Chapter

Evaluation of Botnet Threats Based on Evidence Chain

Liu Shangdong and Ji Yimu

Abstract

The current network security faces a serious threat, which has been brought about by the large-scale proliferation of botnet, and its detection has become one of the important tasks of the existing cyberspace security. At present, although network administrators have firewalls, intrusion detection systems, intrusion prevention systems, and other technical means to achieve partial network protection, they are still confronted with severe challenges in the detection and prevention of a botnet known as a threatening attack platform. The new botnet is characterized by its large scale and multifunction. Further, it is hard to detect, and it may cause a sharp decline in the normal defense level of the protected object in a short period of time. In this chapter, we propose a method of botnet threat assessment based on evidence chain. The DS evidence theory is used for network security situational awareness. On the basis of determining the recognition framework, all possible results are considered, and each evidence is assigned a basic credibility, and the final credibility of the target is fused by using the composition rule. The experiments show that this method can work efficiently and detect the major threats in the protected network in time.

Keywords: botnet, intrusion detection, situational awareness, evidence chain, threat evaluation

1. Introduction

In recent years, with the rapid development of Internet of Things (IOT) technology, more and more devices are exposed to the Internet. These devices are complex in variety and explosive in number. This kind of interconnected environment will make the security risk increase and spread rapidly, and bring severe security problems. Among all kinds of security problems, botnet in particular brings serious harm. Botnets are made up of "zombie hosts" infected with a malicious code that infect normal devices, forming a large-scale "botnet" of IOT, once the "botnet" launches a distributed denial of service attack. This will wreak havoc on the Internet infrastructure [1].

In view of the large scale of botnet, the variety and number of botnet hosts, and the unpredictable vulnerability types, the network security protection should be considered from the overall situation. Therefore, it is very important to grasp the information of the network and to perceive the status and development trend of the network security. Network situational awareness can capture the security elements that cause the change of network situation in a large-scale network environment, and make decisions and actions by acquiring, understanding, predicting, and making decisions [1]. The concept of Situational Awareness (SA) originates from the military demand in the 1980s, and with the rise of network, it was introduced by Tim Bass into the field of network security.

SA should go through several steps, such as situation acquisition, situation understanding, situation prediction, situation visualization and so on [2, 3]. In the situation acquisition stage, there may be a lot of complex, repetitive, or even false alarm information. In addition, the existing SA methods use IDS, firewalls, virus detection and other tools data, based on time series, graph theory, Bayes, game theory and other methods, according to the network environment, the history of the attacker and the network ontology vulnerability; these are used to evaluate and predict the network security situation, without considering the emerging vulnerabilities and their SA.

To solve the above problems, this chapter proposes a botnet SA method based on DS evidence theory. Compared with other SA methods, DS evidence theory not only can solve uncertainty problems, but it also does not need prior probability and conditional probability density. Therefore, we can manually assign it initial trust based on our expertise and individual knowledge.

Botnet SA integrates all kinds of botnet security elements to evaluate the security situation of the network in real time, which provides the basis for the network security analysis, and evaluates the network security more accurately, thus minimizing risks and losses from botnet threats. Botnet security SA plays an important role in improving the ability of network monitoring, emergency response and predicting the development trend of network security.

The main contributions of this chapter are as follows:

1. we propose a method of botnet threat assessment based on evidence chain, which computes the target credibility to determine whether there is a threat in the network;

2. the evidence chain method is applied to botnet to realize the situation of network security. DS evidence theory solves the uncertainty problem of network threat.

3. the experiment is carried out using the public data set of Nanjing University of Posts and Telecommunications (NJUPT). The results show that the network security situation assessment method proposed in this chapter is reasonable and effective, and can improve the accuracy of security situation prediction.

2. Related work

There are already some approaches to network security SA: In the research of network security SA architecture, Kokkonen proposed in 2016 a network security SA architecture, which mainly includes information exchange module and emphasizes standardized information format [4]. In 2017, Eiseler proposed a network security SA architecture from the perspective of IT complexity [5]. The main idea is to abstract a layer of operation (decision) and the result of decision for decision makers from non-technical background. In the research of network security SA, in 2016, Yang et al. used SVM machine learning method for SA [6]. After being trained by classifier, the data can be used to predict the situation value. But the method has the defect that the situation is normalized and the information is not abundant enough. In 2016, KHALID et al., targeting data injection attacks, could lead to unreliability and insecurity of network physical infrastructure such as (WAMS), a wide-area monitoring system. In this chapter, a Bayesian based approximate filter (BAF) method [7] is proposed to minimize the impact of injection attack on oscillatory parameters, so as to improve the resistance of monitoring applications to data injection attacks. In 2016, in the HMM-based network security situation assessment method, Li et al. used to extract the observation values and model parameters by establishing the time period, which is an important factor affecting the real-time and accuracy of the evaluation. However, there are two problems: The results are as follows: (1) the size of the time period is given randomly by people, which cannot represent the security and real-time performance of the current network; (2) the state transition matrix and the observation symbol matrix are usually determined by experience and have strong abstractness. To solve this problem, Li et al. later trained the parameters of the HMM model by mixed multi-population genetic algorithm (MPGA) [8] to improve the reliability of the parameters and to solve the problem that the emergency situation could not be highlighted in a certain period of time. Experiments show that this method can reflect the current network security situation effectively and accurately. [9, 10] put forward the overall goal of network security SA, which is determined by scope, level, requirement and decision. The method of SA is classified from four aspects: data collection, decision making, analysis and visualization.

Through the research of network security SA, to a certain extent, the researchers give other researchers some practical methods, but these methods also have a limited scope of application. Most of the SA methods only consider the calculation of the threat situation caused by an external attack and ignore the problem of the security situation change caused by the insecurity of the system and the equipment itself. This chapter presents a method of network security SA based on evidence chain theory. DS evidence chain theory has many advantages in SA. Firstly, it does not require prior probability and conditional probability density. Secondly, sometimes the information provided by the sensor is not necessarily very accurate, and there may be a certain degree of fuzziness, and the DS evidence method can solve the uncertainty calculation problem. Finally, DS evidence theory can continuously narrow the scope of the hypothesis set by merging evidence. Its basic idea is to fuse several sub-evidences according to the Dempster formula, so as to further determine the possibility of the occurrence of certain propositions.

3. A method of network SA awareness based on evidence chain

The chain of evidence is a collection of evidence formed by two or more evidence links connected by the chain heads for a certain object of proof. Due to the complexity of the current network environment and the emergence of various network attack methods, the management requirements and the means of recording technology are different. The vulnerabilities of most network and system are scattered and independent, and the performance cannot fully reflect the real situation of the network status. It needs to combine the vulnerabilities and network status transformation together through the relevance of vulnerabilities, and to connect them according to the inherent meanings and logical relationships to form a chain structure that is mutually connected and mutually validated, which involves the chain of evidence for network situation awareness.

3.1 The components of the chain of evidence

The components of chain of evidence for audit include chain link, chain connection and chain domain. Among them, chain link refers to the single evidence that constitutes the chain of evidence for situation awareness, also known as the node evidence, which is expressed as a single physical object; chain connection is an overlapping or embedding relationship or logical reasoning relationship between the single evidences; chain domain refers to the entire information set (all evidences) that the auditing entity can understand or know when verifying a certain network activity under the existing cognitive ability and technical conditions. The scope of chain domain is determined by the network activity and the cognitive ability of the network entity, and the maximum value is all the facts required for situation awareness, and the minimum is the main facts of situation awareness.

3.2 The essence and attributes of the chain of evidence

The evidence for situation awareness is essentially the retention of information about the past network activity of the object, and the retention of such information is the record and reflection of the network activity which objectively exists. When these records and reflections do not fully capture the main facts of a network activity, it needs to be achieved by constructing a chain of evidence. Therefore, the essence of the chain of evidence for situation awareness is that different evidences of different segments or conditions of the same network activity, through the multi-component chain-dependent relationship in terms of meaning and logic, mutually confirm each other and connect with each other to jointly reveal the truth of the same economic activity. The chain of evidence for situation awareness not only has the characteristics of the adequacy and appropriateness of general audit evidence, but also has the characteristics of relevance, integrity and complexity, etc. of unique or different meanings. Among them, relevance refers to the objective connection of causal relationship, conditional relationship and space–time relationship between the evidences of each link constituting the chain of evidence. Integrity means that the evidences of each link constituting the chain of evidence have a consistent proof effect and proof direction, and together constitute a complete proof system. Complexity refers to the complex source of evidence of each link that constitutes the chain of evidence. There are some evidences from the same source, that is to say they come from the same network activity; and there are some evidences from different sources, but the contents of them are involved each other. The evidences of each link sometimes have different forms, and the evidence of entity coexists with the evidence of person. The contents of the evidences are coherent and overlapping, and there is other information unrelated to the audit findings.

3.3 Connection mode of chain of evidence

The chain of evidence can be divided into two kinds of connections, explicit and implicit, according to whether there are semantic intersections and overlapping relationships between links, such as explicit texts. Among them, explicit connection refers to the overlapping and embedding of evidences contents between adjacent business processes in the chain of evidence. Implicit connection refers to the connection relationship between evidences formed by logical reasoning. Node evidence in the chain of evidence can be divided into core evidence and auxiliary evidence according to their different proof functions in network activities. Among them, core evidence, also called direct evidence, refers to the evidence that plays a major role in proving the emergence and existence of witnessed network activities. Auxiliary evidence is the evidence supporting core evidence, including making up the quality defects of core evidence and enhancing the persuasiveness of core evidence. The composition of the chain of evidence is shown in **Figure 1**.

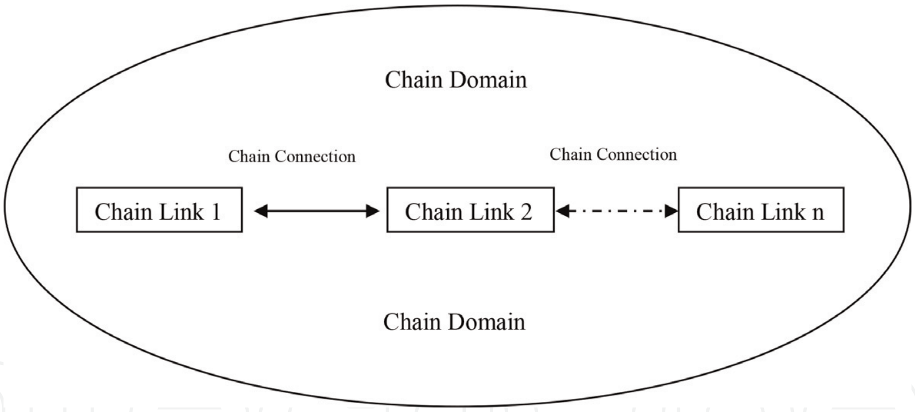


Figure 1.
Composition of chain of evidence.

3.4 Basic concepts of evidence theory

D-S evidence theory [11, 12] adopts mathematical reasoning to perform fusion calculations of inexact and incomplete information. In the D-S evidence theory fusion algorithm, the recognition framework is the framework of the whole judgment; the Basic Probability Allocation is the basis of fusion; the combinational rule is the fusion process, and the trust function and likelihood function are used to express the upper and lower limits of support strength interval of fusion conclusion to a hypothesis.

1. Recognition framework

Θ is a mutually exclusive non-empty finite set, which is known as recognition framework. It consists of N nonintersecting sets of $w_1, w_2, w_3. \dots w_N$, and there are N possible hypotheses in this recognition framework. The task of the evidence theory fusion algorithm is to estimate the trust level to each possible hypothesis.

2. Basic probability allocation

Basic Probability Allocation (BPA) is a function known as E.g. (1)m function.
$m : 2^{\Theta} \to [0, 1]$，
And it satisfied:

$$m(\Phi) = 0; \sum_{A \subseteq \Phi} m(A) = 1 \tag{1}$$

When an evidence is constructed, each possible hypothesis or hypothesis combination within the recognition framework should be assigned with a trust level between [0, 1], and the sum of the trust levels of all hypotheses or hypothetical combinations should equal 1.

3. Trust function

The fusion conclusion of D-S evidence theory expresses the support strength for any hypothesis through an interval, and the lower limit of this interval is called the trust function, and the trust function is also called the Belief Function (bel). The trust function is defined in the recognition framework Θ as is Eq. 3:

$$bel(A) = \sum_{B \subseteq A} m(B)(\forall A \subseteq \Theta) \tag{2}$$

The trust function of a hypothesis in the fusion conclusion only calculates the support strength for the hypothesis directly during the fusion calculation, and does not calculate the support strength for the combination containing the hypothesis. If a part of the support strength in the Basic Probability Allocation is assigned to an unknown domain, then the support strength of this part cannot be calculated in the trust function.

4. Likelihood function

The upper limit of the fusion conclusion interval of D-S evidence theory is called the likelihood function, and the likelihood function is also called the Plausibility Function (pl). The likelihood function is defined in the recognition framework Θ as is Eq. 3:

$$pl(A) = \sum_{B \cap A \neq \Phi} m(B) = 1 - bel\left(\overline{A}\right) \tag{3}$$

The likelihood function of a hypothesis in the fusion conclusion not only calculates the support strength for the hypothesis directly during the fusion calculation, but also calculates the support strength for the combination containing the hypothesis and the support strength allocated to an unknown domain. The fusion conclusion could directly adopt trust function, likelihood function, even the interval formed by the trust function and likelihood function to express the support strength for each possible hypothesis.

5. Dempster's combinational rule

The Dempster's combinational rule, also known as the evidence combination formula, can be expressed as Eq. 4:

$$\begin{aligned} \mathrm{m}(A) &= m_1(A_1) \oplus \mathrm{m}_2(A_2) \oplus \mathrm{m}_3(A_3) \oplus \cdots \oplus \mathrm{m}_n(A_n) \\ &= \frac{1}{1-k} \sum_{A_1 \cap A_2 2 \cap \cdots \cap A_n = A} \prod_{i=1}^{n} \mathrm{m_i A_i} \qquad (\forall A \subseteq \Theta) \end{aligned} \tag{4}$$

Where k is the degree of conflict of evidence, $\frac{1}{1-k}$, $k = \sum_{A_1 \cap A_2 \cap A_3 \cap \cdots A_n \neq \Phi} m_1(A_1) \bullet m_2(A_2) \bullet \cdots \bullet m_n(A_n)$. k = 1, the conflict between the evidences is so great that the evidence cannot be fused using the Dempster formula. When some These, two characteristics of the D-S evidence theory combination rule facilitate us in the combination of evidence. When combining multiple evidences, it does not need to consider combination orders. At the meanwhile, when there are consistency and contradiction between the evidences, group similar evidence into groups and then carry out the combination of grouped combination conclusions.

3.5 Research on application of evidence theory

Evidence theory has been widely used in the fields of expert system, information fusion, intelligence analysis, target judgment, legal case analysis, multi-attribute decision analysis, etc. due to its extensive advantages in algorithm and application level. Many researchers have also carried out corresponding improvement research on the problems in the application. As far as the algorithm itself is concerned, there are three main aspects from the terms of application:

1. Construct a corresponding fast algorithm for a specific evidence organization structure

In different application fields, the organization structure and expression form of evidence are different. Starting from the evidence itself, it is an important point in the application field to study the algorithm that can quickly obtain the fusion conclusion in the application.

2. Approximate calculation

Aiming at the problem that the computation amount will increase rapidly when the dimension of evidence theory fusion algorithm and the quantity of evidence increase, the approximate algorithm is constructed starting from the practical application. The method of approximate calculation can simplify the calculation process under the condition of ensuring the calculation conclusion of uncertain reasoning.

The basic idea of approximate calculation is to reduce the number of focal elements to achieve the purpose of reducing the amount of calculation.

Voorbraak found that if the combination of m functions will produce a Bayes trust function (i.e. a probability measure on a recognition framework), and then the substitution of m function with their Bayes approximation will not affect the result of Dempster's combinational rule, which is called the "Bayes" approximation method.

The meaning of the "Bayes approximation" is that it is very useful and computationally efficient for those cases where the final conclusion is concerned only with identifying the "elements" of the framework (i.e., a single hypothesis) rather than its "subset" (i.e., a subset of multiple hypotheses). Dubois and Prade proposed a "Consonant approximation" which is characterized by that the focal elements are nested after approximate calculation, and the number of focal elements does not exceed the number of hypotheses in the identification framework. The disadvantage is that this method is not suitable for calculation by Dempster's combinational rule, which may produce a large error. The "Consonant approximation" method applies to the expression of evidence.

Tessem proposed "(k, l, x) approximate algorithm ", k represents the minimum number of retained focal elements; l represents the maximum number of retained focal elements; x represents the maximum m value that is allowed to be deleted, and x usually takes a value on [0, 0.1].

First, sort the m value from big to small, and then loop the sum of m function values successively. If the number of retained focal elements is equal to 1, or the sum of the calculated m functions is greater than or equal to 1-x, the loop ends; otherwise, continue the loop, and finally normalize the m function values corresponding to the retained focal elements. The (k, l, x) method gives neither Bayes m function nor a consonant m function, but it does reduce the focal element.

3. Modification of D-S Method

In view of the problems existing in the practical application of D-S evidence theory fusion algorithm, corresponding modifications are made on the basis of traditional combination rules to avoid the irrationality of fusion conclusion under special circumstances.

4. Network security SA approach based on evidence chain

This section briefly introduces the flow of network SA [13] based on DS evidence theory: First, the identification framework should be determined, and all possible results should be considered, and each evidence should be assigned a basic credibility, and then the final credibility value of the target should be fused by using the composition rule. In this section, a method of SA based on DS evidence theory is proposed.

The network security SA based on DS evidence chain collects the protected network information through active and passive network sensors and takes the information as the fusion data of DS evidence theory after processing. Each piece of data collected by the sensor can be corresponding to one evidence, and then the corresponding initial credibility can be given to the evidence. Finally, the composite formula is used to fuse these evidences to obtain the credibility of the protected network threat proposition. This value reflects the degree of trustworthiness of the protected network under the threat of the evidence, and sets the confidence threshold. If the credibility exceeds the threshold, it indicates that the network component has a security threat and is vulnerable to attack, otherwise, the network component is secure.

In this chapter, the identification framework is $\Theta = \{\mathrm{T}, \mathrm{F}\}$ in which T indicates the camera was dangerous and vulnerable to attack while F indicates that the camera is secure and is not vulnerable to attack. Then the power set is $2^{\Theta} = \{\Phi, T, \mathrm{F}, \mathrm{H}\}$ in which Φ indicates the camera is both dangerous and safe while Himplies the camera may or may not be safe. The trust function satisfies $m(\Phi) + m(T) + m(F) + m(H) = 1$ in which $m(\Phi) = 0$ and $m(H) = 0$.

Second, every piece of data that is scanned from a camera device is used as a piece of evidence, and there are three types of evidence. The first is to scan the IOT devices opened on the port 23 all over the school, in which the camera device is the object of our SA so it could be attacked. An initial trust value is assigned to this evidence, that is, the ratio of camera devices to the number of devices opened on port 23 is used as the initial trust probability function of the evidence; the second type of evidence scans camera devices, in which cameras with weak password vulnerabilities are vulnerable to attack. Here we take the ratio of camera equipment with weak password vulnerability to the total number of cameras in NJUPT as the initial confidence probability function of the evidence; the third kind of evidence is to upload the virus to the camera device with weak password vulnerability. The successful uploading of the virus is highly dangerous and vulnerable to attack. We use the ratio of a successful webcam uploaded by a virus to a camera with a weak password vulnerability as the initial trust probability function. Through the above methods, we adopt three different types of evidence, further improve the credibility of evidence fusion, at the same time, we also compress a large number of evidence data into three pieces of evidence, improve the efficiency and time of synthesis. After that, we can use the improved composite formula to fuse the three evidences against the camera, and obtain the ultimate credibility of the dangerous situation of the camera in NJUPT.

Finally, the credibility $m(T)$ after fusion will be compared with a given threshold. If the reliability is greater than the threshold, it shows that the whole situation of the camera in NJUPT is dangerous and vulnerable to attack, otherwise, the overall situation of the camera of NJUPT is safe.

5. Experiment

In order to verify the feasibility and effectiveness of this method, the Telnet port scanning record of the network equipment in the campus network of NJUPT was used as the data source. The data was collected from the outbreak of a large-scale Mirai botnet attack on the East Coast of the United States at the end of 2016. The scope of collection is limited to the campus network of NJUPT. The study found that a large number of cameras in the campus network have weak password vulnerabilities. As shown in **Figure 2**, this vulnerability allows for intrusion into the monitoring system. Moreover, based on the vulnerability, the Mirai botnet can be uploaded to the camera and run. The camera becomes the Mirai botnet broiler, which can launch a large-scale DDoS attack. Because the scope of the research object is relatively small, after discovering the problems existing in the monitoring system in the campus network, we should inform the relevant departments of the school and take timely measures to protect the monitoring system. However, for large-scale protected networks, SA methods are needed to discover threat situation in time. This chapter uses DS theory to verify the feasibility and effectiveness of the proposed approach based on campus network data sources.

This chapter data source contains three kinds of data: (1) all 23 Telnet ports in the campus network in the open device and its type, IP address and other information; (2) the network camera with the weak password vulnerability of 23 Telnet in the campus network; (3) the camera which can upload Mirai virus and run it successfully through weak password vulnerability.

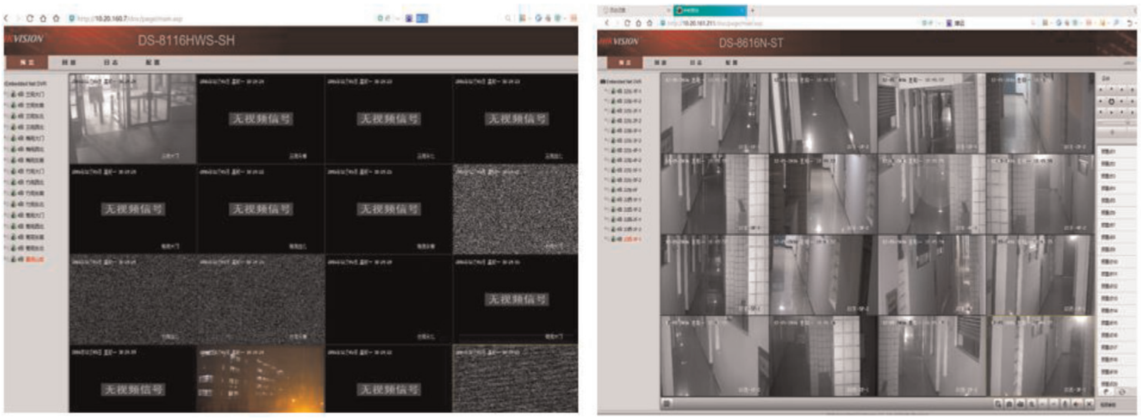
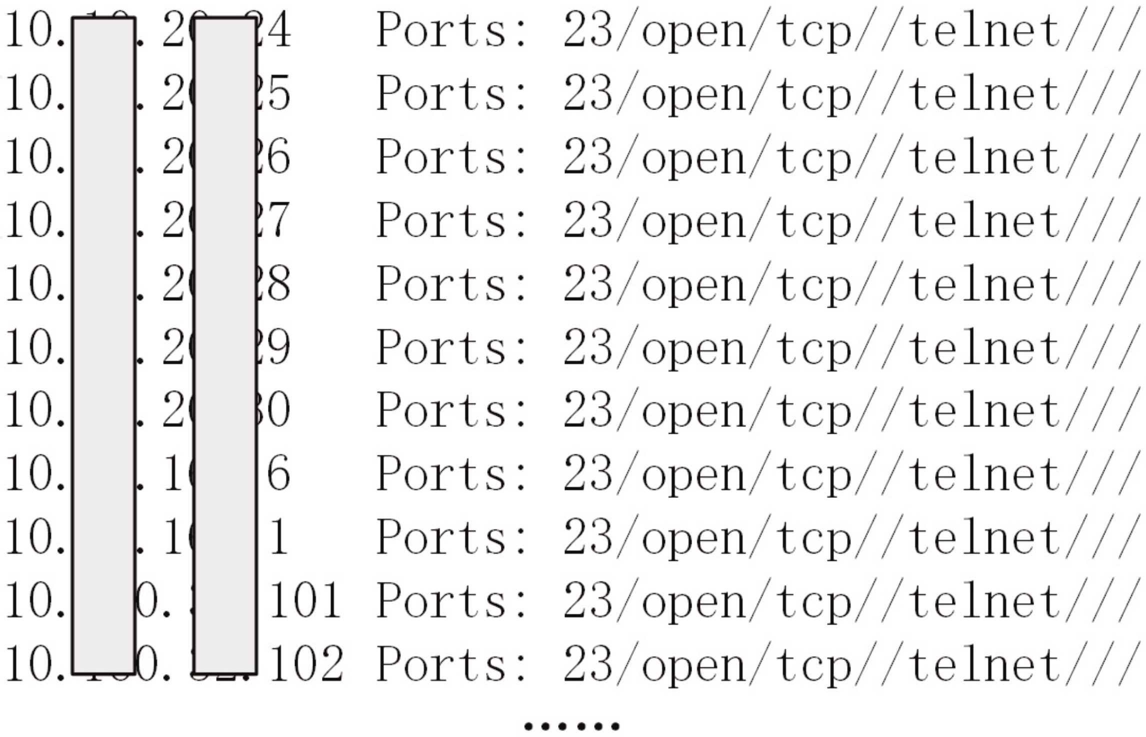


Figure 2.
Schematic diagram of campus monitoring system through weak password vulnerability.



```
10.[redacted]. 2[redacted]4      Ports:  23/open/tcp//telnet///
10.[redacted]. 2[redacted]5      Ports:  23/open/tcp//telnet///
10.[redacted]. 2[redacted]6      Ports:  23/open/tcp//telnet///
10.[redacted]. 2[redacted]7      Ports:  23/open/tcp//telnet///
10.[redacted]. 2[redacted]8      Ports:  23/open/tcp//telnet///
10.[redacted]. 2[redacted]9      Ports:  23/open/tcp//telnet///
10.[redacted]. 2[redacted]0      Ports:  23/open/tcp//telnet///
10.[redacted]. 1[redacted]6      Ports:  23/open/tcp//telnet///
10.[redacted]. 1[redacted]1      Ports:  23/open/tcp//telnet///
10.[redacted]0. [redacted]101   Ports:  23/open/tcp//telnet///
10.[redacted]0. [redacted]102   Ports:  23/open/tcp//telnet///
                        ......
```

Figure 3.
Scanned device records opened on port 23.

First, scan all IOT devices opened on port 23 open and the scan results are shown in **Figure 3**. A total of 464 data opened on port 23 were recorded, including 242 camera devices. So in evidence 1, the initial trust value $\mathrm{m}_1(V_1)$ is 242/464 $\approx$ 0.52 and $\mathrm{m}_1(S_1)$ is 1−0.52 = 0.48.

Secondly, Scan camera equipment in school for leak detection, as shown in **Figure 4**. Among them, there are 142 camera devices with weak password vulnerabilities. So in evidence 2, the initial trust value $\mathrm{m}_2(V_2)$ is 142/242 $\approx$ 0.59 while $\mathrm{m}_2(S_2)$ is 1−0.59 = 0.41.

Finally, we uploaded the virus to the cameras with a weak password, and 86 camera records were uploaded successfully, as shown in **Figure 5**. So in evidence 3, the initial trust value $\mathrm{m}_3(V_3)$ is 86/142 $\approx$ 0.61 and $\mathrm{m}_3(S_3)$ is 1−0.61 = 0.39.

Then, the three evidences are fused by Dempster formula. If the evidence provided by the sensor scan is B, C, and D respectively, the proposition that the investigated camera in the campus network has a network security threat is called V, and the proposition that the investigated camera in the campus network is secure is called S. Then three sets of evidence are combined to calculate the confidence of proposition V as follows:

the normalized constant k is calculated as follows:

$$\mathrm{K} = \sum_{B\cap C\cap D\neq\Phi} m_1(B)\bullet m_2(C)\bullet m_3(D)$$

$$= 0.52^*0.59^*0.61 + 0.48^*0.41^*0.39.$$

$$\approx 0.26.$$

to calculate $m(V)$ by composite formula:

$$m_1\oplus m_2\oplus m_3\{m(V)\}$$

$$=\frac{1}{k}\sum_{B\cap C\cap D=\{m(V)\}} m_1(B)\bullet m_2(C)\bullet m_3(D)$$

$$=\frac{1}{0.26}(0.52 * 0.59 * 0.61).$$

$$\approx 0.71.$$

to calculate $m(S)$ by composite formula:

$$m_1\oplus m_2\oplus m_3\{m(S)\}$$

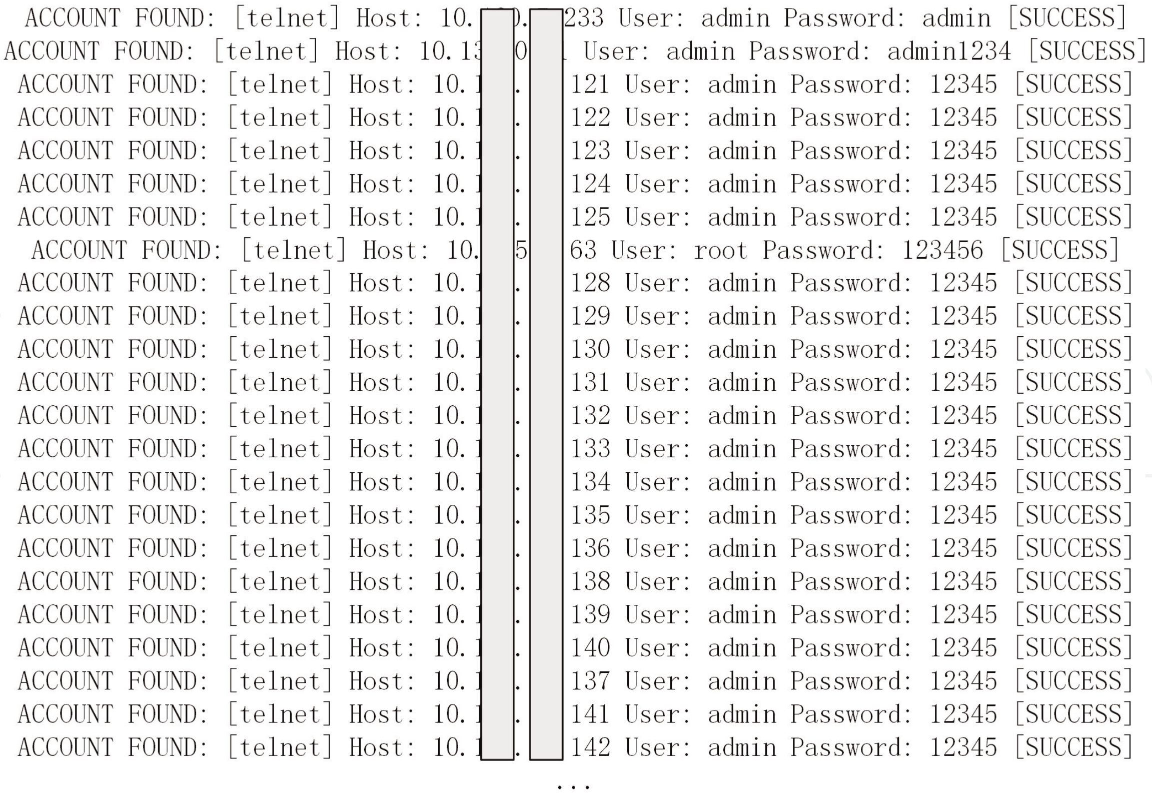
$$=\frac{1}{k}\sum_{B\cap C\cap D=\{m(S)\}} m_1(B)\bullet m_2(C)\bullet m_3(D)$$

$$=\frac{1}{0.26}(0.48 * 0.41 * 0.39).$$

$$\approx 0.29.$$

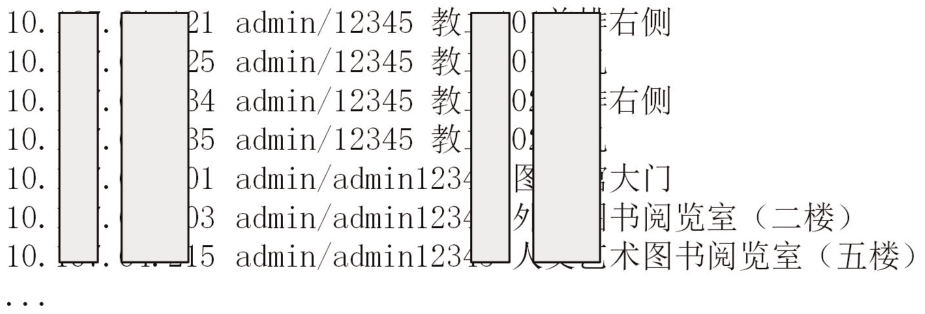
Based on the above calculations, the ultimate trust of $m(V)$ is 0.71 and that of $m(S)$ is 0.29. Because the experimental data source in this chapter contains only campus network camera and no other devices, there is no need to estimate the threshold. In the experiment, $m(V) > m(S)$, it shows that there are serious security threats in the monitoring system of campus network by calculating the method, and the method is effective.

The prototype system based on this method is shown in **Figure 6**. The system includes a scanning module, data query, weak password management and



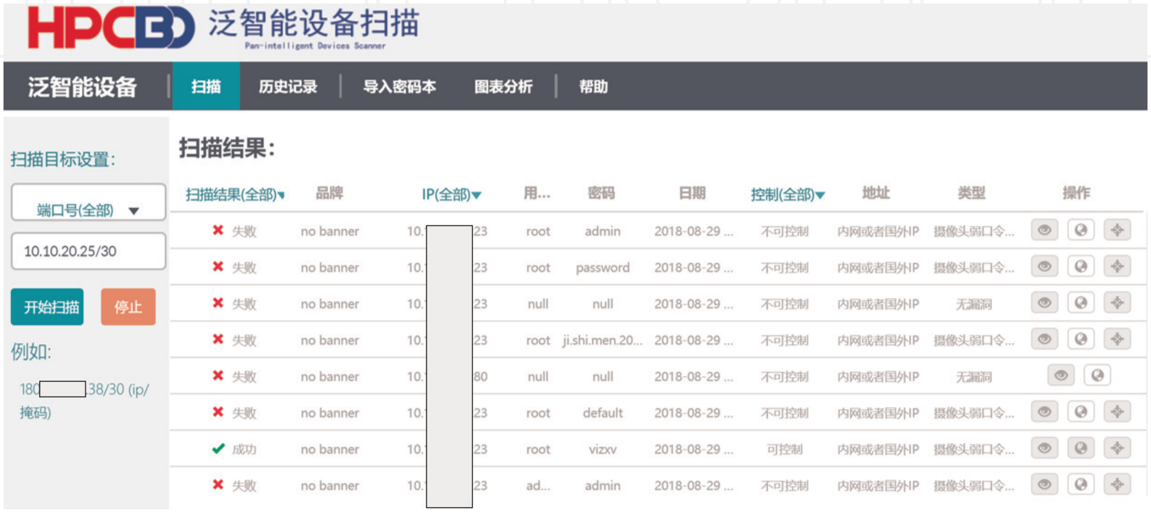
```
 ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]233 User: admin Password: admin [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted][redacted] User: admin Password: admin1234 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]121 User: admin Password: 12345 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]122 User: admin Password: 12345 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]123 User: admin Password: 12345 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]124 User: admin Password: 12345 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]125 User: admin Password: 12345 [SUCCESS]
 ACCOUNT FOUND: [telnet] Host: 10.[redacted][redacted]63 User: root Password: 123456 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]128 User: admin Password: 12345 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]129 User: admin Password: 12345 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]130 User: admin Password: 12345 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]131 User: admin Password: 12345 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]132 User: admin Password: 12345 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]133 User: admin Password: 12345 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]134 User: admin Password: 12345 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]135 User: admin Password: 12345 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]136 User: admin Password: 12345 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]138 User: admin Password: 12345 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]139 User: admin Password: 12345 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]140 User: admin Password: 12345 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]137 User: admin Password: 12345 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]141 User: admin Password: 12345 [SUCCESS]
ACCOUNT FOUND: [telnet] Host: 10.[redacted].[redacted]142 User: admin Password: 12345 [SUCCESS]
                                        ...
```

Figure 4.
Scanned records of cameras for leak detection in school.



```
10.[redacted].[redacted]21 admin/12345 教[redacted]右侧
10.[redacted].[redacted]25 admin/12345 教[redacted]
10.[redacted].[redacted]34 admin/12345 教[redacted]右侧
10.[redacted].[redacted]35 admin/12345 教[redacted]
10.[redacted].[redacted]01 admin/admin123[redacted]大门
10.[redacted].[redacted]03 admin/admin123[redacted]书阅览室（二楼）
10.[redacted].[redacted]15 admin/admin123[redacted]术图书阅览室（五楼）
...
```

Figure 5.
The virus uploading records on the cameras with a weak password.



HPCBD 泛智能设备扫描
Pan-intelligent Devices Scanner

泛智能设备 | 扫描 | 历史记录 | 导入密码本 | 图表分析 | 帮助

扫描目标设置:

端口号(全部) ▼

10.10.20.25/30

开始扫描 停止

例如:

180[redacted]38/30 (ip/掩码)

扫描结果:

扫描结果(全部)▾	品牌	IP(全部)▾	用...	密码	日期	控制(全部)▾	地址	类型	操作
✗ 失败	no banner	10.[redacted]23	root	admin	2018-08-29 ...	不可控制	内网或者国外IP	摄像头弱口令...	
✗ 失败	no banner	10.[redacted]23	root	password	2018-08-29 ...	不可控制	内网或者国外IP	摄像头弱口令...	
✗ 失败	no banner	10.[redacted]23	null	null	2018-08-29 ...	不可控制	内网或者国外IP	无漏洞	
✗ 失败	no banner	10.[redacted]23	root	ji.shi.men.20...	2018-08-29 ...	不可控制	内网或者国外IP	摄像头弱口令...	
✗ 失败	no banner	10.[redacted]80	null	null	2018-08-29 ...	不可控制	内网或者国外IP	无漏洞	
✗ 失败	no banner	10.[redacted]23	root	default	2018-08-29 ...	不可控制	内网或者国外IP	摄像头弱口令...	
✓ 成功	no banner	10.[redacted]23	root	vizxv	2018-08-29 ...	可控制	内网或者国外IP	摄像头弱口令...	
✗ 失败	no banner	10.[redacted]23	ad...	admin	2018-08-29 ...	不可控制	内网或者国外IP	摄像头弱口令...	

Figure 6.
Schematic diagram of network security SA prototype system based on DS evidence chain.

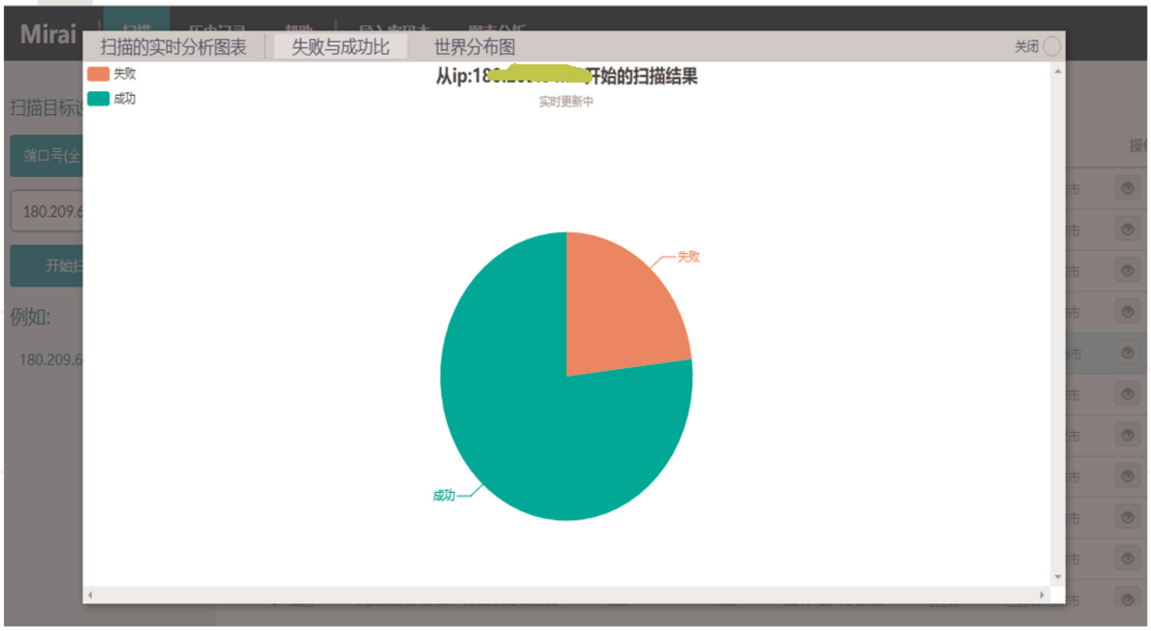


Figure 7.
Schematic diagram for the scanned result page by SA prototype system.

visualization (chart analysis) module, as shown in **Figure** 7. The scanning module integrates the automatic scanning function, as long as we input the network segment to be scanned and click “Start Scanning”, the scanning can be done automatically. The buttons under the “Operation” column on the right enable you to manually access the device. For example, if the device has a weak password vulnerability, you can start shell through the “Operation” button to automatically use the weak password to login to the device for easy viewing. The “Operation” also includes manual uploading of the Mirai zombie program, etc. Data Query is designed for your viewing history scanning records; Weak Password Management for adding or removing the collected camera factory default password; Visual Analysis Module for displaying the network situation by means of geographic information, data statistics and chart, etc.

The prototype system is shown in **Figure 6**.

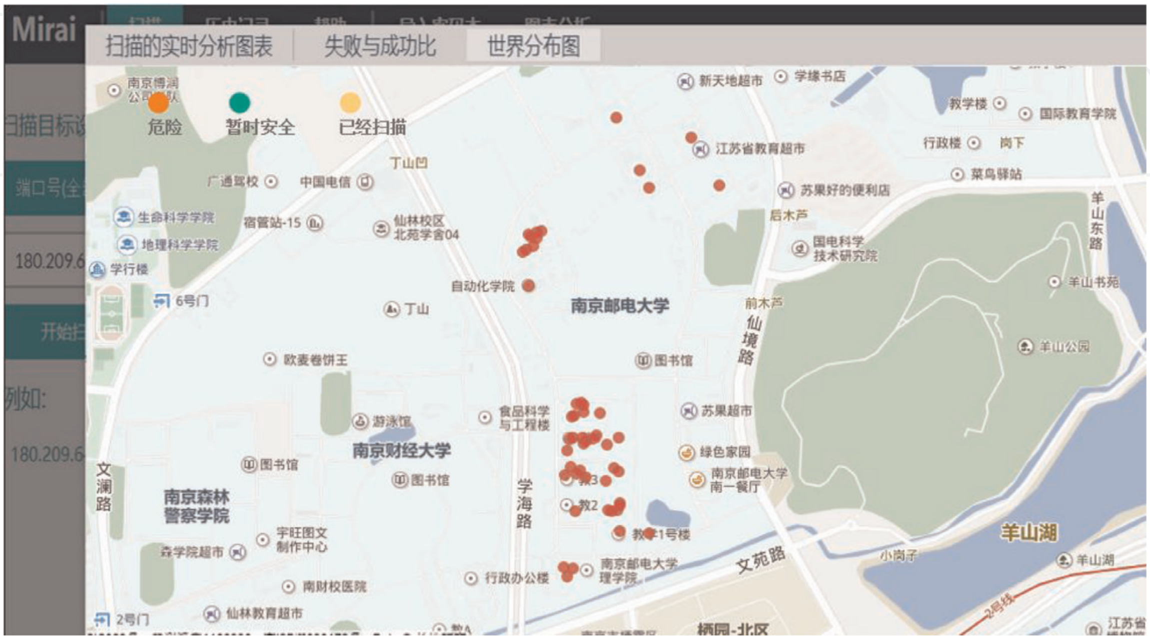


Figure 8.
Campus network security situation diagram based on geographic information.

The security situation of campus network based on the security threat analysis of campus network camera is shown in **Figure 8**. The situation map is based on geographical location information, and the red point indicates that there is a security threat in the corresponding location of the map, which will make the administrator reminded.

6. Conclusion

This chapter first introduces the related work of SA technology, the concept, definition and formula of DS evidence theory, and then aims at the problem of slow response of network security SA to burst vulnerabilities in the network. A method of network security SA based on DS evidence theory is proposed. Finally, according to the experiment of Mirai botnet, a surveillance camera in NJUPT's campus network, it is proved that the SA method based on DS evidence theory is feasible and effective, and this method can detect the major threat in a protected network in time.

Acknowledgements

Thanks to Shu Wang, Qing Ye, Na Wang, Haichang Yao, Kui Li, Ruchuan Wang and Lu Yao for their contributions. This work is supported by the National Key Research and Development Program of China (2017YFB1401301, 2017YFB1401302, 2017YFB0202204), the National Natural Science Foundation Program of China (61373017), the Key Research and Development Program of Jiangsu Province (BE2017166), the Natural Science Foundation Outstanding Youth Fund of Jiangsu Province (BK20170100), the Open Fund of Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks (WSNLBZY201514), the 1311 Project of Nanjing University of Posts and Telecommunications.

Conflict of interest

The authors declare no conflict of interest.

Author details

Liu Shangdong[1,3,4] and Ji Yimu[1,2,3,4,5]*

1 School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, China

2 Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing, Jiangsu, China

3 Institute of High-Performance Computing and Bigdata, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu, China

4 Nanjing Center of HPC China, Nanjing, Jiangsu, China

5 Jiangsu HPC and Intelligent Processing Engineer Research Center, Nanjing, Jiangsu, China

*Address all correspondence to: jiym@njupt.edu.cn

References

[1] Wu D, Cui X, Liu Q, Zhang F. Research on ubiquitous botnet. Netinfo Security. 2018;**2018**(07):16-28

[2] Xi R, Yun X, Jing S, Jin S, Zhang Y. Research survey of network security situation awareness. Journal of Computer Applications. 2012;**32**(1):1-4

[3] Gong Z, Zhuo Y. Research on network situation awareness. Journal of Software. 2010;**21**(7):1605-1619

[4] Zhang S, Liu X, Sun X. Hierarchical awareness of network security situation based on multi-source fusion. Computer Technology and Development. 2016; **26**(10):77-82

[5] Kokkonen T. Architecture for the cyber security situational awareness system. International Conference on Next Generation Wired/Wireless Networking. St. Petersburg, Russia: Springer; 2016. pp. 294-302

[6] Eiseler V, Koch R, Rodosek GD. System complexity meets decision makers: A framework for level-appropriate information processing. In: Bryant AR, Lopez J, Mills RF, editors. Proceedings of the 12th International Conference on Cyber Warfare and Security. 2017. pp. 427-431

[7] Yang Y-L. Research on network security situation awareness system based on machine learning. In: Zeng Z, Bai X, editors. Proceedings of the 2016 2nd Workshop on Advanced Research and Technology in Industry Applications. 2016. pp. 122-125

[8] Khalid HM, Peng JCH. A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks. IEEE Transactions on Smart Grid. 2016;7(4):2026-2037

[9] Hu J, Li Z, Yao D, Yu J. Measuring botnet size by using URL and collaborative MailServers. In: Fifth International Conference on Networking and Services. 2009. pp. 161-164

[10] Evesti A, Kanstren T, Frantti T, et al. Cybersecurity Situational Awareness Taxonomy. IEEE International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). London, UK. 2017

[11] Thomas C, Balakrishnan N. Modified evidence theory for performance enhancement of intrusion detection systems. In: Proc. International Conference on Information Fusion (ICIF), Cologne

[12] Yager RR, Fedrizzi M, Kacprzyk J, editors. Advances in the Dempster-Shafer Theory of Evidence. New York, NY: John Wiley and Sons; 1994

[13] Sabata B, Ornes C. Multisource Evidence Fusion for Cyber-Situation Assessment. 2006. pp. 624201-624201