

2018

Software Intrusion Detection Evaluation System: A Cost-Based Evaluation of Intrusion Detection Capability

Agbotiname L. Imoize


Taiwo Oyedare

Michael E. Otuokere

Sachin Shetty

Old Dominion University, sshetty@odu.edu

Follow this and additional works at: https://digitalcommons.odu.edu/vmasc_pubs

 Part of the [Databases and Information Systems Commons](#), [Information Security Commons](#), and the [Technology and Innovation Commons](#)

Repository Citation

Imoize, Agbotiname L.; Oyedare, Taiwo; Otuokere, Michael E.; and Shetty, Sachin, "Software Intrusion Detection Evaluation System: A Cost-Based Evaluation of Intrusion Detection Capability" (2018). *VMASC Publications*. 37.
https://digitalcommons.odu.edu/vmasc_pubs/37

Original Publication Citation

Imoize, A. L., Oyedare, T., Otuokere, M. E., & Shetty, S. (2018). Software intrusion detection evaluation system: A cost-based evaluation of intrusion detection capability. *Communications & Network*, 10(4), 211-229. doi: 10.4236/cn.2018.104017

Software Intrusion Detection Evaluation System: A Cost-Based Evaluation of Intrusion Detection Capability

Agbotiname L. Imoize^{1,2}, Taiwo Oyedare¹, Michael E. Otuokere², Sachin Shetty³

¹Bradley Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, USA

²Department of Electrical and Electronics Engineering, University of Lagos, Lagos, Nigeria

³Modeling, Analysis and Simulation Center, Old Dominion University, Norfolk, USA

Email: {aimoize,toyedare}@vt.edu, emmaotuoke@gmail.com, sshetty@odu.edu

How to cite this paper: Imoize, A.L., Oyedare, T., Otuokere, M.E. and Shetty, S. (2018) Software Intrusion Detection Evaluation System: A Cost-Based Evaluation of Intrusion Detection Capability. *Communications and Network*, 10, 211-229. <https://doi.org/10.4236/cn.2018.104017>

Received: August 14, 2018

Accepted: November 20, 2018

Published: November 23, 2018

Copyright © 2018 by authors and Scientific Research Publishing Inc. This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

Abstract

In this paper, we consider a cost-based extension of intrusion detection capability (C_{ID}). An objective metric motivated by information theory is presented and based on this formulation; a package for computing the intrusion detection capability of intrusion detection system (IDS), given certain input parameters is developed using Java. In order to determine the expected cost at each IDS operating point, the decision tree method of analysis is employed, and plots of expected cost and intrusion detection capability against false positive rate were generated. The point of intersection between the maximum intrusion detection capability and the expected cost is selected as the optimal operating point. Considering an IDS in the context of its intrinsic ability to detect intrusions at the least expected cost, findings revealed that the optimal operating point is the most suitable for the given IDS. The cost-based extension is used to select optimal operating point, calculate expected cost, and compare two actual intrusion detectors. The proposed cost-based extension of intrusion detection capability will be very useful to information technology (IT), telecommunication firms, and financial institutions, for making proper decisions in evaluating the suitability of an IDS for a specific operational environment.

Keywords

Intrusion Detection System, Intrusion Detection Capability (CID), Information Theory, Software Intrusion Detection Evaluation System (SIDES)

1. Introduction

In recent times, the ease of application of computer systems and availability of

internet services has dramatically changed the way businesses are transacted on the global scene. This has led to rapid developments in the field of computing and e-business. Consequently, the risk of unwarranted access to computer systems has increased in proportionate measures. There is no denying the fact that several cases of computer security attacks are reported daily across the globe. This calls for a serious concern for organizations and corporate bodies to decisively step up the game of securing computer systems from intrusion. In order to ameliorate this ugly incident, individuals and organizations are currently deploying passphrases, antivirus applications, and firewall to protect networks and sensitive data. Unfortunately, these algorithms have limited capabilities to secure information. For example, passwords of such algorithms can be compromised [1]. In addition, fire walls could be inefficient and lack the capacity to allow real time monitoring of security systems [2]. Therefore, the need for intrusion detection systems to improve system security through real time monitoring and detection of attacks and intrusion can not be overemphasized. Intrusion detection system (IDS) refers to the mechanism for identifying an abuse and or compromise of a computer system by attackers from internal and external sources [3]. Therefore, the task of securing all computer systems in an organization from all possible attackers is necessary and should be taken seriously [4].

Although there have been many research and development efforts in IDS, appropriate evaluation of IDS is still a major problem. Some of the problems include 1) no standard benchmark, which makes comparison of IDS difficult, 2) dynamic changing environment, making it difficult to establish a fully descriptive baseline, 3) issues with empirical evaluations (using data-set to test IDS) as there will always be a difference between data-set and real scenario.

However, a key problem in intrusion detection is how to determine the essential metrics to appropriately evaluate IDS in objective terms, especially how to ascertain the capabilities of the IDS to categorise events as normal or intrusive [5]. Although several metrics such as the true positive rate, false positive rate, intrusion detection capability, receiver operating characteristics and several others that measure different aspects of intrusion detection systems, have been reported in the literature, it is very difficult to find a single metric that is completely adequate for the evaluation of the capability of an IDS, especially as it relates to the cost of operation.

In practice, a unifying metric could possibly be deployed to assist the administrator of a particular network in the choice of an appropriate detector from a pool of systems or enhance an existing configuration settings of a known intrusion detector system for a defined network environment [5] [6]. Intrusion detection capability, C_{ID} is a single unified metric proposed by Gu *et al.* [5] based on information theory. For the unified metric, if a given IDS is tuned with respect to the C_{ID} , it becomes very easy to ascertain or determine the particular operating point that gives the minimum level of uncertainty about a defined input event that occurred due to intrusion or not is determined. However, the C_{ID} me-

tric does not take into consideration the expected cost associated with that operating point. In addition, it could be quite expensive to quantify in practical terms of interest like false alarm and detection rates, how to minimize the uncertainty of an attack.

Thus, this study presents a cost-based extension of the intrusion detection capability (C_{ID}). Determining the corresponding costs complements and increases the scope of C_{ID} as an evaluation metric rather than just diminishing the uncertainty of the intrusions as proposed in [7]. This extension provides the expected costs associated with an operating point and also specifies the best response decision to take with respect to the detectors report. Specifically, the objective of this work is to find the corresponding cost of C_{ID} for the optimal operating point. This will provide an explanation for the IDS optimal point in terms of the least expected cost. Thus, the cost of tuning the detector to the optimal point will be determined. Another objective is to determine the optimal operating point of an IDS in terms of cost. This defines the ability of the IDS to classify events at the least expected cost. We then demonstrate how the proposed metric facilitates the comparison of IDSs.

In particular, our contributions include the following: 1) a mathematical formulation is presented using information theory and based on this formulation; 2) a package for computing the intrusion detection capability of IDS, given certain input parameters is developed; 3) to include cost function in C_{ID} , a decision tree approach is used as a method of analysis for evaluation; 4) the cost-based extension is used to select optimal operating point, calculate expected cost and compare two actual intrusion detectors. Finally, the results in this paper are compared with the results of related works reported in [5] [7].

The remainder of this paper is described as follows. Section II summarizes related works on intrusion detection. Section III discusses the theoretical background of intrusion detection as it relates to information theory and the associated cost. Section IV presents the system architecture for software intrusion detection evaluation scheme (SIDES). Section V presents the results with some discussions on changing some of the parameters used in the evaluation. Section VI concludes the paper and states useful contributions as well as recommendations for future studies.

2. Related Work

Recently, there has been an unprecedented growth in technologies involving the use of computer applications. Consequently, this has given birth to rapid cases of denial of service attacks, proliferation of worms and virus attack, and increased activities of hackers have led to increased security concern at all levels of public and private-sector organizations. This has encouraged useful researches on IDS in recent years. In the existing literature, various models for IDS have been proposed based on architecture, fault tolerance, and mobile agent platforms. Some authors compared the distributed model architecture with the traditional centra-

lized models and demonstrated that the future of IDS is pointing towards distributed or hybrid architecture [8]. Other authors focused on the intrusion detection evaluation problem with a focus on an elaborate comparison of various IDS schemes, investigate the performances of IDS, and obtaining the most efficient configuration structure for IDS [5] [9] [10].

In 1998, a study sponsored by DARPA was carried out at the Lincoln Laboratory of Massachusetts Institute of Technology. Prior to this study, not much information on intrusion detection systems is available in the open literature. The 1998 DARPA offline project actually opened up this interesting area of research following a detailed and elaborate report on the test of IDSs in a real world environment [11].

Gu *et al.* [5] argued that lack of a single unified metric makes it difficult to fine-tune and evaluate IDS. It was defined that an information theoretic measure is the ratio of the mutual information between IDS input and output, and the entropy of the input. Through numerical examples and experiments of actual IDSs, it was demonstrated that using the proposed metric, the best (optimal) operating point for an IDS can be obtained. In addition, the new metric can objectively compare different IDSs.

In a similar study [12], a framework for the evaluation of intrusion detection was proposed. Previous studies [5] [7] [8] which introduced evaluation metrics such as the intrusion detection capability (C_{ID}), the expected cost, and the Bayesian detection rate were reviewed. The strengths and drawbacks of the individual performance metrics were investigated and analyzed in a closed form. In addition, a new IDS performance trade-off referred to as intrusion detection operating characteristics (IDOC) curves is introduced, and real world data were used to test the validity of the practical and simulated results.

In the same vein, Sallay *et al.* [9] presented a report on the method of evaluating the performance of intelligent techniques available for the detection and prediction of unauthorized intrusion in security networks. The authors stressed the need for the development of an appropriate technique for enhancing the success rate of the predictions of a detector, and evaluating the cost implications in a situation where a wrong decision is made by the detector. In addition, the authors developed a model suitable for the training of detectors to be able to properly predict and detect intrusion in the network, based on the Bayesian approach. The findings reported in the paper showed that the proposed model predicted intrusion with a very high detection rate, with minimal false alarms. Furthermore, the authors opined that the model proposed would provide an effective and efficient detection of numerous network attacks with false alarm rates provided that there are available anomalies for training.

Authors in [13] proposed a deep learning approach for intrusion detection systems. The model trains a well-known deep learning model called Deep Auto-Encoder in a greedy layer wise fashion so as to avoid local optima and overfitting. A similar dataset (KDD-CUP'99) used in our work was utilized to validate

their model. Different from our work, they did not evaluate the cost of the intrusion detection capability.

In [14], a more interactive approach to detecting and predicting anomaly based on IDS was proposed. This approach takes a metric described as F-score per Cost (FPC) for each attack predictor into consideration. Here, misclassification of attack class “MC” is used to denote instances of wrong predictions of an attack as another attack class. The authors used three competitors in conjunction with “KDD CUP’99” competition to validate the authenticity of the proposed metric. Generally, the findings revealed an enhanced performance by the metric, showing an excellent understanding of the performance of the IDS. It was concluded in the paper that the proposed scheme showed great improvements over existing intrusion detection systems.

On performance metric scorecard-based approach to the evaluation of IDS associated with wireless networks [15], a set of performance metrics that find useful applications in wireless IDS were reported. Here, “scorecards” that have set of values suitable for evaluating and testing wireless IDS are employed. As a test, the proposed scheme was matched to a set of wireless IDS such as the Air defence Gaurd, kismet, and snort wireless.

Authors in [16] provided a review of the metrics and performance evaluation of contemporary intrusion detection systems available in literature. The emphasis was on flexible approaches that are able to perform well with respect to the metrics highlighted. An empirical evaluation of the IDS was discussed via standard and custom metrics. Evaluation criteria used include correctly classified instances (CCI) and incorrectly classified instances (ICCI). The outcome of this type of evaluation shows that different algorithms are required to process different types of attacks in the network based on the detection performance of different IDS.

In a related study, Verma and Ranga [17] reported a statistical description of labelled flow-based CIDDS 001 dataset suitable for the evaluation of Anomaly-based network IDSs. The k-nearest neighbor classification and k-means clustering techniques were employed to measure the robustness of metrics in IDSs. From their evaluation results, both techniques perform well over CIDDS-001 data-set. Metrics used include true positive rate, false positive rate, precision, detection rate and F-measure. Their simulation was done on Weka. Different from our work, they did not investigate the cost of utilizing their intrusion detection system. Popoola *et al.* [18] proposed a feature selection technique for network intrusion detection using discretized differential evolution (DDE). Their technique was able to identify 16 features capable of classifying connections in NSL-KDD data-set with high accuracy. They used standard metrics used in the literature similar to [17]. They also did not consider cost of implementing their technique.

In view of the foregoing, this study is aimed at developing a cost-based extension of the intrusion detection capability which has not been given a fair treat-

ment in the existing literature.

3. Theoretical Background

3.1. Intrusion Detection and Information Theory

Essentially, a quality IDS should be able to distinguish the events monitored (input data) as either intrusive or normal. Here, the IDS provide output information usually in form of alarms, that should give a true picture of the events being monitored. This means that the IDS should be able to detect whether there is actually an intrusion or not at any given time. Therefore, the task of a well designed IDS is to accept and analyze input data stream and give output alerts to show the presence of intrusion. On a careful analysis, each unit of an input data stream could be intrusive or normal and an IDS should be able to know and record these information for the attention of the administrator. This implies that the input of an IDS can be carefully modeled as a random variable X . For instance, if the value of X is high ($X = 1$), there is an intrusion and if X is low ($X = 0$), there is no intrusion and the traffic is normal.

Similarly, the output information of a typical IDS can be modeled as a random variable Y . Here, when $Y = 1$, it means that there is an alert of an intrusion, and when $Y = 0$, there is no alert information from the IDS. In a situation where it is assumed that an IDS output is available, and this corresponds to each input information to the IDS [5]. By leveraging on the knowledge of information theory, a binary symmetric channel can be used to model intrusion detection as illustrated in **Figure 1**. As shown in the model, $p(X = 1)$ denotes the base rate, which means the prior probability that there are intrusions in the input information as detected by the IDS. This is denoted as B .

The probability that an intrusion event can be regarded as normal is represented by $p(Y = 0 | X = 1)$. This is the false negative rate (FN), denoted as γ . Similarly, the probability that a normal event being misclassified as an intrusion is represented by $p(Y = 1 | X = 0)$. This is the false positive rate (FP), denoted as α . From the foregoing, it can be assumed that X is the random variable depicting the IDS input and Y represents the random variable depicting the IDS output. Therefore, intrusion detection capability can be defined as:

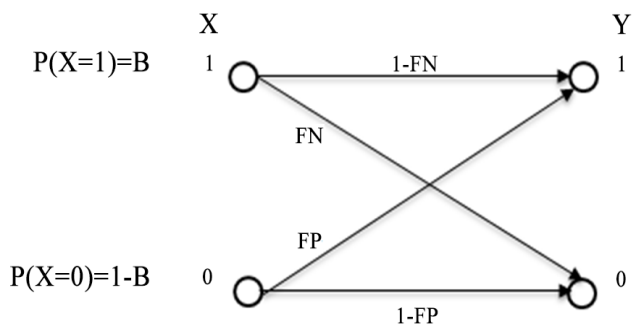


Figure 1. A binary symmetric model for intrusion detection [5].

$$C_{ID} = \frac{I(X;Y)}{H(X)} \quad (1)$$

Given what we know from our knowledge of information theory about mutual information, we can rewrite C_{ID} as Equation (2).

$$C_{ID} = \frac{H(X) - H(X|Y)}{H(X)} \quad (2)$$

Ideally, mutual information captures the decrease in the level of uncertainty of the input by evaluating the IDS output. From (2), it can be deduced that C_{ID} gives the ratio of the reduction of uncertainty of the IDS input given the IDS output. In practice, the value of C_{ID} is in the range of [0; 1]. Here, a large value of C_{ID} implies that the IDS is more capable of accurate classification of events.

The mutual information $H(X)$ is defined as given in Equation (3), and the corresponding mutual information that an event has occurred $H(X|Y)$ is given in Equation (4).

$$H(X) = -\sum_x p(x) \log p(x) = -B \log B - (1-B) \log(1-B) \quad (3)$$

$$\begin{aligned} H(X|Y) &= \frac{-\sum_x \sum_y p(x) p(y|x) \log[p(x) p(y|x)]}{p(y)} \\ &= -B(1-\gamma) \log PPV - B\gamma \log(1-NPV) \\ &\quad - (1-B)(1-\alpha) \log NPV - (1-B)\alpha \log(1-PPV) \end{aligned} \quad (4)$$

Substituting the equations, C_{ID} we obtain Equation (5).

$$C_{ID} = \frac{-B \log B - (1-B) \log(1-B)}{-B(1-\gamma) \log PPV - B\gamma \log(1-NPV) - (1-B)(1-\alpha) \log NPV - (1-B)\alpha \log(1-PPV)} \quad (5)$$

In Equation (5), C_{ID} is intrusion detection capability, B is base rate, γ is false negative (FN) rate, α is false positive (FP) rate, PPV is positive predictive value and NPV is negative predicative value.

- Base rate (B): This is a measure of the environment in which IDS operates. When $B = 0$ or $B = 1$ (the input is 100% normal or 100% intrusion). In practice, it can be quite difficult to measure or control the base rate in an IDS. This is because the base rate is often seen as an operation parameter partly due to the fact that it is used to measure the IDS environment. The estimation of prior probabilities and base rate B has been presented in [8].
- False Positive (FP) Rate: This is the probability that the IDS outputs an alarm when there is no intrusion;
- False Negative (FN) Rate: This is the probability that an IDS does not output an alarm when there is an intrusion;
- Positive Predictive Value (PPV): This is the probability that there is an intrusion when the IDS output an alarm. That is, given IDS alarms, how many of them are real intrusions. It is mathematically expressed in Equation (6) [5] [8];

$$PPV = \frac{B(1-\gamma)}{B(1-\gamma) + (1-B)\alpha} \quad (6)$$

- Negative Predictive Value (*NPV*): This is the probability that there is no intrusion when the IDS does not output an alarm. That is given that there are no IDS alerts; does it mean that there are really no intrusions? Mathematically, it can be expressed in Equation (7) [8].

$$NPV = \frac{(1 - B)(1 - \alpha)}{(1 - B)(1 - \alpha) + B\gamma} \tag{7}$$

3.2. Receiver Operating Characteristics (ROC)

The receiver operating characteristics (ROC) curve shows a graphical illustration of the detection probability against false alarm rate. This means that the curve is capable of showing the probability of detection as seen by the detector at a defined false alarm rate. Alternatively, the curve shows the detector’s captured false rate at a stated probability of detection [7]. During World War II, the ROC curve was used for the first time to analyze radar signals before its usage in signal detection theory. The 1941 Harbor attack motivated the US army to embark on researches on how to improve on accurate detection of the Japanese aircraft as seen from the radar signals captured by the US army. In order to achieve this critical task, they employ the principle of the Receiver Operating Characteristics [19] to determine the capabilities of the radar receiver operators to effectively distinguish between various signals captured from different radars. Generally, ROC analysis helps to select optimal solutions while disregarding sub-optimal solutions.

3.3. Expected Cost

For a given operating point of a particular detector, it is possible to determine the expected cost by analyzing the outputs of the decision tree as illustrated in Figure 2.

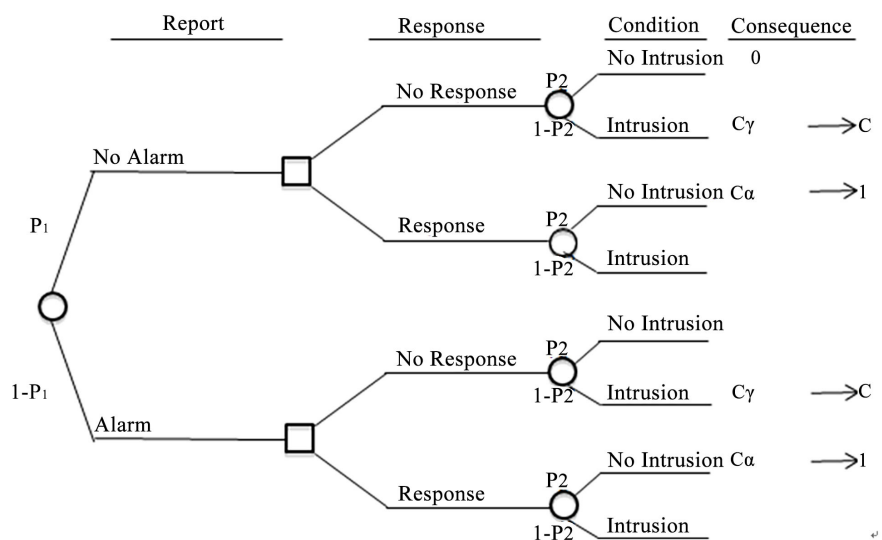


Figure 2. Decision tree showing the detector’s expected cost [7].

As shown in the decision tree of **Figure 2**, the squares represent sequence of actions, which are being controlled by the decision maker, while the circles represent uncertain events that are outside the control of the decision maker. However, these events give useful information on the operation of the detector, and subsequent actions to be taken on the reports. In addition, the decision tree can provide useful tips on the risks involved when some actions and events are combined. Again, it is seen that cost correspond to the consequences, and reflects the cost of a wrong decision. For example, the cost of not giving a response when there is no alarm (NA), and the cost of not providing a response when there is intrusion is represented with C . Here, the cost of no response when there is an intrusion is zero, and the higher the cost, the outcome reduces in value and less appreciated. It should be noted that the probability of occurrence is attached to each uncertain event. As seen on the decision tree, three probabilities $P1$, $P2$, and $P3$ are worth describing. $P1$ refers to the probability that the detector is able to report an alarm, $P2$ is the conditional probability that there is no intrusion given that the detector did not report an alarm, and $P3$ is the conditional probability that there is no intrusion given that the detector actually reports an alarm.

Conventionally, the decision tree is read from left to right [20], and in order to calculate the expected cost associated with any given operating point, costs are carefully calculated for all paths on the decision tree, and the probabilities $P1$, $P2$, and $P3$ are computed. Without loss of generality, cost ratio is defined as in Equation (8);

$$C = \frac{C_\gamma}{C_\alpha} \quad (8)$$

where C_γ refers to the cost of responding to the presence of intrusion and C_α is the cost of responding to an intrusion where there is actually no intrusion. In most practical scenarios, it can be assumed that the cost of correct responses to intrusion is negligibly small or zero [21].

1) Expected Cost Calculation: The formulae depicting the total probability as shown in (9) and (10) can be used to evaluate the probabilities of the detector's reports [22].

$$p_1 = P(NA) = P(NA|NI)P(NI) + P(NA|I) = (1-\alpha)(1-p) + \gamma p \quad (9)$$

$$1 - p_1 = P(A) = P(AN|I)P(NI) + P(A|I)P(I) = \alpha(1-p) + (1-\gamma)p \quad (10)$$

The Bayes Theorem as reported in [16] can be used to calculate the probabilities of the state of the system with respect to the reports given by the detector as shown in Equations (11)-(14).

$$p_2 = P(NI|NA) = \frac{P(NA|NI)P(NI)}{P(NA)} = \frac{(1-\alpha)(1-p)}{p_1} = \frac{(1-\alpha)(1-p)}{(1-\alpha)(1-p) + \gamma p} \quad (11)$$

$$1 - p_2 = P(I|NA) = \frac{P(NA|I)P(I)}{P(NA)} = \frac{\gamma p}{p_1} = \frac{\gamma p}{(1-\alpha)(1-p) + \gamma p} \quad (12)$$

$$p_3 = P(NI|A) = \frac{P(A|NI)P(NI)}{P(A)} = \frac{\alpha(1-p)}{1-p_1} = \frac{\alpha(1-p)}{\alpha(1-p) + (1-\gamma)p} \quad (13)$$

$$1 - p_3 = P(I|A) = \frac{P(A|I)P(I)}{P(A)} = \frac{(1-\gamma)p}{1-p_1} = \frac{(1-\gamma)p}{\alpha(1-p) + (1-\gamma)p} \quad (14)$$

As shown in **Table 1**, the expected cost, which is dependent on the detector's report, is shown mathematically by finding the sum of the products of the probabilities together with the cost of the node following the response.

At any operating point, the expected cost of operating the IDS is given in Equations (15) and (16):

$$C_{EX} = \frac{p_1 \min\{C\gamma p, (1-\alpha)(1-p)\}}{p_1} + \frac{(1-p_1) \min\{C(1-\gamma)p, \alpha(1-p)\}}{1-p_1} \quad (15)$$

$$C_{EX} = \min\{C\gamma p, (1-\alpha)(1-p)\} + \min\{C(1-\gamma)p, \alpha(1-p)\} \quad (16)$$

3.4. Selection of Optimal Operating Point

In practice, the optimal operating point is described as the most suitable point achievable by the given IDS in terms of its intrusion detection capabilities, and minimization of the expected cost. Therefore, choosing an optimal operating point would be equivalent to the best choice of values for the parameters α and γ that can provide the desired least expected cost.

3.5. The Base-Rate Fallacy

On the concept of base-rate fallacy, there seems to be a very large difference between the amounts of events seen as normal and the amount of intrusion events, which are very few. This huge difference can result in the generation of multitudes of false alarms. Here, fallacy maintains that due to the low probability of a real attack, especially when an IDS triggers an alarm, the probability of intrusion occurring could be very minimal. Furthermore, Gu *et al.* [5] argued that the base-rate is significantly small as compared with the composite attacks in the evaluation data-set. Here, it is assumed that the base-rate content in the 1998 DARPA intrusion detection evaluation is given as $p = 6.52 \times 10^{-5}$, unless stated otherwise.

4. System Architecture for Software Intrusion Detection Evaluation System

Introducing the cost-based extensions on C_{ID} metric makes it achieve similar capability as ROC which integrates cost analysis and more practically beneficial, because the various operating points for the IDS will have an associated cost function [23]. The objective is to choose the operating point with the highest C_{ID} at the least expected cost.

4.1. Determining the Optimal Operating Point C_{ID}

A mathematical formula as shown in Equation (5) is derived from an information theoretic point of view. To ease computation, a software intrusion detection evaluation system (SIDES) package is developed. The application provides a tool for calculating the intrusion detection capability C_{ID} of IDS using values from the

Table 1. Expected cost of response with respect to the detectors' report.

Detectors Report	RESPONSE	
	No Response (NR)	Response (R)
No alarm (NA)	$1 - p_2 = C \frac{\gamma p}{(1-\alpha)(1-p) + \gamma p}$	$p_2 = \frac{(1-\alpha)(1-p)}{(1-\alpha)(1-p) + \gamma p}$
Alarm (A)	$1 - p_3 = C \frac{(1-\gamma)p}{\alpha(1-p) + (1-\gamma)p}$	$p_3 = \frac{\alpha(1-p)}{\alpha(1-p) + (1-\gamma)p}$

Receiver Operating Characteristics (ROC) reported in [24]. The ROC was based on the dataset reported in [11]. The proposed package was designed to receive metrics such as Base rate (B), False Positive rate (FP or α), False Negative rate (FN or γ), Positive Predictive Value (PPV), Negative Predictive Value (NPV) and calculates intrusion detection capability C_{ID} .

4.2. Algorithm of the SIDES Package

The algorithm for the SIDES package is as shown in **Algorithm 1**.

Algorithm 1. Algorithm for SIDES package.

```

1: Start
2: Verification Page
3:
4: if Verification = TRUE then
5: Step4
6: else
7: Step1
8: end if
9: Input  $\alpha$ ,  $B$  and  $(1 - \gamma)$ 
10: Calculate  $PPV \leftarrow \frac{B(1-\gamma) + (1-B)\alpha}{B(1-\gamma)}$ 
11: Calculate  $NPV \leftarrow \frac{(1-B)(1-\alpha)}{1-B(1-\alpha)} + B\gamma$ 
12: Calculate  $H(X) = -B \log(B) - (1-B) \log(1-B)$ 
13: Calculate
 $H(X|Y) = -B(1-\gamma) \log PPV - B\gamma \log(1-NPV) - (1-B)(1-\alpha) \log NPV - (1-B)\alpha \log(1-PPV)$ 
14: Calculate  $C_{ID} \leftarrow \frac{H(X) - H(X|Y)}{H(X)}$ 
15: Output  $C_{ID}$ 
16: Stop

```

Using this application and the Receiver Operating Characteristics (ROC) values reported in [24], the results obtained provide a useful guide in the choice of the optimal operating and a fair comparison of the IDSs. The point with the highest C_{ID} is regarded as the best ID capability of the system and gives the most

optimized operating point for the IDS. This is without recourse to the cost implication of operating at this optimal point. It is therefore necessary to attach a corresponding cost to this point.

4.3. Expected Cost

To introduce cost function into C_{ID} , we adopt the decision tree analysis method [7]. We compute the corresponding cost attached to each value of C_{ID} . To have an acceptable trade-off between cost and capability, C_{ID} and C_{EX} values are plotted against α . The lowest point on the C_{EX} curve is matched with the highest point on the C_{ID} curve to determine the optimal operating point. More specifically, the observable deviations in the values of the expected cost could be very useful metric suitable for the comparison of two intrusion detectors.

4.4. Design of SIDES

Text fields were used to receive input; False Positive rate (α), False Negative rate (γ) and Base rate (B). “Reset values” button was designed to clear the input values. Calculate PPV and calculate NPV buttons were designed to calculate PPV and NPV respectively. Calculate C_{ID} button was designed to calculate the intrusion detection capability of the IDS given the initial inputs received. The results panel is designed to display the calculated values PPV , NPV and C_{ID} . Back home button was designed to take the user back to initial information window. Exit button was designed to close the package.

5. Results and Discussion

5.1. Results of Analysis

Results of C_{ID} values were computed using data extracted from two ROC curves reported in [7]. Here, two ROC curves derived from the results reported in [11] are used to represent two intrusion detection systems, denoted as IDS_1 and IDS_2 , respectively. As in [7], IDS_1 ROC curve can be approximated as given in Equations (17) and (18).

$$1 - \gamma = 0.6909 \times (1 - \exp(-65625.64\alpha^{1.19})) \quad (17)$$

$$1 - \gamma = 0.4909 \times (1 - \exp(-11932.6\alpha^{1.19})) \quad (18)$$

Initial findings revealed that in 666,000 network session over a typical day, about 43 intrusion attempts were detected. Based on the assumption that the intrusion responses are achieved per session each time intrusion detectors are applied, the base-rate of intrusion is given as in (19).

$$B = \frac{\text{Total number of intrusion attempts}}{\text{Total number of network sessions}} = \frac{43}{660000} = 6.52 \times 10^{-5} \quad (19)$$

Hence, we can estimate the probability of intrusion by the base-rate $p = 6.52 \times 10^{-5}$. The results obtained from estimating the probability of intrusion are as depicted in **Figure 3** and **Figure 4**, for IDS_1 and IDS_2 , respectively.

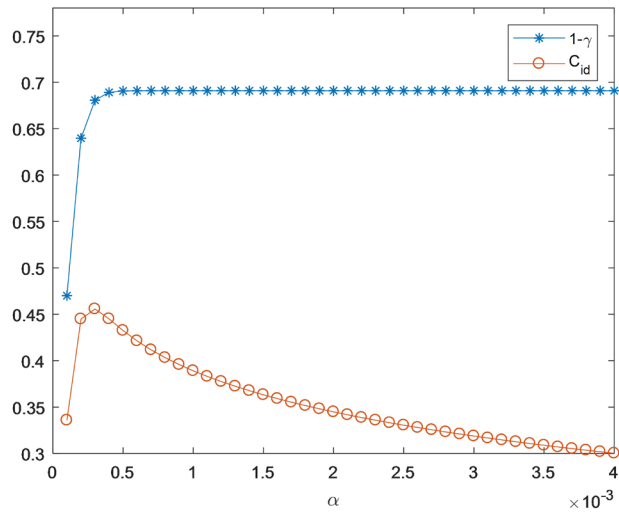


Figure 3. A plot of C_{ID} values computed for IDS_1 .

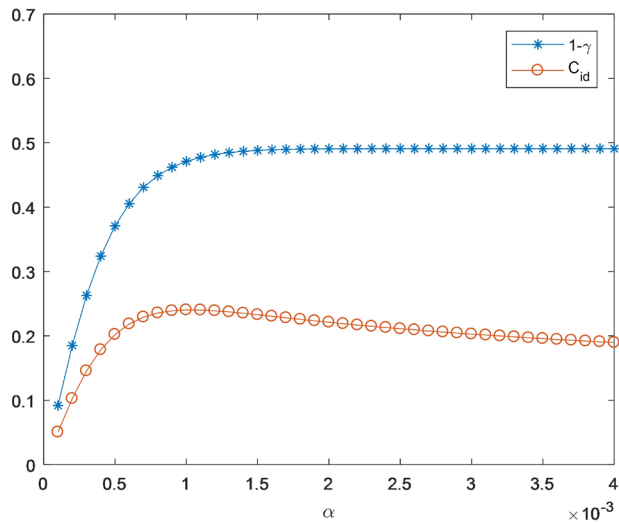


Figure 4. A plot of C_{ID} values computed for IDS_2 .

5.2. Selection of Optimal Operating Point

In practice, the point at which the highest intrusion detection capability and its threshold yields the most suitable threshold is referred to as the optimal operating point. Here, the optimal operating point for IDS_1 occurs at $\alpha = 0.003$, $1 - \gamma = 0.6807$ corresponding to C_{ID} of 0.45567, while that of IDS_2 occurs at $\alpha = 0.001$, $1 - \gamma = 0.47112$, and C_{ID} of 0.2403. From the foregoing, IDS_2 achieves a better ID capability than IDS_1 . By extension, comparing the two detectors based on the above analysis, we can conclude that IDS_2 is better than IDS_1 . However, this is without recourse to the cost of operating at the selected optimal point.

5.3. Minimum Expected-Cost Operating Point

For the derivation of minimum expected-cost operating point, the decision tree as shown in **Figure 2** is adopted. Here, the tree is evaluated from the right hand

side to the left. For instance, if the cost ratio C equals 1000, this means that it could be a thousand times more expensive to fail in response to an intrusion than to respond to no intrusion. Assume also that the base rate (probability of intrusion) were 6.52×10^{-5} as in [5].

From **Figure 5**, the maximum C_{ID} for IDS_1 occurs at $\alpha = 0.0003$, with a C_{ID} value of 0.4557. The minimum corresponding cost occurs at $\alpha = 0.0003$, with an expected cost of 0.0211. Hence, the optimal operating point for IDS_1 is 0.4557, 0.0211.

From **Figure 6**, the maximum C_{ID} for IDS_1 occurs at $\alpha = 0.0010$, with a C_{ID} value of 0.2403. The minimum corresponding cost occurs at $\alpha = 0.0010$, with an expected cost of 0.0355. Thus, the optimal operating point for IDS_2 is 0.2403, 0.0355.

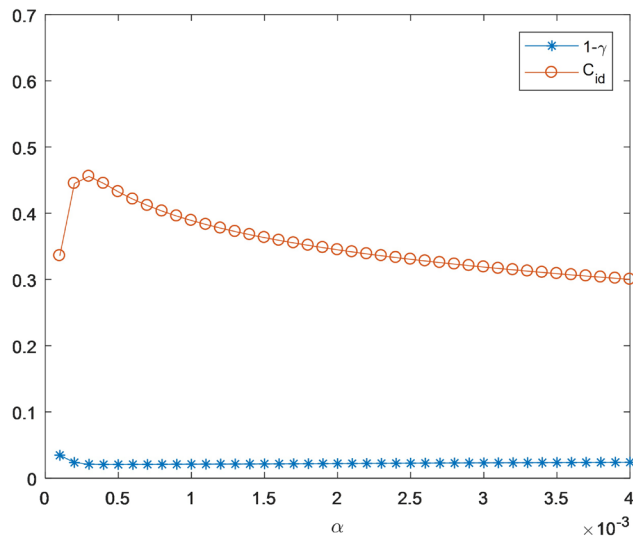


Figure 5. A plot of C_{ID} and C_{EX} values computed for IDS_1 .

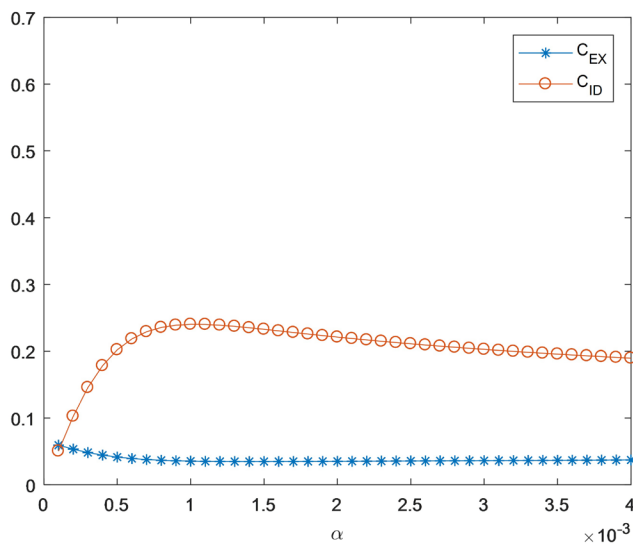


Figure 6. A plot of C_{ID} and C_{EX} values computed for IDS_1 .

5.4. Comparison of IDS₁ and IDS₂

A comparative analysis of IDS₁ and IDS₂ is as shown in **Table 2**.

IDS₁ is a better detector with a C_{ID} of 0.2154 per session higher than the C_{ID} of IDS₂ and an expected cost of 0.0144 per session less than that of IDS₂. The effect of the various input parameters on C_{ID} and C_{EX} is examined.

5.5. Effect of Different Base Rates on C_{ID}

Ideally, an IDS may not be able to effectively control the base rate but it is a very important factor to be considered when presenting reports on intrusion detection capability because the base rate defines the environment of operation [5]. To study the effect of low base rate on Intrusion Detection capability, C_{ID} values were computed for different base rate values. The impact of different base rates on C_{ID} is as shown in **Figure 7**.

From **Figure 7**, assuming an IDS whose base rate $B = 10^{-4}$, $FP = 0.1$ and $FN = 0.1$. In a case where the value of FP is decreased from 0.1 to 0.01, correspondingly, C_{ID} changes from 0.17 to 0.36. However, if FN is decreased by the same magnitude, the C_{ID} only changes from about 0.17 to 0.20. This shows that C_{ID} is more responsive to variations in false positive (FP) than false negative (FN). Hence, for low base rates, reducing FP will improve C_{ID} more than the same reduction in FN .

Table 2. Analysis of IDS₁ and IDS₂ when $C = 1000$ and $p = 6.52 \times 10^{-5}$.

	IDS ₁	IDS ₂
α	0.0003	0.0010
$1 - \gamma$	0.3699	0.4711
C_{ID}	0.4557	0.2403
C_{EX}	0.0211	0.0355

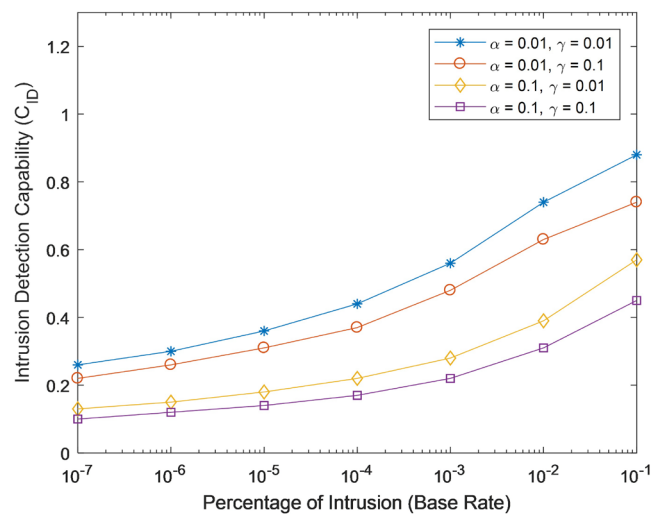


Figure 7. The effect of Base rate (B) for changes in α against fixed γ .

5.6. Effect of False Positive on C_{ID}

The base rate B was fixed and for each value of $FP(\alpha)$, the $FN(\gamma)$ values were varied and the corresponding C_{ID} calculated. A plot of False Positives rates against C_{ID} is shown in **Figure 8**.

From **Figure 8** ($B = 0.0001$), when $FP(\alpha)$ is increased from 0.01 to 0.02 for $\gamma = 0.01$ (a difference of 0.01), C_{ID} changes from 0.44 to 0.37 (a difference of 0.07). However, when FP changes from 0.01 to 0.03 (a difference of 0.02), C_{ID} changes from 0.44 to 0.33 (a difference of 0.11). Hence, for low base rate B , little changes in False Positive result in large changes in C_{ID} as shown in **Figure 8**.

5.7. Effect of False Negative Rate on C_{ID}

The base rate B is fixed while for each value of FN , the FP values are varied and the corresponding C_{ID} calculated. A plot of False Positive rates on against C_{ID} is as shown in **Figure 9**.

From **Figure 9** ($\alpha = 0.001$), when FN is increased from 0.1 to 0.2 (a difference of 0.1), C_{ID} changes from 0.58 to 0.49 (a difference of 0.09). However, when FN changes from 0.1 to 0.15 (a difference of 0.05), C_{ID} changes from 0.58 to 0.54 (a difference of 0.04). Only large changes in FN will significantly affect C_{ID} . Hence, for low base rate B , only a large variation of $FN(\gamma)$ have a significant effect on C_{ID} as shown in **Figure 9**.

5.8. Effect of Cost Ratio C on Expected Cost

As pointed out in [1], the major drawback in the expected cost analysis presented in Section V is that the cost ratio C is chosen subjectively. Thus the effect of cost ratio on the expected cost is examined.

From **Figure 10**, it is shown that the various plots of C indicate that the sharpest drop in the expected cost is between $\alpha = 0.0001$ and $\alpha = 0.0002$. As the FP increases, the expected cost remains fairly constant. This shows that to minimize expected cost, it is imperative that $FP(\alpha)$ is very low. This agrees with

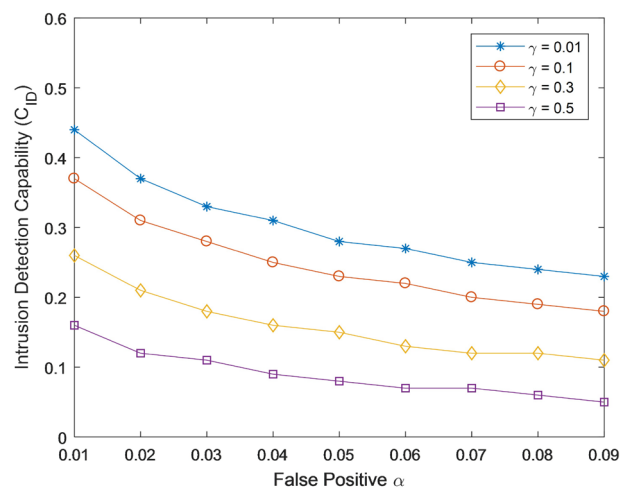


Figure 8. The effect of $FP(\alpha)$ on C_{ID} .

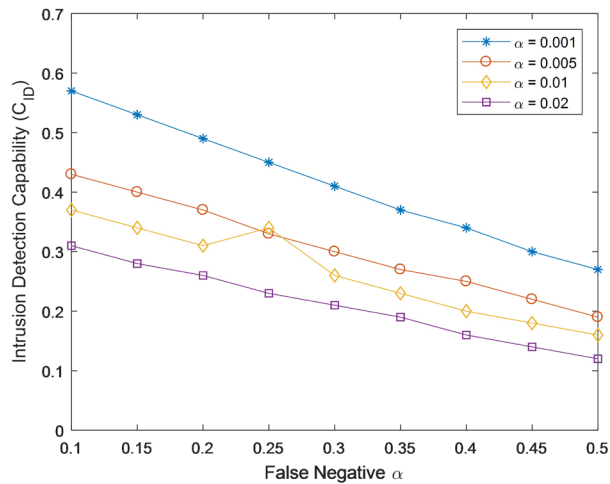


Figure 9. The effect of $FN(\gamma)$ on C_{ID} .

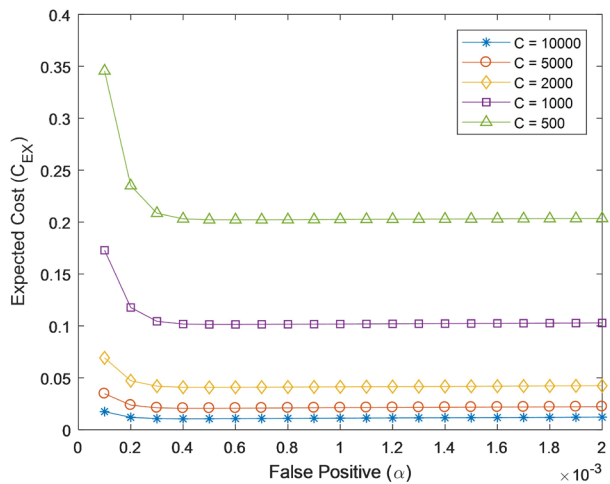


Figure 10. Effect of cost ratio C on Expected cost C_{EX} .

Gu *et al.* [5] that in realistic IDS operation environment, it can be reasonably assumed that $B < \alpha \ll \gamma < 1$. Furthermore, **Figure 10** implies that for large values of FP , the expected cost remains the same.

6. Conclusion and Future Work

In this paper, the concept of cost analysis in intrusion detection capability (C_{ID}) in a typical IDS environment with a low base rate is presented. Information theoretic analysis is used to model IDS and determine the intrusion detection capability of the detector. The decision tree method was introduced to compute the expected cost of operation for each operating point. Findings revealed that the optimal operating point is the point of intersection between the maximum C_{ID} and the expected cost curve. Cost-based extension of C_{ID} can be a very useful method to appropriately evaluate IDS to determine the type and capabilities of an IDS to be deployed in a particular network. This is of great importance in determining the suitability of an IDS in a given environment regarding the ability

of the detector to classify events appropriately at the least expected cost. Future work could include investigating the impact of cost ratio on the expected cost. In addition, future studies can compare the results of this study with other functional forms of the ROC curves (power, polynomial and exponential curves). Furthermore, future studies could be directed towards a single metric mathematical model that combines cost analysis with C_{ID} .

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

- [1] Cárdenas, A.A., Baras, J.S. and Seamon, K. (2006) A Framework for the Evaluation of Intrusion Detection Systems. *Proceedings of 2006 IEEE Symposium on Security and Privacy*, Berkeley, Oakland, CA, 21-24 May 2006, 15 p.
- [2] Janakiraman, S. and Vasudevan, V. (2009) Aco Based Distributed Intrusion Detection System. *JDCTA*, **3**, 66-72. <https://doi.org/10.4156/jdcta.vol3.issue1.janakiraman>
- [3] Beg, S., Naru, U., Ashraf, M. and Mohsin, S. (2010) Feasibility of Intrusion Detection System with High Performance Computing: A Survey. *International Journal for Advances in Computer Science*, **1**, 26-35.
- [4] Sasikumar, R. and Manjula, D. (2011) A Distributed Intrusion Detection System Based on Mobile Agents with Fault Tolerance. *European Journal of Scientific Research*, **62**, 48-55.
- [5] Gu, G., Fogla, P., Dagon, D., Lee, W. and Skoric, B. (2006) Measuring Intrusion Detection Capability: An Information-Theoretic Approach. *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security*, Taipei, 21-24 March 2006, 90-101.
- [6] Eid, M.A., Artail, H., Kayssi, A.I. and Chehab, A. (2008) Lamaiids: A Lightweight Adaptive Mobile Agent-Based Intrusion Detection System. *International Journal of Network Security*, **6**, 145-157.
- [7] Singh, M. and Pathak, S. (2012) Xb@nd Implementation for Intrusion Detection System. *International Journal of Engineering Research and Technology*, **1**, 1-6.
- [8] Singh, M. and Sodhi, S. (2007) Distributed Intrusion Detection Using Aglet Mobile Agent Technology. *Proceedings of National Conference on Challenges and Opportunities in Information Technology (COIT-2007) RIMT-IET*, Mandi Gobindgarh, March 2007, 148-153.
- [9] Sallay, H., AlShalfan, K.A., *et al.* (2009) A Scalable Distributed IDS Architecture for High Speed Networks. *International Journal of Computer Science and Network Security*, **9**, 9-16.
- [10] Saravanan, A., Ahmed, M.I. and Bama, S.S. (2017) A Novel Approach for Intrusion Detection System in Distributed Networks Using Mobile Agents. *Journal of Intelligent and Fuzzy Systems*, **33**, 1-11.
- [11] Gandhi, M. and Srivatsa, S. (2008) Detecting and Preventing Attacks Using Network Intrusion Detection Systems. *International Journal of Computer Science and Security*, **2**, 49-58.
- [12] Dastjerdi, A.V. and Bakar, K.A. (2008) A Novel Hybrid Mobile Agent Based Distributed Intrusion Detection System. *International Journal of Computer, Electrical,*

Automation, Control and Information Engineering, **2**, 2903-2906.

- [13] Farahnakian, F. and Heikkonen, J. (2018) A Deep Auto-Encoder Based Approach for Intrusion Detection System. *20th International Conference on Advanced Communication Technology (ICACT)*, Chuncheon, 11-14 February 2018, 178-183.
- [14] Thakar, U., Dagdee, N. and Varma, S. (2010) Pattern Analysis and Signature Extraction for Intrusion Attacks on Web Services. *International Journal of Network Security & Its Applications (IJNSA)*, **2**, 190-205.
- [15] Farhaoui, Y. and Asimi, A. (2011) Performance Method of Assessment of the Intrusion Detection and Prevention Systems. *International Journal of Engineering, Science and Technology*, **3**, 5916-5928.
- [16] Ernst, J., Hamed, T. and Kremer, S. (2018) A Survey and Comparison of Performance Evaluation in Intrusion Detection Systems. In: Daimi, K., ed., *Computer and Network Security Essentials*, Springer, Cham.
- [17] Verma, A. and Ranga, V. (2018) Statistical Analysis of Cidds-001 Dataset for Network Intrusion Detection Systems Using Distance-Based Machine Learning. *Procedia Computer Science*, **125**, 709-716. <https://doi.org/10.1016/j.procs.2017.12.091>
- [18] Popoola, E. and Adewumi, A.O. (2017) Efficient Feature Selection Technique for Network Intrusion Detection System Using Discrete Differential Evolution and Decision. *International Journal of Network Security*, **19**, 660-669.
- [19] Tape, T. (2000) Using the Receiver Operating Characteristic (Roc) Curve to Analyze a Classification Model. University of Nebraska, 1-3.
- [20] Banerjee, U. and Arya, K.V. (2013) Optimizing Operating Cost of an Intrusion Detection System. *International Journal of Communications, Network and System Sciences*, **6**, 29-36. <https://doi.org/10.4236/ijcns.2013.61004>
- [21] Spafford, E.H. and Zamboni, D. (2000) Intrusion Detection Using Autonomous Agents. *Computer Networks*, **34**, 547-570. [https://doi.org/10.1016/S1389-1286\(00\)00136-5](https://doi.org/10.1016/S1389-1286(00)00136-5)
- [22] Gaffney, J.E. and Ulvila, J.W. (2001) Evaluation of Intrusion Detectors: A Decision Theory Approach. *Proceedings 2001 IEEE Symposium on Security and Privacy, S&P2001*, 14-16 May 2000, Oakland, CA, 50-61. <https://doi.org/10.1109/SECPRI.2001.924287>
- [23] Meng, Y. (2012) Measuring Intelligent False Alarm Reduction Using an ROC Curve-Based Approach in Network Intrusion Detection. *2012 IEEE International Conference on Computational Intelligence for Measurement Systems and Applications (CIMSA)*, Tianjin, 2-4 July 2012, 108-113. <https://doi.org/10.1109/CIMSA.2012.6269608>
- [24] Almgren, M., Lundin, E. and Jonsson, B.E. (2003) Consolidation and Evaluation of Ids Taxonomies. *Proceedings of the 8th Nordic Workshop on Secure IT Systems (NordSec 2003)*, Gjøvik, 15-17 October 2003, 1-14.