False Positives Reduction Techniques in Intrusion Detection Systems-A Review

Asieh Mokarian, Ahmad Faraahi, Arash Ghorbannia Delavar,

Payame Noor University, Tehran, IRAN

Summary

During the last decade with the growth of cyber attacks, information safety has become an important issue all over the world. Intrusion detection systems (IDSs) are an essential element for network security infrastructure and play a very important role in detecting large number of attacks. Although there are different types of intrusion detection systems, all these systems suffer a common problem which is generating high volume of alerts and huge number of false positives. This drawback has become the main motivation for many research papers in IDS area. The aim of conducted research in the field is to propose different techniques to handle the alerts, reduce them and distinguish real attacks from false positives and low importance events.

This manuscript is a survey paper that represents a review of the current research related to the false positives problem. The focus will be on data mining techniques of alert reduction. This paper reviews more than 30 related studies during the last decade with the hope of providing a reference for further research in this area. Several open issues have also been addressed in this paper.

Key words:

network security; intrusion detection system; data mining; false positive rate; alert reduction

1. Introduction

During the last years, the number of unauthorized activities, intrusions and attacks in computer networks has grown extensively. With the explosive increase in number of services accessible through the Internet, information security of using Internet as the media needs to be carefully concerned and a sufficient protection is needed against cyber attacks.

Intrusion detection systems (IDSs) are an essential component of a complete defense-in-depth architecture for computer network security. IDS is an effective security technology, which can detect, prevent and possibly react to the attack [1]. It monitors target sources of activities, collects and inspects audit data looking for evidence of intrusive behaviors. When it detects suspicious or malicious attempts, an alarm is raised giving the network administrator the opportunity to react promptly. The main objective of IDS is to detect all intrusions in an efficient manner. IDSs can be classified from different points of view. Fig. 1 shows different classifications of IDSs. From the viewpoint of detection method, IDSs can be divided into two categories: anomaly and misuse (signature) based detection. Anomaly detection tries to determine whether deviation from the established normal usage patterns can be flagged as intrusions. On the other hand, misuse detection uses patterns of well-known attacks or weak spots of the system to identify intrusions [2]. As shown in Fig. 1, depending on the information source, an IDS may be either host or network-based. A host-based IDS (HIDS) analyzes events such as process identifiers and system calls, mainly related to OS information. On the other hand, a network-based IDS (NIDS) analyzes network related events: traffic volume, IP addresses, service ports, protocol usage, etc. [3]. Although IDS solutions have been used for about twenty years, an important problem is still not fully addressed: Unfortunately, these systems provide huge number of alerts which most of them are false alerts or low importance. For example, a single IDS sensor can generate tens of thousands of alerts in a day [4, 5]. Large volume of alerts is unmanageable and overwhelming to the human analyst. Inspecting thousands of alerts per day is unfeasible, especially if 99% of them are false alerts [6]. False alerts, also known as false positives occur when a legitimate activity has been mistakenly classified as malicious by the IDS. The vast imbalance between the actual and false alarms generated has undoubtedly undermined the performance of IDS [7].

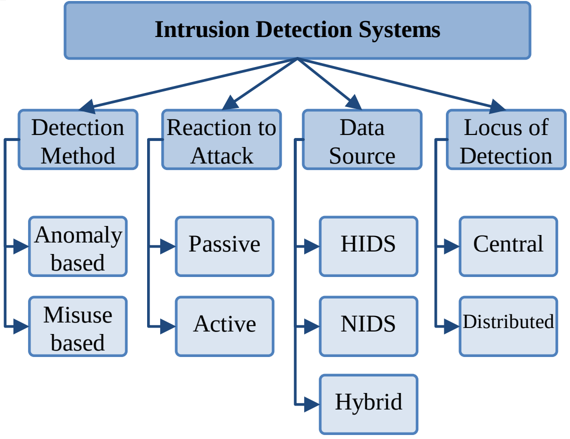

Fig. 1 Characteristics of intrusion detection systems

Manuscript received October 5, 2013
Manuscript revised October 20, 2013

Despite that anomaly-based IDSs produce more false positives rather than misuse-based IDSs, false positives are unavoidable in all types of IDS. Because of these reasons, during the last few years false positives reduction techniques have been extensively researched [4–40] and researches on IDSs have focused on how to handle these alerts.

Many approaches have been suggested for this purpose such as statistics [8], time series [4, 9], machine learning [10], and control charts [11], etc. Among proposed methods, data mining based techniques have been frequently suggested during the past decade. This paper aimed to provide a survey on techniques which are proposed for false positives reduction in IDSs and the focus will be on data mining based techniques. We will discuss and classify different methods and algorithms from a theoretical point of view. We will list important limitations noted from the literature.

This paper is organized as follows. SectionII explains the main measures for evaluating different methods for false positives reduction. Sectiona general classification of proposed methods toward reducing alerts load and false positives and different researches in each category will be reviewed and discussed. The last section offers the conclusions.

2. Evaluation Parameters

There are many factors to evaluate the IDS such as speed, cost, resource usage, effectiveness, etc. [12]. However, recently false alarms rate and accuracy of detection are happen to be the most important issues and challenges in designing effective IDSs [13]. The effectiveness of an IDS is evaluated by its prediction ability to give a correct classification of events to be attack or normal behavior [14]. According to the real nature of a given event and the prediction from an IDS, four possible outcomes are shown in Table I, which is known as the confusion matrix [14, 15]. True negatives as well as true positives correspond to a correct operation of the IDS; True negatives (TN) are events which are actually normal and are successfully labeled as normal, true positives (TP) are events which are actually attacks and are successfully labeled as attacks. Respectively, false positives (FP) refer to normal events being classified as attacks; false negatives (FN) are attack events incorrectly classified as normal events.

According to the confusion matrix, (1)-(6) shows numerical parameters that apply following measures to evaluate the IDS performance.

Table 1: Confusion Matrix [14, 15]

Actual Class	Predicted Class	
	Normal	Attack
Normal	True negative (TN)	False positive (FP)
Attack	False negative (FN)	True positive (TP)

$$\text{False Positive Rate (FPR)} = \frac{\text{FP}}{\text{FP} + \text{TN}} \tag{1}$$

$$\text{False Negative Rate (FNR)} = \frac{\text{FN}}{\text{TP} + \text{FN}} \tag{2}$$

$$\text{True Positive Rate (TPR)} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{3}$$

$$\text{True Negative Rate (TNR)} = \frac{\text{TN}}{\text{TN} + \text{FP}} \tag{4}$$

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FN} + \text{FP}} \tag{5}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{6}$$

False positive rate (FPR) also known as false alarm rate (FAR), refers to the proportion that normal data is falsely detected as attack behavior. A high FPR will seriously cause the low performance of the IDS and a high FNR will leave the system vulnerable to intrusions. TNR also known as detection rate or sensitivity refers to proportion of detected attacks among all attack events. Accuracy refers to the proportion of events classified as an accurate type in total events [15]. So, to have an effective IDS both FP and FN rates should be minimized, together with maximizing accuracy and TP and TN rates.

Nowadays, intrusion detection system requires high detection rate and low false alarm rate. The important issue about evaluating different algorithms which are proposed to reduce false positives is that reducing just false positive rate is not enough. Some false positive reduction techniques will cause low accuracy because of some operations like over generalization, missing real attack alerts, etc. So, effective techniques will reduce the false positives rates while increase the accuracy of the system or at least keep it without change.

2.1 Evaluation Data Sources

Researchers usually evaluate their algorithms by performing some experiments on a typical network scenario, and assessing the effectiveness of the proposed techniques on such a scenario. There are several datasets which are used by different researchers in order to evaluate the efficiency and performance of the proposed techniques and to compare the results with others. The most used dataset is DARPA dataset.

The DARPA dataset created by the MIT Lincoln Laboratory group to conduct a DARPA-sponsored comparative evaluation of different IDS [16]. There are different versions of this dataset used for different purposes which are DARPA 1998, DARPA1999 and DARPA2000. Even though the DARPA dataset has been largely criticized [17], it is the reference dataset in the evaluation of IDS performance. The dataset is made of five weeks of network traffic traces consist of normal user activities and several attacks, extracted from a simulated military department network. The first three weeks of the DARPA1999 dataset contain network traffic that was created to be used as training set and the fourth and fifth weeks of the dataset contain traffic intended to be used as test set during the comparative IDS evaluation performed by the MIT Lincoln Laboratory group [16].

The other dataset which is used by researchers is Knowledge Discovery and Data Mining Cup 99 (KDD Cup 99). This database contains a standard set of data to be audited, which includes a wide variety of intrusions simulated in a military network environment and can be downloaded from [http://kdd.ics.uci.edu].

Besides these standard datasets, some researchers also have used a real world dataset to evaluate their technique in a real environment.

3. Techniques toward Reducing False Positives

Many methods have been proposed in order to reduce false positives. All these methods can be divided into two general approaches, as shown in Fig. 2. The first approach includes methods that operate during detection phase, we call them detection techniques and the second refers to the methods that operate on produced alerts after detection phase, we call them alerts processing techniques. Researches related to the first approach, propose different configuration of IDSs and detection methods and try to reduce false alerts with providing more accurate detection method. Since false positives are unavoidable because of the nature of anomaly detection method, in most of researches related to detection technique approach, the main target is maximizing detection rate and accuracy. It is obvious that a higher detection rate and higher accuracy will result lower false positives rate. These researches often use data mining techniques for better detection to maximize their detection rate and minimize false positives rate.

Toward reducing false alerts, some researches propose different configuration of IDSs but most of them propose alerts processing. Alert processing approach is the main solution to alerts handling and false positives reduction. Through alert processing techniques, data mining based techniques are the most used techniques that are exploited to reduce alerts and false positives.

Alert processing could be performed for different purposes such as: to reduce amount of alerts and false alerts, study the cause of these false positives, recognize high level attack scenarios, and finally provide a coherent response to attacks understanding the relationship between different alerts [18]. The main objectives of alert processing can be categorized as shown in Fig. 3. As this paper is a survey on false positives reduction techniques, we will focus on alert processing techniques as the main solution to alert reduction.

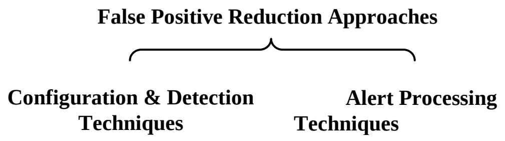
False Positive Reduction Approaches
Configuration & Detection Techniques
Alert Processing Techniques

Fig. 2 General FP Reduction Approaches

3.1 Detection Techniques

In 2008, Wu and Ye [15] compared the accuracy, detection rate, false alarm rate for four attack types: Probe, Dos, U2R, R2L. They provide accuracy comparison of these four kinds of attacks by C4.5 and SVM algorithms. They show that C4.5 acts better than SVM in accuracy of Probe, DoS and U2R attacks detection; but in false alarm rate, SVM is better. They suggest combining the two methods, so that overall accuracy can be increased greatly.

Anuar et al. [19] also have used the classes mentioned above and proposed a strategy to focus on detection involving statistical analysis of both attack and normal traffics based on the training data of KDD Cup99. They prepared a hybrid statistical approach which used data mining and decision tree classification. As a result, the statistical analysis can be manipulated to reduce misclassification of false positives and distinguish between attacks and false positives. They compared rule-based and decision tree algorithms and proved the importance of decision tree for modeling intrusion detection for class of normal, DoS, and R2L. For the class of Probe and U2R, rule-based classification is more suitable. Based on acceptable levels of false alarm rate, decision tree is more suitable than rule-based for modeling intrusion detection systems.

In 2008, Xiang et al. [20] proposed a multiple level hybrid classifier which combined the supervised tree classifiers and unsupervised Bayesian clustering to detect intrusions. Performance of this new approach shown to have high detection and low false alarm rates. They concluded that keeping FNR as low as possible while maintaining an acceptable level of FPR is essential for IDS since the false alarm might bring inconvenience to the administrators.

Later in 2011, Elshoush et al. [21] reviewed collaborative, intelligent intrusion detection system (CIIDS) which is proposed to include both misuse-based and anomaly-based methods. They Provide backgrounds on how to use alert correlation to reduce the false alarms rates (FAR) with different system architectures of CIDSs. They suggested fuzzy logic, soft computing and other AI techniques, to be exploited to reduce the rate of false alarms while keeping the detection rate high.

Also in 2011, Lee et al. [22] developed a framework for fully unsupervised training and online anomaly detection. In the framework, a self-organizing map (SOM) that is seamlessly combined with K-means clustering was transformed into an adaptive and dynamic algorithm suitable for real-time processing. The performance evaluation of proposed approach shows that it could significantly increase the detection rate while the false alarm rate remained low. In particular, it was capable of detecting new types of attacks at the earliest possible time.

In continue we will review the researches which use alert processing techniques to handle alerts load and false positives.

3.2 Alerts Processing Techniques

In 2000, Clifton and Gengo [23] used data mining techniques to identify sequences of alarms that likely result from normal behavior, enabling construction of filters to eliminate those alarms. They have investigated the detection of frequent alert sequences, in order to use this knowledge for creating IDS alert filters.

Julisch [24] in 2001 shows that alarms should be managed by identifying and resolving their root causes. He introduced alarm clustering as a method that supports the discovery of root causes. Julisch models the alarms as tuples of alarm attributes and alarm logs are modeled as a set of alarms. The taxonomies are created for every given attribute as element trees. The description of similarity between alarms given by Julisch is based on defined taxonomies. Thus, alarms are gathered and they are summarized by a general alarm or cluster. To do so, an attribute-oriented induction data mining heuristic algorithm is implemented. As a result, generalized alarms are obtained and this allows discovering the root. Removing the causes, Julisch showed that future alarm load could be reduced over a 90% [21].

Later in 2002, Julisch and Dacier [25] mined historical alarms to learn how future alarms can be handled more efficiently. They investigate episode rules with respect to their suitability in this approach. They have also proposed a conceptual clustering technique to show that intrusion detection alarms can be handled efficiently by using previously mined knowledge. Clusters correspond to alert descriptions, and a human expert can use them for developing filtering and correlation rules for future IDS alerts. During their experiments, Julisch and Dacier found that these hand written rules reduced the number of alerts by an average of 75% [25]. This work was later extended by Julisch who reported the reduction of alerts by 87% [6, 26].

Pietraszek [10] proposed Adaptive Learner for Alert Classification (ALAC) as a new system for reducing false positives. He points that background knowledge can be useful for alert classification. ALAC is an adaptive alert classifier based on the feedback of an intrusion detection analyst and machine-learning techniques. The classification of IDS alerts is a difficult machine learning problem. ALAC was designed to operate in two modes: a recommender mode, in which all alerts are labeled and passed onto the analyst, and an agent mode, in which some alerts are processed automatically. In recommender mode, where it adaptively learns the classification from the analyst, false negative and false positive were obtained. Where in the agent mode, some alerts are autonomously processed (e.g., false positives classified with high confidence are discarded).

In this system, a fast and effective rule learner was used that is RIPPER. It can build a set of rules discriminating between classes (i.e. false and true alerts). The number of false alerts reduced by more than 30%. This system has a disadvantage that is during a system’s lifetime the size of the training set grows infinitely.

Later, he extended his previous work in [27] and presented two complementary approaches for false positives reduction: CLARAty which is based on alert post processing by data mining and root-cause analysis and ALAC which is based on machine learning. CLARAty is an alert-clustering approach using data mining with a modified version of attribute-oriented induction [27]. Using this system, the number of alerts to be handled has been reduced by more than 50%. He has released a complete document of his work in [28] 2006.

In 2005, Bakar et al. [29] implement an intrusion alert quality framework (IAQF), to reduce false positive alerts in IDS. Using this framework, they enrich each alert with quality parameters such as correctness, accuracy, reliability, and sensitivity. Enriching alerts with data quality information help high-level alert operations to filter, correlate, or analyze the alerts. They also normalize enriched alerts in IDMEF format.

Siraj et al. [30] have aimed to develop a unified alert fusion model which will combine alert prioritization, alert clustering and alert correlation in a single framework but they just addressed the alert clustering aspect of sensor data fusion in their work. They used causal knowledge based inference technique with fuzzy cognitive modeling to cluster alerts by discovering structural relationships in sensor data.

In 2006, Long et al. [31] have suggested a supervised clustering algorithm for distinguishing Snort IDS true alerts from false positives. Their technique uses Intrusion Detection Message Exchange Format (IDMEF), which is written in XML and a novel XML distance measure is proposed to implement the clustering algorithm based on this measure.

Perdisci et al. [32], proposed a new strategy to perform alarm clustering whose main objective is to reduce volume of alarms generated by multiple IDS sensors and to produce unified descriptions of attacks from alarms produced by different IDSs. Their work is a revised version of Giacinto et al. [33], where they proposed a new on-line alarm clustering system.

In 2007, Al-Mamory et al. have provided a survey on alert processing techniques [18], later in 2008 they proposed a data mining alert clustering technique that groups alarms whose root causes are generally similar and finds generalized alarms which help the human analyst to write filters [34, 35, 36]. During their experiments, the averaged reduction ratio was about 82% [34], 93% [35] and 74% [36] of the total alarms. Their method can be considered as a variation of Julisch's work; however, they have designed a new data mining technique, which is different in clustering methods, to reduce alarms load. They claim that application of their technique to alarms log greatly helps the security analyst in identifying the root causes and reducing alerts load in the future.

A drawback of most of these techniques is that they are offline and will be applied on alerts in offline mode. The other problem is that their techniques are dependent to human analyst to write filtering rules.

In 2009, Vaarandi [5] proposed a data mining based real-time classification method for distinguishing important network IDS alerts from frequently occurring false positives and events of low importance. He claims that unlike conventional data mining based approaches, the method is fully automated and able to adjust to environment changes without a human intervention. Later in 2010, he extends his previous work in [37] and presents a novel unsupervised real time alert classification method which is based on frequent itemset mining and data clustering techniques.

Spathoulas et al. [8] have proposed a post-processing filter to reduce FPR in network-based IDSs. The filter comprises three components; each one is based upon statistical properties of the input alert set. Their evaluation results indicate that the filter limits false positives by a percentage up to 75%.

Table 2: A review of false positive reduction techniques

	Researches (2000-2011)	False Positive Reduction Techniques	KDD CUP 99	DARPA 1998	DARPA1999	DARPA 2000	Real World	Results	
Detection Techniques	[15]	SVM	*					1.00%	False Positive Rate
	[15]	C4.5	*					1.44%	
	[19]	Decision Tree Classification ,Rule-based Classification	*					3.2%	
	[20]	Decision tree Classification , Bayesian Clustering	*					N/A	
	[22]	Self-Organizing Map , K-means Clustering	*				*	0.91-2.43%	
Alert Processing Techniques	[23]	Sequential Association Mining						NA	False Positive Reduction Ratio
	[25], [26]	Clustering (Attribute Oriented Induction)					*	75%, 87%	
	[10],[27],[28]	Machine-Learning (ALAC), Clustering (CLARAty)			*		*	30%, 50%	
	[29]	Quality Parameters , Normalization				*		98.03%	
	[30]	Multi-Level Clustering (Fuzzy Cognitive Modeling)				*		N/A	
	[31]	Clustering (based on xml distance measure)		*				N/A	
	[32] , [33]	Classification , Clustering			*		*	37%	
	[34],[35],[36]	Clustering , root cause analysis		*	*		*	82%,93%,74%	
	[5], [37]	Classification (Frequent Itemset Mining) , Clustering					*	81-99%,43.31%	
	[8]	Statistical Filtering			*			75%	
	[38]	Classification (Pattern Mining)			*			36%	
	[40]	Clustering , GHSOM					*	15% - 4.7%	
	[7]	Self-Organizing Map , K-means Clustering			*		*	90%,87%,50%	
	[13]	Rule-based Classification	*					N/A	
	[39]	Fuzzy Alert Aggregation			*			N/A	

Tian et al. [38] have used pattern mining method to develop an adaptive alert classifier that classifies alerts in true positives and false positives classes and learns knowledge adaptively by the feedback of the operators.

In 2009, Maggi et al. [39] have focused on alert aggregation as an important component of the alert fusion process. For this purpose they used fuzzy measures and fuzzy sets to design alert aggregation algorithms and to state whether or not two alerts are ‘‘close in time” dealing with noisy and delayed detections.

Mansour et al. [40] have used a data mining technique which is based on a Growing Hierarchical Self-Organizing Map (GHSOM) neural network model that determines the number and arrangement of map units during unsupervised training process. GHSOM clusters alerts to support network administrators in making decisions about true and false alerts and addresses limitations of the SOM. GHSOM reduces false positives from 15% to 4.7% and false negatives from 16% to 4% for the real-world data used.

In 2010, Tjhai et al. [7] developed a two-stage classification system using the combination of two data mining techniques: SOM (self organizing map) neural network and K-means clustering. The first stage classification was developed to properly correlate alerts related to a particular activity and the second classifies alerts into classes of true and false alarms. Their experiments shows that the proposed system effectively reduces all noisy alerts, which often contribute to more than 50% of false alarms generated by a common IDS.

In 2011, Sabri et al. [13] used data mining to extract the useful information from large databases. They have used the KDD CUP 99 dataset to evaluate their method. The results show that the data mining technique reduces the false alarms rate and increase the accuracy of the system.

At the end, we have summarized all reviewed techniques in this paper, their experimental results and their selected dataset to evaluate their method in Table II.

4. Conclusion

In this paper we have provided a review of researches during the last decade, which have aimed to reduce false positives and alerts load. We have categorized these researches into two general approaches, a) the detection techniques that act during detection phase and b) the alert processing techniques that are applied on generated alerts after detection phase. While some of the papers have proposed different configuration of IDSs and detection methods, the majority of them have focused on the alert processing techniques.

In either case, various approaches have been used to deal with the issue. Among different proposed methods, data mining techniques are of much interest recently. Data mining is the main solution to evaluate the quality of alerts and deal with false positives problem in intrusion detection systems. Some researchers have used hybrid data mining techniques to get better results.

There are some open problems and disadvantages related to the previous researches that can be considered for further exploration. First, most of the proposed techniques act in an off-line mode. These techniques will be applied on produced alerts set after attack detection and this will cause delay in an appropriate reaction to detected attack. On the other hand, some of these techniques are depended to human analyst for training phase or developing filtering rules. This dependency causes the delay in developing and updating rules. Some researches have deal with these drawbacks and have proposed real-time, adaptive and unsupervised algorithms. But there are some disadvantages about complexity of the technique and size of training set during a system’s lifetime. Another problem associated to some of the proposed researches is the lack of accuracy. Considering that some false positive reduction algorithms may cause low accuracy and miss real-attack alerts, providing an exact evaluation approach to reveal the accuracy of the proposed algorithms can be a promising field of study.

References

[1] R. Base, P. Mell, “Special publication on intrusion detection systems”, NIST Infidel, Inc., National Institute of Standards and Technology, Scotts Valley, CA, 2001.

[2] J. Anderson, “An introduction to neural networks”, Cambridge: MIT Press, 1995.

[3] P.G. Teodoro, J.D. Verdejo, G.M. Fernandez, E. Vazquez, “Anomaly-based network intrusion detection: techniques, systems and challenges”, Computers Security, 2009.

[4] J. Viinikka, H. Debar, L. Mé, A. Lehikoinen, M. Tarvainen, “Processing intrusion detection alert aggregates with time series modeling”, Information Fusion Journal, vol. 10(4), 2009.

[5] R. Vaarandi, “Real-time classification of IDS alerts with data mining techniques”, in Proc. of MILCOM Conference, 2009.

[6] K. Julisch, “Clustering intrusion detection alarms to support root cause analysis”, ACM Trans. Inf. Syst. Secur. 6, 2003

[7] G.C. Tjhai, S.M. Furnell, M. Papadaki, N.L. Clarke, “A preliminary two-stage alarm correlation and filtering system using SOM neural network and K-means algorithm”, Computers & Security 29, 2010.

[8] G.P. Spathoulas, S.K. Katsikas, “Reducing false positives in intrusion detection systems”, computers & security 29, 2010.

[9] J. Viinikka, H. Debar, L. Mé, R. Séguier, “Time series modeling for IDS alert management,” in Proc. Of ACM Symposium on Information, Computer and Communications Security, 2006.

[10] T. Pietraszek. “Using adaptive alert classification to reduce false positives in intrusion detection,” in Proc. of RAID Symposium, 2004.

[11] J. Viinikka, H. Debar, "Monitoring IDS background noise using EWMA control charts and alert information," in Proc. of RAID Symposium, 2004.

[12] K. Das, "Protocol anomaly detection for network-based intrusion detection", GSEC Practical Assignment Version 1.2f SANS Institute, 2001.

[13] F.N. Sabri, N.M. Norwawi, K. Seman, "Identifying false alarm rates for intrusion detection system with Data Mining", IJCSNS International Journal of Computer Science and Network Security, VOL.11, 2011.

[14] S.X. Wu, W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A Review", Applied Soft Computing Journal 10, 2010.

[15] S. Wu, E. Yen, "Data mining-based intrusion detectors", Expert Systems with Applications 36, 2009.

[16] R. Lippmann, J.W. Haines, D.J. Fried, J. Korba, K. Das, "The 1999 DARPA off-Line intrusion detection evaluation", Computer Networks 34 (4), 2000.

[17] J. McHugh, "Testing intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln laboratory", ACM Transaction on Information and System Security 3 (4), 2000.

[18] S.O. Al-Mamory, H. Zhang, "A survey on IDS alerts processing techniques", 6th WSEAS International Conference on Information Security and Privacy, Tenerife, Spain, 2007.

[19] N. B. Anuar, H. Sallehudin, A. Gani, O. Zakari, "Identifying false alarm for network intrusion detection system using hybrid data mining and decision tree", Malaysian journal of Computer Science, Vol. 21(2), 2008.

[20] C. Xiang, P.C. Yong, L.S. Meng, "Design of multiple-level hybrid classifier for intrusion detection system using bayesian clustering and decision trees", Pattern Recognition Letters 29, 2008.

[21] H.T. Elshoush, I. M. Osman, "Alert correlation in collaborative intelligent intrusion detection systems-A survey", Applied Soft Computing 11, 2011.

[22] S. Lee, G. Kim, S. Kim, "Self-adaptive and dynamic clustering for online anomaly detection", Expert Systems with Applications 38, 2011.

[23] C. Clifton, G. Gengo, "Developing custom intrusion detection filters using data mining", MILCOM 2000. 21st Century Military Communications Conference Proceedings, 2000.

[24] K. Julisch, "Mining alarm clusters to improve alarm handling efficiency", Computer Security Applications Conference, 2001.

[25] K. Julisch, M. Dacier, "Mining intrusion detection alarms for actionable knowledge", in: The 8th ACM International Conference on Knowledge Discovery and Data Mining, 2002.

[26] K. Julisch, "Using root cause analysis to handle intrusion detection alarms", 2003.

[27] T. Pietraszek, A. Tanner, "Data mining and machine learning-Towards reduceing false positives in intrusion detection", Information Security Technical Report, 2005.

[28] T. Pietraszek, "Alert classification to reduce false positives in intrusion detection", Germany, 2006.

[29] N.A. Bakar, B. Belaton, A. Samsudin, "false positives reducetion via intrusion alert quality framework", 13th IEEE International Conference on Communication, 2005.

[30] A. Siraj, R.B. Vaughn, "Multi-Level alert clustering for intrusion detection Sensor Data", Fuzzy Information Processing Society, 2005.

[31] J. Long, D. Schwartz, S. Stoecklin, "Distinguishing false from true alerts in snort by data mining Patterns of alerts", SPIE Defense and Security Symposium, USA, 2006.

[32] R. Perdisci, G. Giacinto, F. Roli, "Alarm clustering for intrusion detection systems in computer networks", Engineering Applications of Artificial Intelligence, 2006.

[33] G. Giacinto, R. Perdisci, F. Roli, "Alarm clustering for intrusion detection systems in computer networks", Machine Learning and data mining in Pattern Recognition, Springer, Berlin, 2005.

[34] S.O. Al-Mamory, H. Zhang, "New data mining technique to enhance IDS alarms quality", Springer-Verlag, France, 2008.

[35] S.O. Al-Mamory, H. Zhang, "IDS alarm reducetion using data mining ", IEEE International Conference on Neural Networks, 2008.

[36] S.O. Al-Mamory, H. Zhang, "intrusion detection alarms reducetion using root cause analysis and clustering", Computer Communications 32, 2009.

[37] R. Vaarandi, K. Podins, "Network IDS alert classification with frequent itemset mining and data clustering", IEEE Conference on Network and Service Management, 2010.

[38] Z. Tian, W. Zhang, J. Ye, X. Yu, H. Zhang, "Reduction of false positives in intrusion detection via adaptive alert classifier", IEEE International Conference on Information and Automation, 2008.

[39] F.Maggi, M. Matteucci, S. Zanero, "Reducing false positives in anomaly detectors through fuzzy alert aggregation", Information Fusion 10, 2009.

[40] N. Mansour, M.I. Chehab, A. Faour, "Filtering intrusion detection alarms", Cluster Computing, Springer, 2010.