steps, and finally the Nash equilibrium in state S_1 is obtained, and the strategy set is obtained. According to the Nash equilibrium of both offense and defense in state S_1, the network security situation value is calculated and the reinforcement strategy is given. The following is the detailed process:

Input: Security data
Output: Network security situation value, protection strategy
Algorithm For Situation Assessment

1) input; current state S_0, game state S_i
2) For each A_{ai} in FA_s {
3) $T = A_a \bullet time_a$
4) $FVS = (HS, T, PVS, VTS)$
5) Let $h_m = S_i \bullet id_n$
6) $sa_{h_m}(A_{ai}, T)\ val_{h_m} \bullet threat_v \bullet PUV(v)$ //
Current host situation, consider spreading below
7) For h_m next two nodes {
8) $sa_{h_n}(A_{ai}, T) = p(S_j)\ sa_{h_n}(A_{ai}, T)$
9) }
10) $sa_{h_m}(V, T)\ val_{h_m} \bullet threat_v \bullet PUV(v) \bullet num(v)$
11) For each node h in HS {
12) $$Sa_h(T) = \sum_{v \in FVS_h} sa_{h_m}(v,T) + \sum_{A_{at} \in FA_{sh}} sa_{h_m}(A_{ai},T)$$
13) }
14) Let SA represents the network situation value
15) $$SA(T) = \sum_{h \in HS} sa_h(T)$$
16) return $SA(T)$

(1) Obtain network security data and perform data fusion to obtain a standardized data set.

(2) According to the basic security data set, conduct security incident analysis, and obtain the threat set S_1 that caused the attack. A security incident is an occurrence that indicates that an organization's systems or data have been hacked, or that the security procedures in place to secure

them have failed. An event in IT is defined as anything that has a significant impact on system hardware or software, whereas an incident is defined as an occurrence that causes a disruption in routine operations.

(3) Build a network of threat propagation and visits to $t \in U_t$.

(4) For $t \in U_t$, consider the K-step propagation of the threat, and the offensive and defensive state of each step $S_k = (S_{k1}, S_{k2}, ..., S_{kl})$ constitutes an defensive random game model, and the equilibrium point is solved according to the sub-algorithm slovel.

(5) According to the equilibrium point in the 4 steps, calculate the game value of both the offensive and defensive networks, and obtain the reinforcement plan.

(6) According to the sub-algorithm slovel, for the S_{1i} state, the attacker's game value v_{ai} and the defender's game value v_{di} are obtained, and the quantitative of the current state S_0 is evaluated as: $sa_t = sa_{exit} + sa_{pro} = \sum_{i=1}^{n} Vdam_i(t) + \delta \sum p_{0i} \bullet S_{1i}$.

(7) Repeat steps 3-6 for all elements in U_t.

(8) Sum the situation caused by all threats to solve the overall situation of network security. The calculation formula is: $U_t sa = \log_c \sum_{t \in U_t} C^{sa_t}$.

1) For each A_{ai} in FA_s {
2) $T = A_a \bullet time_a$
3) $FVS = (HS, T, PVS, VTS)$
4) Let $h_m = S_i \bullet id_n$
5) $sa_{h_m}(A_{ai}, T)\ val_{h_m} \bullet threat_v \bullet PUV(v)$ //
Current host situation, consider spreading below
6) For h_m next two nodes {
7) $sa_{h_n}(A_{ai}, T) = p(S_j)\ sa_{h_n}(A_{ai}, T)$
8) }
9) $sa_{h_m}(V, T)\ val_{h_m} \bullet threat_v \bullet PUV(v) \bullet num(v)$
10) For each node h in HS {
11) $Sa_h(T) = \sum_{v \in FVS_h} sa_{h_m}(v, T) + \sum_{A_{at} \in FA_{sh}} sa_{h_m}(A_{ai}, T)$
12) }
13) Let SA represents the network situation value
14) $SA(T) = \sum_{h \in HS} sa_h(T)$

Result and analysis

The network security situation forecast analyzes the past network data and predicts the network situation to the warning of possible network threats in the future. Cyber security is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber-attacks.

Table 1 shows, network security situation assessment, in this table representation based on thread situation and server.

Figure 7 shows, network security situation assessment, in this grid representation based on thread situation and server.

Table 1. Network security situation assessment

Server	0.586	1.867	2.486	3.85	13.09	23.26	36.39
Thread situation	0.98	4.78	8.58	12.38	16.18	19.98	23.78

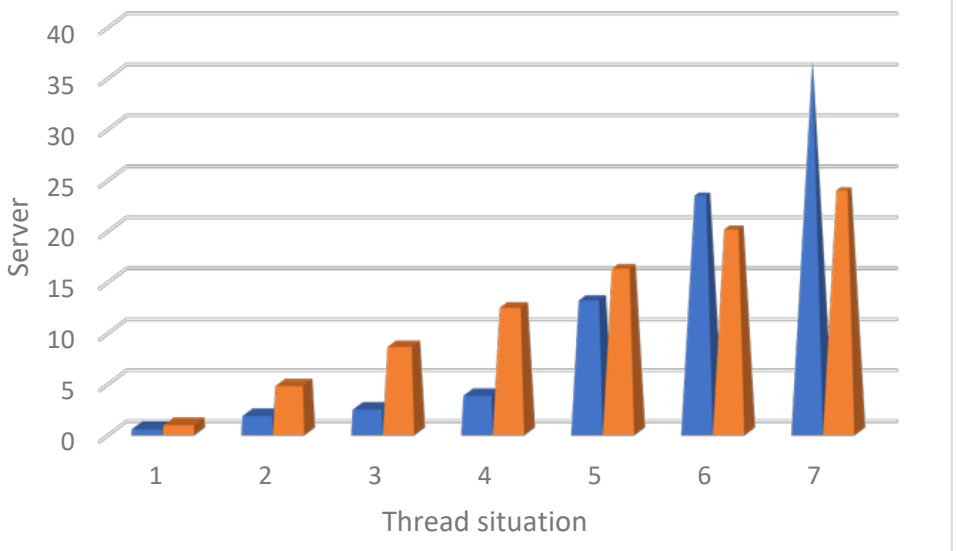


Figure 7. Network security situation assessment

Table 2 shows, network security situation prediction, in this table representation based on quantization period and security situation value.

Figure 8 shows, network security situation prediction, in this grid representation based on quantization period and security situation value.

Table 3 shows, stochastic game model thread propagation, in this table representation based on stochastic signal and thread propagation.

Figure 9 shows, stochastic game model thread propagation, in this grid representation based on stochastic signal and thread propagation.

Table 2. Network security situation prediction

Quantization period	1.67	2.56	3.45	4.34	5.23	6.12	7.01
Security situation value	0.78	3.45	12.7	17.56	23.52	25.48	29.44

Table 3. Stochastic game model thread propagation

Stochastic signal	10	20	30	40	50	60	70
Thread propagation	5.67	23.56	41.45	59.34	77.23	95.12	113.01

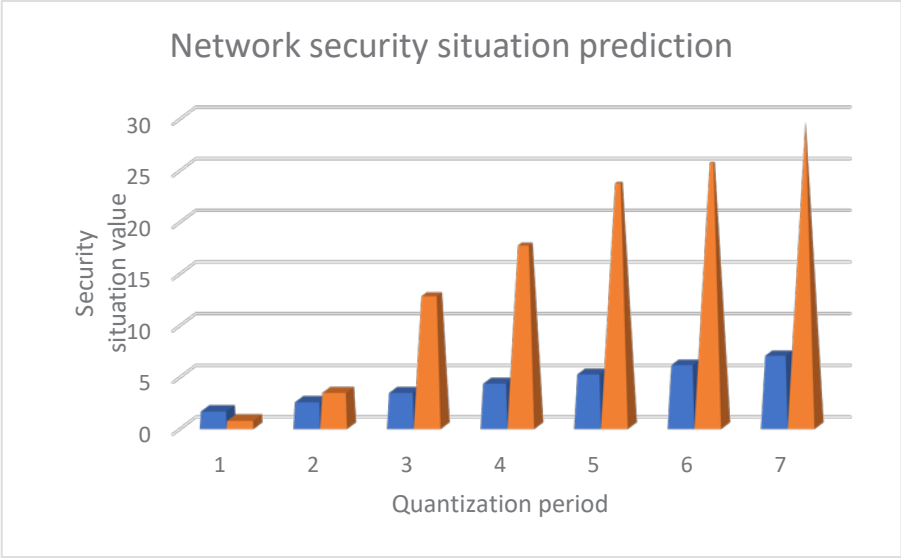


Figure 8. Network security situation prediction

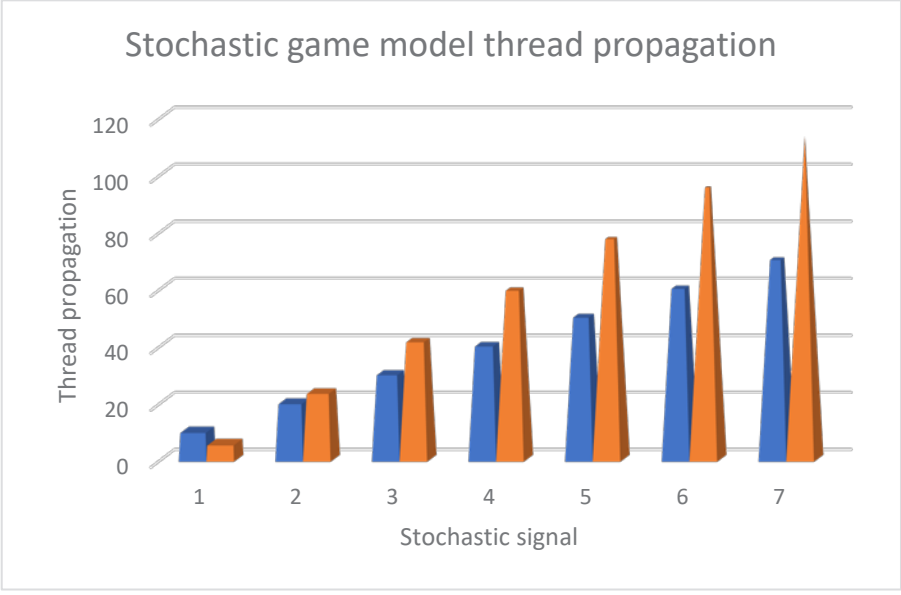


Figure 9. Stochastic game model thread propagation

Table 4 shows, cyber security situational awareness, in this table representation based on awareness program and percentage.

Figure 10 shows, cyber security situational awareness, in this grid representation based on awareness program and percentage.

Table 5 shows, the thread trend analysis process, in this table representation based on thread situation and trend analysis.

Figure 11 shows, the thread trend analysis process, in this grid representation based on thread situation and trend analysis.

Table 4. Cyber security situational awareness

Awareness program	12.45	22.3	32.15	42	51.85	61.7	71.55
Percentage	3.45	4.67	25.89	37.11	48.33	69.55	70.77

Table 5. The thread trend analysis process

Thread situation	2.34	3.56	4.78	6	7.22	8.44	9.66
Trend analysis	3.67	4.98	6.29	7.6	8.91	10.22	11.53

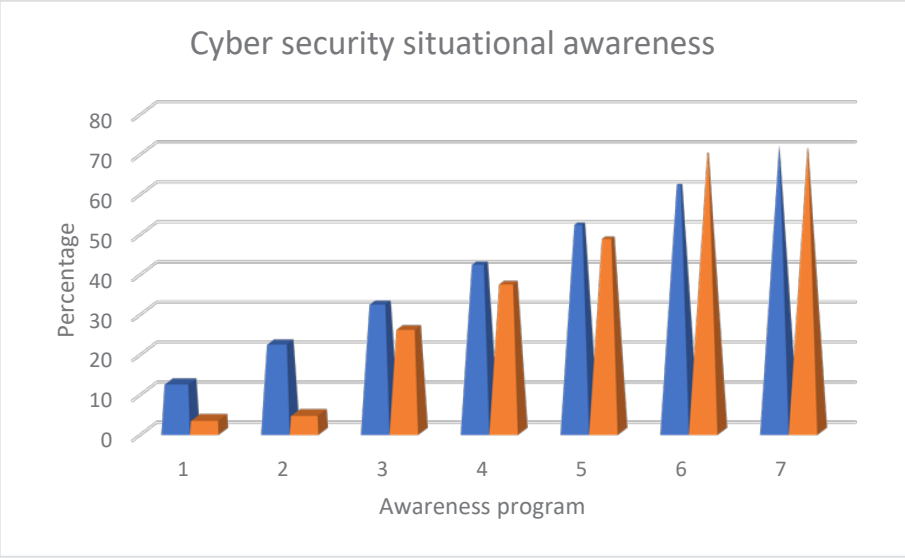


Figure 10. Cyber security situational awareness

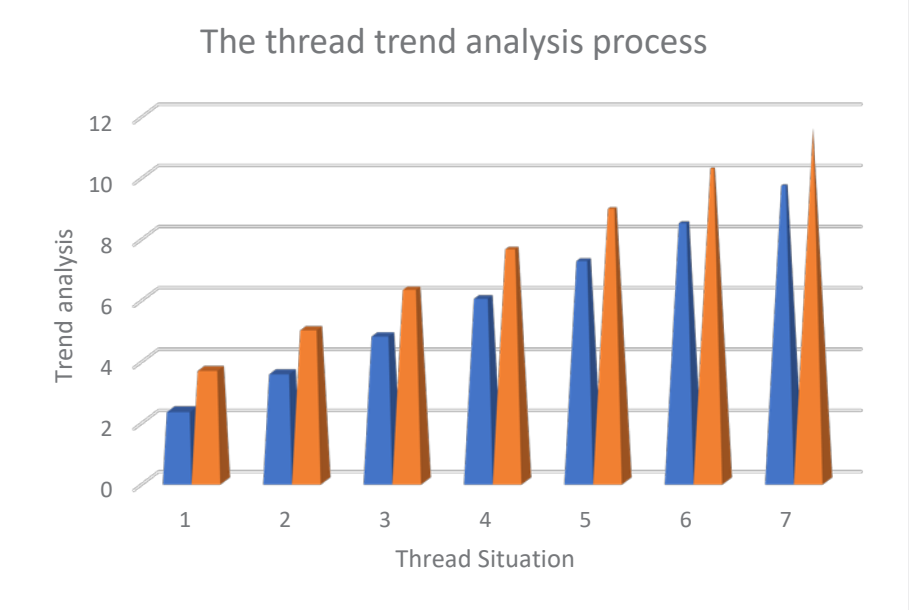


Figure 11. The thread trend analysis process

5 Conclusion

With the popularization of the Internet and the rapid development of network technology, the issue of network security has become a hot issue that cannot be ignored. This article first analyzes the latest developments in network security, introduces the research work of domestic and foreign researchers on the network security situation method, analyzes and summarizes the shortcomings of the existing NSSE and NSP technologies. In terms of evaluation methods, this paper proposes an NSSE model based on offensive and defensive random games, integrates the game information of both offensive and defensive parties, constructs a threat access relationship network. In terms of situation prediction, this paper proposes an NSSP model based on the prediction of security situation elements, which integrates various situation factor information and predicts the overall situation based on changes in situation elements. Through comparative experiments, the effectiveness of these two methods is verified.

The main work of this paper is as follows:

1. Introduce the situational awareness technology from the detailed aspects of situational data collection, data fusion, situational assessment, situational prediction, and visual analysis. It focuses on the current research results and advantages and disadvantages of knowledge reasoning methods, artificial intelligence methods and statistical methods in situation assessment. The network security situation prediction technology is introduced from both qualitative and quantitative aspects. The basic theory of game is introduced, which provides theoretical support for the following research.

2. A NSE model based on offensive and defensive random games is proposed, which integrates threat information, protection information and environmental information, and comprehensively evaluates the network security situation. In response to threat information, a network of threat propagation visits is constructed, and the impact of threats on the situation is divided into two parts: the threat situation that has occurred and the potential threat situation. Quantitative analysis of threat propagation and the implementation of protective measures, and establishing a random game model for its game process, solving the mixed strategy Nash equilibrium, dynamically evaluating the network security situation, and obtaining network security defense measures to provide guidance for network security protection.

6 References

[1] G. Abaei, A. Selamat, A survey on software fault detection based on different prediction approaches, *Vietnam Journal of Computer Science*, Vol. 1, No. 2, pp. 79-95, May, 2014.

[2] C. Cortes, V. Vapnik, Support-vector networks, *Machine learning*, Vol. 20, No. 3, pp. 273-297, September, 1995.

[3] M. S. Nolan, Fundamentals of air traffic control, *Cengage learning*, 1990.

[4] S. Lau, The spinning cube of potential doom, *Communications of the ACM*, Vol. 47, No. 6, pp. 25-26, June, 2004.

[5] W. Hu, J. Li, J. Shi, A novel approach to cyberspace security situation based on the vulnerabilities analysis, *Proceedings of the 6th World Congress on Intelligent Control and Automation*, Dalian, China, 2006, pp. 4747-4751.

[6] P. Liu, W. Zang, Incentive-based modeling and inference of attacker intent, objectives, and strategies, *Proceedings of the 10th ACM Conference on Computer and Communications Security*, Washington, D.C., USA, 2003, pp. 179-189.

[7] D. Shen, G. Chen, Jr. J. B. Cruz, L. Haynes, M. Kruger, E. Blasch, A Markov game theoretic data fusion approach for cyber situational awareness, *Proceedings of SPIE -The International Society for Optical Engineering*, Vol. 6571, pp. 1-12, April, 2007.

[8] W. Jiang, Z. H. Tian, H. L. Zhang, X. F. Song, A stochastic game theoretic approach to attack prediction and optimal active defense strategy decision, *Proceedings of the 2008 IEEE International Conference on Networking*, *Sensing and Control*, Sanya, China, 2008, pp. 648-653.

[9] X. Cui, X. Tan, Y. Zhang, H. Xi, A Markov game theory-based risk assessment model for network information system, *Proceedings of the 2008 International Conference on Computer Science and Software Engineering*, Wuhan, China, 2008, pp. 1057-1061.

[10] O. Sheyner, J. Haines, S. Jha, R. Lippmann, J. M. Wing, Automated generation and analysis of attack graphs, *Proceedings of the 2002 IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, 2002, pp. 1-12.

[11] J. Von Neumann, O. Morgenstern, Theory of Games and Economic Behavior, *Princeton University Press*, 2007.

[12] M. R. Endsley, Situation Awareness Global Assessment Technique, *Proceedings of the IEEE 1988 National Aerospace and Electronics Conference*, Dayton, OH, USA, 1988, pp. 789-795.

[13] O. H. Alhazmi, Y. K. Malaiya, I. Ray, Measuring, analyzing and predicting security vulnerabilities in software systems, *Computers & Security*, Vol. 26, No. 3, pp. 219-228, May, 2007.

[14] E. Rescorla, Is finding security holes a good idea? *IEEE Security & Privacy*, Vol. 3, No. 1, pp. 14-19, January-February, 2005.

[15] H. K. Browne, W. A. Arbaugh, J. Mchugh, W. L. Fithen, A Trend Analysis of Exploitations, *Proceedings 2001 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 2001, pp. 214-229.

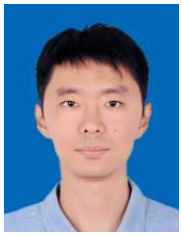
[16] X. Cai, C. Wu, J. Sheng, Y. Wang, B. Ai, Spectrum Situation Awareness Based on Time-Series Depth Networks for LTE-R Communication System, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 23, No. 7, pp. 8629-8640, July, 2022.

[17] M. E. Pérez-Pons, R. S. Alonso, O. García, G. Marreiros, J. M. Corchado, Deep Q-Learning and preference based multi-agent system for sustainable agricultural market, *Sensors*, Vol. 21, No. 16, Article No. 5276, August, 2021.

[18] R. B. Issa, M. Das, M. Rahman, M. Barua, M. Rhaman, K. S. N. Ripon, M. G. R. Alam, Double Deep Q-Learning and Faster R-CNN-Based Autonomous Vehicle Navigation and Obstacle Avoidance in Dynamic Environment, *Sensors*, Vol. 21, No. 4, Article No. 1468, February, 2021.
[19] S. M. Hussain, K. M. Yusof, Dynamic Q-learning and Fuzzy CNN Based Vertical Handover Decision for Integration of DSRC, mmWave 5G and LTE in Internet of Vehicles (IoV), *Journal of Communications*, Vol. 16, No. 5, pp. 155-166, May, 2021.
[20] W. Wang, Y. Qiu, S. Xuan, W. Yang, Early Rumor Detection Based on Deep Recurrent Q-Learning, *Security and Communication Networks*, Vol. 2021, June, 2021, pp. 1-13.

Biographies

Xian Guo received the Ph.D degree in computer applied technology from The University of Chinese Academy of Sciences, Beijing, China, in 2012, and is currently working in China Industrial Control Systems Cyber Emergency Response Team, Beijing, China. Her working areas includes automation equipment programming, protocol analysis, industrial control system information security, cyber security.



Jianing Yang received master degree of engineering from Beihang University, Beijing, China, in 2016, and now is working for China Industrial Control Systems Cyber Emergency Response Team. His working areas includes security of industrial control system, security of the internet of things, security of industrial internet and industrial big data.

Zhanhui Gang obtained Master of Computer Technology from Peking University, Beijing, China, in 2018, and now is working at China Industrial Control Systems Cyber Emergency Response Team. Her primary research areas include security vulnerabilities in industrial control system, cyberspace resources surveying and mapping, security of the internet of things, security in big data for industrial internet

An Yang, PhD of Institute of Information Engineering, Chinese Academy of Sciences and currently works at China Industrial Control Systems Cyber Emergency Response Team. His main research areas include ICS Vulnerability analysis, industrial internet security and IoT security.