A Method of Threat Evaluation for Mobile Network

Wang Bailing*, Li Shang, Qu Yun, Wang Xiaopeng and Liu Yang

Harbin Institute of Technology at Weihai, Weihai, Shandong, 264209
**wbl@hit.edu.cn*

Abstract

A cloud model was introduced to evaluate mobile network threat. As the qualitative knowledge representation and uncertainty handling method, the transform between qualitative concepts and their quantitative expressions become much easier and interchangeable. It bridges the gap between the rigidity of a mobile network system and the uncertainty of human thinking. Conclusion is given at last; it shows that the cloud model is effective and capable of directly analyzing the characteristics of mobile network threat evaluation.

Keywords: *network security, mobile network, threat evaluation*

1. Introduction

Along with the development of the computer technology and the prevalence of Internet, computer has become more important in the people's life. At the same time, the threat for the mobile network is increasing steadily. Mobile network is just like the sword with two blades. It benefits the scientific researcher, and even the common people, but it make the threat increase more quickly and more widely.

The type of the attack can be divided into two groups: the host-based attack and the network-based attack according to the network behaviors. The traditional host-based attack can hide itself in the normal program, and copy itself along with the people's operation. Accompany the spread of the host-based malcode; a new attack occurs, which most relies on the network. The new malcode attacks the weakness on the mobile network to exhaust the resource, so we call it network-based attack. The malcode has more ability to spread itself and do harm to the mobile network than the host-based one. Once a network-based malcode is embedded in a common program, it will spread through the mobile network very quickly. It dresses up itself not to be detected as it spreads, and it spreads more quickly than the traditional host-based one.

The work to detect and control the Threat Situation of Mobile Network (TSMN) has outspreaded accordingly, and we have implemented a system which depicted how to watch and control the threat situation of computer network in detail [1]. And we found that the evaluation of the computer network threat was a key to the watch- control system. However, most previous methods have some common shortcomings. Firstly, these methods usually give one or a sequence of numbers as predictive results.

The quantitative results are difficult for the users to understand, while qualitative knowledge may be more robust and easier to understand, but difficult to express and calculate in computers. Secondly, fewer methods have dealt with the different influences on evaluation of TSMN. To make the results more precise, it is very important to distinguish the influences of various factors. Therefore how to represent this qualitative knowledge and how to maintain the uncertainty of inference is difficult but necessary in TSMN evaluation. We have proposed

a network malcode precaution method in [2], which is a quantitative analyzing method of epidemic situation.

At this junction, a new method to evaluate the TSMN based on cloud is proposed. The theory of cloud techniques is presented in Section 2. Then, Section 3 will expound the new mechanism on how to calculate the qualitative influence of the TSMN and how to assess the situation with cloud-based technology. Furthermore, Section 4 gives the results of experiment and corresponding curve. Lastly, conclusion and discussion are presented in Section 5.

2. The Actuality of Cloud Technology

Cloud model is an uncertain transition model that bridges the gap between the qualitative analysis and the quantitative by language value, as in [4]. Cloud is made of a lot of cloud drops, and every drop is an instance that expresses the qualitative concept in quantity. And in the last ten years, the thinking of the cloud technology has been consummated and used in many evaluation systems and prediction systems successfully, *e.g.*, reliability evaluation of electronic products in [3], reliability count evaluation of computers in [4], representation and prediction of K-line in [5], and so on as in [6, 7]. A more successful appliance of cloud technology is the inverted-pendulum, which is a hard problem in fuzzy control, and the result of the application is surprised.

Let U be the set U={u}, as the universe of discourse. Let $\tilde{A}$ be a qualitative term associated with U. The membership degree of u in U to the term $\tilde{A}$, $\mu_{\tilde{A}}(u) \in [0,1]$, is a random number with a stable tendency. The cloud of $\tilde{A}$ is a mapping from the universe of discourse U to the unit interval [0,1], and $\mu_{\tilde{A}}(u)$ is the degree of u belonging to the term $\tilde{A}$ [4]. The mapping from u U to the interval [0,1] is a one-point to multi-point transition, which shows the uncertainty: fuzziness and randomness of an element belonging to the term. So the degree of membership of u to the qualitative term $\tilde{A}$ is a probability distribution rather than a fixed value.

The cloud can be characterized by three parameters: A (Ex, En, He). The expected value Ex points out the center of gravity of a cloud. And the entropy En is a measure of the fuzziness of the concept over the universe of discourse. The universe of discourse [Ex $\pm$ 3En] is the main universe, in which the most elements can be accepted by the term A. The hyper entropy He is a measure of the uncertainty of the entropy En. And the larger the value of He, the more random the set of membership degrees is distributed. A set of cloud drops can be generated according to the digital characteristics Ex, En, He. Cloud include one-dimensional cloud, two-dimensional cloud, and multi-dimensional cloud, as in [5] and [8].

A one-dimensional cloud to the range of the affected computer in a network is proposed in Figure 1, and the parameters Ex, En, He of moderate range cloud are labeled. From the left to the right, the range and the parameters are described as the following:

Small Range: A (0, 50, 0.5);
Moderate Range: A (200, 50, 0.5);
Big Range: A (500, 100, 2);

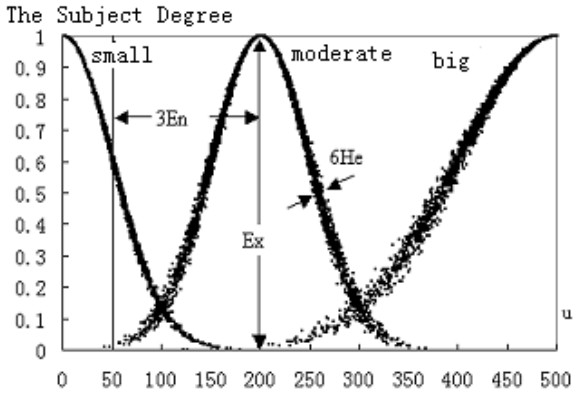


Figure 1. The Cloud-based model of the Range of the Affected Computers

The qualitative meaning is very obvious: along with the increase of the number of the affected computers, the membership degree of u in U to the term A (0, 50, 0.5) decreased and to A (200, 50, 0.5) increased accordingly; if the number of the affected computers is greater than 200, the membership degree of u in U to the term A (200, 50, 0.5) decreased and to A (500, 200, 2) increased along with the increase of the number.

3. Cloud-based Mathematics Model of TSMN

The digital characteristic of the cloud can be characterized by three parameters: the expected value Ex, the entropy En, and the hyper entropy He, so we can evaluate TSMN if we calculate the values of the three parameters. The following is the process to analysis the situation with quantitative value and to generate the cloud model.

A. The Quantitative Analysis of TSMN

Definition 1: The malcode affect-scope-index

1) Once one mobile end is infected, it's scope-index is μ=1.

2) Once one mobile end repeater s_i is infected, and besides, the set of the mobile end, which accesses the mobile repeater s_i directly, is $C_{Si}=\{c_{i0}, c_{i1},\ldots\ldots, c_{in}\}$ and the set of the mobile repeater, which accesses the mobile repeater s_i directly, is $S_{Si}=\{s_{i0},s_{i1},\ldots\ldots,s_{im}\}$, and then the scope-index of the mobile repeater s_i can be defined as:

$$\mu = \left| C_{Si} \cup \left(\bigcup_{j=0}^{m} C_{Sj} \right) \right| \tag{1}$$

3) Once one mobile communication network is infected, and besides, the infected mobile end set is $C=\{c_0, c_1, \ldots\ldots, c_n\}$, the infected mobile repeater set is $S=\{s_0,s_1,\ldots\ldots,s_m\}$, and the mobile end set that accesses s_i in S is $C_{Si} = \{c_{i0}, c_{i1}, \ldots\ldots, c_{ih}\}$, the mobile repeater set that accesses si in S is $S_{Si} = \{s_{i0}, s_{i1}, \ldots\ldots, s_{ik}\}$, and then the scope-index of the subnet can be defined as:

$$\mu = \left| C \cup \left(\bigcup_{i=0}^{m} \left[C_{Si} \cup \left(\bigcup_{j=0}^{k} C_{Sj} \right) \right] \right) \right| \tag{2}$$

Definition 2: The malcode destruct-grade-index

The destruct-grad-index is θ （ 0 < θ < 3 ）.

1) If the malcode wrecks something undesignedly, θ should be smaller than 1.
2) If the malcode changes the configuration, which is not very important, and the content can be recovered easily, and besides, the tiger is nondestructive, θ should be smaller than 2 and be bigger than 1.
3) If some file is modified or the traffic of the mobile repeater is very high, and even there are large-scale losing, which is not recoverable, and the tiger is destructive, θ should be smaller than 3 and be bigger than 2.

Definition 3: The malcode spread-ability-index

The spread-ability--index is σ （ 0 < σ < 3 ）.

1) The malcode, just like code red, is provided with some objective, and the menace cannot be controlled in some case, σ should be smaller than 3 and be bigger than 2.
2) If the malcode spread out only by downloading files or by copying files, σ should be smaller than 2 and be bigger than 1.
3) In other case, σ should be smaller than 1.

B. The Value of The Cloud Parameters In TSMN

Summing up the Definition 1~3, Five ranks, π={Not serious, Serious slightly, Serious, Very serious, Extremely serious}, are proposed accordingly and we can have the following rules as the qualitative rule set:

Rule 1: IF θ<=2 AND σ<=2 AND μ is small range, Then π is not serious

Rule 2: IF θ<=2 AND σ<=2 AND μ is moderate range, Then π is serious slightly

Rule 3: IF θ<=2 AND σ<=2 AND μ is big range, Then π is serious

Rule 4: IF θ>=2 OR σ>=2 AND μ is small range, Then π is serious slightly

Rule 5: IF θ>=2 OR σ>=2 AND μ is moderate range, Then π is serious

Rule 6: IF θ>=2 OR σ>=2 AND μ is big range, Then π is very serious

Rule 7: IF θ>=2 AND σ>=2 AND μ is small range, Then π is serious

Rule 8: IF θ>=2 AND σ>=2 AND μ is moderate range, Then π is very serious

Rule 9: IF θ>=2 AND σ>=2 AND μ is big range, Then π is extremely serious

Then we can generate a cloud with Rule 9. Let μmax be the max number of μ, then the parameters of the cloud μ are described as the following:

$$\begin{cases} Ex = \mu_{\max} \\ En = \mu_{\max} / 3 \\ He = k \end{cases} \tag{3}$$

Let Φ be the product of θ and σ, and Φ_{max} is the max number of Φ, then the parameters of the cloud Φ are described as the following:

$$\begin{cases} Ex = \phi_{\max} \\ En = \phi_{\max} / 3 \\ He = h \end{cases} \quad (4)$$

The value of the parameter He can be adjusted according to the malcode type and the environment of the network. The bigger of He, the more the drops dispersed! The detail of the cloud refers to 4 Experiment.

C. The Implement of The Cloud-based Generator

Input: φ_{max}, μ_{max}

Output: *Some 3-D Drops (Xi, Yi, Zi), i = 1..N*

```
CloudGen (φmax, μmax)  {
        Ex1 = μmax;
        En1 = μmax / 3;
        He1 = En1/100;
        Ex2 =φmax;
        En2 =φmax/3;
        He2 = En2/100;
        for (i = 1; i < N; i++)
        {
                //Call The Normal Random Number Generator.
                X1i = RNORM (Ex1, En1);
                En1i = RNORM (En1, He1);
                X2i = RNORM (Ex2, En2);
                En2i = RNORM (En, He);
                Z1i=exp(-(X1i-Ex1)*(X1i-Ex1)/(2*En1i*En1i));
                Z2i= exp(-(X2i-Ex2)*(X2i-Ex2)/(2*En2i*En2i));
                Zi = Z1i * Z2i;
        }
}
```

4. Experiment

As the formulas in part 3, we give an example of the cloud-based evaluation model. According to formula 3 and formula 4, and let μ_{max}=500, the cloud is described as following:

$$C\mu = \mu\ (500, 167, 2); \quad (5)$$

$$C\varphi=\varphi(9, 3, 0.03); \quad (6)$$

Then the final cloud of the TSMN is described as following:

$$C\ (\mu,\varphi) = C\mu \cap C\varphi = C((500,9),(167,3),(2,0.03)) \quad (7)$$

Figure 2 is the cloud of the formula 7. But in our system, we are only concerned about the ascending half cloud, where $\mu < \mu_{max}$ and $\varphi < \varphi_{max}$.

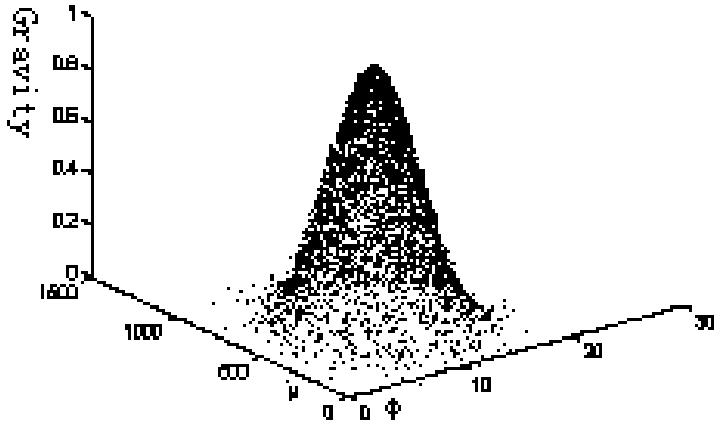
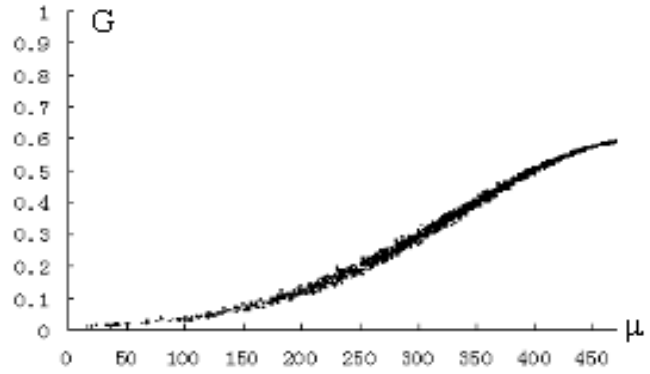


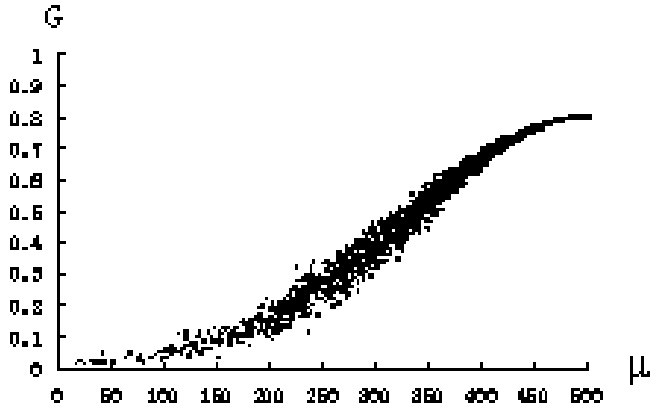
Figure 2. The Gravity Cloud of TSMN

In order to explain the characteristic to use the cloud-based mode to assess TSMN, we give some clouds when Φ is a definite value (referring to Figure 3 I, II and III). As shown in Figure 3, we can see the results predicted by our new cloud methods are precise. We can summarize some characteristics with cloud model to evaluate TSMN referring to Figure 3. Firstly, the drops in chart III of Figure 3 seem more dispersed than chart I and chart II. Because the malcode in the third situation is more ability to spread itself and destroy the environment than the first one, and it can do a large damage even if there is a small range of affected computers. Secondly, referring to Chart I in Figure 3 where Φ is small, we can see that the smaller the value of μ, the smaller of the value of Gravity. Thirdly, the speed increased of Gravity is a remarkable characteristic in cloud model (Refer to Chart I in Figure 3). When μ is very small, *e.g.*, μ<20, which means the number of the affected computers is small, the source of the network malcode is small. So the speed increased of Gravity is slow.

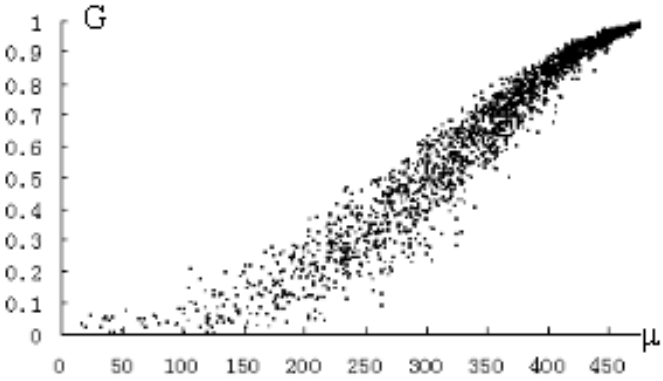
As μ increases, the larger the malcode source, the faster the speed increased of Gravity. But when μ is bigger than 400, the speed increased of Gravity decreased, because the number of the computers that can be affected is few.



I. Φ = 4



II. Φ = 6



III. Φ = 9

Figure 3. A Definite Value of Φ

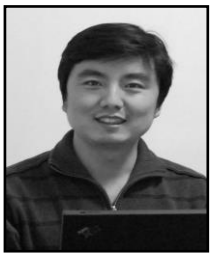
5. Conclusion

In brief, design a TSMN evaluation model and make a qualitative analysis of TSMN is important and necessary in TSMN prediction. The cloud methods not only bridge the gap between quantitative and qualitative knowledge, but also between different granularities of knowledge. Particularly, the soft inference based on cloud methods can not only maintain the uncertainty of the linguistic atoms, but also enhance the robustness of the predictive results. There is extensive real practical value to use the cloud technology introduced in this paper to assess TSMN.

References

[1] B. L. Wang, B. X. Fang and X. C. Yun, "The distributed broadband network malcode precaution system", Journal of China Institute of Communications, vol. 24, **(2003)** August, pp. 225-230.
[2] B. L. Wang, B. X. Fang and X. C. Yun, "The precaution of the network malcode and the quantitative analysis of epidemic situation", The second Internal Conference on Machine Learning and Cybernetics, Xi'an, **(2003)**.
[3] X. J. Xiang, "Research on reliability evaluation of electronic products under environmental conditions", Intelligent Control and Automation, vol. 4, **(2004)**, pp. 33146-3149.
[4] Q. Fu, Z. Cai, Y. Wu, Z. Li, "A Novel Reliability Evaluation Method for Series−Parallel Systems Based on Cloud Model", Journal of Computational Information Systems, vol. 6, no. 10, **(2010)**, pp. 3237-3245.
[5] F. Yang, R. Jiang and D. Y. Li, "Representation and Prediction of K-line with Cloud Method", The fifteenth Graduate-Nanjing Conference on Communication, Nanjing, **(2000)**.
[6] D. D. Lie, X. H. Chen and Z. H. Lou, "Analysis on characteristics of spatial-temporal precipitation distribution based on cloud model", Journal of Hydraulic Engineering, vol. 40, **(2009)** July, pp. 850-857.
[7] H. B. Zhang, Q. Q. Pei and J. F. Ma, "An Algorithm for Sensing Insider Threat Based on Cloud Model", Chinese Journal of Computers, vol. 32, **(2009)** April, pp. 784-792.
[8] Z. H. Yang and D. Y. Li, "Planar model and its application in prediction", Chinese Journal of Computers, vol. 21, **(1998)** November, pp. 961-969.
[9] H. Kraiem, A. flah, M. B. Hamed and L. Sbita, "High Performances Induction Motor Drive Based on Fuzzy Logic Control", Published Papers for International Journal of Control and Automation, vol. 5, **(2012)**, pp. 1-12.
[10] N. Satuluri and M. R. Kuppa, "A Novel Class Imbalance Learning Using Intelligent Under-Sampling", Published Papers for International Journal of Database Theory and Application, vol. 5, **(2012)**, pp. 25-36.
[11] M. M. Hasan, "Performance Comparison of Wavelet and FFT Based Multiuser MIMO OFDM over Wireless Rayleigh Fading Channel", Published Papers for International Journal of Energy, Information and Communications, vol. 3, **(2012)**, pp. 1-8.

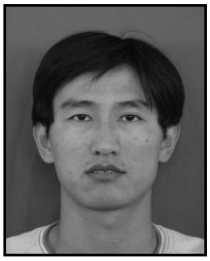
Authors



Wang Bailing is working for Harbin Institute of Technology (abstract as HIT) as an associate professor. He got the Ph.D. degree from HIT in 2006. His research is mainly on information security, network security, parallel computing.

Li Shang is a master student in school of computer science and technology of Harbin Institute of Technology. His research is mainly on network security.

Qu Yun is working for Harbin Institute of Technology as an engineer. She got the master degree from HIT in 2012. Her research is mainly on network security and application technology.



Wang Xiaopeng is working for Harbin Institute of Technology as an senior engineer. He got the master degree from HIT in 2012. His research is mainly on network security and application technology.

Liu Yang, Associate Professor, Liu Yang, his research fields include Network information Security Technology, Internet of Things Security Technology, *etc.* He has participated in many projects of Ministry of Information Industry and National Science, and he has published over 20 academic papers in journals and conferences both home and abroad.