ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

Evaluation of Intrusion Detection using a Novel Composite Metric

T. Augustine[1], P. Vasudeva Reddy[1], P.V.G.D. Prasad Reddy[2]

Department of Engineering Mathematics, A.U. College of Engineering, Andhra University, Visakhapatnam, AP, India[1]

Department of CS&SE, A.U. College of Engineering, Andhra University, Visakhapatnam, AP, India[2]

ABSTRACT: In this technological age, a lot of data that include secrets have been given away to the internet. The exponential growth in the E-Commerce, the challenge of security of the secret data is a huge problem to provide security to data for individuals, companies and governments. It is very important that the data should reach safely to the destination and only the intended person should able to access the data without any intrusions over the network. But in these days, where there is a continuous increase in immorality and decrease in ethical values, cyber crimes have become regular news items in our televisions and news papers. Researchers have been contributing various solutions towards addressing this problem and Network Intrusion Detection Systems (NIDS) is one of the solutions against these cyber crimes and network attacks. However, the performance of these Network Intrusion Detection Systems needs to be measured by effective metrics. There are various primitive metrics available such as Accuracy, Detection Rate and False Alarms Rate etc., but there is no bench mark performance metric available in the literature to evaluate the performance of the NIDSs. On the other hand performance metrics play a very major role in data security because the performance of the NID systems is evaluated through these metrics. In this paper, a novel Composite Performance Metric, called 'DAFAR' has been proposed to evaluate the performance of different Network Intrusion Detection systems. Various experiments were carried out on the benchmark data set (ISCX 2012) [1] to test the efficacy of the NID systems' performance. The experimental results show that the proposed metric gives better direction while evaluating the performance of different Network Intrusion Detection systems.

KEYWORDS: Network Intrusion Detection, NID, Intrusions, False Alarm Rate, Detection Rate, Accuracy, Performance Metrics

I. INTRODUCTION

Evaluating the Intrusion Detection Systems (IDSs) is one of the most important activities in network security tasks. Once an NIDS is designed and developed, it is very important to validate efficiency and effectiveness of such system. Different features of the NIDSs that are considered for evaluation range from accuracy and correctness to usability. For this purpose, a large number of metrics have been proposed in literature [11], [13], [14]. Unfortunately, so far there is no straight forward benchmark metric available in literature. Many researchers used a variety of metrics to measure the performance quantitatively.

In this paper, various existing performance metrics have been explored, these performance metrics are used to evaluate NID systems based upon benchmark datasets. The advantages and drawbacks of these systems were studied. This study would help in better understanding of different metrics for evaluating the performance of NIDSs. After analyzing various primitive performance evaluation metrics, a new and novel composite performance metric has been proposed in this paper. Various experiments were carried out on the benchmark data set (ISCX 2012) [1] to test the efficacy of the NID systems performance but the main objective of this work is not to evaluate the NIDS systems but to arrive at a good novel performance evaluation metric.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

It is believed that along with the new proposed composite metric, 'DAFAR', the experimental results and findings of this paper would provide beneficial insights into literature and would be useful for those who are engrossed in design and developments of NIDSs and related fields.

II. SOME EXISTING PERFORMANCE METRICS IN THE LITERATURE

Many types of metrics have been designed to measure the efficacy and effectiveness of NID systems [3], [4], [5]. These metrics may be categorized into three major classes namely threshold, ranking and probability metrics [7], [12].

Threshold metrics include classification rate (CR), F-measure (FM) and Cost per example (CPE) and so on. It does not matter how close a prediction is to a threshold, it only matters whether a prediction is above or below the threshold. In majority of the cases, the value of the threshold metrics lies in the range from 0 to 1.

Ranking metrics comprise False Positive Rate (FPR), Detection Rate (DR), Precision (PR), Area under ROC curve (AUC) [7] and Intrusion Detection Capability (CID). Even in Ranking Metrics, most of the times the value of ranking metrics exists in the range from 0 to 1. These metrics will depend on the ordering of the cases, not the real predicted values. As long as the ordering is preserved, it makes no difference. These metrics evaluate how well the instances of specific attack are ordered before other normal instances and can be viewed as a summary of model performance across all possible thresholds [6].

Probability metrics comprise Root Mean Square Error (RMSE). The value of RMSE lies in the range from 0 to 1. The metric of it is minimized when the predicted value for each attack class matches with the true conditional probability of that class being a normal class. However, CID is an information theory based metric which gives a better comparison of various NIDSs than the other popular metric like AUC [5]. The value of CID also lies between 0 and 1. Higher the value of the CID better is the performance of the NIDS. Generally, these metrics are computed from confusion matrix. The best way to represent classification results of the NIDS is with the confusion matrix.

A confusion matrix is a technique for summarizing the performance of a classification algorithm [15]. The confusion matrix shows the ways in which a classification model is confused when it makes predictions. It represents the results of true and false classification. In other words, Confusion matrix is a table that reports the number of false positives, false negatives, true positives, and true negatives. Following are the possibilities to classify events in an ideal NDIS and all these possibilities are also depicted in Table 1:

- True positive (TP): Intrusions that are successfully detected by the NIDS: which means if the instance (actual) is positive and it is classified as positive (Predicted), it is counted as a true positive
- False Negative (FN): Normal (Non-intrusive behavior), which is wrongly classified as intrusive by the NIDS. In other words, If the instance (actual) is positive and if it is classified as negative (Predicted), it is counted as a false negative
- False positive (FP): Intrusive behavior, which is labeled as normal/non-intrusive by the NIDS. In other words if the instance is negative (actual), if it is classified as positive (Predicted), it is counted as a false positive. Intrusions that are missed by the IDS, and classified as normal / non-intrusive
- True Negative (FN): Normal/non-intrusive behavior that is successfully labeled as normal/non-intrusive by the IDS. If the instance is negative (Actual) and it is classified as negative (Predicted), it is counted as a true negative

Table 1: Confusion matrix

	Predicted	
Actual	TP	FN
	FP	TN

Though we have the representational power of the confusion matrix in classification, it is not a very useful tool for the sake of comparison of the NIDSs. To address this problem, different performance metrics have been defined in terms of the variables that are found in the confusion matrix. The output of these metrics is some numeric values, which are easy to compare. In the next paragraph, those various metrics from the available literature are presented

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

Accuracy (ACC):
The accuracy of the classifiers is the percentage of the correctly classified instances to the total number of instances.

$$Accuracy\,(ACC) = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

where *TP*, *TN*, *FP*, and *FN* are True Positive, True Negative, False Positive, and False Negative values respectively.

Classification rate (CR):
It is defined as the ratio of correctly classified examples to the total number of examples.

$$Classification\ rate\,(CR) = \frac{Correctly\ classified\ instances}{Total\ number\ of\ instance} = \frac{TP + TN}{TP + TN + FP + FN} \quad (2)$$

Precision (PR):

Precision is the fraction of data instances predicted as positive that are actually positive.

$$Precision\,(PR) = \frac{TP}{TP + FP} \quad (3)$$

***F*-measure (FM):**

F-measure is a harmonic mean of precision

$$F - measure\,(FM) = \frac{2*TP}{(2*TP) + FP + FN} \quad (4)$$

False positive rate (FPR):
False positive rate (FPR) is defined as the ratio between the total number of normal instances detected as attack to the total number of normal instances.

$$False\ Positive\ Rate\,(FPR) = \frac{Number\ of\ normal\ instances\ detected\ as\ attacks}{Total\ number\ of\ Normal\ instances} = \frac{FP}{FP + TN} \quad (5)$$

Detection rate (*DR*):
The detection rate (*DR*) of any NIDS gives the percentage of the correctly detected attacks to the total number of attacks.

$$Detection\ Rate\,(DR) = \frac{TP}{TP + FN} \quad (6)$$

False Alarm Rate (*FAR*):
False Alarm Rate (*FAR*) is the percentage of normal instances that have been incorrectly classified as attacks to the total number of normal instances.

$$False\ Alarm\ Rate\,(FAR) = \frac{FP}{FP + TN} \quad (7)$$

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

Combined:
A new combined metric has been proposed in [2], which is called 'combined'. The formula has been developed by incorporating three metrics together (Accuracy, Detection rate, and FAR)

$$Combined = \left(\frac{ACC + DR}{2}\right) - FAR \quad (8)$$

The authors in [2] stated that the result of this metric will be a real value between −1 and 1, where −1 represents the worst overall system performance of NIDS and 1 represents the best. So obviously, 0 corresponds to 50% overall system performance. In this formula, equal weights to all the three metrics (accuracy, detection rate and false alarm rate) are given. The authors explained with different example scenarios, that this formula directs to determine the performance when there are cases of equal accuracy and equal False Alarm Rate. This looks like a balanced way of measuring the performance of certain applications. But it might not work well with the other applications. The major loop hole with this combined metric is discussed in the further sections of this paper. It is preferable to have a evaluation metric / measure that works for if not for all but for the majority of the applications.

III. NOVEL COMPOSITE METRIC FOR PERFORMANCE EVALUATION OF NIDSS

In the previous section, many available metrics for performance evaluation of Network Intrusion Detection System (NIDS) are presented. Lots of experiments were carried out upon the ISCX 2012 dataset [1] over these primitive metrics. The open source, WEKA 8.3 [9] has been used to test the data on various simulated classifiers with an objective of understanding these individual performance metrics. The results were noted out of the experiments and useful conclusions are drawn.
Individual performance measuring metrics would not serve the purpose of evaluating NID Systems accurately. Hence experiments were carried out with various combinations of these individual metrics by changing the weights of each factor with an objective of arriving at a good composite performance evaluation metric. The experimental results are presented in the next session.
In the present work, an attempt was made to try various combinations of primitive metrics to develop a composite metric through empirical approach using the dataset ISCX 2012. These experimental results are presented to study and analyze various combinations of primitive metrics that are presented in the previous section. These composite metrics are of extreme use when one of these primitive metric (False Alarm Rate or Accuracy or Detection Rate) has equal value. In such case it is very difficult to judge which NIDS performance is better over the other.
These proposed composite metrics have been explained below with different sizes of data sets with same and varying number of normal and attack instances. Table 2 shows some instances (normal, attack) that are considered in this work

Table 2: Normal, Attack instances from the dataset

Normal	100	150	150	300	50	500	1000	450
Attack	100	150	100	200	50	500	1000	300

Confusion matrix is generated for the above instances with different scenarios. In the present work about one hundred scenarios have been considered to establish the efficacy of the proposed new Composite Metric. After so many experiments on the data set and after working through large number of scenarios, the following composite performance metric is proposed. The proposed Composite Performance Metric is named as "**DAFAR**".

$$DAFAR = \left(\frac{ACC + (2 * DR) - FAR}{2}\right) \quad (9)$$

'DAFAR', stands for D-Detection, A-Accuracy, and FAR-False Alarm Rate. It can be observed from the equation (9) that more weight is given to Detection Rate over other two primitive metrics. It is quite simple to understand that in any

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

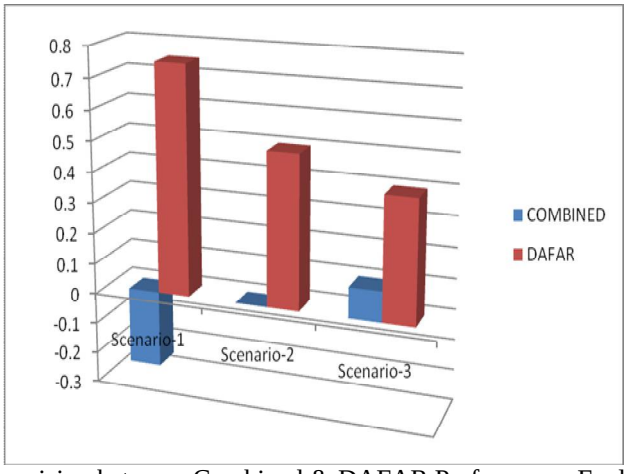
Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

NIDS, Intrusion Detection is the key factor because the very purpose of the NIDS system is to detect the intrusion. The proposed 'DAFAR' is proved to be very effective in measuring the performance of various NDIS systems over different scenarios.

IV. EXPERIMENTAL RESULTS & COMPARISONS

Canadian Institute for Cyber security datasets are used around the world by universities, private industry and independent researchers [8]. In the present work, ISCX 2012 data set from CIC has been extensively used to conduct various experiments. Along with the experiments with primitive metrics, combined metric in [2] was also experimented.



Graph1: Comparision between Combined & DAFAR Performance Evaluation Metric

It can be observed from the Graph1 that the proposed DAFAR Metric gives clear direction on the performance of Network Intrusion Detection System (NIDS) over other ID systems. Authors in [2] considered an example, where a data set of 200 instances are taken and split into 100 normal instances and 100 attack instances, then discussed three different scenarios that have the same accuracy of 50%.

The confusion matrixes are taken as below three scenarios:

Scenario 1:

$$Confusion\,matrix = \begin{bmatrix} 1 & 99 \\ 1 & 99 \end{bmatrix}$$

Scenario 2:

$$Confusion\,matrix = \begin{bmatrix} 50 & 50 \\ 50 & 50 \end{bmatrix}$$

Scenario 3:

$$Confusion\,matrix = \begin{bmatrix} 70 & 30 \\ 70 & 30 \end{bmatrix}$$

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

For these three different confusion matrices, the performance metrics were calculated [2] as per the Equation (8) as shown in the Table3

Table 3: Performance metrics for three different scenarios with equal accuracy [2]

Scenario	Accuracy	DR	FAR	Combined
Scenario 1	0.5	0.99	0.99	−0.245
Scenario 2	0.5	0.5	0.5	0
Scenario 3	0.5	0.3	0.3	0.1

In the above three scenarios, it may be noted that Accuracy values are same and hence the authors in [2] proposed a new combined metric as given in equation (8) but it is very simple to make a mention that Scenario 1 performed much better in terms of Detection Rate. For any NIDS, the priority should be given to the Detection Rate, it does not matter even if there is more False Alarm Rate (FAR) because it does not harm anyone but if detection rate is low, then it would cause lot of damage. Hence the first scenario should be selected from Table3 as the Detection Rate is on the higher side (0.99) but unfortunately Combined Metric in [2], which is in equation (8) selected the third scenario where the detection rate is just 0.3.

Selecting an NID System, whose Detection Rate is 0.3 over other NIDS whose Detection Rate is 0.99 is unfair. The reason for this anomaly in equation (8) is simple; all the three primitive parameters are given equal importance, apart from this it appears as if False Alarm Rate is given more importance over the other two metrics.

This problem is addressed in the proposed Composite Performance Metric, DAFAR, where the Detection Rate is given more importance over the other two primitive metrics and at the same time False Alarm rate is given only half importance. The empirical results proved that the proposed DAFAR Performance Metric evaluates the NIDSs more effectively. To demonstrate the performance of the proposed Composite Metric, the same three scenarios (confusion matrices) that were taken for combined metric in Equation (8) [2] is taken here also towards the calculations with the proposed Composite metric in equation (9). The results are presented in Table4.

Table 4: Performance metrics for three different scenarios with DAFAR Performance Metric

Scenari	Accura	DR	FAR	Combin	DAFA
Scenari	0.5	0.9	0.99	−0.245	0.745
Scenari	0.5	0.5	0.5	0	0.5
Scenari	0.5	0.3	0.3	0.1	0.4

The proposed DAFAR Metric selects the first scenario as the DAFAR value for Scenario 1 is 0.745, which is higher than the other two. In the proposed Composite Metric in Equation (9), Detection Rate is given more priority and False Alarm Rate is given only half priority while evaluating the performance. About 100 different confusion matrices are taken to consider 100 different scenarios and used the proposed Composite Metric over all the 100 scenarios to test the effectiveness and efficiency of this new measure. It is concluded from the results of various experiments that the proposed new Composite Metric is effective in evaluating the performance of NIDS systems.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

Experiments were carried out on ISCX Dataset 2012 by using WEKA, Version 8.3. Apart from taking the confusion matrixes with various boundary conditions to test the effectiveness of the proposed Composite Performance Metric, confusion matrixes were also generated and other primitive metric values were obtained through various simulated classifiers in WEKA software. A sample screenshot window with confusion matrix, other primitive values that were obtained from the simulated classifier is presented in Figure 1. [9]

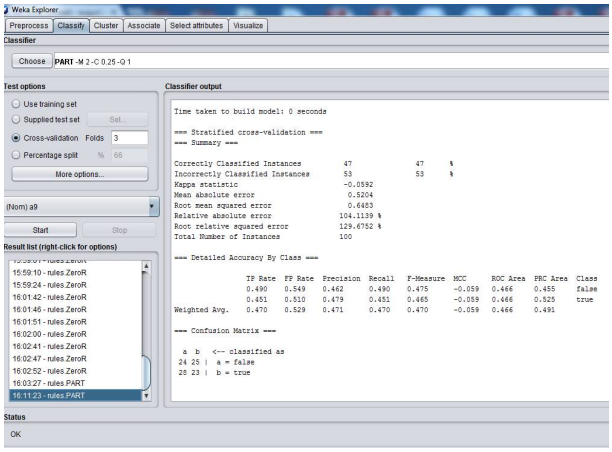


Figure 1: Confusion Matrix and other metrics, generated through 'WEKA'

Tables 5 presents the total values that were calculated through various primitive and combined metrics along with the values of new proposed Composite Performance Metric over 100 different scenarios.

Table 5: Performance metrics for 100 different scenarios with different metrics and DAFAR Performance Metric

Scenario	TP	TN	FP	FN	ACC	DR	FAR	COM.	DAFAR
1	99	1	99	1	0.5	0.99	0.99	-0.25	0.75
2	50	50	50	50	0.5	0.5	0.5	0	0.5
3	30	70	30	70	0.5	0.3	0.3	0.1	0.4
4	50	1	99	50	0.3	0.5	0.99	-0.61	0.13
5	50	99	1	50	0.7	0.5	0.01	0.61	0.87
6	50	50	50	50	0.5	0.5	0.5	0	0.5
7	90	50	50	10	0.7	0.9	0.5	0.3	1
8	10	50	50	90	0.3	0.1	0.5	-0.3	0
9	50	50	50	50	0.5	0.5	0.5	0	0.5
10	75	75	75	75	0.5	0.5	0.5	0	0.5
11	45	105	45	105	0.5	0.3	0.3	0.1	0.4
12	148	2	148	2	0.5	0.99	0.99	-0.24	0.74
13	75	75	75	75	0.5	0.5	0.5	0	0.5
14	75	2	148	75	0.3	0.5	0.99	-0.61	0.14
15	75	148	2	75	0.7	0.5	0.01	0.61	0.87
16	135	75	75	15	0.7	0.9	0.5	0.3	1
17	15	75	75	135	0.3	0.1	0.5	-0.3	0

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

18	75	75	75	75	0.5	0.5	0.5	0	0.5
19	50	75	75	50	0.5	0.5	0.5	0	0.5
20	148	2	148	2	0.5	0.99	0.99	-0.24	0.74
21	40	85	65	60	0.5	0.4	0.43	0.02	0.43
22	50	2	148	50	0.2	0.5	0.99	-0.63	0.11
23	50	75	75	50	0.5	0.5	0.5	0	0.5
24	50	100	50	50	0.6	0.5	0.33	0.22	0.63
25	10	75	75	90	0.3	0.1	0.5	-0.28	0.02
26	40	75	75	60	0.5	0.4	0.5	-0.07	0.38
27	50	75	75	50	0.5	0.5	0.5	0	0.5
28	100	150	150	100	0.5	0.5	0.5	0	0.5
29	296	4	296	4	0.5	0.99	0.99	-0.24	0.74
30	80	170	130	120	0.5	0.4	0.43	0.02	0.43
31	100	4	296	100	0.2	0.5	0.99	-0.63	0.11
32	100	150	150	100	0.5	0.5	0.5	0	0.5
33	100	200	100	100	0.6	0.5	0.33	0.22	0.63
34	20	150	150	180	0.3	0.1	0.5	-0.28	0.02
35	80	150	150	120	0.5	0.4	0.5	-0.07	0.38
36	100	150	150	100	0.5	0.5	0.5	0	0.5
37	50	0.5	50	0.5	0.5	0.99	0.99	-0.25	0.75
38	25	25	25	25	0.5	0.5	0.5	0	0.5
39	15	35	15	35	0.5	0.3	0.3	0.1	0.4
40	25	0.5	50	25	0.3	0.5	0.99	-0.61	0.13
41	25	50	0.5	25	0.7	0.5	0.01	0.61	0.87
42	25	25	25	25	0.5	0.5	0.5	0	0.5
43	45	25	25	5	0.7	0.9	0.5	0.3	1
44	5	25	25	45	0.3	0.1	0.5	-0.3	0
45	25	25	25	25	0.5	0.5	0.5	0	0.5
46	495	5	495	5	0.5	0.99	0.99	-0.25	0.75
47	250	250	250	250	0.5	0.5	0.5	0	0.5
48	150	350	150	350	0.5	0.3	0.3	0.1	0.4
49	250	5	495	250	0.3	0.5	0.99	-0.61	0.13
50	250	495	5	250	0.7	0.5	0.01	0.61	0.87
51	250	250	250	250	0.5	0.5	0.5	0	0.5
52	450	250	250	50	0.7	0.9	0.5	0.3	1
53	50	250	250	450	0.3	0.1	0.5	-0.3	0
54	250	250	250	250	0.5	0.5	0.5	0	0.5
55	990	10	990	10	0.5	0.99	0.99	-0.25	0.75
56	500	500	500	500	0.5	0.5	0.5	0	0.5
57	300	700	300	700	0.5	0.3	0.3	0.1	0.4
58	500	10	990	500	0.3	0.5	0.99	-0.61	0.13
59	500	990	10	500	0.7	0.5	0.01	0.61	0.87
60	500	500	500	500	0.5	0.5	0.5	0	0.5
61	900	500	500	100	0.7	0.9	0.5	0.3	1
62	100	500	500	900	0.3	0.1	0.5	-0.3	0
63	500	500	500	500	0.5	0.5	0.5	0	0.5
64	150	225	225	150	0.5	0.5	0.5	0	0.5

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

65	444	6	444	6	0.5	0.99	0.99	-0.24	0.74
66	120	255	195	180	0.5	0.4	0.43	0.02	0.43
67	150	6	444	150	0.2	0.5	0.99	-0.63	0.11
68	150	225	225	150	0.5	0.5	0.5	0	0.5
69	150	300	150	150	0.6	0.5	0.33	0.22	0.63
70	30	225	225	270	0.3	0.1	0.5	-0.28	0.02
71	120	225	225	180	0.5	0.4	0.5	-0.07	0.38
72	150	225	225	150	0.5	0.5	0.5	0	0.5
73	50	75	75	50	0.5	0.5	0.5	0	0.5
74	148	2	148	2	0.5	0.99	0.99	-0.24	0.74
75	40	85	65	60	0.5	0.4	0.43	0.02	0.43
76	55	70	80	45	0.5	0.55	0.53	-0.01	0.53
77	45	80	70	55	0.5	0.45	0.47	0.01	0.47
78	50	2	148	50	0.2	0.5	0.99	-0.63	0.11
79	50	75	75	50	0.5	0.5	0.5	0	0.5
80	50	100	50	50	0.6	0.5	0.33	0.22	0.63
81	50	70	80	50	0.5	0.5	0.53	-0.04	0.47
82	50	40	110	50	0.4	0.5	0.73	-0.3	0.31
83	40	75	75	60	0.5	0.4	0.5	-0.07	0.38
84	10	75	75	90	0.3	0.1	0.5	-0.28	0.02
85	20	75	75	80	0.4	0.2	0.5	-0.21	0.14
86	35	75	75	65	0.4	0.35	0.5	-0.11	0.32
87	50	75	75	50	0.5	0.5	0.5	0	0.5
88	45	4	45	6	0.49	0.88	0.92	-0.23	0.67
89	40	9	40	11	0.49	0.78	0.82	-0.18	0.62
90	51	0	49	0	0.51	1	1	-0.25	0.76
91	22	21	28	29	0.43	0.43	0.57	-0.14	0.36
92	23	24	25	28	0.47	0.45	0.51	-0.05	0.43
93	27	32	18	23	0.59	0.54	0.36	0.21	0.66
94	15	35	20	30	0.5	0.33	0.36	0.05	0.4
95	35	20	30	15	0.55	0.7	0.6	0.03	0.68
96	4	14	9	14	0.439	0.22	0.39	-0.06	0.25
97	4	10	7	14	0.4	0.22	0.41	-0.1	0.22
98	13	10	8	4	0.657	0.76	0.44	0.27	0.87
99	17	2	10	6	0.542	0.74	0.83	-0.19	0.59
100	12	7	14	12	0.422	0.5	0.67	-0.21	0.38

V. CONCLUSIONS AND FUTURE SCOPE

In the present work, a new Composite Performance Metric, namely DAFAR has been proposed and experimented. The empirical results proved that this newly proposed composite metric is performing effectively in evaluating Network Intrusion Detection Systems. Among the three primitive metrics, DR, ACC, FAR; Detection Rate is given more prominence while designing the proposed metric. Even after decades of research in the area of Network Intrusion Detection Systems (NIDSs), there is no bench mark performance metric available in the literature to evaluate the performance of NIDSs. Thus a new performance metric is proposed in this paper. Even though, the proposed Composite Metric (DAFAR) is not being claimed as the best performance metric but it is surely a better one. There is

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

lot of scope to further extend this work. At present this Performance Metric is being used in the other works of the authors as objective criteria to evaluate the effectiveness of various classifiers.

REFERENCES

[1] Shiravi A, Shiravi H, Tavallaee M, Ghorbani AA. Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Comput Secur 2012;31(3):357–74 doi. Available from: http://dx.doi.org/ 10.1016/j.cose. 2011.12.012, http://www.sciencedirect.com/ science/article/ pii/S0167404811001672.

[2] TarfaHamed , Rozita Dara, Stefan C. Kremer, Network intrusion detection system based on recursive feature addition and bigram technique, computers & s e c u r i t y 73 (2 0 1 8) 137–155

[3] Gulshan Kumar, International Journal of Computer Science and Mobile Applications, Evaluation Metrics for Intrusion Detection Systems - A Study, Vol.2 Issue. 11, November- 2014, pg. 11-17

[4] M. E. Elhamahmy, Hesham N. Elmahdy and Imane A. Saroit, *A New Approach for Evaluating Intrusion Detection System*, CiiT International Journal of Artificial Intelligent Systems and Machine Learning, Vol 2, No 11, November 2010

[5] Kumar, G., Kumar, K.: Ai based supervised classifiers: an analysis for intrusion detection, In: Proc. of International Conference on Advances in Computing and Artificial Intelligence, pp. 170–174. ACM (2011)

[6] Jeni LA, Cohn JF, De La Torre F. Facing Imbalanced Data Recommendations for the Use of Performance Metrics. *International Conference on Affective Computing and Intelligent Interaction and workshops : [proceedings] ACII (Conference)*. 2013;2013:245-251. doi:10.1109/ACII.2013.47.

[7] Fawcett, Tom (2006) "An Introduction to ROC Analysis" (PDF). Pattern Recognition Letters. **27** (8): 861–874. doi:10.1016/j.patrec.2005.10.010

[8] Official Website of CIC: http:// www.unb.ca/cic/datasets/index.html

[9] Open Source, freely available and downloadable from: https: //www .cs. Waikato .ac. nz/ ml/ weka /down loading.html

[10]Lambert Schaelicke, Thomas Slabach, Branden Moore and Curt Freeland, Characterizing the Performance of Network Intrusion Detection Sensors, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.10.7356&rep=rep1&type=pdf

[11]K. Salah and A. Qahtan, Implementation and experimental performance evaluation of a hybrid interrupt-handling scheme, Computer Communications, 32.1(2009) 179–188

[12]Awsan Abdulrahman Hasan, Nur' Aini Abdul Rashid, Atheer Akram Abdulrazzaq, "GPGPU based Hybrid Multi-Pattern Algorithm design for high-speed Intrusion Detection System", *Control System Computing and Engineering (ICCSCE) 2014 IEEE International Conference on*, pp. 141-146, 2014.

[13]Subramanian Neelakantan, Shrisha Rao, "Content-Split Based Effective String-Matching for Multi-Core Based Intrusion Detection Systems", *Computational Intelligence Communication Systems and Networks 2009. CICSYN '09. First International Conference on*, pp. 296-301, 2009

[14] Qingbo Wang, Viktor K. Prasanna, "Multi-Core Architecture on FPGA for Large Dictionary String Matching", *Field Programmable Custom Computing Machines 2009. FCCM '09. 17th IEEE Symposium on*, pp. 96-103, 2009.

[15]https://machinelearningmastery.com/confusion-matrix-machine-learning/