ISSN:0975-9646

Reducing False Positive in Intrusion Detection System: A Survey

Neha Gupta[#1], Komal Srivastava[*2], Ashish Sharma[#3]

[#]*Jaypee Institute of Information Technology*

***Abstract*— Intrusion detection systems (IDSs) are widely used systems to detect malicious intent activities and various attacks on the internet, but these frameworks confront a disadvantage of the huge number of alerts and false positive. Furthermore, in this manner lessen the proficiency of the IDS. This problem becomes motivation for many researchers to find the solution to distinguish alerts to less important events and thus reduce false positives. The aim of the study is to contemplate different procedures designed to distinguish real and false alerts and gaining from them the methods and techniques that lessen the generation of false positives. This paper is a compiled review of research in this field and provide a single metric on techniques of reducing false alarms in IDS which help future researchers gather knowledge about all proposed techniques from the hypothetical perspective**

***Keywords*—Intrusion detection system, false positive, alert reduction.**

I. INTRODUCTION

The internet becomes an essential part of the fast growing society. These networks are connected to form a large information society and thus they become vulnerable to various attacks. For securing these networks researchers have found a complete defense –in-depth solution, i.e. Intrusion Detection System (IDS). IDS automate the process of analyzing the network traffic to detect, prevent and react to the attack [1]. It monitors the events on the network, inspect the data and collect evidence of intrusive behaviors. Whenever, it detects suspicious or malicious attempts, an administrator signal reacts instantly.

On the basis of different monitoring and analysis approaches, the different types of IDS are explained by fig. 1. In the detection method, IDS is divided into two categories: misuse and anomaly based detection. Anomaly detection finds the deviation from normal pattern that can lead to the intrusion. While, misuse detection uses well known attack or weak spots of the system to raise alarms and identify intrusion [2].

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 a 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 is 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.

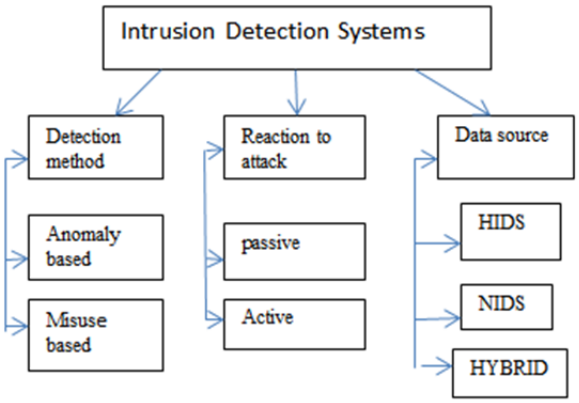


Fig. 1 Intrusion Detection System Characteristics

Despite that misuse based IDS produce less false positive alarms when compared with anomaly based IDSs, these false positives are unavoidable. All these reasons, attracts 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.

The aim of our research is to provide a single metric on techniques of reducing false alarms in IDS which help future researchers gather knowledge about all proposed techniques from hypothetical perspective.

Further, this paper is organized as, section II explains the important measures for evaluating techniques for false positive reduction. In section III, a theoretical review of all proposed techniques is given and last in section IV a brief conclusion is given.

II. MEASURES FOR EVALUATING TECHNIQUES FOR FALSE POSITIVE REDUCTION

The performance and efficiency of IDS are evaluated by various factors such as cost, resource usage, speed, but if the IDS is able to classify the events as normal or event of an attack is the mostly seen parameter [7]. Depending on the nature of a given event and the detection from IDS, we have found four possible outcomes [7, 5].

- True positive (TP): processes which are actually attacks and are successfully detected and labelled as attacks.
- False positive (FP): a normal and legitimate process being classified as attacks.
- True negative (TN): processes which are actually normal and legitimate and are successfully labeled and detected as normal.
- False negative (FN): these are attack events incorrectly classified as normal or legitimate events.

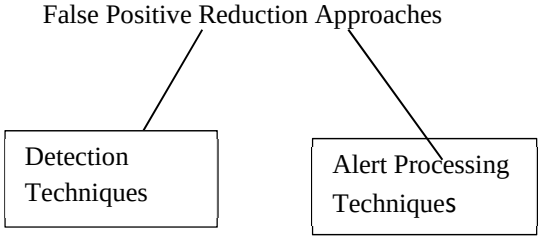
False Positive Rate (FPR)	$= \frac{FP}{FP+TN}$
False Negative Rate (FNR)	$= \frac{FN}{FN+TP}$
True Positive Rate (TPR)	$= \frac{TP}{TP+FN}$
True Negative Rate (TNR)	$= \frac{TN}{TN+FP}$
Accuracy	$= \frac{TP+TN}{TP+TN+FP+FN}$
Precision	$= \frac{TP}{TP+FP}$

Table 1 Parameters for evaluating effectiveness of IDS [11].

False Positive Rate (FPR) specifies to the proportion that legitimate information is mistakenly detected as malicious. It is noted that a high FPR will cause the less effective IDS and a high FNR makes the system vulnerable to intrusions. TNR tells the proportion of detected attacks from all attack events. Next, accuracy with respect to the total events refers to the proportion of events detected or classified as an accurate one [5]. So, to maximize IDS performances, FP and FN rates must be minimized while maximizing accuracy [8]. All the approaches proposed for reducing false positives lacks due to a problem that just reducing false positive is not enough. So, the study says that effective techniques will reduce the false positive rate while keeping the accuracy to the same level or increase up to a certain level.

III. FALSE POSITIVE REDUCTION TECHNIQUES

There are two ways to study the study the false positive reduction techniques as shown in fig. 2. One approach is operated during the detection phase called as a detection technique while the other is operated after detection phase known as alert processing techniques.



A. *DETECTION TECHNIQUES*

We and Ye [5] consider four attack type: U2R, Probe, DOS, R2L and compared their accuracy, the detection rate and false alarm rate. They used C4.5 and SVM algorithms to provide an accurate comparison of above four kinds of attacks. Their analysis shows that C4.5 acts better for probe, U2R and DOS attack, but SVM proved better in false alarm rate.

In 2008, Xiang et al [6] proposed a multiple level hybrid classifier combining the supervised tree classifier and unsupervised Bayesian clustering to detect malicious activity or intrusions. This approach shows low false alarm rates and high detection rates. They concluded that since the false alarm might bring the problem to analysts, the FNR should be kept as low as possible while the FPR maintained at acceptable levels.

Anuar et al. [8]uses training data of KDD Cup99 and proposed a method for detecting and statistical analysis of both attack and normal traffics. The author prepared a hybrid statistical technique based on data mining and decision tree classification. This approach distinguishes between false positives and attacks and thus reduce the misclassification. They prove the importance of decision trees for designing intrusion detection for class of DOS, normal and R2L by comparing decision tree algorithms and rule-based algorithms. Finally, they concluded that for modelling intrusion detection system decision tree is more suitable as compared to rule-based algorithms.

Lee et al. [4]developed a framework for unsupervised training and online anomaly detection. The proposed approach on evaluation shows that it could increase the detection rate significantly while reducing false positive rate, the i.e. it was capable of detecting attacks at the earlier stage only.

B. *ALERT PROCESSING TECHNIQUES*

In 2000, Clifton and Gengo [9] data mining systems on distinguishing successions about the alarms that prone effect from ordinary behavior, empowering development of filters on dispense with the individual alarms. They have investigated those identification of alarm sequences, in place to utilize this learning for making IDS caution filters.

Julisch [10] in 2001 demonstrates that alerts ought to be overseen by distinguishing and determining their main causes. He presented alarm clustering as a technique that supports the disclosure of root causes. Julisch models the alerts as tuples of alert attributes and alert logs are demonstrated as an arrangement of alerts. The scientific categorizations are made for each given property as component trees. The depiction of likeness between alarms given by Julisch depends on characterizing taxonomies. Hence, alerts are assembled and they are compressed by a general alarm. To do as such, a property situated affectation information mining heuristic calculation is actualized. Accordingly, summed up alerts are acquired and this permits, finding the root. Evacuating the reasons, Julisch

demonstrated that future alert burden could be diminished over a 90%.

Later in 2002, Julisch and Dacier [13] mined authentic alarms to figure out how future alerts can be handled more effectively . They research scene rules as to their suitability in this methodology. They have additionally proposed a conceptual clustering method to demonstrate that intrusion detection alerts can be taken care of proficiently by utilizing already mined knowledge. Clusters relate to alert portrayals, and a human master can utilize them in developing correlation rules for future IDS alarms. During their tests, Julisch and Dacier found that these written by hand principles decreased the quantity of alarms by 75% [13]. This work was later amplified by Julisch who reported the decrease of alarms by 87% [16, 12].

Pietraszek[11] proposed Adaptive Learner for Alert Classification (ALAC) as another framework for diminishing false positives. He focuses that foundation learning can be valuable for alert classification. ALAC is a versatile alert classifier based on the input of an interruption discovery investigator and machine-learning strategies. The grouping of IDS alarms is a difficult machine learning issue. ALAC was intended to work in two modes: a recommender mode, in which all alarms are marked and passed onto the examiner, and a specialists mode, in which a few alerts are prepared automatically. In recommender mode, where it adaptively takes in the order from the expert, false negative and false positive were gotten. While in the agent mode, a few alarms are self-sufficiently prepared.

In 2005, Bakar et al. [15] actualize an interruption ready quality system (IAQF), to decrease false positive cautions in IDS. Utilizing this structure, they advance every alarm with quality parameters, for example, rightness, precision, dependability, and affectability. Enhancing alarms with information quality, data help abnormal state ready operations to channel, associate, or investigate the alarms. They additionally standardize improved alarms in IDMEF group.

Siraj et al. [18] have meant to build up a unified alert fusion model which will consolidate alert prioritization, alert clustering and alert relationship in a single system, however, they simply tended to the alert grouping part of sensor information combination in their work. They utilized causal information based derivation strategy with fuzzy cognitive modeling so as to demonstrate to structural connections in sensor information.

In 2006, Long et al. [17] have proposed an administered clustering calculation for recognizing Snort IDS genuine alarms from false positives. Their system utilizes Intrusion Detection Message Exchange Format (IDMEF), which is composed in XML and a novel XML., separation measure is proposed to actualize the clustering calculation taking into account this measure.

Perdisci et al. [14], proposed another technique to perform alert clustering whose primary target is to decrease the volume of alerts created by various IDS sensors and to deliver bound together depictions of attacks from alerts created by different IDSs. Their work is an updated variant of Giacinto et al. [19], where they proposed another on-line alert clustering framework.

In 2007, Al-Mamory et al. have given a study on alert processing procedures [17], later in 2008 they provided a data mining alert clustering strategy that gathers alerts whose root causes are largely comparable and discover generalized alerts which assist the human investigator or analyst to write filters. During their analyses, they found the average value of reducing proportion was around 82% [20], 93% [18] and 74% [21] of the aggregate alerts. Their strategy can be considered as a variety of Julisch's work; on the other hand, they have planned another information mining system, which is diverse in clustering strategies, to lessen alerts load. They guarantee that use of their method to alert log enormously helps the security investigator in distinguishing the underlying drivers and lessening the alert load later on.

In 2009, Vaarandi [22] provided a data mining based real-time order technique for recognizing imperative network IDS alarms from generally occurring false positives and events of low significance. He guarantees that unlike ordinary data mining based methodologies, the system is completely mechanized and ready to acclimate to environment changes without a human intercession. Later in 2010, he amplifies his past work in [21] and presents a novel unsupervised real time alarm system which depends on regular itemset mining and information clustering procedures. In 2010, Tjhai et al. [7]added to a two-stage classification framework utilizing the mix of two data mining strategies: SOM (self arranging guide) neural system and K-means clustering. The first level classification was created to legitimately correlate alerts identified with a specific activity and the second characterizes alerts into classes of genuine and false alerts. Their analyses demonstrate that the proposed framework successfully decreases every single noisy alert, which frequently add to more than half of false alerts produced by a normal IDS. In 2011, Sabri et al. [13] utilized information mining to extricate the helpful data from huge databases. They have utilized the KDD CUP 99 dataset to assess their system. The outcomes demonstrate that the data mining method reduces fal false alarms and increase efficiency of IDS.

IV. CONCLUSION

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 deals with the problem in almost same way. It is reviewed that the problem is the problem is solved by two approaches, one is at the detection phase while the other is applied on generated alerts after the detection phase. From all the studies it is concluded that while some papers proposed different approaches the majority have reduced the false positive in the same way i.e. by alert processing techniques. Correlating alerts improve the efficiency of the IDS. It not only decrease the false positive rate, but also improve the knowledge of attacks on the network. Despite of reduction of false positive, the methods still need to be improved as they still have weak spots.

Another problem is in the process of false positive reduction as same as researchers explained it to be solved by data mining and clustering while others mention it to be a problem of correlation. 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] 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] S.O. Al-Mamory, H. Zhang, "*Intrusion Detection Alarms Reduction Using Root Cause Analysis And Clustering*", Computer Communications 32, 2009.

[4] Sergio Pastrana, Agustin Orfila, "*Randomized Anagram Revisited*", Journal of Network And Computer Applications,MAY 2014.

[5] S. Wu, E. Yen, "*Data Mining-Based Intrusion Detectors*", Expert Systems with Applications 36, 2009.

[6] Wathiq Laftah , Zulaiha Ali OTHman, "*Hybrid Modified K-Means With C4.5 For Intrusion Detection Systems In Multiagent Systems*", THE SCIENTIFIC WORLD JOURNAL · JULY 2015.

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

[8] 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.

[9] Clifton, G. Gengo, "*Developing Custom Intrusion Detection Filters Using Data Mining*", MILCOM 2000. 21st Century Military Communications Conference Proceedings, 2000.

[10] K. Julisch, "*Mining Alarm Clusters To Improve Alarm Handling Efficiency*", Computer Security Applications Conference, 2001.

[11] T. Pietraszek. "*Using Adaptive Alert Classification To Reduce False Positives In Intrusion Detection*" in Proc. of RAID Symposium, 2004.

[12] K. Julisch, "*Using Root Cause Analysis To Handle Intrusion Detection Alarms*", 2003.

[13] K. Julisch, M. Dacier, "*Mining Intrusion Detection Alarms For Actionable Knowledge*", in: The 8th ACM International Conference on Knowledge Discovery and Data Mining, 2002.

[14] 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.

[15] N.A. Bakar, B. Belaton, A. Samsudin, "*False Positives Reducetion Via Intrusion Alert Quality Framework*", 13th IEEE International Conference on Communication, 2005.

[16] K. Julisch, "Clustering Intrusion Detection Alarms To Support Root Cause Analysis", ACM Trans. Inf. Syst. Secur. 6, 2003

[17] 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.

[18] S.O. Al-Mamory, H. Zhang, "*New Data Mining Technique To Enhance IDS Alarms Quality*", Springer-Verlag, France, 2008.

[19] R. Vaarandi, K. Podins, "*Network IDS Alert Classification With Frequent Itemset Mining And Data Clustering*", IEEE Conference on Network and Service Management, 2010.

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

[21] 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.

[22] 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.