A Framework for Network Security Situation Awareness Based on Knowledge Discovery

Fang Lan
Department of Network Research
Institute of System Engineering
Beijing, China
flan721@yahoo.cn

Wang Chunlei
Department of Computer Science
Tsinghua University
Beijing, China
wcl08@mails.tsinghua.edu.cn

Ma Guoqing
Department of Network Research
Institute of System Engineering
Beijing, China
gleader@gmail.com

***Abstract*—Network security situation awareness provides the unique high level security view based upon the security alert events. But the complexities and diversities of security alert data on modern networks make such analysis extremely difficult. In this paper, we analyze the existing problems of network security situation awareness system and propose a framework for network security situation awareness based on knowledge discovery. The framework consists of the modeling of network security situation and the generation of network security situation. The purpose of modeling is to construct the formal model of network security situation measurement based upon the D-S evidence theory, and support the general process of fusing and analyzing security alert events collected from security situation sensors. The generation of network security situation is to extract the frequent patterns and sequential patterns from the dataset of network security situation based upon knowledge discovery method and transform these patterns to the correlation rules of network security situation, and finally to automatically generate the network security situation graph. Application of the integrated Network Security Situation Awareness system (Net-SSA) shows that the proposed framework supports for the accurate modeling and effective generation of network security situation.**

Keywords- network security; situation awareness; data mining; knowledge discovery

I. INTRODUCTION

Traditional network security devices such as Intrusion Detection Systems (IDS), firewalls, and security scanners operate independently of one another, with virtually no knowledge of the network assets they are defending. This lack of information results in numerous ambiguities when interpreting alerts and making decisions on adequate responses. Network systems are suffering from various security threats including network worms, large scale network attacks, etc, and network security situation awareness is an effective way for solve these problems. The general process is to perceive the network security events happened in a certain time period and cyberspace environment, synthetically manipulate the security data, analyze the attack behaviors systems suffered, provide the global view of network security, and assess the whole security situation and predict the future security trends of the network.

There exist several difficulties when implementing network security situation awareness. (1) The amount of alert events generated from various security sensors is tremendous and the false positive rate is too high. (2) The trivial alerts generated from large scale network attacks (e.g. DDoS) are very complex and the relationships among them are difficult to determine. (3) The data type of alert events generated from security sensors are very abundant, while there is a lack of knowledge needed by alert processing, and automatically acquiring these knowledge is rather difficult.

In this paper, we summarize the research progress of network security situation awareness, propose a framework for network security situation awareness based upon knowledge discovery, and apply the framework to our network security situation awareness system (Net-SSA). The rest of this paper is organized as follows: Section 2 introduces the concepts and functionalities of network security situation awareness and summarizes the related work of the area; Section 3 proposes our framework for network security situation awareness based on knowledge discovery; Section 4 presents the experiment results, and Section 5 concludes with some directions for future work.

II. BASIC CONCEPTS AND RELATED WORK

A. Basic Concepts

For the convenience of description and avoiding confusion, the associated notional definitions are given as follows:

Security Situation. It refers to the global security status of the supervised network, the cyber-attacks suffered in a certain time window, and the effect to the total objective of network security. Generally, the security situation information consists of two aspects, the time dimension and the space distribution dimension.

Security Event. It refers to the alert events generated by various network security situation sensors and resulted from network intrusions or from the monitored parameter exceeds the threshold value. It is represented as a multi-tuple: e_i ={ $detectTime_i$, $eventType_i$, $attack_i$, $srcIP_i$, $desIP_i$, $srcPort_i$, $desPort_i$, $protocol_i$, $sensorID_i$, $confidence_i$, $severity_i$, $other_i$ }. where, $detectTime_i$ refers to the time of alert event happens, $eventType_i$ refers to the type of alert event, $attack_i$ refers to the class of attack the detected alert belongs, $srcIP_i$ and $desIP_i$ refer to the source and destination addresses of alert event, $srcPort_i$ and $desPort_i$ refer to the source and destination ports of alert event,

978-1-4244-6349-7/10/$26.00 ©2010 IEEE

$protocol_i$ refers to the type of protocol, $sensorID_i$ refers to the sensor detected that event, $confidence_i$ refers to the confidence level of the alert event, $severity_i$ refers to severity level of the alert event, $other_i$ refers to the other information of the alert event.

Security Situation Modeling. It refers to the process of analyzing the alert events generated from various security sensors and finally generating the global security situation of network. It consists of following functions:

Event Simplification. $[e_1,e_2,...,e_n] \rightarrow e_m$, the redundant alert events are simplified, which have the relation of repetition or concurrency, to reduce the amount of effective events.

Event Filtering. $[e_i, P(e_i) \notin H] \rightarrow \phi$, the alert event is removed or marked as irrelevant event if the property $P(e_i)$ does not belong to a certain legal set of H . The alert events can be deleted if some key attributes are absent or out of the predefined ranges of values.

Event Fusion. $e_i \xrightarrow{confidence} e_{i'}$, it mainly solves the problems of alert collision and alert mergence by using the information fusion techniques such as the Dempster-Shafer evidence theory, so as to improve the confidence level of alert events and reduce the false positive rate.

Event Correlation. $[e_1, e_2,..., e_n] \xrightarrow{correlation} e_{n+1}$, the current network security events, activities and situations can be inferred from different types of alert event sources by using the mathematical or heuristic methods, so as to improve the detection rate and reduce the false negative rate.

Status Assessment. It refers to the assessment of security status from multiple layers based upon the distributions of attack behaviors in the space and time dimensions and the affections to network resources.

Knowledge Discovery (KD). It refers to the nontrivial process of identifying the new patterns from the set of security events collected from sensors, which are understandable and useful for security situation acquisition. The objective of knowledge discovery is to extract the rules required by the fusion and correlation of security events.

Security Situation Generation. During the process of network security situation awareness, the security situation model is standardized, restricted, inferred, corrected and supplemented via the pattern information acquired from knowledge discovery, and finally generate the global network security situation.

B. Related Work

To deal with the increased information security threats, many kinds of security equipments have been used in the large scale network. These equipments produce lots of security events. It's very difficult to obtain the security state of the whole network precisely when facing too much warning information. To settle this problem, many researches had introduced the concept of situation awareness into internet security system. Bass was the first who introduced this concept into network and bring forward the network security perception frame based on multi-sensor data fusion [1] [2]. It helps network administrators to identify, track and measure network attack activities. With references from Endsley's situation awareness framework [3], Jibao et al. [4] developed network security situation awareness model. In the other hand, according to Bass's concept, Liu et al. [5] put forward the model of network security perception based on information fusion.

In order to know the whole network security trend, we have to collect, fusion and analysis a great deal of information, decrease the false positive rate and false negative rate. Yu et al. [6] reported a warning message fusion method based on weighted D-S evidence theory. Fuse information from all sensors with different reliability and weight to increase the reliability of warning message and decrease the false alarm rate effectively. But, the important thing is how to set the reliability and power of each sensor accurately. Wang et al. [7] suggested that using neural network for heterogeneous multi-Sensor data fusion and considerate time and severity of the attack when analysis the security situation. Stefanos et al. [8] find the latent correlation with the help of automatic knowledge discovery and realize correlation analysis among warning information. The advantage is the mechanism of automatic knowledge discovery and the disadvantage is it's not always give satisfaction without the interaction of human. Sometime it may find a great deal of useless message.

After data fusion and correlation analysis of multi-sensor warning information, the security situation model has to be quantified. Bass [9] think the evaluation of security risk should include the assets of the system, degree of threaten and severity of attack. Zhang et al. [10] includes all network environment parameters into the security situation framework, such as the number of the important hosts in the network, the service provided by the hosts, the impact could be caused by the attacks. Chen [11] suggested dividing risk evaluation method into different levels. According to a hierarchical structure of service, host and network to quantitative the network security situation. First defining the importance of assets, the impact of attack and collect the vulnerabilities, then the security situation of the whole network could be evaluated when network attack happened.

It's an integrated process from network security information acquirement to building the network security situation model. But most of the researches were focusing on the fusion of the security events or the method of security risk evaluation. All of them have no formal descriptions of network security situation and lack an integrated situation awareness frame. This paper is not only to bring forward a formal network security situation model based on knowledge discovery, but also to propose an integrated network situation awareness framework which supports the whole process from analysis of security events to perception of the security situation.

III. A FRAMEWORK FOR NETWORK SECURITY SITUATION AWARENESS

The framework for network security situation awareness proposed in this paper is based upon knowledge discovery

and consists of two parts, the modeling of network security situation and the generation of network security situation, as shown in figure 1. The modeling of network security situation is to construct the formal model adapted for the measuring of network security situation based upon the D-S Evidence Theory, and support the general process of the fusion and correlation analysis of various types of alert events from security situation sensors. The generation of network security situation primarily consists of three steps: firstly, acquiring attack patterns through interactive knowledge discovery by introducing FP-Tree algorithm [12] and WINEPI algorithm [13]; secondly, transforming the discovered frequent patterns and sequential patterns to the correlation rules of alert events; finally, implementing the dynamically generation of network security situation graph based upon the network security situation generation algorithm.

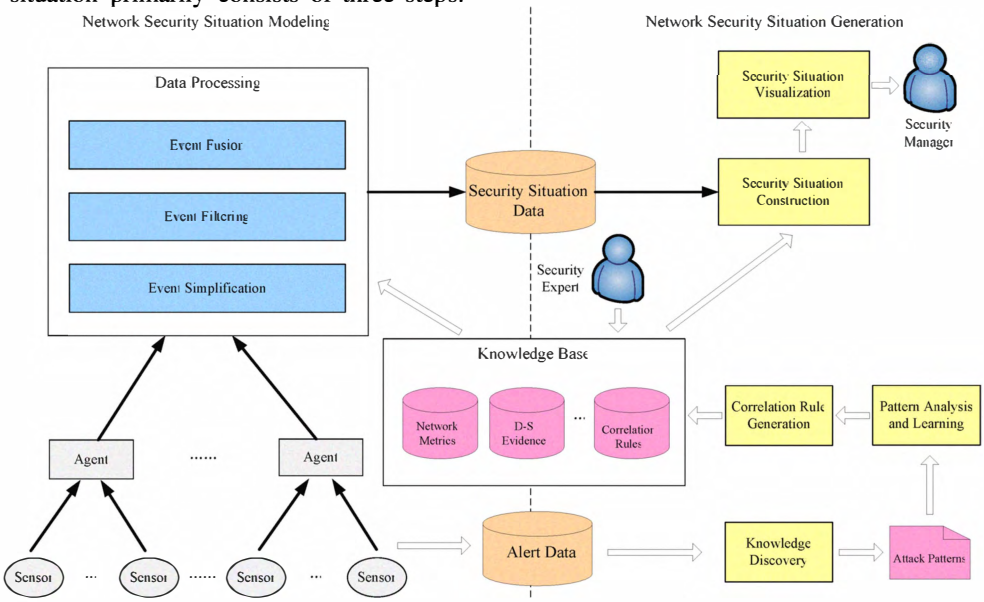

Figure 1. The framework for network security situation awareness consists of two parts, one is to process various events and construct the formal model of network security situation, the other is to acquire attack patterns through knowledge discovery and generate network security situation graph dynamically.

A. *The Modeling of Network Security Situation*

The primary objective of the modeling of network security situation is to construct the standardized data model suited for the measuring of network security situation, and support the general process of the simplification, filtering and fusion of alert events from security situation sensors.

The data sources used for the modeling of network security situation are various types of security alert events collected from heterogeneous situation sensors distributed in the supervised network. The process of the modeling of network security situation is composed of several phases.

During the initial phase of preprocessing, all the received security events are transformed to the standard format that can be understood by data process module through the specification of the alert events. The alert events may be from different sensors, and have distinct formats, such as the events of IDS, the records of firewall, the log file of host system, and the information from netflow, etc. The purpose of specification is to transform all the event attributes of each sensor to a uniform format. In our framework, we provide different preprocessing modules for the corresponding sensors, and transform the information from specific sensor to the attribute values of the information model defined in this paper. Based upon the information model, each primitive event is preprocessed and transformed to the standard format, and each attribute field is set to the appropriate value.

During the phase of security situation data processing, the standardized alert events are received as input, and perform the simplification, filtering and fusion of the standardized alert events. The objective of event simplification is to merge the redundant alert events of the identical attack detected from several sensors. A typical example of event simplification is that the IDS may generate many detection events for each port scanning packet when perform the port scanning attack, and the amount of events may be greatly reduced by simplifying the same type of events from the same source and the same destination host during a given time period. The objective of event filtering is to remove those events dissatisfied with the constraint requirements, and these constraint requirements are stored in the knowledge base in the form of attribute or rule according to the requirements of network security situation awareness. For instance, the events can be removed if the key attributes of these events are absent or out of the required ranges, because they are meaningless for the analysis of network security situation. Through the processing of simplification and filtering, the repeated security events are merged, the amount of security events is greatly reduced and the abstraction degree is improved, at the same time the security situation information implied are preserved.

The foundation of event fusion function is Dempster-Sharer (D-S) evidence theory. The objective of event fusion is to introduce the different confidence level to the security events that received from different sensors and have already preprocessed, simplified and filtered, quantitatively evaluate these security events by fusing multiple attributes, so as to effectively reduce the false positive and false negative of security alerts and provide support for the inference, analysis and generation of network security situations. The general process of D-S evidence theory based event fusion is to infer the security situation of current system based upon the observations of the system security status, $E_1, E_2, \ldots, E_m$. Based upon D-S evidence theory, let the frame of discernment (FOD) be $\{T, F\}$, T refers to the correct alert, F refers to the false alert, and $T \cap F = \phi$. As the most fundamental concept of D-S evidence theory, Basic Probability Assignment (BPA) needs to be defined for given evidence supporting a system status.

Definition 1: Basic Probability Assignment Function m:

$(P\{T, F\}) \rightarrow [0,1]$,

$m(\phi) = 0$,

$m(T) + m(F) + m(\{T, F\}) = 1$,

where, $m(T)$ refers to the confidence level of a security alert detected by a sensor. In our framework, the confidence level is represented by the attribute *confidence* in the format of alert event, and the initial values of this attribute are specified based upon the default values in the detection rules or human experiences.

D-S Evidence theory also provides the combination rule for multiple evidences, which is Dempster rule. The security alert events are fused based upon this rule, not only to reduce false alert rate and improve the confidence level of event detection, but also to identify attack behavior through the fusion of characteristics of multiple low level security events. For instance, let the basic probability assignment function of two evidences be m_1 and m_2, the basic probability assignment function of combined evidence is

$$m(e) = K^{-1} \sum_{e_1 \cap e_2 = e} m_1(e_1) m_2(e_2)$$

$$= m_1(e_1) \oplus m_2(e_2)$$

where, K refers to the normalization factor,

$$K = \sum_{e_1 \cap e_2 \neq \phi} m_1(e_1) m_2(e_2)$$

This method can be utilized repeatedly to cause the security events from multiple sources to be effectively fused. Suppose there are multiple events $e_1, e_2, \ldots, e_n$, and the corresponding basic probability assignment function are m_1, $m_2, \ldots, m_n$, then these n evidences are combined into one evidence and the corresponding basic probability assignment function is

$$m_{1\ldots n}(e) = K_n^{-1} \sum_{\cap_i e_i = e} m_1(e_1) m_2(e_2) .. m_n(e_n),$$

where

$$K_n = \sum_{\cap_i e_i \neq \phi} m_1(e_1) m_2(e_2) \ldots m_n(e_n)$$

When the security situation sensor receives the security alert event, the first thing to do is to calculate the confidence level of the event based upon the system settings or the arguments of the rules. It can effectively reduce the false alert rate that quantifies the confidence degree of the alerts from the level of primitive events. During the phase of alert data processing, the alert events collected from sensors have the quantified confidence level, the redundant and suspect alert events can be greatly reduced and the ability of identifying the attack behavior can be improved through the fusion of security alert events based upon the Dempster rule.

B. The Generation of Network Security Situation

There are two network security situation data sources available for knowledge discovery: one is the set of security alert events generated from the attack simulations, the other is the set of historical security alert events. The function of knowledge discovery in our framework is to find out and extract the knowledge from these set of alert events, which is required for the correlation of security situation. Due to the complexities of alert events generated from various types of security situation sensors, the process is hardly to be performed completely by manual work. In this paper, we propose a knowledge discovery based method, which provides the means of extracting the security situation correlation rules through the pattern mining, analysis and learning from the set of security alert events, and finally generate the network security situation graph. This process is divided into the following steps:

1) Simplification and Filtering of Security Alert Events

We found that there exists large numbers of meaningless frequent patterns in the set of primitive alert events from security situation sensors by examining the experiment data, and these frequent patterns mostly relate to the problems of system configuration or harmless access. If the process of knowledge discovery is directly performed on such set of primitive intrusion events, it is inevitable to generate many types of meaningless knowledge. Therefore, it is necessary to establish the mechanism of alert event filtering in the foundation of D-S evidence theory, which executes the statistical analysis based upon the confidence level of alert events. Firstly, the distributions of various types of security events are statistically analyzed via automatic tools; secondly, the meaningless events are deleted by evaluating the importance of each type of alert events based upon the rules of simplification and filtering, which uses D-S evidence theory as the foundation of event processing.

2) Knowledge Discovery from the Set of Security Alert Events

In this paper, the frequent pattern and sequential pattern discovery algorithm are adopted to obtain the security situation knowledge from the set of security alert events. The frequent pattern refers to the correlations among the

attributes of events, and the objective of which is to infer the constraints among the attributes of events and transform to the filtering rules after adding correlation actions. Similarly, the sequential pattern refers to the sequential relationships among the events, and the objective of which is to discover the sequential relationships or consequences among the events and further transform to the combination rules of trivial events. Usually, the relationships among the attributes of events need to consider the relationship among almost all attributes of security alert events, such as *detectTime* , *eventType* , *attack* , *srcIP* , *desIP* , *srcPort* , *desPort* , *protocol* , *confidence* , *severity* , etc, while the relationships among the events only consider the occurrence sequences among the correlative alert events which have the same or associated *attack* attribute value.

a) Frequent Pattern Mining

The most significant feature of frequent pattern mining algorithm (such as, FP-Tree algorithm [12]) is to compress the large database to the compact tree structure (FP-tree) and quickly mine the set of frequency patterns without the need of generating the candidate items, since it avoids the repeated database scanning. It mainly consists of Insert_Tree generation algorithm and FP_Growth frequency pattern mining algorithm. The correlation rules among the attributes of events can be mined from the set of security alert events by using FP-Tree algorithm and setting the minimal supporting threshold value *min_sup* .

b) Sequential Pattern Mining

WINEPI algorithm [13] is used in sequential pattern mining to discover the sequential relationship among security alert events. Firstly, the set of frequent events is extracted from the set of security alert events with specific type within the given slide window, and the set of candidate frequent episode patterns is generated with shorter length. Secondly, the frequent episode patterns with larger length are discovered through iteration. Finally, the sequential relationships among the episode patterns are discovered based upon the thresholds of frequency and confidence level, that is, the sequential relationship among the security alert events.

c) Pattern Analysis and Learning

Through the analysis of frequent patterns and sequential patterns found in the above mentioned process of knowledge discovery, we observed that some frequent patterns are just statistical phenomena, which are meaningless with respect to the security situation analysis. On the other hand, there are some security alert events which have few occurrences, the regularity are illegible, and the confidence levels of the generated rules are low, whereas these rules are vital to the correlation of security situation. To utilize the discovered knowledge effectively, Prolog-EBG machine learning algorithm are adopted to properly interpret and analyze the discovered knowledge by introducing the prior knowledge of the domain, and the revised and optimized rules are exported from the set of security alert events generated from the attack simulations. Through this optimization process, the confidence levels of the rules are properly evaluated from the statistical view, and the evaluations of discovered knowledge are also enhanced, so as to remove the meaningless knowledge, add the prior knowledge, and make the discovered knowledge more useful.

d) Extraction of Security Situation Correlation Rules

The knowledge obtained from the process of knowledge discovery is transformed to the correlation rules of security situation by adding the correlation actions, and can be applied to the online correlation analysis of network security situation. Firstly, the strong correlation rules among the attributes of alert events are analyzed, which are extracted by FP_Tree algorithm. If this kind of rules is related to some regular access, then the deletion action is added, and these rules are transformed to the filtering rules of alert events. Secondly, the sequential relationships among alert events are analyzed, which are extracted by WINEPI algorithm. If this kind of sequential relationship is associated with some type attack and the combination rules of attack events is formed, then the new security attack event is added. Finally, the generated correlation rules are transformed to the formal rule encodings, and added to the online correlation knowledge base.

3) Generation of Network Security Situation

The generation of network security situation refers to the correlation of network security events, construction of network security situation graph, and assessment of the global network security situation. Net-SSA periodically update the network security situation graph based upon the security situation data calculated from event fusion and correlation. After certain alert event is processed and inserted into evidence base, Net-SSA schedules and activates the associated rules and launches the process of situation correlation, and correlates the security situation by using above mentioned knowledge discovery algorithms. If the correlation results indicate certain type of security attack, then the network security situation graph is dynamically updated in accordance of system settings, and notifies the network security administrator.

IV. EXPERIMENTAL ANALYSIS

The network security situation awareness system we developed by ourselves was applied in the experiment. This system includes a network security situation generation engine based on knowledge discovery. The test data LLDOS 1.0 was provided by MIT Lincoln Lab, which was collected under the attack inspect situation of DARPA2000 [14]. LLDOS 1.0 was the first data collection which was created by DARPA. It was consists of five attack stages: get the list of active hosts, find weak Solaris hosts, invade the system by Solaris Sadmind buffer overflow bug, install mstream DDoS trojan on the controlled hosts, start attack on the remote server by the controlled hosts. The attack data collection was replay in the experiment network and the attack scene was regenerated. With our distribute network security situation awareness system Net-SSA, sensors deplored in the experiment network can detect security events and reported to the control center which was responsible of data fusion and correlation analysis of the multi-sensor information. The

control center also generate the current situation of the network security and user can see the inspect results and the view of the network security situation in real time by graphical interfaces.

TABLE I. THE ATTCACK RECORDS

Stage	Source IP	Destination IP	Event Type
Stage1	202.77.162.213	172.16.112.0/24 172.16.113.0/24 172.16.114.0/24 172.16.115.0/24	ICMP Ping Sweep
Stage2	202.77.162.213	Active hosts in stage1	RPC portmap Sadmind request UDP
Stage3	202.77.162.213	172.16.115.20 172.16.112.10 172.16.112.50	RPC Sadmind overflow attempt RPC Sadmind query with root credentials attempt UDP
Stage4	172.16.115.20 172.16.112.10 172.16.112.50	202.77.162.213	RSERVICES rsh root
Stage5	Forged IP	131.84.1.31	Possible DDoS Attack

Table 1 gave the records reported by the sensors during the 5 stages of the whole network attack process. According with the security situation modeling, alert events generated from various security sensors were simplified, filtered, fused and correlated. The number of the warning events decreased greatly from 64481 to 6164. At the same time, according to the corelation rule, it converts many trivial attacks which aimed at the victim host from Forged IP into a DDoS attack.

With calculation of the risk value, mark the nodes of the experiment network with different colors. The nodes with high risk were marked in red. Furthermore, with analysis of the attack events, the path of the attack was marked, and the current network security situation view is formed, as shown in Figure 2.

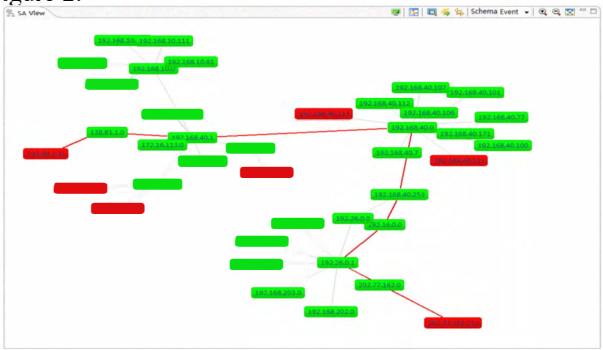

Figure 2. A sample view of network security situation generated by our Network Security Situation Awareness system (Net-SSA).

V. CONCLUSIONS

In this paper, we analyzed the existing problems of network security situation awareness and proposed a framework based on knowledge discovery. The framework consists of the modeling of network security situation and the whole process of the generation of network security situation. We have described the construction of the formal model for network security situation measurement based upon the D-S evidence theory, the extraction the frequent patterns and sequential patterns from the dataset of network security situation based upon knowledge discovery method and the transformation of these patterns to the correlation rules of network security situation, and the automatic generation of network security situation graph. We also present the application of the Net-SSA and show that the proposed framework supports for the accurate modeling and effective generation of network security situation. As this study continues, we plan to explore assessment of global security situation and investigate the problems of real-time predication of upcoming severe security attacks.

REFERENCES

[1] Bass, T., "Multisensor Data Fusion for Next Generation Distributed Intrusion Detection Systems," Invited Paper 1999 IRIS National Symposium on Sensor and Data Fusion, pp.24-27, May 1999.

[2] Bass, T., "Intrusion Detection Systems and Multisensor Data Fusion," Communications of the ACM, Vol. 43, No. 4, April 2000.

[3] Endsley, M., "Toward a theory of situation awareness in dynamic systems," Human Factors, Vol. 37, No.1, pp.32-64, 2005.

[4] Lai Jibao, Wang Huiqiang, and Zhu Liang, "Study of Network Security Situation Awareness Model Based on Simple Additive Weight and Grey Theory," 2006.

[5] Liu Mixi, Yu Dongmei and Zhang Qiuyu et al., "Network Security Situation Assessment Based on Data Fusion," 2008 Workshop on Knowledge Discovery and Data Mining, 2008.

[6] Yu Dong and Frincke, D., "Alert Confidence Fusion in Intrusion Detection Systems with Extended Dempster-Shafer Theory," 43rd ACM Southeast Conference, March 18-20, 2005.

[7] Wang Huiqiang, Lai Jibao, and Ying Liang, "Network Security Situation Awareness Based on Heterogeneous Multi-Sensor Data Fusion and Neural Network," Second International Multisymposium on Computer and Computational Sciences, 2007.

[8] Stefanos Manganaris, Marvin Christensen, Dan Zerkle, et al. A data mining analysis of RTID alarms. Computer Networks, 2000, 34(4):571-577

[9] Bass, T. and Robichaux, R., "Defense-in-depth revisited: qualitative risk analysis methodology for complex network-centric operations," Proceedings of IEEE Military Communications Conference, vol.1, pp.64-70, 2001.

[10] Zhang Yong, Tan Xiaobin and Xi Hongsheng, "A Novel Approach to Network Security Situation Awareness Based on Multi-perspective Analysis," IEEE 2007 International Conference on Computational Intelligence and Security, 2007.

[11] Chen XZ, Zheng QH and Guan XH et al., "Quantitative hierarchical threat evaluation model for network security," Journal of Software, Vol.17, No.4, pp.885-897, April 2006, http://www.jos.org.cn/1000-9825/17/885.htm, Accessed on Jun 2008.

[12] J Hall, J Pei, Y Yin. Mining frequent patterns without candidate generation. 2000 ACM. SIGMOD Int'1 Conf on Management of Data (SIGMOD'00), DallaS, TX, 2000

[13] Mika Klemettinen . A knowledge discovery methodology for telecommunication network alarm databases. [Ph D dissertation]. Helsinki : University of Helsinki, Finland, 1999

[14] Haines JW, Lippmann RP, Fried DJ, Tran E, Boswell S, Zissman MA. DARPA intrusion detection system evaluation: Design and procedures. Technical Report 1062, Lexington: MIT Lincoln Laboratory, 1999.