Accepted Manuscript

Network security situation: From awareness to awareness-control

Xiaowu Liu, Jiguo Yu, Weifeng Lv, Dongxiao Yu, Yinglong Wang, Yu Wu

PII: S1084-8045(19)30146-8

DOI: https://doi.org/10.1016/j.jnca.2019.04.022

Reference: YJNCA 2365

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

Received Date: 25 October 2018

Revised Date: 25 March 2019

Accepted Date: 25 April 2019

Please cite this article as: Liu, X., Yu, J., Lv, W., Yu, D., Wang, Y., Wu, Y., Network security situation: From awareness to awareness-control, *Journal of Network and Computer Applications* (2019), doi: https://doi.org/10.1016/j.jnca.2019.04.022.

Network Security Situation: From Awareness to Awareness-control

Xiaowu Liu[a], Jiguo Yu[b,c,a,*], Weifeng Lv[d], Dongxiao Yu[e], Yinglong Wang[b,c], Yu Wu[f]

[a]School of Information Science and Engineering, Qufu Normal University, Rizhao, Shandong, 276826, China
[b]School of Computer Science and Technology, Qilu University of Technology (Shandong Academy of Sciences), Jinan, 250253. Shandong, P.R. China
[c]Shandong Computer Science Center (National Supercomputer Center in Jinan), Jinan, Shandong, 250014, P.R. China
[d]School of Computer Science and Engineering, Beihang University, Beijing, 100083, P.R. China
[e]School of Computer Science and Technology, Shandong University, Qingdao, 266237, Shandong, P.R. China
[f]School of Computer Science and Network Security, Dongguan University of Technology, Dongguan, 523808, Guangdong, P.R. China

Abstract

Network Security Situation Awareness (NSSA) is a security theory which can perceive the network threat from a global perspective. In this paper, we present a Cognitive Awareness-Control Model (CACM) for NSSA. CACM adopts the cross-layer architecture and cognitive circle which can break through the interactive barrier between different network layers. Firstly, we propose a decision-level fusion method in which different weights are assigned for different data sources so that the fusion accuracy can be improved. Secondly, a hierarchical quantification approach is discussed which can avoid inferring the complex memberships among network components. Finally, a cognitive regulation mechanism is analysed in order to solve the issue of automatic control. The simulation experiments show that our model can perceive and regulate the threat situation effectively. To the best of our knowledge, this is the first discussion which utilizes cognitive awareness-control to solve the regulation problem of NSSA.

Keywords: network security situation awareness, cognitive computing, multi-source fusion, threat gene, reinforced learning, cognitive control

1. Introduction

Network technology becomes an indispensable part of politics and economy either globally or locally. It has reached a higher level than ever before in serving national security and interests. However, due to the heterogeneity, the complexity and the continuous expansion of the scale in current network system, traditional network security techniques are short of adaptability and effective coordination to deal with the network security problems. This results in heavy economic losses, bad social effect and fatal security accidents. Network Security Situation Awareness (NSSA) meets the demands of network system and is regarded as one of the solutions to face the security challenges. It can fuse the alerts acquired from multiple security data sources and perceive the security threat in a real-time manner.

The Situation Awareness (SA) originates from the study of human factors in space flight. As a term, it is widely applied in the military battlefield and regarded as an essential technique to make decisions (Kalloniatis et al., 2017). SA considers security problems from a global perspective including perceiving, understanding and projecting the states of the network elements in a certain space-time condition (Endsley, 1988). Bass introduced SA into the field of network security and proposed the term of Cyberspace Situational Awareness (CSA) (Bass, 1999). After that, SA and the network security are integrated as a new research direction committed to increasing the awareness ability against the network threat in both wire and wireless networks, even in Internet of Things (Saganowski, et al., 2016; Xu et al., 2017). And many countries including USA, Australia, France, Germany, Canada, UK, Netherlands, Russia and so on, consider that CSA is a fundamental capability with respect to the information and control systems of a country (Franke et al., 2014). As an extension of what is mentioned above, we define NSSA as a process to acquire, understand, predict and display the threat evolution trends caused by the situation factors in a large scale network environment.

In the past decades, some key issues have been studied and many schemes have been proposed. However, some challenging problems remain to be investigated with the appearance of new network systems. NSSA models cannot break the interaction barriers among different network layers. The fusion awareness method is also an interesting research point. Furthermore, it is extremely important to construct an automatic control mechanism which may promote the autonomy of NSSA system. Faced with these challenges, we introduce the cross-layer structure and the cognitive circle into the model design of NSSA with four contributions to evolve the NSSA system from awareness to awareness-control.

- We adopt cross-layer and cognitive circle to deal with the information interaction obstacles among traditional

☆This work was supported in part by the National Natural Science Foundation of China under Grants 61672321, 61832012, 61771289, 61373027 and the Shandong Graduate Education Quality Improvement Plan SDYY17138.

*Corresponding author

Email addresses: ycmlxw@126.com (Xiaowu Liu), jiguoyu@sina.com (Jiguo Yu), lwf@buaa.edu.cn (Weifeng Lv), dxyu@sdu.edu.cn (Dongxiao Yu), wangyl@sdas.org (Yinglong Wang), wuyu@dgut.edu.cn (Yu Wu)

network layers and form a close-loop feedback structure which provides a novel network security situation awareness-control mechanism without the intervention of human beings.

- We propose a fusion algorithm which has the ability of producing global optimal fusion within all different network layers. We select the decision-level fusion because it can obtain accurate fusion results and has less prior probability requirement than fusion methods in other levels.
- We extend NSSA to a hierarchical pattern so that we can express the situation knowledge more intuitively than the demonstration of the network traffic or raw alerts in a figure. In particular, we decrease the difficulty of threat gene acquisition using the mathematic reasoning and reach the aim of obtaining them easily without any complex analysis among network components.
- We present a cognitive regulation mechanism which can control NSSA in an autonomic manner.

Using these four supporting points, we can form a complete cognitive feedback structure in which the bridge between dispersed computing and continuous control is constructed. Therefore, NSSA is able to perceive the outside network environment and control the inner running states. Furthermore, we design our simulation network and conduct a series of simulation experiments to verify our model and methods in practice. For the easy understanding, the abbreviation terms will be used in this paper can be found in Table 1.

Table 1: List of abbreviation terms

Aabbrebiation terms	Full name
SA	Situation Awareness
CSA	Cyber Situation Awareness
NSSA	Network Security Situation Awareness
IDS	Intrusion Detection System
D-S	Dempster-Shafer
AHP	Analytical Hierarchy Process
CC	Cognitive Computing
OODA	Observe-Orient-Decide-Act
NIDS	Netwrk Intrusion Detection System
HIDS	Host Intrusion Detetion System
BMM	Bit Matrix Method
CACM	Cognitive Awareness-Control Model
FADC	Fusion-Awareness-Decision-Control
FOD	Frame of Discernment
BBA	Basic Belief Assignment
PSO	Partical Swarm Optimization
CPSO-DS	Cross-layer Particle Swarm Optimization D-S
SSS	Service Security Situation
HSS	Host Security Situation
NSS	Network Security Situation
RL	Reinforce Learning
HS-QRL	Historical Situation based Q-value Reinforce Learning

The remainder of this paper is organized as follows. Section 2 reviews the related works. Section 3 presents our cognitive awareness-control model of NSSA. Section 4 discusses cross-layer fusion algorithm. Section 5 proposes the hierarchical quantification awareness method. Section 6 provides our cognitive control mechanism. Section 7 describes the simulation experiments and the whole paper is concluded in Section 8.

2. Related work

The model and fusion awareness method have attracted the increasing concerns in the study of NSSA. Although the awareness-control model and algorithm are in their infancy, the advancement of cognition science provides a solution for the construction of novel NSSA system.

The NSSA models can be classified into fusion-based model and feedback-based model. The first fusion-based NSSA model was proposed and it promoted fusion model to become a typical research direction (Bass et al., 1999). The fusion-based model holds that NSSA should include many components (factor extraction, awareness and projection) and may be introduced to multiple domains in order to perceive the threat of monitored networks. Many fusion-based NSSA models are derived from the model of Joint Directors of Laboratories (JDL), and they approve of the viewpoint of Department of Defense (DoD) that the fusion awareness should contain all parts of JDL from level 0 to level 5 (Azimirad et al., 2015). With the development of NSSA, more attention has been paid not only to the awareness of the network threat but also to the situation regulation. In the academic scope, Markov game theory has been adopted to construct the feedback-based models with the aim of solving the regulation problem of security situation through the scheme of system reinforce (Zhang et al., 2011). The multi-scale trust framework is also a novel feedback-based model which provides a dynamic adaptation mechanism for security system (Li et al., 2015). In the military scope, the Observe-Orient-Decide-Act (OODA) loop is adopted to form a feedback structure in the battle field which focuses on providing the availability and the robustness of weapons, missile systems and torpedo systems (Franke et al., 2014). In most of existing the NSSA models, the visualization is considered as an important technique to evaluate the security situation in an intuitive manner, which is a notable characteristic different from traditional security technology such as Intrusion Detection System (IDS) and Firewall. It should be pointed out that many research results regard the visualization of threat situation as an important component of NSSA and the visualization technique greatly enhances the administrators's ability to monitor and manage the networks (Shiravi et al., 2012; Hao et al., 2015; Angelini et al., 2017). Although many novel models were designed to cope with the increasing challenges in NSSA, the proposed methods and mechanisms remain to be examined through future applications. As to the visualization, the demonstration of the network traffic,

link state and raw alerts in a figure are difficult to obtain the network security situation in an accurate manner.

The fusion awareness method is the critical part of NSSA which is characterized by quantification threat evaluation under the support of multisource fusion. The fusion algorithm plays a significant role in ensuring accuracy awareness result. However, the priori probability and conditional probability are difficult to achieve for the randomness and suddenness of network events which cause the lack of enough information to manipulate the uncertainty in the process of fusion. The Dempster-Shafer (D-S) evidence theory meets the requirements of fusion and needs little communication bandwidth, low prior probability and conditional probability (Khaleghi et al., 2013), which has potential adaptability in NSSA. Two different schemes have been proposed to promote accuracy and decrease data conflict when D-S evidence theory is introduced into multisource fusion. One viewpoint is that the traditional D-S combination rule needs to be improved (Khaleghi et al., 2013). Adding linear weight can decrease uncertainty and avoid Zadeh paradox to some extent (Wei et al., 2009). However, the linear weight does not meet the requirement of associative law in the process of evidence combination and the fusion algorithm is prone to getting trapped in local optimization. Some researchers think that the distinguished combination rules should be designed for different data sources. For example, the conjunctive combination rule should be adopted if the data source is dependent (Fu et al., 2014) and the cautious combination rule can be applied if the data source is independent (Cattaneo et al., 2011). The other viewpoint holds that the traditional D-S combination rule should be kept in the original form and the conflict is caused by the wrong application or inconsistent evidence. Then, the solutions focus on dealing with the evidence before data fusion. For instance, the distance between two Basic Belief Assignments (BBAs) can be calculated to remove the inconsistent evidence (Feng et al., 2011) or the evidence supporting measure of similarity may regard as an outlier source identification tool so that only part of consistent evidence is fused. The above-mentioned methods are environment dependent and difficult to be applied into heterogeneous sensors fusion in network security systems. In addition, different approaches still have some issues to handle in order to increase the fusion accuracy and decrease the probability of data conflict in many practical networks.

Different from data fusion, the hierarchical security analysis, for its good scalability and low computational complexity (Hong et al., 2016), has become a widely accepted mechanism and attracted more concerns. The security situation may be depicted in different abstraction levels (Li et al., 2016), that is, the service level, the host level and the network level. Although hierarchical awareness is an efficient method to express the evolution trend of network threat, it is challenging to obtain the distinguished weights in different levels. Analytical Hierarchy Process (AHP) is a feasible solution adopted by many researchers (Hu et al., 2007; Zhang et al., 2012; Wang et al., 2018). However, AHP needs a complex correlation analysis among threat factors. As a result, it is short of self-adaptability and difficult to be applied into a dynamic network environment.

In recent years, the control of SA has attracted the attention of researcher (Evesti et al., 2015). It is eager to provide a mechanism which can perceive the security situation and assist the decision-making process as well (Rolim et al., 2016; Li et al., 2017). Meanwhile, the ability to maintain state awareness in the face of errors and threats is regarded as a defining feature of resilient control system (Teixeira et al., 2017). However, existing studies focus on the awareness and neglect the automatic control in NSSA.

The cognitive theory provides a novel solution to construct NSSA model which can offer basic theoretical support for situation awareness (Dapoigny et al., 2013), and the feedback analysis improves the decision-making process to a large extent (Erbachera et al., 2010; Skopik et al., 2013; Nscpoles et al., 2016; Anjaria et al., 2018). Though the cognitive ability is an attractive direction, the concrete architecture and the appropriate method are great challenges in further study of NSSA.

Cognitive Computing (CC), derived from cognitive informatics, is an intelligent computing methodology that simulates the mechanism of brain by autonomous inference. It provides a new mechanism to deal with the problems existing in current NSSA. Although there is no unified infrastructure to be widely accepted, CC which has the similar circle design as that of OODA has become a research direction in the academic scope (Sunilkumar et al., 2015). The cognitive circle of CC is capable of upgrading the adaptability of computing system and is convenient in building close-loop feedback structure. Meanwhile, the cross-layer design is considered to be the foundation of CC which can overcome the interaction obstacles between different layers in traditional network architecture (Fortuna et al., 2009; Kliks et al., 2017). The effectiveness of cross-layer structure has been validated in the field of wireless networks (Tran et al., 2013; Tefek et al., 2016; Sami et al., 2016). Different from wireless networks, the scope of cognitive ability in a wire network is not limited to a given layer and CC needs to solve the problem of optimal function overlap among all network layers. The autonomous characteristic and dynamic configuration are also regarded as preferable measures to actualize the self-adaptation of running system. CC can form a scheme which possess learning, remembering, thinking, awareness and other intelligent abilities for the structure and technology used in the next generation network (Wang et al., 2010). These intelligent activities simulate the basic autonomous evolvement ability of system platform and provide self-configuration (Kim et al., 2015) and running control without the participation of human beings (Gomez et al., 2011; Gupta et al., 2011; Ogiela et al., 2013; Chen et al., 2016).

3. Cognitive awareness-control model for NSSA

We introduce the cognitive idea into the framework design of NSSA and propose a Cognitive Awareness-Control Model (CACM) for network security situation based on fusion as shown in Fig.1. CACM inherits the layering structure which is compatible with traditional networks and embeds the cognitive ability in NSSA in order to solve the issues of cross-layer interaction and autonomous control. Specifically, CACM is composed of a network cognitive layer, a host cognitive layer, a service

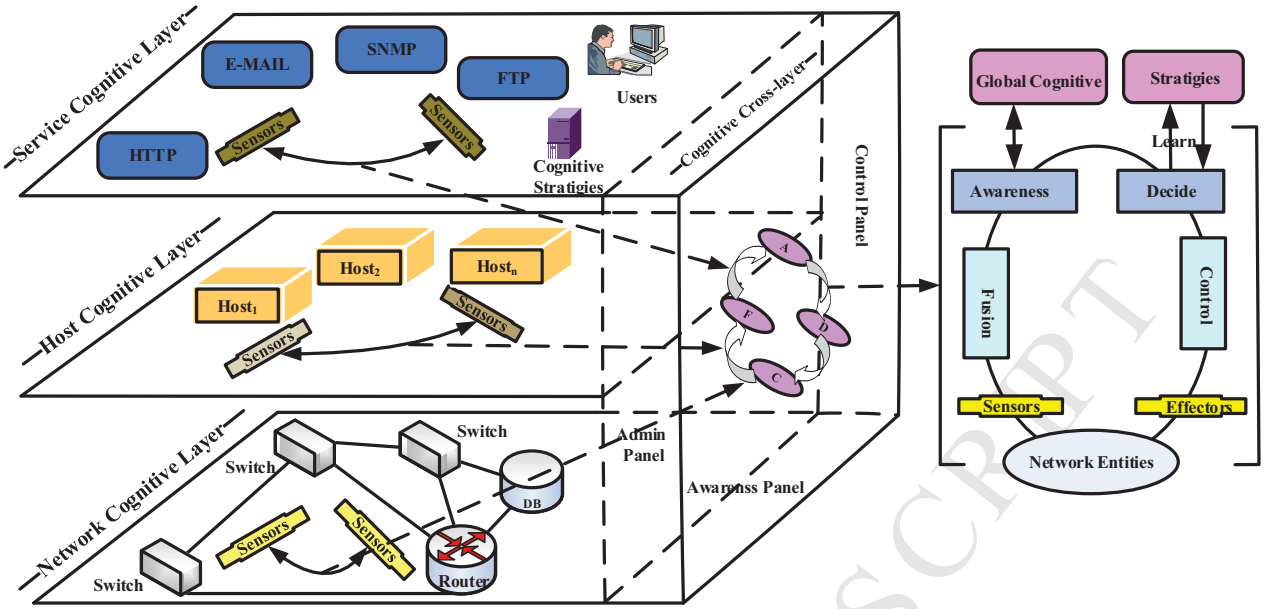

Figure 1: Network security situation cognitive awareness-control model

cognitive layer and a cognitive cross-layer. The network cognitive layer is the lowest one which includes routers, switches and other network entities. These entities run network protocol stack and are embedded in many security sensors such as the Network Intrusion Detection System (NIDS) and firewall. The host cognitive layer is formed by software and hardware resources of network systems. It also possesses the Host Intrusion Detection System (HIDS), the host log sensor and other host sensors. The service cognitive layer is to prepare all services provided by servers and strategies database. Similar to the network and host cognitive layers, it also has many sensors to monitor the operation states of the services.

In our model, the cross-layer structure is a critical part distinguished from the traditional network architecture. It inherits existing layering network structure and meets the hierarchical awareness demands of NSSA. This design solves the problem of communication obstacles among different network layers. Information can be exchanged freely and the interactions through cross-layer provide a solid support for coping with complex network threats. The core of this layer is a cognitive circle constructed by Fusion, Awareness, Decision and Control (FADC). The FADC cognitive circle forms a close-loop feedback structure as shown in Fig.2 and endows NSSA with the characteristic of concurrency and synchronization.

The FADC cognitive circle is one of the rare attempts to integrate cognitive capability into SA and renders the SA system effective in regulating the security situation instead of only fusing or perceiving the security threat of monitored network. We actualize the fusion component through an optimal technique with cross-layer fusion ability (Section 4) which makes the network threat more possible for quantification awareness (Section 5). Different from all the NSSA models in the current literature, we formalize the control component and propose the practical control algorithm by improving the machine learning

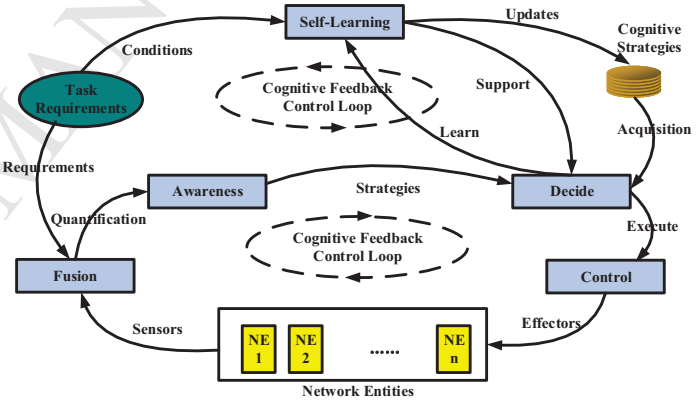

Figure 2: Cognitive circle synchronization response model

mechanism (Section 6). All components of FADC circle will be detailedly discussed in subsequent sections according to the sequence of awareness-control.

4. Cross-layer multi-source fusion

As one of the critical techniques and the foundation of situation awareness, the multi-source fusion determines the accuracy and robustness of quantification evaluation. Though D-S evidence theory is a generally accepted fusion method in NSSA, it is noted that direct fusion of all raw alerts of heterogeneous sensors in various layers with the same credibility is a key reason of producing fusion conflict. Here, we adopt two steps to deal with the above-mentioned issues: (a) eliminating the inconsistent evidences, and (b) constructing new evidence combination rules.

4.1. Eliminating inconsistent evidence

The inconsistent evidence is one of the key factors that produces fusion conflict. The authors in (Feng et al., 2011) illustrated the issue of inconsistent evidence which produced unreasonable fusion results. Many solutions, such as in (Li et al., 2011; Guo et al., 2011), fused the consistent evidences under the support of measuring the similarity of evidences. Different from existing results, we propose a novel scheme called Bit Matrix Method (BMM) to eliminate the inconsistent evidence and fuse the non-conflict evidence set. BMM consists of two steps, that is, the decision of conflict and the elimination of conflict evidence.

Assumed that a finite Frame of Discernment (FOD) $\Theta = \{A_1, A_2, \cdots, A_N\}$ and an evidence set $E = \{E_1, E_2, \cdots, E_n\}$. The Basic Belief Assignment (BBA) is represented as m which is a mapping from the power set of Θ to $[0, 1]$, $m : P(\Theta) \rightarrow [0, 1]$ and satisfies the following conditions:

(1) $m(\emptyset) = 0$;

(2) $\sum_{A \in P(\Theta)} m(A) = 1$.

Let m_i and m_j be two BBAs for $P(\Theta)$ where $i, j = 1, 2, \cdots, 2^N$. Take m_i as an instance, m_i denotes the support probability of the i-th evidence (E_i) to the elements in $P(\Theta)$. Then, the BBA vector of m_i can be represented as $\overrightarrow{m_i} = (m_i(A_1), m_i(A_2), \cdots, m_i(A_N), \cdots)$ where $A_j \in P(\Theta)$. The distance between m_i and m_j is defined in the following Equation (1) (Feng et al., 2011).

$$d_{ij}(m_i, m_j) = \sqrt{\frac{1}{2}(||\overrightarrow{m_i}||^2 + ||\overrightarrow{m_j}||^2 - 2 < \overrightarrow{m_i}, \overrightarrow{m_j} >)} \quad (1)$$

where $< \overrightarrow{m_i}, \overrightarrow{m_j} >$ is the scalar product of m_i and m_j, $||\overrightarrow{m_i}||^2$ and $||\overrightarrow{m_j}||^2$ are the square norms of m_i and m_j, respectively. By (1), the distances among all evidences can be depicted by a BBA Distance Matrix (DM).

$$DM = \begin{vmatrix} d_{11} & d_{12} & \cdots & d_{1n} \\ d_{21} & d_{22} & \cdots & d_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ d_{n1} & d_{n2} & \cdots & d_{nn} \end{vmatrix} \quad (2)$$

where $d_{ij} = d_{ij}(m_i, m_j)$ and $d_{ii} = 0$ for $i, j = 1, 2, ..., n$.

β is a predefined threshold of d_{ij} and can be used to evaluate the compatibility between different evidences as follows.

$$C_{ij} = \begin{cases} 1, d_{ij} \leq \beta \\ 0, d_{ij} > \beta \end{cases} \quad (3)$$

The relation between evidences can be represented using a symmetry Bit Matrix (BM) whose elements are equal to 0 or 1 according to Equation (2) and Equation (3).

$$BM = \begin{vmatrix} 1 & C_{12} & \cdots & C_{1n} \\ C_{21} & 1 & \cdots & C_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ C_{n1} & C_{n2} & \cdots & 1 \end{vmatrix} \quad (4)$$

In matrix BM, $C_{ij} = 0$ $(1 \leq i, j \leq n)$ represents that the i-th evidence and the j-th evidence are incompatible or inconsistent, and $C_{ij} = 1 (1 \leq i, j \leq n)$ denotes that these two evidences are compatible and consistent. We only need to fuse consistent evidences in order to decrease the probability of conflict and increase the accuracy of fusion.

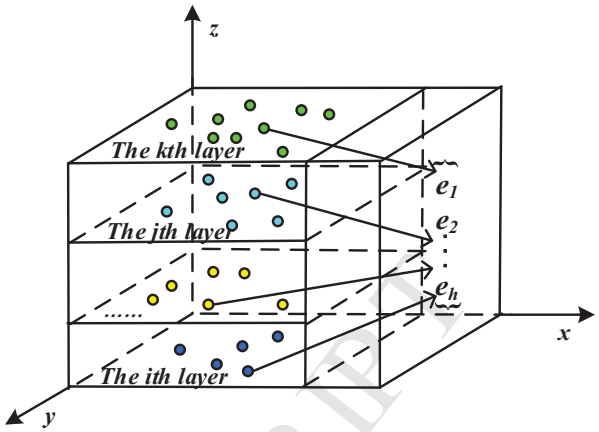

Figure 3: Particle swarm optimization

4.2. PSO-DS multi-source fusion

Although the traditional combination rules can be applied to multi-source fusion in a homogeneous network environment, they are not applicable in networks with heterogeneous security detectors for the reason that the heterogeneous detectors have different importance for the final fusion result. Note that assigning weight for different data sources is a good solution in D-S fusion. It can satisfy important properties of evidence combination (Cattaneo et al., 2011). Therefore, adding distinct weights for evidences become a widely used approach to improving the multi-source fusion in NSSA. However, the linear weight (Wei et al., 2009) does not meet the requirement of associative law in the process of evidence combination and the exponential weight depends on the experience recursion of experts. The nature of these two approaches is a process of parameter optimization by assigning different weights to distinct evidences from multiple data sources. In addition, these methods do not meet the requirement of cognitive awareness-control in the aspects of fusion accuracy and adaptability. Particle Swarm Optimization (PSO) is to obtain the global optimum through the corporation and competition among the particles (Ali et al., 2013; Tsekouras et al., 2013). It is widely applied in the fields of nonlinear and multi-peak optimization, especially in network field (Shakibian et al., 2014; Cao et al., 2018) including network security (Sun et al., 2018). We here extend the PSO to the cognitive fusion and propose a cross-layer PSO algorithm combined with the D-S combination rule (CPSO-DS), as shown in Fig.3, to solve the problem of cognitive fusion. We use the following Equation (5) in PSO to update the velocity (v_{td}) and the position (x_{td}) of the particles distributed in every layer of our model, with the aim of searching for the exponential optimal weights for D-S evidence fusion.

$$\begin{cases} v_{td} = \omega \cdot v_{td} + c_1 \cdot rand - num() \times (p_{td} - x_{td}) + \\ c_2 \cdot rand - num() \cdot (p_{gd} - x_{td}) \\ x_{(t+1)d} = x_{td} + v_{td} \end{cases} \quad (5)$$

where $t = 1, 2, \cdots, s$ and s is the population size; c_1 and c_2 are constants and they can push the particles to the local optimal weight (p_{td}) and global optimal weight (p_{gd}); $rand - num()$ is

a random number function whose value is in [0,1]; w is the decreasing inertia weight. Meanwhile, the optimal weights need to satisfy the fitness function declared in Equation (6).

$$F_i = max\{m(A_i) - max[m(A_j)]\} \tag{6}$$

where $j \neq i$, $j = 1, 2, \cdots, h$ and h is the number of propositions. If A_i is the decision object, then $m(A_i)$ is the BBA of A_i. F_i indicates that it can maximize the difference between the decision object and other non-decision objects. In other words, the D-S fusion can recognize a network attack more easily and accurately after searching for the optimal exponential weights by CPSO. Constrained by fitness function, the CPSO assigns different fusion weights, $e_1, e_2, \cdots, e_h$, for various data from different data sources and the D-S combination rule is improved to Equation (7).

$$m(A) = \frac{\sum_{A_1 \cap A_2 \cap \cdots \cap A_h = A} m(B)}{1 - K_h} \tag{7}$$

where $A \neq \emptyset$, $m(B) = m_1(A_1)^{e_1} m_2(A_2)^{e_2} \cdots m_h(A_h)^{e_h}$ and $K_h = \sum_{A_1 \cap A_2 \cap \cdots \cap A_h = \emptyset} m_1(A_1)^{e_1} m_2(A_2)^{e_2} \cdots m_h(A_h)^{e_h}$.

Through searching for the optimal fusion weights by CPSO, the new combination rule satisfies the basic properties of D-S evidence theory, such as the associative law and the distributive law. Furthermore, CPSO assigns different credibility to distinct data sources. As a result, the improved D-S combination rule can decrease the uncertainty and the rate of conflict. In addition, CPSO itself has the favorable self-adaptability. Even though there are unknown network attacks appearing in a network, we only need to train CPSO using the new attack patterns without duplicated training with all primary samples.

5. Network security situation quantification awareness

After the improvement of D-S evidence theory, we solve the problems of accuracy and consistency in fusion. The situation awareness is a procedure of situation factor quantification according to the fusion results. The situation factors are the reductive information representation of security threats in a higher abstraction layer which can generate security situation more easily. In this section, we discuss an acquisition method of threat genes and a situation awareness method with the characteristic of hierarchy.

5.1. Situation factor quantification

For a successful NSSA system, effective awareness depends on reasonable factor quantification. The situation factors should include all critical attributes causing the change of threat situation, such as threat gene (threat degree), attack intensity (event frequency) and asset importance. Among these factors, the attack intensity and the asset importance are easy to deal with. However, the threat gene is a prerequisite for the perceiving of security situation which is difficult to be quantified. The experience recursion and AHP hierarchical analysis (Hu et al., 2007) are widely accepted methods to overcome the challenge in the current research of threat gene obtaining. Note that, the former

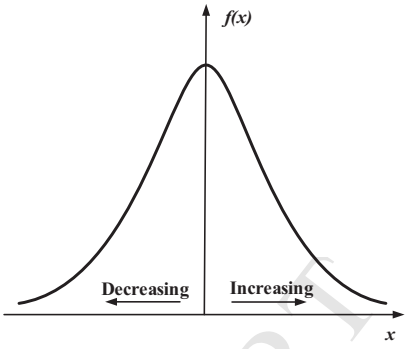

Figure 4: Threat gene pattern

relies on the subjective knowledge and the latter needs complex association analysis among the network components. In the remaining part of this section, we define the connotation of threat gene and discuss a novel method to assess the threat gene.

Definition 1. The threat gene is the quantitative representation of severity degree. In a time window, a network entity undergoes n attacks which can be classified into g ($0 \leq g \leq n$) threat grades (the different attacks may belong to the same threat grade). Then, the threat gene of the k-th grade is defined as Equation (8).

$$l_k = \begin{cases} \frac{1}{2} + \frac{\sqrt{-2ln\frac{2k}{n}}}{6}, 1 \leq k < \frac{n}{2} \\ \frac{1}{2}, k = \frac{n}{2} \\ \frac{1}{2} - \frac{\sqrt{-2ln[2-\frac{2k}{n}]}}{6}, \frac{n}{2} < k < n \end{cases} \tag{8}$$

We expand the weighted coefficient theory in the field of multi-object decision (Chen et al., 2002) into NSSA through discretization of the normal distribution in order to provide a relatively easy way to obtain quantitative threat gene (as shown in Equation (8)). Assumed that there are n different kinds of objects which need to be assigned threat genes. The decision object is to acquire g threat genes for n objects. We regard every threat gene as a binary random variable, x_i, with the values being 1 or -1 for the purpose of ensuring that the variable meets the demand whose mean is zero. Let $X_n = \sum_{i=1}^{n} x_i$ and $Y = \frac{X_n}{\sqrt{n}}$ respectively. If Y obeys the normal distribution, then X_n approximately obeys the normal distribution $N(0, \sqrt{n})$ when $n \to \infty$. In the coordinate, the abscissa (x) represents the importance of the decision objects (the numerical values of threat genes) and the ordinate ($f(x)$) stands for the number of decision object (be sorted by threat grade from high to low). According to the characteristic of normal distribution, we describe the pattern of threat gene as shown in Fig.4. The threat genes of more serious network events are near to the right in the first quadrant. On the contrary, the threat genes of less serious network events are far to the left in the second quadrant. We divide the ordinate with the scaling factor α in Fig.5 and execute symmetry axis transformation using line $f(x) = f(0)$ which transforms Fig.5 to Fig.6. The goal of the following inference process is that we should calculate the threat genes only in the condition of knowing threat grade.

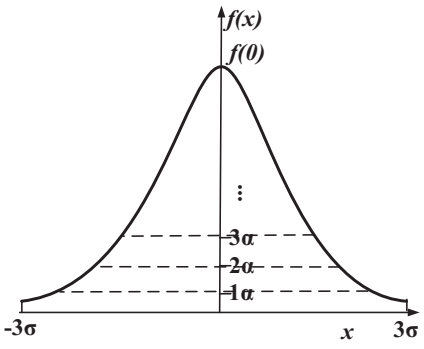

Figure 5: Threat averaging separation using interval α

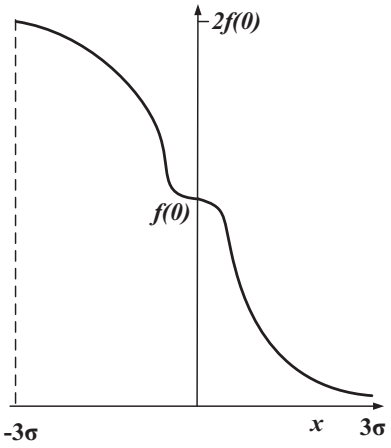

Figure 6: Symmetry axis transformation

The general form of normal density function can be expressed as Equation (9) where μ and σ are the mean value and the standard deviation respectively.

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \tag{9}$$

The Equation (9) can be represented as Equation (10) in the condition of $\mu = 0$.

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{x^2}{2\sigma^2}} \tag{10}$$

Then, the functional relation in Fig.6 can be formalized as Equation (11).

$$f(x) = \begin{cases} \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{x^2}{2\sigma^2}}, x > 0 \\ \frac{1}{\sigma\sqrt{2\pi}}, x = 0 \\ \frac{2}{\sigma\sqrt{2\pi}} - \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{x^2}{2\sigma^2}}, x < 0 \end{cases} \tag{11}$$

We assume that the values of independent variable are approximately distributed in $(-3\sigma, +3\sigma)$ in Fig.6. After that, we shift the normal distribution curve to the left for 3σ and the Fig.6 is transformed to Fig.7. Therefore, the expression of Fig.7

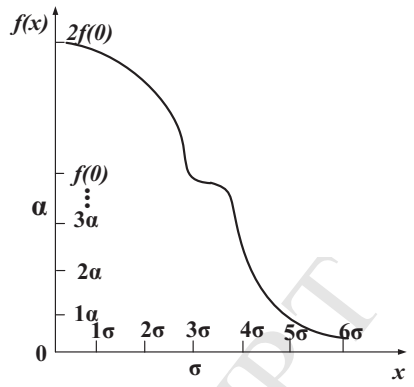

Figure 7: Curve shifting with 3σ

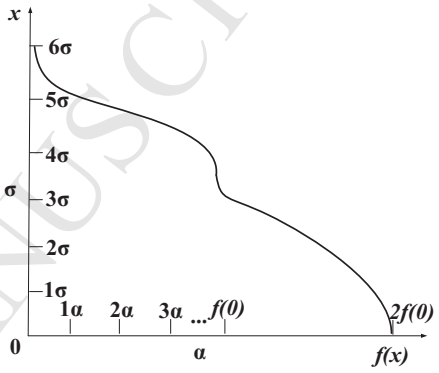

Figure 8: Coordinate transformation

can be deduced to Equation (12) according to Equation (11).

$$f(x) = \begin{cases} \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-3\sigma)^2}{2\sigma^2}}, x > 3\sigma \\ \frac{1}{\sigma\sqrt{2\pi}}, x = 3\sigma \\ \frac{2}{\sigma\sqrt{2\pi}} - \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(3\sigma-x)^2}{2\sigma^2}}, x < 3\sigma \end{cases} \tag{12}$$

In Fig.7, the ordinate is an independent variable (threat grade) and the abscissa is function value (numerical value of the threat genes). This does not accord with the usual representation of function and we change Fig.7 to Fig.8 using coordinate transformation.

Next, we derive the expression of x using $f(x)$ according to Equation (12). Meanwhile, we replace x with y, substitute x for $f(x)$ and obtain Equation (13).

$$y = \begin{cases} 3\sigma + \sqrt{-2\sigma^2 ln[\sigma\sqrt{2\pi}x]}, 0 < x < b_1 \\ 3\sigma, x = b_1 \\ 3\sigma - \sqrt{-2\sigma^2 ln[\sigma\sqrt{2\pi}(\frac{2}{\sigma\sqrt{2\pi}} - x)]}, b_1 < x < b_2 \end{cases} \tag{13}$$

where $b_1 = \frac{1}{\sigma\sqrt{2\pi}}$ and $b_2 = \frac{2}{\sigma\sqrt{2\pi}}$.

According to Equation (13), we know that the domain of x is $(0, \frac{2}{\sigma\sqrt{2\pi}})$ and can be divided into n equal parts, $x_i = \frac{i}{n} \times \frac{2}{\sigma\sqrt{2\pi}} = \frac{2i}{n\sigma\sqrt{2\pi}}$ $(1 \le i \le n)$. We substitute x_i into Equation (13)

and y_i is the threat gene of i-th queue grade.

$$y_i = \begin{cases} 3\sigma + \sqrt{-2\sigma^2 ln[\sigma\sqrt{2\pi}x_i]}, 0 < x_i < b_1 \\ 3\sigma, x_i = b_1 \\ 3\sigma - \sqrt{-2\sigma^2 ln[\sigma\sqrt{2\pi}(\frac{2}{\sigma\sqrt{2\pi}} - x_i)]}, b_1 < x_i < b_2 \end{cases} \quad (14)$$

where $b_1 = \frac{1}{\sigma\sqrt{2\pi}}$ and $b_2 = \frac{2}{\sigma\sqrt{2\pi}}$.

From Fig. 8, we can know the maximum threat gene, y_{max}, is approximately equal to 6σ. Then, we replace x_i in Equation (14) with $\frac{2i}{n\sigma\sqrt{2\pi}}$ and the i-th threat gene, G_i, can be quantified as Equation (15).

$$G_i = \frac{y_i}{y_{max}} = \begin{cases} \frac{1}{2} + \frac{\sqrt{-2ln\frac{2i}{n}}}{6}, 1 \le i < \frac{n}{2} \\ \frac{1}{2}, i = \frac{n}{2} \\ \frac{1}{2} - \frac{\sqrt{-2ln[2-\frac{2i}{n}]}}{6}, \frac{n}{2} < i < n \end{cases} \quad (15)$$

Then, Definition 1 is concluded according to Equation (15). After that, the quantitative threat gene can be obtained if we know the number of different threat types (n) and the threat grades (i). This method also has better adaptability. The new threat gene can be achieved using Equation (15) autonomously without depending on expert knowledge and subjective experience when NSSA is applied into other networks. In addition, we do not need complex correlation analysis similar to AHP and decrease the difficulty in the obtaining of threat gene. For example, the NSSA system is migrated to another network which has m threat types and j threat grades. We only need to set $n = m$ and $i = j$ in Equation (15) and the new threat genes are quantified.

5.2. Threat quantification evaluation

We classify the network security situation into three levels including the service level, the host level and the network level. The core idea is that the security situation value can be generated from the situation factors at all levels.

5.2.1. Service security situation

The service security situation is related to not only threat gene but also attack intensity or other situation factors.

Definition 2. The Service Security Situation (SSS) is a symbol of threat that a certain service suffers from. Under the condition of Definition 1, the weights of attacks are quantified as l_k ($1 \le k \le g$) using Equation (8). Assumed that there are u services deployed in a network system and the i-th service is presented as S_i ($0 \le i \le u$). The total number of the attacks aiming at S_i is N_i and the number of j-th type of attacks is expressed as N_{ij}. N_{ij} is called attack intensity which satisfies $N_i = \sum_{j=0}^{g} N_{ij}$. Then, we describe SSS of S_i as Equation (16) with the above-mentioned factors.

$$V_{S_i} = \sum_{k=1}^{g} (N_{i_k} 10^{l_k}) \quad (16)$$

In Equation (16), we choose 10^{l_k} as the situation parameter in order to emphasize the importance of threat gene and weaken the influence degree of attack intensity on SSS.

5.2.2. Host security situation

The host security situation is mainly related to the number of services, service weights, service security situation and so on.

Definition 3. The Host Security Situation (HSS) is the threat that a host undergoes in a network system. Let that there are u services running on host H_l ($1 \le l \le v$) and v is the number of hosts in a monitored network. The threat factor of the i-th service is f_{S_i} ($1 \le i \le u$). Then, HSS can be defined as Equation (17).

$$V_{H_l} = \sum_{i=1}^{u} (V_{S_i} f_{S_i}) \quad (17)$$

where u represents the number of services on host H_l. We quantify the threat gene of the i-th service, t_{S_i}, out of u services using Equation (8) and normalize it with Equation (18).

$$f_{S_i} = \frac{t_{S_i}}{\sum_{j=1}^{r} t_{S_i}} \quad (18)$$

where $i = 1, 2, \cdots, r$ and r different threat grades are determined by the kickback caused by the services failure. Then, we can normalize all service threat genes, $t_{S_1}, t_{S_2}, \cdots, t_{S_r}$, with Equation (18) and represent the threat of service with quantification value.

5.2.3. Network security situation

Different from the former two security situations, network security situation expresses the network threat from an overall perspective. It is related to every situation factor discussed in service and host security situation. In addition, the number of hosts and the host importance are also significant parts of network security situation.

Definition 4. The Network Security Situation (NSS) perceives the threat situation from the perspective of whole network. In a network system, there are v hosts which are divided into p grades according their importance to the network system. Then, the importance weight of the i-th grade is $g_{H_l}(1 \le l \le p)$. Combined with the HSS, the NSS may be elaborated as Equation (19).

$$V_{NS} = \sum_{l=1}^{p} (V_{H_l} g_{H_l}) \quad (19)$$

As one of the importance weights, the threat genes of all hosts, $q_{H_1}, q_{H_2}, ..., q_{H_p}$, are assigned by Equation (8), then we normalize them using Equation (20) in order to obtain $g_{H_l}(1 \le l \le p)$ in Equation (19).

$$g_{H_l} = \frac{q_{H_l}}{\sum_{j=1}^{p} q_{H_j}} \quad (20)$$

The importance weights of host are composite parameters which depend on different network applications. We will illustrate other environment-dependent parameters in the simulation experiment.

The proposed hierarchical awareness method can change the discrete situation factors to risk values and provide a new

threat presentation in combination with the visualization technique. With the application of this new method, the administrators need not pay most of their efforts to deal with the serious false alerts and they may monitor their network and perceive the threat evolution simultaneously instead.

6. Cognitive control based on reinforce learning

The awareness-control by manual system enhancement (Zhang et al., 2011) is an optional approach to guaranteeing the control ability of NSSA. However, this method is prone to errors and poor in real-time nature. Moreover, it places high requirements on administrators. Faced with these issues, we propose a cognitive control mechanism based on Reinforce Learning (RL) to form the close-loop structure of FADC cognitive circle (shown in Fig.2) and achieve the autonomous awareness-control. In this section, our contributions are twofold including a formal description of NSSA cognitive control and an automatic approach of situation regulation.

6.1. Formal mode of RL in NSSA

A network security system can not only perceive the threat but also possess the abilities of self-control. The cognitive control mechanism based on RL provides an unsupervised regulation method which can adjust the states of NSSA autonomously. RL is independent from the specific mathematical model and has been applied into many automatic control scenarios (Schaal et al., 2010; Bhasin et al., 2011) including network domain (Akhtar et al., 2016; Wang et al., 2016). Compared with other machine learning techniques (e.g., artificial neural network and support vector machine), three aspects have a direct impact on driving us to choose RL as the favorite control mechanism in NSSA. (i) RL endows different importance to the same experience at different times. (ii) RL needs less training than other machine learning techniques. (iii) RL provides more support for Markov decision. Although RL may be more suitable to the control of NSSA, the curse of dimensionality prevents RL from being directly introduced into the scenario with continuous states. In this section, we present a Historical Situation based Q-value RL (HS-QRL) in order to solve the issue of cognitive control in NSSA.

Take a nonlinear dynamic control system based on RL into consideration (Chen et al., 2013),

$$\dot{s}(t) = f(s(t), a(t)) \tag{21}$$

where $s \in S \subset R^n$ represents the state and $a \in A \subset R^m$ denotes the action in RL. The instant reward can be described as

$$r = r(s(t), a(t)) \tag{22}$$

The goal of control is to search a map (policy) π in Equation (23) and meet the requirements that the cumulative reward is maximized and the cost is reduced at the same time.

$$a(t) = \pi(s(t)) \tag{23}$$

Then, a continuous integral function $V^{\pi}(S)$ is obtained,

$$V^{\pi}(s(t)) = \int_t^{\infty} e^{-(y-t)/\tau} r(s(y), a(y)) dy \tag{24}$$

where τ is a time constant, $r(s(y), a(y))$ represents the continuous integrable reward function and $s(y)$ $(t \le y \le \infty)$ is a state function that satisfies Equation (21) and (23). The optimal value function V^* of optimal policy π^* can be defined as follows:

$$V^*(s(t)) = \max_{a[t,\infty)} [\int_t^{\infty} e^{-(y-t)/\tau} r(s(y), a(y)) dy] \tag{25}$$

where $a[t, \infty)$ denotes the actions in $t \le y \le \infty$. If $r(s(y), a(y))$ is non-integrable in the whole interval but it is piecewise integrable, we can transform Equation (25) to a distribution integral according to the additive property.

$$\begin{aligned} V^*(s(t)) = \max_{a[t,\infty)} [&\int_t^{t_1} e^{-(y-t)/\tau} r(s(y), a(y)) dy + \\ &\int_{t_1}^{t_2} e^{-(y-t)/\tau} r(s(y), a(y)) dy + \cdots + \\ &\int_{t_n}^{\infty} e^{-(y-t)/\tau} r(s(y), a(y)) dy] \end{aligned} \tag{26}$$

Based on the optimal value function, a newly designed or an existing policy may be chosen to actualize the regulation of NSSA. We utilize the improved Q-value RL as our cognitive control method and define the related functions as follows in order to achieve the better control performance in NSSA.

According to the formal description, the core of RL is the reward function and the value function. We hope to design an online control mechanism and the Q-value function based on Sarsa algorithm is a reasonable choice.

$$\begin{aligned} Q_{t+1}(s_t, a_t) = &Q_t(s_t, a_t) + \alpha(r(s(t), a(t)) + \\ &\gamma Q_t(s_{t+1}, a_{t+1}) - Q_t(s_t, a_t)) \end{aligned} \tag{27}$$

where $\alpha \in [0, 1]$ and $\gamma \in [0, 1]$ are the learning rate and the discount factor respectively. $Q_t(s_t, a_t)$ is the Q-value in time t with initial value 0. $r(s(t), a(t))$ is the reward function which can be defined using Equation (28).

$$r(s(t), a(t)) = V_{SS}^{Bef} - V_{SS}^{Aft} \tag{28}$$

where V_{SS} is the Security Situation (SS) which may be SSS, HSS or NSS achieved through Equation (16), (17) or (19). The reward function represents the difference between SS before the control is executed (V_{SS}^{Bef}) and SS after the control is carried out (V_{SS}^{Aft}). Then, the optimal policy π can be adopted according to Equation (29) through maximizing the Q-value function.

$$\pi_{t+1}^*(s) = arg \max_a Q_{t+1}(s_t, a_t) \tag{29}$$

If we utilize Equation (29) as the principle of policy choosing, the most severe policy will always be the optimal one for the reason that the most severe policy may desert more data packets and shut down more ports, which causes the greater

reward value according to Equation (28). As a tradeoff, the policy with minimal reward in all feasible policies is chosen in the condition that V_{SS}^{Aft} is less than the control threshold Ω which is considered as a flag to determine whether the regulation is needed or not. Namely, Equation (29) must meet the requirements of Equation (30).

$$\begin{cases} V_{SS}^{Aft} < \Omega \\ a = \min\limits_{a}(r_1, r_2, \cdots, r_m) \end{cases} \tag{30}$$

where m is the number of possible policies and a is the executed action when a policy is adopted. Under the constraint of Equation (30), the more moderate control policy is the favorite one which results in the minimal impact on data packets of normal activity.

In a certain time window, NSSA can achieve a SS using Equation (16), (17) or (19). Different SS values denote different states and the distinctive response policies need to be adopted accordingly. We can store a SS (also called state in RL) with its corresponding policy in data base and a state-policy pair is formed for the future response if the awareness component perceives the same SS at successive time intervals. However, NSSA will produce innumerable SSes as the time goes on and the states explosion will arise unavoidably. This is the main reason why Q-value RL is not suitable when it is directly applied into a nonlinear dynamic system with continuous states and actions. As a reasonable solution, we present a term called ε-state ($\varepsilon \geq 0$) and two or more SSes may be considered as one state if their difference is no more than ε.

Definition 5. Let s_i and s_j ($s_i, s_j \in S$) be two arbitrary SSes (states), they are defined as ε-state and regarded as the same state if and only if

$$|s_1 - s_2| \leq \varepsilon \tag{31}$$

6.2. Cognitive control mechanism

In our cognitive control mechanism, we utilize the historical state-policy pair as experience data and present the HS-QRL cognitive control method. In the process of cognitive control, we need to coordinate many elements such as resources, algorithms and parameters. These elements stay in components of the FADC circle and also need to be combined with historical state-policy pair in order to actualize the cognitive awareness-control. The HS-QRL cognitive control mechanism can be depicted in Fig. 9.

Let the situation function, $\varphi(t_k)$, be a two-dimension function or a piecewise function in a time window t_k. We evaluate the SS ($\varphi(t_{cur}) = s$) in the current time window and search for the precursor state-policy pair which has the same SS with s in the state-policy data base, $P_{SP} = \{s_1 \rightarrow p_1, s_2 \rightarrow p_2, \cdots, s_n \rightarrow p_n\}$. If there is a state-policy pair whose SS,s_k ($1 \leq k \leq n$), is a ε-state with s, the policy p_k is chosen and the corresponding action is executed. Otherwise, the reward values and Q-values of all feasible actions are calculated using Equation (27) and (28). The action with maximal Q-value under the constraint of Equation (30) is regarded as the optimal one and a new state-policy pair is stored into P_{SP}. The proposed HS-QRL control method of NSSA is shown in Algorithm 1.

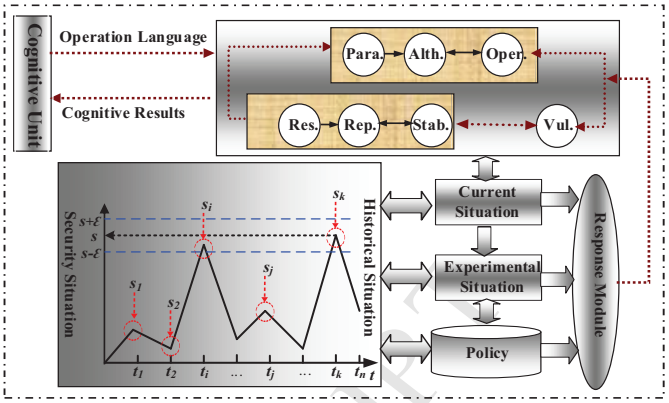

Figure 9: The HS-QRL cognitive control mechanism

In Algorithm 1, we configure a threshold Ω which determines whether the control policy needs to be executed or not. If the situation value is higher than the threshold, the regulation will be adopted. Otherwise, the regulation will be ignored. The same approach can be adopted to regulate the SSS and the HSS. The difference is that we should utilize different reward functions $r(s(t), a(t)) = V_{S_i}^{Bef} - V_{S_i}^{Aft}$ and $r(s(t), a(t)) = V_{H_l}^{Bef} - V_{H_l}^{Aft}$ respectively compared with the regulation of NSS. Algorithm 1 can be regarded as a Markov decision process with continuous state and action which has been proved to be convergent (Wei et al., 2017). This guarantees that the HS-QRL control algorithm is bounded and we are capable of obtaining an optimal policy to carry out the corresponding action or actions in a finite time complexity. The complexity of Algorithm 1 mainly comes from the searching of situation-policy pair and the calculating of reward value and Q-value. We take the worst case into consideration. A new attack pattern emerges and a state-policy pair is not found in historical data base. Assumed that the number of state-policy pairs is n in P_{SP} ($|P_{SP}| = n$), then the algorithm need to search n times in historical data base. In addition, the algorithm executes all feasible actions ($|actions| = m$) one by one (line 7 to line 9) in order to calculate reward value and Q-value. Therefore, the searching complexity of our algorithm is $O(n)$ and the computation complexity is $O(2m)$ in the worst condition. The searching complexity may be decreased if we sort the state-policy pairs in P_{SP}. Take Binsearch as an instance, the searching complexity can be promoted to $O(logn)$.

Through the above mentioned treatment, NSSA possesses the abilities of decision and execution without the manual intervention. Along with the fusion and awareness component in the FADC cognitive circle, the feedback structure is formed, which can not only perceive the security situation but also execute the control policy autonomously.

7. Simulation experiments and analysis

7.1. Simulation experiment setup

We design an experimental network as shown in Fig.10 and deploy Netflow, Snort and Snmp sensors in different layers of

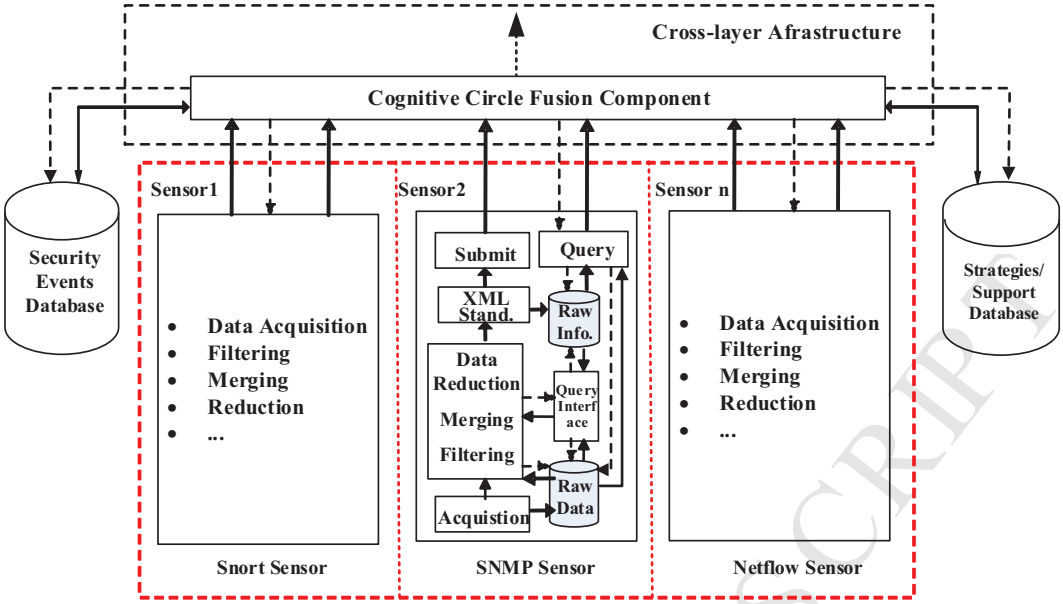

Figure 11: SNMP sensor design structure and the relations between sensors and cognitive circle

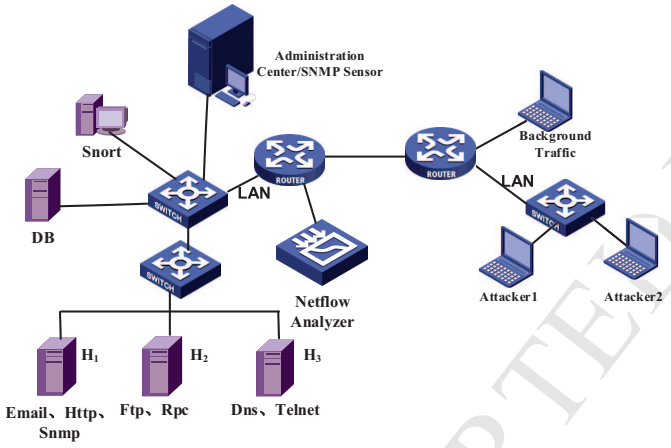

Figure 10: Experimental topology

our model. We utilize XML to treat the format and the transmission of heterogeneous sensor data. The relations between three sensors and the cross-layer cognitive circle are demonstrated in Fig.11 including the detailed design structure of Snmp sensor.

The training set and the test set are 20% and 9% of the DARPA 10% dataset respectively and we extract the number of different attacks in proportion to the traffic in a real network in order to simulate the Internet to a large extent. Using the detection results of the three sensors, we initialize the CPSO-DS fusion engine with iterative training in which the population size is 55 and search the optimal weights in $[0, 1]$. The BBAs of three sensors are obtained using expectation deviation, port changing rate of Netflow and in-out ratio of the traffic. We list all the data for subsequent experiments in Table 2.

Table 3: Performance comparison with other D-S fusion

Parameters	TDS	EDS	TPDS	CPSO-DS
DR	73.33%	82.60%	86.67%	88.11%
FDR	9.86%	5.80%	5.63%	5.06%

7.2. *Fusion performance*

We replayed the testing set and utilized the CPSO-DS to fuse the alerts provided by Snort, Netflow and Snmp sensors. We compare our fusion method with the traditional D-S (TDS) fusion, empirical weight D-S (EDS) fusion and two data source PSO-DS (TPDS) fusion (Liu et al., 2012) in the Detection Rate (DR) and False Detection Rate (FDR). The experiment results shown in Table 3 indicate that CPSO-DS fusion is superior to other fusion methods in DR and FDR. As a decision-level fusion algorithm, CPSO-DS has the better ability in dealing with the heterogeneous and multiple dimension inputs than data-level and feature-level fusions. Compared with two sensors fusion, adding sensors may provide higher DR and lower FDR.However, more sensors do not promote the DR and FDR to a great extent. This proves that more sensors do not necessarily produce a better result. We should not simply improve the fusion ability by increasing the number of sensors. The fusion performance is not only related to the number of sensors but also restricted by the accuracy and property of a single sensor.

7.3. *Hierarchical quantification awareness*

7.3.1. *Service Security Situation*

According to the outputs of CPSO-DS fusion engine, we follow the steps of factor extraction, factor quantification and hierarchical awareness to evaluate the network threat. The situation factors are attack intensity, attack type, threat gene and

Table 2: Initial experimental data

Attack Type	Training Set	Testing Set	Netflow BBA	Snort BBA	Snmp BBA	$e_{Netflow}$	e_{Snort}	e_{Snmp}	Threat Grade	Threat Gene
R2L	226	98	0.098	0.194	0.347	0.26	0.71	0.67	1	0.726
U2R	31	11	0.146	0.203	0.261	0.23	0.91	0.69	1	0.726
DoS	78291	33665	0.283	0.189	0.167	0.93	0.34	0.22	2	0.611
Probe	822	354	0.367	0.288	0.188	0.88	0.60	0.41	3	0.389
New	*	*	0.106	0.126	0.037	0.58	0.71	0.43	0	1

Algorithm 1 HS-QRL control algorithm

Input: Time window t_k, control threshold Ω
Output: Optimal policy $\pi^*_{t_k}$ and action(s)

Calculate the NSS in time window t_k using Equation (19), $\varphi_{t_k} = V^{t_k}_{NS} = \sum_{i=1}^{p}(V_{H_i} g_{H_i})$;
if $\varphi_{t_k} \geq \Omega$ **then**
  Use φ_{t_k} as an index to search for ε-state situation-policy pair in P_{SP};
  if $s_j \in P_{SP}$ is a ε-state with φ_{t_k} **then**
    Choose p_j as the optimal control policy $\pi^*_{t_k}$;
  else
    for $i = 1$ to $|actions|$ **do**
      Calculate reward value $r(\varphi(t_k), a_i(t_k))$ and Q-value $Q_(t_k)$ for each action a_i;
    end for
    Choose an optimal policy according to $\pi^*_{t_k}(\varphi_{t_k}) = arg\max_{a_i} Q_{t_k}(\varphi_{t_k-1}, a_{t_k-1})$ under the constraint of Equation (30);
    Store φ_{t_k} with π_* (state-policy pair $(s_{t_k} \rightarrow p_{t_k})$) to P_{SP};
  end if
end if
return π_* and related action (or actions);

so on. The factor quantifications of the former two factors are relative easy. For example, we can obtain the attack intensity through counting the outputs of CPSO-DS in a time window. The attack types are R2L, U2R, DoS, Probe and unknown attack according to the standard of DARPA. We quantify the threat genes using Equation (8) and show them in Table 2 where the threat type is $n = 5$ and the threat grade is $g = 4$. The simulation network ran for a week and the testing set was replayed by the attackers. We obtained the SSS by Equation (16) and set two hours as the size of the time window. Fig.12 is the SSS of Email, Http and Snmp on host H_1. Http and Snmp services suffered from a serious attack on Sunday and the threat situation of Http also needed close attention on the afternoon and evening of Wednesday. The service of Snmp was in a serious threat situation at the midnight of Saturday. But the situation of the Email service was relatively stationary at the monitoring time. Form Fig.12, we find that there is a disciplinarian which gradually becomes severe before a very serious threat appears. According to this, the administrators should take action in advance when a noteworthy security situation arises. We only demonstrate the

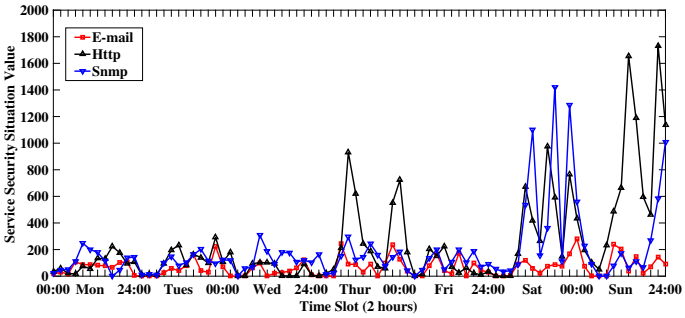

Figure 12: Service security situation of host $H1$ in a week where threat type $n = 5$ and threat grade $g = 4$

SSS of H_1 and omit other service security situation views of H_2 and H_3 that may be generated using the same method as H_1.

7.3.2. Host security situation

From the perspective of H_1, the importance degree of Email, Http and Snmp, t_{S_i} $(1 \leq i \leq 3)$, can be classified into three grades, medium(t_{s_1})), high(t_{s_2}) and low(t_{s_3}) respectively. The quantification values of $t_{S_i}(1 \leq i \leq 3)$ can be calculated by Equation (8) where $g = n = 3$ and formalized by Equation (18) ($f_{s_1} = 0.33$, $f_{s_2} = 0.50$ and $f_{s_3} = 0.17$). According to above-mentioned parameters and SSS, the values of HSS were achieved using Equation (17). As for hosts H_2 and H_3, the same method could be adopted to obtain respective SS and we show them in Fig.13. These three hosts encountered very serious attacks at the weekend. Besides, H_1 was subject to a notable security situation on the afternoon and evening of Wednesday. The view of HSS reflects the activity regularity that more serious attacks usually occur in the afternoon or the evening. In these time quantum, the administrators need to pay more attention to the monitored network and take the response measures in advance before the most severe threat appears.

7.3.3. Network security situation

The network security situation needs to determine the weights of the hosts that are more complex than the services. These weights are closely related to the asset value (V_h), the pivotal degree to whole network (C_s), the access frequency (A_f) and the confidential level (D_c). We arrange the grades of these factors in Table 4 and quantify them using Equation (8). The weight of a host is a composite one and we set the weight of the i-th host as q_{H_i} where $q_{H_i} = k_V V_{h_i} + k_C C_{S_i} + k_A A_{f_i} + k_D D_{c_i}$ and

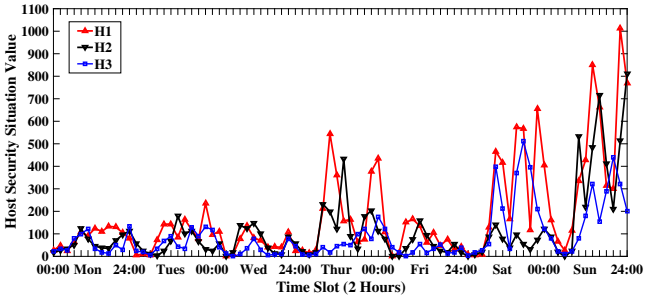

Figure 13: Host security situation of H_1, H_2 and H_3

Table 4: Host factor grades

Host	V_h	C_s	A_f	D_c
H_1	High	Medium	Medium	High
H_2	Medium	Low	Medium	Medium
H_3	Medium	Low	Low	Low

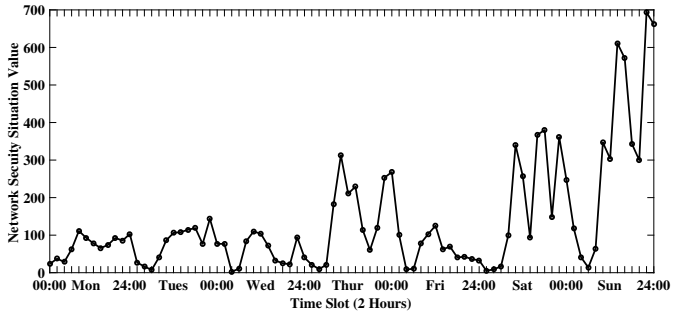

Figure 14: Network security situation

$k_V = 0.20, k_C = 0.30, k_A = k_D = 0.25$. Based on HSS and Table 4, we utilized Equation (19) to obtain the view of NSS in Fig.14 which illustrated the situation evolution in a week. Although the security situations did not reach a serious degree and the network maintenance was not necessary on Thursday, the threat evolution deserved our attention. This may be caused by the attack attempts. However, the very serious situation appeared and the proper measures should be taken on Sunday in order to avoid the poor performance which may result in the failure of network even crash.

7.3.4. Self-adaptation ability of hierarchical quantification

The hierarchical fusion awareness method can evaluate the security situations of service level, host level and network level. Besides, the method has favorable environmental suitability which reflects the cognitive ability to a certain degree. From the perspective of fusion, CPSO-DS multi-source fusion algorithm does not need complex repeated learning and we only train CPSO-DS with the new samples when the situation awareness system is migrated to a new network. From the viewpoint of threat gene, our generation method has minor requirements for expert knowledge and we can obtain the threat gene automatically by providing a new threat grade. We demonstrate the self-adaptation ability of HSS instead. Let host H_1 be deployed to a network that has the different service importance as shown in Table 5.

Table 5: Host threat grades and threat fenes of new network

Service	Threat Degree	Threat Grade	New Threat Gene
E-mail	High	1	0.50
Snmp	Medium	2	0.33
Http	Low	3	0.17

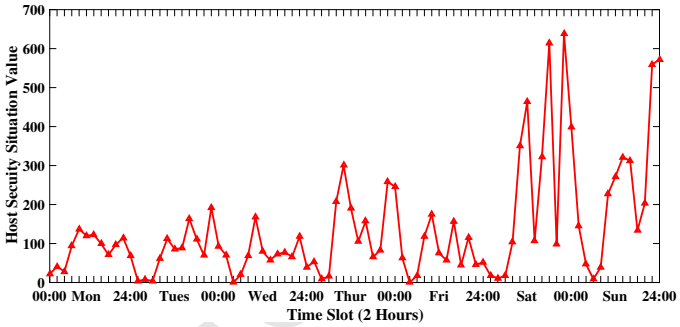

Figure 15: Host security situation of H_1 after self-adaptation

We calculated the threat genes using Equation (8) without complex analysis among all the network components and situation factors. We generated the situation evaluation views of three hosts in Fig.15 according to Table 5. We only demonstrate the HSS of H_1 using the new threat genes. The figure shows the same situation evolution trend as Fig.13. However, it demonstrates a different threat situation in the new network environment even under the same attacks and SSSes. Compared with the awareness methods proposed in (Hu et al., 2007; Zhang et al., 2012; Dapoigny et al., 2013), we do not need to define the complex relations between attacks and services, the new threat genes and the HSS of new network environment can be obtained automatically using Equation (8) and Equation (17).

7.4. Cognitive control

In the current experiment, we design a simple response policy to filter the traffic based on source address, destination address, source port and destination port as demonstrated in Table 6. During the control process, the components of FADC cognitive circle call the fusion component and awareness component to fuse the alerts and perceive the new security situation. Taking the ability of network tolerance into consideration, we set a situation threshold $\Omega = 150$ in Equation (30) and $\varepsilon = 30$ in Equation (31). The cognitive unit will not make any operation if the situation values are less than the threshold and the aim is to avoid frequent regulation and decrease the appearance probability of control jitter. We utilized the same attack pattern in Table 2 to validate the effectiveness of our cognitive mechanism. In this section, we only demonstrate the HSS view of H_1 after autonomous control and show it in Fig.16.

Fig.16 denotes that the threat of H_1 decreases to a great extent without artificial participation through the autonomous

Table 6: Policies and actions

Policy	Policy Level	Action
P_1	Low	a_1=Null
P_2	Moderate	a_2=Close a port of hosts
P_3	Medium	a_3=Desert attack packets with specified source IP address
P_4	Medium	a_4=Desert attack packets with specified destination IP address
P_5	Severe	a_6=Desert all packets
...	...	...

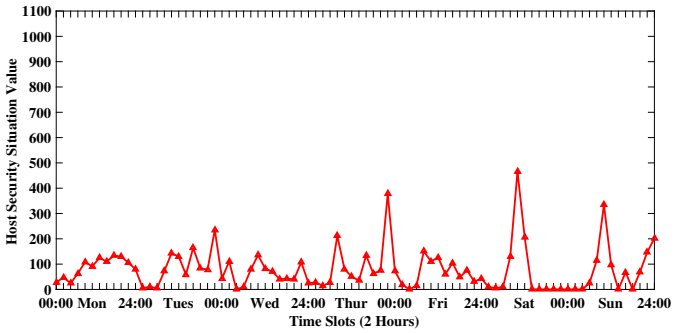

Figure 16: Host security situation of H_1 after cognitive control based on HS-QRL

cognitive control compared with HSS in Fig.13. HSQ-RL demonstrates the favorable performance in the situation of continuous threat (on Thursday and Sunday). However, the performance in certain short slots should be improved (on Thursday). This is related to the hysteresis of control, the size of time window and the control policy. Furthermore, the least severe policy is also an important reason. This denotes that we should set a smaller time window and design more complex policies due to the random nature of attacks. However, the advantages are remarkable and they prove that HS-QRL is a good tradeoff between normal and abnormal activities. (i) HS-QRL decreases the influence to the normal activity. As it is should be, the severe policy can decrease the threat situation to a lower degree even zero, but many data packets of normal activity will also be deserted in a practical system. (ii) HS-QRL has the resilience to forged IP attack. In the process of attacking, the attacker may utilize different IP addresses to launch abnormal activities. In this condition, we cannot eliminate the threat situation under the threshold Ω through executing policy P_3. HS-QRL will choose the policy P_4 to decrease the threat value and avoid applying the more severe polices such as P_5 and P_6 to defend against the forged IP address attack. (iii) HS-QRL can decrease the times of control and improve the control jitter. Table 7 shows the distribution of policies in our experiment and this guarantees that the control actions are executed as few as possible (65.5% P_1 Null action) and the optimal policy is prone to be applied between the moderate level and the medium level (P_2 to P_4). Through the analysis of HSQ-RL cognitive control, we know that our control mechanism is feasible, but more reasonable improvements still need to be studied. We can also apply HS-QRL into the

Table 7: Policy distribution

Policy	Policy Level	Execution times	Percentage
P_1	Low	55	65.5%
P_2	Moderate	16	19.0%
P_3	Medium	10	11.9%
P_4	Medium	3	3.6%
P_5	Severe	0	0%

situation regulation of SSS and NSS, which will be discussed in our future study.

In the process of validation of our awareness-control mechanism, we can set a different time window and show the security situation views with the intervals of hours, minutes even seconds from Fig.12 to Fig.16 to realize the finer granularity awareness. NSSA not only transforms the discrete alerts to continuous situation evolution view instead of reporting the massive alerts to the administrators, but also undermines the false alerts to the statistic characteristic. This provides a novel threat presentation. We can obtain the changing trend and the law of the network abnormality from the current and historical situations, which makes the automatic response possible.

We discuss the situation awareness-control mechanism based on fusion which has a prominent feature in the aspects of threat gene obtaining, quantification awareness and cognitive control as shown in Table 8. In comparison with those typical mechanisms discussed in the current researches, CACM is suitable for the heterogeneous system and broadens the application prospect of the NSSA in the current and next generation networks. Meanwhile, the obtaining of the threat gene based on weighted coefficient possesses a better adaptability and the complex association analysis is not needed compared with AHP. Furthermore, our formal description of the hierarchical awareness method standardizes the process of quantification awareness and defines the relations among the situation factors. As a result, we can express the situation knowledge and its evolution law in a different target field. In addition, the HS-QRL control mechanism may realize the autonomous and unattended regulation. The CACM and the proposed methods form a close-loop feedback FADC cognitive circle which can perceive the threat situation and regulate the system state autonomously. As a result, the purpose of managing technology by technology is achieved.

8. Conclusion and future work

NSSA has become a novel technology in defending the networks from being compromised. Through analyzing the model, the fusion algorithm, the awareness method and the cognitive computing, we come to the conclusion that the research on NSSA is pushing ahead form awareness to awareness-control. In the framework of CACM, we proposed our heterogeneous multi-source fusion algorithm, hierarchical awareness method and HS-QRL mechanism to deal with the problem of cognitive awareness-control. We examined our model and validated the effectiveness and feasibility of the proposed methods through

Table 8: Comparison with typical researches

Related work	Data Source	Fusion Algorithm	Evaluation Pattern	Threat Gene	Adaptability	Control Mechanism
Bass (1999)	IDS/Sniffer	–	Qualitative	–	–	–
Hu et al.(2007)	IDS	–	Hierarchy	AHP	Weaker	–
Wei et al.(2009)	Vulnerability/ Log	D-S	Node level	Subjective experience	Weak	–
Erbachera et al.(2010)	Raw attack/log	–	Visualization	–	–	Inter-external response
Zhang et al.(2011)	Vulnerability/ IDS/Firewall	–	Game analysis	Threat propagation network	Weaker	Manual
Feng et al.(2011)	Evidence case	D-S	Hierarchy	Fuzzy weight	Weak	–
Zhang et al.(2012)	Numerical example	D-S	Hierarchy	AHP	Weak	–
Skopik et al.(2013)	Link/Traffic/ Access Monitor	–	Hierarchy	–	–	Response cycle
Li et al.(2015)	–	–	Hierarchy	Dynamic trust	Weaker	Trust feedback
Li et al.(2016)	IDS	–	Hierarchy	Hidden Markov	Weaker	Genetic algorithm
Xu et al. (2017)	Vulnerability/ attack netflow	–	Ontology model	–	Weaker	–
Wang et al.(2018)	IDS/Firewall	D-S	Hierarchy	AHP	Weak	–
Ours	IDS/Traffic/ SNMP	PSO-DS	Formalization	Weight coefficient	Stronger	Autonomous

a series of simulation experiments. The results show that the model and the methods can perceive the evolution trends of the security situation and possess the favorable cognitive ability by constructing a closed feedback circle. This study has achieved the purpose of autonomous awareness-control which can be used for promoting the security level and providing a new approach to resisting against the attacks aiming at the monitored network.

This paper only proposed a series of preliminary solutions to certain critical problems in the study of NSSA. We are pursuing the formal validation of CACM model and the states space of FADC cognitive circle. Research on the fusion algorithm with better real-time nature and accuracy should be addressed, which may provide a more solid support for the fusion, awareness and control. Finally, the complex regulation policy and situation forecast should be discussed in subsequent studies in order to improve the problem of regulation hysteresis and construct a practical NSSA system that supports the current network and the next generation security system.

References

Ali, H., Khan, F., 2013. Attributed multi-objective comprehensive learning particle swarm optimization for optimal security of networks. Appl. Soft Comput. 13(9), 3903-3921.

Akhtar, M., Ghaffar, R., Rashid, I., 2016. A q learning and fuzzy q Learning approach for optimization of interference constellations in femto-macro cellular architecture in downlink. Wireless Pers. Commun. 88(4), 797-817.

Angelini, M., Santucci, G., 2017. Cyber situational awareness: from geographical alerts to high-level management. J. of Visual. 20, 1-7.

Anjaria, K., Mishra, A., 2018. Relating winener's cybernetics aspects and a situation awareness model implementation for information security risk management. Kybernetes. 47(1), 58-79.

Azimirad, E., Haddadnia, J., Izadipour, A., 2015. A comprehensive review of the multi-sensor data fusion architectures. J. of Theor. and Appl. Inform. Technol. 71(1), 33-42.

Bass, T., 1999. Multi-sensor data fusion for next generation distributed intrusion detection systems. In: the National Symposium on Sensor and Data Fusion. pp. 24-27.

Bhasin, S., Sharma, N., Patre, P., 2011. Asymptotic tracking by a reinforcement learning-based adaptive critic controller. J. of Control Theory and Appl. 9(3), 400-409.

Cao, B., Zhao, J., Lv, Z. and et al., 2018. Deployment optimization for 3D industrial wireless sensor networks based on particle swarm optimizers with distributed parallelism. J. of Netw. and Comput. Appl. 103, 225-238.

Cattaneo, M., 2011. Belief functions combination without the assumption of independence of the information sources. Int. J. of Approx. Reason. 52, 299-315.

Chen, J., 2002. Multi-sensor administration and information fusion. Northwester Polytechnical University Press, Xi'An, China. pp. 49-55.

Chen, X., Liu, F., 2013. Optimal control of a class of nonlinear dynamic systems based on reinforcement learning. Control and Decision. 28(12), 1889-1893.

Chen, Y., Argentinis, J. E., Weber, G., 2016. IBM Watson: how cognitive computing can be applied to big data challenges in life sciences research. Clinical Therapeutics. 38(4), 688-701.

Dapoigny, R., Barlatier, P., 2013. Formal foundations for situation awareness based on dependent type theory. Inform. Fusion. 14(1), 87-107.

Endsley, M., 1999. Design and evaluation for situation awareness enhancement. In: the 32nd Human Factors Society Annual Meeting, pp. 97-101.

Erbachera, R., Frinckeb, D., Wong, P., Moodya, S., Finkb, G., 2010. A multi-phase network situational awareness cognitive task analysis. Inform. Visual. 9(3), 204-219.

Evesti, A., Frantti, T., 2015. Situational awareness for security adaptation in industrial control Systems. In: ICUFN 2015 - 7th IEEE International Conference on Ubiquitous and Future Networks, pp. 1-6.

Feng, N., Li, M., 2011. An information systems security assessment model under uncertain environment. Appl. Soft. Comput. 11, 4332-4340.

Fortuna, C., Mohorcic, M., 2009. Trends in the development of communication networks: cognitive networks. Comput. Netw. 53(9), 1354-1376.

Franke, U., Brynielsson, J., 2014. Cyber situational awareness - a

systematic review of the literature. Comput. & Secur. 46, 18-31.
Fu, C., Yang, S., 2014. Conjunctive combination of belief functions from dependent sources using positive and negative weight functions. Expert Syst. with Appl. 41, 1964-1972.
Gomez, I., Marojevic, V., Gelonch, A., 2011. ALOE: an open-source sdr execution environment with cognitive computing resource management capabilities. IEEE Commun. Mag. 49(9), 76-83.
Guo, K., Li, W., 2011. Combination rule of D-S evidence theory based on the strategy of cross merging between evidences. Expert Syst. with Appl. 38, 13360-13366.
Gupta, M., 2011. On fuzzy logic and cognitive computing: some perspectives. Scientia Iranica. 18(3), 590-592.
Hao, L., Healey, C., Hutchinson, S., 2015. Ensemble visualization for cyber situation awareness of network security data. In: VizSec 2015-IEEE Symposium on Visualization for Cyber Security, pp. 1-8.
Hong, J. B., Dong, S. K, 2016. Towards scalable security analysis using multi-layered security models. J. of Netw. and Comput. Appl. 75, 156-168.
Hu, W., Li, J., Jiang, X., 2007. A hierarchical algorithm for cyberspace situational awareness based on analytic hierarchy process. High Tech. Lett. 13(3), 291-296.
Kalloniatis, A., Ali, R., Neville, T., et al., 2017. The situation awareness weighted network (sawn) model and method: theory and application. Appl. Ergon. 61, 178-196.
Khaleghi, B., Khamis, A., Karray, F., 2013. Multisensor data fusion: a review of the state-of-the-art. Inform. Fusion. 14(1), 28-44.
Kim, Y., Zhang, Y., Li, P, 2015. A reconfigurable digital neuromorphic processor with memristive synaptic crossbar for cognitive computing. Acm J. on Emerg. Tech. in Comput. Syst. 11(4), 1-25.
Kliks, A., Triantafyllopoulou, D., Nardis, L., et al., 2017. Cross-layer analysis in cognitive radio context identification and decision making aspects. IEEE Trans. on Cogn. Commun. & Netw. 1(4), 450-463.
Li, X., Desert, J., Smarandache, F., Huang, X., 2011. Evidence supporting measure of similarity for reducing the complexity in information fusion. Inform. Sci. 181, 1818-1835.
Li, F., Nie, Y., Zhu, J., Zhang, H., Liu, F., 2015. A decision-aided situation awareness mechanism based on multiscale dynamic trust. Int. J. of Distrib. Sens. Netw. 11(10), 1-14.
Li, X., Zhao, H., 2016. Network security situation assessment based on HMM-MPGA. In: ICIM 2016-International Conference on Information Management, pp. 57-63.
Li, J., Huang, C., Qi, J., et al., 2017. Three-way cognitive concept learning via multi-granularity. Inform. Sci. 378(1), 244-263.
Liu, X., Wang, H., Yu, J., Cao, B., Gao, Z., 2012. Network security situation awareness model based on multi-source fusion. Adv. Sci. Lett. 5(2), 775-779.
Nscpoles, G., Grau, E., Papageorgiou, E., et al., 2016. Rough cognitive networks. Knowledge-based Syst. 91(C), 46-61.
Ogiela, M., You, I., 2013. Cognitive and secure computing in information management. Int. J. of Inform. Manage. 33(2), 243-244.
Rolim, C., Rossetto, A., Leithardt, V., et al., 2016. Situation awareness and computational intelligence in opportunistic networks to support the data transmission of urban sensing applications. Comput. Netw. 111, 55-70.
Saganowski, L., Andrysiak, T., Kozik, R., et al., 2016. DWT-based anomaly detection method for cyber security of wireless sensor networks. Secur. & Commun. Netw. 9(15), 2911-2922.
Sami, M., Noordin, N., Khabazian, M., 2016. A TDMA-based cooperative mac protocol for cognitive networks with opportunistic energy harvesting. IEEE Commun. Lett. 20(4), 808-811.
Schaal, S., Atkeson, C., 2010. Learning control in robotics. IEEE Robot. and Automat. Mag. 17(2), 20-29.
Shakibian, H., Charkari, N. M, 2014. In-cluster vector evaluated particle swarm optimization for distributed regression in WSNs. J. of Netw. and Comput. Appl,. 42(4), 80-91.
Shiravi, H., Shiravi, A., Ghorbani, A., 2012. A survey of visualization systems for network security. IEEE Trans. on Visual. and Comput. Gr. 18(8), 1313-1329.
Skopik, F., Ma, Z., Smith, P., Bleier, T., 2013. Designing a cyber attack information system for national situational awareness.In: Future Security, pp. 277-288.
Sunilkumar, G., Thriveni, J., Venugopal, K., et al., 2015. A perspective to adopt continuous dynamic cognition for malicious node detection in heterogeneous networks. Procedia Comput. Sci. 46, 997-1004.
Sun, Z., Liu, Y., Tao, L., 2018. Attack localization task allocation in wireless sensor networks based on multi-objective binary particle swarm optimization. J. of Netw. and Comput. Appl. 112, 29-40.
Tefek, U., Lim, T., 2016. Interference management through exclusion zones in two-tier cognitive networks. IEEE Trans. on Wireless Commun. 15(3), 2292-2302.
Teixeira, A., Shames, I., Sandberg, H., et al., 2017. Distributed fault detection and isolation resilient to network model uncertainties. IEEE Trans. on Cybern. 44(11), 2024-2037.
Tran, N., Hong, C., Lee, S., 2013. Cross-layer design of congestion control and power control in fast-fading wireless networks. IEEE Trans. on Parallel and Distr. Syst. 24(2), 260-274.
Tsekouras, G., 2013. A simple and effective algorithm for implementing particle swarm optimizati on in rbf network's design using input-output fuzzy clustering. Neurocomputing. 108, 36-44.
Wang, Y., 2010. Cognitive computing and world wide wisdom (www+). In: ICCI 2010 - the 9th International Conference on Cognitive Informatics, pp. 4-5.
Wang, K., Chai, T., Wong, W., 2016. Routing, power control and rate adaptation: a q-learning-based cross-layer design. Comput. Netw. 102, 20-37.
Wang, H., Chen, Z., Feng, X., Di, X., Liu, D., Zhao, J., Sui, X., 2018. Research on network security situation assessment and quantification method based on analytic hierarchy process. Wireless Pers. Commun. 102, 1401-1420.
Wei, Y., Lian, Y., Feng, D., 2009. A network security situational awareness model based on information fusion. J. of Comput. Res. and Dev. 46(3), 353-362.
Wei, Q., Lewis, L. F., Sun, Q., Yan, P., Song, R., 2017. Discrete-time deterministic q-learning: a novel convergence analysis. IEEE Trans. on Cybern. 47(5), 1224-1237.
Xu, G., Cao, Y., Ren, Y., Li, X., Feng, Z. 2017. Network security situation awareness based on semantic ontology and user-defined rules for internet of things. IEEE Access. 5(99), 21046-21056.
Zhang, Y., Tan, X., Cui, X., et al., 2011. Network security situation awareness approach based on markov game model. J. of Softw. 22(3), 495-508.
Zhang, Y., Deng, X., Wei, D., Deng, Y., 2012. Assessment of e-commerce security using ahp and evidential reasoning. Expert Syst. with Appl. 39, 3611-3623.

Author Biography

Xiaowu Liu received the MS and PhD degrees in computer science from Harbin Engineering University in 2005 and 2009, respectively. He is currently associate professor at the school of computer science and engineering in Qufu Normal University. His research interests are focused on network security, wireless sensor network and data fusion.

Jiguo Yu received his Ph.D. degree in School of mathematics from Shandong University in 2004. He became a full professor in the School of Computer Science, Qufu Normal University, Shandong, China in 2007. Currently he is a full professor in Qilu University of Technology (Shandong Academy of Sciences), Shandong Computer Science Center (National Supercomputer Center in Jinan), and a professor in School of Information Science and Engineering, Qufu Normal University. His main research interests include privacy-aware computing, wireless networking, distributed algorithms, peer-to-peer computing, and graph theory. Particularly, he is interested in designing and analyzing algorithms for many computationally hard problems in networks. He is a senior member of IEEE, a member of ACM and a senior member of the CCF (China Computer Federation).

Weifeng Lv received his Ph.D. degree in computer science from Beihang University in 1998. His current research interests include massive information system, urban cognitive computing, swarm intelligence, and smart cities. He is a professor of computer science and the dean of the School of Computer Science and Engineering, as well as the vice director of the State Key Laboratory of Software Development Environment, at Beihang University. He also serves as the Vice-President and Secretary-General of the China Software Industry Association and the director of National Engineering Research Center for Science and Technology Resources Sharing Service. He received multiple internationally renowned awards, including the second prize of the 2016 China National Science and Technology Invention Award and the first prize of the 2010 Beijing Science and Technology Award.

Dongxiao Yu received the BSc degree in 2006 from the School of Mathematics, Shandong University and the PhD degree in 2014 from the Department of Computer Science, The University of Hong Kong. He became an associate professor in the School of Computer Science and Technology, Huazhong University of Science and Technology, in 2016. He is currently a professor in the School of Computer Science and Technology, Shandong University. His research interests include wireless networks, distributed computing and graph algorithms.

Yinglong Wang received his M.S. degree in Industrial Automation from Shandong University of Technology in 1990, and Ph.D. degree in Communication and Information Systems from Shandong University in 2005. He is a Professor in Qilu University of Technology (Shandong Academy of Sciences) and Shandong Computer Science Center (National Supercomputer Center in Jinan). He has completed 20+ projects including 863 and some other important science and technology projects, won the first prize award of science and technology of Shandong Province two times and the second prize award four times. He organized the

compilation of three national technical standards. His current research interests include IoT, cloud computing and big data.

Yu Wu received his B.E and M.E. degrees in 2006 and 2009 respectively, from Department of Computer Science and Technology, Tsinghua University, China, and his Ph.D. degree in 2013 from the Department of Computer Science, the University of Hong Kong. He was a postdoctoral scholar in the School of Electrical, Computer and Energy Engineering (ECEE), ASU, from Nov 2013 to Oct 2015. Yu Wu is currently an Associate Professor in the School of Computer Science and Network Security in the Dongguan University of Technology, China. His research interests include network virtualization, internet of things and blockchain technology.