Study of Threat Scenario Reconstruction based on Multiple Correlation

Xuejun Yuan, Jing Du, Futong Qin and Yunyan Zhou

Luoyang Electronic Equipment Test Center of China, Luoyang, China
Email: whotrustme@163.com, yuan boo@163.com, ftqin@163.com, 54zyy@sina.com

Abstract. The emergence of intrusion detection technology has solved many network attack problems, ensuring the safety of computer systems. However, because of the isolated output alarm information, large amount of data, and mixed events, it is difficult for the managers to understand the deep logic relationship between the alarm information, thus they cannot deduce the attacker's true intentions. This paper presents a method of online threat scene reconstruction to handle the alarm information, which reconstructs of the threat scene. For testing, the standard data set is used.

1. Introduction

In response to the security threats faced by the computer systems, the defensive side has deployed a large number of network security products, and achieved positive results. IDS, as a representative of the security products, has good technical indicators and is an effective solution to detect the variety of attacks, ensuring the safety of computer systems. However, the isolated output alarm information, large amounts of data, event errors and omissions, and unorganized alarm flow are presented to the managers, making it difficult to understand the deep logic relationship between the alarm information, and difficult to deduce the attacker's true colors and true intentions. Therefore, how to deal with a large number of alarm data online, mine the deep logical relationship between the alarm information, reconstruct the threat scenario and provide decision support for the managers, become hot spots of the current research.

There are many ways of analyzing and processing the information generated by network security equipment such as IDS. The commonly used methods include: correlation based on attribute similarity [1], correlation based on the attack template [2], correlation based on the causal relationship [3][4], correlation based on timing relationship [5], the cross correlation and so on[6]. These methods have the following problems: low efficiency of the alarm correlation, underuse of the existing data, incompatible with online mode and so on.

To this end, this paper firstly describes the concept of threat scene reconstruction, and analyzes the current typical correlation technologies and methods. Then, a framework of threat scene reconstruction which can be used in the online mode is proposed, and the correlation algorithm is improved. Finally, the experimental test is carried out. The method proposed in this paper can meet the requirements of the online correlation mode, and its resource occupancy is reasonable. With it, it is more convenient for the managers to discover the security threats in time and formulate the corresponding protection strategy.
2. Background

2.1 The Concept of Threat Scene Reconstruction

With the extensive application of the security equipment such as IDS, from the underlying hardware, the basic system, the upper application to the end user, the security of network information system is significantly enhanced. It is difficult for the attackers to just exploit one single vulnerability to achieve its attack attempt. In order to achieve its attack intention, Attackers use a number of vulnerabilities to implement a series of attacks, which gradually expands the attacker’s access, and ultimately achieves its intention of attack. The range of the attacks described here is called a threat scenario, also called an attack scenario[7].

In order to detect the attacking intention of the attacker and achieve rapid response, the security managers analyze and associate the alarm information generated by the network security equipment, and then reconstruct a series of attack behaviors implemented by the attacker. This process is called threat scenario reconstruction, also called attack scenario reconstruction.

There are two patterns for threat scene reconstruction. One is online reconstruction, which reconstructs the threat scene while the alarm is generated. In this mode, the traffic of the alarm information is generated constantly, which requires high reconstruction efficiency. The other one is off-line reconstruction, which reconstructs the threat scene after all of the alarms have been generated. The accuracy of threat scenario reconfiguration in this mode is high, but it can only be used in post hoc analysis.

The alarm information, as the data source of the alarm correlation, among which the relationship must be clearly classified. In this paper, the relationship between the alarm information is classified and abstracted into the following three logical relations: redundant relationship, causality relationship, and timing relationship. The core technology of threat scene reconstruction is the alarm correlation technology.

2.2 Alarm correlation technology

1) Correlation based on attribute similarity. The core of the method is to define the similarity function of the important attribute values, determine the threshold and weight, and then correlate the alarm information whose attribute similarity is greater than the threshold. This method can deal with the alarm information with redundant relationship and greatly reduce the number of alarm information, but it cannot reveal the causal relationship and timing relationship between the alarm information, thus fails to reveal the deep logical relationship of alarm information.

2) Correlation based on the attack template. This method, based on the expert knowledge or empirical data, extracts the characteristic information of the threat scene in a user-defined manner or from the training data set, and then saves it as an attack template which is described by a formal language. By comparing alarm information with the attack templates, the correlation of attacks is achieved.

The advantage of this method is the ability to accurately and quickly detect attack patterns which have been clearly described in the threat scene. The disadvantage is that it is difficult to cope with an unknown attack in the threat scenario or some of the attacks that are not defined in the attack template.

3) Correlation based on the causal relationship. Researchers believe that the attack event always depends on a specific premise, and will have specific consequences. For example, there are two attack events, the time of their occurrences are $T_0$ and $T_1$, and $T_0 < T_1$. Comparing the consequences of the attack behavior happened at $T_0$ and the premise of the attack behavior happened at $T_1$, if the set (consequence, premise) matches, the two are considered as causal and related. The most significant advantage of the causal relationship-based alarm correlation method is that it does not need to capture all the possibilities of the threat scenario, but it can still detect unknown attacks. This method is highly accurate. It need to establish a knowledge database, which contains the premise and the consequences of attacks. Its disadvantage is that if the knowledge database is too large, it cannot adapt to the occasion of online correlation.
4) **Cross Correlation.** This method is mainly based on the background knowledge, such as network topology information, vulnerability information and host configuration information, to improve the quality of the alarm, and to assess the risk of alarm information. This method is often used in conjunction with other methods.

### 3. The Design of Threat Scene Reconstruction Method

#### 3.1 The Idea

In order to accurately deduce the attack behavior scene, this paper intends to compress the number of the alarm messages and the size of the causal knowledge, based on the causal relationship. Specific implementation ideas are discussed as follows:

1) **Alarm correlation based on the causal relationship.** The causal relationship-based correlation method is mostly responsive to the deep logical relationship between the alarm information, and thus it has the highest accuracy. Therefore, this paper chooses the causal correlation method, and uses attack itself as the main body of the correlation.

2) **Causal knowledge compression based on cross correlation.** The basis of the causal relationship-based correlation is to establish the knowledge of the prerequisite and consequence set of the attack event. If processing the causal knowledge introduce large overhead due to its size, this method cannot adapt to the online mode. For this reason, this paper borrows the idea of cross-correlation, combines the background knowledge of the protected network, such as the network topology information, the vulnerability information and the host information, simplifies the causal knowledge and generates the customized knowledge of the protected network, which in the end successfully reduces the size of the causal knowledge base.

3) **Elimination of redundancy alarm information based on attribute similarity.** The causal relationship-based correlation method needs to analyze the premise and consequences of the alarm information. If the oversized and redundant alarm information is not preprocessed, information accumulation will inevitably occur in the online mode, and results in the correlation failure. In this paper, the correlation method based on attribute similarity is used to preprocess the alarm information before using the correlation method based on causality, and the redundant relationship between the alarm information is eliminated. In addition, because Distributed Denial of Service (DDoS) attacks can easily generate a large number of alarm information in a short time, this paper will prioritize DDoS attack alarm information.

#### 3.2 Threat Scenario Reconstruction Framework

Based on the above ideas, the threat scene reconstruction method designed in this paper adopts a multi-layer correlation structure. With the preprocessed information, the redundant relation is analyzed by the alarm fusion unit, and the causal relationship and the timing relation are solved by the alarm correlation unit. The information flows through these units in turn, transforming data into knowledge.

The threat scene reconstruction framework is shown in Figure 1.

At first, the original alarm information is preprocessed by the preprocessing unit. It eliminates the difference among the different types of the alarm information which are generated by different IDS. The main purpose is to convert the original alarm information so that the generated data to meets the relevant format specifications of the alarm information that could be further processed in the following stages.

The alarm fusion unit leverages the correlation method based on attribute similarity, mainly dealing with the redundant relationship of the alarm events. In order to solve the problem of the large number of alarm information generated in a short time, the alarm fusion unit adopts a sliding time window, and preferentially processes the DDoS attack alarm information in batches.

The alarm correlation unit leverages the causal relationship-based correlation algorithm, which is mainly used to exploit the causal relationship and potential timing relationship of the alarm information.
The correlation is based on the causal knowledge, using attack itself as a correlation subject to meet the requirements of the online mode. The input of the alarm correlation unit is the alarm information that has been merged by the alarm fusion unit, and its output is the possible attack sequence.

![Diagram](image)

**Figure 1** The threat scenario reconstruction framework

The causal knowledge database is the basis of the alarm correlation, and is related to the quality of the correlation effect. It uses predicates to formalize the description of the alarm information, the consequences of information and the super alarm type.

The scene information database stores the static scene information of the network information system. Compared to the business information flow, the scene information of specific network information system is static, which will not be changed frequently. In this paper, we use the idea of cross correlation, simplifies the knowledge with the scene information, generate custom knowledge, thus reduce the correlation matching range.

The basic database, as a storage unit of this framework, has data interaction with each unit. From the original alarm information, the formatted alarm information, the high-level alarm, to the alarm attack sequence, these data are all stored in the basic database.

The threat scene visualization unit displays the threat scene generated in the end in a more intuitive way.

### 3.3 Design of the Fusion Algorithm based on Attribute Similarity

To meet the requirements of the online processing mode, the algorithm uses a sliding time window to read the preprocessed alarm information. Firstly it checks the sliding time window, then it determines in bulk whether the information within the window matches the DDoS attack alarm characteristics or not. If so, the information will be placed into the DDoS attack alarm queue. Otherwise, the information in the time window will be processed one by one to determine whether it can be merged into the other attack alarm queues.

**1) Alarms attribute similarity.** In this paper, we select 6 kinds of the alarm attribute for similarity calculation, which include alert time, source IP, target IP, protocol type, source port, and target port. The similarity function is defined as follows:

- **a) Time attribute similarity function**

  \[
  S(t_{ime_i}, t_{ime_j}) = \begin{cases} 
  \frac{T - |t_{ime_i} - t_{ime_j}|}{T}, & |t_{ime_i} - t_{ime_j}| \leq T \\
  0, & |t_{ime_i} - t_{ime_j}| > T
  \end{cases}
  \]

  Where \( T \) denotes the threshold of time, and \( t_{ime_i} \) and \( t_{ime_j} \) are the occurring time of two alarms.

- **b) IP address attribute similarity function**
\[ S(ip_i, ip_j) = \frac{n}{32} \]  

Where \( n \) denotes the number of identical in the IP address bits from high to low, obtained by calculating XOR on \( ip_i \) and \( ip_j \) in their binary format. In this paper, \( n \geq 24 \) (\( n > 23 \)), therefore, 0.72 is used as the IP address class attribute similarity threshold.

c) **Protocol type attribute similarity function**

\[
S(type_i, type_j) = \begin{cases} 
1, & type_i = type_j \\
0, & type_i \neq type_j 
\end{cases}
\]  

(3)

d) **IP port attribute similarity function**

In this paper, we find that the similarity of the port attributes is not only related to distance, but also has a close relationship with the distribution of port numbers. Consider the characteristic of the port number distribution, expand the definition of the adjacent port, and then determine based on the distance from port to port. Different thresholds are set for different ranges of port numbers. If the difference between ports is less than the given threshold, the pair of ports is considered as adjacent ports. The similarity of the port is defined as follows:

\[
S(X_p, Y_p) = \begin{cases} 
\frac{\text{stepL} - |X_p - Y_p|}{\text{stepL}}, & |X_p - Y_p| \leq \text{stepL} \\
0, & \text{otherwise}
\end{cases}
\]  

(4)

Where \( \text{stepL} \) denotes the threshold of the difference between the two ports:

\[
\text{stepL} = \begin{cases} 
1, & 0 < \max(port_i, port_j) \leq 255 \\
2, & 256 \leq \max(port_i, port_j) \leq 1024 \\
4, & 1025 \leq \max(port_i, port_j) \leq 5000 \\
8, & 5001 \leq \max(port_i, port_j) \leq 65535
\end{cases}
\]  

(5)

2) **Overall similarity.** Whether the alarm information can be integrated depends on the overall similarity of the alarm information. The overall similarity of the alarm information given in this paper is defined as follows:

\[
S(X, Y) = \prod_{j=1}^{6} \max\{0, SIM(X_j, Y_j) - V_j\}
\]  

(6)

Where the variable \( j \) is the index value of the attribute. \( V_j \) denotes the minimum similarity expected for the \( j \)-th attribute. Because the algorithm selects six important alarm attributes, so \( j \) is an integer value from 1 to 6. The variable \( SIM(X_j, Y_j) \) is calculated with the Eq.(1) to Eq.(4).

When the overall similarity value \( S(X, Y) > 0 \), the alarm events \( X \) and \( Y \) are considered to be similar.

3) **DDoS attack alarm attribute similarity.** According to the characteristics of DDoS alarm information, the fusion method is specially designed to prioritize such information. The alarm information generated by the DDoS attack has the following two characteristics:

a) The alarm information in which the destination IP address equals the target host are the attack packets. In a certain period of time, for these alarm information, the source IP address is not similar but the source port is similar, and the target IP address is the same, and large amount of alarms are generated.
b) If the source IP of the alarm information is the target host, then these are response packet for the attack packets. In a certain period of time, for these alarm information, the source IP address is the same and the destination IP address is different, but the target port is similar, and large amount of alarms are generated.

According to the above characteristics, the proposed batch fusion algorithm is described as follows:

a) In the time slice $t$, $S(sourceIP_i, sourceIP_j)=1, S(targetPort_i, targetPort_j) \geq 0.8$; or $S(targetIP_i, targetIP_j)=1, S(sourcePort_i, sourcePort_j) \geq 0.8$;

b) If the number of the similar alarms obtained in the previous steps is greater than $T$, which is a threshold for the number of the alarm information, then correlate these alarms to the DDoS attack queue. Among them, the similarity of the IP address is calculated with the formula 2, and the similarity of the port is calculated with the formula 7:

$$S(X_p, Y_p) = \begin{cases} \frac{\text{stepL} - |X_p - Y_p|}{\text{stepL}} & |X_p - Y_p| \leq \text{stepL} \\ 0 & \text{otherwise} \end{cases}$$

(7)

Where $\text{stepL}$ has a big threshold within the port range of 5001 to 65535.

$$\text{stepL} = \begin{cases} 1 & 0 \leq \max(port_i, port_j) \leq 255 \\ 2 & 256 \leq \max(port_i, port_j) \leq 1024 \\ 4 & 1025 \leq \max(port_i, port_j) \leq 5000 \\ 200 & 5001 \leq \max(port_i, port_j) \leq 65535 \end{cases}$$

(8)

4) Alert fusion algorithm workflow. The workflow of the alarm fusion algorithm is shown in Figure 2:

![Figure 2 The alert fusion algorithm workflow](image-url)
3.4 Design of correlation algorithm based on causal relationship

In order to meet the requirement of the online alarm correlation mode, this paper based on custom knowledge database, analyzes the current attack and the subsequent attack list, which can be generated by the current attack itself.

The structure of the custom knowledge database is the same as the knowledge database. They use the predicate to describe the causal relationship between the alarm information, which mainly covers three aspects: firstly, the predicate knowledge, indicating the prerequisite and the consequence information of the alarm information; secondly, the implication of the relationship, indicating the relationship between predicates; and lastly, the super alarm type, indicating the abstraction of each attack corresponding to a type of alarm.

The correlation process is specifically described as follows. When attack-A occurs, an attack list L1 is created based on attack-A and the custom knowledge, which lists all the subsequent attacks that may be generated by attack-A. When attack-B occurs, an attack list L2 is created based on attack-B and custom knowledge database. At the same time, use the previous attack list L1 match attack-B. If the parameters match successfully, then attack-A and attack-B correlated. Iteratively, whenever a new attack occurs, establish the subsequent attack list and match it with the existing attack lists, to achieve the alarm information correlation.

The workflow of the alarm correlation algorithm is shown in Figure 3. One thread processes the next alarm message and the other thread outputs the alarm correlation result.

![Figure 3 The alarm correlation algorithm workflow](image)

An attack can be divided into several attack stages, and the occurring time of the alarm information generated in the same attack phase, is temporally close to each other. So there is a "blank time window" between different attack phases. This is due to the fact that the consequences of the previous attack phase needs to be confirmed by attackers, and the next attack stage will start only if the previous attack phase works. On the other hand, after the success of the previous stage, both of the system state conversion and the changes on the implementation of the attacking environment require extra time to be paid. These are the two reasons causing the "blank time window" between different attack phases.

In this paper, although the algorithm needs to query all possible follow-up alarm, but on the one hand, follow-up alarm information using the custom knowledge which has been simplified, has reduced
the match range. On the other hand, the algorithmic time overhead and resource overhead are introduced in the "blank time window" after the alarm message occurs, so there is little impact on the subsequent alarm information correlation of an attack sequence.

4. Experiment and result analysis
To verify the effectiveness and accuracy of this method, the experiment was tested using the DARPA 2000 LLDoS 1.0 data set [9]. The data set is a commonly evaluated and widely used benchmark data set for intrusion detection.

The software experimental environment consists of the Windows 7 operating system, the Microsoft visual studio 2010 development environment, and the Microsoft SQL server 2008 database. The used hardware experimental environment is an Intel i5 4590 CPU(3.2GHz) with 8G memory. TCPPreplay3.4.4 [10] was used for data playback, and the snort intrusion detection system for alarm information collection was on the other side.

Through the alarm fusion processing, the number of alarms is greatly reduced, the details of the results are shown in Table 1:

| Attack phase | Inside area input | Inside area output | Inside area rate | Dmz area input | Dmz area output | Dmz area rate |
|--------------|------------------|-------------------|-----------------|----------------|----------------|---------------|
| 1            | 31               | 6                 | 19.35%          | 785            | 8              | 1.02%         |
| 2            | 32               | 12                | 37.50%          | 25             | 8              | 32.00%        |
| 3            | 35               | 23                | 65.71%          | 80             | 21             | 26.25%        |
| 4            | 22               | 12                | 54.55%          | 19             | 9              | 47.37%        |
| 5            | 33787            | 29                | 0.09%           | 33943          | 13             | 0.04%         |
| Total        | 33907            | 82                | 0.24%           | 34852          | 59             | 0.17%         |

The number of alarms in the inside area are reduced to 19%, 37%, 65%, 54% and 0.09% after the alarm fusion. The number of alarms in the DMZ area are reduced to 1%, 32%, 26%, 47% and 0.04%. Obviously, the proposed algorithm is effective to eliminate the redundant relationship of the alarm information.
The results of data fusion shows that the fusion efficiency of phase 1 and phase 5 is very high. It is found that because the phase 1 is the pre-detection phase, which results in a large number of redundant information, the integration of the information in this phase is more efficient. And the phase 5 is a DDoS attack phase, the alarm fusion algorithm detects and fuses the DDoS attack alarms.

Figure 4 is the correlation graph generated by the method described herein. It can be seen from the figure that the attack process described in this figure is consistent with the DARPA2000 data set and is more clear and intuitive than the literature [3] [8].

5. Conclusion
In this paper, an online threat scene reconstruction method based on multiple correlation is designed, and the related algorithms are improved. The experiment uses the internationally recognized DARPA 2000 data set LLDoS1.0. The test results show that the threat scene reconstruction method is effective, the alarm fusion effect is ideal, and the correlation graph generated by the alarm correlation method is concise and intuitive. This method can meet the needs of online correlation, and the resource occupancy is reasonable. It is more convenient for the security managers to find security threats in time.

Follow-up work is planned as follows:
A. Improve the causal correlation knowledge database. Design automate mining tools, and update regularly according to the CVE vulnerability library and other related libraries, to enrich the causal knowledge database.
B. Explore further match methods between the "attack - follow-up attack" information and the background knowledge, calculate the probability of the subsequent attacks, reduce the subsequent attack search space, and improve the online matching ability.

6. Acknowledgement
This paper is sponsored by the National Natural Science Foundation of China with Grant No. 61303061, 61402485 and the Open Fund from HPCL with Grant No. 201513-01.

7. References
[1] ValdesA, SkinnerK. Probabilistic alert correlation[J] //Recent advances in intrusion detection. Springer Berlin Heidelberg, 2001:54-68.
[2] Mahboubian M, Udzir NI, Subramaniam S, et al. An alert fusion model inspired by artificial immune system[C]//Cyber Security, Cyber Warfare and Digital Forensic(CyberSec), 2012 International Conference on. IEEE, 2012:317-322.
[3] Ning P, Cui Y, Reeves DS, et al. Techniques and tools for analyzing intrusion alerts[J]. ACM Transactions on Information and System Security (TISSEC), 2004, 7(2):274-318.
[4] Zhaowen L, Shan L, Yan M. Real-time intrusion alert correlation system based on prerequisites and consequence[C]//Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on. IEEE, 2010: 1-5.
[5] Qin X, Lee W. Discovering novel attack strategies from INFOSEC alerts[M]//Data Warehousing and Data Mining Techniques for Cyber Security. Springer US, 2007: 109-157.
[6] Yu Beng L, Ramadass S, Manickam S, et al. A survey of intrusion alert correlation and its design considerations[J]. IETE Technical Review, 2014, 31(3): 233-240.
[7] Cheung S, Lindqvist U, Fong M W. Modeling multistep cyber attacks for scenario recognition[C]// DARPA information survivability conference and exposition, 2003. Proceedings. IEEE, 2003, 1: 284-292.
[8] TIARA project. http://discovery.csc.ncsu.edu/software/correlator/ver1.0/index.html.
[9] DARPA 2000 dataset. https://www.ll.mit.edu /ideval/data/2000 data.html.
[10] Tcpreplay tools. http://sourceforge.net/projects/tcpreplay/.