A Novel Solution on Alert Conflict Resolution Model in Network Management

Yi-Tung F. Chan  
University of Wales  
United Kingdom  
FrankChan2005@gmail.com

Ramaswamy D. Thiagu  
University of East London  
United Kingdom  
r.thiyagu@uel.ac.uk

Chou Chia-Jung  
Takming University of Science and Technology  
Taiwan  
raychou1999@gmail.com

Abstract

The concept of Situation Awareness (SA) is initially from the aviation security territory. SA deals with complexity, dynamics, high-risk, and situation that requires intervention. The introduction of SA in Network Security Situation Awareness (NSSA) is to respond to an 'Alert Conflict', but still the problem remains unsolved. Therefore, we proposed Heterogeneous Network Sensors Management Service (HNSMS), a method of analysing the Alert Conflict in a Heterogeneous Network Sensor Environment (HNSE) using different Alert Fusion technique to understand the security status of the whole network system. Thus, we use Fuzzy Cognitive Maps (FCM) and policy to fuse multiple inputs.

1. Introduction

The Web Service security and the Network Management are more critical, no matter how secure an organization transactions, everyone transaction is open to threats. In order to cope with the various threats, organizations deploy various defense mechanisms.

2. Related Work

Endsley (1988) [1] defined SA as the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future and further classified SA into three levels which are Perception, Comprehension, and Projection (see Figure 1).

![Figure 1: Endsley’s the SA Model [2]](image)


In IT Security, the IPO model (Input-Process-Output Model) present the process of the Data Fusion, which is the use of techniques that combine data from multiple sources and gather that information in order to achieve inferences, which will be more efficient if they were achieved by means of a single source [7] (see Figure 2).
In the Alert Confidence Fusion aspect, the Distributed Intrusion Detection System (DIDS) will be based on different source of the alerts to make a decision whether the system will respond to the attack or not depends on the following [8]:

1. The alert confidence information from the remote sensors might be less than local sensors.
2. The same network sensors are installed different in place, therefore, the detection ability will be different.
3. When different sensors detect the same type of attack, they have different degree of accuracy.

Yu and Frincke (2005) [8] proposed “Alert Confidence Fusion in Intrusion Detection Systems with Extended Dempster-Shafer Theory”, starting that different sensors, different confidence degree, and weight will process the Alert Confidence Fusion. Although the Alert Fusion is efficiency to solve the Alert Conflict by using confidence and weight from different source of the security system, this method does not detect abnormal behavior and respond quickly.

In FCM model, the intrusion detection system used the multi-intrusion sensors at the same time in order to reach the maximum of level of confidence. Siraj et al. (2006, 2004, 2001) [9, 10, 11] used FCM and Fuzzy rule-based to support the causal relationship and inference procedure to detect the potential attack.

The conceptual understanding of FCM model is that C_i and C_j has a link value which is e_{ij}. The link value is between -1 and 1. When the link value is 0, this means that C_i and C_j do not have any relationship. When the link value is more than 0, these mean that C_i and C_j have the positive causal relationship. When C_i is increasing, C_j will be multiple increase of e_{ij}. When the modulus of e_{ij} is higher, the impact of the causal relationship is stronger (see Figure 3).

### Figure 2: Simple the IPO Model of the Data Fusion

FCM model shows different security events which are Disclosure of Service, Disclosure of Host, System Distress, System Seizure, and System Environment Corruption. It can count the Incident Association Strength (IAS) and represented as a real value in t = 1 and the Ik (the influence from e_{ij}) from the evidence of the different security events resource (Rj) (security status of the host). The formula is shown in Equation 1 below.

\[
IAS(R_j)(t_{n+1}) = \left[ \sum_{k=1}^{n} (I_k(t_n)) \times e_{kj}(t_n) \right] / \sum_{k=1}^{n} e_{kj}(t_n)
\]

(1)

The I represents the five different security events. The IAS value can be gotten from each security event when the security event is become the quantification of value and the value multiplies the possessed of influence of evidence such as the weight.

### Figure 4: Evidence of combining with different security event

The Figure 4 shows that the influence of the security event (Disclosure of Service) is 0.2 (positive influence of evidence) and the value is divided by the total amount of all influence of evidence. Therefore, the FCM model can be combined with the evidence of the different security events to estimate whether the whole network environment is safe or not.

### 3. Alert Conflict Model

We proposed the HNSMS system that is based on three levels of the SA (Perception, Comprehension, and Projection) and sub divided into nine modules (see Figure 5).
The Figure 6 flowchart shows various network alerts from the Multi-sensors that are sent to the HNSMS system. The alerts have to pass through the Pre-processing and accept the unified format. When the format is accepted by the Pre-processing, the alert will go through the Confidence Assign and Weight Assign to process the Attack Alert Fusion. If it is a critical alert, the alert will be directly reported to the related network administrators. However, if there is no critical alert, the procedure will continue until the alerts are confirmed by the Policy Definition. The next stage will process the Overall Alert Fusion. Finally, when the alerts are confirmed by the network administrators, the secondary data will be stored in the Knowledge Base (Attack Signature Definition and the Security Policy Definition). The ‘Attack Signature Definition’ is the confidence lever and weight value of the attack for the network sensors while the ‘Security Policy Definition’ recognizes the attack type in the secondary data.

3-1. Weight Assign

The different security equipment can be used to measure and detect the accuracy. Thus, we adopted MaxEnt [5] principle to measure the weight (the condition is known and the Entropy is the biggest object). Therefore, in order to get the proportion of the weight of attack representative from different security equipment, we have to define the scope in advance. We applied it with the MaxEnt theory as follows:

\[
\eta_i = \begin{cases} 
\log (H_i) & \text{if } H_i > 0 \\
0 & \text{otherwise}
\end{cases}
\]

Berger et al. (1996) [12] proposed the IIS Algorithm (Improved Iterative Scaling) to estimate the MaxEnt parameter. We used the MaxEnt theory and IIS Algorithm to figure out the best parameter value.

In order to be able to discover every attack, we use the FCM model to support the security policy definition. For example, when an invader wants to intrude a specific workstation, the invader has to try to use the account and password from many users to access the workstation illegally. In order to observe this phenomenon, it is impossible to discover the attack from a single feature. The FCM model is shown in Figure 7. Thus, it has to set up different weighting. For example: “Interval Time” with -0.5. The negative number represents the interval time and the judgement generated by the abnormality and the inverse relationship. In other words, when the interval time is longer, it is impossible to produce the abnormal phenomenon. Furthermore, as to the part of the digital number, it will be indicated how much difference for the influence degree from the positive and negative number. In addition, due to the feature of the multi-attack situation, we have to set up the rule to find out whether the phenomenon is happened or not. In our solution, we used the Fuzzy rule-based to set up the rule (see Figure 7).

If number of login failures is moderate and
interval is short and this happened for
same machine and different users

then, Login_Failure_Same_Machine_Diff_User is activated highly.

In other words, when the current situation matches the fuzzy rule, it will give abnormal judgement, and the situation will then be reported to the network administrator for further processing.
4. Case Analysis

In order to deliberate the efficacy of the HNSMS model, we simulate the situation awareness of the defense in depth (see Figure 8). In the simulation of the security environment, we build four kinds of different sensors. We put the Firewall in the first line of defense. The second line of defense, we put the NIDS (Network Intrusion Detection System). The last line of defense, we put the HIDS (Host Intrusion Detection System) and Anti-Viruses. Through the four kinds of the network security sensors, it will be achieved the efficacy of the defense in depth. As soon as the exogenous factor touches off the alert from sensors, the alert data will be sent to HNSMS server. At this time, the HNSMS system will integrate the alert information, make a judgement for the situation, process the early warning for the information security, deal with the contingency or emergency, and follow the trail. The HNSMS system collects the alert information from different detection sensors and transferred the alert standard format into the consolidation form. We used two case studies to check how the HNSMS operate (see Figure 8 below).

Case Study One: Remote Invasion:

In this case, when a remote invader tries to access the network and invade a specific workstation, the invader has to try different account and password in the workstation and the invader tries to login to access the resource in this workstation. At this time, because of the login failure, the NIDS and the HIDS will send the alert to the HNSMS server to analyze the alert events (see Figure 9).

<table>
<thead>
<tr>
<th>id</th>
<th>sid</th>
<th>sig_id</th>
<th>Confidence</th>
<th>Weight</th>
<th>Last Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>4</td>
<td>0.01</td>
<td>1</td>
<td>2007-04-11 00:00:00</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0.2</td>
<td>0.5</td>
<td>2007-04-11 00:00:00</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>4</td>
<td>0.4</td>
<td>1</td>
<td>2007-04-11 00:00:00</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>4</td>
<td>0.01</td>
<td>1</td>
<td>2007-04-11 00:00:00</td>
</tr>
</tbody>
</table>

2. We fuse the confidence from two kinds of the network security sensors to make the judgement whether the workstation is in secure state or not. We use the concept of the data fusion from the Dempster-Shafer theory. Moreover, we also use the value of the confidence and the weight from the network security sensors. We use the information which we got and we use it into the formula 2. The result of the Attack Alert Fusion is shown below.

\[
m_{23}(\{A_4\}) = \frac{0.2 \cdot 0.5 \cdot 0.4}{0.2 \cdot 0.4 + 0.4 \cdot 0.5 + 0.6 \cdot 0.8} = 0.25
\]

3. Hypothesis: when the confidence value of the Attack Alert Fusion is lower, we can say that the system is in normal state. The situation does not need to report to the network security administrator immediately. The threshold value will be set up by the different situation.

4. In this case, the report from the sensors and fact
are not conformed to each other. The reason is that it is common situation when the normal users type wrong account and password. It will be caused the login failure. Therefore, it is impossible to make the judgement through a single timing.

5. Overall Alert Fusion used other auxiliary information to give the judgement whether the system is in secure state or not. The other auxiliary information involved “the number of times for Login Failure”, “Interval Time”, “Users”, and “Machines” (see Figure 7) and we use the security policy which is from the FCM model. We use the estimated criterion in the knowledge module to process the Overall Alert Fusion (see Equation 3 below).

\[
\frac{4 \times 1 + 4 \times (-0.5) + 4 \times 0.5 + 4 \times 0.75}{1 + (-0.5) + 0.5 + 0.75} = 4
\]

6. From this result, we know that the confidence value is quite high. Therefore, it can be confirmed that the system is in abnormal status and it has to report this situation to the network security administrator. On the other hand, it had better to be provided the automatic control interface, the fast response event interface, and the real time monitored interface for the final alert module. Therefore, because of that, the HNSMS system will be able to produce timely and effective response.

7. Through the friendly users’ interface, the network security administrator can amend and adjust the content information from the knowledge module anytime. For example, when the administrator found that the confidence degree of the Login Failure on the HIDS is not only 40%, the administrator can process the confidence tuning. Therefore, when the HNSMS system processes the alert fusion next time, the operation procedure will be more precise.

From the foregoing case study, when the attacker launched the attack at the first timing, only two security equipments sent out the alert. If the alert information does not process the Attack Alert Fusion via the HNSMS system and the alert does not report the “Login Failure” to the security administrator, the security administrator will have the higher possibility to look at the alert as useless information and the administrator will ignore this attack event. Although it seems that the alert is the useless information after processing the Attack Alert Fusion in the system, the alert can be executed the further processing such as the Overall Alert Fusion via the security policy and other auxiliary information. It will be a higher possibility to find out the attack behavior and the administrator can make appropriate response to the attack behavior.

Case Study Two: Virus Invasion:

When a user opens the E-mail which is infected by the Sasser virus, the infected computer will be sending a lot of network packets into the network. Through sending a lot of malicious E-mail, it can achieve the goal which is disseminating the virus. At this time, because of the malicious procedure invasion, the four kinds of the network security sensors will be operated. In this case, the NIDS and the Anti-viruses will send the alert to the HNSMS server but the Firewall and the HIDS do not send any information. Moreover, when the NIDS and the Anti-virus sent the alert data to the HNSMS server, the server will be analyzing the alert events (see Figure 10).

![Figure 10: Case Study for the Virus Invasion](image)

In this case, the alert will be sent to the HNSMS server from two kinds of the network security sensors. Different network security sensors will prevent different security events. From this case, we know that it would be happened certain level of the alert conflict. Therefore, the alert will be sent to the HNSMS server to process the integration. The procedure is shown below.

1. In order to process the event analysis, we refer to the information from the knowledge module and this module supports the information. We use the information to give the confidence and the weight on the alert. We also use the related judgement information from the knowledge module to process the Attack Alert Fusion. The Table 2 shows each confidence and weight from the network security sensors in this case study.
2. We fuse the confidence from two kinds of the network security sensors to make the judgement whether the computer system is in secure state or not. We use the concept of the data fusion from the Dempster-Shafer theory. Moreover, we also use the value of the confidence and the weight from the network security sensors. We use the information which we got and we use it into the formula 2. The result of the Attack Alert Fusion is shown below.

\[ m_{24}(A_5) = \frac{0.2^{0.2} \times 0.7^{0.4}}{0.2^{0.2} \times 0.7^{0.4} + 0.98^{0.2} \times 0.3^{0.4}} = 0.52 \]

3. Hypothesis: when the confidence value of the Attack Alert Fusion is higher, we can say that the system is in abnormal state. The HNSMS has to report this situation to the network security administrator immediately. The threshold value will be set up by the different situation.

4. The system interface had better to be provided the automatic control interface, the fast response event interface, and the real time monitored interface for the final alert module. Thus, because of that, the HNSMS system will be able to produce timely and effective response for the security events.

From the above case study, when the virus is processing proliferation at the first time, only two security systems sent out the alert. The HNSMS system processes the Attack Alert Fusion and reports the abnormal state to the network security administrator.

5. Conclusion

The HNSMS system processes the Attack Alert Fusion and reports to the administrator. The HNSMS system has to use other auxiliary information to find out the abnormal state. The HNSMS system will execute two modules of the Attack Alert Fusion and the Overall Alert Fusion. Furthermore, as soon as the system receives the information, the system will process the Alert Confidence Fusion. If the alert fusion does not reach the threshold value, the network is in secure state. Thus, the HNSMS system will give up reporting this alert to the administrator. On the other hand, we consider that it would be probably failed to report the alert problem after the alert fusion in a specific timing. Therefore, the HNSMS system has to cooperate with the security policy which is the Policy Definition module. The module is associated with other auxiliary data to recognize the integral security state of the computer system and the network.

6. References


