Complex Intell. Syst. (2017) 3:33–39
DOI 10.1007/s40747-016-0033-5

ORIGINAL PAPER

Performance improvement of intrusion detection with fusion of multiple sensors

An evidence-theory-based approach

Vrushank Shah[1] · **Akshai K. Aggarwal**[2] · **Nirbhay Chaubey**[3]

Received: 19 March 2016 / Accepted: 15 November 2016 / Published online: 22 November 2016

Abstract Intrusion detection has become a challenging task with the rapid growth in numbers of computer users. The present-day technology requires an efficient method to detect intrusion in the computer network system. Intrusion detection system is a classifier which collects evidences for the presence of intrusion and raises an alarm for any abnormalities present. However, the use of intrusion detection system encounters two major drawbacks: higher false alarm rate and lower detection rate; these limit the detection performance of intrusion detection system. A prospective approach for improving performance is through the use of multiple sensors/intrusion detection system. Evidence theory is a mathematical theory of evidence which is used to fuse evidences from multiple sources of evidence and outputs a global decision. The work in this paper discusses the limitations and issues with evidence theory and proposes a modified framework for fusion of alarms of multiple intrusion detection systems.

Keywords Intrusion · KDD99 · Fusion · Evidence theory · False alarm rate

✉ Vrushank Shah
vrushank26@yahoo.in

[1] 21/246 Parasnagar-2, Solaroad, Ahmedabad, India

[2] Gujarat Technological University, Chandkheda, Ahmedabad, India

[3] S.S. Agarwal Institute of Computer Science, Navsari, Gujarat, India

Introduction

The technological advancement in computer network system and its related infrastructure is the reason for an increased occurrence rate of computer intrusions. An intrusion is defined as any set of actions to violate the security protocol of a computer network system [8]. Intrusion detection system is a classifier which collects evidences for the presence of intrusion and raises an alarm for any abnormalities present [7]. There is tremendous research going on to improve the efficiency of an intrusion detection system. The major research in [2,4,9,12] shows that intrusion detection system encounters two major drawbacks: higher false alarm rate and lower detection rate. A prospective approach to improve the detection rate and to reduce the false alarm rate is through the use of distributed IDS systems.

The distributed IDS systems consist of multiple intrusion detection systems which are dissimilar in nature. The dissimilarity is by the fact that they extract different features of network traffic or might have completely different detection algorithms, viz., signature-based IDS or anomaly-based IDS [6]. Authors in [14] present the alert fusion process and show that when anomaly detection techniques and signature recognition techniques are applied simultaneously to the same observed activities of computer and network systems, anomaly detection techniques and signature recognition techniques complement one another for achieving a high detection rate and a low false alarm rate. However, along with the potential benefits of distributed IDS system, deciding an efficient fusion rule to combine evidences from diverse IDS systems is still a loophole. Also, there is a concern on finding the reliability value of an IDS. The work in this paper proposes a new fusion rule that incorporates reliability of evidence and also efficiently handles the information for diverse IDS.

Evidence theory

Evidence theory is a mathematical theory used to combine the evidence from multiple sources of information to calculate the probability of an event. The Dempster–Shafer theory proposed by Arthur Dempster and modified by Glenn Shafer in [11] is the first mathematical theory proposed to combine uncertain information of sources to make an inference. The fusion rule proposed under Dempster–Shafer framework is called as Dempster–Shafer rule. Dempster–Shafer rule has been a topic of debate for researchers working in the field of information fusion.

The fusion theory is used to combine masses from n evidence sources and outputs a fused decision. For number of evidence sources $n \geq 2$, let $\Theta = \{\theta_1, \theta_2, \theta_3, \ldots, \theta_n\}$ be the frame of discernment for the fusion problem under consideration having n exclusive and exhaustive hypothesis. The sets of all subsets of Θ is called as power-set of Θ and is denoted by 2^{Θ}. In Shafer's framework [11], the basic belief assignment (bba) is a function m from 2^{Θ}, the power set of Θ to [0, 1]. The mass assignment will satisfy the property

$$m(\phi) = 0 \quad \text{and} \quad \sum_{A \in 2^{\Theta}} m(A) = 1 \tag{1}$$

Let $m_1(B)$ and $m_2(C)$ be two independent masses from two sources of evidence; then the combined mass $m(A)$ obtained by combining $m_1(B)$ and $m_2(C)$ through the rule:

$$m(A) = \frac{\sum_{\substack{B,C \in 2^{\Theta} \\ B \cap C = A}} m_1(B) m_2(C)}{1 - \sum_{\substack{B,C \in 2^{\Theta} \\ B \cap C = \phi}} m_1(B) m_2(C)} \tag{2}$$

$$m(\phi) = 0 \tag{3}$$

Reliability of intrusion detection system

The purpose of designing a fusion-based distributed intrusion detection system is to detect intrusion which was rather not detected by single IDS system. The success of fusion depends upon the accuracy of evidence provided by the individual IDS. Majority of fusion rules proposed in the literature along with DS rule assume all evidences to be equally reliable and assign the same weightage during the fusion process. However, it is often the case that some IDS are completely reliable, while others are completely unreliable for a particular frame of discernment. Reliability of IDS is defined as the level of trust about the evidence provided by the IDS for the presence of an intrusion [10]. Reliability indicates the relative stability of IDS whose value lies between 0 and 1 [10].

Within the framework of distributed IDS, the evidence provided by IDS with zero reliability should be completely ignored and the evidence provided by IDS with higher reliability should be given more weightage. This calls for a fusion rule that effectively handles the reliability of each evidence while making the decision. However, one major concern in incorporating reliability of IDS into the fusion rule is the problem of obtaining reliability values. The problem of finding reliability can be related to the problem of conflict between various intrusion detection systems. The mere existence of conflict between the evidences provided by intrusion detection systems indicates the presence of an unreliable IDS which may cause the fusion result to be complementary from reality.

Another approach for finding reliability is to relate reliability with the true alert rate of IDS. In this approach, it is assumed that the IDS having highest true alert rate and lowest false alert rate will be assigned highest reliability and, thereby, given highest weightage in fusion process, while all other IDS is assigned relative reliability value based on their true alert rate and false alert rate. The approach of assigning reliability based on true alert rate requires the ground truth knowledge. While the approach of assigning reliability based on conflict between the IDS can work without the knowledge of ground truth.

Alert fusion method

A distributed IDS is a framework where multiple heterogeneous IDS systems are deployed to sniff the incoming network traffic. Each IDS while sniffing the incoming network traffic raises an alert for the presence of an attack. The alerts can be positive alerts or negative alerts. Positive alerts are the alerts favouring the occurrence of an intrusion/attack and negative alerts are alerts opposing the presence of an intrusion/attack. The alerts generated by IDS are converted to a mass value. Alert-to-mass conversion is done using the formula proposed by Jøsang [5]. If we denote the hypothesis that attack is present by H and attack not present by $-H$, then, according to [5], we have,

$$m(H) = \frac{P}{P + N + C} \tag{4}$$

$$m(-H) = \frac{N}{P + N + C} \tag{5}$$

$$m(H \text{ or } -H) = \frac{C}{P + N + C} \tag{6}$$

where P is the positive evidence in favour of hypothesis H, N is negative evidence opposing the hypothesis H or favouring hypothesis $-H$, and C is constant which is equal to 2 for binary frame of hypothesis. $m(H)$ is the mass value for hypothesis H. $m(H \text{ or } -H)$ is mass value for hypothesis H or H and can be called $m(\text{uncertain})$ i.e., mass value for

uncertainty between H and $-H$. The converted mass is then fused using fusion rule to make an inference.

The Dempster–Shafer rule as defined by Eq. (2) has the following limitations:

- The Dempster–Shafer rule does not incorporate the reliability of source whose evidences are to be fused. Thus, there is no real-time criteria which assign a numerical value of reliability to the evidence given by the source.
- The Dempster–Shafer rule considered all the sources of evidence to be equally reliable. However, in fusion framework, there might be some unreliable sources which mislead the fusion rule to give wrong decision.
- Another drawback in Dempster–Shafer rule as suggested by Goodman [3] is that in an environment consisting of many hypotheses and many sources, it is difficult to decide whether to accept or reject the result of such fusion rule. If sources of evidences are highly conflicting, the DS rule completely fails. If analyst blindly believes on the result, then the decision can be misleading or complementary.

To overcome the limitations of Dempster–Shafer rule, we propose a new fusion rule which is the modification of Shafer's framework [11]. The proposed rule is defined as below:

$$m(A) = \mathrm{CRF}(A) \sum_{\substack{B,C\in 2^{\Theta} \\ B\cap C=A}} m_1(B)m_2(C) + \mathrm{DRF}(A) \sum_{\substack{B,C\in 2^{\Theta} \\ B\cup C=A}} m_1(B)m_2(C) \tag{7}$$

where

$$\mathrm{CRF}(A) = \prod_n R_n \tag{8}$$

$$\mathrm{DRF}(A) = \left(1 - \prod_n R_n\right)\left(1 - \prod_n (1 - R_n)\right) \tag{9}$$

Here, R_n is the reliability value of nth source of evidence. $\mathrm{CRF}(A)$ is conjunctive reliability value about A, and $\mathrm{DRF}(A)$ is disjunctive reliability value about A. CRF and DRF values act as weighting factors to compromise between conjunctive mass and disjunctive mass. The complete flow diagram of the proposed alert fusion method is as shown in Fig. 1.

Experimental setup

For alert fusion of multiple intrusion detection systems, four heterogeneous intrusion detection systems namely, Snort,

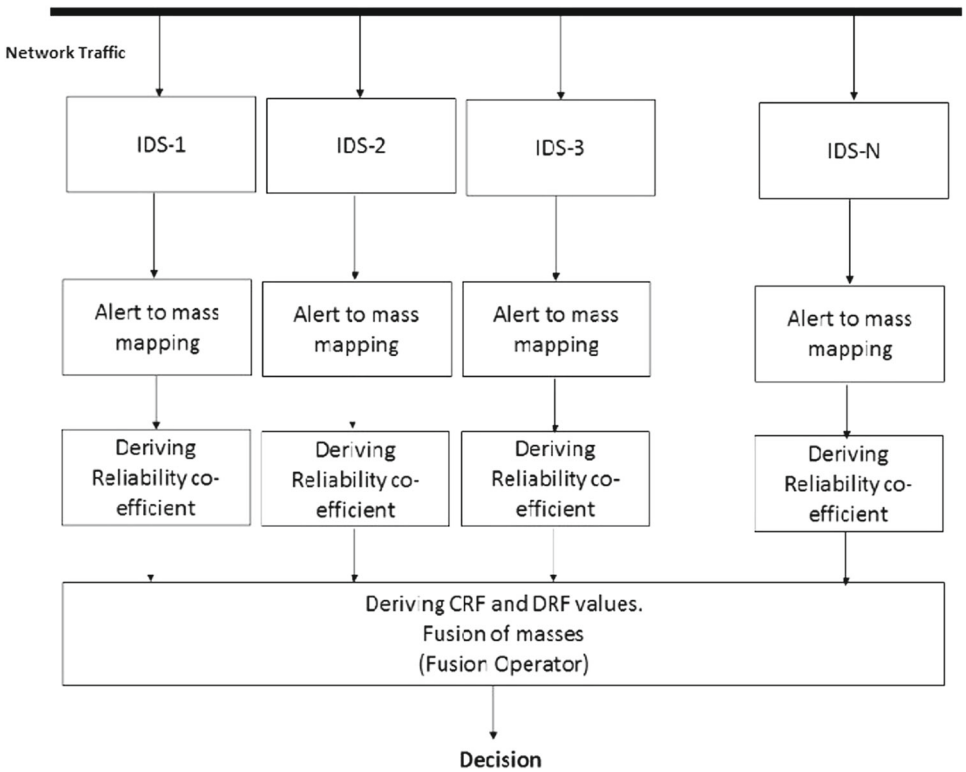

Fig. 1 Flowchart of the proposed fusion approach

Suricata, packet header anomaly detector (PHAD) and network anomaly detector (NETAD) have been selected. The reason behind such selection is that snort and suricata are signature-based intrusion detectors, while PHAD and NETAD are anomaly detectors. Thus, both types are complementary to one another which enhances the performance of fused IDS. The simulation environment consists three third-generation Intel Core i5 processors (1.6 GHz); Operating system installed is Linux Ubuntu with 4 GB RAM. One machine is deployed with signature-based IDS such as snort and suricata. Another machine is deployed with anomaly detectors such as PHAD and NETAD. Third machine acts as an attacker machine having KDD99 Dataset. The packets of the dataset are being replayed with TCPREPLAY tool [13].

KDD99 dataset

KDD is the abbreviation of knowledge discovery in databases. KDD refers to the overall process of recovering knowledge from data. Specifically, KDD99 is designed for evaluation of intrusion in computer networks [1]. It is like a benchmark on which many researchers have tested their methodologies. The dataset is available in tcpdump format. The original tcpdump files were preprocessed for utilization of intrusion detection benchmark. KDD99 dataset consists of 4,900,000 single connection vectors, each of which contains 41 features and is labeled as either normal or an attack. The attack falls in one of the types and subtypes shown in Table 1. The list of 41 features of dataset is shown in appendix as Table 4. The KDD99 was preprocessed, and then, total 3456 packets containing attack and non-attacks packets in various types were loaded on the network and are replayed using TCPREPLAY [13].

Table 1 Types of attack categories in KDD99 dataset

Attack type	Sub attack types
DOS	Smurf, teardrop, pod, back, land, apache2, udpstrom, mailbomb, processtable, Neptune
Probe	Ipsweep, portsweep, nmap, satan, saint, mscan
U2R	Bufferoverflow, rootkit, perl, loadmodule
R2L	Imap, ftpwrite, guesspasswd, multihop, phf, spy, warezclient, warezmaster

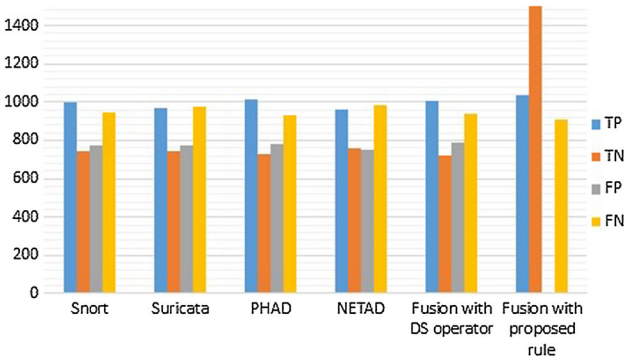

Fig. 2 Comparison of individual IDS with fusion with DS and fusion with proposed rule in terms of TP, TN, FN and FP with conflict as a reliability parameter

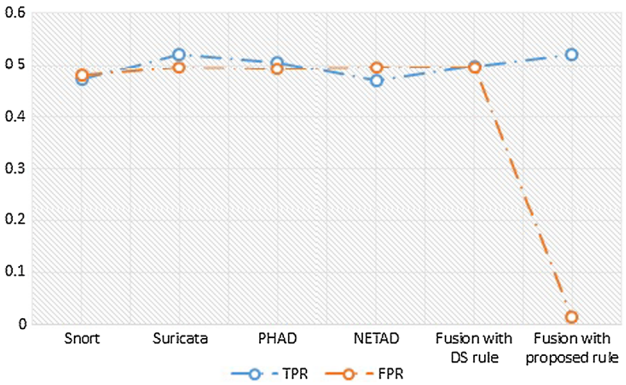

Fig. 3 Comparison of TPR and FPR values for proposed rule with DS rule

Results

The evaluation of proposed rule against KDD99 [1] is done by considering two different approaches of reliability. The experiment focuses on detection of smurf attack. Hence, the frame of discernment is $\Theta = \{\text{smurf}, -\text{smurf}, \theta\}$. In KDD99

Table 2 Comparison of individual IDS with fusion with DS and fusion with proposed rule in terms of PPV, NPV, TPR, FPR and ACCURACY with conflict as a reliability parameter

	Snort	Suricata	PHAD	NETAD	Fusion with DS rule	Fusion with proposed rule
TPR	0.5129	0.4974	0.5221	0.4938	0.5185	0.5314
FPR	0.5093	0.5099	0.5172	0.4987	0.5218	0.0073
PPV	0.5642	0.5564	0.5648	0.5601	0.5609	0.9895
NPV	0.4393	0.4313	0.4400	0.4351	0.4358	0.6223
ACCURACY	0.5032	0.4942	0.5049	0.4971	0.5009	0.7332

Table 3 Comparison of individual IDS with fusion with DS and fusion with proposed rule in terms of PPV, NPV, TPR, FPR and ACCURACY with true positive rate as a reliability parameter

	Snort	Suricata	PHAD	NETAD	Fusion with DS rule	Fusion with proposed rule
TPR	0.4712	0.5221	0.5051	0.4681	0.4985	0.5216
FPR	0.4788	0.4954	0.4914	0.4960	0.4940	0.0146
PPV	0.5545	0.5754	0.5693	0.5482	0.5647	0.9788
NPV	0.4339	0.4509	0.4443	0.4243	0.4397	0.6160
ACCURACY	0.4931	0.5145	0.5067	0.4838	0.5017	0.7248

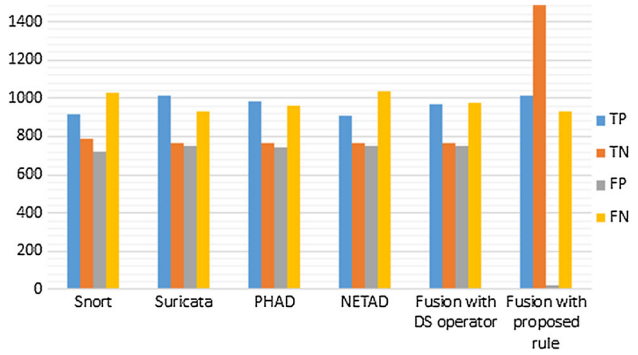

Fig. 4 Comparison of individual IDS with fusion with DS and fusion with proposed rule in terms of TP, TN, FN and FP with true positive rate as a reliability parameter

Fig. 5 Comparison of TPR and FPR values for proposed rule with DS rule

dataset [1], total 1944 smurf attack is present. Table 2 shows the results of true positive rate (TPR), false positive rate (FPR), positive prediction value (PPV) and negative prediction value (NPV) of Snort, Suricata, NETAD and PHAD as an individual IDS. Table 2 also shows the result of alert fusion of Snort, Suricata, NETAD and PHAD using Dempster–Shafer rule and the proposed rule. The results of fusion are derived by considering conflict between IDS evidence as a reliability factor. It can be observed from Fig. 2 that with alert fusion using proposed rule, the number of true negatives are higher compared to individual IDS, while there is a drastic reduction in the number of false positives. Figure 3 shows that the alert fusion with proposed rule drastically reduces the false positive rate (FPR) without affecting the true positive rate.

Table 3 shows the results of true positive rate (TPR), false positive rate (FPR), positive prediction value (PPV) and negative prediction value (NPV) of Snort, Suricata, NETAD and PHAD as an individual IDS. Table 3 also shows the result of alert fusion of Snort, Suricata, NETAD and PHAD using Dempster–Shafer rule and the proposed rule. The results of fusion are derived by considering true positive rate of an IDS as a reliability factor. Figures 4 and 5 show the comparison of individual IDS systems with fusion using DS and fusion using proposed rule in terms of true positives, true negatives, false negatives and false positives and FPR and TPR, respectively.

Conclusion

Distributed alert fusion can be achieved with Dempster–Shafer rule. The proposed alert fusion system described here improves the performance of detection by reducing the ad hoc created by high amount of false alerts. The reduction in false alerts is achieved by the fact that the DS rule assumes all evidence sources to be equally reliable, while the proposed rule incorporates variable reliability of IDS measured either from conflict between IDS or from true positive rate of IDS.

Appendix

See Table 4.

Table 4 KDD'99 features list

Feature number	Feature name	Description
1	Count	No. of connections to the same host as the current connection in the last 2 s
2	Destination bytes	Bytes sent from destination to source
3	diff srv rate	Percentage of connections to different services
4	dst host count	Count of connections having the same destination hosts
5	dst host diff srv rate	Percentage of different services on the current host
6	dst host rerror rate	Percentage of connections to the current host that have an RST error
7	dst host same src port rate	Percentage of connections to the current host having the same src port
8	dst host same srv rate	Percentage of connections having the same destination host and using the same service
9	dst host serror rate	Percentage of connections to the current host that have an S0 error
10	dst host srv count	Count of connections having the same destination host and using the same service
11	dst host srv diff host rate	Percentage of connections to the same service coming from different hosts
12	dst host srv rerror rate	Percentage of connections to the current host and specified service that have an RST error
13	dst host srv serror rate	Percentage of connections to the current host and specified service that have an S0 error
14	Duration	Duration of the active connection
15	Flag status	Flag of the connection
16	Hot	No. of "hot" indicators
17	Is guest login	1 if the login is a "guest" login; otherwise 0
18	Is host login	1 if the login belongs to the "host"; otherwise 0
19	Land	1 if connection is from/to the same host/port; otherwise 0
20	Logged in	1 if successfully logged in; otherwise 0
21	Num access files	No. of operations on access control files
22	Num compromised	No. of compromised conditions
23	Num failed logins	No. of failed logins
24	Num file creations	No. of file creation operations
25	Num outbound cmds	No. of outbound commands in an ftp session
26	Num root	No. of "root" accesses
27	Num shells	No. of shell prompts
28	Protocol type	Connection protocol (e.g. tcp, udp)
29	rerror rate	Percentage of connections that have "REJ" errors
30	Root shell	1 if root shell is obtained; otherwise 0
31	Same srv rate	Percentage of connections to the same service
32	serror rate	Percentage of connections that have "SYN" errors
33	Service	Destination service (e.g. telnet, ftp)
34	src bytes	Bytes sent from source to destination
35	srv count	No. of connections to the same service as the current connection in the last 2 s
36	srv diff host rate	Percentage of connections to different hosts
37	srv rerror rate	Percentage of connections that have "REJ" errors

Table 4 continued

Feature number	Feature name	Description
38	srv serror rate	Percentage of connections that have "SYN" errors
39	su attempted	1 if "su root" command attempted; otherwise 0
40	Urgent	No. of urgent packets
41	Wrong fragment	No. of wrong fragments

References

1. Archive TUK (1999) Kdd99 dataset. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
2. Brugger ST (2004) Data mining methods for network intrusion detection. University of California at Davis
3. Goodman IR, Mahler RP, Nguyen HT (2013) Mathematics of data fusion, vol 37. Springer Science & Business Media, Dordrecht
4. Huang LC, Hwang MS (2012) Study of intrusion detection systems environment. J Electron Sci Technol 4:6
5. Jøsang A (2011) Subjective logic. Book draft
6. Katar C (2006) Combining multiple techniques for intrusion detection. Int J Comput Sci Netw Secur 6(2B):208–218
7. Kendall K (1999) A database of computer attacks for the evaluation of intrusion detection systems. Technical report, DTIC Document
8. McHugh J, Christie A, Allen J (2000) Defending yourself: the role of intrusion detection systems. IEEE Softw 17(5):42
9. Raut AS, Singh KR (2014) Anomaly based intrusion detection—a review. Int J Netw Secur 5(3):7
10. Rogova GL, Nimier V (2004) Reliability in information fusion: literature survey. In: Proceedings of the seventh international conference on information fusion, vol 2, pp 1158–1165
11. Shafer G et al (1976) A mathematical theory of evidence, vol 1. Princeton University Press, Princeton
12. Thomas C, Balakrishnan N (2009) Performance enhancement of intrusion detection systems using advances in sensor fusion. Supercomputer Education and Research Centre Indian Institute of Science, Doctoral Thesis. http://www.serc.iisc.ernet.in/graduation-theses/CizaThomas-PhD-Thesis.pdf
13. Turner A, Bing M (2012) tcpreplay tool
14. Ye N, Li X, Chen Q, Emran SM, Xu M (2001) Probabilistic techniques for intrusion detection based on computer audit data. IEEE Trans Syst Man Cybern Part A: Syst Hum 31(4):266–274