Reducing False Alarms in Intrusion Detection Systems – A Survey

Milan[1], Hariom Sardana[2], Kamalpreet Singh[3]

[1,2,3]The NorthCap University

Abstract - *Intrusion detection systems (IDSs) are an essential element for network security infrastructure and play a very important role in detecting large number of attacks. They are widely used systems to detect malicious intent activities and various attacks on the internet. Although there are different types of IDS, all these systems suffer from a common problem which is generating high volume of alerts and huge number of false alarms. This lessens the proficiency of the IDS. 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 paper is a compilation of research in this field which reviews existing false alarm minimization techniques in signature-based Network Intrusion Detection System (NIDS).*

***Key Words*: Intrusion detection system, false alarms, root cause analysis, data mining.**

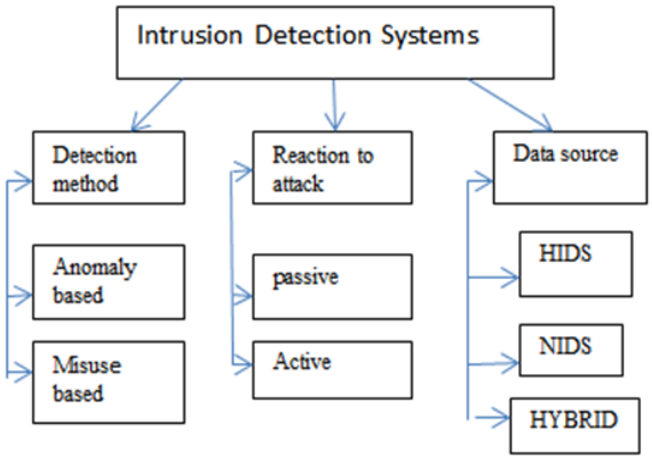
1. INTRODUCTION

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 needs to be carefully monitored and sufficient protection is needed against cyber-attacks. The traditional technology such as firewall is used to defense attacks. Thus, the IDS is usually used to enhance the network security of enterprises. The major difference between firewall and IDS system is that firewall is a manual passive defense system.

An Intrusion Detection System (IDS) monitors the system activity and reports on observation of any security violations. Traditionally there are two broad classes of IDS such as signature- based and anomaly-based. The former uses a database of known attack signatures and raises an alarm whenever network traffic matches any signature , whereas the latter uses a model of normative system behaviour and observable deviations are raised as alarms. The different types of IDS are represented in Fig 1

Although IDS proved their capability of detecting various attacks on the network and become a complete defense-in-depth infrastructure, a big challenge is that it generates huge amount of alarms and maximum of them are false positive alarms. This reduces the efficiency of IDS. Also, a large number of alarms are unmanageable to the human analyst. False positive alarms are the one which are generated when a legitimate activity has been mistakenly considered as malicious by the IDS. In recent years, false alarm rate is used to identify the efficiency of IDSs thus they play a key role in reducing the overall output of these detection systems. Despite that misuse (signature) based IDS produce less false positive alarms when compared with anomaly based IDSs, these false positives are unavoidable. All these reasons attract researchers to find the techniques that can reduce false positives respectively. Many techniques have been proposed for this purpose, such as machine learning, control charts, intelligent false alarm filter etc.

Fig-1: Types of IDS



This paper aims to provide a survey on techniques which are proposed for false positives reduction in IDSs. The review will help future researchers gather knowledge about all proposed techniques from hypothetical perspective and would serve as a quick reference for a person relatively new to the subject.

2. EVALUATION PARAMETERS

Evaluating intrusion detection systems is very important for enhancing the computer security. It provides essential data and conclusions to help developers to improve their IDS and enable users to know the capability and limitations of the IDS which is in use. The effectiveness of an IDS is evaluated by its prediction ability to give correct classification of events to be attack or normal behaviour. According to the real nature of a given event and the prediction from an IDS, four possible outcomes are shown in Table I

Table -1: Parameters for evaluating effectiveness of IDS

Actual Class	Predicted Class	
	Normal	Attack
Normal	True Negative(TN)	False Positive(FP)
Attack	False Negative(FN)	True Positive(TP)

False Positive Rate (FPR)	$= \frac{FP}{FP+TN}$
False Negative Rate (FNR)	$= \frac{FN}{FN+TP}$
True Positive Rate (TPR)	$= \frac{TP}{TP+FN}$
True Negative Rate (TNR)	$= \frac{TN}{TN+FP}$
Accuracy	$= \frac{TP+TN}{TP+TN+FP+FN}$
Precision	$= \frac{TP}{TP+FP}$

False positive rate (FPR) also known as false alarm rate (FAR), refers to the proportion that normal data is falsely detected as attack behaviour. A high FPR will seriously cause the low performance of the IDS and a high FNR will leave the system vulnerable to intrusions. So, to maximize IDS performances, FP and FN rates must be minimized while maximizing accuracy. All the approaches proposed for reducing false positives lack due to a problem that just reducing false positive is not enough. So, effective techniques are required that will reduce the false positive rate while keeping the accuracy to the same or higher level.

3. REVIEW OF VARIOUS TECHNIQUES

Julisch in [1] states that each alarm occurs for a reason, which is referred to as the alarm's root cause. These root causes are persistent and account for over 90% of the alarms that an Intrusion Detection System triggers. So, to remove the most persistent and predominant root causes, a novel alarm clustering method is used to which helps in identifying root cause. Significant improvement is observed if these root causes are eliminated.

Authors in [2] propose a new strategy to perform alarm clustering which produces unified descriptions of attacks from alarms produced by multiple IDS. In order to be effective, the proposed alarm clustering system takes into account two characteristics of IDS: (i) for a given attack, different sensors may produce a number of alarms reporting different attack descriptions; and (ii) a certain attack description may be produced by the IDS in response to different types of attack. Experiments performed in different attack scenarios on a live network showed that the proposed algorithm effectively groups alarms related to the same attack, even though IDS produced alarms whose descriptions were erroneously referred to different types of attacks.

Authors in [3] propose a data mining based method for classification to distinguish serious alerts and irrelevant ones with a performance of 99.9 % in comparison with other recent data mining methods which have reached the performance of 97%. A frequent pattern based outlier detection based method for discovering knowledge from the IDS alert logs and creating alert classifiers from this knowledge in a semi-automated manner has been used in their proposed technique. The result showed that the performance has been enhanced as they reduced the number of alerts to 99.9 % in comparable with the performance of other recent techniques which have reduced the number of alerts by 74-97%.

The research in [4] intends to compare efficiency of machine learning methods in intrusion detection system, including classification tree and support vector machine. Compared with other related works in data mining-based intrusion detectors, the authors proposed to calculate the mean value via sampling different ratios of normal data for each measurement, which lead them reach a better accuracy rate for observation data in real world. They compared the accuracy, detection rate, false alarm rate for four attack types. Moreover, it shows better performance than KDD Winner, especially for U2R type and R2L type attacks.

The study in [5] is aimed at detecting denial of services attack and normal traffic using Knowledge Discovery and Data Mining Cup 99(KDD CUP 99) dataset to reduce the false alarm rates. IDA analyser software is used as it is capable of classifying large amount of data within seconds depending on the speed and condition of computer processors. The results have shown that the data mining technique reduces the false alarm rates and increase the accuracy of the system. In conclusion, this technique has reduced the numbers of false alarm rates and increases the accuracy of the systems.

[6] Also focuses on handling root causes to reduce false alarms in IDS. The authors propose a two-step paradigm for alarm handling. Step one identifies root causes that account for large numbers of alarms, and step two removes these root causes and thereby reduces the future alarm load. To support the discovery of root causes, a novel data mining technique is proposed, called alarm clustering. These experiments show that alarm clustering makes the identification of root causes very efficient. Moreover, the experiments demonstrate that by judiciously responding to root causes one can reduce the future alarm load by 70%, on the average.

In [7], authors present a data mining based real-time method for distinguishing important network IDS alerts from frequently occurring false positives and events of low importance. Unlike conventional data mining based approaches, this method is fully automated and able to adjust to environment changes without a human intervention. With this approach, knowledge is mined from IDS logs and processed in an automated way, in order to build an alert classifier. The classifier is then used in real-time for distinguishing important IDS alerts from frequently occurring false positives and events of low importance.

[8] Demonstrates the use of Computational Intelligence in Intrusion Detection Systems. Characteristics of computational intelligence (CI) systems, such as adaptation, fault tolerance, high computational speed and error resilience in the face of noisy information, fit the requirements of building a good intrusion detection model. The paper take into account some core techniques like artificial neural networks, fuzzy systems, evolutionary computation, artificial immune systems, swarm intelligence, and soft computing. The results show that soft computing has the power to combine the strengths of all the other stated methods in such a way that their disadvantages will be compensated.

Authors in [9] present two orthogonal and complementary approaches(CLARAty and ALAC) to reduce the number of false positives in intrusion detection using alert post processing by data mining and machine learning. The system uses CLARAty in the first stage to periodically mine raw alerts, discover their root causes and either remove them or install alert filters. The output from the first stage would then be forwarded to ALAC interacting with an operator. The main focus of this approach is to improve the quality of alerts and identify true and false positives using alert pre-processing utilizing the expertise of a human domain experts.

In [10], authors focus on the aggregation of IDS alerts which is an important component of the alert fusion process. They exploit fuzzy measures and fuzzy sets to design simple and robust alert aggregation algorithms. Exploiting fuzzy sets, they are able to robustly state whether or not two alerts are ‘‘close in time’’, dealing with noisy and delayed detections. A performance metric for the evaluation of fusion systems is also proposed. The proposal defines simple, but robust criteria for computing the time distance between alerts in order to take into account uncertainty on both measurements and the threshold-distance sizing.

Authors in [11] present a data mining technique based on a Growing Hierarchical Self-Organizing Map (GHSOM) that adjusts its architecture during an unsupervised training process according to the characteristics of the input alarm data. GHSOM clusters these alarms in a way that supports network administrators in making decisions about true and false alarms. Experimental results show that GHSOM reduces false positives from 15% to 4.7% and false negatives from 16% to 4% for the real-world data used.

[12] Proposes a graphical signature for intrusion detection given alert sequences. By correlating alerts with their temporal proximity, it build a probabilistic graph-based model to describe a group of alerts that form an attack or normal behaviour. Using the models, the authors design a pairwise measure based on manifold learning to measure the dissimilarities between different groups of alerts. A large dissimilarity implies different behaviours between the two groups of alerts. The proposed method makes the following contributions: (a) It automatically identifies groups of alerts that are frequent; (b) It summarizes them into a suspicious sequence of activity, representing them with graph structures; (c) It suggests a novel graph-based dissimilarity measure.

Authors in [13] propose a new approach to manage alerts flooding in IDSs. The proposed approach uses semantic analysis and ontology engineering techniques to combine and fuse two or more raw IDS alerts into one summarized hybrid/metaalert. In contrast to previous works this approach ensures that the aggregated alert will not lose any valuable information that exists in the raw alerts set. The experimental results show that the approach is effective and efficient in fusing massive number of alerts comparing to previous works in the area.

3. CONCLUSIONS

This study tries to provide a review of all the research done in the last decade to reduce false positive alarms in IDS. It is noted that all researchers deal with the problem in almost same way. 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. 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.

Despite of reduction in false positives, the methods still need to be improved as they still have weak spots. Also, most of the techniques work in offline mode so there is a need of automated techniques that reduce the false positive in real time, so that the response rate will be more accurate and efficient. Finally, there is a large scope for researchers to reach to the solution that can stop and reduce these false positive to increase the overall efficiency of IDS.

REFERENCES

1. K. Julisch, “Clustering Intrusion Detection Alarms To Support Root Cause Analysis”, ACM Trans. Inf. Syst. Secur. 6, 2003

2. 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

3. Gabra, H.N., Bahaa-Eldin, A.M., Korashy H.:Classification of ids alerts with data mining techniques . In: 2012 International Conference on Internet Study (NETs2012), Bangkok, Thailand, 2012

4. S. Wu, E. Yen, “Data Mining-Based Intrusion Detectors”, Expert Systems with Applications 36, 2009.

5. 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.

6. K. Julisch, "Using Root Cause Analysis To Handle Intrusion Detection Alarms", 2003.

7. R. Vaarandi, "Real-Time Classification Of IDS Alerts With Data Mining Techniques", in Proc. of MILCOM Conference, 2009

8. S.X. Wu, W. Banzhaf, "The Use Of Computational Intelligence In Intrusion Detection Systems: A Review", Applied Soft Computing Journal 10, 2010.

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

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

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

12. H. K Pao, C.H. Mao, H. M Lee, C. D Chen, and C. Faloutsos. An intrinsic graphical signature based on alert correlation analysis for intrusion detection. Journal of Information Science and Engineering, pages 243–262, 2012

13. Saad, S., & Traore, I. (2011). A Semantic Analysis Approach to Manage IDS Alerts Flooding. 7th International Conference on Information Assurance and Security (IAS) (pp. 156- 161). Malacca: IEEE.