Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Computer Science 17 (2013) 530 – 536

Procedia Computer Science

Information Technology and Quantitative Management (ITQM2013)

A Multi-Level Analysis Framework in Network Security Situation Awareness

Haoliang Zhang*, Jinqiao Shi, Xiaojun Chen

Institute of Information Engineering, Chinese Academy of Sciences,
Min Zhuang Rd 89# A3, Beijing 100093, China

Abstract

Network Security Situation Awareness (NSSA) technology has been extensively studied in multi-data analyzing research these years. In this paper, we use a historical war story to explain the key points in situation awareness, present the conceptualizations and challenges aspects of NSSA, and discuss the methodologies of solving these problems. We provide an evaluation method for network security situation, and represent how to apply this method to NSSA. A multi-level analysis framework for NSSA is presented to demonstrate the advantages and effectiveness by using this method.

© 2013 The Authors. Published by Elsevier B.V.
Selection and peer-review under responsibility of the organizers of the 2013 International Conference on Information Technology and Quantitative Management

Keywords: situation awareness, multi-level analysis, situation assessment, data fusion ;

1. Introduction

Network Security Situation Awareness (NSSA) has been studied for more than ten years, and we have derived many definition and descriptions about this technology, while we also see that the research is in its early stages and has some critical issues to be resolved. Firstly, NSSA is a conception pertinent to assessing and showing the global and comprehensive situation of network security[1][2][3][4], so it requires people to collect all kinds of data and analysis for as many dimensions as possible in order to reflect the macroscopic pictures. Secondly, a uniform standard for estimating network security situation is needed[5][6][7]. Thirdly, there is a severe lack of methodologies to form comprehensive perception of the current network security situation from the multi-sources data[8][9][10]. Lastly, it is very hard to predict the future trend of network security situation effectively and even precisely[11][12][13][14].

* Corresponding author. Tel.: +86-010-82546723.
E-mail address: zhanghaoliang@iie.ac.cn.

1877-0509 © 2013 The Authors. Published by Elsevier B.V.
Selection and peer-review under responsibility of the organizers of the 2013 International Conference on Information Technology and Quantitative Management
doi:10.1016/j.procs.2013.05.068

Fortunately, the NSSA research community have mainly been consistent with Endsley's definition on SA,, see Fig 1(a), which is considered as a three-level processing model of perception, comprehension and projection. On the basis of Endsley's work we would like to do some research on refining each step process in network security area to gain a global awareness.

This paper is an endeavour to discuss how to do assessment on a kind of situation, including how to choose key elements and how to organize the elements for creating a coordinate for evaluation, and then to apply this method to the network security field for the purpose of finding an appropriate logical process in NSSA. Finally, we propose a multi-level analysis framework in NSSA which provides a prototype of comprehension process and is flexible enough to extend its analytical capabilities.

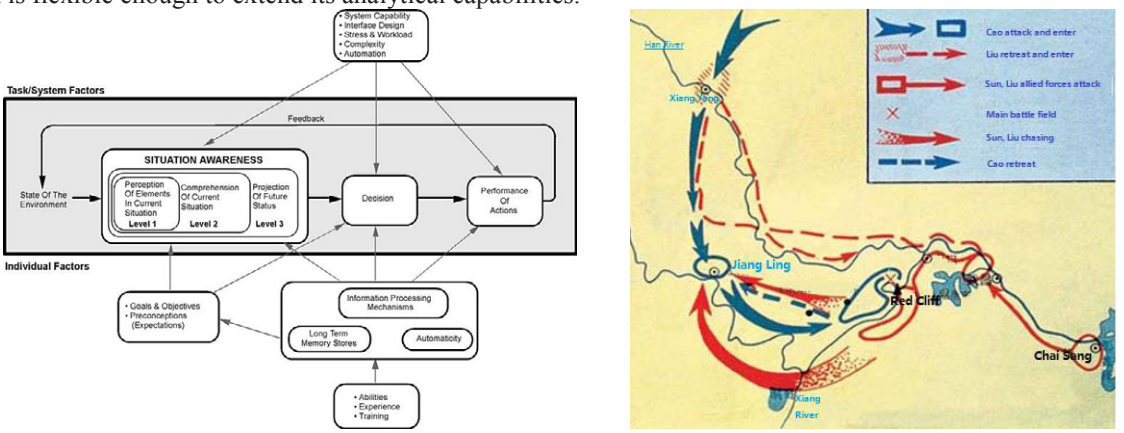

Fig. 1. (a) Three-level Model of SA; (b) Map of the Battle of Red cliff

2. A War Example for Assessment in Situation Awareness

At the very beginning Situation Awareness comes from the wars, so we take a classic war story, the Battle of Red Cliff, as an example to explain the key points in each level of SA. It was fought in 208 AD between the allied forces of Liu and Sun and the superior forces of Cao, see Fig 1(b). Firstly, Cao sent Sun a letter boasting of commanding 800,000 men and demanding Sun's surrender. Then, Sun convened all his counselors to assess the situation, and some advocated surrender citing Cao's overwhelming numerical advantage, however, the other Sun's chief commander presented arguments to persuade Sun to agree to the alliance against the Cao's forces. How did Sun make this most critical decision? What had he aware about the situation?

- Numerical Analysis: Although Cao had boasted command of 800,000 men, Sun estimated Cao's actual troop strength to be closer to 220,000, including 150,000 from the far north and 70,000 surrendered recently from deceased former-lord. And with the 15,000 soldiers that Liu had gathered, the alliance consisted of approximately 95,000 soldiers, including 50,000 marines who were trained and prepared for battle.
- Influencing Factors Analysis: We compared the main factors that have effect on how much potential power can be played out between the two forces in the following table,

Table 1. Influencing factors comparison

Influencing Factors	Forces of Cao	Forces of the Alliance
Tactical Factor	Unfamiliar with naval warfare	Familiar with naval warfare
Health Factor	Tied of long run and fall ill	Immune for tropical

	by tropical diseases	diseases
Moral Factor	Uncertain Loyalty	Prepared for battle
Commander Factor	Cao is Suspicious	Sun trust subordinates

- The results expected: After the comparison on influencing factors of both sides, Sun got to know that though he does not have equivalent size of ground forces, he had greater advantages on the other factors that listed in table1, such as they are better adapted to the environment and their forces have more confidence in each other, to name a few. He realized that to win all these unviewed influencing factors were real battles, which could reverse the balance of strength for the two sides. Then he acquired the reasonable expectations that he could win the battle if he manage to find the defects of the enemy forces and scale down enemy's strength essentially by chasing victories on the factors he had advantages, and when he get a chance to organize superior fighting capacity, then he will win, see Fig 2(a). However, he should also be clear about the risks he faced with. The balance of friend-and-foe strength kept changing all the time, and the decisive factors varied according to the changes of environmental healthy and subjective factors, so the result expectation also involved the real risk that if the enemies get chances to take occasional advantage, then the balance will shift into the opposite direction.

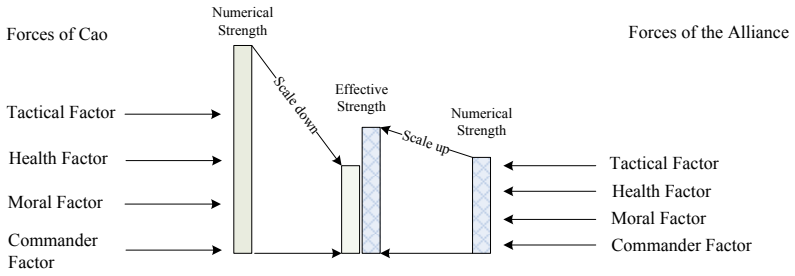

Fig. 2. (a)effective strength balance;

The above three steps of Battle Situation Awareness is corresponding to the three-level SA model. They can be concluded as following points:

- **Perception**: Recognize the enemy, then detect and determine the basic properties (e.g. the basic forces power and the structure of the troop) and the effective factors(e.g. the influencing factors for forces strength) of the target objects including both enemies and themselves,
- **Comprehension**: Identify main influencing factors and organize these factors to evaluate how much impact will have on the current situation (e.g. the balance of the effective strength for both sides) based on action rules. This kind of evaluation will lead to a changing status of current situation along with the relevant factors playing roles in progress. The action rules varied very much for each factor, but they can be evaluated by how much do they have effect on the core strength,
- **Projection**: Make assumptions of all the branches that can be take based on current situation status and give assessment on each critical point on the path. We can view it as a decision tree, the node of tree contains a core status which reflects the balance of favorable and unfavorable strength, the next node depends on the changes of important factors that can be affected by our decisions or some outer impacts.

From these processes we note that the input of assessment is the factors and relations derived from perception step. And the output of assessment is a comparison of two strengths, direct mark of the situation stat, which plays a key role in both comprehension step and projection step. In the comprehension step, assessment show us what the current situation is, and in the projection it step show us what situation will be if some particular factors change.

So if we want to assess the situation we need to clear the important points as following:

- **Evaluation standard**: situations always have its two sides for us, good side and bad side, and we need to clarify the core strength of the two sides, and the comparison of these two strengths mainly compose the evaluation standard.
- **Main factors**: there are many factors that have important impact on the evaluation standard contained in the enemy side, our side and also environment. Some of the factors can scale up the power to be played out, some may play a restricting role.
- **Evaluation rules**: these rules reflect the relation between each evaluation factor and the evaluation results and even describe how to combine multi-factors together to raise effect on the final results. These rules generally direct the calculation of the situation exponent which represents the comprehensive stat of the specified situation.

While all these three points have been identified and investigated, it is feasible to gain the comprehension of any kinds of situations by evaluating the current factors and forecast the changes of situations by evaluating the possible factors in the near future. Hence, we can regard the data generated by Perception as the input of evaluation, and regard the output of evaluation as the measure of Comprehension and Projection result.

3. Apply evaluation methodology in Network Security Situation Awareness

Internet is a huge device for people to transfer information. It connects all types of computing equipment together by forming a virtual space which is named cyber space. The security situation in this virtual world is called Cyberspace Situation or Network Security Situation. We are dedicated to evaluate the security situation of cyberspace by the methodology aforementioned. Before evaluation we have to clear and define the environment and the working principle in the cyberspace. Then we explore through this virtual environment to find out the contrary strengths that can be chosen as the evaluation exponent, the factors that could affect situation notably, and the rules that every factors comply within cyberspace.

3.1. Model on Network Security Situation

Network environment is very complex, it consists of all kinds of computers, operating systems, services and programs, while it also can be simply concluded as a system to transfer data. By defining its single working pattern as transferring data, the network environment can be simplified as a world made up of many castles which are connected with highways, in the castle there are some houses filled with gold coins and some workers working in the house, their work is very easy, just send letters out to another place that connected by roads, see Fig 3(a).

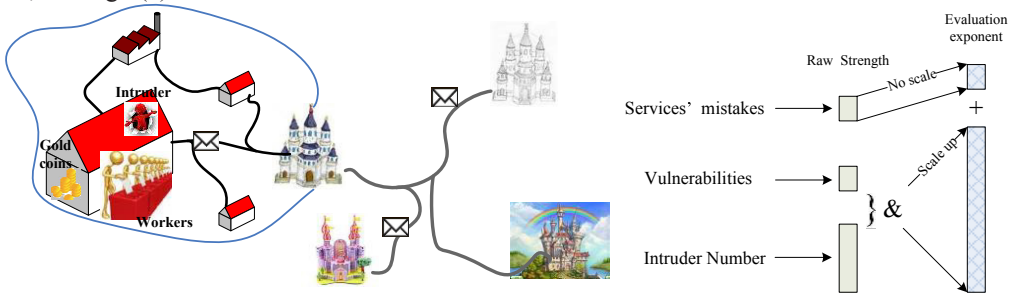

Fig. 3. (a)network environment model; (b) Calculate NSSA evaluation exponent

If the workers make mistake then they may send out a gold coin, if they have weakness then they may invite in some intruders who are intended to steal the gold coins or be controlled by someone to send out the gold

coins.

In this model, we consider the local networks as a castle, view the computers as houses and view the operating system and programs as the workers. The network security problems are abstracted as a mission to keep the gold safe in its house.

3.2. Evaluation of Network Security Situation

The network security situation is always studied in a local network background, so we set the discussion in a local network environment. Based on the model aforementioned, the key point of measure network security situation is how well we can keep gold safe, and on the opposite side it also can be measured by how easily to steal the gold. Because it is hard to measure how well we keep gold safe, and the possibility of the gold coins be stolen is measurable, so we choose the later approach to do the evaluation.

The three main factors to lead to gold coins lost include the frequency of each worker makes mistake, the weakness of the workers who are easy to control. The frequency of workers to make mistake is a statistic data which is relatively stable. The weakness of the workers means they are more easily to take control of, and if the new weakness ranked a lower level, then the more intruders will have the ability to take control of the workers, so it plays a scale up role in the calculation.

Evaluation of the Network Security Situation is a process to count out the possibility of lost data from the internal users, and combine the vulnerabilities and historical intruders' quantity scale to speculate on the possibility of being controlled by intruders. At last we add the two evaluation exponents together as the result of evaluation, see Fig 3(b).

This theoretical method is a direction of getting comprehensive knowledge of Network Security Situation. It emphasizes the importance to form logical relation among the situation factors other than mixing all the low level data together via variety of analysis methods. As we do evaluation based on a higher level knowledge, we encounter new challenges as following:

- **Identification**: situation factors is a virtual object to be identified, so there have to be some specific identification methods for every kinds of low-level data to assign data to the right factor objects;
- **Relation rules**: Network environment is a virtual space that we can't gain awareness directly by our sense organ, we can't see it neither hear it, but by using sensor tools in the network, so it is hard work to work out the relation among the factors manually.

To implement this method, we have to resolve these problems beforehand.

4. Design of a multi-level analysis framework of NSSA

We derive a multi-level analysis framework of NSSA, see Fig 4(a), which make a little change from Endsley's three level model of situation awareness. First it proposes that every kind of data should have a corresponding process engine for identifying the data belong to a particular factor. Second, it divides the perception into two parts, factor identification and relation rules, because the purpose of perception is to get knowledge of who will take part in the activities and how they act. Last, it clarifies that the core process of NSSA is situation evaluation, and this process will generate the knowledge of current situation and then forecast the situation in two days or a week time.

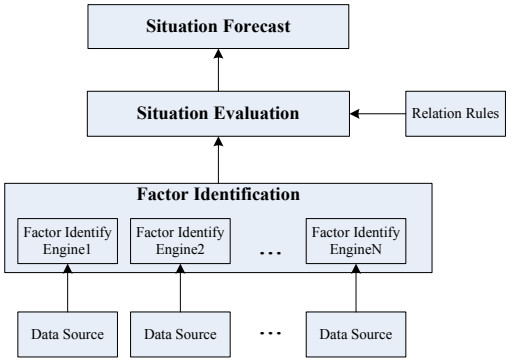

Fig. 4. (a)multi-level analysis framework of NSSA;

The accuracy of evaluation and forecast mainly depends on the integrity of information we get, so we should make it a scalable framework to extend new data acquisition capabilities.

5. Conclusion

This paper displays the challenges of Network Security Situation Awareness, and tries to give the corresponding resolutions. We point out that the relationship between the situation evaluation and the situation awareness, and then propose a method for situation evaluation. At last, we introduce the multi-level analysis framework for Network Security Situation Awareness. While there are still some detail methods should be studied deeply, and we will give a further discussion in the future work.

Acknowledgements

This work is supported by National Natural Science Foundation of China (Grant No. 61272500, 61202226)，National High Technology Research and Development Program of China, 863 Program (Grant No. 2011AA010701, 2011AA01A103), and Strategic Priority Research Program of the Chinese Academy of Sciences (Grant No. XDA06030200)

References

[1] Endsley, M., 1988. Situation awareness global assessment technique (SAGAT). *In Proceedings of the IEEE 1988 National Aerospace and Electronics Conference*, vol. 3, p. 789-795.

[2] Bass, T., 1999. “Multisensor data fusion for next generation distributed intrusion detection systems,” 1999 IRIS National Symposium on Sensor and Data Fusion.

[3] Bass, T., 2000. Intrusion systems and multisensor data fusion. *Communications of the ACM*; **43(4)**: 99−105.

[4] Ticha, B., Ranchin, T., 2006. “A case based reasoning data fusion scheme: Application to offshore wind energy resource mapping,” 9th International Conference on Information Fusion. Florence, Italy, paper #206.

[5] Tadda, G., Salerno, J., Boulwarea, D., Hinmana, M., Gorton, S., 2006. Realizing situation awareness in a cyber environment. In: Dasarathy, BV., editor. *Proceedings of SPIE vol. 6242, Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications*.

[6] Zhuo, Y., Zhang, Q., Gong, ZH., 2008. “Cyberspace situation representation based on niche theory,” International Conference on Information and Automation. Zhangjiajie, China, p. 1400-1405.

[7] Endsley, M., 1995. Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*; **37(1)**: 32–64.

[8] Salerno, J., Hinman, M., Boulware, D., 2005. A situation awareness model applied to multiple domains. *In Proceedings of the Defense and Security Conference*. Orlando, FL, USA.
[9] Smets, P., 2007. Analyzing the combination of conflicting belief functions. *Information Fusion*; **8 (4)**: 387-421.
[10] Tadda, G., 2008. "Measuring performance of cyber situation awareness systems," 11th International Conference on Information Fusion. Cologne, Germany, p. 1-8.
[11] Leigh, F., Gordon, S., Andrew, P., 2003. Bringing knowledge to network defense. *In Proceedings of the 2007 Spring Simulation Multiconference*, vol. 3, p. 370-377.
[12] Wang , HQ., Liang, Y., Ye, HZ., 2008. "An Extraction Method of Situational Factors for Network Security Situational Awareness," International Conference on Internet Computing in Science and Engineering. Harbin, China, p. 317-320.
[13] Erbacher, R., Frincke, D., Wong, P., Moody, S., Fink, G., 2010. A multi-phase network situational awareness cognitive task analysis. *Information Visualization: Special issue on selected papers from visualization and data analysis* 2010; **9(3)**: 204-219.
[14] Erbacher, R., 2012. Visualization design for immediate high-level situational assessment. *In Proceedings of the 9th International Symposium on Visualization for Cyber Security*, ACM New York, USA; p. 17-24.