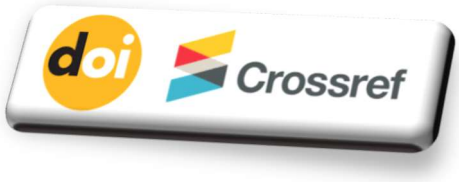
Journal, Advances in Mathematical & Computational Sciences
Vol. 10 No. 3, September, 2022
www.isteams.net/mathematics-computationaljournal



Journal of Advances in Mathematical & Computational Sciences
An International Pan-African Multidisciplinary Journal of the SMART Research Group
International Centre for IT & Development (ICITD) USA

Available online at https://www.isteams.net/ mathematics-computationaljournal.info
CrossREF Member Listing - https://www.crossref.org/06members/50go-live.html

A Strategic Review of Existing Cost-Sensitive Intrusion Response System

Ikuomola, A.J.
Department of Computer Science,
Olusegun Agagu University of Science and Technology
Okitipupa, Nigeria
E-mails: aj.ikuomola@oaustech.edu.ng; deroniknng@yahoo.com,

ABSTRACT

In the process of detecting an attack, it is necessary to take corrective action to tackle the attack and ensure safety of the system. The process of counter-measuring these attacks is referred to as intrusion response. In recent years, the trend toward modeling of cost-sensitive response system has become more important. The main goal of cost-sensitive response system is to strike a balance between damages made by the intrusion and the cost of response. This paper strategically reviews the existing cost-sensitive intrusion response system focusing on the approach, architecture, strength and limitation.

Keywords: Cost-Sensitive, Intrusion, Detection, Response

Ikuomola, A.J. (2022): A Strategic Review of Existing Cost-Sensitive Intrusion Response System. Journal of Advances in Mathematical & Computational Science. Vol. 10, No. 3. Pp 61-74. Available online at www.isteams.net/mathematics-computationaljournal.

1. INTRODUCTION

The amount of financial losses resulting from cyber-attacks has grown tremendously over the years. The constant increase of attacks or intrusions against networks and their resources inspire a necessity to protect these valuable assets. In the process of detecting an attack, it is necessary to take corrective action to tackle the attack and ensure safety of the system. The process of counter-measuring these attacks is referred to as intrusion response (Stakhanova et al., 2007). Intrusion Response Systems (IRS) continuously monitor system health based on intrusion detection system alerts so that malicious or unauthorized activities can be handled effectively by applying appropriate countermeasures to prevent problems from worsening and return the system to a healthy mode (Shameli-Sendi et al., 2012). The problem of IRS is that when the responses are deployed against a detected intrusion, they often alter the state of the system negatively, affecting resources and leading to damage.

An IRS needs to be cost-effective such that the cost of deploying the response action must be less than the cost of the effect of the intrusions. In recent years, the trend toward modeling of Cost-Sensitive response system has become more important. The main goal of cost-sensitive response system is to strike a balance between damages made by the intrusion and the cost of response. However, defining an accurate measurement of these cost factors and ensuring consistent evaluation across various computing environments are common challenges in using a cost-sensitive approach.

2. REVIEW OF RELATED WORK ON COST-SENSITIVE INTRUSION RESPONSE SYSTEMS

Compared to automated response in general, the area of response cost assessment has received considerably less attention. A number of significant contributions in this area had being witnessed in the past decade.

2.1 Lee's Intrusion Response System (Lee's IRS) by *Lee et al.* (2002)

Approach

The authors directly addressed the cost of deploying responses. The work introduced a cost-benefit measure which incorporates multiple dimensions of cost in the face of an intrusion: the response cost, damage cost and operational cost. The authors introduced the idea of considering responses with respect to the specific intrusion context, using intrusion taxonomy to address unknown intrusions.

Design

Three cost factors were identified: operational cost that includes the cost of processing and analyzing data for detecting intrusion; damage cost that assesses the amount of damage that could potentially be caused by attack and response cost that characterizes the operational cost of reaction to intrusion. These factors present the foundation of intrusion detection and consequently provide the basis for selection of an appropriate response.

Strength

(i) The model attempts to balance intrusion damage and response cost.

Limitations

(i) It relates the response cost to the required labour effort only.
(ii) This model is easily affected by false positive alerts which lead to false response decision.

2.2 Network Intrusion Response System (Network IRS) by Toth and Kruegal (2002)

Approach

The authors addressed the problem of response to network intrusions by constructing dependency trees that model configuration of the network and then give an outline of a cost model for estimating the effect of a response. The response cost is considered in association with the system resources. It is calculated as a function of system capability reduction. The capability c(r) reflects the overall ability of a resource (r)to fulfill its function/duty, whereas the penalty is an abstract measure of loss when a resource (r) is no longer available. The penalty costs p(r) need to be re-computed after c(r) was updated according to the proposed depth-first-search (DFS) based update algorithm discussed in their paper:

$$p(r) := (1 - c(r)) * \text{penalty} \quad (1)$$

The overall penalty p is the sum of all penalty costs. The response action with the smallest value of p is chosen for deployment.

Design

The proposed algorithm for optimal response selection takes into account the penalty cost of a resource being unavailable and the capability of a resource that indicates the resource performance if the specified response strategy is triggered, compared to the situation when all resources are available. Clearly, the set of responses with the least negative impact on the system (lowest penalty cost) is chosen to be applied in response to the detected intrusion.

Strengths

(i) It is a network model that allows an IRS to evaluate the effect of a response on the network services.
(ii) In spite of requiring complex evaluations of the graph structure, the performance results are very fast using optimized data structures for locally optimal responses.

Limitations

(i) The primary weaknesses of this approach are the complexity involved in establishing the dependency graph and the course granularity of the resource model (only availability is taken into account, ignoring potential effects on integrity and confidentiality).
(ii) The model is system dependent. The approach focuses on network of systems. They are designed to reflect characteristics of the considered system. This significantly limits the applicability of the models to varying system constraints and thus, their practicality (i.e. it cannot be deployed in different environmental setting)
(iii) The approach uses the concept of response benefit or effectiveness as a factor related to the response's ability to mitigate the intrusion damage, the operational cost of the response as well as its potential negative impact on the system are not considered.
(iv) Accurate measurement of the cost and negative effect is one of the challenges in using this model.

2.3 Specification-based Intrusion Response System (Specification-based IRS) by Balepin *et al.* (2003)

Approach

The authors proposed the costs of priority resources as base metric for response choice. In their system map, only priority nodes – representing the important system resources –have a cost value of their own. Cost values are assigned to other nodes based on the fact that priority nodes depend on them. The cost values are set by the network security officer on creation of the system map. Subsequently, the following values are computed: intrusion damage (sum of all cost values of the affected nodes), response benefit (sum of all cost values of the nodes that are restored to safe state by the response) and response costs (sum of all cost values of the nodes that are negatively affected by the response).

Design
In this system, local resource hierarchy is represented by a directed graph. Nodes of the graph are specific system resources and graph edges represent dependencies between them. Each node is associated with a list of response actions that can be applied to restore working state of resource intrusion and in case of an attack. A particular response for a node is selected based on the cost of the response action (sum of the resources that will be affected by the response action), the benefit of the response (sum of the nodes previously affected but restored to working state) and the cost of the node or resource.

Strength
(i) The map has only a few static and dynamic nodes that are critical to the system's operation. They are not updated periodically; rather, they are updated when significant event happens. Therefore, if the system runs for a long time without getting attacked, the map will not be updated (minimize the overhead).

Limitation
(i) The process of cost assignment is completely manual and the cost assignment method is only an approximation of the real resource cost.
(ii) The construction of the map itself and analysis of node dependencies are done manually.
(iii) It considers response cost in terms of system resources. It measures response cost as the sum of manually assigned cost of affected resources.
(iv) It is specifically designed to reflect characteristics of the considered system (i.e. host-based). It is not adaptable to different environment settings.

2.4 Adaptive Intrusion Tolerant System (ADEPTS) by Foo *et al.* (2005, 2007)
Approach
A proactive approach to response deployment is applied. The mechanism maps alarms provided by the IDS to Intrusion-Graph (I-Graph) nodes and then estimates the likelihood of the attack based on the alarm confidence values. Finally, appropriate response actions are deployed targeting identified attack goals

Design
The framework for determining automated responses against attacks was proposed based on two types of graphs: a Service Graph (S-Graph) that expresses inter-dependencies between available services and an attack or I-Graph that represents possible attack states and their probabilities. While the S-Graph is used only during the initial creation of the I-Graph, the I-Graph itself is used for selection of possible response deployment points (the I-Graph that is, graphs of intrusion goals, determine the spread of the intrusion and the appropriate response). The responses are selected based on the effectiveness of the response, the disruptiveness of the response to legitimate users and the confidence level that indicates the probability that a real intrusion is taking place.

Strength
(i) ADEPTS supports automatic update of the response effectiveness metric.

Limitations

(i) The model is system dependent. The approach focuses on networks of systems. ADEPTS is specifically designed to reflect the characteristics of the considered system. This significantly limits the applicability of the model to varying system constraints (i.e. it is not adaptable to different environment settings).
(ii) The approach uses the concept of response benefit or effectiveness as a factor related to the response's ability to mitigate the intrusion damage, the operational cost of the response is not considered.
(iii) ADEPTS approach relies on semi-manual development of I-Graph to determine the spread of network attacks.
(iv) The graph is static and acts as auxiliary information used in conjunction to the actual IDS. If the computing environment changes, the I-Graph needs to be updated accordingly using expert guidance.

2.5 User-Centric Metric for Denial-of-Service Measurement by Mirkovic *et al.* (2006, 2007)

Approach

Two recent papers from the authors proposed a relatively pragmatic way of defining metrics and characterizing Denial-of-Servise (DoS) effects on the user of a network. The authors suggested that these metrics can also be used for selecting appropriate response measures; though no specific implementation details are given. However, they present a lot of practical measurement results and also discuss ways of implementing measurement methods for simulation environments.

Design

The main metric used for evaluation of DoS impact is the percentage of failed transactions (pft), within a conversation. A conversation is defined as the set of all network packets exchanged between a client and a server with a goal of providing a specific service to the client, at a given time. A transaction is defined as the part of a conversation that represents a task, whose completion is meaningful to a user, such as browsing to the next link of a website.

A transaction can fail due to the exceeding of the predefined thresholds of one or more of its parameters, such as:
(i) One-Way Delay (e.g. for chat, multimedia traffic, games),
(ii) Request-Response-Delay (e.g. for email, web, ftp),
(iii) Packet Loss and Jitter (e.g. for multimedia traffic).

Using the information about the transactions, different representations are derived from providing further information, such as *pft*-histogram, an abstract level for the service degradation

$DoSLevel = \sum_k pft(k) \bullet w_k$ or the severity of the attack (where k goes over all application categories, and w_k is a weight associated with a category k), given by *QoSDegrade* = (*d*−*t*)/*t* , where *d* is the value of the parameter that exceeded its threshold value *t*.

Strength

(i) The metric defines a threshold-based model to capture the quality of service expectation of the end-user and the pft metric captures the impact of the attack as experienced by the end-user.

Limitation

(i) Although Mirkovic's paper does not focus on selecting response measures, the authors proposed to compare the DoS measurement results before and after deployment of a response in order to determine its value.

2.6 Cost-Sensitive Model for Preemptive Intrusion Response System by Stakhanova *et al.* (2007a)

Approach

The authors approach uses a very simple Response Cost (RC) and Damage Cost (DC) metrics that reflects the effect of either the response or the attack on the system and has to be set up by the network security officer and updated over time. As in other approaches, a high level of expertise is needed to set those metrics to suitable values. For a first response step, the set of applicable measures is selected. This is the set of response for which the following condition holds:

DC *Confidence Level > RC (2)

Where
the Confidence Level is the probability that the attack, the DC belongs, is actually taking place.

In a second step, the most appropriate element of the applicable measure or set is chosen,based on two metrics, namely the Success Factor (SF) and the Risk Factor (RF). The former is the percentage of times that the response succeeded in the past; whereas, the latter represents the negative impact that the response has on the system and legitimate users. Intuitively, the response providing a maximum benefit at the lowest risk is chosen. This is done by choosing response (rs) with the maximum Expected Value (EV(rs)) for the given attack sequence S, given by

EV (rs) = (Prsucc(S) *SF) + (Prrisk (S) * (−RF)) (3)

Prsucc(S) is the probability that attack-sequence S occurs and Prrisk (S) = 1−Prsucc(S) (4)

The Success Factor is adaptive; it is increased by one if the response succeeds in stopping an attack and it is decreased by one if it fails. Thus, this approach also takes the benefit and risk of a response into account for selection of responses.

Strengths

(i) The graphical structure records the attack patterns and it is an integral constituent of the IDS. This structure can be dynamically and automatically updated with the introduction or classification of new attacks.

(ii) The response selection and deployment are performed automatically without any user's intervention. Consequently, this allows fast containment of the intrusion and thus makes system defense more effective

Limitation

(i) The model considers only response measure at the expense of response time in decision making process.

2.7 Cost-Sensitive Assessment of Intrusion Response System by Strasburg *et al.* (2009)

Approach

The authors introduce a set of measures which characterize the potential cost associated with the intrusion handling process and proposed a method for evaluating intrusion response with respect to potential intrusion damage, response effectiveness and response cost for a system.

Evaluation of the response actions effectiveness in the context of a specific intrusion requires analysis of several factors such as likelihood and severity of intrusion; the extent of the potential intrusion damage; the effectiveness of suitable response actions; response cost for the system, among others. These factors are associated with intrusion damage and factors describing response cost.

Strengths

(i) The propose model is adaptable to different environment setting

(ii) It provides a more complete cost assessment of the attack handling process, considering not only direct damage caused by the intrusion but also direct costs that often remain hidden.

Limitations

(i) The model is easily affected by false positive alert, which leads to false response decisions.

(ii) The model considers only response measure but no response time in decision making process.

2.8 New Genetic Algorithm Approach for Intrusion Response System (NGAA-IRS) by Fessi *et al.* 2009

Approach

This approach is characterized by a new data encoding based on a binary matrix of response-resource entries for individual definition and by a cost benefit model that assesses the fitness of each individual, by considering the costs of the related resources and responses.

Design

The algorithm starts by creating a parent (initial) population randomly. Then it applies the reproduction operators to diversify the population and to widen the exploration space. A natural selection operator is applied, after that, to evaluate the population and select the survival individuals for the next generation. Finally, the appropriate solution is selected according to the highest fitness value.

Strengths

(i) The main strength of the approach is in using a different individual structure, comparing to existing models, based on an arbitrary matrix of binary response resource.

(ii) The structure is efficient to determine the most suitable set of actions to respond to the detected intrusions.

(iii) Large scale of the search space is explored; as infeasible solutions are discarded only in the last stage of the genetic algorithm (natural selection).

Limitation

(i) The system is easily affected by false positive alert, which lead to false response decision

2..9 Cross-Layer Intrusion Detection and Response (XIDR) by Svecs *et al.* (2010)

Approach

The cross-layer approach is used to detect signature-based and anomaly-based attacks. Multiple detection sources are used for different layers and the sources that inspect network layer properties of incoming packets could flag particular packets if they originate from known but untrusted internet protocol address ranges. This information could later be used by application-layer sources to issue alerts with greater confidence. Also, a cross-layer approach will help stop attacks by deploying a response at all necessary layers, with a minimal total cost across layers.

Design

The basic components include multiple intrusion detection sources, data sources, automated response selection engine and a collection of response deployment modules. The model uses two data stores for short (active alert database) and long term (oracle) information storage. The response selection engine is layer-agnostic, as all intrusions and responses reside in a flat space. The operational cost metric of each response is used to indicate the severity of a response. After the appropriate response is selected by the engine, a response deployment module that consists of custom scripts and runs as a service on each protected host is invoked. Figure 1 shows the architecture of an XIDR

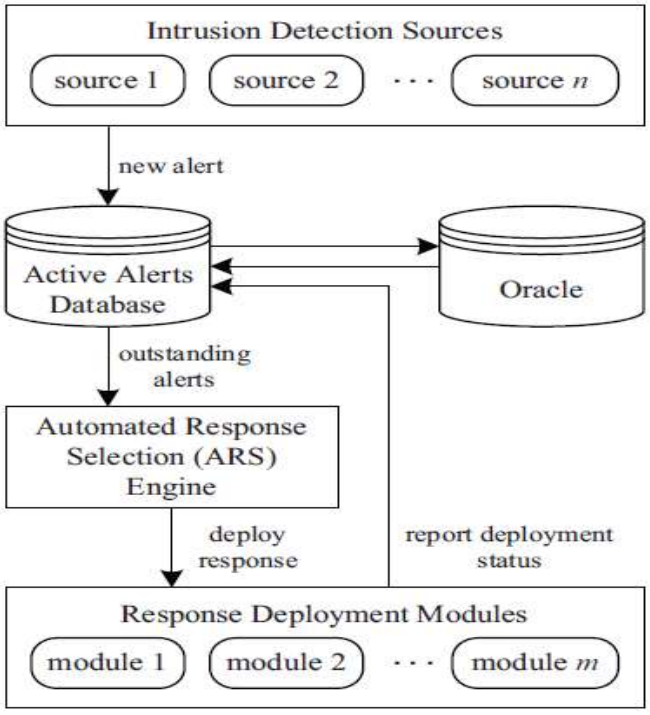


Figure 1: Architecture of Cross-Layer Intrusion Detection and Response (Svecs *et al.,* 2010)

Strength

(i) XIDR consists of multiple intrusion detection sources to utilize cross-layer based detection in a wired environment and deploy a response across various layers using a cost-sensitive response selection mechanism to minimize the cost of intrusion.

Limitation

(i) The operation cost is considered to be the intrusion response impact on the system

2.10 Improved Cost-Sensitive Model of Intrusion Response System Based on Clustering by Zhou and Yao (2012)

Approach

The authors introduced an integrated intrusion response model in the Automatic IRS (AIRS). This model adopts the multidimensional classification model of intrusion events, and applies the clustering model formula in order to reduce the unnecessary loss.

Design

As shown in Figure 2, IDS monitors the network. If an intrusion event is detected, IDS writes it to the log and submits it to the decision-making system. Through cluster analysis, it can be checked if it is a repeat alarm. If it gets together in any one cluster, then it will be considered as a repeat alarm. In the event that it is not a repeat alarm, the Damage Cost (DCost) is compare with its Response Cost (RCost). If RCost is not smaller than DCost, the event is recorded without any response; but if not, a corresponding strategy is carried out to protect the system.

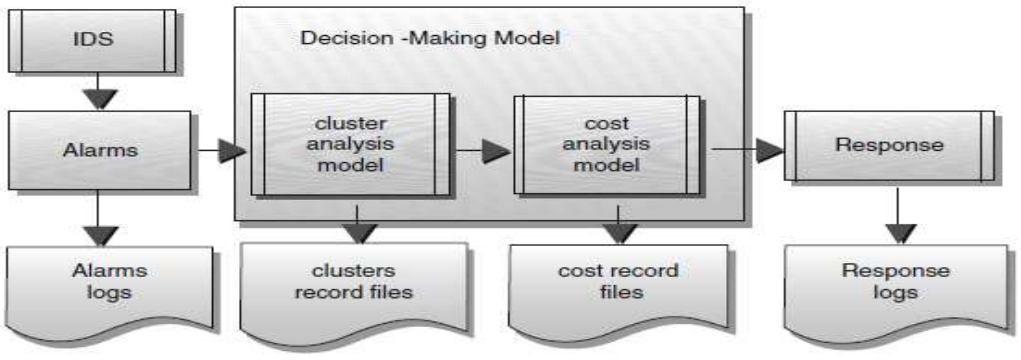


Figure 2: The Frame of Improved Automatic Intrusion Response System (Zhou and Yao, 2012)

Strength

(i) Through clustering of the intrusion events, the repeated intrusions were classified.

Limitations

(i) The cost analysis method is not accurate enough (Zhou and Yao, 2012).

(ii) The increasing number of sophisticated attacks and their costs cannot be defined primitively.

2.11 Cost Minimization Model for an Adaptive Intrusion Response System by Enikuomehin *et al.* (2012)

Approach

The authors investigated the intrusion detection process, its technical cost implication, and its divergent nature and further proposed a system that is platform independent for an appropriate impact sensitive IRS with an embedded database.

Design

When IDS detect an intrusion, it sends the information about detected intrusion as input into the response logic manager where it is analyzed and sent to the alert manager, the alert manager sounds a warning alert and invokes a response immediately. Figure 3 shows the cost minimization model for an adaptive IRS.

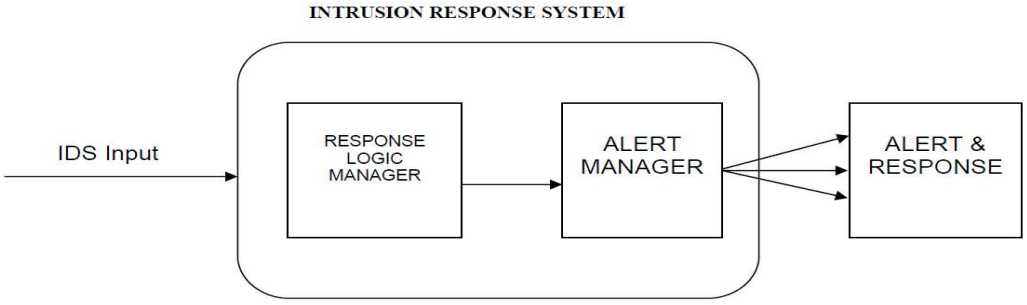


Figure 3: Cost Minimization Model for an Adaptive Intrusion Response System (Enikuomehin *et al.,* 2012)

Strength

(i) The system can be deployed over a network or on a standalone system

Limitations

(i) The cost of response was not actually evaluated
(ii) The false positive and false negative rate of the attack were not considered

2.12 Toward Cost-Sensitive Assessment of Intrusion Response Selection (CRS) by Stakhanova *et al.* (2012)

Approach

The authors' presented a framework for the cost-sensitive assessment of intrusion response. They introduce a set of measurements to characterize potential costs associated with the intrusion handling process in terms of the risk of potential intrusion damage, effectiveness of response action and response cost for a system. They developed a model to assess these factors with respect to the resources of the affected system, and selected the optimal response. Their model takes into account the relative importance of system resources determined through system policy goals, according to three main security facets: confidentiality, availability and integrity.

Strength

(i)The response metrics are quantified with respect to the security policies and properties of the specific system.

Limitations

(i) Large amount of manual input (parameters) required by the system
(ii) The false positive and false negative rate of the attack were not treated

2.13 An Improved Cost-Sensitive Intrusion Response Model by Ikuomola et al. (2012, 2013)

Approach

The authors' proposed a model called COSIRS for evaluating intrusion damage and response cost and which was able to automatically choose the least costly response in time to minimize the damage caused by an attack. The proposed model identifies three main factors that constitute response cost, namely the cost of damage caused by the intrusion, the cost of manual or automatic response to an intrusion and the operational cost. These response metrics provide a consistent basis for assessing response across systems while allowing the response cost to adapt to system environment. The adaptability of the response is based on the effectiveness of the previous response action and feedback received.

Design

The architecture of COSIRS comprises of six components namely; alert filter and correlation module, response manager, database, cost-sensitivity evaluation module, adaptability module and response-deployment module. Principal Component Analysis was employed to reduce the dimension of alerts raised by the intrusion detection system. A Neural Network-based classifier scheme that distinguishes among true positive, false positive and false negative alerts was deployed to enable COSIRS learn from its previous behaviour. COSIRS combines the response efficiency and response cost in its inference engine for deploying cost-sensitive responses based on the inherent cost parameters (cost of damage, cost of automatic response and operational cost).

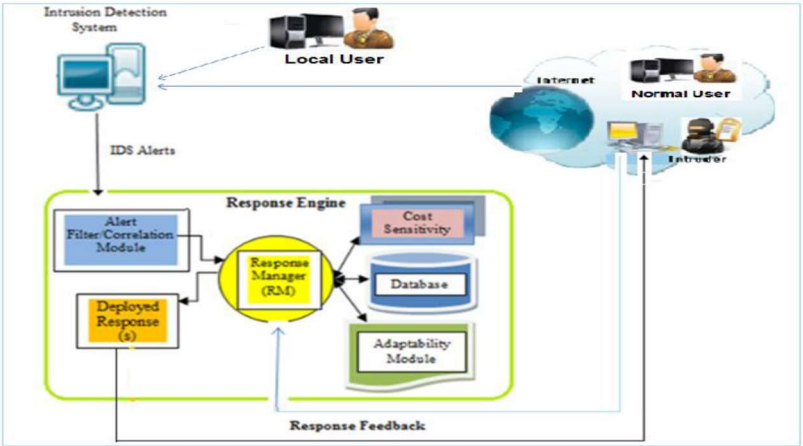


Fig 4: Architecture of a Cost-Sensitive Intrusion Response System (COSIRS)

Strength

(i) The work shows how to define a standardized metric for response cost evaluation.
(ii) It presents an improved response model that is adaptable to different operational environments.
(iii) The design provides an efficient methodology for solving identified and known problems of false negative and false positive intrusion.

Limitation

(i) More computational intelligent method need to be adopted.

2.3 Summary of the Cost-Sensitive Intrusion Response System

About 12 previous works on Cost-Sensitive IRS have been reviewed in this work. The summary of the reviewed Cost-Sensitive IRS is shown in Table 1.

Table 1: Summary of Reviewed Cost-Sensitive Intrusion Response Systems

IRS	Name of Author(s)	Year Published	Response Selection	Response Time	Adjustment Ability	Cooperation Ability
Lee's Intrusion Response System	Lee *et al.*	2002	Cost-sensitive	Delayed	Static	autonomous
Network Intrusion Response System	Toth T. and Kruegel C.	2002	Cost-sensitive	not defined	Static	Cooperative
Specification-Based Intrusion Response System	Balepin *et al.*	2003	Cost-sensitive	Delayed	Static	Autonomous
Adaptive Intrusion Tolerant System	Foo *et al.*	2005, 2007	Cost-sensitive	Proactive	Adaptive	Autonomous
User-Centric Metric for Denial-of-Service Measurement	Mirkovic *et al.*	2006, 2007	Cost-sensitive	Proactive	Not defined	Not defined
Cost-Sensitive Model for Preemptive Intrusion Resonse System	Stakhanova *et al.*	2007	Cost-sensitive	Proactive	Adaptive	Cooperative
Cost-Sensitive Assessment of Intrusion Response System	Strasburg *et al.*	2009	Cost-sensitive	Proactive	Adaptive	Autonomous
New Genetic Algorithm Approach for Intrusion Response System	Fessi *et al.*	2009	Cost-sensitive	Not defined	Adaptive	Not defined
Cross-Layer Intrusion Detection and Response	Svecs *et al.*	2010	Cost-sensitive	Proactive	Adaptive	Cooperative

IRS	Name of Author(s)	Year Published	Response Selection	Response Time	Adjustment Ability	Cooperation Ability
Improved Cost-Sensitive Model of Intrusion Response System Based on Clustering	Zhouand Yao	2012	Cost-sensitive	Proactive	Not defined	Autonomous
Cost Minimization Model for an Adaptive Intrusion Response System	Enikuomehin *et al.*	2012	Cost-sensitive	Active	Adaptive	Not defined
Toward Cost-Sensitive Assessment of Intrusion Response Selection	Stakhanova *et al.*	2012	Cost-sensitive	Not defined	Adaptive	Not defined
An Improved Cost-Sensitive Intrusion Response Model	Ikuomola et al.	2012, 2013	Cost-sensitive	Proactive	Adaptive	Not defined

3. CONCLUSION

In this paper, some existing cost-sensitive intrusion response systems have been critically reviewed. It is noted that some of these existing cost-sensitive intrusion response systems are still faced with drawbacks/limitations.

REFERENCES

1. Balepin, I., Maltsev, S., Rowe, J. and Levitt K., 2003. Using specification-based intrusion detection for automated response. *In Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection,*2820(2003), 136-154.
2. Enikuomehin A. T., Idowu A. G., Akerele C. B., Owate A. P. and Aina B. A., 2012. Cost minimization model for an adaptive intrusion response system. *Indian Journal of Computer Science and Engineering (IJCSE), 3(2).*
3. Fessi, B. A., BenAbdallah, S., Hamdi, M. and Boudriga, N., 2009. A new genetic algorithm approach for intrusion response system in computer networks. *Computers and Communications, 342-347.*
4. Foo, B., Wu, Y.S., Mao, Y.C., Bagchi, S. and Spafford, E. H., 2005. ADEPTS: Adaptive intrusion response using attack graphs in an e-commerce environment. *In Proceedings of the 2005 International Conference on Dependable Systems and Networks, 508–517.*
5. Foo, B., Wu, Y., Mao, Y, Bagchi, S. and Spafford, E. 2007. Automated adaptive intrusion containment in systems of interacting services. *Computer Networks 51(5):1334–1360.*

6. Ikuomola A. J. and Sodiya A. S. (2012).*A Credible Cost-Sensitive Model For Intrusion Response Selection, 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN), IEEE, 222-227*
7. Ikuomola A. J., Sodiya A. S., Akinwale A. T. and Aborisade D. O. (2013). *An Improved Cost-Sensitive Intrusion Response Model,* Journal of Information Assurance and Security,8(2013), 147-155.
8. Lee, W., Fan, W., Miller, M., Stolfo, S. J. and Zadok, E., 2002. Toward cost-sensitive modelling for intrusion detection and response, in *Journal of Computer Security,* 10(1/2), 5-22.
9. Mirkovic, J., Hussain, A., Wilson, B., Fahmy, S., Reiher, P., Thomas, R., Yao, W. and Schwab, S., 2007. Towards user-centric metrics for denial-of-service measurement. *In Proceedings of the Workshop on Experimental Computer Science, Part of ACM FCRC.*
10. Mirkovic, J., Reiher, P., Fahmy, S., Thomas, R., Hussain, A., Schwab, S. and Ko, C., 2006. Measuring denial of service. *In Proceedings of the 2nd ACM workshop on Quality of protection,* Alexandria, VA, USA, 53 – 58.
11. Shameli-Sendi A., Ezzati-Jivan N., Jabbarifar M. and Dagenais M. (2012). Intrusion response systems: survey and taxonomy. *ijcsns international journal of computer science and network security, vol. 12.*
12. Stakhanova N., Basu S. and Wong J. (2007a). "A cost-sensitive model for preemptive intrusion response systems," *in proceedings of the IEEE international conference on advanced information networking and applications, niagara falls, Canada.*
13. Stakhanova N., Basu S. and WongJ. (2007b.). "A taxonomy of 5ntrusion response systems," I*nternational journal of information and computer security*, 1, 169–184.
14. Stakhanova N., Strasburg C., Basu S. and Wong J., 2012. "Towards cost-sensitive assessment of intrusion response selection", *Journal of Computer Security, 20(2012):169-198.*
15. Strasburg C.R., Stakhanova N., Basu S. and Wong J., 2009. A framework for cost sensitive assessment of intrusion response selection. *33rd Annual IEEE International Computer Software and Applications Conference,* Seattle, WA, 355-360.
16. Svecs I., Sarkar T., Basu S.and Wong J. S. 2010. XIDR: A Dynamic framework utilizing Cross-layer Intrusion Detection for effective response deployment. *34th Annual IEEE Computer Software and Applications Conference Workshops,* Seoul, 287 -292.
17. Toth T. and Kruegel C. (2002). Evaluating the impact of automated intrusion response mechanisms. In *ACSAC '02: Proceedings of the 18th Annual Computer Security Applications Conference*, Las Vegas, NS, USA, 301.
18. Zhou M. and Yao G. 2012. Improved cost-sensitive model of intrusion response system based on clustering. *International Conference in Electrics, Communication and Automatic Control Proceedings, 931-937.*