Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

False Positives Reduction in Intrusion Detection Systems Using Alert Correlation and Data mining Techniques

[1]El Mostapha Chakir*, [2]Chancerel Codjovi, [3]Youness Idrissi Khamlichi, [4]Mohammed Moughit
[1, 2] Laboratory of Computer Networks, Mobility and Modeling Faculty of Science and Technology University Hassan First Settat, Morroco
[3, 4] Laboratory of Computer Networks, Mobility and Modeling National School of Applied Sciences University Hassan First Settat, Morroco

Abstract— During the last years and with the growth of the cyber-attacks, the information safety has become an essential element. Therefore we must find the best ways to protect our IT system from these attacks. Researchers have proposed different methods and algorithms to improve intrusion detection systems (IDS). There are different types of these systems and all of them are suffering from a common problem which is generating an important number of alerts and huge volume of false positives. This disadvantage has become the main motivation for many researchers in IDS area. The aim of conducted research in this field is to propose different techniques to handle the alerts, to reduce them and distinguish real attacks from false positives and low importance events.
This paper is a survey that represents a review of the current research related to the false positives problem. The focus will be on alert correlation and data mining techniques to reduce false positives.

Keywords— Intrusion Detection System, false positive, data mining, alert correlation, event correlation.

I. INTRODUCTION

Computer networks become an essential part of today's information society. These networks are usually connected to the global internet network and then they become an easy target for attacks. In recent years securing networks against intrusion and attacks has become very important. An intrusion can be defined as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" [1].
Recently, various security systems and tools are deployed in networks to provide security such as Intrusion Detection Systems (IDS). An IDS is used to detect all intrusions in an efficient manner and when it observes any suspicious event representing a threat or abnormal behavior which may result in damaging computer networks and systems it produces alerts.
IDS solutions generate a huge number of alerts which most of them are false alerts, duplicates alerts or low importance. Large volume of these alerts is unmanageable and overwhelming to the human analyst especially if 99% of them are false alerts [2]. False alerts, also known as false positives occur when an activity has been mistakenly classified as an attack by the IDS.
Many approaches have been proposed to reduce the number of false positives. Among proposed approaches, data mining based and alert correlation have been frequently suggested during the last years. This paper aimed to provide a survey on techniques which are proposed for false positives reduction in IDS and the focus will be on data mining based techniques and alert correlation.
This paper is organized as follows: Section II explains the main measures for evaluating different methods for false positives reduction, Section III false positive reduction techniques, Section IV data mining techniques, Section V alert and intrusion correlation techniques, Section VI classification of alert correlation techniques, and Section VII conclusion and future works.

II. EVALUATION PARAMETERS FOR FALSE POSITIVES REDUCTION

The performance of IDS is evaluated by its ability to give a correct classification of events to be an attack or a normal behavior [3]. According to the real nature of a given event and the prediction from IDS, we found four possible outcomes [3, 4]:

- **True negative (TN):** events which are actually normal and are successfully labeled as normal.
- **True positive (TP):** events which are actually attacks and are successfully labeled as attacks.
- **False positive (FP):** a normal events being classified as attacks.
- **False negative (FN):** are attack events incorrectly classified as normal events.

Table 1 shows some numerical parameters that apply following measures to evaluate the IDS effectiveness:

Table 1: Numerical parameters to evaluate the IDS effectiveness [11]

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) refers to the proportion that normal information is mistakenly detected as attack behavior. A high FPR will cause the low performance of the IDS and a high FNR will leave the system vulnerable to intrusions. TNR 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 [4]. So, to have IDS with high performances, both FP and FN rates should be minimized together with maximizing accuracy, TP and TN rates [5].

The most important issue about evaluating different approaches which are proposed to reduce false positives is that reducing just false positive rate and that is not enough. Some false positive reduction techniques 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.

III. FALSE POSITIVES REDUCTION TECHNIQUES

Many methods have been proposed to reduce false positives rate. All these methods can be divided into two 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.

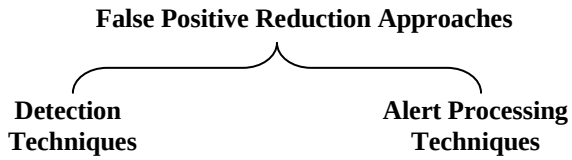

Fig. 1 General FP Reduction Approaches [18]

III-1 Detection Techniques

Wu and Ye [4] compared the accuracy, false positive rate and detection rate for four attack types: Probe, Dos, U2R, R2L. They provide accuracy comparison by C4.5 and SVM algorithms. As a result, C4.5 acts better than SVM in accuracy of Probe, DoS and U2R attacks detection; but SVM is better in false positive rate. They suggest combining the two methods, so that overall accuracy can be increased greatly.

Anuar et al. [5] prepared a hybrid statistical approach which used data mining and decision tree classification. As a result, the statistical analysis approach can be manipulated to distinguish between attacks and false positives and reduce misclassification of false positives. They compared rule-based and decision tree algorithms and proved that the decision tree is better than rule-based for modeling intrusion detection systems.

Xiang et al. [6] 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 positive rates. They concluded that keeping FNR as low as possible while maintaining an acceptable level of FPR is essential for IDS since the false positive might bring inconvenience to the administrators.

Lee et al. [8] 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 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.

III-2 Alerts Processing Techniques

Pietraszek [11] proposed Adaptive Learner for Alert Classification (ALAC) as a new system for reducing false positives. ALAC is an adaptive alert classifier based on the feedback of an intrusion detection analyst and machine learning techniques. 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. In this system, a fast and effective rule learner used is RIPPER. It can build a set of rules discriminating between classes. The number of false alerts was reduced by more than 30%. This system has a

disadvantage: during a system's lifetime the size of the training set grows infinitely. Later, he extended his previous work in [12] 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 [12]. Using this system, the number of alerts handled has been reduced by more than 50%.

Julisch and Dacier [10] proposed a conceptual clustering technique to show that intrusion detection alarms can be handled efficiently. 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, they 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].

Clifton and Gengo [9] used data mining techniques to identify sequences of alarms that 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.

Siraj et al. [13] developed 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.

Al-Mamory et al. have provided a survey on alert processing techniques [15], later 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 [16, 17, 18]. During their experiments, the averaged reduction ratio was about 82% [16], 93% [18] and 74% [19] 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.

Long et al. [14] have proposed 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.

Maggi et al. [22] 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.

Vaarandi [19] 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 he extends his previous work in [20] and presents a novel unsupervised real time alert classification method which is based on frequent item set mining and data clustering techniques.

Mansour et al. [23] 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.

Tian et al. [21] 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.

Sabri et al. [24] 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.

Table 2: A review of false positive reduction techniques [18]

	Researches	**False Positive Reduction Techniques**	**Results**	
Detection Technique	4	SVM	1%	**False Positive rate**
	4	C4.5	1.44%	
	5	Decision Tree Classification ,Rule-based Classification	3.2%	
	6	Decision tree Classification , Bayesian Clustering	N/A	
	8	Self-Organizing Map , K-means Clustering	0.91-2.43%	
A lert Processing Techniques	9	Sequential Association Mining	N/A	**False Positive ratio**
	10	Clustering (Attribute Oriented Induction)	75%,87%	
	11,12	Machine-Learning (ALAC), Clustering (CLARAty)	30%,50%	
	14	Clustering (IDMEF based on xml distance measure)	N/A	
	16,17,18	Clustering , root cause analysis	82%,93%,74%	
	19,20	Classification (Frequent Itemset Mining) ,	81-	

		Clustering	99%,43,31%	
	21	Classification (Pattern Mining)	36%	
	23	Clustering , GHSOM	15%,4.7%	
	24	Rule-based Classification, KDD CUP 99	N/A	

IV. DATA MINING TECHNIQUES

Data Mining is to extract knowledge interested by people from large database or data warehouse; the knowledge is implied, unknown and potentially useful information. Extracted knowledge is represented as concept, rule, law and model. The purpose of data mining is to help the decision-maker to find potential association between data, found neglected elements which are perhaps very useful for trends and decision-making behavior.

According to [37], common data mining methods and technologies are:

A. Correlation Analysis: also called association rules, it is to find item set model knowledge frequently appeared from given data set, the purpose is to excavation the relationship that was hidden in data, for example, the customers that buy computer will buy some software, this is an association rules.

B. Sequential patterns: the purpose is also to excavate connection that between data, however, time series analysis focused more on the relationship of data in times, for example, and 80% people among printer buyer will buy printing paper after three months.

C. Classification: classification is to find model or function that can describe the typical characteristics of data set, so that it can identify ownership or categories of unknown data. Typical classify models have the linear regression model, the decision tree model, the model based on rule and the neural network model.

D. Clustering: Data was divided into a series of meaningful subset according to certain rules. In the same cluster, the gap between the individual is smaller, and in the different cluster, the gap is greater.

E. Deviation analysis: to find abnormal data from the database

F. Forecast: to find law according historical data, establish model, and to predict types, characteristics of the future data, etc based on the model.

V. ALERT AND INTRUSION CORRELATION TECHNIQUES

According to [25], alert is defined as an alarm generated by Intrusion Detection system (IDS) to notify interested parties of interesting event. An event is a low level entity analyzed by IDS. Single event can cause multiple alerts and it can be represented in mathematical expression as below:

$$Event = \{alert1, alert2, alert3,\ldots, alertn\}$$

Intrusion correlation refers to the interpretation, combination and analysis of information from all available sources about the target system activity for the purpose of intrusion detection and response. There are two types of intrusion correlation as in Fig. 2: intrusion event correlation and intrusion alert correlation [26].

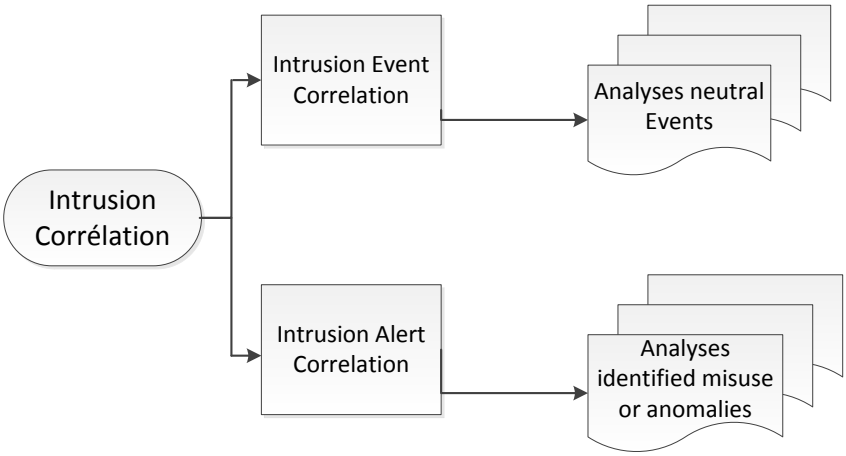

Fig.2 Types of intrusion Correlation

The difference between these two types of intrusion correlations is that intrusion event correlation analyses neutral events, while intrusion alert correlation analyses identified misuse or anomalies. This relation is also stated in IDMEF specification [27] specifying that each time an analyzer detect an event that match the rule, it sends an alert to its manager(s). It will depend on the analyser as an alert message can correspond to a single detected event, or multiple detected events.

Alert can be produced from various types of sources and it may cause multiple stages of attack. Alert correlation is multi-step processes that receives alerts from one or more IDS as input and produce a high-level description of the malicious activity on the network. According to [25], to achieve good recognition, the data needs to be collected from various sources (for example firewall, web server logs, IDS of multiple manufacturers and so on). Correlation of alerts produced by heterogeneous log resources can provide a number of potential advantages and the most obvious benefit is the reduction in the number of alerts that a security officer must address.

VI. CLASSIFICATION OF ALERT CORRELATION TECHNIQUES

There are three techniques exist in correlating alerts which are Similarity-based, Pre-defined attack scenarios and Pre-requisites and consequences of individual attack [28]. In addition, [29] has proposed one more technique for alert correlation, known as Statistical causal analysis (Fig. 3).

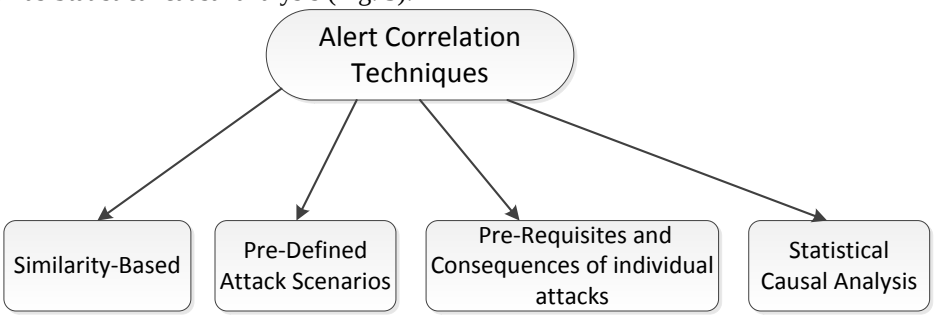

Fig. 3 Classification of Alert Correlation Technique

VI-1 Similarity-Based

This technique will compare an alert to all alert threads that have similar attributes or features (e.g source IP address, destination IP address, ports) and then correlates alerts with a high degree of feature similarity if match or a new thread is created if none is match [30, 31].

Valdes & Skinner [31] implemented alert similarity metric in three phases as in Fig. 4. In the first phase, the low-level events are aggregated using the attack threads concepts to cluster alert that are part of the same ongoing attack. The alerts are clustered if attribute is overlap which mean that it will only consider attributes that present in both alerts. The metric for this phase demand that sensor field, attack class, attack name, source and target in both alerts are similar. In second phase, different levels of similarity are expected for different attributes in different situation whereby similar sensor field is dropped and similar alert name is maintained. This phase is to ensure that detection of the same attack by multiple sensors should be fused.

Then in third phase, it requires similar attack class in both alert. Certain threshold is adjusted for example for synthetic threads, sensor id and IP is set high and for multistep attack detection, threshold for attack class is set to low. This phase will merge alerts representing different attack steps to provide a higher-level view of the security state of the system.

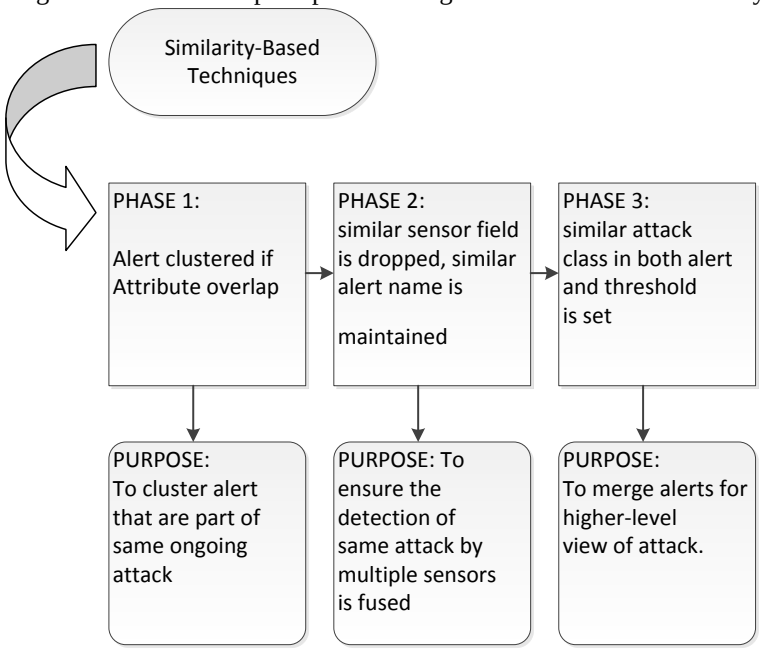

Fig. 4 Similarity-based intrusion alert correlation process by Valdes & Skinner

VI-2 Pre-Defined Attack Scenarios

Debar & Wespi [32] presented a detailed alert model and developed adapter modules to map proprietary alert formats into this model. This alert model was refined and is now the de-facto format for intrusion detection alerts known as Intrusion Detection Message Exchange Format (IDMEF). They have proposed a system that performs correlation and aggregation of intrusion detection alerts produced by various sensors as in Fig. 5. In correlation phase, there are two types of correlation which are duplicate removal and consequence correlation. Duplicates removal are instances of the same attack as detected using rules read from a specified configuration file by two different sensors. Consequences are rules that specify one event should be followed by another type of event. It will link together alerts that are sequential in nature. Once alerts have correlated, aggregation phase will cluster alerts with similar attributes (source, target and attack

class). It identifies the source of the attack, the target of the attack and popular attack class. It will group alerts based on certain criteria to aggregate severity level, reveal trends and clarify attacker's intentions. This phase consists of large number of false positive. However there is no specific technique can eliminate this problem. Major weakness of this method is it requires that human users specify attack scenarios and it is limited to detection of known attacks.

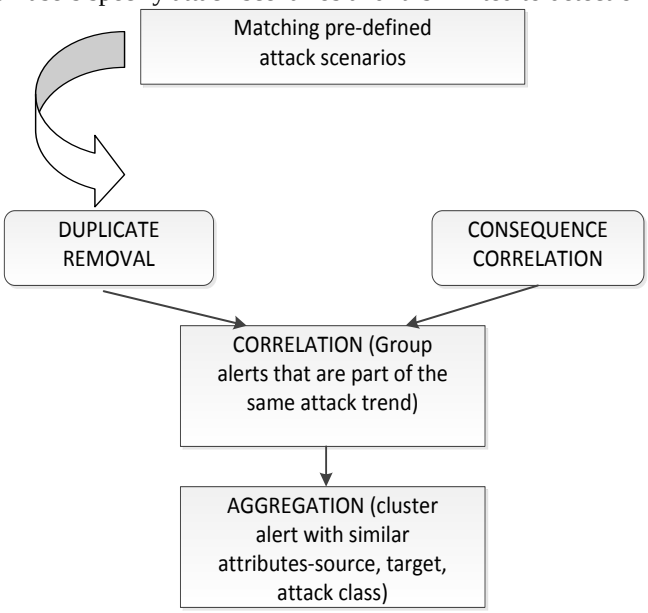

Fig. 5 Pre-defined attack scenarios intrusion alert correlation process by Debar & Wespi

VI-3 Pre-Requisites and Consequences of individual attacks

By using these techniques as depicted in Fig. 6, Cuppens & Miege [33] included five functions including alert base management, alert clustering, alert merging, alert correlation and intention recognition function. In alert base management function, it receives alerts generated by IDS and stores them for further analysis by cooperation module. This alert will be normalized to IDMEF format and store in the relational database. Alert cluster and alert merging function can access the database and will use the similarity function to cluster and merge the alert. Alert correlation function will further analyses the cluster alerts provided by alert merging function using explicit correlation rules with pre-defined and consequence statement. This approach attempt to generate correlation rules automatically which can introduce correlated alerts that are similar by chance and this could increase the noise in the alert stream. [34], [35] has implemented causal relationships between alerts using pre-requisite and consequences.

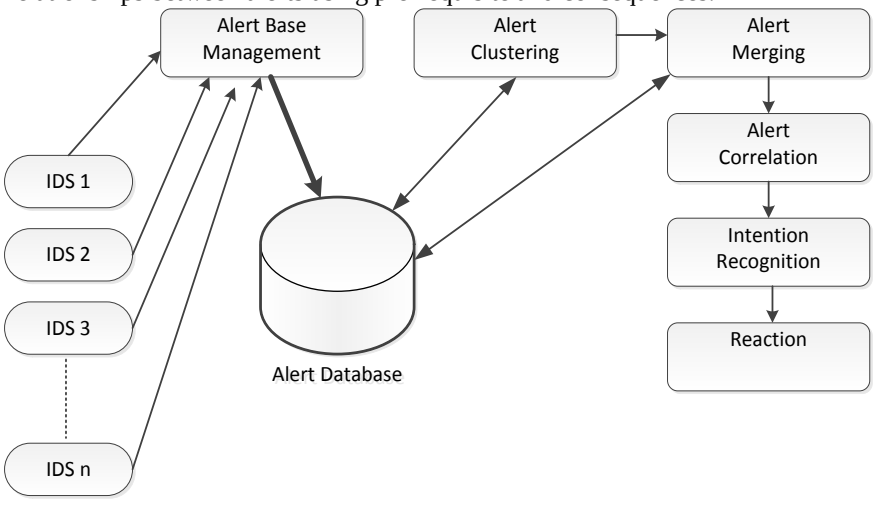

Fig. 6 Pre-requisite and Consequences of individual attack intrusion alert correlation process by Cuppens & Miege

VI-4 Statistical Causal Analysis

This technique proposed by Cuppens & Miege [29] as shown in Fig. 7, implements anomaly detection and use Granger Causality Test (time series analysis method) to correlate events which emphasis on attack scenario analysis. In order to reduce the volume of raw alerts, it will combine low-level alert based on alert attributes. It uses clustering technique to process low-level alert-data into high-level aggregated alerts. Prioritization alerts is used based on relevance of attacks and impacts on the mission goal. It will then conduct causality analysis to correlate alerts and constructs attack scenario. It is pure statistical causality analysis and does not need pre-defined knowledge about attack scenarios. Hence, new attack scenarios can be identified.

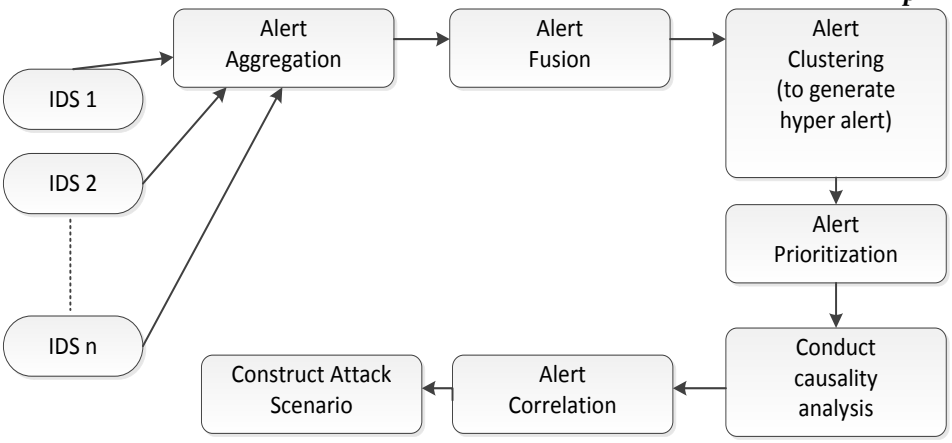

Fig. 7: Statistical Causality Analysis alert correlation process by Qin & Le

This technique declares that every multi-step attack will generate alert that have statistical similarities in their attributes, and this attack steps have causal relationship. [29] run the statistical correlation engine offline with training datasets to compute and store correlations so that it can be used for pattern matching at run-time. This technique is not a feasible solution for the complete correlation process. However it can be utilized as a part of a larger system to pre-process alerts or to provide meta-alert signatures.

VI-5 Alert Correlation Techniques Comparison

All reviewed techniques have their advantages and disadvantageous as summarized in Table 3.

Table 3: Alert Correlation Techniques Comparison [38]

Technique	Advantage	Advantage
Similarity-based	Can reduce large number of redundant alert generated by multiple sensors.	• False alert can only be detected if multiple sensors can detect the same attack. • Cannot detect multi-step attack • Can detect only misuse detection and not
Pre-defined attack scenario	Can reduce large number of redundant alert generated by multiple sensors • Can cluster multiple related alert (contextual alert) • Can detect precise attack as stated in the rules (specification).	• Could generate large number of false positive alarm [36] • it requires that users specify attack scenarios manually • It is limited to detection of known attacks or misuse detection and not anomaly detection. • multi-step attack alert is disregarded
Pre-requisites and Consequences of individual attack	Multi-step attack can be detected to provide a high-level view of the attack associated with a security compromise • [34] generate useful graph to determine the attacker's objective	Automatic generation correlation rules can generate large false alarm [33].
Statistical Causality Analysis	does not need pre-defined Knowledge about attack scenarios. • Using anomaly detection technique • new attack scenarios can be identified • can be used as pre-process alerts or meta-alert signatures.	Not feasible for complete correlation process [25].

VII. CONCLUSION AND FUTURE WORK

In this paper we have provided a review of researches during the last decade, which have aimed to reduce false positives. The focus was on data mining and alert correlation techniques. Firstly we have categorized these researches into two general approaches: the detection techniques that act during detection phase and the alert processing techniques that are applied on generated alerts after detection phase. Secondly we have reviewed and analysed the existing alert correlation and data mining technique to overcome the IDS's problems discussed.

There are some open problems and disadvantages related to the studied techniques. First, most of the proposed techniques act in an off-line mode. Second, some of these techniques are depended to human analyst for training phase or developing filtering rules. Another problem associated to some of the proposed techniques is the lack of accuracy.

By studying all these techniques and detecting there weakness, we aim to proposed a new approach using a SIEM system which combine between the data mining and alert correlation techniques to improve the IDS system to reduce the false positive rate, the next work will be the subject of a future article.

REFERENCES

[1] Anita Rajendra Zope et al , International Journal of Computer Science & Communication Networks,Vol 3(3),182-186 J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

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

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

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

[5] 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

[6] 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.

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

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

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

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

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

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

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

[14] 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

[15] 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

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

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

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

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

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

[21] 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

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

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

[24] 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

[25] Hattala, A., Sars, C., Addams, R., & Virtanen, T. (2004). Event Data Exchange and Intrusion Alert Correlation in Heterogeneous Networks. 8th Colloqium for Information Systems Security Education. West Point, New York

[26] Gorton, D. (2003). Extending Intrusion Detection with Alert Correlation and Intrusion Tolerance. MPhil Thesis , Chalmers University of Technology, Department of Computer Engineering, Goteborg, Sweden

[27] Curry, D., & Debar, H. (2007, March). Intrusion Detection Message Exchange Format. Retrieved July 7, 2008, from IETF: http://www.rfc-editor.org/rfc/rfc4765.txt

[28] Zhai, Y., Ning, P., & Xu, J. (2005). Integrating IDS alert correlation and OS-level dependency tracking. North Carolina: North Carolina State University.

[29] Qin, X., & Le, W. (2003). Statistical Causality of INFOSEC Alert Data. Proceedings of Recent Advances in Intrusion Detection.

[30] Julisch, K. (2001). Mining Alarm Clusters to Improve Alarm Handling Efficiency. Proceedings of the 17th Annual Conference on Computer Security Applications. New Orleans, LA

[31] Valdes, A., & Skinner, K. (2001). Probablistic Alert Correlation. Proceedings of the Recent Advances in Intrusion Detection (RAID).Davis, CA.

[32] Debar, H., & Wespi, A. (2001). Aggregation and Correlation of Intrusion Detection Alerts. Proceedings of the International Symposium on Recent Advances in Intrusion Detection, (pp. 85-103). Davis, CA

[33] Cuppens, F., & Miege, A. (2002). Alert Correlation in a Cooperative Intrusion Detection Framework. Proceedings of IEEE Symposium Security and Privacy.

[34] Ning, P., Cui, Y., & Reeves, D. (2002). Analyzing Intensive Intrusion Alerts via Correlation. Proceedings of the International Symposium on the Recent Advances in Intrusion Detection, (pp. 74-94). Zurich, Switzerland.

[35] Ning, P., Cui, Y., & Reeves, D. (2002). Constructing Attack Scenarios through Correlation of Intrusion Alerts.Proceedings of the ACM Conference on Computer and Communications Security, (pp. 245-254). Washington D.C.

[36] Valeur,F., (2006). Real-time Intrusion Detection Alert Correlation. PhD Thesis, University of California Santa Barbara, USA.

[37] Sharada K A et .al IJARCSSE International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 8, August 2012

[38] Robiah Yusof et .al IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.9, September 2008

