Cost Analysis for Classification-based Autonomous Response Systems

Yudha Purwanto[1,2], Kuspriyanto[1], Hendrawan[1], and Budi Rahardjo[1]
(Corresponding author: Yudha Purwanto)
School of Electrical Engineering and Informatics, Bandung Institute of Technology[1]
Jl. Ganesha, Tamansari, Bandung, Indonesia
Telkom University[2]
Jl. Telekomunikasi, Dayeuhkolot, Bandung, Indonesia
(Email: omyudha@telkomuniversity.ac.id)
(Received Apr. 18, 2017; revised and accepted Aug. 23, 2017)

Abstract

Recently, cost-based Autonomous Response System (ARS) proposals are based on intrusion detection analysis. However, the implementation of the analysis in multi-class classification-based ARS potentially leads to a wrong response action set decision. This is because the analysis may produces irrelevant response value, as it is not considering the false possibility in a true positive condition. In this paper, we introduce ARS based on cost analysis from a multi-class classification output. The analysis is not only considering the possibility of a right response, but also the possibility of a wrong response from false classification prediction. The response value and expected lost rate are introduced to quantitatively estimate the best response action set. Our simulation for Denial of Service (DoS) attack cases, confirmed the capability of response action set decision algorithm. Our proposed system provides more accurate estimation of response value which leads to lower expected lost rate.

Keywords: Autonomous Response System; Classification; Decision Analysis; Denial of Service; Intrusion Detection

1 Introduction

To stop the traffic flooding attack in Denial-of-Service (DoS) is one important task in network security. Intrusion Detection and Response System (IDRS) is one security mechanism which aims to mitigate the attack impacts on a victim while keeping the damage level to a minimum [8]. Autonomous response system (ARS) is a kind of IRS, which responses to the detected attack autonomously without human intervention. The system is not only required to accurately detect the attacks, but also adaptively determines the best response action set to stop the attacks. Actions such as traceback [28], Intrusion Detection System (IDS) based filtering [12, 16], rate-limiting [13, 20], artificial immunity [1, 2], are examples of DoS attack response proposals. And in [17], the defensive mechanism was categorized by capability focus of each approach.

The heart of an ARS is the decision analysis process, as it is responsible for the decision to be made. Research on cost-based decision analysis has their own characteristics and mechanism in determining the variables. Most approaches obliged to assess every single risk and cost embroiled in decision analysis, such in [3, 6, 10]. But, the major issue of cost-based decision analysis is the necessity to estimate many building factors which have to be defined first during implementation.

To overcome above limitations, several research has proposed the decision analysis, which only directly concerns with IDS effectiveness. In [25], they have proposed decision analysis which considers damage lost and response cost consequences by no intrusion condition. These approaches have not considered the lost or cost consequences by intrusion condition. And in [15], they have modified the previous analysis of cost and lost consequences according to IDS possible conditions which are no intrusion and intrusion. The research has proposed IDS value to quantitatively measure IDS effectiveness by considering most relevant costs of the decision process. Cost analysis also used in Intrusion Detection Network research [4, 5] which used to measure the effectiveness of detection feedbacks in collaboration selection process.

However, the cost-based decision analysis for intrusion detection cannot be directly applied to the multi-class intrusion classification cases. Furthermore, it potentially leads to less precise response action set and higher lost rate. This is because the output of intrusion classification provides more action set possibilities. Thus, the decision analysis must take into account all consequences possibility, including from wrong response possibility. This is because there is still the possibility of false in every classification algorithm. From previous intrusion classification

Table 1: Example of intrusion classification output case

Actual	Classification Prediction		
	Normal	Attack A	Attack B
Normal	TN	FP A	FP B
Attack A	FN A	TP AA	TP AB

algorithm research reports; such in [18, 19, 22]; still, no classifier has a perfect accuracy. For example, in Table 1, the true positive (TP) state in intrusion classification, may consist of several specific false predictions, such as TP_{AB} (false as attack A was predicted as attack B), etc. Each false prediction will take effect on cost and lost consequences in the decision analysis. When this situation is neglected, then the lack of proper decision may be ended in higher system lost.

Therefore, we propose false-aware cost-based decision algorithm for classification-based ARS. Our decision algorithm quantitatively estimates response value of each possible set of response action, and determine best response action set based on response value. We have upgraded the state-of-the-art cost-based decision analysis in [15], by considering the possibility of right or wrong response consequences in the analysis process. Thus, it leads to estimate the relevant best response action set, as it provides more precise response value estimation on all possible responses. We have validated and tested the decision algorithm by synthetic confusion matrices and by the used of three different classification algorithms using KDD Cup 1999 DoS/DDoS revised dataset in [24].

Our decision analysis can accommodate the necessity of cost-based decision analysis for classification-based ARS. To the extent of our knowledge, this is the first research that shows false-aware cost-based decision analysis on intrusion classification. Our decision analysis provides a quantitative estimation of response value and expected lost rate based on classification output. Our proposal is important due to the recent development of ARS, which does not only detect the existence of attack but also determines relevant response action set. In addition, our paper differs from the related study by providing a complete algorithm that covers an autonomous response capability.

This paper is orderly written as follows. In Section 2, discuss the state-of-the-art of response system. In Section 3, our novel decision analysis proposal is introduced with an example of an intrusion classification case. Section 4 shows the response system design in complete framework and algorithm, and also discuss experimental and performance evaluation procedure. Finally, in Section 5, the evaluation results are shown and analyzed to validate our proposal. Section 6 summarized our conclusions and an open problem for possible further research.

2 Related Work

In respect of response system, decision analysis has already been studied in previous research. Game theory is one widely used analysis in response system. In [29], they proposed automated response based on a Stackelberg stochastic game which is a two-player game-theoretic response and recovery strategy, named response and recovery engine (RRE). The multi-objective response action selection quantitatively ranks by fuzzy logic, and the optimal action is determined from game-theoretic optimization process.

The probabilistic method also occupied in decision analysis. In [14], a probability analysis based on stochastic Petri nets, consider detection result in a network which comprised of many nodes. By adjusting a minimum threshold, a dynamic response system was developed based on the detected attacker strength. Reinforcement learning was used in [13], which proposed autonomous response by distributing reinforcement learning of throttle agents. Those agents adaptively and autonomously response DoS attack by learning the scale of rate-limiting action during reinforcement learning.

Cost-benefit analysis is one promising method in response system [15]. However, it has limitation as all of the cost must be defined first and have to be updated periodically, otherwise it will be static cost analysis. Research in [11] has proposed risk analysis by damage cost, operational cost and response cost in a cost-sensitive analysis for IDS. This proposal determines the autonomous response, according to the cumulative cost matrix that combines the different cost features. While others work in the scope of technical approach, in [6] has proposed a cost-benefit analysis which has considered the technical and managerial aspects. The analysis estimates the Return on Investment (ROI) variables in determining best IDS system which provides better ROI.

Cost-based decision analysis based on intrusion detection in [5, 15, 25, 26] have gone beyond the static cost by dynamically calculate the cost based on IDS output. In [25, 26], they have proposed decision analysis based on cost per unit lost ratio, which considers damage Lost and response Cost by no intrusion condition. Then, [15] have upgraded the decision analysis by simplifying cost-benefit estimation. It proposed IDS Value to quantitatively measure IDS effectiveness by considering most relevant costs in an ARS (Believe Desire Intention (BDI) agent environment.

Research in [5] also consider cost analysis of detection feedbacks by the used of false positive and false negative feedbacks. However, those proposals still not pay attention to the possibility of wrong response in intrusion classification output case. We develop beyond those existing cost-based decision analysis by concentrating on cost-based analysis which considers the possibility of wrong response.

3 False-Aware Cost-based Decision Analysis

Research in [5, 15, 25, 26], are fundamentally constructed our false-aware cost-based decision analysis for classification-based response system. The analysis consists of response decision nodes and event nodes. A response decision node is possible response action taken by response system at an operating point. An event node is network condition uncertainty at an operating point. From the combination of possible taken response and condition uncertainty, decision analysis may end up in consequences which are cost or lost condition. In decision analysis, the first important step is to determine the environment and workflow of the system. It significantly affects the result of decision analysis. In this proposal, the analysis is developed according to the framework such in Figure 1.

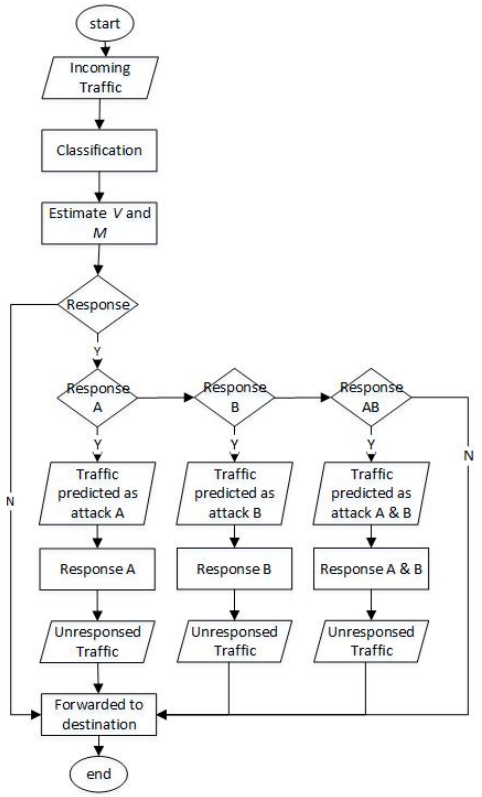

Figure 1: Traffic flow in our proposed ARS

Definition 1. *The Possible responses are all possible response actions that available for the ARS to react to any predicted attack.*

The possible responses at a given operating point are whether the system chose to respond or not respond to any predicted attack. By this situation, the possible responses are no-response and response to the predicted attacks. In classification case, the predicted attack may consist of several types of attack. Thus, the possible responses are no-response and power set of responses to predicted attacks. For example, from a classification report such in Table 1, the all possible responses are no-response, response to attack A, response to attack B, and response to both attacks A and B.

Definition 2. *Cost is a condition where the system takes any precautionary response action. The response took specific cost related to certain action set, based upon the predicted class of attack.*

Definition 3. *Lost is a condition where the system suffers any lost from the attack as system take no-response or wrong response when the attack occurred. The lost is related to damage lost from not responding to the predicted class of attack.*

We have upgraded the decision tree analysis proposed in [5, 15, 25, 26], by considering all possible consequences according to intrusion classification output. Our decision tree analysis not only considers lost consequence by the no-response decision but also lost consequence by wrong response decision. This approach is based on the real condition probability from possible responses. As system took response due to any certain type of attack, it might end up in cost consequence when the response was right, or in lost consequence as the response was wrong. From this process, we have optimized the decision tree analysis as depicted in Figure 2.

Definition 4. *The expected cost of response is the sum of product of expected consequence if the system takes any response. In intrusion detection case, the expected cost of response is related to false positive, false negative, and a true positive.*

In a cost-based decision analysis for intrusion classification, it estimates the expected cost and lost condition for each possible response. From classification output confusion matrix in Table 1, the system has information of hit rate ($H = TP/(TP + FN)$) and False alarm rate ($F = FP/(FP+TN)$). Given the prior probability of an intrusion is happening (p), the expected cost in each possible condition is then estimated by decision tree analysis in Figure 2.

Definition 5. *The expected cost of an operating point is the sum of the product of the expected cost of response from each possible condition. Thus, the expected cost per unit lost of operating point (M) is the cost of an operating point normalized by unit lost.*

The expected cost per unit lost of an operating point is dependent on the cost of an operating point in No-Alarm and in an Alarm condition. To estimate the cost per unit lost ratio (M), all cost per unit lost ratio of all possible responses need to be defined first. For example, in classification case such in Table 1, the all possible responses are summarized in Table 2. In No-Alarm condition, the cost per unit lost ratio given every possible response are

Table 2: Cost analysis based on possible responses in Table 1

Report	**Traffic**	**PossibleResponse**			
		No Response	**Response Attack A**	**Response Attack B**	**Response Attack A B**
No Alarm	Normal	0	C(TN)	C(TN)	C(TN)
	Attack A	$L(FN_A)$	$C(FN_A)$	$L(FN_A)$	$C(FN_A)$
Alarm	Normal	0	$C(FP_A)$	$C(FP_B)$	$C(FP_A + FP_B)$
	Attack A	$L(TP_{AA} + TP_{AB})$	$C(TP_{AA}) + L(TP_{AB})$	$C(TP_{AB} + L(TP_{AB} + TP_{AA})$	$L(TP_{AB}) + C(TP_{AA} + TP_{AB})$

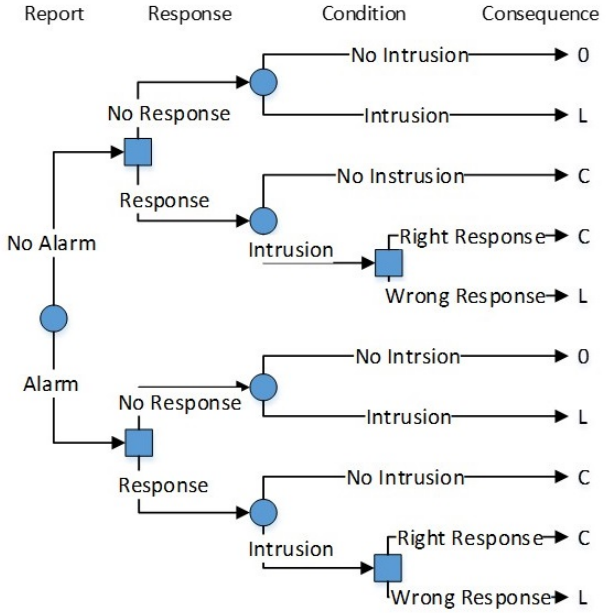

Figure 2: Cost-based decision tree for intrusion classification that considers right or wrong response

such in Equation (1) to Equation (4).

$$M(NoResponse|NoAlarm) = C_{(NoResponse|normal)} + C_{(NoResponse|Attack_A)} = p(1-H) \quad (1)$$

$$M(Response_A|NoAlarm) = C_{(Response_A|normal)} + C_{(Response_A|Attack_A)} = \frac{C}{L}((1-p)(1-F)) + \frac{C}{L}(p(1-H)) \quad (2)$$

$$M(Response_B|NoAlarm) = C_{(Response_B|normal)} + C_{(Response_B|Attack_A)} = \frac{C}{L}((1-p)(1-F)) + (p(1-H)) \quad (3)$$

$$M(Response_{A+B}|NoAlarm) = C_{Response_{(A+B)}|normal)} + C_{(Response_{(A+B)}|Attack_A)} = \frac{C}{L}((1-p)(1-F)) + \frac{C}{L}(p(1-H)) \quad (4)$$

From Equation (1) to Equation (4) system can estimates expected cost to lost ratio from No-Alarm condition which is such in Equation (5).

$$M_{NoAlarm} = min \left\{ \begin{array}{l} (p(1-H)), \\ \frac{C}{L}(((1-p)(1-F)) + (p(1-H)))), \\ ((\frac{C}{L}((1-p)(1-F))) + p(1-H)), \\ (\frac{C}{L}((1-p)(1-F)) + (p(1-H))) \end{array} \right\} \quad (5)$$

The same procedure is performed to estimate the cost per unit lost ratio in an Alarm condition. The cost per unit lost ratio is estimated as every possible response given Alarm condition, such in Equation (6) to Equation (9).

$$M(NoResponse|Alarm) = C_{(NoResponse|normal)} + C_{(NoResponse|Attack_A)} = pH(\frac{(TP_{AA} + TP_{AB})}{TP}) \quad (6)$$

$$M(Response_A|Alarm) = C_{(Response_A|normal)} + C_{(Response_A|Attack_A)} = \frac{C}{L}((1-p)F(\frac{FP_{AA}}{FP}) + pH(\frac{TP_{AA}}{TP})) + pH(\frac{TP_{AB}}{TP}) \quad (7)$$

$$M(Response_B|Alarm) = C_{(Response_B|normal)} + C_{(Response_B|Attack_A)} = \frac{C}{L}((1-p)F(\frac{FP_{BB}}{FP}) + pH(\frac{TP_{AB}}{TP})) + pH \quad (8)$$

$$M(Response_{A+B}|Alarm) = C_{(Response_{A+B}|normal)} + C_{(Response_{A+B}|Attack_A)} = \frac{C}{L}((1-p)F + pH)) + pH(\frac{TP_{AB}}{TP}) \quad (9)$$

Thus, the expected cost to lost ratio given Alarm con-

dition will be such in Equation (10).

$$M_{Alarm} = min \left\{ \begin{array}{l} pH(\frac{(TP_{AA}+TP_{AB})}{TP}), \\ \frac{C}{L}((1-p)F(\frac{FP_{AA}}{FP}) + pH(\frac{TP_{AA}}{TP})) \\ \quad +pH(\frac{TP_{AB}}{TP}), \\ \frac{C}{L}((1-p)F(\frac{FP_{BB}}{FP}) + pH(\frac{TP_{AB}}{TP})) + pH, \\ \frac{C}{L}((1-p)F + pH)) + pH(\frac{TP_{AB}}{TP}) \end{array} \right\} \quad (10)$$

Finally, the expected cost per unit lost(M) is the sum of the product of the expected cost per unit lost of detector's reports at an operation point which are No-Alarm and Alarm condition, which is $M = M_{NoAlarm} + M_{Alarm}$.

Definition 6. *The response value such in [15]; namely IDS value; is an estimated value of the possible responses at a given operating point.*

It was derived from the normalization between actual reduction of expected cost and maximum possible reduction of expected cost. Actual reduction of expected cost is the reduction of actual expected cost (M) over the expected cost which based only on the information of the probability of intrusion (M_{prop}). And maximum possible reduction is the reduction between actual expected cost per unit lost of operating point (M) over the expected cost of perfect classifier (M_{per}). M_{prop} is the expected cost that corresponds only to the information of the probability of intrusion (p), such in Equation (11). The expected cost of a perfect classifier (M_{per}) was achieved when expected cost per unit lost was applied in a perfect classifier which has $H = 1$ and $F = 0$, such in Equation (12).

$$M_{prop} = min(p, \frac{C}{L}) \quad (11)$$

$$M_{per} = min(p, \frac{C}{L}p). \quad (12)$$

The system estimates the response value (V) which is the same procedure as IDS value from [15] such in Equation (13). The difference is in response value, the system objective is to evaluate the value of every action response set. To extend the analysis, we provide the response value calculation algorithm in Section 4.

$$V = \frac{(M_{prop} - M)}{(M_{prop} - M_{per})} \quad (13)$$

Definition 7. *Best response action set (a), is the set of action determined from related to cost to lost ratio ($\frac{C}{L}$) when decision analysis reaches a maximum response value.*

For the ARS, the best response was automatically determined from minimal expected cost per unit lost. However, from this analysis, the best response is just the decision of whether to respond or not to all predicted attacks (chosen from possible responses). The actual action taken by ARS is response action set ($\{a\}$) at a determined best response. The best response action set then acquired from action set which is related to cost to lost ratio ($\frac{C}{L}$) from obtained maximum response value (V_{max}).

Definition 8. *Lost rate parameter (L) is the expected lost consequence at a given expected cost per unit lost, normalized by maximum lost consequence.*

To estimate lost rate (L), the system estimates the maximum cost consequence from confusion matrix input. It is the sum of product of true in true positive, and all False Negative. From the resulting expected cost consequence, the system can estimate expected lost consequence by a reduction between maximum lost consequence and expected cost consequence. The lost rate is then estimated by the expected lost consequence divided by the maximum lost consequence, such in Equation (14).

$$L = \frac{(TP + FN) - (\frac{M(trueTP+FN)}{M|V_{max}}}{TP + FN}. \quad (14)$$

4 System Design

4.1 Framework and Algorithm

Our proposed system may reside on any node in a network, including in near destination network as it provides more benefit in security system [22]. Figure 3 represents our framework. The input of our system is basically raw incoming traffic records, which is packet level data. The first stage of our framework is basic features generation process, which is to generate each traffic feature of each data traffic. Assumed, the output of traffic features generation process is a set of traffic features records $X = \{x_1, x_2, x_3, \ldots x_g\}$. Each data in x then enters the second stage; the classification system; to predict types of each individual data in record x. The system evaluates every classification output in confusion matrix and gets set of g confusion matrix records $Y = \{y_1, y_2, y_3, \ldots y_g\}$. Hit rate ($H$), false rate ($F$) and the probability of attack (p) are straightly calculated from each confusion matrix records y in Y. When the traffic data are predicted as normal, then the data enter the fifth stage which is traffic forwarding process. But, when the traffic data are predicted as an attack, then the system enters the third stage. At this stage, the system estimates the response value of each confusion matrix from the earlier step. The decision analysis applied to estimates a set of response value of each y; which produces $V = \{v_1, v_2, v_3, \ldots v_g\}$. In the final stage, the system determines the best responses $Z = \{z_1, z_2, z_3, \ldots z_g\}$ for every estimated response value (v). And finally determines best response action set $A = \{a_1, a_2, a_3, \ldots a_g\}$ from related cost to lost ratio ($\frac{C}{L}$) at given maximum response value.

In this research, we present the algorithm of autonomous response in Algorithm 1. The algorithm firstly determines all possible responses of given classification output (y_g), which is no-response and all subsets of the attack detected responses. Then, the system estimates the cost per unit lost value for every possible response in No-Alarm and Alarm condition. This was done by following decision-tree analysis in Figure 2. All possible

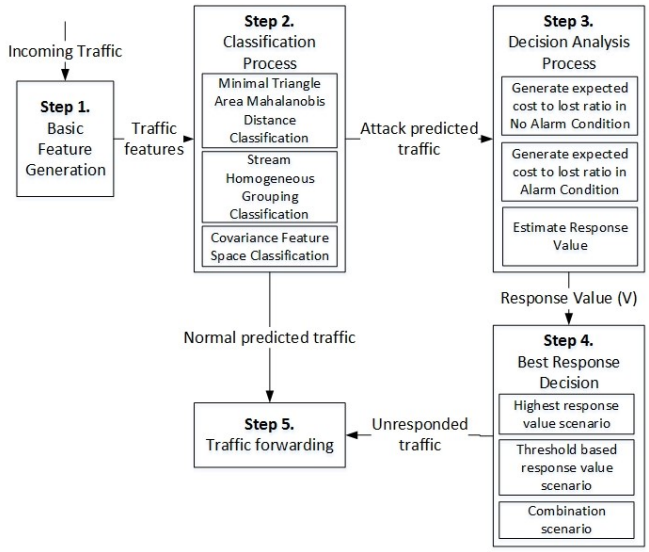

Figure 3: Framework of classification-based response system

responses are represented in a predicted set. The system then estimates the expected cost per unit lost (M_g) from the minimal value of $M_{Alarm} + M_{NoAlarm}$, for every possible action (represented by $col = \forall predicted$). From the expected cost per unit lost calculation (M_g), the system then estimates the best response (z_g), response value (v_g) using Equation (13) and best response action (a_g).

4.2 Test and Data Acquisition

In general, we evaluate our proposed ARS in two stages by doing a comparison between our decision analysis and state-of-the-art cost-based decision analysis in [15]. First is validation, using synthetic confusion matrix which best represents the possible condition of classification output. Second, we evaluate the system by the used of three different classification algorithms. We use KDDCup 99 revised dataset in [24] as input for three classification algorithm to evaluate our decision analysis. The classification was done for all DoS/DDoS data in KDDCup 99 revised, except for Pod, teardrop, and Land attack. This proposal is the extension of our previous research in the classification algorithm in [18]. First is Minimal Mahalanobis Distance Classification (MMDC) algorithm, which is our proposed classification algorithm. We have upgraded the algorithm by the used of minimal triangle area Mahalanobis distance to classify data from [22, 23]. Second is Stream Homogeneous Group Classification (SHGC) algorithm, which is our proposal in [18]. And the last is the covariance feature space classification (CFSC) algorithm in [7], which is stream group-based classification without homogeneous grouping. However, in this paper, we only present the comparison to reveal the effectiveness of false-aware decision analysis, instead of doing a comparison between detection or classification algorithms.

Algorithm 1 Response value (V) estimation

Begin
Initialize input : $ConfusionMatrixY = \{y_1, y_2, \cdots, y_g\}$; $p = \{predictedattackiny_g\}$; $q = \{actualtraffic inx_g\}$
while $y_g \neq \{\}$ **do**
  for $(\frac{C}{L})$ =0.01 to 0.99 **do**
    Calculate H, F, p
    $\{attack\} \leftarrow Powersetof\{p\}$
    $predicted \leftarrow \{normal\} \cup \{attack\}$
    $i \leftarrow size(predicted)$
    $\{traf\} \leftarrow Powersetof\{q\}$
    $actual \leftarrow \{normal\} \cup \{traf\}$
    $j \leftarrow size(actual)$
    GenerateCostTableNoAlarm
    GenerateCostTableAlarm
    for $col = 1$ to j **do**
      $CostNoAlarm_{orderX(col))} \leftarrow sum(CostTableNoAlarm_g(:, col, 1) * (\frac{C}{L}))$
      $LostNoAlarm_{(orderX(col)))} \leftarrow sum(CostTableNoAlarm_g(:, col, 2))$
      $CL_{NoAlarm(col)} \leftarrow CostNoAlarm_{orderX(col)} + CostNoAlarm_{orderX(col)}$
      $CostAlarm_{(orderX(col)))} \leftarrow sum(CostTableAlarm_g(:, col, 1) * (\frac{C}{L}))$
      $LostAlarm_{(orderX(col)))} \leftarrow sum(CostTableAlarm_g(:, col, 2))$
      $CL_{Alarm(col)} \leftarrow CostAlarm_{orderX(col)} + CostAlarm_{orderX(col)}$
    end for
    for $col = 1$ to j **do**
      $M_{(NoAlarm_{orderX(col)})} \leftarrow min(CostNoAlarm_{orderX(col)} + CostNoAlarm_{orderX(col)})$
      $z_{g(\frac{C}{L})NoAlarm} \leftarrow predicted|min(orderX(col))$
      $M_{(Alarm_{orderX(col)})} \leftarrow min(CostAlarm_{orderX(col)} + CostAlarm_{orderX(col)})$
      $z_{g(\frac{C}{L})Alarm} \leftarrow predicted|min(orderX(col))$
    end for
    $M_g \leftarrow M_{(NoAlarm_{orderX(col)})} + M_{(Alarm_{orderX(col)})}$
    $M_{Per} \leftarrow min(p, \frac{C}{L}p)$
    $M_{Prop} \leftarrow min(p, \frac{C}{L})$
    $V_{g(\frac{C}{L})} \leftarrow (M_{Prop} - M_g)/(M_{Prop} - M_{Per})$
  end for
  $z_g \leftarrow z_{g(\frac{C}{L})NoAlarm} \cup z_{g(\frac{C}{L})Alarm}$
  $v_g \leftarrow max(V_{g(\frac{C}{L})})$
  $a_g \leftarrow \exists a_g : (\frac{C}{L}|a_g) = (\frac{C}{L}|v_g)$
end while
End

5 Result and Analysis

5.1 Validation Using Synthetic Confusion Matrices

We do validation of our proposal by generating synthetic confusion matrix such in Table 3. Suppose, we have

Table 3: Synthetic confusion matrix cases

ConfMat1				
Actual	Predicted			
	Norm	Nept	Smu	Back
Norm	200	0	0	0
Nept	2	18	0	0
Smu	3	0	297	0
Back	5	0	0	395

ConfMat2				
Actual	Predicted			
	Norm	Nept	Smu	Back
Norm	192	1	2	5
Nept	0	20	0	0
Smu	0	0	299	0
Back	0	0	0	400

ConfMat3				
Actual	Predicted			
	Norm	Nept	Smu	Back
Norm	199	0	1	0
Nept	0	20	0	0
Smu	1	5	294	0
Back	0	20	0	380

ConfMat4				
Actual	Predicted			
	Norm	Nept	Smu	Back
Norm	199	0	1	0
Nept	0	20	0	0
Smu	1	5	294	0
Back	0	200	0	200

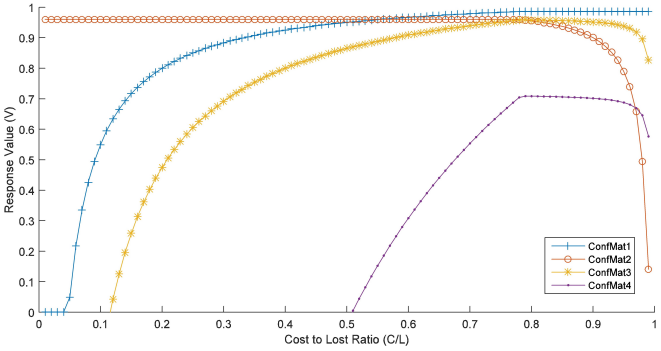

Figure 4: Response value computed over four synthetic confusion matrix cases

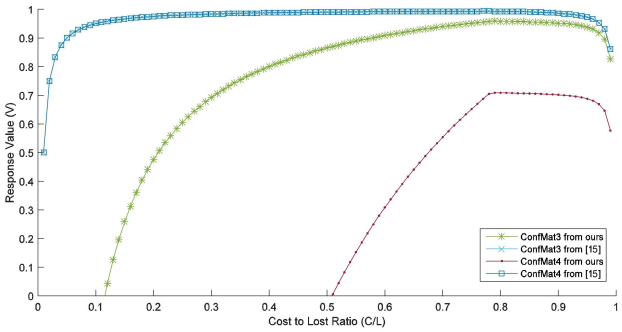

Figure 5: Response value comparison from the validation process

ConfMat1 which represents a high accuracy with some False Negative, ConfMat2 which represents a high accuracy with some false positive, ConfMat3 which represents a low accuracy with low false in true positive, and ConfMat4 which represents a low accuracy with high false in true positive. From these examples, the system determines possible responses set.

The curves of response value (V) toward the different cost to lost ratio ($\frac{C}{L}$), show the value of best response action set for given best response set which is $bestresponse = responsetoNeptuneSmurfBack$. It is obtained as the response provides minimal cost per unit lost among all possible responses set elements. Figure 4 shows that ConfMat2 is the best classification algorithm among these four. The curve from ConfMat2 shows high response value in $\frac{C}{L} < 0,56$ which means the damage cost is almost two times higher than response cost. However, when $\frac{C}{L} > 0,56$ then the best algorithm is ConfMat1, which means the system may afford the higher cost to reach a higher response value. In ConfMat2, higher false positive affects the higher cost but no lost consequences. It means when the $\frac{C}{L} > p$, the higher cost has no benefit as the lost consequence of false positive is none. Even when the cost of action gets higher, the damage lost is none. As for ConfMat1 with higher false negative, the higher cost takes effect on higher response value. It means more response need to be taken to lower the lost consequence from undetected attack in a false negative.

The used of response value in our proposal can accurately estimate the performance of ARS at the corresponding response action set. The lower response value represents the lower accuracy of classification output, which mostly influences by higher false prediction in true positive (TP). The differences are depicted in Figure 5. In the case of ConfMat3 and ConfMat4, our analysis can differentiate the quality of response estimated from classification output. The lower accuracy of ConfMat4 can be estimated by lower response value. However, the analysis in [15] can not differentiate the quality between them. Even when the accuracy of ConfMat4 is getting worse (increasing false in true positive), the IDS value remains high as long as the H, F and p values are the same. For ConfMat1 and ConfMat2 input, which have no false prediction in true positive, both decisions generate the same IDS values.

Wrong estimation of response value (V) potentially leads to poor response action set $\{a\}$. It is important as the action set is determined from the relation between estimated response value (V) and cost to lost ratio ($\frac{C}{L}$). If the response value is wrong, so does the action set determined. In this research, best response action set $\{a\}$ is determined from the maximum response value. For example, in ConfMat3 case. By the used of our proposed analysis, the best response action set was action set related to $\frac{C}{L} = 0.79$ at $V_{max} = 0.956$. By this condition, estimated best response action set is an action set $\{a_{(\frac{C}{L})} : \frac{C}{L} = 0.79\}$ and the expected cost was estimated at $M = 0.625$. Thus, the system potentially experiences a maximum unresolved attack (expected lost rate (L)) of maximum expected lost divided by maximum actual lost, which is 3,47%. However, when the system occupies decision analysis from [15], the best response value is achieved at $V = 0.956$. Then the response action set is estimated at $\{a_{(\frac{C}{L})} : \frac{C}{L} = 0.77\}$ and expected cost $M = 0.610$. Thus, it is worse than our proposal as it potentially raises maximum unresolved attack to 5.83%. The raising ex-

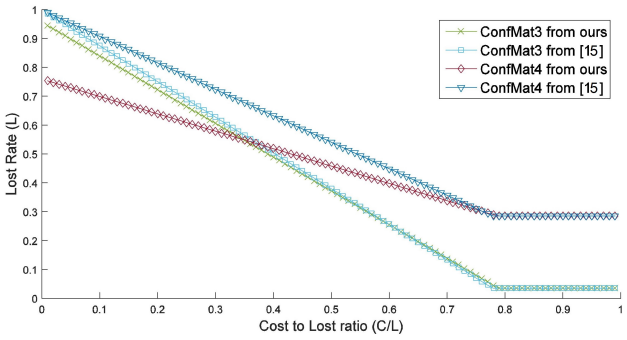

Figure 6: Lost rate exploration from the validation process

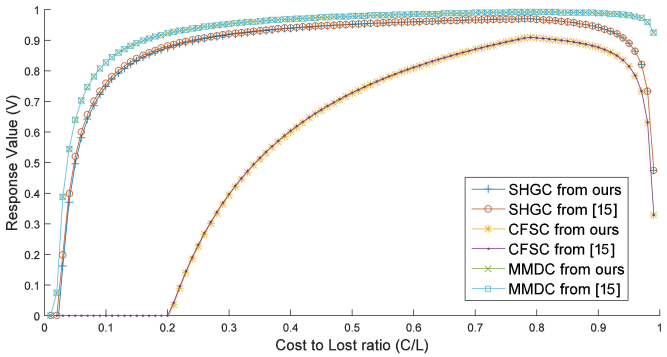

Figure 7: Response value comparison computed over KDD'99 revised dataset

pected lost rate (L) is also shown in ConfMat4 condition, which is the L increases from 28.47% to 29.72%.

From the response system point of view, the expected lost rate is expected lost when the system takes any action on estimated response value. Thus, the difference lost rates are revealed from the difference expected cost per unit lost (M) provided by both decision analysis. The expected lost rate also can be used to estimates response action set. It is used when the system has any expected toleration of lost rate. Figure 6 shows the comparison of expected lost rate(L) between our proposal and [15] for ConfMat3 and ConfMat4. The lower curves show better expected lost rate result. As for ConMat1 and ConfMat2, the lost rates are exactly the same as there are no false in the true positive in both cases.

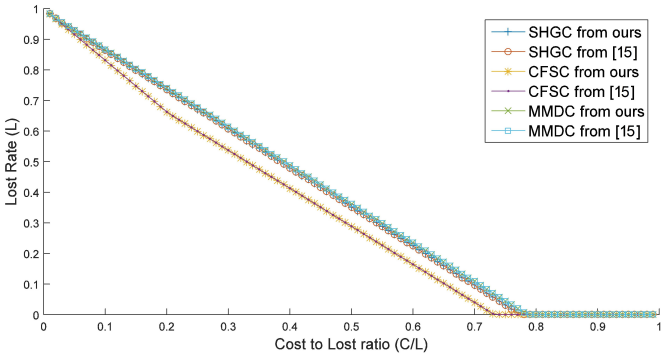

Figure 8: Lost rate exploration computed over KDD'99 revised dataset

5.2 Simulation Using Classification Algorithms

From classification outputs, the ARS autonomously decide whether to respond or not with $1 + 2^n$ possible response subsets (1 is for no-response, and n is the number of predicted attacks). From our simulation using KDD-Cup 99 revised dataset, decision analysis adaptively decides whether to respond or not according to a certain operating point. Best response from minimal expected cost per unit lost is $\{bestresponse\} = \{responsetoNeptune \cap Smurf \cap Back\}$, which is the same for all classification outputs. However, the minimal expected cost per unit lost value of each analysis and case is different. It makes the response value and best response action set are different among these three. The MMDC algorithm which is single by single data analysis provides best response value as the accuracy is relatively higher than SHGC, which is 99.48% compared to 99.05% at an SHGC group size of 50. The higher IDS value from [15] analysis does not always represent better classification accuracy, which leads to wrong response action set ($\{a\}$). The response value curves of these three algorithms are shown in Figure 7 for a group size of 50.

The expected lost rate of an SHGC algorithm at a group size of 50 is the lowest among test cases, which has a minimum expected lost rate at 0% for $\frac{C}{L} >= 0.78$. It is because when the system occupies best response action set at $\frac{C}{L} > 0.78$ then the minimum lost is only influenced by the value of false in false positive which is zero. However, as the false negative rate of MMDC is slightly higher than SHGC, then the expected lost rate is slightly higher for $\frac{C}{L} < 0.79$. And from the expected lost rate curves, it visually seems that CFSC has lower expected lost rate for $\frac{C}{L} < 0.79$. The lost rate of classification outputs is depicted in Figure 8. From all result of expected lost rate, our proposal has shown better expected lost rate in every test case. However, as the number of false in true positive is very small compared to overall data, then the lost consequence is remained unnoticed in the scale of 10^{-3}%.

In this paper, we only describe the autonomous response action set as a common process. But still, this proposal has not managed to decide which is possible response action set specified to specific cost to lost ratio ($\frac{C}{L}$). It remains an open problem in this report. This is because each response action in a set has a different response cost in a different environment. And up until now, there is still no proposal to describe the specific response action related to specific response cost to lost ratio. In [6], specified cost related to dollar cost in investment and op-

erational process are operated in a cost-based analysis. In [21], the response actions optimal strategy was identified by decision weight and decision sequence in the analytical hierarchy process. This approach has developed optimal strategy selection analysis, but still, has not mentioned the appropriate lost if the strategy was not deployed. For example, in report and alert process, it certainly takes response cost but has no effect on the targeted attack. Research in [9] has proposed a taxonomy of response actions for a specific case in a relational database. The response action set was divided into three categories which are conservative, fain-grained and aggressive. In [27], the time processing costs of request packets were analyzed by implementing DoS rate limiting process in Linux Click router.

6 Conclusions

This paper has proposed ARS based on cost-based decision analysis for multi-class DoS classification. Our cost-based decision analysis takes beneficial of classification output, which leads to related consequences of every possible response. The false-aware analysis is done by considering the possibility of wrong response in decision analysis. Our proposed system provides a quantitative calculation of response value which is used to estimate the best response action set autonomously. In low accuracy of classification output, our false-aware decision analysis provides more precise estimate of response value and expected lost rate than traditional cost-based analysis. It can accurately differentiate the classification output quality with the existence of false in true positive. Result regarding response value and expected lost rate have validated using synthetic test-case, and tested by the used of a well-establish KDD Cup 1999 DoS/DDoS attack dataset.

In this study, ARS is developed based on the classification algorithm output. Later, classification results can be exchanged between ARS and forming collaborative multi-agent system. It looks promising because, by information exchange between agents, ARSs can form collaborative ARSs that can classify, do decision analysis, evaluate, and ultimately overcome the attacks on the network. The exploration of the cost of the different response action also a part of our future research as it will beneficial for the cost-based response system.

References

[1] R. H. Dong, D. F. Wu, and Q. Y. Zhang, "The integrated artificial immune intrusion detection model based on decision-theoretic rough set," *International Journal of Network Security*, vol. 19, no. 6, pp. 880–888, 2017.

[2] Y. Farhoui, "Design and implementation of an intrusion prevention system," *International Journal of Network Security*, vol. 19, no. 5, pp. 675–683, 2017.

[3] A. Fawaz, R. Berthier, and W. H. Sanders, "A response cost model for advanced metering infrastructures," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 543–553, 2016.

[4] C. Fung and R. Boutaba, *Intrusion Detection Network: A Key to Collaborative Security*, Boca Raton, Florida: CRC Press, 2014.

[5] C. Fung and Q. Zhu, "Facid: A trust-based collaborative decision framework for intrusion detection networks," *Elsevier Ad Hoc Networks Journal*, vol. 53, pp. 17–31, 2016.

[6] C. Iheagwara, A. Blyth, and M. Singhal, "Cost effective management frameworks for intrusion detection system," *Journal of Computer Security*, vol. 12, no. 5, pp. 777–798, 2004.

[7] S. Jin, D. S. Yeung, and X. Wang, "Network intrusion detection in covariance feature space," *Pattern Recognition*, vol. 40, no. 8, pp. 2185–2197, 2007.

[8] P. Kabiri and A. A. Ghorbani, "Research on intrusion detection and response: A survey," *International Journal of Network Security*, vol. 1, no. 2, pp. 84–102, 2005.

[9] A. Kamra and E. Bertino, "Design and implementation of an intrusion response system for relational databases," *IEEE Transactions on Knowledge and Data Engineering*, vol. 23, no. 6, pp. 875–888, 2011.

[10] Y. B. Leau and S. Manickam, "A cost-sensitive entropy-based network security situation assessment model," *Advanced Science Letters*, vol. 22, no. 10, pp. 2865–2870, 2016.

[11] W. Lee, W. Fan, M. Miller, S. Stolfo, and E. Zadok, "Toward cost-sensitive modeling for intrusion detection and response," *Journal of Computer Security*, vol. 10, no. 1, pp. 5–22, 2002.

[12] Z. Ling, J. Luo, K. Wu, W. Yu, and X. Fu, "Torward : Discovery, blocking, and traceback of malicious traffic over tor," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2515–2530, 2015.

[13] K. Malialis, S. Devlin, and D. Kudenko, "Distributed reinforcement learning for adaptive and robust network intrusion response," *Connection Science*, vol. 27, no. 3, pp. 234–252, 2015.

[14] R. Mitchell and I.-R. Chen, "Effect of intrusion detection and response on reliability of cyber physical systems," *IEEE Transactions on Reliability*, vol. 62, no. 1, pp. 199–210, 2013.

[15] A. Orfila, J. Carbo, and A. Ribagorda, "Autonomous decision on intrusion detection with trained BDI agents," *Computer Communications*, vol. 31, pp. 1803–1813, 2008.

[16] E. Popoola, A. O. Adewumi, "Efficient feature selection technique for network intrusion detection system using discrete differential evolution and decision," *International Journal of Network Security*, vol. 19, no. 5, pp. 660–669, 2017.

[17] Y. Purwanto, Kuspriyanto, Hendrawan, and B. Rahardjo, "Traffic anomaly detection in DDoS flood-

ing attack," in *Proceeding of 8th International Conference on Telecommunication Systems Services and Applications (TSSA'14)*, pp. 1–6, Oct. 2014.

[18] Y. Purwanto, Kuspriyanto, Hendrawan, and B. Rahardjo, "Multistage process to decrease processing time in intrusion prevention system," in *Proceeding of 3rd International Conference on Wireless and Telematics*, Palembang, Indonesia, July 2017.

[19] Q. S. Qassim, A. M. Zin, and M. J. A. Aziz, "Anomalies classification approach for network-based intrusion detection system," *International Journal of Network Security*, vol. 18, no. 6, pp. 1159–1172, 2016.

[20] V. M. Shah, A. K. Agarwal, "Reliable alert fusion of multiple intrusion detection systems," *International Journal of Network Security*, vol. 19, no. 2, pp. 182–192, 2017.

[21] M. Sun and Y. Guo, "The research on enhanced cost-based auto intrusion response decision," in *Proceeding of International Conference on Wireless Communications*, pp. 4550–4553, Sept. 2009.

[22] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "A system for denial of service attack detection based on multivariate correlation analysis," *IEEE Transaction on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 447–456, 2013.

[23] C. F. Tsai and C. Y. Lin, "A triangle area based nearest neighbors approach to intrusion detection," *Pattern Recognition*, vol. 43, pp. 222–229, 2010.

[24] UCI KDD, *KDD Cup 1999 Data*, Information and Computer Science University of California, Irvine, Oct. 28, 1999. (`http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html`)

[25] J. W. Ulvila and J. John E. Gaffney, "A decision analysis method for evaluating computer intrusion detection systems," *Decision Analysis*, vol. 1, no. 1, pp. 35–50, 2004.

[26] J. W. Ulvila and J. John E. Gaffney, "Evaluation of intrusion detection systems," *Journal of Research of NIST*, vol. 108, no. 6, pp. 453–473, 2003.

[27] X. Yang, D. Wetherall, and T. Anderson, "Tva : A dos-limiting network architecture," *IEEE/ACM Transactions on Networking*, vol. 16, no. 6, pp. 1267–1280, 2008.

[28] G. Yao, J. Bi, and A. V. Vasilakos, "Passive ip traceback: Disclosing the locations of ip spoofers from path backscatter," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 471–484, 2015.

[29] S. A. Zonouz, H. Khurana, W. H. Sanders, and T. M. Yardley, "Rre : A game-theoretic intrusion response and recovery engine," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 395–406, 2014.

Biography

Yudha Purwanto completed his undergraduate degree at STTTelkom, Bandung and master degree at Electrical Engineering, Institut Teknologi Bandung. He currently work as a lecturer at Telkom University in Bandung. His research interests is security system esspecially in network security and cryptography.

Kuspriyanto completed his undergraduate degree at Electrical Engineering, Institut Teknologi Bandung in 1974. He received his Master and Doctoral degree from Universit des Sciences et Techniques de Montpellier (USTL) France. He is currently a Full Professor at the Department of Electrical Engineering, Institut Teknologi Bandung, Indonesia. His current research interests include real time computing systems, computer architecture, and robotics. Contact at kuspriyanto@lskk.ee.itb.ac.id.

Hendrawan is an Associate Professor in School of Electrical Engineering and Informatics, Institut Teknologi Bandung, Indonesia. He completed undergraduate degree at Electrical Engineering, Institut Teknologi Bandung, Master and Doctoral degree in Telecommunications and Information Systems from University of Essex, UK. Contact at hend@stei.itb.ac.id.

Budi Rahardjo completed undergraduate degree at Electrical Engineering, Institut Teknologi Bandung. And received his Master and Doctoral degree from Manitoba University, Canada. His current research interests include network security, forensic and cryptography. Contact at rahard@lskk.itb.ac.id.