New Cost-Sensitive Model for Intrusion Response Systems Minimizing False Positive

Jalal Baayer[1], Boubker Regragui[2]
[1, 2,] *SIME Laboratory, ENSIAS, Mohammed V Suissi University, B.P. 713 Rabat, Morocco*

ABSTRACT :*Dynamic Cost-sensitive Intrusion Response System (Dy-COIRS) is considered as one of the challenging intrusion response model in intrusion detection and prevention systems (IDS/IPS) field. This type of intrusion response system is faced to the issue of false positive responses (FPR) such as an error responses toward normal activities that does not affect the integrity, confidentiality availability and authentication of computer systems. This leads to high overhead which harms severally the overall network performances. In this paper, we propose an intelligent automatic dynamic cost sensitive model intended for IRS related to IDS/IPS field where the impact of false positive responses are minimized. This FPR reducing is based on an algorithmic approach with a linear model theory.*

Keywords*: Dynamic Cost-sensitive Intrusion Response System (Dy-COIRS), IDS (Intrusion Detection System), IPS (Intrusion Prevention System), false positive responses, linear model.*

I. INTRODUCTION

Dy-COIRS is able to assure responses against attacks which are generally divided into the following four categories [1], [13]: Denial of service, User to root (U2R), Remote to local (R2L) and Probe. The decision of response launch is based on cost approach without the aid of manual interventions of a network administrator. A Dy-COIRS is seen as an automatic intelligent system because its components can dynamically establish a release in the form of response further to intrusions analysis.

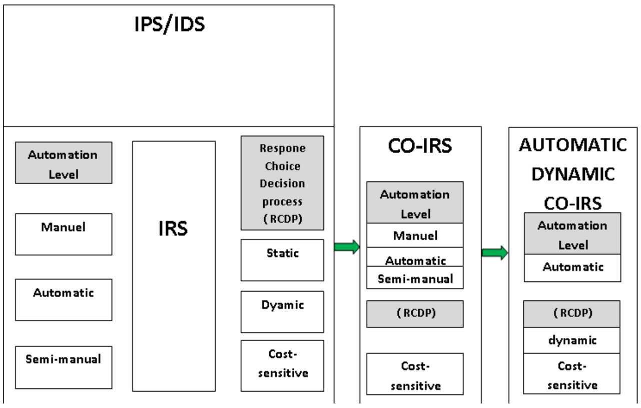


Fig. 1. Dy-COIRS used with IPS / IDS Systems

In a Dy-COIRS, the response can be given dynamically for IDS or IPS systems, by considering two values: intrusion affectation damage and response deployment cost.

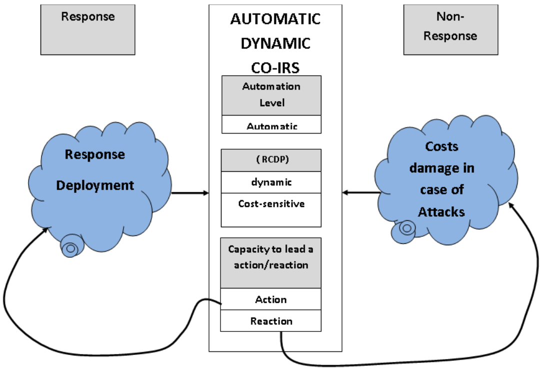


Fig. 2. The Functioning of Dy-COIRS

Those costs values are analysed to decide on the necessity of an optimal given response [2]. So, the success of a given response is strongly dependent on the good balance between the attack affectation damage and the system resources restoring costs.

In practice, the IRS has a false positive response when it lunches a wrong response against a real attack or in front of a normal activity. False positive responses in Dy-COIRS can seriously affect, disrupt the efficiency and harshly degrade the overall performances of IDS/IPS [3] [4] [12].

When the most known intrusions can be avoided or countermeasured by appropriate responses, false positive responses are still subject of various research works. This fact is due to their presence in IRS and Dy-COIRS field as "mistake" phenomena related to an abnormal action in front of an innocent behaviour. So, to decrease the impact of these false positive responses in IDS/IPS field, many reducing models concepts were developed [6] [7] [8] [9] [10]. Indeed, these false positive reducing models permit to report the real intrusions and attacks with false positive responses minimization. Consequently, given appropriate responses against real intrusions increase the operation quality and the accuracy of such IRS and specially Dy-COIRS.

In a Dy-COIRS, the fixed cost model is pre-discussed and related to the cost of each intrusion and the cost of the response launched as countermeasure [11]. In reality, the choice of a model with a big enough cost of false positive responses generates a large extra cost which clearly undermines the performance and efficiency of an Dy-COIRS. So, to avoid this problem a new cost-sensitive model for intrusion response systems is required.

In this paper, we present a new intelligent cost-sensitive model for intrusion response systems used for IDS/IPS to limit and minimize the impact of false positive responses. Our proposed model is based on an algorithmic approach with a linear model theory and on cost approach of intrusions and responses. Moreover, our proposition of false positive minimization enables to network administrators to limit and reduce the cost generated by a false positive response and increase the performance of Dy-COIRS.

The rest of this paper is organized as follows. Section 2 presents a related work that gives an overview on Dy-COIRS and false positives responses minimization related to intrusions responses systems. Section 3 presents models with mathematical approach and especially linear models. Section 4 presents our improvement. Section 5 presents simulations and results. The conclusion is given in the last section 6.

II. RELATED WORK

The domain of Dy-COIRS with FPR minimization was not enough targeted by the researchers these last years as it was generally with intrusions detection, prevention or response systems. But, there are few numerous research works in this domain which can be revealing.

In the field of Dy-COIRS, many research works are done independently of the purpose of FPR minimization. We can mention the following researchers works: B. Foo [14], T. Toth [2], I. Balepin [15], M. Jahnke [16], S. Yu [17], M. Papadak [18], K. Haslum [13], C. P. Mu [19], W. Kanoun [20] and N. Kheir [21]. All these works present different models of Dy-COIRS without the explicit false positive responses minimization.

At the first, Denning asserted in his study [22], that the study of the costs is not seen in the aspect of an authentic knowledge. This work switched on the first light around the notion of cost in the field of intrusions responses. Northcutt came to treat in [23] the methodology of studies of the risks in the computer systems by describing measures basing itself on degrees of criticality and destruction. Approach proposed by Balepin [15] basing on the principle of the representatives of services used a graphic prototype for the selection of the optimal responses with the institution of a typical hierarchy of resources by engendering the maximum of privileges with the minimum of cost. Toth [2] used of a prototype of a computer network by taking into account means (functions/ services), the users, the type of the network and the control access systems. The costs of the responses are measured by basing on the decrease of the values of the capacities of the resources. The work of followers [14] was presented as Framework allowing the choice and the deployment of the automatic response against intrusions basing on two categories of graphic plans: a plan of service and plan of response.These models and these solutions evoked above are not coherent between them. Every proposal has a concept of evaluation and selection of response cost sensitive with a different vision. The works of [22] and [23] evoked for the first time the notion of cost, and the method of study of the risks in the field of detection of intervention without treating the response cost with connection with intrusion cost. The works presented by [2] and [20] considered the response cost in contribution with the resources of system, by showing several processes of estimation. Toth [2] calculates the cost of response as a function of decrease of capacity of system. [15] measured the cost of answer being the sum of the costs manually committed by the affected system resources. All works done by [2], [13], [14], [15], [16], [17], [18], [19], [20],[21], [22] and [23] did not take into account the impact of cost false positive response, and his necessary minimization to have appropriate responses.

Other side, in the field of false positive responses minimization, many research works are done independently of the purpose of Dy-COIRS field. We can mention the following researchers works: Subramanian [6], Benjamin [7], Emmanuel Hooper [8], Hassen Sallay [9] and Kai Hwang [10]. Subramanian [6] introduced a Content Split Approach (CSA), made particularly for the signature databases related to network intrusion detection and prevention to reduce false positive responses. Benjamin [7] suggested a relationship of the information associated to the characteristics of the supervised information system, information about the faults, information security utilities of information security used to supervision events. Hooper [8] proposed a model to minimize false positives responses based on adaptive responses of firewall rules. This model represents a mixture of firewall structural design connected with response rules, to reject entrance to crucial segments to doubtful hosts in the computer network. Hassen Sallay [9] reflected on a scalable structure for IDS shared for networks with a large flow to amend efficiency. Kai Hwang [10] suggested a hybrid model of signature based Intrusion Detection System IDS and Anomaly Detection System (ADS), to reduce false-positive and to detect unknown intrusions.

There are little research works that targeted the minimization of false positive responses within the Dy-COIRS. We can mention the following researchers works: W. Lee[1], Strasburg [24], S. Tanachaiwiwat [25], and N. Stakhanova [5]. Work by Lee [1] considered experimental costs of the effects of the intrusions and the measures taken by the responses as criteria for the responses choice against the intrusions already classified. This work introduces a cost-benefit measure which incorporates multiple dimensions of cost in the face of an intrusion: response cost. This work is done only for IDS and not IPS. It did not target the Dy-COIRS. And the minimization of the cost of False Positive was treated usually implicitly with Consequential Cost Reducing and not explicitly as specific False Positive minimization. The works of Strasburg [24] and N. Stakhanova [5] presents a host-based framework for cost-sensitive intrusion response selection with a method for evaluating each intrusion response with respect to the risk of potential intrusion damage, effectiveness of response action and response cost for a system. The minimization of false positive response is treated implicitly with damage cost optimization. S. Tanachaiwiwat [25] presented a framework constructed with three essential modules: the IDS (intrusion detection system), the RAS (risk assessment systems), and the IRS (intrusion response system). The RAS is able to distinguish different kinds of false alarms or miss detections. The minimization of false positive responses is made in the context of the risk assessment systems without a using of specific algorithm for FP reducing.

III. LINEAR CONTROL SYSTEM

In the mathematics sense, a system is linear if we can apply it the principle of superimposing. Basing on a physical point, linear system can be defined more restrictive as a system that is can be described by differential equations with finished order and constant coefficients. With this definition, we can associate with the system, by means of the transformed of Laplace, a transmittance H (p) which is a rational fraction with p=jw. In automatic, we complete frequently the of linearity with the transmittance associated with the pure delay, that is a term of the form exp (-αp) with α is a constant time. The methods of study of the linear systems are very powerful in reason of the available tools (linear algebra, differential equations and differential systems.

The linear systems are relatively simple from a mathematical and algorithmic point of view, and purely exactly because of the linearity of the equations.

An linear control system is a commanded system possessing a device of return allowing to compensate for the infidelity of a physical system. It includes:

- **The direct chain H(p):** it is the commanded system which is subjected to the influence of the disturbances and thus miss of fidelity. Its transmittance is often noted H (p).
- **The chain of return K:** it converts the greatness of exit in a tension which is the signal of return **xr**. This sensor must be faithful, so, insensible with the disturbances.
- **The organ of display K:** it transforms the wished value Ye of y (instruction) to tension x. it is not present in all control process.
- **The comparator:** it elaborates the signal of error e = x – xr

A linear control system in a certain range around the point of rest, provided with an organ of display, a buckle of return and supposed initially in the rest, has the following functional plan:

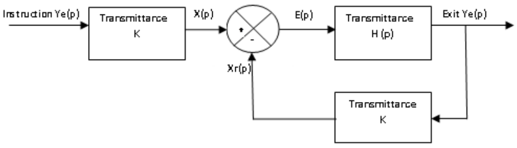


Fig. 3. Functional plan of linear control system

IV. OUR IMPROVEMENT

Generally, each activity in the computer network has two states: real attack or normal activity. Each such Dy-COIRS can have three reactions: no response, true response or false response. We can present all possible combinations between intrusions cases and responses cases on the following figure:

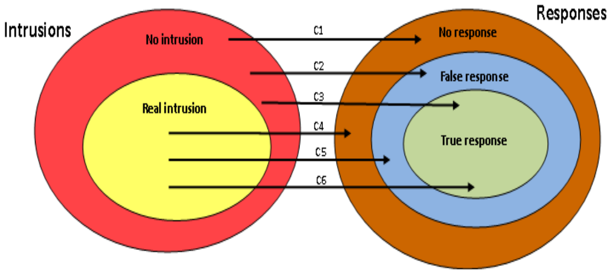


Fig. 4. The Reaction cases of Dy-COIRS

The false positive response is a simple wrong countermeasure which can be launched by IDS or IPS through IRS and specially Dy-COIRS when a legitimate activity is considered wrongly as attack.

The Figure 4 illustrates that the false positive response corresponds to the two cases: C2 and C5. False negative response corresponds to the case C4. True response corresponds to the two cases: C1 and C6. The case C3 is not feasible because it cannot logically happen in reality.

This problem of false positive responses can be treated at two basic approaches. The first approach is the conception of the IDS and IPS. The second is the implementation part of these systems. Indeed, for a given legitimate activity in the network, the IDS or IPS intercepts it as an attack, and sent an order to the IRS to launch immediately a response independently to any estimation to the cost or the impact of this countermeasure on the actual environment. So the intrusion detecting processing shown with conception and implementation approach of IDS or IPS is not enough to limit the impact of this phenomenon of false positive on network performance and efficiency security strategy.

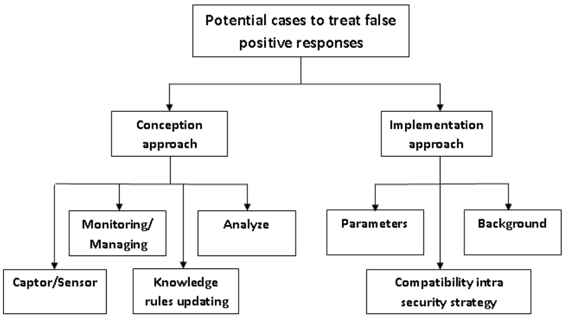


Fig.5. Typical cases of false positive treating

The Figure 5 illustrates typical cases and approaches of treating of false positive responses. In the first step, for a given innocent activity in the network, IDS or IPS considers it wrongly as intrusion at design or operational approach. In second strep and after making mistake, IDS or IPS send an order to Dy-COIRS to launch an passive response as alarms or an active response as blocking of the traffic considered as doubtful or stopping packages every time an attack is discovered. As a result, all passive or active false positive responses that verify the classic conditions detection through conception and operational approaches present an overhead which impact directly the network performance and the IDS or IPS severity.

Recent works [1], [5], [24] and [25] are still using the minimization of false positive responses implicitly with damage cost optimization and in some cases it is made in the context of the risk assessment systems without a using of specific algorithm for FP reducing. This choice of classic process give a greatest weakness related to the cost minimizing of false positive. Indeed, without this cost model for false positive, administrators will have difficulty to understand the cost of false positive in their organizations, depending on the way they implement their IDS, IPS and Dy-COIRS. Thereafter, without this model, we have not an effective tool to help network administrators to describe quantifiable costs of false positives responses and other costs that are concrete, still difficult to quantify such as loss of services.

In this section, we present a cost sensitive responses model aiming to limit the impact of false positives responses launched wrongly by Dy-COIRS in the case of an innocent activity in the network. Our approach has the advantage not to require any complex process because it only based on the linear system theory. Our cost model presents the responses costs launched against attacks and intrusions threatening a network during a period and this model helps for minimizing of false positive responses impact. Moreover, this responses costs presentation and false positive responses impact minimizing is a lightweight calculation and it is based on the standard theory of linear systems. The choice of the linear approach is due to its simplicity

Referring to the Figure 5, the phenomena of false positive appears when a IDS or IPS detect wrongly a legitimate activity as an attack. This mistake aspect can appear at design or implementation approach. So, an error response as false positive should be launched by Dy-COIRS. That means that minimizing false positives responses can be done by reducing their responses costs.
Based on this observation, we can define the cost response results of an Dy-COIRS relates to IDS or IPS through the Cost Response Matrix

$$M= (cij)$$
(1)

M is a square matrix of order n+1, where n is the number of different intrusion types. For 1 < i, j < n, the i-th row corresponds to intrusion type i. The j-th column corresponds to response type j launched by The Dy-COIRS. The matrix element (mij) is equal to the cost represented by response type j against the attack type i. The intrusions are indicated by the rows and responses by columns.

The costs false negative responses correspond to all miss detection at the last column marked as the FNR domain. The cost false positive response are at bottom row with i = n+1 for no attacks marked as the FPR domain.

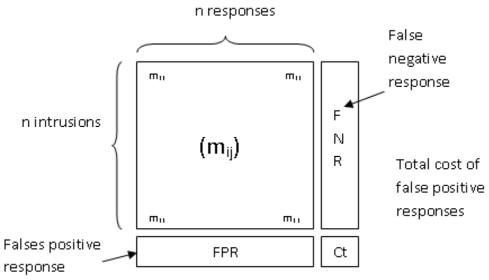


Fig.6. M cost Response matrix

In the following part of this work, in order to show the importance of our proposed, we define the matrix A as the initial cost matrix of cost related to the Dy-COIRS. It represents the knowledge module of cost rules using to evaluate the cost response. Each (a_{ij}) show the cost deployment of the response j against the intrusion i. The values of (a_{ij}) are evaluated by technical and financial administrators using a real journal of history of events and specially different intrusions. The costs of different responses deployed are calculated and noted in this journal. The matrix A is a represents cost rules module defined for each Dy-COIRS.

Indeed, We consider also, the matrix B representing the number of responses launched against intrusions following the the random low. This matrix will be constructed after a long observation of system targeted by intrusions during the study period. Each (b_{ij}) illustrates the number of the response of type j against the intrusion of type i.
For each intrusion of type i, the total number of responses launched against it is represented by Ni:

$$Ni=\sum_{k=1}^{k=n} b_{ik}$$
(2)

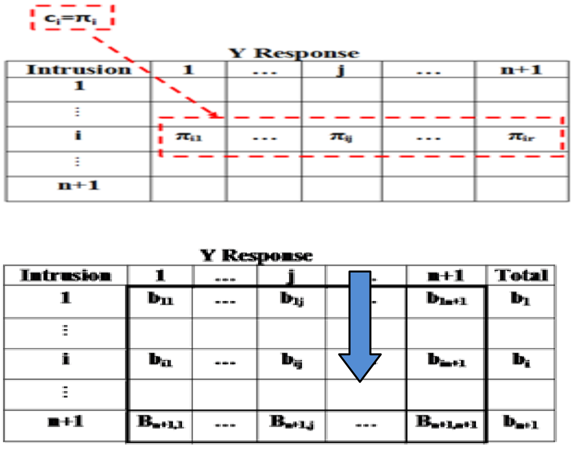
Where:

- b_{ik} is the number of the response of type k against the intrusion of type i.
- n is the total number of intrusions and responses

The probability that a response of type k, will be launched against the intrusion of type i is represented as following:

$$\pi_{ik} = (b_{ik} / \sum_{m=1}^{m=n} b_{im})$$
(3)

We define also the matrix C=(c_{ij})= (π_{ij}) that represents the probability matrix of responses launched against intrusions . The probability matrix is described as following in the proposed model:



Y Response

Intrusion	1	...	j	...	n+1
1					
⋮					
i	π_{i1}	...	π_{ij}	...	π_{ir}
⋮					
n+1					

Y Response

Intrusion	1	---	j	..	n+1	Total
1	b_{11}	---	b_{1j}	.	b_{1n+1}	b_1
⋮						
i	b_{i1}	---	b_{ij}	.	b_{in+1}	b_i
⋮						
n+1	$B_{n+1,1}$	---	$B_{n+1,j}$	---	$B_{n+1,n+1}$	b_{n+1}

Fig.7. C probability matrix of responses

Thereafter, define D=(d_{ij}) as the matrix of real response cost or the normalized cost matrix .It is observed during period study. We can define the matrix D as a multiplication of the two matrixes A and C.

$$D=A\times C$$
(4)

Each d_{ij} is obtained as the cost of response j launched against an intrusion i, following the term:

$$d_{ij} = \sum_{k=1}^{k=n} a_{ik}\times c_{kj}$$
(5)

For our proposed algorithm for the minimization of false positive, we consider the definitions bellow:

- *Tolerance value (TV):* a value chosen for each IDS/IPS, under it , the rate of false positive allows to have an optimal work of IDS/IPS.
- *Cfp:* false positive responses cost defined following the matrix D.
- *Ctotal:* responses total cost defined following the matrix D.
- Rt: false-Positive Cost Ratio= Cfp / Ctotal
- Rav: the average false-Positive Cost Ratio
- Matrix A_0 : Present the initial values of the matrix A_0 related to each IDS/IPS/ Dy-COIRS.

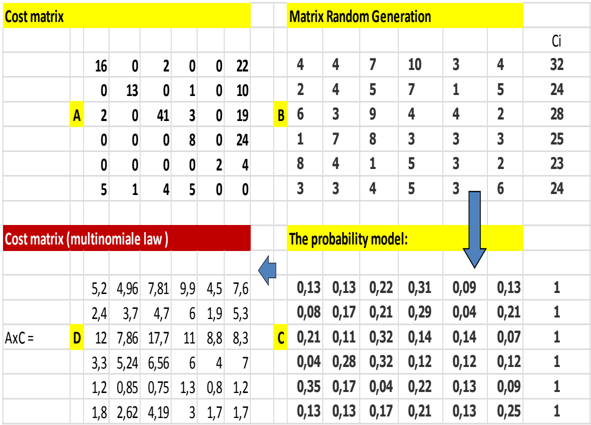
Our proposed algorithm for the minimization of false positive is presented as following:

```
Matrix A = Matrix $A_0$;
TV=$TV_0$;
Step 1: Matrix B $\longrightarrow$ Matrix C;
D=A×C;
Cfp= $\sum_{i=1}^{i=n+1} d_{i,\,n+1}$;
Ctotal= $\sum_{i=1}^{i=n+1} \sum_{j=1}^{j=n+1} d_{i,j}$;
If  (Rt < TV) then (our IDS/IPS is working optimally : OK);
If not (Rt ≥ TV) then (our IDS/IPS is working non optimally: NOK):
        { Rav= Rt/(n+1);
          For i=1 to i=n+1;
                If ($a_{ij}$≥ Rav) then
                      $a_{ij}$=$a_{ij}$ – 1 ;
                EndIf;
          EndFor; }
EndIfnot;

Go to step1;
```

V. SIMULATION AND RESULT

For illustrative purpose, we tested our model on real IDS with simulation experiments over the following alarm matrix resulted from data entries extracted from an IDS evaluation report by IT maintenance dept. in Q1/2012.This matrix corresponds five 5 attacks types in the following Table. The matrix entries correspond to a 3 month-long monitoring of a troubleshooting and maintenance entity.

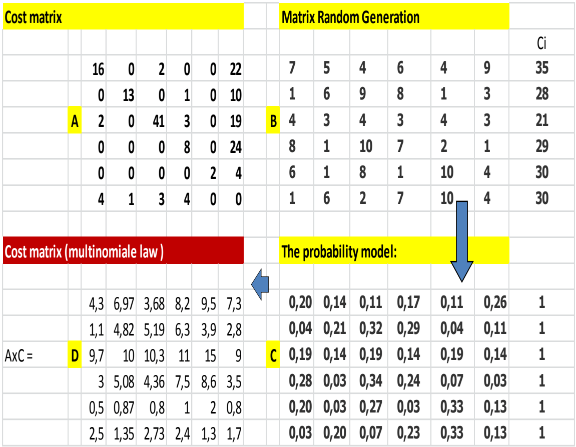


Cost matrix									Matrix Random Generation						
															Ci
		16	0	2	0	0	22		4	4	7	10	3	4	32
		0	13	0	1	0	10		2	4	5	7	1	5	24
	A	2	0	41	3	0	19	B	6	3	9	4	4	2	28
		0	0	0	8	0	24		1	7	8	3	3	3	25
		0	0	0	0	2	4		8	4	1	5	3	2	23
		5	1	4	5	0	0		3	3	4	5	3	6	24
Cost matrix (multinomiale law)									The probability model:						
		5,2	4,96	7,81	9,9	4,5	7,6		0,13	0,13	0,22	0,31	0,09	0,13	1
		2,4	3,7	4,7	6	1,9	5,3		0,08	0,17	0,21	0,29	0,04	0,21	1
AxC =	D	12	7,86	17,7	11	8,8	8,3	C	0,21	0,11	0,32	0,14	0,14	0,07	1
		3,3	5,24	6,56	6	4	7		0,04	0,28	0,32	0,12	0,12	0,12	1
		1,2	0,85	0,75	1,3	0,8	1,2		0,35	0,17	0,04	0,22	0,13	0,09	1
		1,8	2,62	4,19	3	1,7	1,7		0,13	0,13	0,17	0,21	0,13	0,25	1

Fig.8. Our first simulation of the cost model of responses

We define the knowledge module that can compare the False-Positive cost Ratio with a tolerance value (TV).

- Step 1 : If the 8% is less than the TV our IDS/IPS is working optimally → OK
- Step 2 : If the 8% is more than the TV our IDS/IPS is working non optimally→ NOK
  - We have to react to this situation by minimizing the false-Positive Cost Ratio cost line
    - The average of the False-Positive cost is = 15/6 = 2.5
    - If the Cost is > 2.5 → put Cost – 1
- Goto Step 1



Cost matrix									Matrix Random Generation						
															Ci
		16	0	2	0	0	22		7	5	4	6	4	9	35
		0	13	0	1	0	10		1	6	9	8	1	3	28
	A	2	0	41	3	0	19	B	4	3	4	3	4	3	21
		0	0	0	8	0	24		8	1	10	7	2	1	29
		0	0	0	0	2	4		6	1	8	1	10	4	30
		4	1	3	4	0	0		1	6	2	7	10	4	30
Cost matrix (multinomiale law)									The probability model:						
		4,3	6,97	3,68	8,2	9,5	7,3		0,20	0,14	0,11	0,17	0,11	0,26	1
		1,1	4,82	5,19	6,3	3,9	2,8		0,04	0,21	0,32	0,29	0,04	0,11	1
AxC =	D	9,7	10	10,3	11	15	9	C	0,19	0,14	0,19	0,14	0,19	0,14	1
		3	5,08	4,36	7,5	8,6	3,5		0,28	0,03	0,34	0,24	0,07	0,03	1
		0,5	0,87	0,8	1	2	0,8		0,20	0,03	0,27	0,03	0,33	0,13	1
		2,5	1,35	2,73	2,4	1,3	1,7		0,03	0,20	0,07	0,23	0,33	0,13	1

Fig.9. Our second simulation minimizing cost false positive

If we suppose that the TV = 7.5% and as we decrease the False-Positive Cost value by 1, we have u = 12 false-positive alarms at the bottom row. Our total cost is 182 that mean our false-Positive Cost Ratio is 7% which means that our IDS/IPS is now with an optimal Dy-COIRS.

VI. CONCLUSION AND PERSPECTIVES

In this paper, we propose a cost-sensitive model for Intrusion Response Systems to limit the impact of false positive in IRS and specially Dy-COIRS. Our approach reduces the cost of false positive responses launched by Dy-COIRS in the case of an innocent activity comparing to the classic methods based on detection without cost approach revealing defined at the beginning of a communication. Therefore, the cost of false positive responses are reduced which increase the IRS and COSIRS performance. As a future work, we plan to study the COSIRS performance in the case where we combine our cost model, based on linear system theory, with another model minimizing the false negative responses.

REFERENCES

[1] W. Lee, W. Fan, M. Millerand, S. Stolfo, and E. Zadok. Toward cost-sensitive modeling for intrusion detection and response. *In Journal of Computer Security, volume 10, pages 5–22, 2002.*

[2] T. Toth and C. Kregel, Evaluating the impact of automated intrusion response mechanisms, *In*

proceeding of the 18th Annl Computer Security Applications Conference, Los Alamitos, USA, 2002.

[3] K. Timm, *Strategies to reduce false positives and false negatives in NIDS*, Security Focus Article, available online at: http://www.securityfocus.com/infocus/1463, 2009

[4] M.J. Ranum, *False Positives: A User's Guide to Making Sense of IDS Alerts* (ICSA Labs IDSC, 2003).

[5] N. Stakhanova, S. Basu, and J. Wong. A cost-sensitive model for preemptive intrusion response systems *In Proceedings of the IEEE AINA, pages 428–435*, 2007.

[6] Subramanian Neelakantan et. al. (2009) "Content-Split Based Effective String-Matching for Multi-Core Based Intrusion Detection Systems , First International Conference on Computational Intelligence, Communication Systems and Networks Pages: 296-301 ISBN:978-0-7695-3743-6

[7] Benjamin Morin 1, Ludovic M, Herv Debar, and Mireille Ducass (2007) *M2D2: A Formal Data Model for IDS Alert Correlation, Volume 2516/2002, pages 115-137* onlinehttp://www.springerlink.com/content/cwp428tlhf35rwba/

[8] Emmanuel Hooper (2006), "An Intelligent Intrusion Detection and Response System Using Network Quarantine Channels: Adaptive Policies and Alert Filters", *Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology* (WI-IAT 2006 Workshops)(WI-IATW'06), pp. 16-21, 0-7695-2749-3/06 $20.00 © 2006.

[9] Hassen Sallay, Khalid A. AlShalfan, Ouissem Ben Fred, (2009), "A scalable distributed IDS Architecture for High speed Networks", *IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.*

[10] Kai Hwang, MinCai, Ying Chen and Min Qin "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes"(2007), *IEEE Transactions On Dependable And Secure Computing, Vol.4, No.1, January-March 2007*, accessed on22.02.08,http://ieeexplore.ieee.org/search/wrapper.jsp?arnumber=4099191.

[11] J. Baayer, B.Regragui- *WOTIC'09* – " Architecture Fonctionnelle d'un IPS, Etat de l'Art et Classification de Ses Systèmes de Réponse d'Intrusion (IRS) ", *December 25 2009*, Université Ibn Zohr, Agadir, Morocc

[12] Stefano Zanero(2007), *Flaws and Frauds in the Evaluation of IDS.IPS Technologie, first accessed on 21.09.07,*http://www.first.org/conference/2007/papers/zanero-stefano-paper.pdf

[13] K. Haslum, A. Abraham and S. Knapskog, "DIPS: A framework for distributed intrusion prediction and prevention using hidden markov models and online fuzzy risk assessment," *In 3rd International Symposium on Information Assurance and Security*, pp. 183-188, Manchester, United Kingdom, 2007.

[14] B. Foo, Y.-S.Wu, Y.-C. Mao, S. Bagchi, and E. H. Spafford. ADEPTS: Adaptive intrusion response using attack graphs in an e-commerce environment. *In Proceedings of DSN*, pages 508–517, 2005.

[15] I. Balepin, S. Maltsev, J. Rowe, and K. Levitt. Using specification-based intrusion detection for automated response. *In Proceedings of RAID*, pages 136–154. Springer, 2003.

[16] M. Jahnke, C. Thul, and P. Martini. Graph based metrics for intrusion response measures in computer networks. *In Proceedings of the IEEE LCN*, pages 1035–1042, 2007.

[17] S. Yu and Z. Rubo, "Automatic intrusion response system based on aggregation and cost," *in International Conference on Information and Automation (ICIA)*, 2008, pp. 1783-1786.

[18] M. Papadaki and S. M. Furnell, "*Achieving automated intrusion response: a prototype implementation*," Information Management and Computer Security, vol. 14, no. 3, 2006, pp. 235-251.

[19] C. P. Mu and Y. Li, "*An intrusion response decision making model based on hierarchical task network planning*," Expert systems with applications, vol. 37, no. 3, 2010, pp. 2465-2472.

[20] W. Kanoun, N. Cuppens-Boulahia, F. Cuppens and S. Dubus, "Risk-Aware Framework for Activating and Deactivating Policy-Based Response," *Fourth International Conference on Network and System Security*, pp. 207-215, 2010.

[21] N. Kheir, N. Cuppens-Boulahia, F. Cuppens and H. Debar, "A service dependency model for cost sensitive intrusion response," *Proceedings of the 15th European Conference on Research in Computer Security*, pp. 626- 642, 2010.

[22] D. Denning. *Information Warfare and Security* (Addison-Wesley, 1999).

[23] S. Northcutt. *Intrusion Detection: An Analyst's Handbook*. (New Riders Publishing, 1999).

[24] C. Strasburg, N. Stakhanova, S. Basu and J. S. Wong, "A Framework for Cost Sensitive Assessment of Intrusion Response Selection," *Proceedings of IEEE Computer Software and Applications Conference*, 2009.

[25] S. Tanachaiwiwat, K. Hwang and Y. Chen, *Adaptive Intrusion Response to Minimize Risk over Multiple Network Attacks* (ACM Trans on Information and System Security, 2002).