International Journal of Security and Its Applications
Vol. 10, No. 5 (2016) pp.215-224
http://dx.doi.org/10.14257/ijsia.2016.10.5.20

Representation of Network Security Situation Elements Based on Cloud Model*

Kou Guang [1*], Yang Haopu [2], Wang Kun [3], Zhang Yuchen[4] and Wang Shuo[5]

[1,2,3,4,5](Zhengzhou Information Science and Technology Institute,Zhengzhou,450001,China)
[1,4](Science and Technology on Information Assurance Laboratory,Beijing,100072,China)
[*]kg5188@163.com

Abstract

Aiming at efficiently aware the network security situation, we proposed a framework of Network Security Situation Awareness on the base of Cloud Model. With network security situation elements at the core, we modified the Cloud Model to a novel concept, situation cloud, which act as theoretical foundation in the transition between the qualitative and quantitative representation on situation elements. Finally, the experimental results showed that these two kind of representations can directly summarize the security condition of network as well as precisely recognize the changes of situation elements.

Keywords: *network security; situation elements; cloud model; qualitative and quantitative representation*

1. Introduction

To correctly aware the security situation of a sophiscated network, we need to deal with original security data from all kinds of network security sensors which are large scale, with different structures and with low value density[1]. Abstracting security situation from those original data is a hierarchical process which combine several network security technologies and intelligent algorithms. Several problems have been proposed and discussed by many related organizations and experts.

Mustafa M, Al-Bahar J *et al.*, [2] proposed modle-based network security situation assessment method according to different system hierarchical layers. But it's difficult to satisfy the environmental requirement. Jie Lu *et al.*, [3]awared the security situation in qualitative method, which was hard to implement in large-scale and with poor speed. Wei S *et al.*, [4] brought in the Rough Sets Theory to assess security situation. This method had a excellent performance in usability as well as in dealing with uncertained information without prior knowledge. But it couldn't satisfy the need of real-time implement because of vast computing. In Srihari R's research [5], the information that situation awareness needed could be gained by the element abstracting concept-based method. This method only took intrusion attack into account, which was not suitable for the complicated environment.

*Supported by the Foundation of Science and Technology on Information Assurance Laboratory under Grant Nos.KJ-14-106.

ISSN: 1738-9976 IJSIA

The groundwork of Network Security Situation Awareness is to represent the situation elements precisely. However, it's hard to realize due to the rapidly increasing of the network's scale. In 1995, Academician Li Deyi proposed the Cloud Theory [6] to handle the problem of uncertainty in complicated systems. With the building of Cloud Model, we can efficiently realize the transition between qualitative and quantitative variables. Then demonstrating the fuzziness and randomness with a 3-tuple, we can study the regular patterns of uncertainty to obtain the range as well as distributed regularity of quantitative data from qualitative information expressed by language value. The reverse process can be realized in the meanwhile. Thus, the Cloud Theory can be used in the research of transition between qualitative and quantitative representation of network security situation elements.

This paper proposed the cloud-model-based representation of network security situation. In the proposed method, we merged different kinds of situation elements from several security events to realize the qualitative and quantitative representation as well as transition, and describe the network security situation in view of the above.

2. Related Research

2.1 Representation of Network Security Situation

In order to correctly understand the network security situation, appropriate representation of situation elements is indispensable. Figure 1 shows the framework of network security situation elements merging different data from several kinds of sensors.

This framework contains three layers. With network security situation elements at the core, each layer respectively awares and represents the network situation. Detailed description of the three layers is in the following:

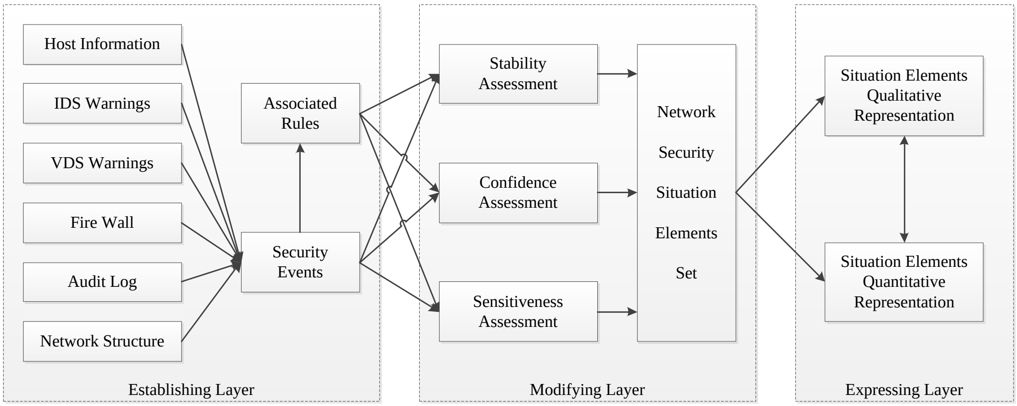

Figure 1. The Framework of Network Security Situation Elements

1. Establishing Layer. Based on the assessment of network security situation elements, this layer analyzes the related data from situation-related information (such as network structure, host information, IDS warning, VDS warning, firewall warning, audit log and etc.) to gain the security events and generate situation elements through correlation analysis.
2. Modifying Layer. According to the requirement of stability, confidence and sensitiveness, this layer modifies a mass of situation elements from Establishing Layer to generate Network Security Situation Elements Set. This layer efficiently reduce the secondary elements which provide tiny influence on the whole security situation.
3. Expressing Layer. This layer correctly describes the security condition of targeted system.

The format of situation elements is shown in Table 1.

Table 1. The Format of Situation Elements

Number	Associated Rules	Confidence
r_1	$c_1 \cap c_3 \cap c_8 \cap c_{13} \rightarrow c_{12}$	Confidence(r_1)=0.84
r_2	$c_3 \cap c_5 \cap c_9 \cap c_{16} \rightarrow c_6$	Confidence(r_2)=0.76
r_3	$c_4 \cap c_6 \cap c_{10} \cap c_{15} \rightarrow c_{16}$	Confidence(r_3)=0.62
r_4	$c_4 \cap c_{10} \cap c_{15} \cap c_{16} \rightarrow c_6$	Confidence(r_4)=0.71
……	……	……

2.2. Cloud Theory and Improvement

Aiming at the uncertainty problem of complicated systems, the Cloud model efficiently finish the transformation between qualitative and quantitative representation of parameters. The Cloud refers to the mapping from a qualitative notion in a quantitative domain to interval distribution, [0,1], while the arbitrary parameter in the sub-domain of the quantitative domain refers to the Cloud Dropts. Because the Cloud Dropts are random variables, the most important character of them is unorder. In this paper, the situation of network security can be discribed more precisely with more Cloud Dropts.

The key factor of Cloud Theory is to describe the cloud that constitute of various Cloud Dropts (similar random variables) by three quantitative eigen-values, from which can combine the fuzziness and randomness of semantics by qualitative representation with the help of Cloud Dropts.

Network security situation is a dynamic process, which is influenced by several factors. For example, the spatial environments as well as vulnerability of target system, the existing audit logs, the knowledge base and so on. Because of the continue changing of data, as well as the fuzziness and randomness, the network security situation elements have the character of uncertainty. For the sake of applying Cloud Theory into Network Security Situation Awareness, we need to adjust the Cloud Model to represent the situation elements.

3. Representation of Network Security Situation Elements Based on Cloud Model

3.1. Construction of Situation Cloud

Definition 1 Situation Cloud. Suppose *U* is a numerical domain representing quantitative network security situation, $X \subseteq U$, *T* represents the network security situation elements defined on *U*. If $\forall x \in X$, $\exists C_T(x) \in [0,1]$, where $C_T(x)$ is a random number with steady tendency, then call $C_T(x)$ as Subjection Degree, and call the mapping from *U* to [0,1] as Situation Cloud.

Situation Cloud is the set of situation elements' distribution. We regard situation elements in every space-time interval as the Cloud Dropts of the Situation Cloud. Detailed description of Situation Cloud is in the following:

(1)In the Situation Cloud Model, the Subjection Degree is a random number that follows a certain Gaussian Distribution Function.

(2)While generating a Situation Cloud, a lot of Cloud Dropts are required to express the fuzziness and randomness of the mapping.

(3)The Thickness of the cloud, representing the randomness of the Subjection Degree, is asymmetrical.

3.1.1. Mapping from elements to 3-tuple

According to the definition, network security situation element can be expressed as the following:

$$El_{n1}^{1} = (num, pol, pro) \tag{1}$$

Where the superscript *1* represents the first situation element, the subscript *n1* represents the network., *num* represents the sequence number, *pol* represents a polynomial, and *pro* represents the probability.

Then, the definition has to be reflected into a 3-tuple to express the character of situation cloud.

Definition 2 Quality of Situation Cloud. Using a 3-tuple to represent the situation cloud model qualitatively:

$$SC = (Ex, En, He) \tag{2}$$

where *Ex* represents the average value of cloud dropts; *En* represents entropy, which is used to express the degree of dispersion; and *He* represents hyper entropy, which is used to express the uncertainty of the whole cloud.

3.1.2. Construction of Network Security Situation Cloud

In the Situation Cloud Model, a Forward Cloud Operator transfers the qualitative concept of situation into quantitative data, and a Backward Cloud Operator inverses the process. We can measure the similarity between these two kind of representations through the definition of Cloud Similarity Operator.

Definition 3 Forward Cloud Operator. If the mapping function $\varphi_{forward} : SC \to T$ satisfy the following conditions:

$$(1)\ X = \{ \mathrm{x}_i \mid x_i = Norm(\mathrm{Ex}, \mathrm{En}, He), \mathrm{i} = 1, 2, \cdots, \mathrm{N} \} \tag{3}$$

$$(2)\ T = \{ (\mathrm{x}_i, \mathrm{y}_i) \mid x_i \in X, y_i = e^{-(\mathrm{x}_i - \mathrm{Ex})^2}, z_i \} \tag{4}$$

Then, we can sign the mapping function as $Ar^{Forward}(SC(Ex, En, He))$, which is used to transfer the qualitative representation of situation elements into quantitative data set.

Definition 4 Backward Cloud Operator. If the mapping function $\varphi_{backward} : T \to SC$ satisfy the following conditions:

$$(1)\ Ex = \overline{X}, X = \{ x_i \mid (x_i, y_i, z_i) \in T \} \tag{5}$$

$$(2)\ En = \sqrt{\frac{\pi}{2}} \overline{|x_i - Ex|}, x_i \in X \tag{6}$$

$$(3)\ He = \sqrt{\frac{\pi}{2}} \overline{|Ex_i - En|}, x_i \in X \tag{7}$$

Then we can sign the mapping function as $Ar^{Backward}(T)$, which is used to transfer the quantitative data set of situation elements into qualitative representation.

Definition 5 Situation Cloud Similarity Operator. If the mapping function $\pi : (S\mathrm{C}_i = SC_j) \to sim(i, j)$ satisfy the following conditions:

(1)when $sim(i, j) \in [0,1], S\mathrm{C}_i = SC_j$ then, $sim(i, j) = 1$;

$$(2)\, sim(i,\ j) = (1 - \frac{\left|En_i - En_j\right|}{\left|En_i + En_i\right|})(1 - \frac{\left|Ex_i - Ex_j\right|}{\left|Ex_i + Ex_i\right|})(1 - \frac{\left|He_i - He_j\right|}{\left|He_i + He_j\right|}) \qquad (8)$$

Then we can sign the mapping function as $Ar^{likeness}(SC_i(Ex_i, En_i, He_i), S\,C_j(Ex_j, En_j, He_j))$, which is used to express the similarity between the two kind representations of situation elements.

Applying the Situation Cloud to represent the situation elements, we can utilize the quantitative data to represent the situation elements, and utilize the situation cloud to express the overall condition of the network situation. As the original data inputing and changing continually, the situation elements change quickly, while the Situation Cloud changes slowly.

3.2. Transition between Qualitative and Quantative Representation

3.2.1. Transition Flow between Qualitative and Quantitative Representation

The Transition Flow between qualitative and quantitative representation of network security situation elements is shown in Figure 2.

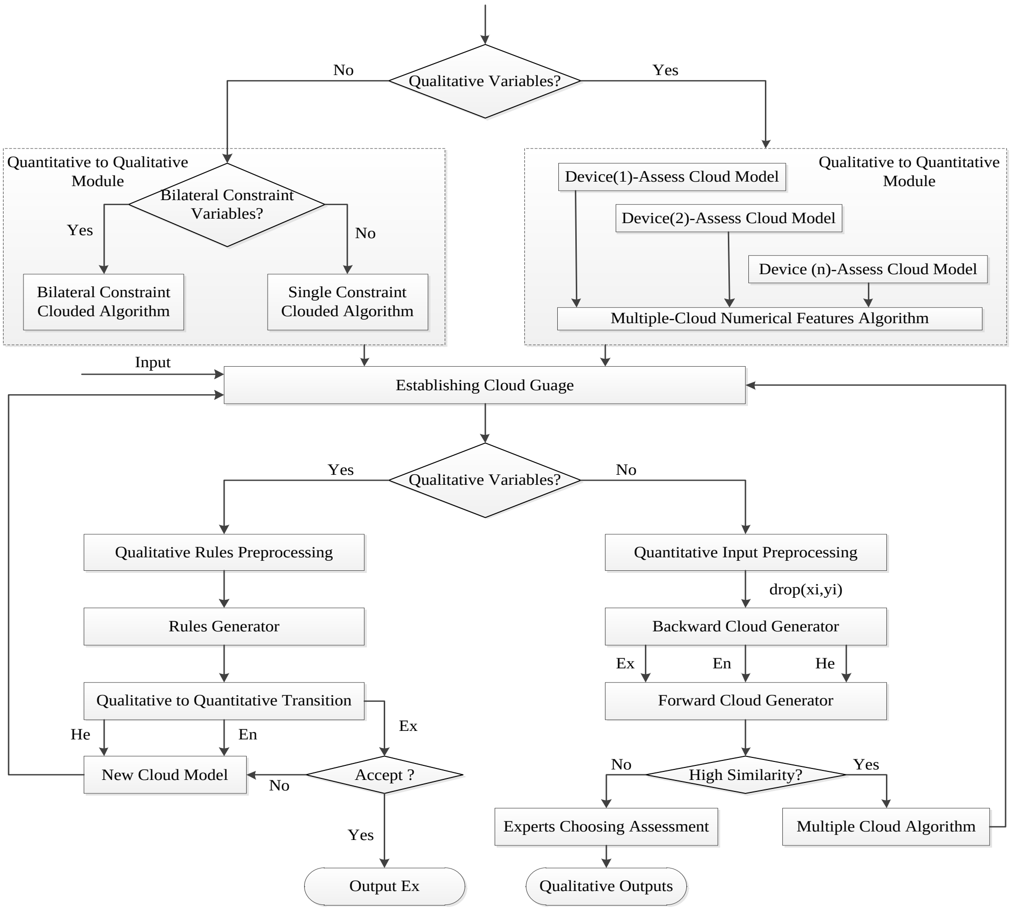
No
Qualitative Variables?
Yes
Quantitative to Qualitative Module
Bilateral Constraint Variables?
Yes
No
Bilateral Constraint Clouded Algorithm
Single Constraint Clouded Algorithm
Device(1)-Assess Cloud Model
Qualitative to Quantitative Module
Device(2)-Assess Cloud Model
Device (n)-Assess Cloud Model
Multiple-Cloud Numerical Features Algorithm
Input
Establishing Cloud Guage
Yes
Qualitative Variables?
No
Qualitative Rules Preprocessing
Quantitative Input Preprocessing
drop(xi,yi)
Rules Generator
Backward Cloud Generator
Ex
En
He
Qualitative to Quantitative Transition
Forward Cloud Generator
He
En
Ex
New Cloud Model
No
Accept ?
No
High Similarity?
Yes
Yes
Experts Choosing Assessment
Multiple Cloud Algorithm
Output Ex
Qualitative Outputs

Figure 2. Transition Flow between Qualitative and Quantitative Representation

3.2.2. Construction of Variable and Establishing Cloud Guage

According to the definition of situation cloud model, the quantitative variables in a domain *U* can be transferred into qualitative forms according to the above Transition

Flow. On the contrary, the flow can also acquire the numerical features as well as the shape of the cloud, (*Ex*, *En*, *He*), through the Clouding-description of qualitative variables. The reversible process is named as the Clouding of variable. The detailed descriptions are shown in the following.

The Clouding of Quantitative Variable. If quantitative variables are limited by upper and lower boundary, such as $V_{Q1} = [B_{\min}, B_{\max}]$, then the clouding process is a Forward Cloud Model. Take the mid-value of the constraint condition as the average value, the quantitative variables can be approximate represented by the cloud whose main-effect area is bilateral constraint. The Clouding variables can be figured out by the following equation: $Ex = (B_{\min} + B_{\max})/2, En = (B_{\max} - B_{\min})/6, He = k$; where k is a constant and can be adjusted by the threshold range of the variable. If the quantitative variables are limited by single constraint, such as $V_{Q1} = [-\infty, B_{\max}]$ or $V_{Q2} = [B_{\min}, +\infty]$, then the first step is to determine the missing boundary or average value based on the maximum or minimum of the testing data.

The Clouding of Qualitative Variable. Qualitative variables are assigned by the devices' natural language assessment. The following equations calculate the numerical features on the base of Cloud Model proposed by devices:

$$\begin{cases} Ex = (Ex_1 \times En_1 + Ex_2 \times En_2 + \cdots + Ex_n \times En_n)/(En_1 + En_2 + \cdots + En_n) \\ En = En_1 + En_2 + \cdots + En_n \\ He = (He_1 \times En_1 + He_2 \times En_2 + \cdots + He_n \times En_n)/(En_1 + En_2 + \cdots + En_n) \end{cases} \tag{9}$$

The function of Cloud Guage is to put the qualitative and quantitative Clouding variable into an identical coordinate system, where the cloud clusters constitute an active space with qualitative and quantitative variables in it. At discretionary moment T, qualitative or quantitative input choose the transferring cloud model by activate the corresponding interval.

3.2.3. Forward Transition

Forward Transition means the transition from qualitative to quantitative representation, which is realized by the Forward Cloud Generator. The qualitative representation usually indicates the devices' assessments by natural language. The detailed procedure is shown in the following:

(1) Qualitative Rules Preprocessing

This step clears up the qualitative assessments according to index such as the priority or frequency. Then we can get some qualitative rules like *if* $X=X_i$, *then* $Y=Y_i$, $i=1,2,\cdots$, where *X* is called *X*-condition Cloud, and *Y* is called *Y*-condition Cloud.

(2)Establishing Rules Generator

This step establishing Rules Generator in accordance with different *X*-condition Clouds to handle the qualitative input. There are four types of Rule Generators on the basis of Cloud Model: Single Rule, Single Condition Multiple Rule, Multiple Condition Single Rule and Multiple Condition Multiple Rule. This paper takes Multiple Condition Multiple Rule Generator as example to demonstrate the principles of Rules Generator

(3)Forward Transition

After the establishment of Multiple Condition Multiple Rules Generator, the CR_{Xi} will create a number Y_j randomly when the *X*-condition Cloud $CR_{Xi}(i=1,2,\cdots)$ is activated by inputting a qualitative variable $X=X_i$. The Subjection Degree determines which number will be activated, and the active frequency. Thus it can express the active intensity shown by the generator, or the Cloud Guage's active level in the corresponding interval.

The method of determining the prior rule is choosing the maximum Y_{max} from all Y_j. Y_{max} can control the Cloud Dropt, *drop(ui*, Y_{max}*)*, generated by the CR_{Yj} corresponding to the output plane, and the *ui* can be calculated by the reversible computing.

Delete the numbers that the distance with the calculated mid-value ∂ is greater than the setting threshold θ. The remaining cloud dropt will be used to obtain the numerical features, (*Ex*, *En*, *He)*, by input them into the Reverse Cloud Generator CR^{-1}.

3.2.4. Backward Transition

Backward Transition means the transition from quantitative to qualitative representation. According to Cloud Model generated by the quantitative numbers, the devices can get the feedback of the intuitional description from a mass of numercial features. Then take the experienced data or simulated output as the Cloud Dropts, the holistic features of the cloud generated by repeatedly simulation reflect the security level of the target-network.

4. Experimental Analysis

In order to prove the feasibility of the proposed method, we designed a experiment to observe the transition from qualitative to quantitative representation.

(1)Ensure the Object

We suppose the security situation of a target network in the attack-defense environment as the object. The real-time condition of the network as well as the changing tendency can be described by the situation elements. Considered the numerical value of the elements, we need to gain the corresponding security indexes in different environments.

(2)Set the Security Level

We divided the condition of the security situation into three levels: (High Risk, Normal, Low Risk).

(3)Obtain the Devices' Assess Value

Select 6 devices to evaluate the condition of target network security situation (shown in Table 2).

Table 2. Devices' Assessment

	High Risk （*Exh, Enh, Heh*）	Normal （*Exn, Enn, Hen*）	Low Risk （*Exl, Enl, Hel*）
a	(120, 23, 11)	(60, 15, 6)	(17, 5, 0.8)
b	(122, 20, 12.5)	(62, 18, 6)	(20, 6, 1)
c	(135, 22, 12)	(50, 14, 5)	(15, 5, 0.8)
d	(130, 24, 12)	(54, 23, 4)	(15, 7, 1)
e	(140, 25, 13)	(68, 10, 5)	(23, 10, 1)
f	(132, 28, 11.5)	(70, 23, 4)	(25, 5, 1.2)

(4)Clouding the Qualitative Variable and Establish the Cloud Guage

This step we Clouding the qualitative assessments given by the above devices, and established the Cloud Guage by setting all the Clouding results into the coordinate system whose coordinate axis defined as security index *S*. The related parameters could be calculated by Equation 3-3 respectively:

- $Cloud_{high}$(130.18, 142, 11.99)
- $Cloud_{nomal}$(60.66, 103, 4.87)

- *Cloud$_{low}$*(19.47, 38, 0.97)

(5)Establish the Rules Generator

The rules set described as the following:

- If the security index *S* meet the limitation: $S\in$[15, 45], then the security condition is “Safe”;
- If the security index *S* meet the limitation: $S\in$[45, 85], then the security condition is “Normal”;
- If the security index *S* meet the limitation: $S\in$[85, 135], then the security condition is “Danger”;

Then we established the Rules Generator accordingly (shown in Figure 3).

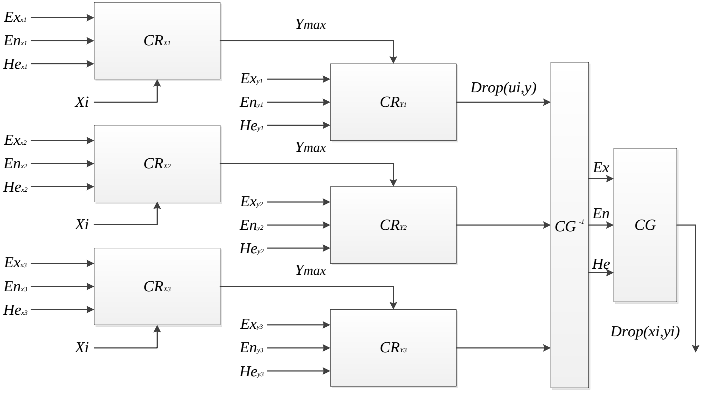

Figure 3. Rules Generator

The numerical features of every Cloud Generators can be calculated: *CR$_{x1}$*(30, 5, 2)、*CR$_{x2}$*(65, 6.7, 1)、*CR$_{x3}$*(110, 8.3, 4).

(6)Forward Transition

The input variable of Forward Transition Algorithm is represented qualitatively. Supposed the input variable *Xi=23.2*. We can get the active intensity *CR$_{x1}$*、*CR$_{x2}$*、*CR$_{x3}$* respectively. Then we can locate it in the Cloud Guage.

We take the calculation of *CR$_{x1}$* as an example. Detailed procedures are shown as follows:

1.Generate the random number *En'* on the basis of *En=5, He=2*;

2.According to the equation $Yj = e^{-\frac{(X_{ij} - Ex_{x_{ij}})^2}{2 En_{x_{ij}}'^2}}$, we can get $Y_{A1}=0.0463$;

3.With the same way, we can get $Y_{A2}=0.0238$, $Y_{A3}=2.317e\text{-}057$.

4.Select the maximum Y_j, that is Y_{A1}, as the condition to activate the corresponding Cloud Guage, *Cloud$_{low}$*(19.47, 38, 0.97), and calculate ui;

5.Rebuild the Rules Generator according to several rounds of assessment.

We can get the qualitative variable sampling set *[dropt(ui, Y_{jmax})]*. Put this set into the reverse Cloud Generator CR^{-1}, and restore the final cloud numerical features (*Ex, En, He*)=(21.7, 23.1, 3.6). Here the number 21.7 reflects the quantitative security condition of target network. On the one hand, the value can be regarded as the input in the next simulation. On the other one hand, it can be used to generate a new Cloud. Shown in Figure 4.

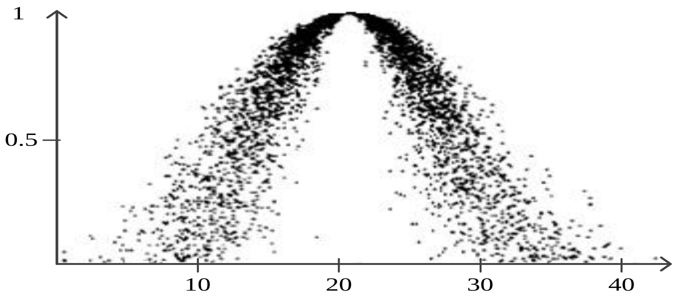

Figure 4. Restore Cloud of the Target Network Security Condition

(7)Generate the Situation Cloud. Then deliver the results to devices and re-assess them to modify the Rules Generator.

5. Conclusion

Nowadays, the uncertainty problem of data and information in the network is still existing. In order to correctly aware the network security condition, this paper proposed a novel framework of situation awareness, combined the feature that situation elements can be represented by qualitative as well as by quantitative variables. Based on the network security situation elements, the proposed framework analyze the origin of the uncertainty, and present the Situation Cloud which is modified by the cloud theory. Then this paper described the transition flow between qualitative and quantitative representation of situation elements. According to a typical network attack scene, the effectiveness of the proposed framework was proved. The experimental results showed that the qualitative and quantitative representation of situation elements can directly described the security condition of the target network, and precisely recognized the changes of them. The future research will focus on the following aspects: 1. utilize a novel cloud computing platform to analyze the network security situation data; 2. apply the proposed method into other scenes.

References

[1] M. Armbrust, A. Fox and R Griffith, A View of cloud computing", Commun ACM, 2010, 53(4): 50-58.

[2] L. Poap and M. Yu, "Cloud police: taking access control out of the network", Hotnets' 10. ACM 2010[C]. New York: ACM, 2010. 1-6.

[3] Mell P, Grance T. The NIST Definition of Cloud Computing[R]. National Institute of Standards and Techn -ology, 2011.

[4] Luo Junzhou, Jin Jiahui, Song Aibo, et al. Cloud Computing: Framework and Key Technology[J]. Journal on Communications, 2011, 32(7):3-21.

[5] Zhao Shenghui, Wu Guoxin, Zhang Sanfeng, et al. Review of QoS based on SOA[J]. Computer Science, 2009, 36(4):16-20.

[6] Li Qiao, Zheng Xiao. Review of Cloud Computing[J]. Computer Science, 2011, 38(4):32-37.

[7] Vaquero L, Rodero-Marino L, Caceres J, et al. A break in the clouds: towards a cloud definition[J]. SIGCOMM Computer Communication Review, 2009, 39(1): 50-55

[8] Armbrust M. Fox A, Grith R, et al. Above Berkeley View of Cloud Computing[R]. UCB/EECS-2009-28. Berkeley, USA: Electrical Engineering and Computer Sciences, University of California at Berkeley, 2009.

[9] Dustdar S, Scheriner W. A surveyon Web services composition[J]. International Journal of Web and Grid Services, 2005, 1(1): 1-30.

[10] Cloud Computing, www.google.com.

[11] IBM Blue Cloud Initiative Advances Enterprise Cloud Computing, http://www.ibm.com

[12] Microsoft Cloud Computing Infrastructure, http://www.microsoft.com

[13] Amazon Elastic Compute Cloud, http://www.amazon.com

[14] Peng Liu, Yao Shi, San-li Li, Computing Pool-a Simplified and Practical Computational Grid Model, the Second International Workshop on Grid and Cooperative Computing (GCC 2003), Shanghai, Dec 7-10, 2003, Published in Lecture Notes in Computer Science (LNCS), Vol. 3032, Heidelberg: Springer-Verlag, 2004.

[15] Zhang Y X, Zhou Y Z. 4VP+: A novel meta OS approach for streaming programs in ubiquitous computi -ng. In: Proe of IEEE the 21st Int'l Conf on Advanced Information Networking and Applications(AINA 2007), Los Alamitos, IEEE CS, 2007.

[16] Zhang Y X, Zhou Y Z. Transparent computing: a new paradigm for pervasive computing. In: Prec of the 3rd Int'l Conf on Ubiquitous Intelligence and Computing(UIC 2006), Berlin, Heidelberg: Spring-Verlag, 2006.

Authors

Kou Guang was born in 1983. He received a M.S. and Ph.D. degree in Zhengzhou Information Science and Technology Institute, Zhengzhou in 2015. He is now an lecturer at the Henan Province Key Laboratory of Information Security, Zhengzhou Information Science and Technology Institute. Her research interests include situation awareness, cloud security and security protocols.

Yang Haopu was born in 1993. She is receiving a M.S. degree in Zhengzhou Information Science and Technology Institute, Zhengzhou. Her research interests include cloud data security, intrusion detection and situation awareness.

Wang Kun was born in 1975. He received a M.S. and Ph.D. degree in Zhengzhou Information Science and Technology Institute, Zhengzhou in 2004. He is now an associate professor at the Henan Province Key Laboratory of Information Security, Zhengzhou Information Science and Technology Institute. Her research interests include situation awareness, cloud security and neural network.

Zhang Yuchen was born in 1977. He received a M.S. and Ph.D. degree in Zhengzhou Information Science and Technology Institute, Zhengzhou in 2012. He is now an associate professor at the Henan Province Key Laboratory of Information Security, Zhengzhou Information Science and Technology Institute. Her research interests include situation awareness, information security and risk assessment.

Wang Shuo was born in 1991. He is receiving a M.S. degree in Zhengzhou Information Science and Technology Institute, Zhengzhou. Her research interests include cloud data analysis, intrusion detection, and situation awareness.