Li *et al. EURASIP Journal on Wireless Communications and Networking* (2019) 2019:205
https://doi.org/10.1186/s13638-019-1506-1

EURASIP Journal on Wireless Communications and Networking

REVIEW Open Access

Analysis framework of network security situational awareness and comparison of implementation methods

Yan Li[1*], Guang-qiu Huang[2], Chun-zi Wang[1] and Ying-chao Li[1]

Abstract

Information technology has penetrated into all aspects of politics, economy, and culture of the whole society. The information revolution has changed the way of communication all over the world, promoted the giant development of human society, and also drawn unprecedented attention to network security issues. Studies, focusing on network security, have experienced four main stages: idealized design for ensuring security, auxiliary examination and passive defense, active analysis and strategy formulation, and overall perception and trend prediction. Under the background of the new strategic command for the digital control that all countries are scrambled for, the discussion of network security situational awareness presents new characteristics both in the academic study and industrialization. In this regard, a thorough investigation has been made in the present paper into the literature of network security situational awareness. Firstly, the research status both at home and abroad is introduced, and then, the logical analysis framework is put forward concerning the network security situational awareness from the perspective of the data value chain. The whole process is composed of five successive stages: factor acquisition, model representation, measurement establishment, solution analysis, and situation prediction. Subsequently, the role of each stage and the mainstream methods are elaborated, and the application results on the experimental objects and the horizontal comparison between the methods are explained. In an attempt to provide a panoramic recognition of network security situational awareness, and auxiliary ideas for the industrialization of network security, this paper aims to provide some references for the scientific research and engineering personnel in this field.

Keywords: Network security, Network situational awareness, Big data network security, Intrusion detection, Data fusion analysis

1 Introduction

The information technology revolution has made great changes in the way of human communication in the world today. Especially in recent years, in-depth studies of the industrialization concepts of cloud computing, large data, Internet of Things, and mobile terminals have made the control of digital information become a new strategic commanding point, and the problem of network security has also received more attention in a wider range. The exposure of "prism plan" in June 2013 brought information security from economic interest to the level of national security. In February 2014, the establishment of the "central network security and information group" marked the awakening of the national consciousness of the Internet in China and highlighted the importance of the national information security strategy. However, the ability of network overall defense at the national level to attack risk is still relatively weak [1]. How to prevent organized malicious network attack has become a hot topic in the field of security.

Studies on network security have started since the birth of information networks. The exponential growth of network size and application, especially the random dynamic access relationship built on the static Internet physical connection network based on OSI model, makes the study of network security more complicated. Before the 1960s, the focus on the network security research is how to build an absolute security system and reduce design vulnerabilities to ensure the confidentiality, integrity, and availability of the system, which can be regarded as

---

* Correspondence: sayidli@xpu.edu.cn
[1]Xi'an Polytechnic University, Xi'an 710048, Shaanxi, China
Full list of author information is available at the end of the article

the first stage of network security research. However, people soon realized the impossibility in practical operation [2]. The existence of malicious intrusion provokes the thought to build a security assistant system with an aim to detect the intrusion in time and take corresponding measures. The most typical application is the intrusion detection system (IDS) [3]. The intrusion detection is originated from Anderson's Technical Research Report [4], and the subsequent researches can be divided into two categories: anomaly detection and misuse detection. At present, the IDS of most research institutions and commercial organizations is based on these two categories. Intrusion detection technology provides predictive warning information to ensure network security when network attacks occur, but it is too weak to do anything about the wall-around stealth attack and multi-step compound attack. Such a passive defense technology is unsatisfactory in the real-time detection. On this basis, the focus of the third stage research after the 1990s shifted from passive defense to active analysis [5, 6], which is originated from the development of hacker technology. The intent is to carry out an integrated safety assessment before the occurrence of network attacks, formulate a defense strategy, or still provide predetermined service function given the damaged network. In 1990, Bass first proposed the concept of Cyber Situation Awareness CSA [7, 8], which intends to perceive elements in the time and space environment, so that people can better grasp the overall network security situation and predict future trends, which to a certain extent promotes the integration of network security research and other disciplines. The development, especially the combination with some advanced stochastic models, has made theoretical progress (such as stochastic algebra [9], game theory [10], Bayesian network [11]). However, most of them are based on CSA conceptual model to optimize the evaluation algorithm with few breakthroughs in the practical application and systematic expositions (Table 1 gives a brief summary of the four main stages of the development of network security studies).

This paper gives a systematic introduction to the field of network security situational awareness, with an aim to provide insightful guidance for understanding the related concepts, promoting their application in practice and carrying out large-scale network expansion. In addition, a general analysis framework of network security situational awareness is proposed from the perspective of value chain. The framework divides the process of network security situational awareness into five stages: factor acquisition, model representation, measurement establishment, solution analysis, and situation prediction, which summarizes the current research progress in each stage and discusses the practical application results of typical methods. Moreover, this paper also elaborates the visualization of perception analysis results and situational awareness in the large data environment and prospects the key issues and research trend of this topic.

2 Research status at home and abroad

Situational awareness is first seen in the study of military academia. The human factor analysis of Theureau [12] in aviation has greatly promoted the application of this field in human-machine interaction, medical emergency scheduling, and real-time battlefield command. In 1988, Endsley [13] defined situation awareness as the three-level model of situation factor acquisition, situation understanding, and situation prediction, and the application framework of situational awareness in dynamic decision making was proposed in 1995 [14]. On this basis, the case study of the practical application of situational awareness is started, for example, Boyd control cycle model [15], Tadda JDL data fusion model [16] based on Endsley's three-level model, cognitive fusion control model [17], and so on.

Inspired by the air traffic control (ATC) situational awareness, Bass [7] of the US Air Force Communications and Information Center first proposed the concept of network situational awareness, in an attempt to apply the ATC data fusion to network situational awareness. Since then, the attention of most studies is paid to the data fusion analysis with the ignorance of the essential definition of cybersecurity situational awareness. At present, there is no clear and unified expression of

Table 1 Four main stages of network security research

NO	Time Period	Stage	Main Idea	Core Technology
1	Before 1960's	Design ensures safety	Build an absolutely secure system to ensure that attacks don't happen	Technology architecture design on software and hardware level
2	From1970's to 1980's	Intrusion detection	Build a security assistance system that can detect and defense when an attack occurs	Intrusion detection system (misuse detection, anomaly detection)
3	In 1990's	Active analysis and defense	Not just passive defense, active evaluation, make defense strategy before attack occurs	Attack model (attack tree, attack graph, state graph, etc.)
4	After 2000	Network situation awareness	Comprehensive evaluation of various elements in time and space environment, predicting future trends of overall network security	Combined with advanced stochastic model (complex network evolution, game theory, etc.)

network security situational awareness. However, confirmation is made that network security situational awareness and situational awareness belong to the relationship between instance and type instead of that of subset, which means the relevant theory of situational awareness and the method can be applied in the field of network security situational awareness after the specific processing. The literature [19] has a systematic explanation for the definition of network security situational awareness and the understanding of the basic concept. Based on the explanation above, this paper offers the basic operation mechanism of network security situational awareness and illustrates the role of each link in the cognitive process of network security status in the mechanism.

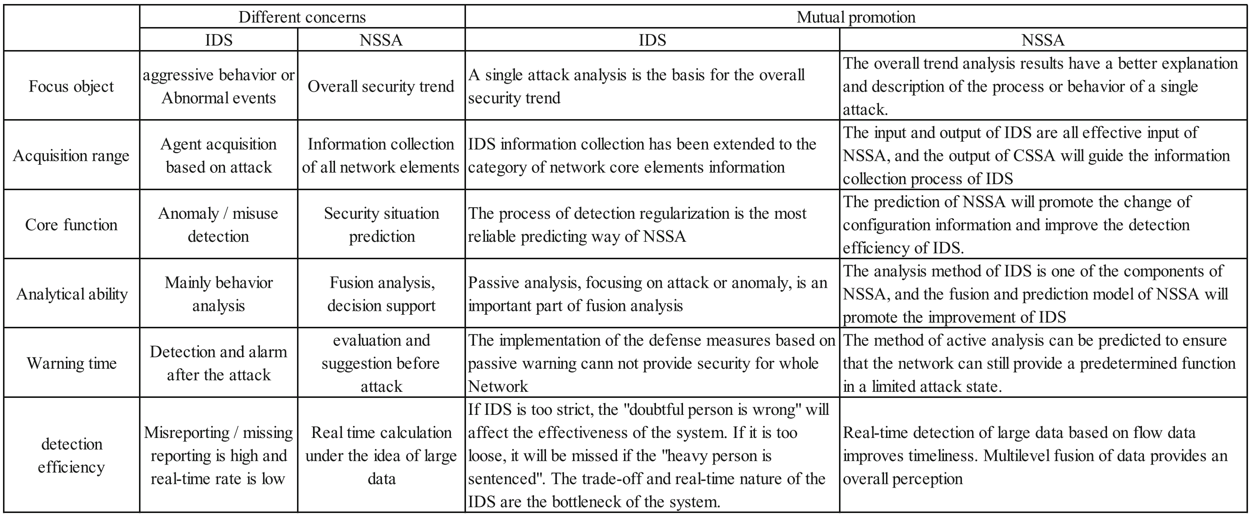
2.1 Network security situation awareness and intrusion detection

The general model of the intrusion detection system (IDS) is first proposed by Denning [20]. Its core idea is to set up a regular set of rules that can be updated and modified under the condition of a unified clock. Thereafter, information is collected by an agent from the network process records and compared with the defined rules, and then, determination is made whether the activity set exists, which is trying to break the integrity, confidentiality, and availability of resources. The structure of IDS can be mainly divided into three types: host-based detection [21], network-based detection [22, 23], and agent-based detection [24]. The host-based detection mainly matches the process record information on a single host. This obviously does not meet the security requirements under the network environment; thus, the network-based detection is built after adding some elements on the host-based detection, such as network traffic and protocol information; however, with the gradual use of distributed systems, IDS on distributed hosts also needs information interaction, which contributes to the formation of agent-based detection. Technically, IDS is mainly divided into two types [25], abnormal intrusion detection and misuse intrusion detection. Abnormal behavior is the opposite of normal or harmless behavior, so the rule set in abnormal behavior detection is the mode of the normal operation of the system. When detecting the deviation from the normal model, the alarm signal is generated. The advantage of this method is that any exploratory behavior will be recorded in addition to the prescribed "normal" action. But there will be a higher "false alarm rate" because the normal mode of the system is dynamic and cannot be completely normalized at the beginning of the establishment of the detection model; misuse behavior is abnormal or harmful behavior, so the rule set of misuse behavior detection is a model of system harmful behavior. When it detects the behavior that matches the harmful pattern, it produces an alarm. In the case of clear matching, this method has high accuracy, especially for the typical known attack model. But there is a big "rate of missing report" because it is almost impossible to passively carry out the whole sample summarization of harmful behavior under the background of diverse aggressive behaviors.

Through the brief summary of IDS, there are two main bottlenecks: passive response and false alarm rate/missing report rate, and the researchers have done a great deal of improvement on these two points. The main improvement of the passive response mode is on the automatic or semi-automatic response mode [26]. The main reason for false alarm rate or missing report rate is that there is a gray area between normal and abnormal, for which the IDS system and administrators cannot be analyzed in a unified perspective. Therefore, the improvement of this aspect is mainly the multi-level fusion analysis of more information [27–29], which is consistent with the summary of the four main stages of network security research in Table 1. In fact, the initial research on network situational awareness is also based on IDS. Bass [7, 30] proposed a multi-sensor integration intrusion detection framework after the concept of situation awareness, and literature [31, 32] also put forward a similar framework. On this basis, lots of influential security situational awareness applications appeared, such as NVisionIP [33], VisFlowConnect-IP [34], and UCLog+ [35].

It can be seen that the network security situational awareness is a more advanced research stage and development direction to make up the defects of IDS. On the one hand, the existing results of IDS are the basis of the in-depth study of the network security situational awareness, and the latest methods and results of the network security situational awareness can relieve the contradictions of IDS. As shown in Table 2, there are differences and strong connections between network security situational awareness and IDS. First of all, the focus of IDS is the presence or occurrence of attacks (or exceptions) in the network, and network security situational awareness is concerned with the security trend of a whole network. The analysis of attack behavior in network security situational awareness plays a fairly important part, and attack behavior is carried out step by step in normal behavior steps. Furthermore, the results of fusion analysis in network security situational awareness will also make IDS better explain and describe the rules of abnormal behavior or misuse behavior; secondly, before rule comparison, the core information acquisition results of IDS is the attack precursor and post which is in the network management audit category. However, the fusion analysis of network security situational awareness is definitely the element information abstraction of the

Table 2 The difference and connection between IDS and network security situational awareness



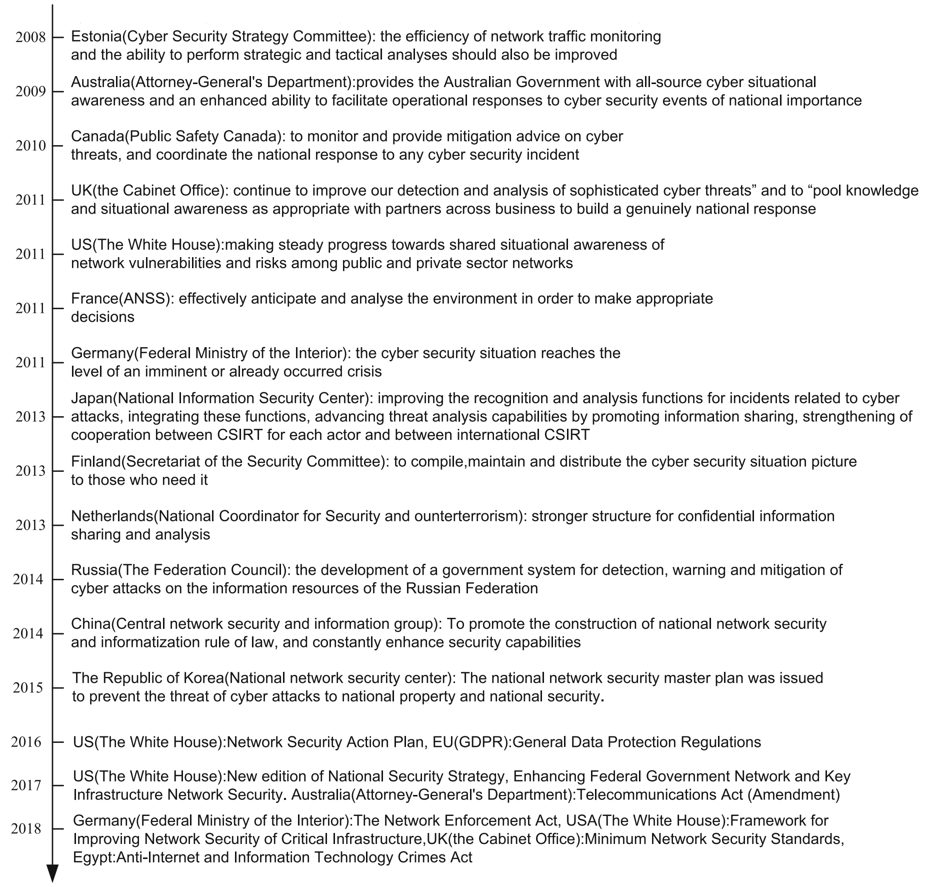
	Different concerns		Mutual promotion	
	IDS	NSSA	IDS	NSSA
Focus object	aggressive behavior or Abnormal events	Overall security trend	A single attack analysis is the basis for the overall security trend	The overall trend analysis results have a better explanation and description of the process or behavior of a single attack.
Acquisition range	Agent acquisition based on attack	Information collection of all network elements	IDS information collection has been extended to the category of network core elements information	The input and output of IDS are all effective input of NSSA, and the output of CSSA will guide the information collection process of IDS
Core function	Anomaly / misuse detection	Security situation prediction	The process of detection regularization is the most reliable predicting way of NSSA	The prediction of NSSA will promote the change of configuration information and improve the detection efficiency of IDS.
Analytical ability	Mainly behavior analysis	Fusion analysis, decision support	Passive analysis, focusing on attack or anomaly, is an important part of fusion analysis	The analysis method of IDS is one of the components of NSSA, and the fusion and prediction model of NSSA will promote the improvement of IDS
Warning time	Detection and alarm after the attack	evaluation and suggestion before attack	The implementation of the defense measures based on passive warning cann not provide security for whole Network	The method of active analysis can be predicted to ensure that the network can still provide a predetermined function in a limited attack state.
detection efficiency	Misreporting / missing reporting is high and real-time rate is low	Real time calculation under the idea of large data	If IDS is too strict, the "doubtful person is wrong" will affect the effectiveness of the system. If it is too loose, it will be missed if the "heavy person is sentenced". The trade-off and real-time nature of the IDS are the bottleneck of the system.	Real-time detection of large data based on flow data improves timeliness. Multilevel fusion of data provides an overall perception

whole network. With the elaborate study, the input information of IDS also has a great expansion, but the input of IDS must be a subset of the input of the network security situational awareness, and the output of the IDS can also be used as the input element of the network security situational awareness. In turn, the result of the network security situational awareness will make IDS's information collection more precise and effective. Thirdly, at the functional level, the core function of IDS is to intercept suspected attack behavior through abnormal/misuse detection comparison and guide network administrators to take measures to defend the next attack. The core purpose of network security situational awareness is to carry out the security situation prediction, which is intended to guide the administrator to take configuration measures before the attack, which will certainly improve the detection efficiency of IDS. The pre/post-rule detection method based on standard IDS is also the most effective and reliable prediction method of network security situational awareness; fourthly, the analysis of IDS mainly focuses on attack behavior, but it is not capable of multi-step attack or attack around the wall. Most fusion analysis of network security situational awareness also deals with the analysis of aggressive behavior or abnormal behavior, because such behavior produces more benefit than normal access behavior. However, the overall analysis results including other behaviors will give IDS guidance both in particle size and in the accuracy of description; fifthly, in the early warning period, IDS carries out the acquisition analysis and warning based on audit information after attack, and the passive response mode is difficult to guarantee the network security in real time. Network security situational awareness does the active security situation perception before the attack, and it does not aim to eliminate the attack but to ensure that the network system is still safe or can still provide a predetermined function under the conditions of a certain attack. At last, in the detection efficiency, the core breakthroughs of IDS are high rate on false alarm/missing report and weak real time. If the configuration is too strict, the assertion of "suspect is wrong" will affect the effectiveness of the system. Loose configuration means "only heavy person should be judged" will miss the report. The compromise state between the two extremes requires the system to have the human gray perception ability, rather than the computer cognitive logic which means one or the other. The fusion process of network security situational awareness (NSSA) is easier to cross boundaries with artificial intelligence and other multidisciplinary research results for further improving the flexibility of detection, and the fusion analysis of flow data in large data environment will greatly promote the real-time performance of detection.

2.2 Status of foreign research

The study of situational awareness comes from a series of studies and elaborations of more than 15 articles by Endsley [13, 14, 36]. Bass [7] proposed the concept of network situational awareness for the first time and combined it with cyberspace. Driven by the new technologies such as the Internet of Goods, big data, and mobile applications, the innovation and promotion of the Internet application level have expanded rapidly, and the topology has become increasingly complex. As the public information shows (Fig. 1), all countries have raised their network security awareness to the national strategic level. From the summary of the cybersecurity strategies, publicized in various countries in recent years, it can be seen that although countries have different understandings of cybersecurity and strategy implementation, countries are aware of the need to take action to protect the key information and related infrastructure, as well as to achieve the prediction of intelligent network security situation with new methods and technologies.

The great emphasis from governments can bring more financial support in terms of the fund. Besides, the spontaneous and continuous attention of many researchers to this field has made the researches on cybersecurity the top hot issue. In order to fully understand the research status of network security situational awareness, this paper firstly searched and reviewed articles on this topic in the past 10 years in the core database in September 2017, and sorted out a total of 10 large citations of review literature [16, 37–45]. Based on the actor-network theory, Kopylec et al. [37] explored the critical relationship between physical and network infrastructure, and demonstrated the results of situational awareness through visual cascading. From the viewpoint of network's key equipment administrators, he managed to maximize the understanding of the process of the risk propagation, thus providing systematic guidance in related planning and emergency response. Based on the combination of computer automation technology with human irregularity (abnormal or new mode) processing capabilities, literature [38] describes the research ideas and tools provided by the VizSec R&D community, which enables network managers to better identify the potential cyber threats. With aspect to the multidisciplinary integration, Jajodia et al. [39] conducted the research in relation to the questions and methods of network situational awareness in 2010 with an excellent conclusion and analyzed the key problem of the network situational awareness, as well as summarizes the main reasons for the lack of network situational awareness. Tadda and Salerno [16], Giacobe [40], and Schreiber-Ehle and Koch [42] inquired into the application process of JDL model in the field of situational awareness, especially in literature [40] for the favorable induction and summary of the data source information at level 0/1 in JDL model. In addition, Klein et al. [41] and Vincent [45] et al. applied the OODA loop model [15] to the network situational awareness and some stages in the model are prerequisites for others. Through such a class decision paradigm, the various activities in network



2008 Estonia(Cyber Security Strategy Committee): the efficiency of network traffic monitoring and the ability to perform strategic and tactical analyses should also be improved

2009 Australia(Attorney-General's Department):provides the Australian Government with all-source cyber situational awareness and an enhanced ability to facilitate operational responses to cyber security events of national importance

2010 Canada(Public Safety Canada): to monitor and provide mitigation advice on cyber threats, and coordinate the national response to any cyber security incident

2011 UK(the Cabinet Office): continue to improve our detection and analysis of sophisticated cyber threats" and to "pool knowledge and situational awareness as appropriate with partners across business to build a genuinely national response

2011 US(The White House):making steady progress towards shared situational awareness of network vulnerabilities and risks among public and private sector networks

2011 France(ANSS): effectively anticipate and analyse the environment in order to make appropriate decisions

2011 Germany(Federal Ministry of the Interior): the cyber security situation reaches the level of an imminent or already occurred crisis

2013 Japan(National Information Security Center): improving the recognition and analysis functions for incidents related to cyber attacks, integrating these functions, advancing threat analysis capabilities by promoting information sharing, strengthening of cooperation between CSIRT for each actor and between international CSIRT

2013 Finland(Secretariat of the Security Committee): to compile,maintain and distribute the cyber security situation picture to those who need it

2013 Netherlands(National Coordinator for Security and ounterterrorism): stronger structure for confidential information sharing and analysis

2014 Russia(The Federation Council): the development of a government system for detection, warning and mitigation of cyber attacks on the information resources of the Russian Federation

2014 China(Central network security and information group): To promote the construction of national network security and informatization rule of law, and constantly enhance security capabilities

2015 The Republic of Korea(National network security center): The national network security master plan was issued to prevent the threat of cyber attacks to national property and national security.

2016 US(The White House):Network Security Action Plan, EU(GDPR):General Data Protection Regulations

2017 US(The White House):New edition of National Security Strategy, Enhancing Federal Government Network and Key Infrastructure Network Security. Australia(Attorney-General's Department):Telecommunications Act (Amendment)

2018 Germany(Federal Ministry of the Interior):The Network Enforcement Act, USA(The White House):Framework for Improving Network Security of Critical Infrastructure,UK(the Cabinet Office):Minimum Network Security Standards, Egypt:Anti-Internet and Information Technology Crimes Act

Fig. 1 Departments and public security strategies for network security in time series of countries

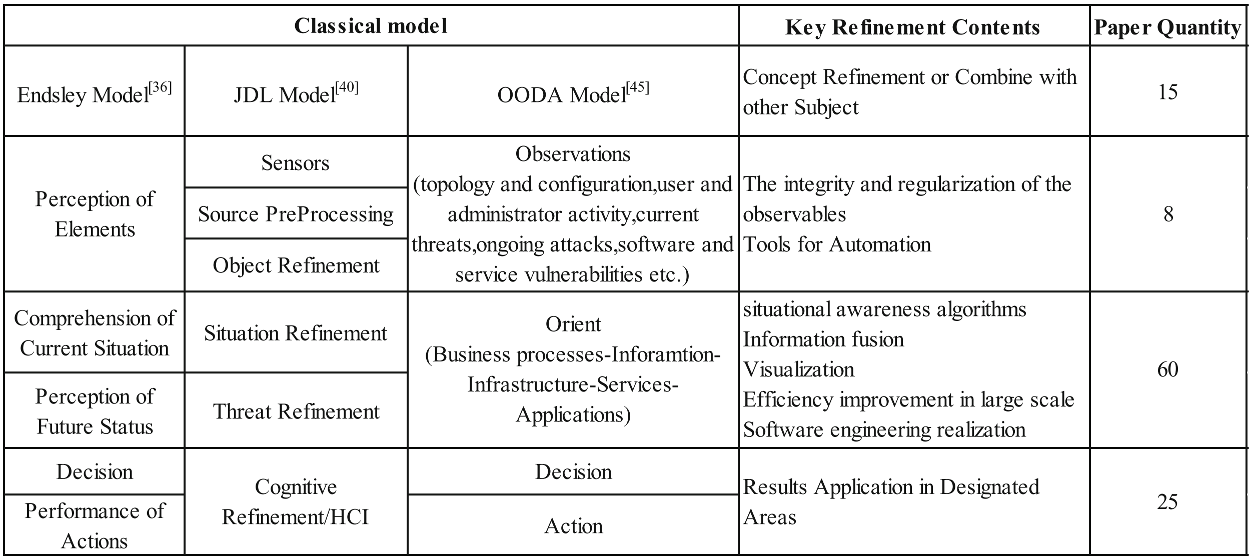
defense are integrated. Much emphasis in literature [43] is attached to the information security of industrial networks. The difference between industrial networks and general computer networks makes the commonly used "detection/repair" methods in general computer networks not fully applicable. In light of this, the current state of distributed computing systems has been evaluated in the present paper, and the key elements in defensive countermeasures can help to reduce the risks to an acceptable threshold. In 2014, Franke and Brynielsson [44] conducted an effective summary of 102 articles in the four major scientific databases, being regarded as one of the best researches in the past 3 years, where 11 sub-categories were compared and the current status of the research was discussed according to the research field or content. The literature [46] provides an overview of the problems, challenges, threats, and solutions in social network security. In a strict sense, computer network security is an integral part of social network security. Therefore, some of the methods mentioned provide a meaningful reference, and the logic of their induction and comparison has greatly inspired this current paper.

By summarizing the literature review, it can be found that the main thread of foreign research is to instantiate the situational awareness model and method in the field of network security situational awareness, and continuously test and optimize the process in practice. In order to effectively analyze the research details of network security situational awareness, this paper concludes 75 papers in the core database in recent years and the research points of these articles are mainly concentrated on 9 aspects (the key points in these 9 aspects are shown in Table 3). The research content is mapped with the traditional Endsley model [36], the JDL model [40], and the logical phase of the OODA model [45]:

- The concept of the model (integration with other disciplines) [16, 18, 39, 45, 50–57, 63, 67, 68]
- The completeness and regularization of data acquisition variables [40, 42, 45, 47, 73, 87]
- The optimization of related algorithms [58–67]
- The information fusion analysis [40, 42, 53, 69–74]
- The automation of process tools [33–35, 73, 75, 84, 85, 87]
- The visualization of work at each stage [5, 11, 55, 61, 76–79, 86]
- Practice testing and efficiency gains in large-scale real-world networks [80–82]
- The software engineering implementation of sensing methods [42, 83–85, 88]
- The practical application of analysis and prediction results in specific fields [42, 47, 73, 79, 87, 89, 90]

(1). In the research for the concept of model, some papers are aimed at explaining interpretations of traditional situational awareness models in network security situational awareness (such as literature [16, 39, 45]). Some papers focus on the combination of situational awareness with security issues in specific fields. For example, Ralston et al. [47] summarize the safety perception problem of distributed control system and data acquisition control system. Barford et al. [48] defines and explains the scope, background, and research objectives of network-aware defense. Alexandros

Table 3 A statistical classification summary of 75 foreign languages based on literature abstracts



Classical model			Key Refinement Contents	Paper Quantity
Endsley Model[36]	JDL Model[40]	OODA Model[45]	Concept Refinement or Combine with other Subject	15
Perception of Elements	Sensors	Observations (topology and configuration,user and administrator activity,current threats,ongoing attacks,software and service vulnerabilities etc.)	The integrity and regularization of the observables Tools for Automation	8
	Source PreProcessing			
	Object Refinement			
Comprehension of Current Situation	Situation Refinement	Orient (Business processes-Inforamtion-Infrastructure-Services-Applications)	situational awareness algorithms Information fusion Visualization Efficiency improvement in large scale Software engineering realization	60
Perception of Future Status	Threat Refinement			
Decision	Cognitive Refinement/HCI	Decision	Results Application in Designated Areas	25
Performance of Actions		Action		

et al. [49] summarizes the security threats and detection technologies in the field of wireless networks. Literature [50] has incorporated sensitive devices into the priority perception area and showed that how the DPI is installed at the boundary of the network perceives the health of the system; some literatures try to integrate the concepts of other disciplines into network security situational awareness, such as the combination with game theory in literature [51–53, 63], the combination with Petri network [54], and the combination with the Bayesian network [55]; also, some other articles try to provide a more general operational model (such as the literature [56, 57, 67]).

(2). Data acquisition is the basis of network security situational awareness. The attention now is paid to how to ensure that the collected information is a complete set for the fusion analysis in next step (completeness) and to standardize the collected information to promote the mutual call between different systems (regularization). Giacobe [40] has effectively combed the scope of source data and entities. In literature [45], the categories of sensors are divided into three categories: activity, configuration, and topology. In addition, in the specific field, the scope or type of collected information may be different [42, 47, 73, 87].

(3). The research on perception algorithm or architecture accounts for the largest part in all literature, with a proportion of more than 70%. Most of the articles give the logic of the algorithm and the demonstration effect in the experimental application. Literature [58] divides the common methods in situation awareness into five categories: Bayesian approach, knowledge-based approach, artificial neural systems approach, fuzzy logic approach, and genetic algorithm approach. In the algorithm for network security situational awareness, there are algorithms for data sources (such as the algorithm for the attacker [59], the algorithm for intrusion detection data [60], and the algorithm for the vulnerability logic association analysis [61]). Some algorithms are targeted at the behavior analysis of attackers or defenders (for example, hidden Markov chains are used to predict internal attack threats in document [62], combined with game theory [63], machine learning method [64], and honeypot technology [65], etc.); also, there are many algorithms for improving efficiency and enabling them to be extended in large scale networks (such as real-time decision analysis method [66], and fast calculation method for static statistical data [67]).

(4). The fusion analysis ability on the related information is the advantage of network security situational awareness. The core method is to derive the hidden knowledge from the data from different sources. The related literatures are divided into three parts: one is the instantiation of data fusion model in traditional situational awareness in the network security situational awareness (such as [40, 42]); one is to propose a specific fusion technology or idea based on the characteristics of network security data. For example, Paffenroth et al. [70] and Mathews et al. [71] have designed data models or coordinate working systems to integrate data from different network sensors. Literature [69, 72] discuss the uncertainty in the network security situation. Sanfilippo [73] design a multi-sensor fusion framework to improve the perception ability; other literatures attempt to promote the efficiency of information fusion (e.g., [53, 74]).

(5). Automation based on the full use of the computing power of the computer is one of the effective ways to improve efficiency. In the IDS phase (the second stage of Table 1), the working mechanism of IDS is automated, but it also becomes the bottleneck of the system in turn, since the rule of the computer is not consistent with the perspective of human fuzzy evaluation. At present, the research on automation is mainly focused on information collection (such as literature [33–35, 75]). In addition, systematic implementation of the overall application effect has realized automatic processing to a certain extent (such as [84, 85]); the automation ability is also a prerequisite for the practical application of large-scale networks (e.g., [73, 87]).

(6). Visualization is undoubtedly an important part of network security situational awareness [86]. Tamassia et al. [76] give a clear statistical result on this aspect. Most of the current literature focuses on the friendly interaction between human and machine. Beaver et al. [77] effectively filter the analysis process and data in IDS and present them to administrators in a visual way. In literature [78], with the help of the unique professional knowledge of the participants, a real-time evaluation visual framework is designed to allow network managers to participate in the analysis loop manually; some articles focus on machine learning methods for visual rendering (such as artificial neural network [79] and cluster analysis [77]). In addition, most active analysis models such as attack graphs are combined with visualization technology [5, 11, 55, 61].

(7). Effect test constitutes the core of the model construction. In most of the articles, there is a chapter for the simulation experiment, but most of these experiments are analyzed with a brief abstract topology, for the verification of the correctness of the model. There are two aspects of research in this segment. One is the construction of basic data sets that can be used for horizontal comparison among multiple models (for example, the data set produced by the security contest held in literature [80] in 2010. Fink [81] collates the data set by each team in the competition). The other is the practice of wide area environment (at present, the attention to this aspect is little; literature [82] has made a preliminary attempt on this).

(8). Consideration for the overall logic rather than a certain segment is the consensus view of the scholars [83], in view of the fact that the overall logic means that it should be designed from the perspective of software engineering. Only on this basis, the process and result of perceptual analysis can become effective tools. D'Amico and Whitley [84] design the overall analysis process based on the different roles and present it visually; literature [85] gives a task flow chart according to processes, goals, and concerns. There is a long way to go now, and the design and realization of network security situational awareness can be done from the perspective of instrumentalism software, which integrates the characteristics of all kinds of users in the network, and give a friendly target understanding method when human-machine interaction with necessary attention [42].

(9). There are some articles concerning the analysis method of network security situational awareness and the practical application of prediction results in specific fields. The present statistical results mainly concentrate on three parts: one is the application of industrial control networks [47], especially in the field of power grid control [79, 87]; one is for the emergency management of the key equipment, such as the shared situational awareness metamodeling proposed in Literature [89] and the operational architecture proposed by Adams [90]; and another is in the military field [42], such as the practice application of nautical training [73].

2.3 Status of domestic research

When it comes to the dominance of policies China, great importance is attached to the network security from top to bottom. As a consequence, China has established the emergency response mechanism related to network security at all levels, which is similar to European and American countries, such as CCERT(China education and scientific research network computer emergency team), set up in May 1999, and CNCERT/CC (National Computer Network Emergency Technology Processing Coordination Center, referred to as the "National Internet Emergency Center"), established in September 2002, as well as the central network security and information leading group, formed on February 27, 2014. On April 19, 2016, General Secretary Xi Jinping emphasized the importance, task, and goal of network security in his speech at the Symposium on Network Security and Informatization [91], and clearly put forward that perceiving network security situation is the most basic and basic work. Due to the limited space, this paper does not make too much interpretation of China's network security policies and industrial development.

Domestic scholars have devoted great interest and enthusiasm to academic research. Almost every relevant core journal has dealt with the topics related to "network security." In order to summarize the current research situation in China and keep in line with the research ideas of foreign literature, this paper firstly sorted out the review literature based on the author's accumulation and effective search in this field. A total of 9 [17, 19, 92–98] comprehensive literature has a large number of citations or strong reference significance. In literature [92], the research and development of cryptography, trusted computing, network security, and information hiding in information security theory and technology are introduced. Especially in Section 4, Professor Feng Dengguo summarizes the research status and development trend of network information security and points out that the network-based security technology is the future trend of the development of the information security technology. Almost all network attacks are implemented by using the security flaws in system software or application software. Based on this premise, Liu and other scholars [93] conclude the research status at home and abroad from three aspects: malicious software, software vulnerabilities, and software security mechanisms from the perspective of software design for ensuring safety (study of the first stage in Table 1). Literature [94] provides an interpretation from the concept, necessity, structure of system, and basic model of intrusion detection and points out the development direction of intrusion detection system. In recent years, the research on the intrusion detection system probes further into the existing problems. Yingxu et al. [95] analyzes the characteristics and detection difficulties of industrial control system attacks. The performance and characteristics of different detection techniques are compared in order to provide theoretical support for researchers in the field of industrial control security. In 2005, Professor Lin Chuang of Tsinghua University [96] discusses the research methods and evaluation techniques used in the stochastic network security model which can be employed for the active evaluation and improves the network survivability. The analysis shows that most of the active evaluation models in the last 10 years (the third stage in Table 1) are extended on the basis of the models described in this article. In the study of situational awareness, literature [97] introduces the basic concepts of network situational awareness and expounds the relationship between situational awareness and IDS. Gong et al. [98] put forward a logical research framework on the basis of full understanding of situational awareness and attached emphasis on the method of network assessment. Based on the fusion algorithm of cross-layer swarm optimization, Liu et al. [17] puts forward a cognitive sensing and control model. Under the background of the transition of network development from perceptual network to perceptual network, the related algorithms of quantitative perception are given. Gong et al. [19] discuss the relationship between network security situational awareness and situational awareness at the conceptual level and further proposes the definition and explanation of network security situational awareness. Based on Endsley's three-stage model [14], the stages of network security situational awareness are divided, and the specific analysis methods of each stage are compared.

In light of the comparison between the domestic and foreign literature, it is found that the time Chinese scholars pay attention to network security situational awareness is close to that of foreign scholars, but most of them are in the state of "following," with few original and innovative articles. Most of the high-cited articles in ESI are aimed at the breakthrough of the model algorithm optimization and application level [96, 99], especially in the aspect of situation quantitative computing perception [115, 117, 124, 129], which can be regarded as the main line of domestic research in this field. At the same time, after a careful screening of domestic research literature, it can be found that a considerable number of articles on the topic of "information fusion, situational awareness" only stay at the micro-cognitive level (which is generally different from foreign literature based on the improvement of Endsley's model [36], JDL model [40], and OODA model [45]), that is, more data sources are integrated from the bottom up instead of the top down. However, these first partial then overall studies have also made remarkable progress and have played an obvious role in promoting the whole field. By summarizing about 100 articles among core journals in the CNKI, the research focus of these articles is mainly concentrated on five aspects (the summary of the key research contents in these five aspects and the typical article representatives are listed in Table 4):

- The definition or explanation of concept [17, 19, 97, 98, 100–102]
- The intrusion detection data fusion [103–107]
- The active evaluation model attempt [96, 101, 108–114, 124–126, 128, 129, 132, 143, 153–155, 159–162, 177]
- The systematic evaluation after quantification [102, 109, 115–117, 121–124, 173]
- The implementation of design and application in special fields [92, 118–120]

(1) The research on the definition or interpretation of the concept mainly focuses on two aspects: one is the basic conceptual explanation, and the other is the practical significance of network security situational awareness in special field after merging with other subjects. The basic conceptual explanation is mostly found in the summary literature, such as the definition of the basic content and research category in literature [100], the description of the concept of intrusion detection in literature [19], and the definition of the network security situation perception by the literature [17, 19, 97, 98]. Prior to achieving multisensory integration with other disciplines, it is necessary to do the abstract definition,

Table 4 Statistical classification of about 100 Chinese literature based on titles and abstracts

No	Focus	Key Improvement Contents	Typical Case	Paper Quantity
1	Definition or explanation of concept	General conceptual interpretation Model meaning after combining with other disciplines	Definition of basic content and research category in SA[101] Review Papper[17,19,98-99] Color Petri Net[102], Risk propagation model[103]	12
2	Intrusion detection data fusion	More data sources Data fusion and utilization	Data classification[104], Combination of data attributes and temporal and spatial attributes[105] Fusion example in [106],[107],[108]	26
3	Trying in Active evaluation model	Model definition based on cross discipline Model solving algorithm Application of solution result	Petri Net[97]、Game Theory[109]、Bayse Net[115] Algorithm and its application(Analysis based on attack graph[110-115])	42
4	Systematic evaluation after quantification	Systematization of evaluation index Index quantification Solving quantization results and using	Classification based on Security attribute angle[122] Classification based onaggressive behavior[103, 123-125] Application of risk assessment[116-118]	16
5	Tools and application in specific field	Implementation of software tools Application results in specific fields	ISACISAC, Safety incident plan system, Large scale network security state simulation platform[93] ICS[119-120], ECPS[121]	25

which can explain whether the integration is effective, and the effect after the combination, such as the definition of color Petri net (CPN) in literature [101] and the definition of risk propagation model in [102].

(2) The fusion and utilization analysis on IDS includes two aspects: the collection of more complete data sources and the integration and utilization of multiple types of data. In the collection of multi-data sources, there is a good display in the evaluation framework of literature [103]. Li and Lan [104] combine data attributes with time attribute and space attribute, which is beneficial to the evidence fusion of subsequent data; there are lots of articles for multi-type data fusion; literature [105] combines multiple IDS and manual survey techniques, and studies its optimal allocation and strategy based on game theory. Ren et al. [106] puts forward an intrusion detection model based on data mining and ontology, which can cluster and classify the underlying alerts, discover and filter attacks, and then based on the established ontology attack knowledge model, correlate these attacks to identify, track, and predict the effect of multi-step attacks, such as the fuzzy clustering anomaly intrusion detection method in literature [107].

(3) The attempt of the active evaluation model mainly revolves around the attack model, and each article usually contains three components: model definition, model solving algorithm, and solution result. The definition of the model is generally combined with other disciplines, such as Petri network [96, 153–155], game theory [108, 124, 159–162], and Bayesian network [114, 132], and some articles also focus on the improvement of model description ability [125, 126]; the solution algorithm depends on the definition of the model, and it is generally shown together with the solution result. There are lots of literature [109–114] trying to improve on this point, such as the reachable path analysis based on attack graph [101, 128, 129, 143, 177], defense strategy analysis [111, 124, 161], and survivability analysis [126].

(4) There are three main parts in the systematic evaluation after quantifying: systematization of evaluation index, index quantification, and quantified results and its application. The research on the systematization of evaluation index and the quantification of corresponding indicators mainly proceed from two angles: security attribute and attack behavior. From the perspective of security attributes, it is more focused on the definition and interpretation of network security. For example, Wang et al. [121] propose an attack technology classification method to meet the Amoroso classification standard; from the perspective of attack behavior, most of the researches take the attack as the center to quantify the important factors in the attack process. According to the statistics and analysis of the existing literature, the quantification of the 3 elements (attack severity, attack occurrence/success probability, and attack income) has basically formed a certain standard [102, 122–124]. On the basis of index system and index quantification, risk assessment algorithm can be developed to get the perception or evaluation result [109, 115–117].

(5) The active participation of all parties will definitely promote the production of relevant research results and deepen the application in the industry. The emergency response of China's network security follows the PDCERF methodology (the preparation, detection, eradication, suppression, recovery, and tracking of 6 stages). A large number of practical products and systems have been put into use, such as information sharing and analysis center, large network security events coordination early warning positioning and rapid isolation control, security event planning system, large-scale network security state simulation platform, linkage system, and backup and recovery system [92]; on the combination of industry applications, similar to foreign countries, it mainly focuses on two aspects: ICS [118, 119] and ECPS [120].

2.4 Summary of the present research

This section summarizes the research history, development stage, and present situation at home and abroad of network security situational awareness. In general, in the background of winning the commanding heights of network security strategy for all countries, the research on this aspect is of great significance and has made considerable progress, but the result of the study is still on the path of exploration, and the main problems are concentrated in three aspects.

Firstly, there is no comprehensive analytical perspective in terms of concept and ideology. Foreign researches mainly focus on the instantiation of situational awareness in this field, and domestic researches concentrate more on the integration of more information and efficiency improvement. However, according to the summary of Table 1 in this paper, network security situational awareness is a more advanced stage of network security research. It is not a model or a method. It should be a more valuable framework from all the existing network security concepts or means.

Secondly, there is no practical deep integration at the level of model and algorithm. Both foreign and domestic articles on models and algorithms are over 70%. Although multidisciplinary integration is an important breakthrough in this field, after the groundbreaking formulation, most of the articles begin to model and algorithm optimizations blindly. This is incorrect since these improvements should be carried out on the basis of integration practice. In addition, fusion perception must be a process of multiple cycles between information and decision-making. Most of the existing models are unidirectional, and the level of feedback effect should be effectively embodied in the model after perception decision.

Thirdly, there is no meaningful horizontal comparison in terms of effectiveness and application level. Every article or model will be verified by experiments, but few articles are compared as a whole. The existing and previous literature are more compared in the complexity of the algorithm, and the result of perception is a comprehensive synthesis of intelligence. It is different to judge directly for so many constraint factors, and the current application value comparison should focus on the horizontal comparison within a certain stage based on a standard data set.

The following chapters are arranged as follows: The second section abstracts the experiment object from the actual network topology and configuration of a medium scale software company to ensure the accuracy verification and relative comparison in the following chapters under the same standard. In the third section, from the perspective of system engineering, the network security situational awareness analysis is divided logically and gives out a new reasonable frame. From the fourth to the eighth, each segment of the whole framework is expounded, focusing on the role of this segment, the mainstream method, the application results on the experimental network, and the horizontal comparison between the methods within a certain segment. The ninth section briefly introduces the research dimension and direction of network security in a big data environment. The tenth section is the summary of the full text.

3 Experimental basis

In order to effectively compare and summarize the different methods in different stages of the proposed framework, this section first briefly introduces the experimental environment used in this paper as the basis for subsequent chapters. A medium-sized software development company is chosen as an experimental object. Figure 2 is the network topology graph of the enterprise. The network God is used as the monitoring device between the internal and external networks through the dedicated telecommunication lines and the external network links. 10.10.0.10 is a web server which provides the function of publicity website and product demonstration. 10.10.0.140 is a log server that can be accessed from the external network (because company personnel are often on business trips, both internal and external network access are required to go through the external network). 10.10.0.15 is the company's database server, running SQL Server, Oracle, the two relational databases, and a non-relational database MongoDB. 10.10.0.16 is the test server, and the products the company has delivered and is developing have the latest version of the deployment on the test server. 10.10.0.11 is the internal development server. All the company's source code and important project solutions, process information, etc. are all on this server. The company has a development team of about 100 people, which is mainly divided into two categories due to the different development technologies. 10.10.0.58 represents the technical team developed by.net, and 10.10.0.59 denotes the technical team developed by Java.

4 Logical analysis framework

Network security situational awareness usually involves multiple different phases, and the systematic approach is preferred to process the data related to cybersecurity. There are two main methods for logical division: the first method is the engineering hierarchical method (such as Figure 2 in literature [45], Figure 3 in literature [97], Figure 1 in literature [103], and Figure 4 in literature [126]) and the second is the conceptual hierarchy (such as Figure 3 in literature [45] and Figure 1 in literature [14]), but neither of these methods can provide an

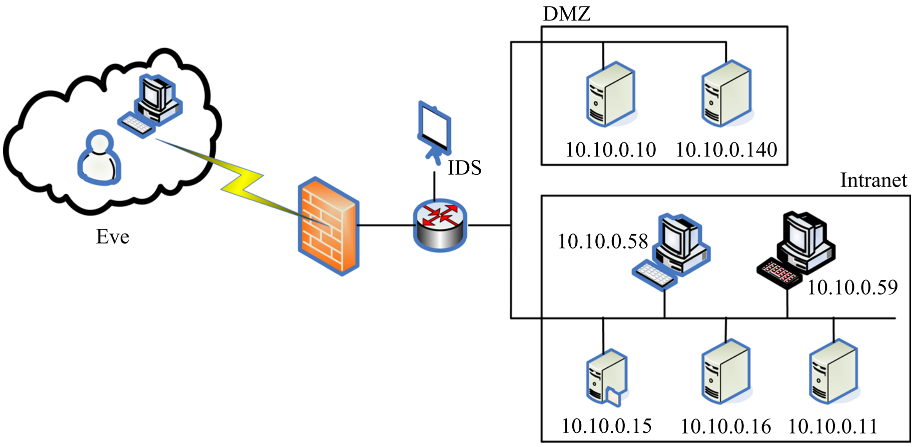


Fig. 2 The graph of experimental network topology

easy-to-understand architecture from the perspective of the data processing stage. From the perspective of data value chain, the present paper adopts the systematic engineering method which is widely accepted by industry to decompose the typical cybersecurity situational awareness process into five continuous processing stages, including element acquisition, model representation, metric establishment, solution analysis, and situation prediction, as is shown in Fig. 3 below.

(1) The element acquisition phase is concerned with how to effectively obtain the security-related data as much as possible, which is mainly divided into two tasks: data acquisition and data preprocessing. Data acquisition refers to the effective storage process including collecting configuration information in the network, behavior information in the log, and vulnerability information which can be achieved by using a scanner, a sensor, or a specially written tool. Data preprocessing is a process of regularizing original data before data modeling or analysis and utilization.

(2) The model representation stage is focused on the correlative expression of the effective elements, which is mainly divided into two tasks: element reduction and formal representation. According to the purpose of the analysis, it is necessary to reduce the acquired objects effectively during the element acquisition process in order to achieve the efficient analysis. The formal expression refers to the process of precision abstraction including the attributes of the reduced elements, the relationship between the elements, and the order relationship.

(3) The metric establishment stage is the process of refining the value of each element object before the solution analysis, mainly including the quantitative classification and evaluation index system to determine two tasks. The quantitative process is a process of numerically assigning the attribute values of each element (in this present paper, the qualitative classification is treated as a special quantitative classification without special explanation), and the confirmation of the evaluation index system is the process to regularize the logical relationship between the attribute values of the elements.

(4) Solution analysis is the algorithmic process based on the first three stages mentioned above, which mainly includes three tasks: the determination of the solution algorithm, the verification of the correctness of the algorithm, and the improvement of the algorithm. The solution algorithm is the process of effectively combining the target with the model and the metric to ascertain the analysis step. The correctness verification of the algorithm is to validly correspond to the input and output of the algorithm. On this basis, the efficiency of the algorithm should be considered to improve in order to expand in the true scale network environment.

(5) Situation prediction is a process of comprehensive evaluation and decision-making based on the analysis results, which mainly includes two tasks: result visualization and decision-making after knowledge application. The result visualization is the process of presenting and constructing the solution results in an easy-to-understand way. After the analysis and decision-making, the feedback loop will be applied to the current network for cybersecurity reinforcement (such as vulnerability repair and configuration upgrade) to complete a perceptual loop.

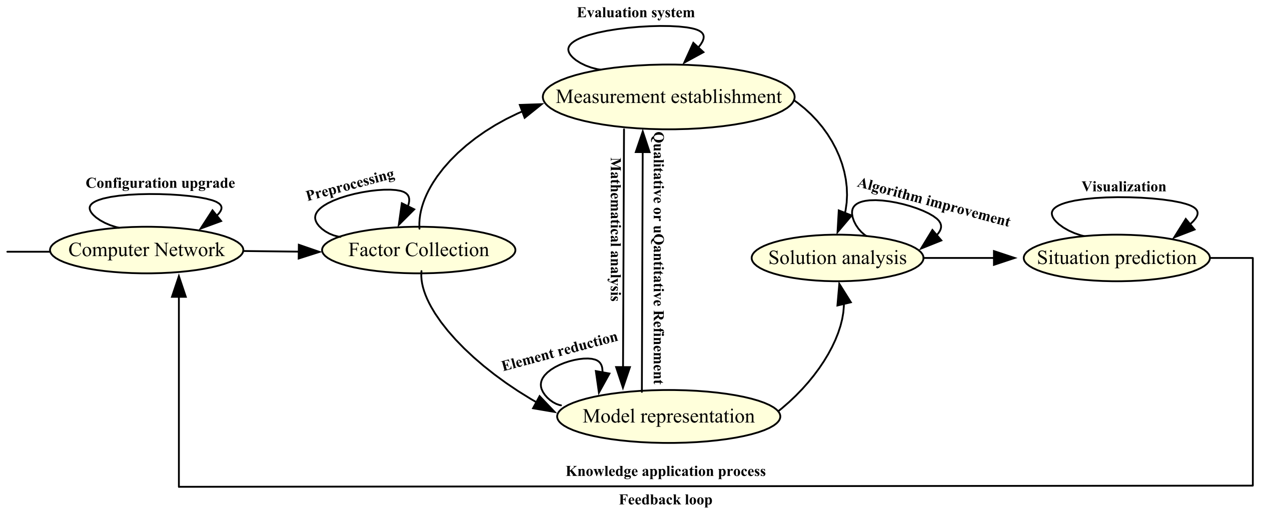


Fig. 3 Network security situational awareness operation mechanism

5 Phase I: Element acquisition

The function of the element acquisition phase is to effectively capture the key data used in each phase of the cybersecurity situational awareness. In general, element acquisition refers to the collection of all the elements related to cybersecurity. In the narrow sense, element acquisition refers to the collection of the elements involved in a certain perception process. The purpose of this present paper is to sort out the basic framework of cybersecurity situational awareness, and the core implementation methods of each stage are compared horizontally, so the element acquisition in this current paper refers to the generalized element acquisition.

Undoubtedly, element acquisition is the premise of cybersecurity situational awareness. Other subsequent stages are unable to work without basic data collection. Most of the documents collected so far have clearly defined the functions and important impacts of this stage in the logical description of the framework. However, as for the implementation, most of them only mention the data acquisition through automated scanning tools or sensors, and according to the following-up model to directly stipulate or preprocess, there are also some literature introducing the way to obtain data or tools [33–35] and so on. Strictly speaking, element acquisition is divided into three parts: data generation, data acquisition, and data preprocessing. In light of the division of logic analysis framework in Section 3, data preprocessing is generally carried out after the model definition or measurement establishment phase. Data acquisition is generally completed by combining manual and automatic methods. The focus is generally on the development of automated tools. This section focuses on the classification of data from the perspective of data generation.

In the existing cybersecurity situational awareness literature, the basic data collection part is mostly according to the needs of model analysis to reverse the data used (narrow element acquisition), which is not conducive to data standard unification and model-to-model comparison verification. According to the logic of engineering, this present paper briefly summarizes and classifies the data in cybersecurity analysis from the perspective of data generation.

Here, the data is divided into two categories: static data and dynamic data. Static data refers to data that does not change substantially in a cybersecurity situational awareness analysis cycle shown in Fig. 3. Dynamic data refers to changes in the cybersecurity situational awareness analysis cycle shown in Fig. 3 as the analysis process going on. As shown in Table 5, the static data mainly includes host information (such as host IP address or MAC address unique identifier, running service or program, file, data and other confidential assets, operating system, hardware composition, system configuration, and permission configuration), network information (such as network device information, network topology information, protocol information, firewall information, and network configuration information), and IDS information (such as basic information of intrusion detection system, expert knowledge base, and alarm information), and the dynamic information mainly includes activity information (such as source address, destination address, and activity description), behavior information (such as source address, destination address, protocol in use, transmission data size, and compression algorithm), vulnerability information (such as vulnerability name, logo, basic information such as release time, vulnerability host information, attack methods, attack effects, and repair methods), attack information (such as attack source address and attack method), and perceived result information (e.g., perceptual result information of the last perceived loop and the action information after perception).

6 Phase II: Model representation

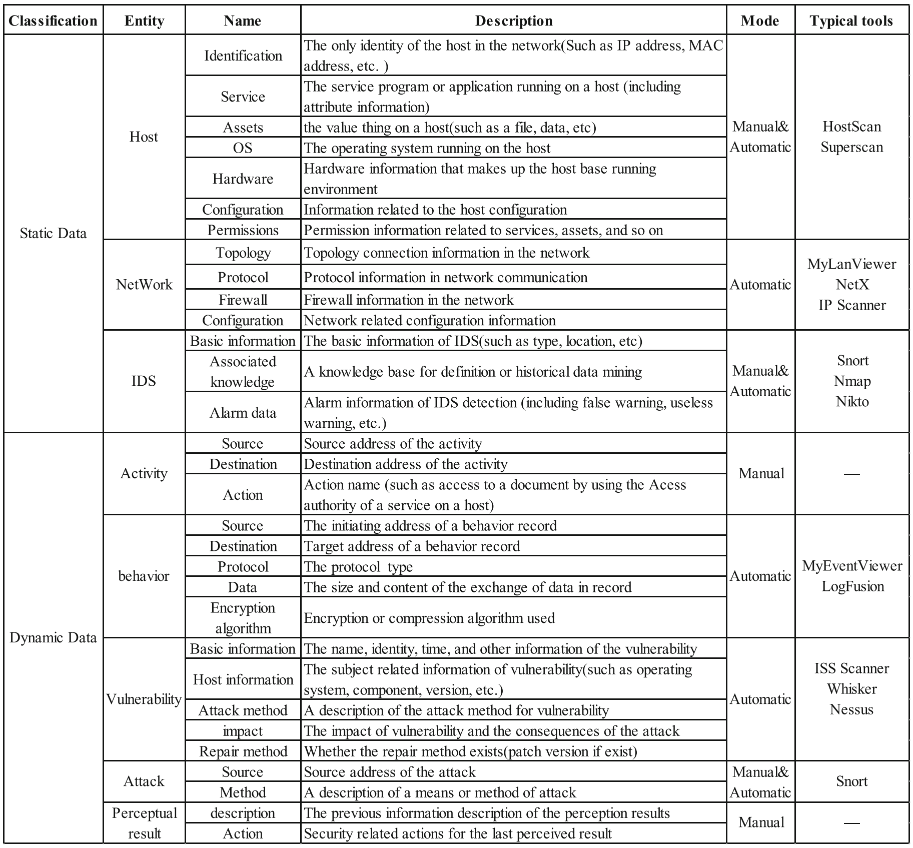
Formal modeling is the key link in the cybersecurity situational awareness operation mechanism. The description ability in the modeling stage of reduced state and formalization will directly affect the subsequent perceptual analysis results. Through the summary of the existing literature, the cybersecurity situational awareness model is mainly divided into three categories: mathematical model, stochastic model, and biological heuristic model. The core concepts and typical representatives of each classification are shown in Table 6 below.

6.1 Mathematical model

The mathematical model is used to analyze the cybersecurity situational awareness. The main idea is to use mathematical language or mathematical symbols to summarize or approximate the security-related features or quantity dependencies of computer network systems. The mathematical model here refers to the mathematical model in the narrow sense, that is, the mathematical expression of the relationship between variables in the cybersecurity system. Therefore, the perceptual analysis method based on a mathematical model is more biased towards the form of quantitative analysis. It mainly includes analytic hierarchy model, Bayesian model, fuzzy set/rough set model, reliability/survability model, etc.

The Analytic Hierarchy Process (AHP) was proposed by Professor T.L. Saaty and is now widely used in decision-making. Chen et al. [99] proposed a hierarchical security threat assessment model (Fig. 4 is the model results obtained by the experimental network according to the method in literature [100]), and Fig. 5 is Tomcat service, FTP service, and the overall security situation of each host

Table 5 Classification results of entity and data in element collection

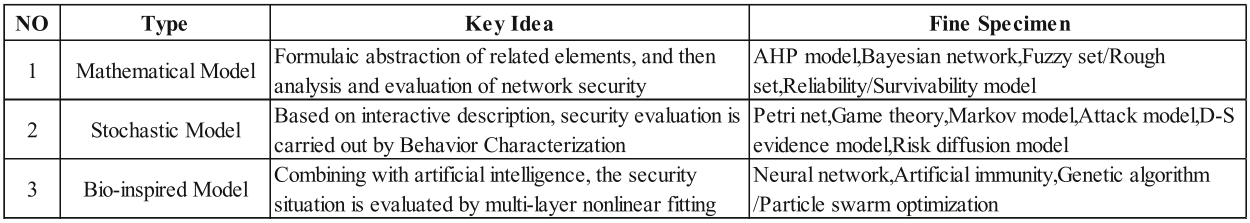


Classification	Entity	Name	Description	Mode	Typical tools
Static Data	Host	Identification	The only identity of the host in the network(Such as IP address, MAC address, etc.)	Manual& Automatic	HostScan Superscan
		Service	The service program or application running on a host (including attribute information)		
		Assets	the value thing on a host(such as a file, data, etc)		
		OS	The operating system running on the host		
		Hardware	Hardware information that makes up the host base running environment		
		Configuration	Information related to the host configuration		
		Permissions	Permission information related to services, assets, and so on		
	NetWork	Topology	Topology connection information in the network	Automatic	MyLanViewer NetX IP Scanner
		Protocol	Protocol information in network communication		
		Firewall	Firewall information in the network		
		Configuration	Network related configuration information		
	IDS	Basic information	The basic information of IDS(such as type, location, etc)	Manual& Automatic	Snort Nmap Nikto
		Associated knowledge	A knowledge base for definition or historical data mining		
		Alarm data	Alarm information of IDS detection (including false warning, useless warning, etc.)		
Dynamic Data	Activity	Source	Source address of the activity	Manual	—
		Destination	Destination address of the activity		
		Action	Action name (such as access to a document by using the Acess authority of a service on a host)		
	behavior	Source	The initiating address of a behavior record	Automatic	MyEventViewer LogFusion
		Destination	Target address of a behavior record		
		Protocol	The protocol type		
		Data	The size and content of the exchange of data in record		
		Encryption algorithm	Encryption or compression algorithm used		
	Vulnerability	Basic information	The name, identity, time, and other information of the vulnerability	Automatic	ISS Scanner Whisker Nessus
		Host information	The subject related information of vulnerability(such as operating system, component, version, etc.)		
		Attack method	A description of the attack method for vulnerability		
		impact	The impact of vulnerability and the consequences of the attack		
		Repair method	Whether the repair method exists(patch version if exist)		
	Attack	Source	Source address of the attack	Manual& Automatic	Snort
		Method	A description of a means or method of attack		
	Perceptual result	description	The previous information description of the perception results	Manual	—
		Action	Security related actions for the last perceived result		

and local area network are security situation quantification results, based on the subjective quantization method in literature [99]; Tomcat service, FTP service, and the overall security situation of each host and local area network are security situation quantification results. The hierarchical model is consistent with the decision-maker's thinking process in both the analysis and the calculation process, which ensures the results are intuitively understandable (for example, the security situation index is relatively high in Fig. 5 at around 17:30; because most people fill in the logs around this moment, the frequent external network mapping will lead to higher security risks). The construction of an effective hierarchical structure is the key to the application of this model, and some literature has studied the instantiation of the hierarchy [127], but the current element quantization process basically adopts the subjective experience value method, which cannot be compared and quantified between every two factors in the classical analytic hierarchy process, thus leading to the lack of objectivity, and the current hierarchical structure is only suitable for the local area network which contributes to the difficulty in carrying out large-scale promotion, as well as no effective prediction of the future situation.

In order to effectively reflect the uncertainty and subjective elements in the cybersecurity situational awareness analysis, the probabilistic method is usually used for quantitative description [128, 129], in which Bayesian logic is the most commonly used model. The relationship rules and mathematical reliability of Bayes are very similar to those of human thinking reasoning. Bayesian calculation

Table 6 The main model and its classification of network security situational awareness



NO	Type	Key Idea	Fine Specimen
1	Mathematical Model	Formulaic abstraction of related elements, and then analysis and evaluation of network security	AHP model,Bayesian network,Fuzzy set/Rough set,Reliability/Survivability model
2	Stochastic Model	Based on interactive description, security evaluation is carried out by Behavior Characterization	Petri net,Game theory,Markov model,Attack model,D-S evidence model,Risk diffusion model
3	Bio-inspired Model	Combining with artificial intelligence, the security situation is evaluated by multi-layer nonlinear fitting	Neural network,Artificial immunity,Genetic algorithm /Particle swarm optimization

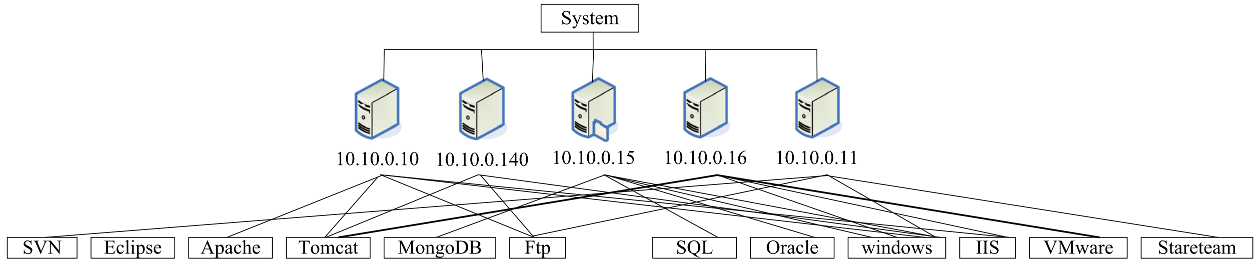
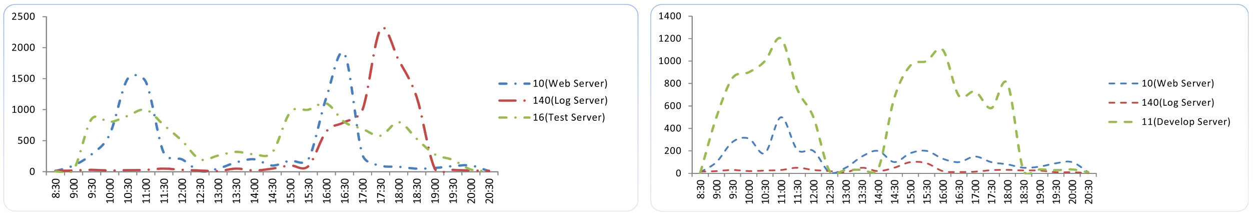


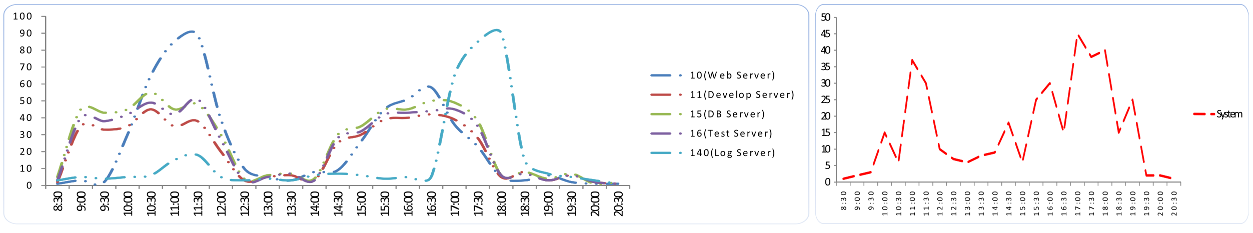
Fig. 4 Hierarchical structure partition diagram of experimental network

can synthesize the latest evidence information and prior information to ensure that the calculation results maintain two important characteristics: continuity and accumulation. There are literatures adopting Bayesian mathematical methods for cybersecurity situational assessment [131], but most of them are used as quantitative computing tools in combination with other models, especially the combination of Bayesian and attack graphs [114, 130, 132], combining graph theory and probability theory to complete a Bayesian network, using graph theory to show the structure and interdependence at the qualitative level, and using probability theory to carry out quantitative expression and reasoning at the quantitative level. Some progress has been made in this perspective, but the Bayesian network is a decomposition form of the joint probability distribution at the theoretical level. The variables in the actual solution are not independent from each other, and the joint probability is too complex to suit the large-scale networks.

The fuzzy set contraposes the traditional set. In the traditional set, the relationship between the object and the set is clear (either one or the other), but in reality, some objects do not have a clear affiliation of the set, There exists an interval of degree of membership (membership function). Some literatures apply fuzzy similarity and fuzzy comprehensive evaluation in cybersecurity situational awareness analysis [133, 134]; the rough set extends the classical set theory, which uses the upper and lower approximations to approximate any set, and it can analyze incomplete information such as inaccuracy, inconsistency, and incompleteness without prior knowledge, discover hidden knowledge, and reveal potential laws. Zhao and Xue [135] and Kong et al. [136] utilized the idea of rough concentration mode classification in the cybersecurity situational assessment, using each security evaluation index as the condition attribute set C, and determining the decision attribute D of the load situation assessment result according to C and then according to the D synthesis comprehensive security situation network. However, the current research in this area is limited to describe the uncertainty in the process of fuzzy sets or rough sets, and it is impossible to combine the target or core problem of cybersecurity situational awareness with the fuzzy set or rough set method. The practicability and the continuity of research are limited. In combination with other models or methods, it is generally carried out at a certain point in



a threat situation of Tomcat on server **b** threat situation of FTP on server



c threat situation of Host Level **d** threat situation of System Level

Fig. 5 Hierarchical security situational awareness results of experimental network. **a** Threat situation of Tomcat on server. **b** Threat situation of FTP on server. **c** Threat situation of host level. **d** Threat situation of system level

the analysis process and adopted more as a quantitative tool for uncertainty.

Feng et al. [137] combined the reliability theory with the vulnerability analysis process to quantify the security of the distributed system. It is intended to ascertain the system maintenance probability of the security state under the specified conditions and the specified cost *c* through the reliability function Rs(*c*). Figure 6 below is the vulnerability state modeling result of the attack on the Ftp service on 10.10.0.11 (internal development server) according to the literature [137], and the average attack cost for this service is $E(C) = 1/\lambda_1 + 1/\lambda_2 + 1/\lambda_3 + 1/\lambda_4 + 1/\lambda_5$. In literature [138], the mathematical conditions are used to obtain the criteria of complete probability control or partial probability control of complex attack networks. It is theoretically proved that if there are effective defense nodes in the network, the complex network can still provide normal service when it is attacked and destroyed and suggests ways to defend against node selection and control networks. The advantage of adopting the reliability or survivability model for cybersecurity situational awareness analysis is that there is a mathematical derivation process to ensure the rigor of the analysis, but the preconditions of these formulas also greatly limit its large-scale network conditions of actual perceptual analysis, the diversity of influencing elements in the real network often makes the calculation result unsatisfied, and the model generally cannot provide the repair method after confirming the network insecurity state, so that the system has the ability of active defense.

6.2 Stochastic model

The stochastic analysis model is a non-deterministic model. Its main feature is that the exogenous variables in the model will change with specific conditions, which has a high degree of fit with the occurrence of cybersecurity-related behaviors. During the attack, the choice of the attacker's assault means the choice of the defender's resist strategy and the normal user's operation are random. Using a stochastic model for cybersecurity situational awareness, it is possible to describe the logical relationship between the random behaviors and behaviors of various elements of the system more clearly, and thus, it is easier to fully describe the network status, and it can also include the influence of unknown behavior, based on Stochastic model cybersecurity situational awareness is the focus of current academic circles, including attack tree/graph model, Petri net, game theory, and Markov's model.

The attack tree model was proposed by Scheier [139] in 1999. It can be seen as an extension of the fault tree, which is intuitive and easy to understand, but the description capabilities are limited. The attack graph model was first proposed by Swiler and Phillips [5] in 1998. It is currently the most widely used method. Sheyner et al. [140] adopt the model detection method to generate the attack graph, and Ammann et al. [61] generate an attack graph through the idea of graph theory which starts from the initial state and searches forward. The literature [141] focuses on the attack, and a tool for generating an attack graph is given. There are also literature focuses on large-scale construction and visualization of attack graphs [142, 143]. Early attack graphs tend to construct state attack graphs [5, 61, 140–143], but it is easy to cause the explosion of state space. As the research progresses, it tends to construct the causality diagram [144], and its edges represent the connection relationship between nodes or the logical relationship of atomic attacks, which is more scalable and easier to use for large-scale networks. Figure 7 is the result of the attack graph of attacker Eve attacking the FTP service located on the development server (10.10.0.11) in the experimental network in Section 2. Figure 7a is a graphical description, and Fig. 7b is a formal description of the attack step. The advantages of attack graph model is directness and descriptive and is easy to combine with other methods which are the currently basic model of cybersecurity situational awareness analysis; the current research focuses on the refinement of the original [125]

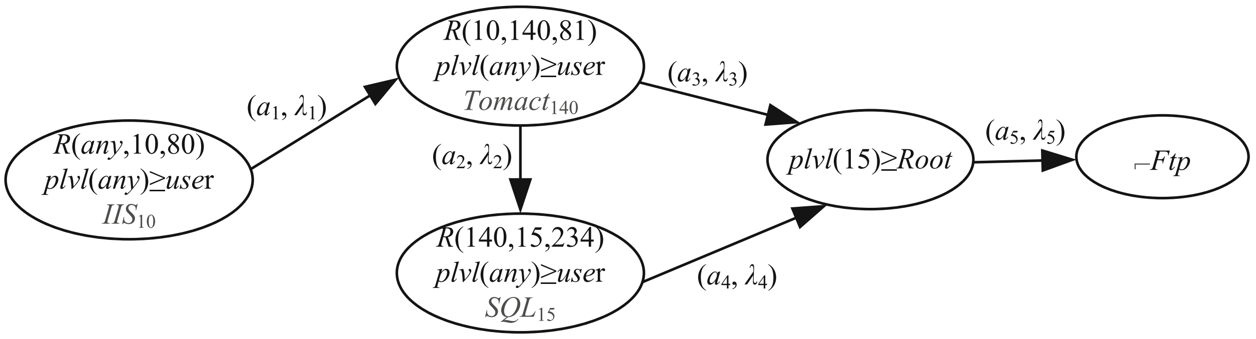
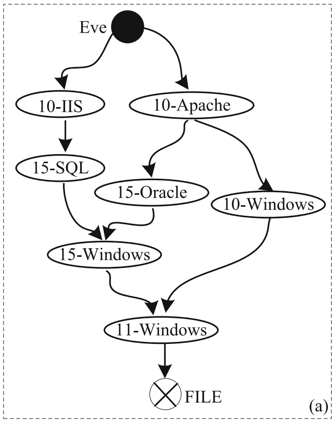


Fig. 6 Modeling results of reliability quantitative model of experimental network



Attack Apache Privilege escalation (CVE-2011-3607) is
Intruder preconditions
[*User-level privileges on host S*]
$plvl\ (S) \geq \text{user}$
[*No root-level privileges on host T*]
$plvl(T) < root$
Network preconditions
[*Host T is running Apache*]
$Apache_T$
[*Host T is reachable from S on port* s_p]
$R(S,T,s_p)$
Intruder effects
[*Root-level privileges on host T*]
$plvl\ (T) = root$
Network effects
[*Host T is not running Apache*]
$\neg$Apache
End
(b)

a A graphical description of an attack graph **b** Formal description of Apache attacks in attack steps

Fig. 7 An attack map for FTP on 11 servers in the experimental network. **a** A graphical description of an attack graph. **b** Formal description of Apache attacks in attack steps

or improved model [145] to enhance the description ability and fusion with other disciplines [11, 146] and thus to enhance the analytical ability.

Models similar to the attack graph also include privilege graphs and state transition graphs. Dacier [147] abstracted the nodes in the graph into the permission state and proposed the privilege graph model. Ortalo et al. [148] established the Markov model based on the concept of privilege graph and presented the security evolution process. Dr. Wang Lidong [149] refined this process, but the privilege graph model is difficult to describe the dependencies between states or random events, so subsequent research on the extension of this model has little influential results; Porras and Kemmerer [150] proposed the intrusion detection method based on state transition graph for the first time. Each node in the graph represents a temporary state of the system, and the edge represents the state transition and transfer process. The probabilistic model in literature [151], the semi-Markov process model in literature [152], and so on are all the extensions based on it. The advantage of the state diagram is that it is more descriptive, but there are problems of state space explosion under large-scale networks, and the solutions to this problem [128, 143] are still not satisfied.

Petri Net (PN) was first proposed by Karl A. Petrie in 1962 to perform effective mathematical simulations of discrete parallel systems. It consists of three elements: place, transition, and the directed arc (Arc); $N = (P, T; F)$ can have any number of tokens in the place to represent the resource (Token), and the initial application scenario is through the flow of Token in the place to detect the protocol Error (deadlock state). In the combination of Petri net and cybersecurity situational awareness, the place P usually represents the descriptive local state of the system. The transition T represents an attack event or normal activity that can change the state of the system. The directed arc F effectively associate the local state and the event. On the one hand, it refers to the local state that can cause the change to occur, and on the other hand, it points to the change of the local state caused by the change. The following Fig. 8 shows the experimental network in the second section which is the Petri net model modeling result of the FTP service attack for 10.10.0.11. Compared with the classic Petri net, the place is not a Token, but the probability of a transition occurring in a local state. The number attached to the transition represents an attack or success probability, on this basis, qualitative reachable identity analysis or quantitative analysis by correlation matrix, state equation, etc., for example, using the "or" principle of maximum risk estimation (maximum probability between different paths) and the probability of the intermediate place P7 is max $(0.4 \times 0.4,\ 0.7 \times 0.5,\ 0.8 \times 0.1) = 0.35$. It can be seen that Petri net not only has the characteristics of intuitive and vivid of graphical modeling, but also is more suitable for asynchronous and parallel attack process. The research progress in this direction includes coloring Petri nets with increased model description ability [153], a stochastic Petri net with increasing random occurrence time for transitions [154], a fuzzy Petri net described for uncertainty in the modeling process [155], etc.

With the deepening of cybersecurity situational awareness research, researchers have realized two problems: First, the cybersecurity confrontation process is not simply a technical matter, and different people who apply in different scenarios will produce the opposite result with the same technology implementation means; Second, the analysis of cybersecurity must not be the behavior of one party. In an environment with active defense, the security situation will variate on the choice of two or more

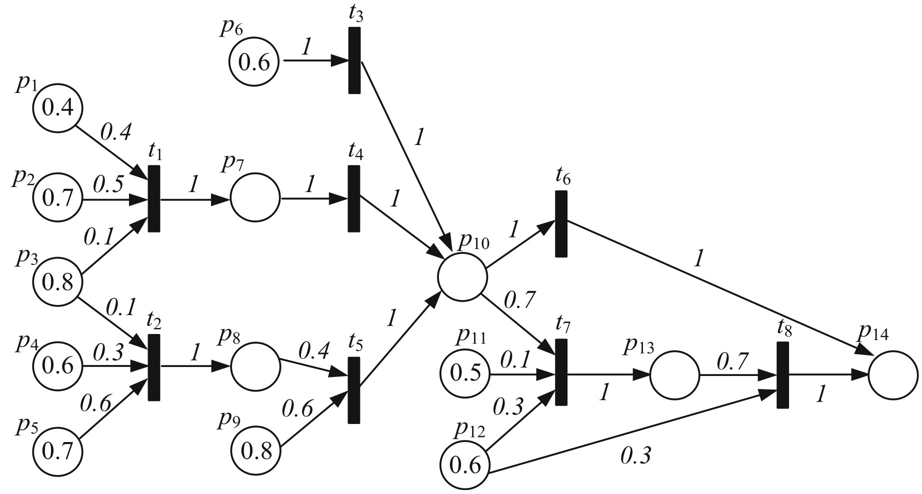


Fig. 8 Petri net modeling results for FTP attacks on 11 servers in the experimental network

parties, which has a very high degree of agreement with the strategic dependence of game theory. Once proposed, it has become a hot topic of research [156]. Traditional research on intrusion detection or aggression behavior is based on a game analysis [157]. Considering the application in the real environment, it is certainly a repetitive multistage incomplete information dynamic game [158], and there is a refined Bayesian Nash equilibrium. Each cybersecurity situational awareness model based on game theory contains at least five parts: $N = \{1, 2,\ldots,n\}$ is a collection of people in the game (generally combines multiple similar objects and divides them into attackers, defender, and normal user $|N| = 3$). $S = \{S_1,S_2,\ldots,S_k\}$ is the set of game states in the offensive and defensive process. $\theta = \{\theta_A, \theta_D\}$is the set of action strategies of both offense and defense. P is the transition probability between game states S. $R_n = S_i \times \theta \times S_j \in (-\infty,+\infty))$, which represents the income function of the person n in the state S_i transitioning to the state S_j; $GM = \{N,S,\theta,P,R\}$, according to this basic definition, after a finite-step (k-step) game process, the system transforms between different states to form a tree structure, the goal of the player is to make their function maximized, and the model's Nash equilibrium strategy f^{*} can be obtained by means of Shapley algorithm or problem transformation solution [162]. The combination of game theory makes the focus of cybersecurity situational awareness rise from technology to management strategy and can portray the psychological activities of each participant, which greatly improves the description ability of the model and the scientific nature of the analysis results. The improvement direction focuses on static game turning to dynamic game [159], model-related element quantification [10], or combining with other methods [160] and presents practical application effects [108, 124, 161], etc.

The basic idea of the Markov model is that the transition of the next state is only related to the current state but not the historical state. The Markov model consists of three elements: S is the set of non-empty states composed of all possible states of the system, P is the system state transition probability matrix, and Q is the initial probability distribution of the system, $M = \{S,P,Q\}$. The intention of applying the Markov model to the cybersecurity situational awareness is to predict the attack and defense evolution effectively when the initial conditions are met, but there will be a large number of camouflage attacks or covert attacks during the attack. Forcing the application with inefficiency will lead to the extreme result of statistics (overexaggerating the impact of a certain accident or neglecting the impact of a key step), so Markov is generally combined with other models [53, 109, 162]. To obtain causal knowledge through Markov's method, and to simplify the operation process by one-step transition probability matrix, the model can be performed efficiently under large-scale networks.

The risk communication model is proposed by Zhang et al. [102], whose core idea is that the risk of a network subject will spread to the object with non-vulnerability or even the whole network because of the high relevance of the network system, so it needs effective means to effectively evaluate the risk state of the whole network information system. The risk communication model (vulnerability diffusion model) is generally composed of two parts: network abstraction and propagation algorithm. The network abstraction describes the logical access relationship structure of the system, and the propagation algorithm describes the rules of risk diffusion. Figure 9 below is the result of abstract modeling of the risk diffusion logic access to the development server (10.10.0.11), the database server (10.10.0.15), and the test server (10.10.0.16) in the second section of the experimental network, after the attacker's attack on the web server (10.10.0.10), in which the weight of the directed edge represents the attack revenue. If we use the cumulative effect algorithm that ensures the optimal result of the final risk diffusion to determine the diffusion value between the nodes λ_{uv}, that is $\lambda_{uv} = \frac{w(u,v)}{\sum_{m\in N(v)} w(m,v)}$ where $w(u,v)$ represents the weight between nodes u and v; we can get the results shown in Table 7 below. From the result, we can see that the risk state of the network is not only related to the object with vulnerabilities, but also related to the logical access structure and the distribution state of the vulnerabilities, and the risk propagation model can be used to identify the most security threats or risk propagation paths.

6.3 Biological heuristic model

The intelligent computing method, which is inspired by the natural phenomena or processes of nature, is called the biological heuristic calculation method. The basic principle is to explore the solution of a problem combined with the known information and to effectively record and accumulate related information during the exploration process and guide the next move and correct the previous steps, and then get better overall results. The attacker's attack process and the defender's defense process are also the same. They are all based on the current knowledge state to seek the maximum benefit at the least cost. This promising approach can be regarded as the specific application of artificial intelligence in the field of cybersecurity situational awareness. At present, the research is in its infancy, the high-dimensional and non-linear data in the offensive and defensive process are abstracted, and the results of the solution through heuristic calculation are tested and improved in terms of feasibility and optimality. Models that have made some progress include neural network models and artificial immune models.

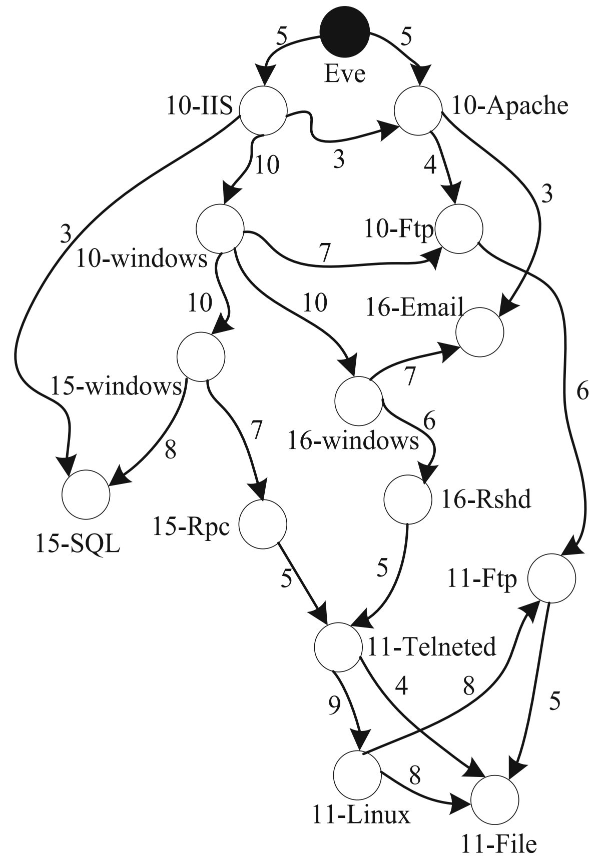


Fig. 9 Logic access modeling results of risk diffusion for experimental network

The general method based on neural network is to use the collected real-time security status indicators (such as vulnerability information, attack methods, and defense methods) as the input vector X, and regard the indicators of situation awareness results (such as confidentiality and integrity) as the output vector Y. In this regard, a non-linear mapping from X to Y is constructed by effective training [163, 164]. Literature [165] introduced the neural network learning method in IDS research, which greatly improved the accuracy of the alarm effectively. The literature [166] integrated the self-encoding network and deep belief network structure technology into the risk identification model and proposed a lightweight intrusion detection model which can reduce training time and test time to a certain extent and reduce the false alarm rate.

Computer immunology, which imitates the biological immune system [167], has been widely used in cybersecurity situational awareness analysis. The literature [168] proposed an immune model that applies the dynamic clonal selection algorithm to the network intrusion detection system. Based on the correspondence between the changes of antibody concentration in the human immune system and the invasion intensity of pathogens, Li Tao proposed an immune-based cybersecurity risk detection model [169], and an immune-based network monitoring model was established by the dynamic model of immune memory and the recursive equation of response [170]. In literature [171], the artificial immune algorithm is used as a multi-objective solution method for risk assessment, which shows the change of cybersecurity status under different attack strategies to some extent. However, as a new approach to cybersecurity situational awareness analysis, the immune model must fully mimic the mechanism of immunology to function. The complexity and agnostic of immunology will make the modeling and solving process more complicated.

Table 7 The *λuv* calculation results of each node's in Fig. 10

10-IIS	10-IIS	10-IIS	10-Apache	10-Apache	10-windows
10-Apache	10-windows	15-SQL	10-Ftp	16-Email	10-Ftp
3/8	1	3/11	4/11	3/10	7/11
10-Ftp	15-Windows	15-Windows	15-Rpc	16-Windows	16-Windows
11-Ftp	15-SQL	15-Rpc	11-Telneted	16-Email	16-Rshd
6/14	8/11	1	5/10	7/10	1
10-windows	10-windows	11-Ftp	16-Rshd	11-Linux	11-Linux
15-Windows	12-Windows	11-File	11-Telneted	11-Ftp	11-File
1	1	5/17	5/10	8/14	8/17

Whether it can effectively reflect the evolution of the security situation remains to be tested.

6.4 Combination and comparison between models

Table 8 shows the classification results of each model in 9 dimensions. It can be seen that there is no model that can meet the high standard requirements of more than 5 dimensions at the same time, which also indicates that the research on network security situational awareness is still in the exploration stage. For the formal modeling phase of model representation, there are two main improvement aspects: one is to improve or enhance the research for a certain model, such as in-depth analysis based on attack graph [101, 143, 146] and the application of fuzzy set ideas in the field of perception [107]. Most of them belong to the second category, that is, through the combination of models, the purpose of analysis can be achieved by means of the advantages of multiple models, such as Bayesian attack map [114, 128, 129], fuzzy Petri net [155], and Markov game [162].

7 Phase III: Establishment of metrics

The core purpose of metric establishment is to refine or quantify the value of each element object involved in cybersecurity situational awareness before solving the solution. According to the cybersecurity situational awareness operation mechanism in Fig. 3, the metric establishment phase may occur after the formal representation of the model, or directly on the basis of element acquisition, so this phase is mainly divided into two cases: one is model element quantification and the other is the evaluation system and index.

7.1 Model element quantification

In the process of formal modeling in Section 5, the relevant elements have been defined in detail. To conduct the solution analysis needed for cybersecurity situational awareness, it is also necessary to quantify each element in the model (from the perspective of model description ability, the process of quantifying the value of elements is also the process of describing the refinement of capabilities). Therefore, this stage has a strong correlation

Table 8 Comparison results of each model

Model	Theoretical	Granularity	Ability	Real-time	Form	Associability	Literature	Solving	Extensibility
AHP Model	Mathematical	Middle	Middle	S+D	Quantitative	Difficulty	Less	Easy	Middle
Bayesian Model	Mathematical	Coarse	Middle	S+D	Quantitative	Easy	More	Easy	Middle
D-S Model	Mathematical	Coarse	Middle	S+D	Quantitative	Middle	Less	Middle	Middle
Fuzzy set	Mathematical	Coarse	Weakness	Static	Quantitative	Middle	Less	Middle	Middle
Rough set	Mathematical	Coarse	Weakness	Static	Quantitative	Middle	Less	Middle	Middle
Reliability Model	Mathematical	Coarse	Weakness	Static	Quantitative	Middle	Less	Easy	Middle
Survivability Model	Mathematical	Coarse	Weakness	Static	Quantitative	Middle	Less	Easy	Middle
Attack Tree	Stochastic	Coarse	Middle	Dynamic	Qualitative	Easy	More	Middle	Middle
Attack Graph	Stochastic	Fine-grained	Strength	Dynamic	Qualitative	Easy	More	Middle	Middle
Privileged graph	Stochastic	Middle	Middle	Dynamic	Qualitative	Middle	Less	Middle	Difficulty
State transfer graph	Stochastic	Fine-grained	Strength	Dynamic	Qualitative	Easy	Less	Difficulty	Difficulty
Pretri Net	Stochastic	Fine-grained	Strength	Dynamic	Qualitative	Easy	More	Middle	Middle
Game theory Model	Stochastic	Fine-grained	Strength	Dynamic	QA+QL	Easy	More	Difficulty	Difficulty
Markov Model	Stochastic	Middle	Middle	Dynamic	QA+QL	Easy	More	Easy	Middle
Risk diffusion model	Stochastic	Middle	Middle	Dynamic	QA+QL	Middle	Less	Easy	Middle
Neural network	Biological	Middle	Weakness	Dynamic	Quantitative	Difficulty	Less	Difficulty	Difficulty
Artificial immunity	Biological	Middle	Weakness	Dynamic	Quantitative	Difficulty	Less	Difficulty	Difficulty

with the idea of model construction. Through the existing literature statistics and analysis, it is found that the models are focused on different points, but each model contains a description of the attack behavior. The quantification of the three elements of attack severity, attack occurrence, success probability, and attack revenue has basically formed certain standards or norms.

The metrization premise of serious attacking is the qualitative classification of attack types. The variety of cyber attacks leads to different types of attack. At present, the six-member representation method, proposed by Christy [122], has strong practicality and has been accepted by most people. Based on the qualitative classification method, it is divided into several levels to quantify the severity of the threat [102, 124]. This method is generally associated with the alarm mechanism of IDS and is widely used in intrusion detection. The widely used method in the attack model is CVSS vulnerability evaluation mechanism [10, 123], which is divided into three aspects: basic evaluation criteria, life cycle assessment, and environmental assessment. The final result is 0~1. The higher score indicates the greater threat to the vulnerability.

The purpose of quantifying the occurrence of attack/successive probability is to measure the authenticity of the attack or the possibility of successful attack. The network attack process is filled with a large amount of false and useless information. The information provided by each host and security device is often inaccurate; this brings great difficulty to the comprehensive estimation of the information fusion model. Currently, the subjective probability estimation method of experts is mainly used in each experimental model [10, 128, 162] (Tables 9 and 10 are the quantitative criteria used in the follow-up analysis of this article [124]), and the Bayesian network can effectively express the probabilistic reasoning of uncertainty knowledge, and thus in this research, Bayesian-based estimation methods [55] have also made some progress.

The quantification of the attack revenue is an important part of the attack effectiveness evaluation. Generally, the destructive size of the attack is qualitatively measured (for example, the attack acquires the root permission of a service [5, 6], etc.), and then the quantitative value of the damage degree is given according to the qualitative classification. The quantitative research can be carried out from the perspective of the attacker and the defender. From the view of the attacker, the quantitative research refers to the return obtained by the attack under a certain attack cost, while the defender refers to the loss of the system at a certain defense cost. In general, the attack revenue is less than the network system loss. For the sake of simplicity, the defense loss is used as the attack benefit in most models [124]. This method is also adopted in the subsequent analysis of this paper.

Table 9 Reference table for the probability of atomic attack

Access Complexity Value	Confidence probability value
H (High)	0.2
M (Medium)	0.6
L (Low)	0.8
U (Undefined)	0.85

Table 10 Reference table for attack success probability

Degree of difficulty in attack	Confidence probability value
Vulnerability utilization	1
Easy	0.9
Medium	0.5
Difficulty	0.1

7.2 Indicator system and index

The indicator system is used to evaluate and reflect a certain situation in a certain field and is widely used at all levels. Different from the point-based quantification of each element in the model, the cybersecurity situational assessment index system should proceed from the whole, intending to exhaustively classify the attributes related to the cybersecurity situational evaluation, giving the clear meaning of each class; the quantitative operation is carried out based on mutual related and complementary systematic indicators, and through the mathematical calculation method to obtain the cybersecurity situational index value to be evaluated, through the change of the index value to reflect the change of cybersecurity status.

The cybersecurity situational indicator system and index distract the network administrator's concerns free from the scattered or massive log data monitoring; facilitate the intuitive response to the cybersecurity state, especially the relative number of changes help to find abnormalities better; and then confirm the main influencing elements and achieve effective protection. It mainly includes two aspects of work: one is to comprehensively and systematically ascertain the elements related to cybersecurity situational awareness (the evaluation system in Fig. 3 and the quantified parts of each metric element) and the second is to establish a mapping model between systemic elements and result index (mathematical analysis method and solution analysis part are confirmed in Fig. 3).

Based on the effective synthesis of the explanation of the specific meaning of network security and the study of reliability, Lin etal. [96], divides the attributes that are generally concerned about in security into five parts: reliability, availability, insurance, confidentiality and integrity, and gives the concrete content of each index in the field of security. Meaning and the way of quantification are discussed. Survivability goes beyond the concept of security. It quantifies the ability to correctly perform predetermined functions. It is the ability to provide normal services when the system is facing threats based on the security evaluation. Feasibility quantifies the operational performance of the network system in the event of possible failures, providing a comprehensive quantitative evaluation standard between security and system performance. Figure 10 provides a brief summary of the cybersecurity assessment indicators in literature [96].

Based on the hierarchical index system [99], the literature [172] proposed a cybersecurity situational assessment method based on the configuration index system. In this method, the indicators are divided into three levels: comprehensive index, evaluation dimension, and situation element (as shown in Fig. 11 below). The cybersecurity situational comprehensive index is divided into five levels. The evaluation dimensions are mainly based on three dimensions: basic operation index (reflecting the safe operation of network equipment and services), vulnerability index (reflecting the vulnerability of the network itself in the absence of attacks) and risk index (reflecting the impact of network attacks on the network). Each dimension can choose different situation assessment factors. The proposed quantification methods for each factor are also given (e.g. the factor in the basic operation index is quantified by overload rate, etc.).

8 Phase IV: Solution analysis

After the formal description of the model in stage II and the element refinement measurement in stage III, the fine-grained abstraction of the related perceived objects in the network is basically completed. The next step is the solution analysis, the core of the cybersecurity situational awareness, whose main aim is to analyze and calculate the corresponding models and data effectively, so as to obtain the qualitative or quantitative results which can reflect the network security status and express the mapping process from elements and their quantitative features to the judgment results of network security status. In some research papers, this part is generally touched upon in the form of "model solution algorithm." In addition, some researches extend traditional methods in the field of cybersecurity situational awareness, and some introduce new theories and methods into this area. At present, more than 60% of the literature on cybersecurity situational awareness searched in China and abroad is targeted at the improvement of solution methods, trying to improve the accuracy and efficiency of the analysis results.

8.1 Classification of solution analysis method

Although there are various methods in the process of cybersecurity situational awareness, theoretically, they can be divided into three categories: formula analysis method, logical reasoning method, and information fusion analysis method, as is shown in Fig. 12 below.

Formula analysis method is also called mathematical calculation method, the earliest one applied to cybersecurity situational awareness, including statistical description analysis and decision evaluation analysis. Statistical description analysis uses the basic mathematical statistics to reflect the network security status, such as the statistics of the number of real-time network security events [33–35], network congestion [35, 92], and vulnerability top-*k* sorting [10, 123, 172], which has been widely used in network security monitoring systems at all levels. This method has high objectivity and strong maneuverability. However, it can only present the results, but cannot effectively retrospect the causes of the state. Decision-making evaluation analysis method is elicited from the multi-objective decision theory, relies on the first three stages of element abstraction and index system to construct the evaluation function, and obtains situation awareness results through the evaluation function. Dapoigny's fast calculation method of static statistical data [68], the formula of analytic hierarchy process (1) - (12) in reference [100], the formula (1) - (4) of fuzzy evaluation method [135], and the formula of average attack cost in reference [138] are all the application fields of this method in network security situational awareness. Formula analysis is generally used in conjunction with the mathematical model in stage II and is also the basis for the quantitative analysis of other solving methods in this

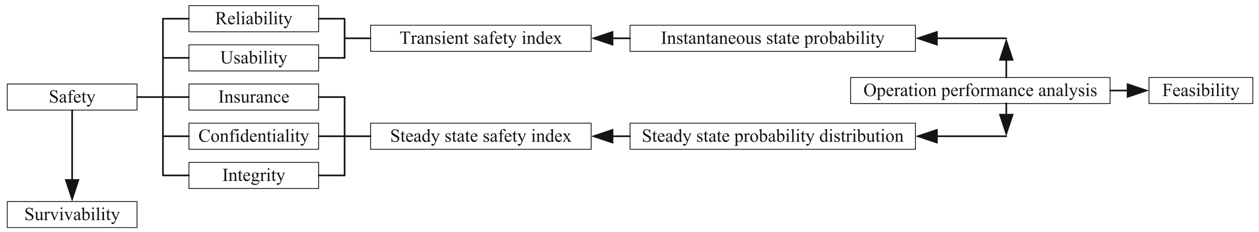

Reliability
Usability
Insurance
Confidentiality
Integrity
Safety
Survivability
Transient safety index
Steady state safety index
Instantaneous state probability
Steady state probability distribution
Operation performance analysis
Feasibility

Fig. 10 Security attributes system and index calculation method

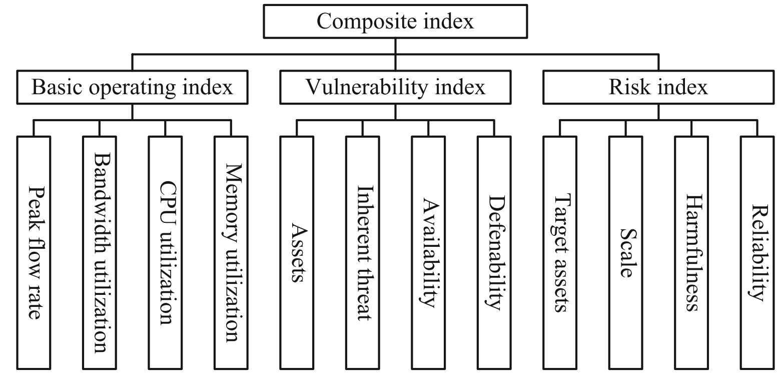


Fig. 11 The index evaluation system based on configuration

section. The advantage of this method is that it can intuitively and visually perceive the results of the reaction and the computational complexity of polynomial content can be easily generalized in large-scale networks. However, owing to no unified criterion for the function evaluation and related parameters selection, the high subjectivity easily leads to a large deviation between the mapping $Y = F(X)$ from the set of factor indicators X to the set of perceptual results Y and the actual situation.

In view of the shortcomings of formula analysis method, logical reasoning method has gradually become a breakthrough in problem-solving. It can gather uncertain information from multi-sources and with multi-attributes, simulate human thinking modes, and obtain intelligent evaluation results, including rule reasoning method, graph model reasoning method, and pattern recognition method. Rule-based reasoning method is developed from the rule-based expert system. It can be tentatively solved by imitating the association reasoning ability of experts. In the field of network security situational awareness, it is mainly combined with intrusion detection system to improve the efficiency or accuracy of intrusion detection such as the model for compound attack mode detection proposed by Bao et al. [28], the effective parameter selection method put forward by Ilgun et al. [29] based on the category principal component analysis, the multifunctional simulation platform proposed in literature [32], an ontology-based attack knowledge model established in literature [106] by clustering and classifying the underlying alerts, and the hierarchical intrusion scene reconstruction methods brought up by Fu et al. [127]. Graph model reasoning analysis is one of the most effective methods to explore the correlation of related elements in network security situational awareness. The knowledge of logic relation, reasoning method, and probability calculation is included in the state transition of directed graph. Attack graph model [5, 101, 112, 128, 129], Bayesian model [11, 62, 114, 132], Markov model [53, 109, 162], and so on all adopt this method. The solution method mainly includes two steps: reachability analysis and quantitative calculation analysis. The reachability analysis mainly explains whether the current network system or a service component has the possibility of being attacked, including the analysis results such as attack reachability and attack path. Figure 13 below is the result of the reachability analysis of the internal development server (10.10.0.11) in the experimental network using the analysis method in reference [5]. It can be seen that (a) the file on the server 11 is likely to be attacked and (b) there are nine attack paths (left 3, middle 2, right 4) in Fig. 13. These attack paths can be attacked. They fall into 3

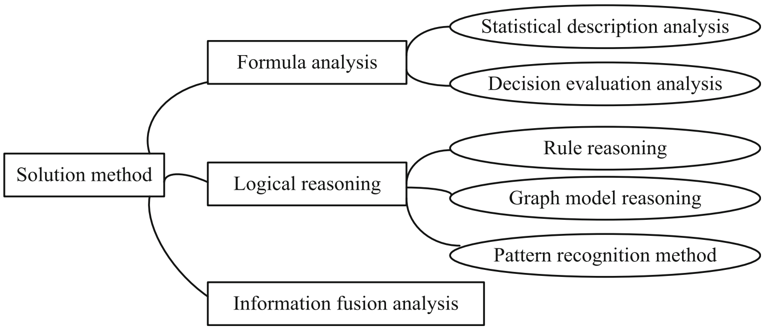

Solution method
Formula analysis
Statistical description analysis
Decision evaluation analysis
Logical reasoning
Rule reasoning
Graph model reasoning
Pattern recognition method
Information fusion analysis

Fig. 12 Classification of network security situation aware solution analysis method

categories (Fig. 13, left, middle right). On the basis of reachability analysis, the quantitative computational analysis provides comparative criteria such as maximum attack probability [6, 129, 132], maximum attack revenue [102, 146], and minimum cut set analysis [115, 116]. The number in each node in Fig. 11 below is the result of using the method of quantifying model elements in phase III to evaluate the attack benefit [124]. Using the algorithm of maximum reachability in literature [129], the maximum probability path in each attack path can be known (represented by the dotted lines in Fig. 13). The analysis process of graph model reasoning is clear, which conforms to human logical thinking and is easy to understand, but it also increases the complexity of reasoning (such as large storage cost of graph and reasonableness of uncertain representation). Therefore, the promotion of graph model reasoning in large-scale networks is the most important breakthrough of this method. With the development of machine learning, the pattern recognition method is used to solve the perceptual process in which the relationship between the factor index set X and the perceptual result set Y cannot be established by function or logic reasoning. It uses the historical monitoring data (including both the factor data and the result data) as the training sample to determine the situation template and evaluates the situation by the implicit pattern matching. The combination of intrusion detection and unknown attack detection has made some progress [7, 27, 168]. However, this method cannot provide scientific evidences for the results of perception because of the large amount of calculation, and it is still far from the actual use.

Formula analysis method and logic reasoning method have their advantages and disadvantages. There is no general solution method to solve all the problems encountered at present. Therefore, the original intention of information fusion analysis method is to combine the advantages of various solution methods and try to use the solution method in a complementary way. One is to provide more data sources and obtain more accurate perception results through data diversity and association degree on the premise of the basically unchanged solution method. For example, Bass [7, 8] integrates the heterogeneous distributed network sensor data into intrusion detection system, and Yong et al. [103] bring the vulnerability information and service information together for the theory of multi-source fusion through D-S evidence. Moreover, in literature [32], the real-time perceptual slicing and its fusion methods are introduced. The other is to take the mutual complement of solution algorithms on the premise that the input elements and measurement values are basically unchanged. For example, Poolsappasit et al. [11] combine the Bayesian network with the qualitative causal analysis of attack tree/graph to form a multi-objective optimization platform. Furthermore, the concept of fuzzy centralized credibility is introduced into the Petri net model in literature [155] and is evaluated by the hierarchical method. Zhang et al. [162] combines Markov's inefficiency analysis with the attack-defense game and proposes a security situation evaluation algorithm with three sub-algorithms.

Table 11 compares the results of the three categories of the six methods of solution analysis in this section. The comparison is made from seven dimensions: time complexity, space complexity, generality, scalability, number of articles, the visual property of the analysis results, and the degree of difficulty in understanding of the analysis results.

8.2 Verification and optimization

After stage IV, the first four stages are usually validated in the way of experiments. The verification work is mainly divided into two parts: one is to verify the validity of the model abstraction and the other is to verify the rationality of the analysis results. The validity verification of model abstraction is to judge whether the formal expression of network elements and their associations tally with the actual situation of the experiment and to verify whether the initial results of the solution analysis are in line with the current network security status. The

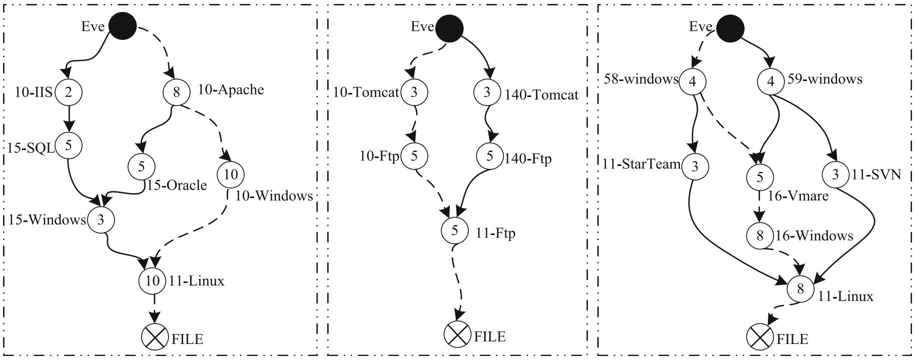


Fig. 13 Inference analysis results of experimental network diagram model

Table 11 Comparison between analytical methods

classification	method	Time complexity	Space complexity	Generality	Extensibility	Number of articles	Result intuition	Understanding difficulty
Formula analysis	Statistical description analysis	Low	Low	High	High	Less	High	Difficulty
	Decision evaluation analysis	Middel	Middel	Middel	Middel	Middel	Low	Middle
Logical reasoning	Rule reasoning	Middel	Middel	Middel	Middel	Middel	Middel	Middle
	Graph model reasoning	High	High	Middel	Low	More	High	Easy
	Pattern recognition method	High	High	Low	Low	Middel	Low	Middle
Information fusion analysis	Fusion analysis	Middle	Middle	Middel	Middel	More	Middel	Middle

rationality of the analysis results includes not only the correctness verification of the solution method in Section 7.1, but also the verification concerning the conformity of the initial results of the analysis to the real security state of the current network.

Validation is the comparison between the experimental results and the expected objectives in the model, and optimization is the comparison of the descriptive ability, solution efficiency, and analysis results between models. Some researchers have improved the formal abstraction in order to describe the key elements of network security situational awareness more concisely. For example, Ammann et al. [59] proposed a more concise and extensible model based on the core concept of attack graph. Hamid et al. [125] combined the take-grant protection model with attack graph and refined the node granularity to component level. Besides, Luo et al. [110] constructed the hierarchical attack graph based on the underlying data to improve the accuracy of intrusion intention detection, and characterized the random strategy selection of attack and defense parties by game theory, which is targeted at making the analysis results more accurate or reduce the complexity of the algorithm to adapt to large-scale networks. Poolsappasit et al. [11], based on the risk management framework of Bayesian network, can ensure to obtain more decision information under resource constraints. Wu et al. [101] proposed an attack-based framework. In literature [112], the problem of the optimal compensation set is transformed into a single-weighted collision set to solve the problem. It is proved that the method based on such transformation has better performance. The attack graph simplification algorithm and the maximum reachable probability algorithm in literature [129] can be better adapted to the large-scale complex network. In addition, Yun et al. [143] raised an automatic attack algorithm for large-scale networks. There are also researches that aim to improve both the formal abstraction and the algorithm to obtain better analysis results. This aspect is more a combination of the formal method in Section 5 and the solution method in Section 7.1. For example, in literature [11, 114], the combination of Bayesian operation and attack graph is used for dynamic security risk assessment. Moreover, Dietterich et al. [64] applied the theory of machine learning in the process of network security situational awareness, the combination of Petri nets and fuzzy sets [155], and the combination of game theory and Markov [74, 162], as well as the comprehensive application of information fusion methods in network security situation [7, 67, 74, 103].

9 Phase V: Situation prediction

According to the stage division of the operation mechanism of network security situation awareness in Section 3 of this paper, the last stage is situation prediction, whose core role is through knowledge application to enhance network security and form feedback loop process on the basis of the analysis results obtained in the first four stages. However, most of the literature on this stage is missing, and in a simple experimental network or some special scenarios, the results of solution analysis can directly reflect the current situation and correspond to the defense decision-making measures. In the real network environment, there is a certain distance from the solution results to the situation judgment and then to the application of the decision-making measures, requiring the effective methodological support. The failure to validate the decision-making knowledge and form feedback loop is one of the main reasons why most of the cybersecurity situation awareness methods cannot be popularized.

9.1 Result visualization

As is shown in Fig. 3, the first four stages of the network security situation awareness mechanism fully utilize rational thinking and the computing advantages of machines, but cannot make full use of human perception ability to turn abstract model or language representation graphical more easily to express the intrinsic meaning and enhance cognitive effect. To present the hidden information and rules in data through visual graphics is the main function of information visualization, also the research emphasis [174]. Visualization analysis is a new direction of multidisciplinary research, which undoubtedly shares great similarities with the status quo of multidisciplinary integration of cybersecurity situation awareness research. At present, the combination is mainly carried out at two points after the model representation in stage II and the solution analysis in stage IV.

After stage II, the visualization of the elements and their relations is mainly carried out. Simple graphics, such as Figs. 8a and 10 in this paper, reveal the visual graphic expression of the abstraction of the experimental network model. The visualization of the physical and logical connections of the network is the basis of all the analysis methods. Phan et al. [175] propose time visualization system of the self-building structure, and the graphical descriptions of various attack graphs [128, 129, 140–142] belong to this category; the visualization of the analysis results is carried out after stage 4 solution analysis, and the focus can be more easily understood by graphical analysis. Tamassia et al. [76] conduct a basic investigation on the visualization of security perception. Figure 13 is a concise example of visualization of analysis results, especially in large-scale network analysis, and visualization can greatly improve the efficiency of analysis. Figure 14 shows the results of the attack graph analysis results visualization reduction effect.

Graphical representation is an important part of information visualization, but it is also the primary stage of visualization. Visualization is not only the process of passive information mining, but also the process of human subjective consciousness participation. The framework proposed by Erbacher [78] allows network managers to participate artificially in the analysis loop, to make immediate assessments with the help of the unique expertise of the participants and to combine artificial intelligence with visualization [77, 79], but most of these articles remain within the technical perspective [44]. There is still a long way to go for the flexible analysis of network security situational awareness in general scenarios.

9.2 Knowledge application

The effective analysis of the above stages brings the perception results of network security status. If there are potential threats or attacks in the results, network security administrators are required to take corresponding defensive measures to strengthen the security of the target network, which is called the application feedback loop process of perception knowledge in the cybersecurity situation awareness mechanism, as shown in Fig. 3. Obviously, it is unrealistic to completely eliminate the loopholes or threats in the perception results. The feedback process of knowledge application based on perceptual analysis results is transformed into an optimal reinforcement decision-making problem. At present, relative research mainly involves three categories: the minimum cost reinforcement of key objectives, the maximum benefit reinforcement of the whole network, and the multi-objective security reinforcement.

The concept of minimum cost reinforcement based on key objectives is to take the key assets in the network as the starting point of reinforcement and to seek a method to ensure security at the minimum cost. Most of the literature will give the defense measures to ensure that the key objectives do not suffer losses [11, 101, 140–142] after the case study. Based on the analysis results of the experimental network in this paper (Figs. 9 and 13), assuming that the data on the 10.10.0.11 internal development server is the key objective, the reinforcement objective g can be expressed as $g = (\text{10-Apache}\wedge\text{10-Windows}\wedge\text{10-Linux})\vee(\text{10-Tomact}\wedge\text{10-Ftp}\wedge\text{11-Ftp})\vee(\text{58-Windows}\wedge\text{16-Vmare}\wedge\text{16-Windows}\wedge\text{11-Linux})$. Thirty-six kinds of reinforcement solutions can be obtained as $\{D_i,D_j,D_k\}$, and the minimum reinforcement cost is $\min\limits_{i,j,k}[\mathrm{Cost}(D_i)+\mathrm{Cost}(D_j)+\mathrm{Cost}(D_k)]$, among which $D_i\in\{\text{10-Apache, 10-Windows,10-Linux}\}$, $D_j\in\{\text{10-Tomact,10-Ftp,11-Ftp}\}$, and $D_k\in\{\text{58-Windows,16-Vmare,16-Windows,11-Linux}\}$. On this basis, in literature [177], the important assets in the network are represented by the combination of the initial condition logic expressions of the network, and the reinforcement scheme is obtained from the attack source. Wang et al. [178] quantify the probability relationship of the state transition caused by vulnerability through Markov model, analyze the possible attack means and the corresponding defense cost, and put forward the scheme of minimum cost of reinforcement. Starting from the view of network administrator's concern, this method can guarantee the core assets against loss at a relatively minimum cost. However, it neglects the correlation between defense measures and other normal access and easily leads to the failure to normally respond for some other assets or services not listed as key objectives.

The focus of the maximum benefit reinforcement of the whole network is how to ensure its maximum security with the current perceptual analysis results. Noel et

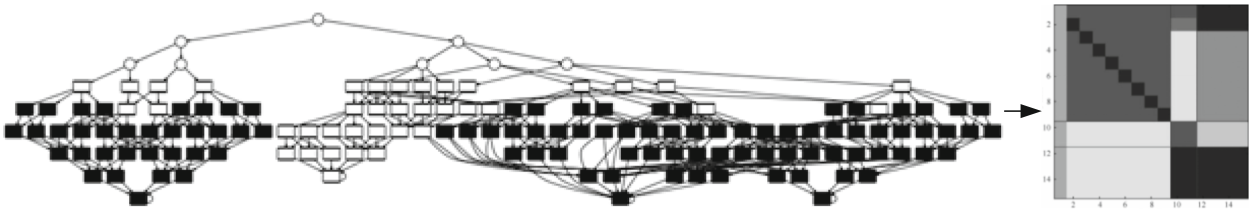


Fig. 14 Attack graphical analysis [140] and visualize simplified [176]

al. [179] set out from the initial conditions of the network, calculating the true value of the logical expression to find the security measures to maximize the security of key assets. Jajodia and Noel [180, 181] start from the perspective of network administrators as defenders, focusing on maximizing the security protection of enterprise networks, to seek the most effective defense measures to ensure the maximum return. This method can maximize the network security efficiency to a certain extent, but taking security as the starting point will lead to excessive time complexity or loss of normal service function for security in practical applications.

Multi-objective security reinforcement attempts to combine the advantages of minimum cost reinforcement of key objectives and maximum benefit reinforcement of the whole network to achieve maximum security of the whole network under the premise of the normal operation of key objectives and basic functions. Frigault et al. [130] and Bayesian attack graph are combined with and calculate the probabilistic relationship between the attack behavior and the defense alarm index in the course of attack. Several sets of reinforcement measures are established under the guidance of the safety index and compared with each other by quantitative analysis. Dewri et al. [182] take the idea of game and adopt the theory of multi-objective analysis and co-evolution of competition to construct an optimal security reinforcement model, ensuring the maximum security return under the premise of certain security costs and normal functions in the co-evolution of attack decision and defense decision. This method can consider the application effect of decision-making from different angles. But the subjectivity of the expense or reward in the objective matrix of this method is so large that it will lead to the lack of objectivity of knowledge application feedback, and also have great limitations in storage and calculation during the large-scale network promotion.

10 Network securities under large data

With the development of the information society, the age of big data has come quietly, the speed of data production is getting faster and faster, and the value implied in the data will bring about a revolutionary development to the society. As the carrier of digital resources, the computer network has penetrated into all aspects of social life, and the network structure is becoming more and more complex. With the rapid growth of interaction, new technologies are needed to ensure network security. Information security is becoming a big data analysis problem, and large security data need to be effectively associated, analyzed, and excavated [183]. The discussion of data classification and storage in the fourth section in this article also indicates that the data of cybersecurity situational awareness conforms to the 4V characteristics of big data [184]. The combination of big data analysis and cybersecurity situational awareness naturally produces new network security solutions: network securities analysis under large data. Big data is a mixture of new resources, new technologies, and new concepts [185]; the research of network security analysis under large data also naturally revolves around these three dimensions.

From the dimension of new resources, large data is more resources, which can be collected, preprocessed, and stored on the basis of more large-scale data throughput. The combination of mass data and traditional models or analysis methods will achieve better perception accuracy. For example, the collection of relevant data in the security competition in literature [80, 81], 35 billion network intrusion detection system alarm data sets collected worldwide from the HP laboratory, used to identify malicious attacks. The BotCloud project analyzed 720 million Netflow data involving 16 million hosts to establish the correlation between hosts. Cerullo et al. [186] embody the advantages of mass data association analysis in network security and form a multi-type security event intelligent association analysis model in a wide time period. Behavioral association analysis based on large data volume can greatly improve the detection rate of network anomaly [103, 187].

From the dimension of the new technology, large data is a new generation of data management and analysis technology. It can apply large data technology in the field of cybersecurity situation awareness and mine more data value. Based on the flow data processing method in large data analysis, OpenSOC [188] constructs a large data security analysis framework for network packets and streams to realize real-time detection of network anomalies. Using large data batch processing architecture Apache Spark, Fischer and Keim [189] designed the network security situation visualization tool NStreamAware, which can monitor and visualize the network data flow. Marchal et al. [190] also proposed a security monitoring framework for mass data analysis based on Spark. Based on Hadoop and Map Reduce technology, WINE project [191] can efficiently handle large-scale security datasets, including 5,500,000 malware samples, 30 TB data set based on reputation, 100,000 spam samples, and 75 million security threats and telemetry data sets of sensors from the whole world. Giura and Wang [192] proposed a conceptual attack pyramid model, which grouped all possible security-related events in the organization into multiple scenarios; used the MapReduce method to do parallel progress in each scene or between scenes; and used different algorithms to detect possible attacks.

From the perspective of new concept, big data is a new way of thinking. The way that from the traditional analysis centered on computing to data centric brings new connotation of data-driven decision. In the traditional analysis and decision-making method, we first analyze the possible causality, and then establish the model which is restricted by the factors, and get the results through the algorithm analysis to predict and take measures. The core concern is the rationality of the model abstraction and the effectiveness of the algorithm. In the mechanism shown in Fig. 3, model abstraction and solution analysis play a key role. However, in the model of large data analysis, the first is to collect relevant data, carry out time series analysis, determine the implicit intrinsic relationship, then carry on the evolution prediction, and determine the key parameters to control effectively. The core concern is data association and the way of evolution. A typical application of big data analysis concepts in cybersecurity situational awareness is deep learning. Literature [193] applies deep learning to network traffic protocol classification and unknown protocol detection, which greatly improves the accuracy of protocol recognition, especially when the protocol is not encrypted, annd the recognition rate can reach 54.94%. The results of Deep Instinct [194] also show that the security solution using deep learning technology can resist unknown attacks.

Through the summary of this paper, we can see that there are still some difficulties in information collection, model representation, measurement establishment, and solution analysis and situation prediction. The combination of technology and concept of big data and network security situational awareness can greatly expand the research space in the field of network security, and to a certain extent, it has improved the technical level of APT attack detection, network anomaly detection, network intelligence analysis, advanced threat discovery, threat information acquisition and sharing, and so on [190, 192]. The Ali Co's cloud shield platform, the 360 company's NGSOC platform [195], and a series of academic research [183–195] all show that the massive storage, parallel processing, and fusion analysis of large data can provide effective support for the research difficulties of cybersecurity situation awareness. The introduction of large data technology provides an opportunity for the ladder breakthroughs in this field.

11 Conclusion

This paper introduces the basic concept and core methods of network security situation awareness and highlights the system engineering perception framework from the perspective of data value chain which consists of five stages: element acquisition, model representation, measurement establishment, solution analysis, and situation prediction. It gives a detailed introduction of the basic function, main methods, and application effects of different stages. In the element acquisition stage, the perceptual data are classified and summarized, and the standardized design and implementation of the database are briefly described. In the model presentation stage, the core concepts, representative technologies, and modeling results of each model are discussed. In the measurement establishment stage, the model elements are quantified and the index volume is evaluated according to the model elements. In the solution analysis stage, the application premise and analysis of typical algorithms are discussed, and the horizontal comparison between algorithms is made. In the situation prediction stage, the importance of knowledge application feedback loop is emphasized, and the basic methods of visualization of analysis results and selection of defense measures are discussed.

Acknowledgements
Not applicable

About the Authors

Yan Li was born in Chengde City, Hebei Province in 1984. He received the B.S., M.S., and the Ph.D. degree from Xi'an University of Architecture & Technology, Xi'an, China, all in information management and information system. He is currently working in the School of Management of Xi'an Polytechnic University. His main research directions include system engineering, big data application analysis, and network security. He worked in software companies from 2009 to 2017. He has been engaged in software development for 4 years in active network, and later served as general manager in medium-sized software enterprises. He has rich theoretical and practical experience. At present, he focuses on theoretical research and system development in the field of block chain security and certification. (corresponding author; email: sayidli@xpu.edu.cn)
Guang-qiu Huang received the B.S. and the M.S. degree from Xi'an University of Architecture & Technology, Xi'an, China, and the Ph.D. degree from Northeast University, Shenyang, China, all in mining engineering. He has worked in education for 25 years at Xi'an University of Architecture & Technology, where he is now a professor and doctoral supervisor in the School of Management. His teaching and research involves systems engineering, information management and information systems, computer intelligence, and optimization design of mining engineering. He is the consultant expert of the Government of Xi'an City and the assessment expert of National Natural Science Foundation. He has completed 78 research projects including national key scientific research projects, projects of National Natural Science Foundation, and provincial and ministerial level research projects. He won the Henry Fok Prize, the Baosteel Education Award, the First Prize of the Government of Shaanxi Province, and has published over 300 refereed conference and journal papers, 8 books, 43 software copyrights, and 9 patents. (email:huangnan93@163.com)
Chun-zi Wang received the B.S., M.S., and Ph.D. degree from Xi'an University of Architecture & Technology, Xi'an, China, all in Management Science and Engineering. She has worked in education for 8 years at Xi'an Polytechnic University, where she is now an associate professor and master supervisor in the School of Management. She has taught 4 courses, such as Java language programming, network information security, object-oriented technology, and statistics. Her teaching and research involves network security, risk management, and optimal decision. She has published over 20 refereed conference and journal papers and presided over 10 research projects, including Natural Science basic Research Project of Provincial Science and Technology Department and Provincial Education Department project. (email: wangchunzi@xpu.edu.cn)
Ying-chao Li received a bachelor's degree from Xi'an Technological University in 2009, specializing in software engineering. He has 10 years of experience in the industry, mainly engaged in software project system architecture design and research and development management. He is good at distributed and big data technology. He had in-depth study of design patterns and database optimization. His main work experience is as

follows: in 2017, he is the project leader of Shaanxi Province’s key industrial project “Research on Complex Heterogeneous Data Fusion and Management Model of Provincial Food and Drug Regulation,” “Shaanxi food safety supervision comprehensive business system" project leader,” and “Emaplink Smart Distributed Service Platform” project leader. The technical leader of “Cisco Smart Business Configurator for Collaboration (SBCC)” project. “Shaanxi Telecom Electronic operation and maintenance system” takes charge of database design, performance optimization, and so on. At present, he holds the position of technical director of Legend Software Co., Ltd. and is responsible for the construction of information projects in the field of food and drug supervision. Many software project copyright and invention patents were created during the period. (email: 147393765@qq.com)

Authors’ contributions

LY conceived of the whole article and has completed two to seven sections of the article. HG completed the first section and participated in the overall discussion and proofreading. WC completed the content of the eighth section and conclusion and participated in the overall discussion and proofreading. LY-C participated in the discussion and proofreading work. All authors read and approved the final manuscript.

Funding

This study was funded by The Fund Project for Science and Technology Research and Development Plan of Shaanxi Province (grant number: 2013 K1117) and Xi’an Polytechnic University doctoral research start-up fund(grant number: 20170914)

Availability of data and materials

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Competing interests

The authors declare that they have no competing financial interests.

Author details

[1]Xi’an Polytechnic University, Xi’an 710048, Shaanxi, China. [2]Xi’an University of Architecture & Technology, Xi’an 710075, Shaanxi, China.

Received: 10 April 2019 Accepted: 3 July 2019

References

1. China Information Yearbook 2014[M], *Editorial board of China Information Yearbook* (Publication of the electronics industry, 2015)
2. Miller B P. Fuzz-revisited: a re-examination of the reliability of UNIX utilities and services. ftp://grilled.cs.wisc.edu/technical_papers/fuzz-revisited.ps.Z, 2001.
3. S.E. Smaha, *Haystack: an intrusion detection system[A]. Aerospace Computer Security Applications Conference[C]* (IEEE, 2002), pp. 37–44
4. J.P. Anderson, *Computer security threat monitoring and surveillance[A]* (James P Anderson Co Fort [C], Washington, 1980), pp. 26–32
5. C. Phillips, L.P. Swiler, *A graph-based system for network-vulnerability analysis[A]* (The Workshop on New Security Paradigms[C]. IEEE, 1998), pp. 71–79
6. R.W. Ritchey, P. Ammann, *Using model checking to analyze network vulnerabilities[A]* (Proceedings of IEEE Symposium on Security and Privacy[C]. IEEE, 2000), pp. 156–165
7. T. Bass, *Multisensor data fusion for next generation distributed intrusion detection systems[A]* (Proceedings of the Iris National Symposium on Sensor & Data Fusion[C]. Hopkins University Applied Physics Laboratory, 1999), pp. 24–27
8. T. Bass, Intrusion systems and multisensor data fusion: creating cyberspace situation awareness. Commun. ACM **43**(4), 99–105 (2000). https://doi.org/10.1145/332051.332079]
9. J. Mcdermott, *Attack-potential-based survivability modeling for high-consequence systems[A]* (IEEE International Workshop on Information Assurance[C]. IEEE Comp. Soc, 2005), pp. 119–130
10. W. Yuanzhuo, L. Chuang, C. Xueqi, et al., Analysis for network attack-defense based on stochastic game model[J]. Chin. J. Comput. Phys. **33**(33), 1748–1762 (2010)
11. N. Poolsappasit, R. Dewri, I. Ray, Dynamic security risk management using Bayesian attack graphs[J]. Dependable Secure Comput. **9**(1), 61–74 (2012)
12. J. Theureau, Nuclear reactor control room simulators: human factors research and development[J]. Cogn. Tech. Work **2**(2), 97–105 (2000)
13. M.R. Endsley, Design and evaluation for situation awareness enhancement[J]. Proceed. Hum. Factors Ergon. Soc. Ann. Meet. **32**(1), 97–101 (1988)
14. M.R. Endsley, Toward a theory of situation awareness in dynamic systems[J]. Hum. Factors **37**(1), 32–64 (1995)
15. Boyd J R. A Discourse on Winning and Losing[C]// Strategic game of 1987.
16. G.P. Tadda, J.S. Salerno, *Overview of cyber situation awareness. Cyber Situational Awareness[M]* (Springer US, 2010), pp. 15–35
17. X.W. Liu, H.Q. Wang, H.W. Lü, J.G. Yu, S.W. Zhang, Fusion-based cognitive awareness-control model for network security situation[J]. J. Soft. **27**(8), 2099–2114 (2016)
18. U. Franke, J. Brynielsson, Cyber situational awareness a systematic review of the literature. Comput. Secur. **46**, 18–31 (2014). https://doi.org/10.1016/j.cose.2014.06.008
19. J. Gong, X.D. Zang, Q. Su, X.Y. Hu, J. Xu, Survey of network security situation awareness[J]. J. Softw **28**(4), 1010–1026 (2017)
20. D.E. Denning, An intrusion-detection model. IEEE Trans. Softw. Eng **13**(2), 222–232 (1987)
21. H. Debar, M. Dacicr, Andreas wespi towards taxonomy of intrusion-detection systems. Comput. Netw **31**(8), 805–822 (1999)
22. http://www.cs.ucsb.edu/~kemm/NetSTAT/documents.html.
23. G. Vigna, R.A. Kemmerer, NetSTAT: a network-based intrusion detection system. Journal of Computer Security **7**(1), 37–71 (1999)
24. http://www.cs.purdue.edu/coast/projects/aafid.html.
25. B. Mukherjee, L.T. Heberlein, Network Intrusion Detection[M]. IEEE Netw., 26–41 (1994)
26. J. Shi, S.Q. Guo, Y. Lu, L. Xie, An intrusion response method based on attack graph. J. Softw. **19**(10), 2746–2753 (2008)
27. Z.H. Tian, X.Z. Yu, H.L. Zhang, B.X. Fang, A real time network intrusion forensics method based on evidence reasoning network. Chin. J. Comput. Phys. **5**(37), 1184–1193 (2014)
28. X.H. Bao, Y.X. Dai, P.H. Feng, P.F. Zhu, J. Wei, A detection and forecast algorithm for multi-step attack based on intrusion intention. J. Softw. **16**(12), 2132–2138 (2005)
29. K. Ilgun, R.A. Kemmerer, P.A. Porras, State transition analysis: a rule-based intrusion detection approach. IEEE Trans. Softw. Eng. **21**(3), 181–199 (1995)
30. T. Bass, R. Robichaux, in *Proc. of the Communications for Network-Centric Operations: Creating the Information Force (MILCOM)*. Defense-in-depth revisited: qualitative risk analysis methodology for complex network-centric operations (IEEE, 2001), pp. 64–70
31. Batsell S G, Rao N S, Shankar M . Distributed intrusion detection and attack containment for organizational cyber security. http://www.ioc.ornl.gov/projects/documents/containment.pdf, 2005
32. J. Shifflet, A technique independent fusion model for network intrusion detection. Proceedings of the Midstates Conference on Undergraduate Research in Computer Science and Mathematics **3**(1), 13–19 (2005)
33. R. Bearavolu, K. Lakkaraju, W. Yurcik, *NVisionIP: an animated state analysis tool for visualizing NetFlows* (FLOCON Network Flow Analysis Work shop (Network Flow Analysis for Security Situational Awareness), 2005)
34. X. Yin, W. Yurcik, A. Slagell, *The design of VisFlowConnect-IP: a link analysis system for IP security situational awareness[A]* (IEEE International Workshop on Information Assurance[C]. IEEE, 2005), pp. 141–153
35. Z. Li, J. Taylor, E. Partridge, et al., *UCLog: A unified, correlated logging architecture for intrusion detection[J]* (Telecommunication Systems – TELSYS, 2004), pp. 12–27
36. Endsley, M. R. and Garland D.J(Eds.)(2000) Situation awareness analysis and measurement. Mahwah: Lawrence Erlbaum Associates.
37. J. Kopylec, A. D'Amico, J. Goodall, in *Critical Infrastructure Protection[M]*. Visualizing cascading failures in critical cyber infrastructures (Springer US, 2007), pp. 351–364
38. Goodall J R. Introduction to visualization for computer security[A]. The Workshop on Vizsec[C]. DBLP, 2008.1-17.
39. Jajodia S, Liu P, Swarup V, et al. Cyber situational awareness[M]. Springer US, 2010.132(2):1-4.
40. N.A. Giacobe, Application of the JDL data fusion process model for cyber security[J]. Proc Spie **7710**(5), 1–10 (2010)
41. Klein G, Tolle J, Martini P. From detection to reaction - a holistic approach to cyber defense[A]. Defense Science Research Conference and Expo[C]. IEEE, 2011.1-4.

42. S. Schreiber-Ehle, W. Koch, *The JDL model of data fusion applied to cyber defense - a review paper[A]* (Sensor Data Fusion: Trends, Solutions, Applications[C]. IEEE, 2012), pp. 116–119
43. M. Cheminod, L. Durante, A. Valenzano, Review of security issues in industrial networks[J]. IEEE Trans. Ind. Inf. **9**(1), 277–293 (2013)
44. U. Franke, J. Brynielsson, Cyber situational awareness – a systematic review of the literature[J]. Comput. Sec. **46**, 18–31 (2014)
45. V. Lenders, A. Tanner, A. Blarer, Gaining an edge in cyberspace with advanced situational awareness[J]. IEEE Secur. Priv. **13**(2), 65–74 (2015)
46. S. Rathore, P.K. Sharma, V. Loia, Y.-S. Jeong, J.H. Park, Social network security: issues, challenges, threats, and solutions. Inf. Sci **421**, 43–69 (2017)
47. P.A. Ralston, J.H. Graham, J.L. Hieb, Cyber security risk assessment for SCADA and DCS networks[J]. ISA Trans. **46**(4), 583–594 (2007)
48. P. Barford, M. Dacier, T.G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, et al., in *Cyber Situational Awareness*. Cyber SA: situational awareness for cyber defense (Springer, 2010), pp. 3–13
49. A.G. Fragkiadakis, E.Z. Tragos, I.G. Askoxylakis, A survey on security threats and detection techniques in cognitive radio networks. IEEE Comm. Surveys Tutorials **15**, 1 (2013)
50. D. King, G. Orlando, J. Kohler, in *Proceedings – IEEE Military Communications Conference MILCOM*. A case for trusted sensors: encryptors with deep packet inspection capabilities (2012)
51. X. Liang, Y. Xiao, Game theory for network security[J]. IEEE Commun. Surv. Tutorials **15**(1), 472–486 (2013)
52. M.H. Manshaei, Q.Y. Zhu, T. Alpcan, et al., Game theory meets network security and privacy. ACM Comput. Surv. **45**(3), 25 (2013)
53. H. He, Y. Shuping, P. Wu, in *Proceedings e2009 International Conference on Information Engineering and Computer Science*. Security decision making based on domain partitional Markov decision process (ICIECS, 2009), p. 2009
54. S. Stevens-Adams, A. Carbajal, A. Silva, et al., in *Foundations of Augmented Cognition[M]*. Enhanced training for cyber situational awareness (Springer, Berlin Heidelberg, 2013), pp. 90–99
55. S. Roschke, F. Cheng, C. Meinel, High-quality attack graph-based IDS correlation[J]. Log. J. IGPL **21**(4), 571–591 (2013)
56. J. Preden, L. Motus, M. Meriste, A. Riid, in *2011 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA 2011*. Situation awareness for networked systems (2011), pp. 123–130
57. Y. Cheng, Y. Sagduyu, J. Deng, J. Li, P. Liu, in *Proceedings of SPIE - The International Society for Optical Engineering*. Integrated situational awareness for cyber attack detection, analysis, and mitigation (2012), p. 8385
58. M.L. Hinman, *Some computational approaches for situation assessment and impact assessment[A]* (International Conference on Information Fusion[C]. IEEE, 2002), pp. 687–693
59. B. D' Amhrosio, *Security situation assessment and response evaluation (SSARE)//DISCEX'O1. Proceedings: DARPA Information Survivability Conference & Exposition II* (IPPP Computer Society, Los Alamitos, 2001), pp. 387–394
60. H. Hu, X. Wang, X. Yang, in *1st International Conference on Multimedia Information Networking and Security, MINES 2009*. A decision-support model for information systems based on situational awareness, vol 2 (2009), pp. 405–408
61. P. Ammann, D. Wijesekera, S. Kaushik, in *ACM Conference on Computer and Communications Security 2002[C]*. Scalable, graph-based network vulnerability analysis[A] (DBLP, Washington DC, 2002), pp. 217–224
62. T. Ke, M.-T. Zhou, W.-Y. Wang, in *Proceedings of 2009 4th International Conference on Computer Science and Education, ICCSE 2009*. Insider cyber threat situational awareness framwork using dynamic bayesian networks (2009), pp. 1146–1150
63. J.-Y. Cai, V. Yegneswaran, C. Alfeld, P. Barford, Honeynet games: a game theoretic approach to defending network monitors. J Comb Optim **22**(3), 305–324 (2011)
64. T.G. Dietterich, X. Bao, V. Keiser, et al., in *Cyber Situational Awareness[M]*. Machine learning methods for high level cyber situation awareness (Springer US, 2010), pp. 227–247
65. P. Barford, Y. Chen, A. Goyal, Z. Li, V. Paxson, V. Yegneswaran, in *Cyber Situational Awareness*. Employing honeynets for network situational awareness (Springer, 2010), pp. 71–102
66. A. Stotz, M. Sudit, in *FUSION 2007-2007 10th International Conference on Information Fusion*. Information fusion engine for real-time decision-making (inferd): a perceptual system for cyber attack tracking (2007)
67. R. Dapoigny, P. Barlatier, et al., Formal foundations for situation awareness based on dependent type theory[J]. Information Fusion **14**(1), 87–107 (2013)
68. W. Streilein, J. Truelove, C. Meiners, G. Eakman, in *Proceedings e IEEE Military Communications Conference MILCOM*. Cyber situational awareness through operational streaming analysis (2011), p. 1152e7
69. J. Li, X. Ou, R. Rajagopalan, in *Cyber Situational Awareness*. Uncertainty and risk management in cyber situational awareness (Springer, 2010), pp. 51–68
70. R. Paffenroth, P.D. Toit, R. Nong, et al., Space-time signal processing for distributed pattern detection in sensor networks[J]. IEEE J. Sel. Top. Sign. Proces. **7**(1), 38–49 (2013)
71. M.L. Mathews, P. Halvorsen, A. Joshi, et al., in *International Conference on Collaborative Computing: Networking, Applications and Worksharing[C]*. A collaborative approach to situational awareness for cybersecurity[A] (IEEE, 2012), pp. 216–222
72. L. Wang, Sushil Jajodia. k-zero day safety: a network security metric for measuring the risk of unknown vulnerabilities. IEEE Transac. Depend Secure Comput **11**, 1 (2014)
73. F. Sanfilippo, A multi-sensor fusion framework for improving situational awareness in demanding maritime training[J]. Reliab. Eng. Syst. Saf. **161**, 12–24 (2017)
74. D. Shen, G. Chen, J. Cruz Jr., L. Haynes, M. Kruger, E. Blasch, in *Proceedings of SPIE e The International Society for Optical Engineering*. A markov game theoretic data fusion approach for cyber situational awareness, vol 6571 (2007)
75. Renaud Deraison. Nessus Scanner. http://www.nessus.org. [EB/OL].2004.
76. R. amassia, B. Palazzi, C. Papamanthou, in *Graph Drawing[C]*. Graph drawing for security visualization[A] (Springer, 2009), pp. 2–13
77. J. Beaver, C. Steed, R. Patton, X. Cui, M. Schultz, in *Proceedings of SPIE e The International Society for Optical Engineering*. Visualization techniques for computer network defense, vol 8019 (2011)
78. R. Erbacher, in *ACM International Conference Proceeding Series*. Visualization design for immediate high-level situational assessment (2012), pp. 17–24
79. K.J. Ross, K.M. Hopkinson, M. Pachter, Using a distributed agent-based communication enabled special protection system to enhance smart grid security[J]. IEEE Transactions on Smart Grid **4**(2), 1216–1224 (2013)
80. A. Doupé, M. Egele, B. Caillat, et al., in *Twenty-Seventh Computer Security Applications Conference[C]*. Hit 'em where it hurts: a live security exercise on cyber situational awareness[A] (DBLP, Orlando, 2011), pp. 51–61
81. G. Fink, D. Best, D. Manz, et al., in *Foundations of Augmented Cognition [M]*. Gamification for measuring cyber security situational awareness (Springer, Berlin Heidelberg, 2013), pp. 656–665
82. S. Lee, D.H. Lee, K.J. Kim, in *Frontiers of High Performance Computing and NetworkingeISPA 2006 Workshops*. A conceptual design of knowledge-based real-time cyber-threat early warning system (Springer, 2006), pp. 1006–1017
83. G. Klein, H. Günther, S. Träber, Modularizing cyber defense situational awareness – technical integration before human understanding[J]. Commu. Comp. Inform. Sci **318**, 307–310 (2012)
84. A. D'Amico, K. Whitley, *The real work of computer network defense analysts[A]* (The Workshop on Vizsec[C]. DBLP, 2008), pp. 19–37
85. R.F. Erbacher, D.A. Frincke, P.C. Wong, et al., A multi-phase network situational awareness cognitive task analysis[J]. Inform. Visual. **9**(3), 204–219 (2010)
86. K. Giles, W. Hagestad, *Divided by a common language: cyber definitions in Chinese, Russian and English[A]* (International Conference on Cyber Conflict[C]. IEEE, 2013), pp. 1–17
87. U. Adhikari, T.H. Morris, N. Dahal, et al., *Development of power system test bed for data mining of synchrophasors data, cyber-attack and relay testing in RTDS[A]* (Power and Energy Society General Meeting[C]. IEEE, 2012), pp. 1–7
88. U. Franke, Optimal IT service availability: shorter outages, or fewer? Netw. Serv. Manag. IEEE. Transactions. **9**(1), 22e33 (2012)
89. I.A. Kirillov, S.A. Metcherin, S.V. Klimenko, *Metamodel of shared situation awareness for resilience management of built environment[A]* (International Conference on Cyberworlds[C]. IEEE, 2012), pp. 137–143
90. K. Adams, A. Wassell, M.G. Ceruti, et al., *Emergency-management situational-awareness prototype (EMSAP)[A]* (IEEE First International Multi-disciplinary Conference on Cognitive Methods in Situation Awareness & Decision Support[C]. IEEE, 2011), pp. 110–114
91. X. Jinping, *Speech at the Symposium on Internet Security and information technology (April 19, 2016) [N]* (people's daily, 2016), p. 2
92. S. Changxiang, Z. Huanguo, F. Dengguo, C. Zhenfu, H. Jiwu, Overview of information security[J]. Sci. Chin. Ser. E. Inform. Sci. **37**(2), 129–150 (2007)
93. J. Liu, P. Su, M. Yang, L. He, Y. Zhang, X.Y. Zhu, H. Lin, Software and cyber security - a survey[J]. J. Software **29**(1), 42–68 (2018)
94. J.-c. Jiang, H.-t. Ma, D.-e. Ren, S.-h. Qing, A survey of intrusion detection research on network security[J]. J. Software **11**(11), 1460–1466 (2000)

95. Y.-x. Lai, Z.-H. Liu, X.-t. Cai, K.-x. Yang, Research on intrusion detection of industrial control system[J]. J. Commun. **38**(2), 143–156 (2017)
96. L. Chuang, W. Yang, L. Quanlin, Stochastic modeling and evaluation for network security. Chin. J. Comput. **28**(12), 1943–1956 (2005)
97. H.Q. Wang, J.B. Lai, L. Zhu, Y. Liang, Survey of network situation awareness system. J. Comput. Sci. **33**(10), 5–10 (2006)
98. Z.H. Gong, Y. Zhuo, Research on cyberspace situational awareness. J. Software **21**(7), 1605–1619 (2010)
99. X.Z. Chen, Q.H. Zheng, X.H. Guan, C.G. Lin, Quantitative hierarchical threat evaluation model for network security. J. Software **17**(4), 885–897 (2006)
100. Us: progress and trend of network situational awareness research [J]. Anonymous. China information security, 2011 (2).
101. D. Wu, Y.-f. Lian, K. Chen, Y.-l. Liu, A security threats identification and analysis method based on attack graph. Chin. J. Comput. **35**(9), 1938–1950 (2012)
102. Y.Z. Zhang, B.X. Fang, Y. Chi, X.C. Yun, Risk propagation model for assessing network information systems. J. Software **18**(1), 137–145 (2007)
103. W. Yong, L. Yifeng, F. Dengguo, A network security situational awareness model based on information fusion. J. Comput. Res. Dev. **46**(3), 353–362 (2009)
104. M.-z. Li, J.-p. Lan, Smart home intrusion detection algorithm based on spatial-temporal field information fusion. J. Beijing Univ. Posts Tel. **40**(3), 76–84 (2017)
105. F. Ling, Z. Weijun, M. Shue, Security technology management strategy of multi-intrusion detection systems and manual investigation portfolio[J]. J. Southeast Univ. (Natural Science Edition) **45**(4), 811–816 (2015). https://doi.org/10.3969/j.issn.1001-0505.2015.04.034]
106. W.-w. Ren, L. Hu, K. Zhao, Intrusion alert correlation model based on data mining and ontology. J Jilin Univ. (Eng. Sci.) **45**(3), 899–906 (2015)
107. T. Chenghua, L. Pengcheng, T. Shensheng, X. Yi, Anomaly intrusion behavior detection based on fuzzy clustering and features selection. J. Comput. Res. Dev. **52**(3), 718–728 (2015)
108. W. Yichuan, M. Jianfeng, L. Di, Z. Liumei, M. Xianjia, Game optimization for internal DDoS attack detection in cloud computing. J. Comput. Res. Dev. **52**(8), 1873–1882 (2015)
109. F. Xuewei, W. Dongxia, L.J. Huang Minhuan, A mining approach for causal knowledge in alert correlating based on the markov property. J. Comput. Res. Dev. **51**(11), 2493–2504 (2014)
110. Z.-y. Luo, B. You, J.-z. Xu, Y. Liang, Automatic recognition model of intrusive intention based on three layers attack graph. J Jilin Univ. (Eng. Sci.) **44**(5), 1392–1397 (2014)
111. Y. Yu, C.-h. Xia, X.-y. Hu, Defense scheme generation method using mixed path attack graph. J. Zhejiang Univ. (Eng. Sci) **51**(9), 1745–1759 (2017)
112. F. Yan, S.-f. Liu, H. Leng, Study on analysis of attack graphs based on conversion. Chin. J. Electronics **42**(12), 2477–2480 (2014)
113. M. Chunguang, W. Chenghong, Z. Donghong, L. Yingtao, A dynamic network risk assessment model based on attacker's inclination. Journal of Computer Research and Development **52**(9), 2056–2068 (2015)
114. N. Gao, L. Gao, Y.-y. He, Dynamic security risk assessment model based on bayesian attack graph[J]. Journal of Sichuan University(Engineering Science Edition) **48**(1), 111–118 (2016)
115. H.U. Hao, Y.E. Run-guo, Z.H.A.N.G. Hong-qi, Y.A.N.G. Ying-jie, L.I.U. Yu-ling, Quantitative method for network security situation based on attack prediction[J]. Journal on Communications **38**(10), 122–134 (2017)
116. G. Hai-Hui, X. Da, C. Tian-Ping, Yang Yi-Xian. Quantitative evaluation approach for real-time risk based on attack event correlating. **35**(11), 2630–2636 (2013)
117. L. Kenan, Z. Yuqing, W. Chensi, M. Hua, A system for scoring the exploitability of vulnerability based types. Journal of Computer Research and Development **54**(10), 2296–2309 (2017)
118. H.U.A.N.G. Jia-Hui, F.E.N.G. Dong-Qin, W.A.N.G. Hong-Jian, A method for quantifying vulnerability of industrial control system based on attack graph. Acta Automatica Sinica **42**(5), 792–798 (2016)
119. G. Meng-Zhou, F. Dong-Qin, L. Cong-Li, C. Jian, Vulnerability analysis of industrial control system based on attack graph. Journal Of Zhejiang University (Engineering Science) **48**(12), 2123–2131 (2014)
120. W. Yufei, G. Kunlun, Z. Ting, Q. Jian, Assessing the harmfulness of cascading failures across space in electric cyber-physical system based on improved attack graph. Proceedings of the CSEE **36**(6), 1490–1499 (2016)
121. W. Jinrong, F. Dingyi, C. Xiaojiang, W. Huaijun, H. Lu, Taxonomy of software attack technique oriented to automated modeling[J]. Journal of SiChuan University: Engineer Science Edition. **47**(Z1), 91~98 (2015)
122. J. Christy, *Cyber threat & legal issues[A]* (Shadowcon Conference[C], USA, 1999), pp. 29–50
123. CVSS. Common Vulnerability Scoring System[EB/OL]. http://nvd.nist.gov/cvss.cfm, 2008.
124. J. Wei, F. Bin-Xing, Z. Hong-Li, Evaluating network security and optimal active defense based on attack-defense game model[J]. Chinese Journal of Computers. (4, 1), 817–827 (2009)
125. H.R. Shahriari, R. Jalili, Vulnerability take grant (VTG): an efficient approach to analyze network vulnerabilities[J]. Computers & Security **26**(5), 349–360 (2007)
126. H. Tianfield, in *IEEE International Conference on Internet of Things[C]*. Cyber security situational awareness[A] (IEEE, 2017), pp. 782–787
127. X. Fu, J. Shi, L. Xie, Layered intrusion scenario reconstruction method for automated evidence analysis. Journal of Software **22**(5), 996–1008 (2011)
128. C.X. Jun, F.B. Xing, T.Q.F.Z.H. Liang, Inferring attack intent of malicious insider based on probabilistic attack graph model. Chinese Journal of Computers. **37**(1), 62–72 (2014)
129. Y. Yun, X. Xi-shan, J. Yan, An Attack graph based probabilistic computing approach of network security. Chinese Journal of Computers. **33**(10), 001987–001996 (2010)
130. M. Frigault, L.Y. Wang, A. Singhal, S. Jajodia, Measuring network security using dynamic Bayesian network[A]. Proceedings of the 4th ACM Workshop on Quality of Protection[C]. IEEE, 23–30 (2008)
131. L. Wang, B. Wang, Y. Peng, *Research the information security risk assessment technique based on Bayesian network[A]. International Conference on Advanced Computer Theory and Engineering[C]* (IEEE, 2010), pp. 600–604
132. S.J. Zhang, J.H. Li, S.S. Song, L. Li, X.Z. Chen, Using Bayesian inference for computing attack graph node beliefs. Journal of Software **21**(9), 2376–2386 (2010)
133. Y.T. Liao, C.B. Ma, C. Zhang, A new fuzzy risk assessment method for the network security based on fuzzy similarity measure. The 6th World Congress on. Intelligent Control and Automation **2**, 8486–8490 (2006)
134. T.P. Chen, X.Y. Zhang, L.Q. Zheng, Network security risk assessment based on fuzzy integrated judgment[J]. Journal of Naval University of Engineering, 38–41 (2009)
135. L. Zhao, Z. Xue, Synthetic security assessment based on variable consistency dominance-based rough set approach. High Technology Letters. **16**(4), 413–421 (2010)
136. L.S. Kong, X.F. Ren, Y.J. Fan, in *IEEE International Conference on Intelligent Computing and Intelligent Systems[C]*. Study on assessment method for computer network security based on rough set[A] (IEEE, 2009), pp. 617–621
137. Feng PH, Lian YF, Dai YX, Bao XH. A vulnerability model of distributed systems based on reliability theory. Journal of Software, 2006,17(7):1633 – 1640.
138. L. Yan, H. Guangqiu, C. Lixia, The probability controllability of complex network via attack[J]. Journal of Frontiers of Computer Science & Technology **10**(10), 1407–1419 (2016)
139. B. Scheier, Attack trees: modeling security threats[J]. Dr Dobb's Journal **12**(24), 21–29 (1999)
140. O. Sheyner, J. Haines, S. Jha, in *Proceedings of the IEEE Symposium on Security and Privacy*. Automated generation and analysis of attack graphs[C] (IEEE Computer Society Press, Oakland, 2002), pp. 273–284
141. L.P. Swiler, C. Phillips, D. Ellis, S. Chakerian, in *Proceedings of the DARPA Information Survivability Conference and Exposition II, Anaheim, CA*. Computer attack graph generation tool (2001), pp. 307–321
142. J. Homer, A. Varikuti, X.M. Ou, M.Q. MA, *Improving attack graph visualization through data reduction and attack grouping //Proceedings of the 5th International Workshop on Visualization for Computer Security(VizSec2008) Cambridge, MA, USA, 2008* (Springer Verlag, Belin Heidelberg, Germany, 2008), pp. 68–79
143. Y. Yun, X. Xishan, Q. Zhichang, et al., Attack graph generation algorithm for large-scale network system[J]. Journal of Computer Research and Development **10**, 2033–2139 (2013)
144. K. Ingols, M. Chu, R. Lippmann, S. Webster, S. Boyer, *Modeling modern network attacks and counter measures using attack graphs//Proceedings of the 25th Annual Computer Security Applications Conference* (Honolulu, Hawaii, USA, 2009), pp. 117–126
145. L. Weixin, Z. Kangfeng, W. Bin, Alert processing based on attack graph and multi-source analyzing [J]. journal of communications **2015**(9), 135–144
146. L.I.U. Wei-xin, Z.H.E.N.G. Kang-feng, H.U. Ying, et al., Approach of goal-oriented attack graph-based threat evaluation for network security[J]. JOURNAL OF BEIJING UNIVERSITY OF POSTS AND TELECOM **38**(1), 82–86 (2015)
147. M. Dacier, *Towards quantitative evaluation of computer security[D]* (Institut National Polytechnique de Toulouse, France, 1994)

148. R. Ortalo, Y. Deswarte, M. Kaaniche, Experimenting with quantitative evaluation tools for monitoring operational security. IEEE Transactions on Software Engineering **25**(5), 633–650 (1999)
149. L. Wang, *A quantitative computer system and network security risk assessment method[D]* (Harbin Institute of Technology, 2002)
150. P.A. Porras, R. Kemmerer, in *Proceedings of the Eighth Annual Computer Security Applications Conference[C]*. A penetration state transition analysis: a rule-based intrusion detection approach[A] (IEEE, 1992), pp. 220–229
151. F. Stevens, T. Courtney, S. Singh, A. Agbaria, J.F. Meyer, W.H. Sanders, P. Pal, *Model-based validation of an intrusion-tolerant information system[A]* (Proceedings of 23rd Symposium on Reliable Distributed Systems (SRDS 2004)[C]. Florianópolis, Brazil, 2004), pp. 184–194
152. B. Madan, Go eva-Popstojanova K, Vaidyanathan K,Trivedi KS. A method for modeling and quantifying the security attributes of intrusion tolerant systems[J]. Performance Evaluation **56**(1-4), 167–186 (2004)
153. G. Xiang, Zhu Yue-fei,Liu Sheng-li. Attack composition model based on generalized stochastic colored Petri nets[J]. Journal of Electronics & Information Technology **35**(11), 2608–2614 (2013)
154. L.I.N. Chuang, W.A.N.G. Yuan-zhuo, Y.A.N.G. Yang, Q.U. Yang, Research on network dependability analysis methods based on stochastic Petri net[J]. ACTA ELECTRONICA SINICA **34**(2), 322–332 (2006)
155. G.A.O. Xiang, Z.H.U. Yue-fei, L.I.U. Sheng-li, F.E.I. Jin-long, L.I.U. Long, Risk assessment model based on fuzzy Petri nets[J]. Journal on Communications **2013**(s1), 126–132
156. R. ANDERSON, in *Proceedings of 17th Annual Computer Security Application Conference[C]*. Why information security is hard-an economic perspective[A] (IEEE Computer Society, Washington, DC, USA, 2001), pp. 39–40
157. Y.B. REDDY, *A game theory approach to detect malicious nodes in wireless sensor networks[A]. Procof the 3rd International Conference on Sensor Technologies and Application[C]* (IEEE Computer Society, Washington, DC, 2009), pp. 462–468
158. S.G. SHEN, Y.J. LI, H.Y. XU, Signaling game based strategy of intrusion detection in wireless sensor networks[J]. Computers & Mathematics with Applications **62**(6), 2404–2416 (2011)
159. J. Chunful, Z. Anming, Z. Wei, M. Yong, Incomplete informational and dynamic game model in network security[J]. J. Comp. Res. Dev **43**(s2), 530–533 (2006)
160. J.-M. Zhu, B. Song, Q.-F. Huang, Evolution game model of offense-defense for network security based on system dynamics[J]. J. Comm. **1**, 54–61 (2014)
161. W. Lin, H. Wang, J. Liu, L. Deng, A. Li, Q. Wu, Y. Jia, Research on cooperative active defense technology in network security based on non-dynamic game theory[J]. J. Comp. Res. Dev. **48**(2), 306–316 (2011)
162. Y. Zhang, X.B. Tan, X.L. Cui, H.S. Xi, Network security situation awareness approach based on Markov game model. J. Software **22**(3), 495–508 (2011)
163. J.X. Ran, B. Xiao, *Risk evaluation of network security based on NLPCA–RBF neural network[A]. International Conference on Multimedia Information Networking and Security[C]* (IEEE, 2010), pp. 398–402
164. Y. Liang, H.Q. Wang, J.B. Lai, *Quantification of network security situational awareness based on evolutionary neural network. The 6th International Conference on Machine Learning and Cybernetics*, vol 6 (2007), pp. 3267–3272
165. G. Wang, J. Hao, J. Ma, et al., A new approach to intrusion detection using artificial neural networks and fuzzy clustering[J]. Expert Syst. Appl. **37**(9), 6225–6232 (2010)
166. N. Gao, L. Gao, Y.Y. He, A lightweight intrusion detection model based on autoencoder network with feature reduction[J]. Acta Electron. Sinica **45**(3), 730–739 (2017)
167. S.A. Hofmeyr, S. Forrest, Architecture for an artificial immune system. Evolutionary Computation **7**(1), 45–68 (2000)
168. J. Kim, J.B. Peter, in *Proceedings of the World Congress on Computational Intelligence[C]*. Towards network intrusion detection: artificial immune system for investigation of dynamic clone selection[A] (IEEE Press, Piscataway, 2002), pp. 1015–1020
169. L. Tao, Network security risk detection based on immune[J]. Sci. Chin. Ser. E. Inform. Sci. **35**(8), 798–816 (2005)
170. L. Tao, An immune based model for network monitoring [J]. Chin J Comp **29**(9), 1515–1522 (2006)
171. F. Dai, K. Zheng, S. Luo, B. Wu, in *Proc of 2015 IEEE International Conference on Communications[C]*. Towards a multi objective framework for evaluating network security under exploit attacks [A] (IEEE Press, New York, 2015), pp. 8814–8819
172. J. Zhang, F. Liu, W. Han, et al., *Research and implement of configurable network security index system[A]* (International Conference on Applied Robotics for the Power Industry[C]. IEEE, 2012), pp. 645–648
173. Y.Z. Zhang, X.C. Yun, Network operation security index classification model with multidimensional attributes. Chin. J. Comp. **35**(8), 1666–1674 (2012)
174. D. Keim, J. Konlhammer, G. Ellis, F. Mansmann, *Mastering the information age: solving problems with visual analytics* (Eruographics Association, Goslar, 2010), pp. 1–168
175. D. Phan, J. Gerth, M. Lee, A. Paepcke, T. Winograd, in *Viz SEC 2007[C]*. Visual analysis of network flow data with timelines and event plots[A] (Springer, 2008), pp. 85–99
176. Y. Ye, X.-S. Xu, Y. Jia, Z.-C. Qi, W.-C. Cheng, Research on the risk adjacency matrix based on attack graphs[J]. J. Comm. **32**(5), 112–120 (2011)
177. L. Wang, S. Noel, S. Jajodia, Minimum cost network hardening using attack graphs [J]. Computer Communications **29**(18), 3812–3824 (2006)
178. S. Wang, Z. Zhang, Y. Kadobayashi, Exploring attack graph for cost-benefit security hardening [J]. Comp. Security **32**, 158–169 (2013)
179. S. Noel, S. Jajodia, B. O'Berry, et al., *Efficient minimum-cost network hardening via exploit dependency graphs [A].// Proc of the 2003 Annual Computer Security Applications Conference [C]* (IEEE Press, New Jersey, 2003), pp. 86–95
180. S. Jajodia, S. Noel, *Topological vulnerability analysis: a powerful new approach for network attack prevention, detection, and response [J]* (Algorithms, architectures and information systems security, Indian institute platium jubilee series, 2009), pp. 285–305
181. K. Ingols, M. Chu, R. Lippmann, et al., in *Proc of the 2009 Annual Computer Security Applications Conference [C]*. Modeling modern network attacks and countermeasures using attack graphs [A] (IEEE Press, New Jersey, 2009), pp. 117–126
182. R. Dewri, I. Ray, N. Poolsappasit, et al., Optimal security hardening on attack tree models of networks: a cost-benefit analysis. Int. J. Info. Security **11**(3), 167–188 (2012)
183. Gartner. Information security is becoming a big data analytics problem[EB/OL].[2012]. https://www.gartner.com/doc/1960615/information-security-big-data-analytics.
184. V. Mayer-Schnberger, K. Cukier, *Big data: a revolution that will transform how we live, work, and think* (John Munay Publishers, USA, 2013)
185. Big data white paper (2016). Beijing: China information and Communication Research Institute (Institute of telecommunications, Ministry of industry and information technology), 2016.
186. G. Cerullo, L. Coppolino, S. D'Antonio, et al., *Enabling convergence of physical and logical security through intelligent event correlation[M]//Intelligent Distributed Computing IX* (Springer, Berlin, 2016), pp. 427–437
187. M.H. Bhuyan, D.K. Bhattacharyya, J.K. Kalita, Network anomaly detection: methods, systems and tools. IEEE Commun. Surveys Tutorials **16**(1), 303–336 (2014)
188. Cisco. OpenSOC: Big data security analytics framework [EB/OL]. http://opensoc.github.io/, 2017.
189. F. Fischer, D.A. Keim, *NStreamAware: real-time visual analytics for data streams to enhance situational awareness[C]// Proceedings of the Eleventh Workshop on Visualization for Cyber Security* (ACM, New York, 2014), pp. 65–72
190. S. Marchal, X. Jiang, R. State, et al., A big data architecture for large scale security monitoring[C]//Proceedings of the 2014 IEEE International Conference on Big Data. Anchorage: IEEE, 56–63 (2014)
191. T. Dumitras, D. Shou, *Toward a standard benchmark for computer security research: the worldwide intelligence network environment (WINE)[C]// Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security* (ACM, New York, 2011), pp. 89–96
192. P. Giura, W. Wang, Using large scale distributed computing to unveil advanced persistent threats. Science **1**(3), 93–105 (2012)
193. Wang Z. The applications of deep learning on traffic identication [EB/OL]. [2017]. https://www.blackhat.com/docs/us-15/materials/us-15-Wang-The-Applications-Of-Deep-Learning-On-Traffic-Identification-wp.pdf.
194. Musthaler L. How to use deep learning AI to detect and prevent malware and APTs in real-time[EB/OL]. [2017-03-20]. http://www.networkworld.com/article/3043202/security/how-to-use-deep-learning-ai-to-detect-and-prevent-malwareand-apts-in-real-time.html.
195. X. Chen, Z. Xuemei, W. Wang, et al., Big data analytics for network security and intelligence. Adv. Eng. Sci. **49**(3), 1–12 (2017)

Publisher's Note