



Issues with Fusion of Heterogeneous IDS with Reliability

Mr. Vrushank Shah*

PhD Scholar,

Gujarat Technological University, India

Dr. A. K. Aggarwal

Vice Chancellor,

Gujarat Technological University, India

Abstract— Internet and its related infrastructure have achieved a great developmental leap during the last decade. However, along with the development there is more concern about the security issues. Intrusion detection System (IDS) is a system that detects an attack and raises an alert. Individual IDS has its limitations in terms of attack coverage and number of false positives. The present paper shows the fusion of multiple IDS having heterogeneous nature. However the success of the fused system depends on the effectiveness of individual IDS involved in fusion process. The present paper raises issues which are to be deal with while performing fusion process.

Keywords— Intrusion detection system, Sensor fusion, reliability, Dempster-shafer rule, belief mass assignment.

I. INTRODUCTION

The importance of internet is being increasing in our day-to-day life. Internet has opened a hidden well of knowledge. Now knowledge sharing and data transfer can be done with more ease. Research in the field of Science and Technology has reached new avenues with the help of internet. E-shopping, e-marketing, e-banking are few other advantages of internet. Generation by generation it is adding new applications to its domain. The present generation has seen a great leap in wireless technology. Internet along with wireless technology has created a kind of revolution in the field of information communication technology. Every revolution is like two sides of coin, it can bring a good change and a bad also. The good about internet is all the benefits it provides. However, on the other side internet security is a matter of concern. These is due to illegal, unethical or reprehensible behavior of people, unauthorized use of system or network, services being denied and system failing to respond. A network is asset of large amount of information. Every network has fixed security policies. An attempt to violate security system is called an attack or an intrusion [2]. Thus an attack/intrusion is an act of disrupting, disabling, destroying or maliciously controlling a computing environment infrastructure or destroying integrity of the data or stealing controlled information. Intrusion results in services being denied, system failing to respond or data stolen or lost. Intrusion detection System (IDS) is a system that detects an attack and raises an alert. It is an active process or device that analyses system and network activity for unauthorized entry and/or malicious activity [3]. IDS in general can be of two types: Anomaly based IDS and Signature based IDS. Anomaly based IDS looks for deviation from normal usage behaviour to identify abnormal behaviour. By defining what's normal, any violation can be identified whether it is a part of threat model or not. Signature based IDS recognize patterns of attacks. It contains attack descriptions or signatures and matches them against the audit data stream, looking for evidence of known attacks.

The major concern in the area of sensor fusion is to make a robust fusion model that combines local decisions of single IDS and outputs a global decision [2]. Section-II discusses about sensor fusion, some basic definitions and list out some basic rules of fusion. The importance of incorporating reliability parameter for sensor fusion is discussed in Section- III. In Section-VI we summarize our conclusion derived from survey.

II. SENSOR FUSION

Sensor fusion can be defined as the process of combining local decisions given by each sensor about the network situation and reaching a global conclusion about the network [2]. There are varieties of fusion rules available in literature each based on some basic property. Following sub-section will give you the brief description of the fusion properties.

i) Definitions

a) Frame of Discernment

It is the complete (exhaustive) set describing all the valid elements about which an IDS is capable of giving evidence. Generally, the frame is denoted as Θ . The elements in the frame must be mutually exclusive. If the number of the elements in the set is n , then the power set of all subsets of (Θ) will have 2^n elements.

b) Belief probability assignment

The theory of evidence assigns a belief mass to each subset of the power set. It is a positive number between 0 and 1. It exists in the form of a probability value.

If Θ is the frame of discernment, then a function $m: 2^\Theta \rightarrow [0, 1]$ is called a bpa, whenever, $m(\emptyset) = 0$ and

$$\sum_{X \subseteq \Theta} m(X) = 1 \quad (1)$$

c) *Belief Function*

Given an Frame of discernment of Θ and a body of empirical evidence $\{m(y_1), m(y_2), m(y_3), \dots\}$, the belief committed to $X \in \Theta$ is

$$Bel(X) = \sum_{Y \subseteq X} m(Y_i) \quad (2)$$

Also, $Bel(\Theta) = 1$

d) *Plausibility function*

The plausibility is the sum of all the masses of the sets Y that intersect the set of interest X. It is given by

$$Pl(X) = \sum_{Y|Y \cap X \neq \phi} m(Y_i) \quad (3)$$

The interval $[Bel(X), Pl(X)]$ is called belief range. Plausibility and belief are related as follows:

$$Pl(X) = 1 - Bel(X)$$

ii) **Properties of fusion operator**

Here, we have considered the case of two sensors. However, each rule can be extended for n sensors. Let us consider a hypothesis X which two sensors are evaluating. So we have two masses, one from each sensor denoted by $m_1(Y)$ and $m_2(Z)$

1) *Conjunctive rule*

If both sensors is giving true information then conjunctive rule is applied which means consensus between the sensors.

For $X \in 2^\Theta$. We have,

$$m_{12}(X) = \sum_{\substack{Y, Z \in 2^\Theta \\ Y \cap Z = X}} m_1(Y)m_2(Z) \quad (4)$$

The amount of mass allotted to null set is called the amount of conflict between two sensors.

$$m_{\cap}(\phi) = \sum_{\substack{Y, Z \in 2^\Theta \\ Y \cap Z \neq X}} m_1(Y)m_2(Z) \quad (5)$$

This rule has a limitation that if any one source fails i.e. its mass function is zero, irrespective of all other sources the fusion result will be zero.

2) *Disjunctive rule*

If anyone sensor is providing true information then we use disjunctive rule which means union between two sensors.

For $X \in 2^\Theta$. We have,

$$m_{\cup}(X) = \sum_{\substack{Y, Z \in 2^\Theta \\ Y \cup Z = X}} m_1(Y)m_2(Z) \quad (6)$$

$$m_{\cup}(\phi) = 0$$

Here, Single sensor failure can be tolerated. However, consensus decision is not obtained.

3) *Dempster- Shafer rule*

D-S rule [1] is a mathematical theory of evidence used to combine evidences from different sources and arrive at a degree of belief. D-S rule is completely based on conjunctive property and is given below,

$$m_{12}(X) = \frac{1}{1 - k_{12}} \sum_{\substack{Y, Z \in 2^\Theta \\ Y \cap Z = X}} m_1(Y)m_2(Z) \quad (7)$$

Here k_{12} is the amount of conflict between sources and is given by equation (5). The major issue with D-S theory is dealing with the conflicting situations.

4) Consensus rule

Consensus rule has been proposed by Audun josang [2]. The rule has been defined for binary frame of discernment. However, it can be extended to m-ary frame of discernment by using coarsening method. Let Θ be the binary frame of discernment containing elements x and \bar{x} . Let m_Θ be the belief mass assignment on Θ .

Josang defines four different metrics. Each one of that is given by following definitions.

$$\begin{aligned} \text{Belief } b(x) &= \sum_{y \subseteq x} m_\Theta(y) \\ \text{Disbelief } d(x) &= \sum_{y \cap x = \emptyset} m_\Theta(y) \\ \text{Uncertainty } u(x) &= \sum_{\substack{y \cap x \neq \emptyset \\ y \not\subseteq x}} m_\Theta(y) \\ \text{Relative atomicity } a(x/y) &= \frac{|x \cap y|}{|y|} \end{aligned}$$

The final fusion rule is defined by combining above four metrics.

5) Yager's rule

Yager proposed amendment in Dempster-shafer [3] rule of combination by taking ground probability mass assignment instead of basic probability mass assignment (m) to overcome the issues of conflicting evidences in case of D-S theory. The only difference was normalization factor and mass assigned to universal set Θ .

$$\begin{aligned} q(X) &= \sum_{Y \cap Z = X \neq \emptyset} m_i(Y) m_i(Z) \\ q(\emptyset) &= m_i(\emptyset) m_i(\emptyset) + \sum_{Y \cap Z = \emptyset} m_i(Y) m_i(Z) \end{aligned}$$

Here, Conflicts were ported over to uncertainty. So, its advantage is that it has solved the problem of conflicting situations but raises new problem of more uncertain or inconclusive result.

III. RELIABILITY

The best of fusion rule will depends on the effectiveness of sources involved in the fusion process. Thus, it inherently depend on how well a individual sensor classifies an attack One issue of concern with all types of fusion rules is that fusion rules consider the sources of information to be reliable. According to [1] in the heterogeneous environment this does not hold true. One of the reasons is that remote sensors are considered less reliable compared to local sensors. Assuming all the sensors behaving in same way could lead to an incorrect fusion result. Each sensor has different detecting capabilities and they all will behave in different manner for different class of attacks within the same domain. Some sensors might give complementary results while some may be giving redundant information and failure of them can be tolerated. However, instead of completely ignoring sensor's capability we need to find out a parameter of reliability i.e. reliability co-efficient. In general reliability of the sensor and data supplied by sensor has a direct relationship. However, the link between two is highly complex.

Thus, reliability can be defined as level of trust we can put on sensor about the information it provides. Following example shows the importance of reliability. Here we have considered three sensors which are classifying the data in three different attack class categories. The masses of all three sensors are fused using Dempster-Shafer rule. Table-1 shows the fused results without consideration of reliability and it is found that the fused answer is erroneous. Let us consider sensor-1 to be 25 % reliable, sensor-2 to be 10% reliable and sensor-3 is 95 % reliable. It can be seen from Table-2 that the erroneous result obtained due to fusion rule is highly scaled down.

TABLE I
MASSES PROVIDED BY SENSOR WITHOUT CONSIDERING RELIABILITY

Class	Sensor-1	Sensor-2	Sensor-3	Fusion result
Attack Class-1	0.9	0.8	0.0	0.0
Attack Class-2	0.1	0.1	0.1	1.0
Attack Class-3	0.0	0.1	0.9	0.0

TABLE III
MASSES PROVIDED BY SENSOR CONSIDERING RELIABILITY

Class	Sensor-1	Sensor-2	Sensor-3	Fusion result
Attack Class-1	0.225	0.08	0.0	0.0
Attack Class-2	0.225	0.10	0.095	0.00002
Attack Class-3	0.0	0.10	0.855	0.0

IV. DISCUSSION AND CONCLUSION

To determine the effect of above fusion rules on actual sensor fusion problem and to design an effective fusion rule. We have considered three proposition hypothesis and three sensors evaluating three propositions.

Following conclusions are derived from the result obtained:

- The fusion rule should be capable of handling the conflicting situations between the sensors. Thus, if all sensors agree a particular proposition, Conjunctive rule should be utilized. If any sensor fails to give evidence for particular propositions, Disjunctive rule is used. Dempster-shafer rule has its limitations while dealing with conflicting sources. However consensus operator can handle conflicting situations.
- The second requirement raised from above survey is that all the fusion rules consider the information provided by the sensor is reliable. However, there is requirement to find actual reliability value of sensor.
- The third and most important requirement is to determine the reliability of fusion result itself.

REFERENCES

- [1] Helen Svensson, Audun Jøsang, Correlation of Intrusion Alarms with Subjective Logic, Generic System, Distributed Systems Technology Centre, Brisbane, 2010.
- [2] A. Jøsang. A Logic for Uncertain Probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 9(3):279–311, June 2001.
- [3] G. Giacinto, and F. Roli, Intrusion detection in computer networks by multiple classifier systems, In Proc. of the 16th International Conference on Pattern Recognition (ICPR), Volume 2, Quebec City, Canada, pp. 390393.IEEE press, 2002.
- [4] S. T. Brugger, J. Chow, An assessment of the DARPA IDS evaluation dataset using Snort, Tech. Report, CSE-2007-1, 2005
- [5] C. Siaterlis, B. Maglaris, Towards Multisensor Data Fusion for DoS detection, ACM Symposium on Applied Computing, 2004.
- [6] W. Hu, J. Li, Q. Gao, Intrusion Detection Engine on Dempster-Shafer's Theory of Evidence, Proceedings of International Conference on Communications, Circuits and Systems, vol.3, pp. 1627-1631, Jun 2006.
- [7] H. Wu, M. Seigel, R. Stiefelhagen, J. Yang, Sensor Fusion using Dempster-Shafer Theory, IEEE Instrumentation and Measurement Technology Conference, 2002