Reliable Alert Fusion of Multiple Intrusion Detection Systems

Vrushank M. Shah[1], and A. K. Agarwal[2]
(Corresponding author: Vrushank M. Shah)
Department of Electronics and Communication, Indus University[1]
21/246 Parasnagar-2, Solaroad, Ahmedabad, Gujarat
Vice Chancellor, Gujarat Technological University[2]
(Email: vrushank26@yahoo.in)
(Received Jan. 27, 2016; revised and accepted Apr. 6 & Apr. 25, 2016)

Abstract

Alert Fusion is a process of combining alerts from multiple Intrusion Detection Systems to make a decision about the presence of attack or intrusion. A reliable decision from an alert fusion requires that Intrusion detectors involved in the fusion process generates fully reliable alerts. The unreliable alerts from intrusion detectors may completely misleads the decision making process. The existing alert fusion operators doesn't incorporate reliability of Intrusion detectors. In this work, we have proposed a novel alert fusion method which overcomes the limitations of existing fusion methods and fulfils the requirements for alert fusion domain. We have demostrated the results for two different approaches of deriving reliability value of intrusion system detector which are based on conflict and true positive rate of intrusion detectors. The results shows the robustness of proposed rule in fusing alerts from multiple intrusion detection system. Our proposed approach shows a drastic reduction in false positive rate without affecting the true positive rate.

Keywords: Alert fusion, DARPA99, IDS, KDD99, reliability

1 Introduction

Intrusion Detection system (IDS) is a security system that monitors the traffic on a computer network system, analyzes the traffic and generates a warning called as alert or alarm in case any abnormalities found [5, 11]. In this sense intrusion detection system (IDS) is defined as a classifier which collects the evidences about the presence or absence of an intrusion. The evidences collected are usually incomplete, uncertain, contradictory or conflicting and may be complementary. The use of single IDS as a detector has two major drawbacks: higher false alarm rate and lower intrusion detection coverage, these limits the detection performance of an IDS in presence of multiple categories of attack/intrusion.

An prospective approach of tackling with multiple categories of attack is through the use of distributed IDS [1]. The distributed IDS consists of multiple intrusion detection systems which are dissimilar in nature. They are dissimilar 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 [3]. Unfortunately, Along with the potential benefits of distributed Intrusion detection system there are two major problems. The first problem is to decide an efficient fusion rule to combine the diverse evidences provided by this systems and second problem is to determine whether the evidence provided by these systems are reliable, i.e., finding reliability value of IDS involved in the fusion process. The reliability of intrusion detection system is defined as the amount of trust on the ability of IDS and the evidence provided by IDS. The value of reliability factor decides the discounting factor for discounting the evidences of conflicting, complementary and unreliable IDS. The classical method of fusing evidences from multiple intrusion detection systems assume all the IDS to be equally reliable and assign same weighage to each of the evidences. However, in real scenario it is not true because some IDS are dominant for detecting certain class of attack and also its evidence can be more reliable compared to other IDS involved in fusion process.

Our focus in these work is to overcome the limitations and issues in the method of fusing dissimilar evidence from multiple IDS and to derive the numerical value of reliability of IDS. In this paper, we propose a novel fusion operator that not only fuses the evidence but also incorporate the reliability value.

The rest of the paper is organized as follows: Section 2 introduces the traditional alert fusion flow and explains various fusion rules proposed in literature [2, 12, 17]. Section 3 discusses the requirements and limitations of an ideal fusion rule. Section 4 describes the proposed alert fusion approach and discusses various features of the pro-

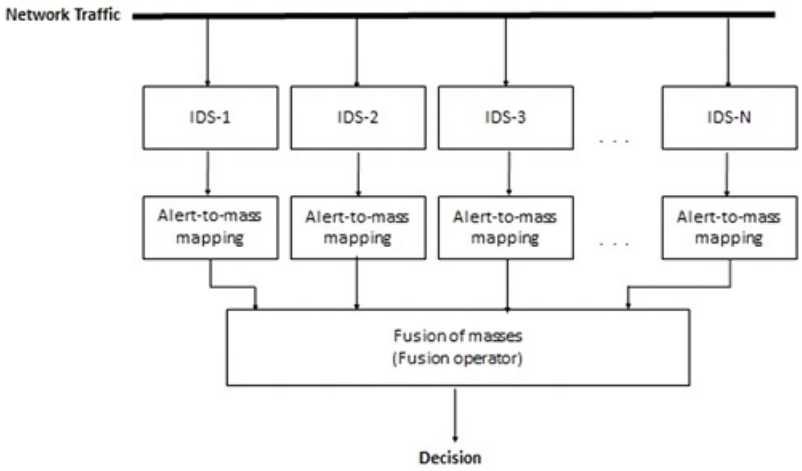

Figure 1: Traditional Alert Fusion Flow Diagram

posed alert fusion approach. Section 5 shows the simulation setup and describes the dataset. Section 6 shows results of proposed fusion rule under four different experiments. Finally in Section 7 we draw the conclusion.

2 Related Work

Figure 1 shows the traditional method for combining alerts from N different intrusion detection system. Each IDS sniffs the incoming network traffic and alerts for the presence of an attack. The alerts generated by IDS is converted to a mass value and all such masses are fused by fusion operator. This section will show the process of alert-to-mass mapping and gives a brief overview on existing fusion rule.

2.1 Alert to Mass Mapping

An IDS sniffs the traffic and generates positive and negative alerts. If we denote the hypothesis that attack is present by H and attack not present by -H then according to [6] we have,

$$\begin{aligned} m(H) &= \frac{P}{P+N+C} \\ m(-H) &= \frac{N}{P+N+C} \\ m(Hor-H) &= \frac{C}{P+N+C}, \end{aligned}$$

where, P- positive evidence in favor of hypothesis H, N-Negative evidence opposing the hypothesis H or favoring 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. $m(Hor-H)$ is mass value for hypothesis H or $-H$ and can be called $m(uncertain)$ i.e, mass value for uncertainty between H and -H. Figure 2 shows the effect of increase in positive evidence on mass value of $m(H)$, $m(-H)$ and $m(uncertain)$.

2.2 Fusion Rules

The fusion rules are 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}. The power-set is usually closed under unions, intersections and complements and is defined as a Boolean algebra. The fusion rules such Dempster shafer Rule in [12], Yager's Rule in [17] and Smet's TBM Rule in [13] are rules which are closed under Union operator. However, this rules doesn't contain intersections of element of Θ.

A basic belief assignment (BBA) is a function m from 2^{Θ}, the power set of Θ to [0,1]. The belief mass assignment will satisfy the property:

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

Here, $m(\phi)$ is the mass assigned to null set. Let, $m_1(B)$ and $m_2(C)$ are two independent masses from two sources of evidence. Then the combined mass $m(A)$ is obtained by combining $m_1(B)$ and $m_2(B)$ through conjunctive rule,

$$\begin{aligned} m(A) &= \sum_{\substack{B,C \in 2^{\Theta} \\ B \cap C = A}} m_1(B) m_2(C) \\ m(\phi) &= \sum_{\substack{B,C \in 2^{\Theta} \\ B \cap C = \phi}} m_1(B) m_2(C). \end{aligned}$$

Disjunctive rule of combination is defined for union of elements of Θ. If $m_1(B)$ and $m_2(C)$ are two independent masses from two sources of evidence then the combined mass m(A) obtained by combining $m_1(B)$ and $m_2(C)$

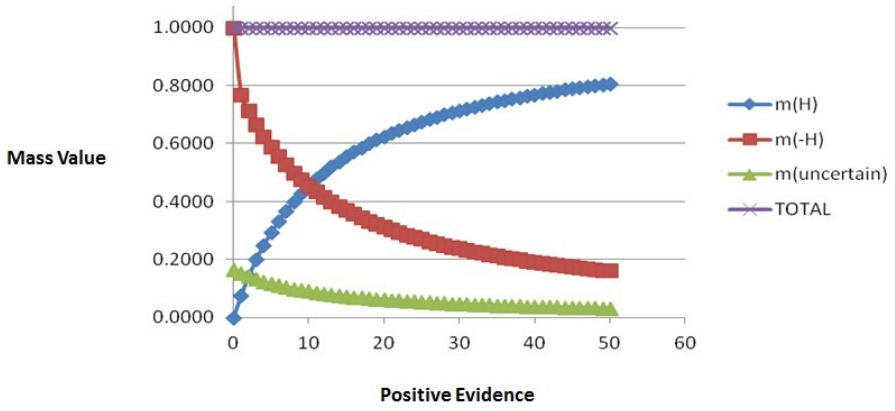

Figure 2: Effect of increase in positive evidence on mass value

through the rule,

$$m(A) = \sum_{\substack{B,C \in 2^{\Theta} \\ B \cup C = A}} m_1(B) m_2(C).$$

The disjunctive rule is preferable when some sources of evidence are unreliable but we don't know which one is unreliable.

The normalized version of conjunctive rule was proposed by Dempster and Shafer in [12] and is known as Dempster-Shafer rule. In DS rule, the fused masses m(A) is obtained from two independent sources of evidence $m_1(B)$ and $m_2(C)$ using following equation:

$$\begin{aligned} m(A) &= \frac{\sum_{\substack{B,C \in 2^{\Theta} \\ B \cap C = A}} m_1(B) m_2(C)}{1 - \sum_{\substack{B,C \in 2^{\Theta} \\ B \cap C = \phi}} m_1(B) m_2(C)} \\ m(\phi) &= 0. \end{aligned}$$

The above rule is defined for fusing two independent masses from sources of evidence. However, the same can be extended for n independent and equally reliable sources.

Dubois and Prade rule of combination by Dubois and Prade [2] is applicable when out of two sources, one source is unreliable and these unreliability is because of high conflict between the evidence they provide. DP rule assigns the value of conflict between two sources under union operator to the total mass value.

$$m(A) = \sum_{\substack{B,C \in 2^{\Theta} \\ B \cup C = A \\ B \cap C = \phi}} m_1(B) m_2(C) + \sum_{\substack{B,C \in 2^{\Theta} \\ B \cap C = A \\ B \cap C \neq \phi}} m_1(B) m_2(C).$$

3 Requirements and Limitations of Fusion Rules

Thomas in [15] suggests that the timely detection of intrusion in multiple IDS framework requires an efficient fusion rule that effectively combines evidence from multiple IDS and outputs a decision that accurately matches with existing ground truth. Following are the basic requirements for fusion rule as mapped out by authors:

- Fusion rule should incorporate the reliability of intrusion detection system for the evidence it provide about the presence of intrusion.
- The rule should be able to compromise between the reliable IDS and unreliable IDS.
- If all the IDS involved in fusion are unreliable then fusion rule should discard the available IDS and then new sets of IDS has to be found for concerned fusion problem.

According to Katar in [7] the quality of decision from a fusion operator varies application to application. In present work the goal is to combine alerts from multiple IDS systems, so the trustworthiness of alerts is a matter of concern. The existing fusion rules discussed in Section 2 have following limitations:

- None of the existing rule incorporates the reliability of source whose evidence 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 existing fusion rule considered all the sources of evidence to be equally reliable. However, in fusion framework there might be some unreliable sources which misleads to the fusion rule to give wrong decision.
- One major drawback related to the fusion rule as suggested by Goodman in [4] 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 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.

Table 1: DARPA 99 experiment description

Characteristic	Name
Dataset Name	DARPA 1999
Frame of Discernment (Θ)	[probe, -probe, θ]
Reliability criteria	TPR of IDS
No. of packets processed	5766

Table 2: Comparison of single IDS with fusion using DS and fusion using proposed rule by deriving reliability value using TPR

	Snort	Suricata	PHAD	NETAD	DS Rule	Proposed Rule
TP	127	124	144	118	131	143
TN	2715	2721	2730	2681	2644	5324
FP	2784	2778	2769	2818	2855	32
FN	140	143	123	149	136	267

The above requirements and limitations shows that we need a framework which can evaluate the numerical value of reliability of intrusion detection systems and discount the evidences based on their reliability beforehand. Also, there must be robust way as to handle conflict between sources and uncertainty assigned by sources to hypotheses.

4 Proposed Fusion Approach

To overcome the limitations and to match the requirements, we propose a novel method of fusing the evidences provided by source (Alerts generated by Intrusion Detection System). The flowchart of proposed fusion approach is as shown in Figure 3. The mass generated from alert to mass mapping block is used to derive reliability values along with CRF and DRF values. The input masses are discounted using this values and discounted masses are then fused using proposed rule. This section will explain the proposed rule, features of proposed rule and method for deriving reliability co-efficient of an Intrusion detection system.

4.1 Proposed Rule

The proposed rule is based on DS framework [12]. Here, $m_1(B)$ and $m_2(C)$ are two independent masses from two sources of evidence. Then the combined mass m(A) is obtained by combining $m_1(B)$and $m_2(C)$ through the rule,

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

Where,

$$CRF(A) = \prod_n R_n$$

$$DRF(A) = (1 - \prod_n R_n)(1 - \prod_n (1 - R_n)).$$

Here, R_n is the reliability value of n^{th} source of evidence. $CRF(A)$ is conjunctive reliability value about A and $DRF(A)$ is disjunctive reliability value about A. CRF and DRF value acts as a weighting factor to compromise between conjunctive mass and disjunctive mass.

4.2 Features of Proposed Rule

The proposed rule effectively incorporates reliability of each source of evidence. If all the sources of evidence are reliable we get $CRF(A)$=1 and $DRF(A)$=0, so the proposed rule converge to conjunctive rule. If all the sources of evidence are unreliable we get $CRF(A)$=0 and $DRF(A)$=0, so the proposed rule does not give any solution and new sources of evidence has to be found. If some sources are reliable and some are unreliable we get $CRF(A)$=0.5 and $DRF(A)$=0.5, so the proposed rule will shows the compromise between conjunctive mass and disjunctive mass.

4.3 Deriving Reliability Co-efficient

One of the major problems of incorporating reliability of IDS into the fusion is problem of obtaining reliability coefficients. Reliability coefficients basically show a numerical value of trust in the mass value provided the Intrusion Detection system. 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 mass provided by Intrusion detection systems indicates the presence of an unreliable IDS which may cause the fusion result to be complementary from reality. An highly conflicting IDS will be assigned least reliability and least conflicting IDS will be assigned with highest reliability.

Another Approach of finding reliability is to relate reliability with the true alert rate of IDS. In these approach it is assumed that the IDS having highest true alert rate and lowest false alert rate will be assigned highest reliability and thereby, giving 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 knowledge of ground truth. In these work, we have use both the approaches and have compared result of proposed rule with existing rules.

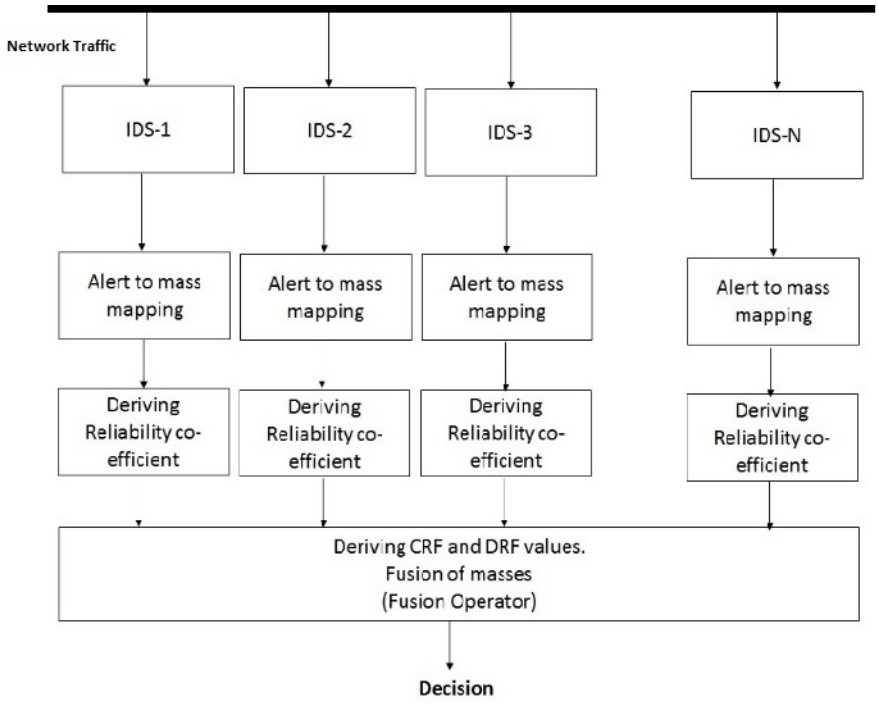

Figure 3: Flowchart of proposed fusion approach

Table 3: Comparison of single IDS with fusion using DS and fusion using proposed rule by deriving reliability value using TPR

	Snort	Suricata	PHAD	NETAD	DS Rule	Proposed Rule
TPR	0.4757	0.4644	0.5393	0.4419	0.4906	0.5356
FPR	0.5063	0.5052	0.5035	0.5125	0.5192	0.060
PPV	0.0437	0.0429	0.0494	0.0402	0.0439	0.8171
NPV	0.9510	0.9501	0.9569	0.9473	0.9511	0.9522
ACC	0.4929	0.4934	0.4984	0.4854	0.4813	0.9481

Table 4: DARPA 99 experiment description

Characteristic	Name
Dataset Name	DARPA 1999
Frame of Discernment (Θ)	[probe, -probe, θ]
Reliability criteria	Conflict between IDS
No. of packets processed	5766

Table 5: Comparison of single IDS with fusion using DS and fusion using proposed rule by deriving reliability value using conflict between evidences

	Snort	Suricata	PHAD	NETAD	DS Rule	Proposed Rule
TP	128	107	129	129	119	136
TN	2751	2718	2689	2768	2693	5130
FP	2748	2781	2810	2731	2806	244
FN	139	160	138	138	148	256

Table 6: Comparison of single IDS with fusion using DS and fusion using proposed rule by deriving reliability value using conflict between evidences

	Snort	Suricata	PHAD	NETAD	DS Rule	Proposed Rule
TPR	0.4794	0.4007	0.4831	0.4831	0.4457	0.3579
FPR	0.4997	0.5057	0.5110	0.4966	0.5103	0.0454
PPV	0.045	0.0377	0.0439	0.0439	0.0451	0.3579
NPV	0.9519	0.9444	0.9512	0.9525	0.9479	0.9525
ACC	0.4993	0.4899	0.4887	0.5024	0.4877	0.9133

5 Simulation Setup

5.1 Dataset Description

The MIT Lincoln Laboratory under the project DARPA has collected and distributed the first standard dataset for offline evaluation of IDS. DARPA98 and DARPA99 are two datasets available under DARPA project for the use of researchers. DARPA99 is modified and refined version of DARPA98 which consists of total 5 weeks of data which is divided into 3 weeks of training dataset and 2 weeks of testing dataset. Each week of dataset consists of five day of data from Monday to Friday of inside and outside traffic. The detailed explanation of various intrusions/attacks present in DARPA99 along with normal traffic is explained in detail in [8] by Kendall.

Most research in the field of IDS have been done using DARPA99 dataset. However, many of the researchers have criticized and argued about its applicability for IDS evaluation. Most of them consider that the dataset is very outdated and unable to create behavior like the present day attack. Along with the critics, there are significant argument in favor of DARPA99. In [15], Thomas argued that the non-availability of any other dataset that includes the complete network traffic was probably the initial reason to make use of the DARPA dataset for IDS evaluation by researchers. In [9], authors comment that if an present day advanced system could not perform well on DARPA dataset, it could also not perform acceptably on realistic data. Authors in [10] argued that even though there are shortcomings, the Lincoln evaluation indicates that even the best of the research IDS systems falls far short of the DARPA goals for detection and false-alarm performance. MCHugh in his work [10] believe that any sufficiently advanced IDS should be able to achieve good true positive detection performance on the DARPA IDS evaluation dataset. Demonstrating such performance, however, is only necessary to show the capabilities of such a detector, it is not sufficient.

The KDD99 dataset is knowledge discovery database originally created from DARPA98. The KDD99 dataset has 41 features along with one class label. The Class label consists of attack in four categories R2L, U2R, Probe and DOS. The complete details on types of attacks present in each categories and list of 41 features is available in the work by [14].

Authors in [14] suggested a new dataset called as NSL-KDD in order to solve the issues with KDD99. NSL-KDD was distributed for testing in year 2009 by University of New Brunswick. This new version of dataset does not have redundant records in train set, so the classifier does not get biased towards more frequent records. Also, the test set does not have duplicate records which give better detection rates. The reduced NSL-KDD make it reasonable to run the experiments without need of randomly selecting small set as in KDD99. The results by Tavallaee et al. [14] shows that the results obtained by NSL-KDD makes the evaluation results more consistent and comparable.

5.2 Selection of IDS

For alert fusion of multiple intrusion detection systems, we have selected four dissimilar IDS namely, Snort, Suricata, PHAD and NETAD. The reason behind such selection is that snort and suricata are signature based intrusion detectors while PHAD and NETAD are anomaly detectors. Thus, both categories are complementary to one another which enhances the performance of fusion system and within the category they are redundant which increases the accuracy.

5.3 System Configuration

The simulation environment consists three 3^{rd} Generation IntelCorei5processor (1.6GHz), Operating system installed is Linux Ubuntu with 4GB RAM. One machine deployed with Signature based IDS such as snort and suricata. Another Machine deployed with Anomaly detectors such as PHAD and NETAD. Third machine acts as an attacker machine having dataset loaded and is being replayed using TCPreplay.

6 Results

This section will discuss the results obtained under four different experiments namely, DARPA99 Experiment, KDD99 Experiment, NSL-KDD Experiment and some random experiments in order The performance metrics used to compare the results are true positive (TP), true negative (TN), false positive (FP), false negative (FN), true positive rate (TPR), false positive rate (FPR), positive prediction value (PPV), negative prediction value

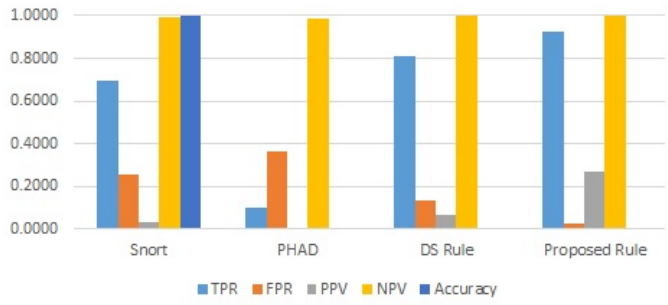

Figure 4: Comparison of proposed rule with DS rule against NSL-KDD for detecting R2L attack

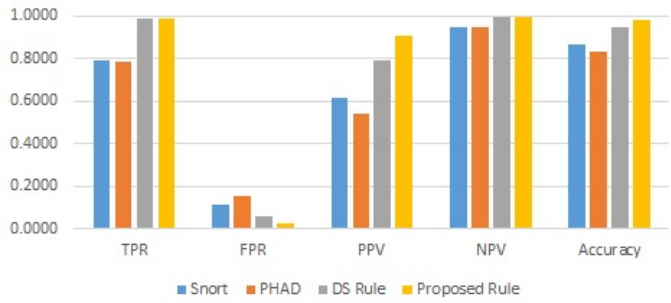

Figure 5: Comparison of proposed rule with DS rule against NSL-KDD for detecting DOS attack

(NPV) and Accuracy (ACC). The formal definition of each of this parameters are explained in Appendix A along with its significance.

6.1 DARPA99 Experiment

In DARPA99 Experiment, we preprocessed the dataset and total 5766 packets where loaded on to the network. In first experiment as per Table 1, we use the TPR of IDS as a reliability criteria. Table 2 and Table 3 shows the performance comparison of single IDS against the fusion using DS and fusion using proposed rule. The observed results shows an efficient reduction in number of false positives and an significant increase in the accuracy of IDS.

Table 4 shows the description of second experiment performed using DARPA99 where reliability is derived by calculating the amount of conflict between the IDS systems. Table 5 and Table 6 shows the comparison results of single IDS with fusion using DS and fusion using proposed rule by deriving reliability value using conflict between evidences.

Table 7: KDD 99 Experiment description

Characteristic	Name
Dataset Name	KDD 1999
Frame of Discernment (Θ)	[smurf, -smurf, θ]
Reliability criteria	TPR of IDS
No. of packets processed	3456

6.2 KDD99 Experiment

In KDD99 Experiment, we preprocessed the dataset and total 3456 packets containing attack and non-attack packet was loaded on the network and replayed using TCPReplay tool. The Frame of Discerment is selected to detect smurf attack. The total 1944 smurf attacks were present in processed dataset.

Figure 6: Confusion matrix of two IDS system having conflicting behavior

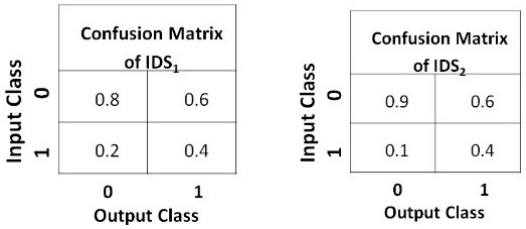

Figure 7: Confusion matrix of two IDS system having harmonious behavior

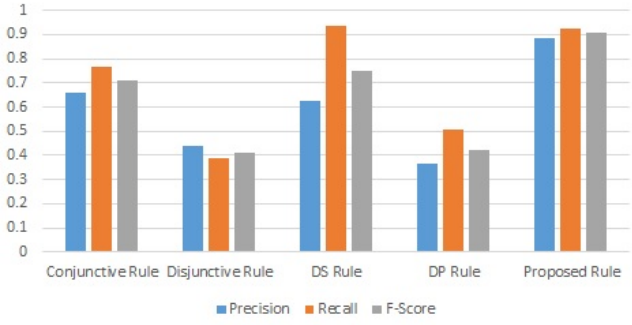

Figure 8: Comparing fusion rules under conflict behavior

Table 8: Comparison of single IDS with fusion using DS and fusion using proposed rule by deriving reliability value using TPR

	Snort	Suricata	PHAD	NETAD	DS Rule	Proposed Rule
TP	916	1015	982	910	969	1015
TN	788	763	769	762	765	1490
FP	724	749	743	750	747	22
FN	1028	928	962	1034	975	929

Table 9: Comparison of single IDS with fusion using DS and fusion using proposed rule by deriving reliability value using TPR

	Snort	Suricata	PHAD	NETAD	DS Rule	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	0.4243	0.4397
ACC	0.4931	0.5145	0.5067	0.4838	0.5017	0.7248

Table 10: KDD 99 experiment description

Characteristic	Name
Dataset Name	KDD 1999
Frame of Discernment (Θ)	[smurf, -smurf, θ]
Reliability criteria	Conflict between IDS
No. of packets processed	3456

Table 11: Comparison of single IDS with fusion using DS and fusion using proposed rule by deriving reliability value using conflict between IDS

	Snort	Suricata	PHAD	NETAD	DS Rule	Proposed Rule
TP	997	967	1015	960	1008	1033
TN	742	741	730	758	723	1501
FP	770	771	782	754	789	11
FN	947	977	929	984	936	911

Table 12: Comparison of single IDS with fusion using DS and fusion using proposed rule by deriving reliability value using conflict between IDS

	Snort	Suricata	PHAD	NETAD	DS Rule	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
ACC	0.5032	0.4942	0.5049	0.4971	0.5009	0.7332

Table 13: NSL-KDD experiment description

Characteristic	Name
Dataset Name	NSL-KDD
Frame of Discernment (Θ)	[R2L, -R2L, θ]
Reliability criteria	Conflict between IDS
No. of packets processed	5000
No. of R2L attacks present	52

Table 14: NSL-KDD experiment description

Characteristic	Name
Dataset Name	NSL-KDD
Frame of Discernment (Θ)	[DOS, -DOS, θ]
Reliability criteria	Conflict between IDS
No. of packets processed	5000
No. of R2L attacks present	944

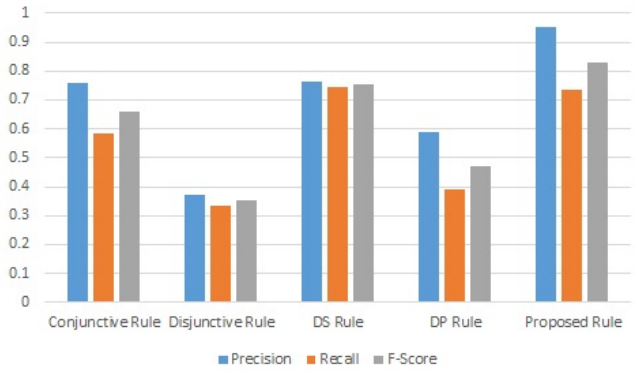

Figure 9: Comparing fusion rules under harmonious behavior

The KDD99 Experiment description is shown in Table 7. Table 8 and Table 9 shown the performance of proposed rule along with DS rule. Table 10 gives description about KDD99 experiment by using conflict between the IDS as a reliability criteria. Table 11 and Table 12 shows the results obtained under this experiment.

6.3 NSL-KDD Experiment

To perform evaluation of our proposed technique against NSL-KDD, We utilized two IDS systems out of four installed in the environment namely, snort and PHAD. In the work by Thomas [16], it is shown that PHAD has performs badly during detection of R2L and U2R attack. While, snort performs well against DOS and R2L categories of attack. In pre-processing of NSL-KDD using wireshark tool, it is found that DOS and R2L have very low variations and hence it is difficult to detect such attacks using traditional detection method.

Table 13 shows the description of NSL-KDD experiment for detecting R2L attack considering conflict as reliability criteria. Table 14 shows the description of NSL-KDD experiment for detecting DOS attack considering conflict as reliability criteria. Figure 4 shows the results of proposed rule with DS rule against NSL-KDD for detecting R2L attack and Figure 5 shows the results of proposed rule with DS rule against NSL-KDD for detecting DOS attack. It can be observed from the result that proposed rule gives highest accuracy and least false positive rate compared to individual IDS and DS rule.

6.4 Random Experiment

The behavior of proposed rule against existing rules is further checked with some random experiments. Here, we perform some random experiments under following situations:

- Conflicting Behavior;
- Harmonious Behavior.

We artificially generated the random packets but controlled them to have a conflicting behavior and harmonious behavior as shown in Figure 6 and Figure 7.The results for fusion of two intrusion system detectors having conflicting behavior is shown in 15. The proposed rule increases the accuracy by 20% compared to individual IDS. However, in the case of harmonious behavior the DS Rule improves accuracy by 10% while proposed rule improves it by 18% compared to individual IDS. Table 16 shows the results for harmonious behavior of IDS. Figure 8 and Figure 9 shows the results in terms of precision, recall and F-score under conflicting and harmonious behavior.

7 Conclusion

In this paper, a reliable alert fusion approach for combining alerts from multiple intrusion detection systems is proposed. The proposed rule incorporates reliability of intrusion detection during fusion process. The rule is designed to make compromise between conjunctive logic and disjunctive logic. The simulation was done against DARPA99, KDD99 and NSL-KDD and shows the performance of proposed approach with an improvement in false positive rate. We demonstrated the results for random situation under complementary and harmonious behavior to prove the robustness of our rule in terms of reducing false alert and enhancing accuracy of detection.

References

[1] G. G. Deverajan, R. Saravanan, "A novel trust based system to detect the intrusive behavior in MANET," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 31–43, 2015.

[2] D. Dubois and H. Prade, "On the combination of evidence in various mathematical frameworks," in *Reliability Data Collection and Analysis*, pp. 213–241, Springer, 1992.

Table 15: Comparison of proposed rule with existing rules under conflicting behavior

	IDS_1	IDS_2	Conjunctive Rule	Disjunctive Rule	DS Rule	DP Rule	Proposed rule
TP	1000	2500	1915	745	2341	820	2377
TN	2500	1000	1505	2141	1106	1960	2133
FN	1500	0	585	1160	159	800	190
FP	0	1500	995	954	1394	1420	300
TPR	0.4	1.0	0.766	0.3910	0.9364	0.5061	0.9259
FPR	0.0	0.60	0.398	0.3082	0.4424	0.5798	0.123
PPV	1.00	0.63	0.560	0.4384	0.6267	0.366	0.8879
NPV	0.625	1.00	0.720	0.648	0.874	0.710	0.9182
Accuracy	0.7	0.7	0.6847	0.5772	0.6894	0.556	0.9020

Table 16: Comparison of proposed rule with existing rules under harmonious behavior

	IDS_1	IDS_2	Conjunctive Rule	Disjunctive Rule	DS Rule	DP Rule	Proposed rule
TP	1000	1000	1461	800	1863	950	1906
TN	2000	2250	2036	1240	1929	1900	2303
FN	1500	1500	1039	1600	637	1490	691
FP	500	250	464	1360	571	660	100
TPR	0.40	0.40	0.58	0.33	0.75	0.39	0.73
FPR	0.20	0.10	0.19	0.52	0.23	0.26	0.04
PPV	0.67	0.80	0.76	0.37	0.77	0.59	0.95
NPV	0.57	0.60	0.66	0.44	0.75	0.56	0.77
Accuracy	0.60	0.65	0.70	0.41	0.76	0.57	0.84

[3] R. Goel, A. Sardana, and R. C. Joshi, "Parallel misuse and anomaly detection model," *International Journal of Network Security*, vol. 14, no. 4, pp. 211–222, 2012.

[4] I. R. Goodman, R. P. Mahler, and H. T. Nguyen, *Mathematics of Data Fusion*, vol. 37, Springer Science & Business Media, 1997.

[5] L. C. Huang and M. S. Hwang, "Study of intrusion detection systems environment," *Journal of Electronic Science and Technology*, vol. 4, p. 6, 2012.

[6] A. Jøsang, *Subjective Logic*, Book Draft, 2011. (`http://folk.uio.no/josang/papers/subjective_logic.pdf`)

[7] C. Katar, "Combining multiple techniques for intrusion detection," *International Journal of Computer Science and Network Security*, vol. 6, no. 2B, pp. 208–218, 2006.

[8] K. Kendall, "A database of computer attacks for the evaluation of intrusion detection systems," Technical Report DTIC Document, 1999.

[9] M. V. Mahoney and P. K. Chan, "An analysis of the 1999 darpa/lincoln laboratory evaluation data for network anomaly detection," in *Recent Advances in Intrusion Detection*, pp. 220–237, Springer, 2003.

[10] J. McHugh, A. Christie, and J. Allen, "Defending yourself: The role of intrusion detection systems," *IEEE Software*, vol. 17, no. 5, pp. 42, 2000.

[11] E. U. Opara, O. A. Soluade, "Straddling the next cyber frontier: The empirical analysis on network security, exploits, and vulnerabilities," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 10–18, 2015.

[12] G. Shafer et al., *A Mathematical Theory of Evidence*, vol. 1, Princeton University Press Princeton, 1976.

[13] P. Smets and R. Kennes, "The transferable belief model," *Artificial Intelligence*, vol. 66, no. 2, pp. 191–234, 1994.

[14] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the kdd cup 99 data set," in *Proceedings of the Second IEEE Symposium on Computational Intelligence for Security and Defence Applications*, pp. 1–6, 2009.

[15] C. Thomas and N. Balakrishnan, "Improvement in intrusion detection with advances in sensor fusion," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 542–551, 2009.

[16] C. Thomas and N. Balakrishnan, "Performance enhancement of intrusion detection systems using advances in sensor fusion," *Supercomputer Education and Research Centre Indian Institute of Science*, Doctoral Thesis, 2009. (`http://www.serc.iisc.ernet.in/graduation-theses/CizaThomas-PhD-Thesis.pdf`)

[17] R. R. Yager, "On the dempster-shafer framework and new combination rules," *Information Sciences*, vol. 41, no. 2, pp. 93–137, 1987.

Vrushank Shah was born in Ahmedabad, Gujarat, India, in 1985. He received the B.E. degree in electronics and communication engineering from the North Gujarat

Appendix A

Table 17: Formal definition and significance of performance metrics

Name	Definition	Formula
True positive (TP)	Number of attacks that are correctly detected	-
False positive (FP)	Number of normal traffic packet that are incorrectly detected as attacks	-
True negative (TN)	Number of normal traffic packets that are correctly classfied	-
False negative (FN)	Number of attacks that are not detected	-
True positive rate (TPR)	Is the ratio of total true positives and sum of true positives with false negatives	$\frac{TP}{TP+FN}$
False positive rate (FPR)	Is the ratio of total false positives and sum of false positives with True negatives	$\frac{FP}{TN+FP}$
Positive prediction value (PPV)	Is the ratio of total true positives and sum of true positives with false positives.	$\frac{TP}{TP+FP}$
Negative prediction value (NPV)	Is the ratio of total true negative and sum of true negatives with false negatives.	$\frac{TN}{TN+FN}$
Accuracy (ACC)	Is the ratio of sum of TP and TN to the sum of TP, TN, FP and FN	$\frac{TP+TN}{TP+TN+FP+FN}$
Precision(P)	Is a measure of what fraction of test data detected as attack is actually from the attack class	$\frac{TP}{TP+FP}$
Recall (R)	Is a measure of what fraction of attack class is correctly detected	$\frac{TP}{TP+FN}$
Fscore (F)	Is the balance between precision and recall	$\frac{2PR}{P+R}$

University, Patan, Gujarat in 2007 and the M.Tech. in communication systems engineering from Gujarat University, Ahmedabad in 2010. In 2010, he joined the Department of Electronics and Communication, L.J. Institute of Engineering and Technology as an Assistant Professor and in 2012, he joined Department of Electronics and Communication, Indus University, Ahmedabad as an assistant professor. Currently he is PhD Research Scholar at Gujarat Technological University and doing research in the field of Intrusion Detection system under the guidance of Dr. A. K. Aggarwal. His current research interests include Intrusion Detection system, Probability and Statistics, Decision making theory, Image processing and Speech Processing.

Honourable Dr. A. K. Aggarwal is currently the Vice Chancellor, Gujarat Technological University, Chandkheda, Ahmedabad. He received the B.Sc. degree in electrical engineering, Punjab University in 1964 and M.E. and PhD Degree in electrical engineering from M.S. University of Baroda in 1968 and 1981 respectively. He was with M.S. University of Baroda at different levels starting from Assistant professor, Associate professor, Professor and Head of electrical and computer science department from the 1967-1989. In year 1989, he joined as the Professor and Head of computer science department, Gujarat University. In 1999, he moved to Canada and joined University of Windsor as Associate professor. He has been honored with IEEE Millennium Medal and IEEE Outstanding Branch Counselor Award 1997. In 1999, he was the chair, IEEE India Council. His research interests involves cyber security and computer networking.