A Method of Evaluating Network Attack Probability based on TWDS

Zhengxing Huang
Officers College of Chinese Armed Police Force, 610213, China

Abstract

According to the problem of omitting the deflection caused by response time of different network security equipments in the research of network security situation awareness, Time Window D-S evidence theory is improved from traditional D-S evidence theory. Then the method of evaluating network attack probability is proposed. Experiments show that TWDS has higher accuracy than traditional D-S, and achieved good ideal detection of network attack.

Keywords: Time Window; Network Security; Attack Probability; D-S Evidence Theory

Introduction

Network security situational awareness has become a hot topic in the area of network security research in recent years for its ability to fuse multi-source information. In the research of network security situational awareness, D-S evidence theory is often used to fuse information from different network security equipments. Quantitative Evaluation Model for Network Security Threats Situation[1] introduces D-S evidence theory to fuse the information of network performance. Under the Network Security Situation Awareness Model Based on Multi-source Fusion[2], D-S evidence is improved and used to fuse multi-source information. In the research of Network Security Situation Assessment Model Based on Time Parameter[3], time-varying D-S evidence is proposed to fuse the multi-sensor evidence. Novel Multi-heterogeneous Sensor Based Network Security Situation Awareness Model[4] uses improved D-S evidence theory to fuse security data submitted from different sources combing with AHP algorithm. In the research on network security situation forecast[5], a method ,which can forecast future network security situation with fusing history and current situation, is proposed based on D-S evidence theory. In article[6], a quantitative awareness of network security situation based on fusion is proposed, which uses improved D-S evidence theory to realize multi-source fusion. Aiming at solving the problem of lack of correctness and rationality in situation assessment, article[7] set up the situation index identification space and evaluation criteria based on the D-S evidence theory. Although above models have used D-S evidence theory to get good fusion effect, they all still have the same deficiency of omitting the deflection caused by the response time of different network security equipments.

Making up for the deficiency from above analysis, in this paper, TWDS(Time Window D-S) is improved from traditional D-S, and the method of evaluating network attack probability is proposed. At last, the experiment proves the validity of this method.

Proposition of Time Window D-S Evidence Theory

D-S evidence theory in network security assessment is used to fuse alarm information, and the purpose of TWDS(Time Window D-S) proposed in this paper is to improve the fusion accuracy.

The full name of D-S evidence theory is Dempster/Shafer evidence, and Dempster was the man who proposed D-S evidence theory, while Shafer was the man who promoted the theory. Compared with Bayesian theory of probability, D-S evidence has less constraints and stronger ability to express uncertainty. In this paper, related concepts are as follows:

(1) Identification Framework. Identification Framework is a complete set which is composed of mutually incompatible basic propositions. These propositions can represent all possible answers to a problem, and only one answer is correct.

(2) Proposition. Proposition is the subset of Identification Framework.

(3)m Function. It is the assigned trust degree of each proposition, also known as the basic probability assignment. m(A) is a basic probability number, expressing the extent of A being trusted.

If the basic belief assignment from multi-sensors is obtained in a scene, a new probability distribution can be got with D-S evidence theory. The whole fusion process is shown in figure 1.

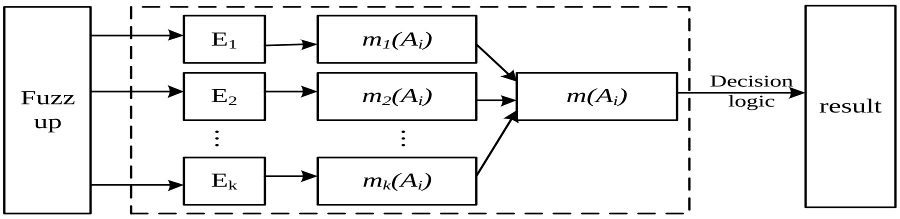

Figure 1 the process of fusion with D-S evidence theory

In figure 1, E_1, E_2, …, E_k is k attacks detected by network security detection device. $m_1(A_i)$, $m_2(A_i)$, …, $m_k(A_i)$(i=1,2, …,n, n propositions) respectively represent the basic probability assignment of k attacks to a proposition A_i, and $m(A_i)$ is a new probability distribution.

Dempster synthetic formula:

$$m(\varnothing) = 0$$

$$m(A_i) = \frac{1}{1-K} \sum_{\substack{A_1,\cdots,A_n \subseteq \Theta \\ A_1 \cap \cdots \cap A_n = A}} \prod_{1 \le i \le k} m_k(A_i), A \ne \varnothing$$

$$K = \sum_{\substack{A_1,\cdots,A_n \subseteq \Theta \\ A_1 \cap \cdots \cap A_n = A}} \prod_{1 \le i \le k} m_i(A_i)$$

K is a normalization factor， which can reflect the extent of evidence conflict.

In order to avoid the conflict in D-S evidence theory, Sun Quan[8] proposed a improved D-S evidence theory, its synthetic formula is

$$m(h) = \prod_{i=1}^{k} m_i(h) + Kq(h) \qquad (1)$$

$$K = 1 - \prod_{1 \le i \le k} m_i(h) - \prod_{1 \le i \le k} m_i(\bar{h}) \text{ ， } q(h) = \frac{1}{n} \sum_{i=1}^{k} m_i(h)$$

Although improved D-S evidence theory has avoided the conflict, it is still necessary to study on what alarm information is regarded as evidence.

In traditional evidence fusion process, the time of network security equipments recording alarm information is regarded as the time of attack happening. But in fact, different equipments have different response time, so it leads to two problems bellow:

(1) Two or more logs recorded at same time may not record a same attack;

(2) Two or more logs recorded at different time may record a same attack.

Above two problems easily lead to omitting alarm information. In order to solve these two problems, Time Window is introduced in this paper.

The definition of TW (Time Window) in this paper is the longest time among the response time of all network security equipments to an attack under a certain environment. And the response time in this paper is the time for network security equipments to record log after an attack once happen.

When using D-S evidence theory to fuse alarm information, only the information recorded during time window can be included. Therefore, D-S evidence theory in this paper is called Time Window D-S evidence theory, and its shortened form is TWDS. In TWDS, the value of k in formula (1) is depending on how many alarm information recorded in the time window.

Up to now, TWDS is proposed in this paper.

Method of Evaluating Network Attack probability

Step one: get recognition framework. Set two basic incompatible propositions as recognition framework for D-S evidence theory. Because D-S evidence theory is used for calculating network attack probability, its two incompatible propositions respectively are: If a network attack is happening, it is h; if a network attack is not happening, it is $\bar{h}$. Above all, recognition framework, $\Theta = \{h, \bar{h}\}$, is got.

Step two: get basic probability assignment. With known knowledge and experience, the probability of all alarm information, detected by network security equipments under a certain network environment, supporting an attack's happening should be known. In this step, which alarm information should be included is depending on the thought of Time Window proposed in section two.

Step three: get the network attack probability. In this step, use D-S evidence theory to fuse each probability got in step two. And the value of fusion result can evaluate network attack probability.

Test results

The aim of bringing forward TWDS is to solve the two problems mentioned in second section. So in this section, the rationality of TWDS will be proved and expressed. An experiment is designed in NS2. And the network security equipments used is listed in table 1.

Table 1 Information of equipments in this experiment

Equipments' name	The function of equipment
server	Provide service, generate logs
IDS	Detect attack, generate logs
firewall	Defend attack, generate logs

The experiment scenario is that an attack is started at t_1, and then each network security equipment generates alarm log. The scenarios can be described as figure 2.

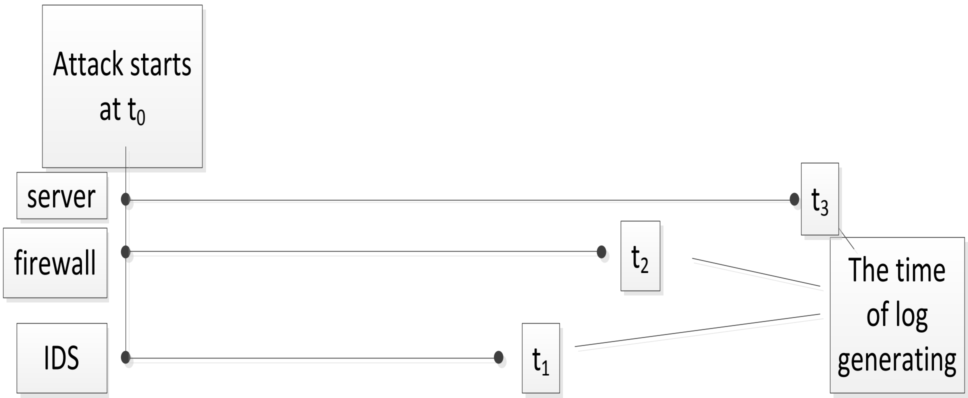

Figure 2 attack scenarios

To this experiment scenario, the attack probability got with traditional D-S evidence theory and TWDS is shown in figure 3,

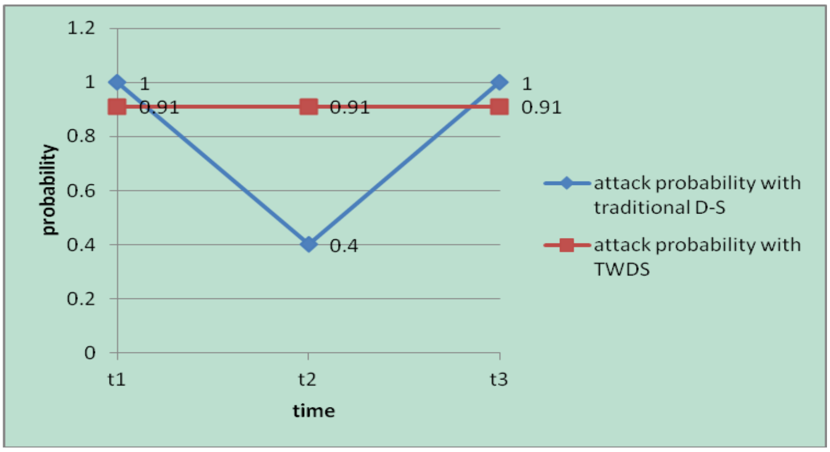

Figure 3 attack probability with two methods

At t_1 and t_3, traditional D-S and TWDS both have high probability, they can detect the attack well. But at t_2, TWDS can still detect the attack exactly while the probability got with traditional D-S is too low.

The reason why TWDS has better result is that the objects for TWDS to fusion are alarm information during time window, which includes all related alarm information. Therefore, TWDS can avoid omitting alarm information.

Conclusion

Based on the analysis of D-S theory applied in network security as the foundation, introduced Time Window, proposed TWDS to avoid omitting important information, designed the method of evaluating network attack probability . At last, Experiments show that TWDS has higher accuracy than traditional D-S, and achieved good ideal detection of network attack.

References

[1] Zhu Lina, Zhang Zuochang, Feng Li. Research on Hierarchical Network Security Threat Situation Assessment. Application Research of Computers[J]. 2011, 28(11) 4303-4306.

[2] Liu Xiaowu, Wang Huiqiang, Yu Jiguo, Cao Baoxiang. Network Security Situation Awareness Model Based on Multi-source Fusion. Journal of PLA University of Science and Technology (Nature Science Edition)[J]. 2012, 13(4) 403-407 .

[3] Meng Jin, Xu Jia, He Jialang, Zhang Hong. Network Security Situation Assessment Model Based on Time Parameter. Application Research of

Computers[J]. 2012, 29(10) 3820-3823.

[4] Zhang Yan, Guo Shize, Huang Shuguang, Wang Yongyi. Novel Multi-heterogeneous Sensor Based Network Security Situation Awareness Model. Application Research of Computers[J].2012, 29(1) 286-289.

[5] Shi Bo, Xie Xiaoquan. Research on Network Security Situation Forecast Method Based on D-S Evidence. Computer Engineering and Design[J]. 2013, 34(3).

[6] Liu Xiaowu, Wang Huiqiang, Lv Hongwu, An Shuzhao. Quantitative awareness of network security situation based on fusion. Journal of Jilin University(Engineering and Technology Edition). 2013, 43(6).

[7] Tang Chenghua, Tang Shensheng, Qiang Baohua. Assessment and Validation of Network Security Situation Based on DS and Knowledge Fusion. Computer Science[J]. 2014, 41(4) 107-110,125

[8] Sun Quan, Ye Xiuqing, Gu Weikang. A New Combination Rules of Evedence Theory. Journal of Software[J]. 2000(08) 117-119.