UNIVERSITY OF SOUTHAMPTON

Faculty of Engineering and Applied Science

School of Electronics and Computer Science

A supplementary progress report submitted for continuation towards a PhD

Supervisors: Ed Zaluska and Dr. Nick M. Gibbins

Examiner: Prof. Mark S. Nixon

FALSE ALERT REDUCTION SYSTEM USING OUTLIER DETECTION METHODS

by Iwan Syarif

September 15, 2010

False Alert Reduction System (FARS) Using Outlier Detection Methods

1. Introduction

1.1. Overview

An Intrusion Detection System (IDS) is a security mechanism that can intelligently monitor computer systems and networks to detect intrusions in real time, and then respond to attacks quickly and effectively. An IDS is an important tool to defend against computer attacks and is considered to a key defence in a secure network. However, the typical IDS still has significant limitations such as generating a high number of false positive alerts. Alerts are generated from multiple sensors and may also be derived from multiple proprietary systems or different types of IDSs. An IDS typically does not have the ability to ensure that all alerts reflect actual or real attacks. The high volume of false positive alerts is a significant problem in network security because it becomes very difficult for network administrators to analyze alerted security incidents. Furthermore, reactions to dangerous attacks are often delayed, because the true alerts are hidden in huge amounts of false positive alerts. Therefore, a key topic in the current research into intrusion detection has been focused on the post-processing of IDS alerts, in order to produce more meaningful alerts which will be significantly more useful to a human analyst.

1.2. Research Problems

Lippmann (Lippman,2000) reported that more than 99% of IDS alerts are false positive or repetitive. Surveys by (Zurutuza,2004; Sadoddin,2006) reported that since the year 2000 IDS research has focused on how to handle alerts. The main objectives of this recent research have been how to reduce the amount of false alerts, to study the cause of these false positives, to create a higher-level view or scenario of the attacks, and finally to provide a coherent response to attacks which understands the relationship between different alarms. Alert correlation is the term now being used for the overall process which takes as input the alerts produced by one or more IDSs and provides a more succinct and high-level view of security intrusions in a form suitable for human monitoring and possible action (Kruegel,2005).

A number of research studies have already been conducted in alert correlation systems, but significant unsolved problems still remain:

1. An alert correlation system should significantly reduce the number of false alerts, intelligently analyze the alerts and correctly identify the attack strategies. Most of the proposed approaches have limited capabilities because they rely on predefined knowledge of attacks. This means that these approaches cannot recognize a correlation between IDS alerts when an attack is new or the relationship between attacks is new (Kruegel, 2005).
2. It is obvious that the number of potential correlations is very large and it is computationally infeasible to predict all possible matching conditions between attacks. Therefore, it is very important to develop new alert correlation algorithms with

improved performance that are able to discover new and complex attack sequences (Qin, 2004).

3. Most current alert correlation approaches usually need a significant amount of labelled training data or domain knowledge to build their alert reduction model. However such data is often difficult to obtain (Xiao, 2010).
4. Adaptation to new environments and changes of an individual environment is another important challenge in this area. Most current approaches are unable to adapt to new configuration easily (Xiao, 2010).

1.3. Research Objectives

In order to address the problems described above, I propose a False Alert Reduction System (FARS) which is able to identify the true alerts and to reduce IDS false positive alerts efficiently and also be able to analyze the root cause of false alerts. The proposed method is based on an unsupervised data mining technique called outlier detection. This approach does not need domain knowledge and labelled training data, more over it requires relatively little human assistance.

1.4. Research Contributions

In this research, I will make the following contributions:

1. I will propose a FARS which not only be able to reduce IDS alerts efficiently, but also be able to analyze the root cause of false alerts.
2. I will study the effectiveness of the apriori algorithm for root cause analysis then investigate its weaknesses and finally I will improve its performance.
3. I will implement a FP-Outlier algorithm, which is a relatively new algorithm to detect outliers which represent possibly real intrusions, then compare its performance to several other outlier detection approaches. I will also analyze the advantages and disadvantages of the FP-Outlier algorithm and improve its performance.
4. I will test the robustness of my proposed FARS on various simulated intrusion data sets and provide a novel practical interpretation of the results using reduction rates, completeness and soundness.
5. Finally, I will also test the performance of my proposed FARS on the real network traffic inside the University of Southampton

1.5. Organization of the Report

This report is organized into 4 chapters. In chapter 2, I will describe the current researches on false alert reduction, outlier detection and root cause analysis. In chapter 3, I propose a False Alert Reduction System (FARS) that I will adopt based on the apriori algorithm and the outlier detection approach and finally chapter 4 consists of conclusions and my overall plan to cover the next six months.

2. Literature Review

2.1. Research on False Alert Reduction

False Positives Reduction is a technique that can be used to combine repetitive alerts, reduce the number of false alerts and abstract high-level attack scenarios from a large collection of low-level intrusion alerts (Spathoulas, 2010). The first step of false alert reduction is to remove the alarms that are known to be of no interest then the most frequent alerts need to be investigated. These may be an indication of misconfigurations, software bugs, denial of service (DoS) attacks or virus/worms.

Several approaches have been applied in the field of false alert reduction. (Pietrazek, 2004) uses data mining techniques to build an alert classifier based on feedback from a human analyst. This approach firstly generates training examples based on the analyst feedback. Then these examples are used with a machine learning technique called RIPPER to build and subsequently update the classifier. Finally the classifier is used to process new alerts. This method can classify alerts automatically, but it requires labelled training which is difficult to obtain and also expensive. The need for human interaction is always an additional practical difficulty for an IDS platform to be effective. (Alshammari, 2007; Xiao, 2010) use a somewhat similar approach to Pietrazek, but they use different approaches, Alshammari adopts Neural Networks and Fuzzy Logic to reduce false positive alerts while Xiao use data mining approach to reduce false alerts and root cause analysis.

(Julisch, 2003) proposes a model based on conceptual clustering to connect clusters of false positives to root causes in order to eliminate them. It first generalizes alerts according to generalization hierarchies built from each alert attribute, and then the final generalized alerts are presented to users to assist in root cause analysis. This method firstly discovers and understands the root causes of IDS alerts. Then according to these causes, the alerts triggered by attacks can be distinguished from those triggered by benign events.

(Alharby, 2005) reduce the false alerts rate by classifying the alerts sequences into two patterns classes, continuous and discontinuous. While the continuous patterns represent the real alerts, the discontinuous patterns reflect the sequences mixed with noisy data. (Valdes, 2001) used the minimum similarity specification to fuse alerts from multi-sensors. These clustering algorithms do not require prior knowledge, can integrate alerts with high similarity, reduce the number of alerts and discover new attacks. However, it is difficult to calculate the similarity value between alert attributes to detect attack scenarios.

2.2. Outlier Detection Approach

Outlier detection is a relatively new data mining technique which has attracted many researchers recently. Outlier detection refers to the problem of finding patterns in data that do not conform to expected behaviour and the technique is able to identify abnormal data in large datasets. Outlier detection has already been used in a wide variety of applications such as fraud detection (for credit cards, insurance or health care), intrusion detection for cyber security, fault detection in safety critical systems and military surveillance for enemy activities. In the field of network security, many researchers have already successfully implemented outlier detection to detect intrusions or network anomalies. However, to the best of my knowledge it has not been applied in alert reduction and alert correlation. In fact, compared with false positives (which are the majority of IDS alerts), true alerts are outliers. I believe that the outlier detection technique can also be used to filter and correlate IDS alerts.

Most of current false alert reduction methods such as (Pietraszek,2004; Alshammari,2007; Julisch, 2003 and Alharby,2005) can obtain true alerts only after removing all false positives or clustering all alerts. These approaches need longer processing time because the number of false alert is so much higher than the true alerts. In this case, the use of outlier detection technique can directly identify the outliers (true alerts), hence it can improve the overall IDS performance significantly.

2.3. Root Cause Analysis

Root cause analysis is a method that studies the root causes of the false alarms. This method makes use of the alarm history to refine future alarm quality. The root cause analysis approach which is firstly proposed by (Julisch,2003), analyzes IDS output to detect alarms that almost always have similar features. These similar alarms can be clustered together using some specific algorithms to extract patterns from each cluster. The extracted patterns assist the security analyst in specifying the root causes behind these false alarms and in writing accurate filtering rules. Root cause analysis has been used to identify the most basic factors that contribute to an incident. In other words, root cause analysis is essentially a tool designed to help security analysts describe what happened during a particular incident, to determine how it happened, and to understand why it happened. The key concern is to learn from past failures and avoid similar incidents in the future (Al-Mamory, 2009).

The frequent alert sets will be treated as the normal behaviour. (Vaarandi,2009) reported that most alerts are triggered by only a few signatures. He stated that around ten of the most prolific signatures produced 85%-96% of the alerts; furthermore just five signatures produced 68% of the total alerts. These pattern describe the majority of alerts that will appear again in the future (these can be then classified as *routine alerts*) and produce high false positive alarm. The apriori algorithm can be used to handle this problem.

3. Proposed Methods

In my research I propose to develop a FARS which has two functions. The first function is designed to detect outliers which possibly represent true attacks/intrusions. The second function is designed to analyze the root cause of false alerts. These approaches will work on unlabelled data and minimize the use of human assistance. The apriori algorithm will be used to build frequent-item sets and generate association rules to model the false positive alerts. This method assumes that the most frequent alerts are the most likely to be generated from normal network activities.

3.1. False Alert Reduction System (FARS) Design

My FARS design will extend the work of (Pietrazek,2004) and (Xiao, 2010). In my research, I propose to divide the FARS into two parts: the learning phase and the implementation phase. The goal of the learning phase is to build a false alert reduction classifier and to find outliers which possibly identify real attacks. The apriori algorithm will be used for mining frequent alerts. These item sets are regarded as the features of false positive alerts. The false alert classifier will be used as a false alert filter in the online implementation and the true alerts will be investigated by a security analyst to update the IDS knowledge-base. The learning phase is described in Figure 2.1. below.

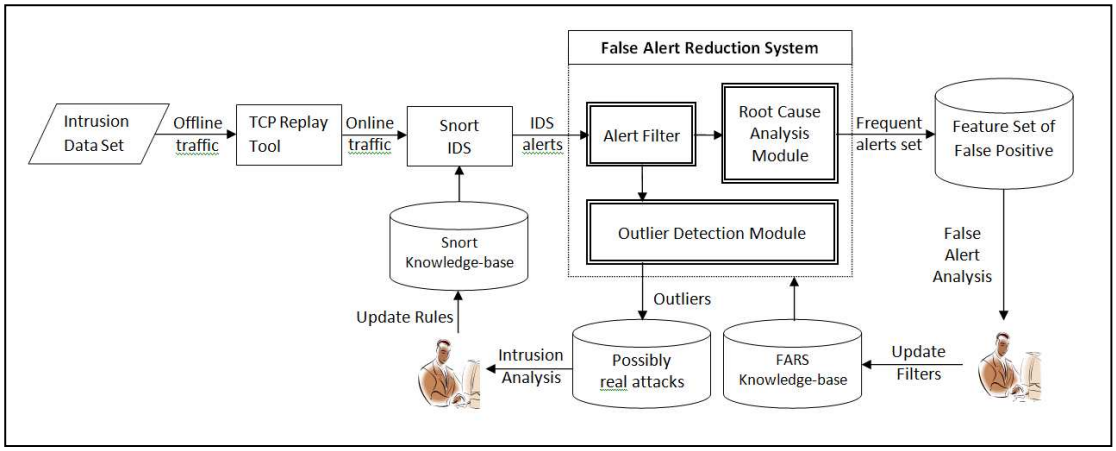

Figure 3.1. FARS Design: Learning Phase

In the implementation phase, the alert classifier will be used on a real network to analyze all IDS alerts. The false positive alerts will directly be discarded while the true alerts will be sent to a security analyst for further investigation. The implementation phase is described in Figure 2.2. below.

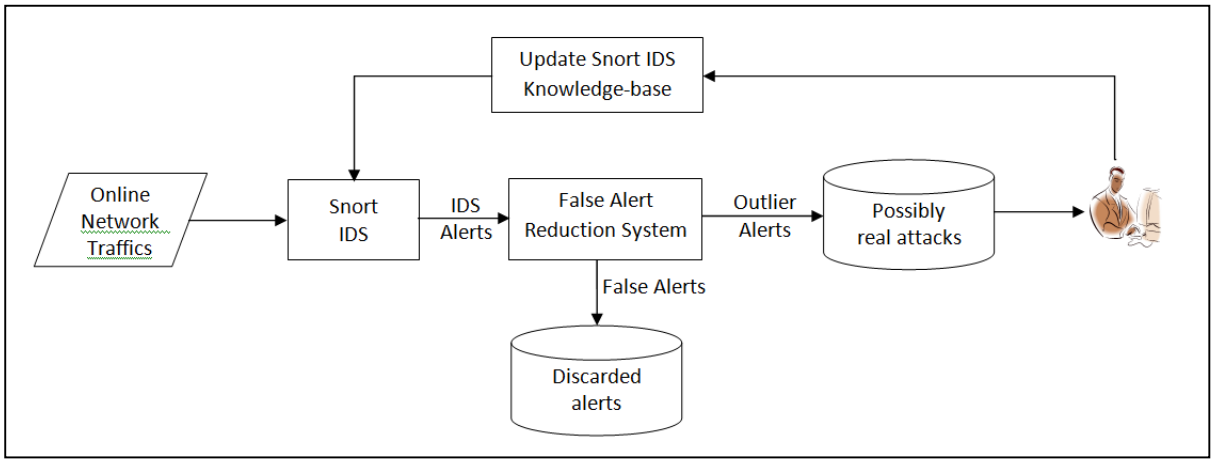

Figure 3.2. FARS Design: Implementation Phase

3.2. Root Cause Analysis Module

The goal of root cause analysis module is to build feature set of false positive alerts. A number of algorithms can be used to mining frequent patterns from IDS alerts but in the first stage of my research I will use the apriori algorithm because it is very simple and is widely used by many researchers.

3.2.1. Apriori Algorithm

Apriori is an algorithm proposed by R. Agrawal and R Srikant in 1994 (Agrawal and Srikant, 1994) for mining frequent item sets for boolean association rules. Apriori is designed to operate on databases containing transactions. As is common in association rule mining, given a set of *itemsets*, the algorithm attempts to find subsets which are common to at least a minimum number C (confidence threshold) of the itemsets. Apriori uses a bottom up approach, where frequent subsets are extended one item at a time (a step known as *candidate generation*), and groups of candidates are tested against the data. The algorithm

terminates when no further successful extensions are found. Usually, the problem of mining association rules can be divided into two phases: Phase one, developed by the users in accordance with the minimum degree of support from the database to find a frequency greater than or equal to the minimum support of all frequent item sets; and phase two which is generated by the first phase of the project set to produce frequent association rules (Goswami, 2010).

3.2.2. Apriori Algorithm Pseudo code

Given a data set, the problem of association rule mining is to generate all rules that have support and confidence greater than a user-specific minimum support and minimum confidence respectively. Candidate sets having k items can be generated by joining large sets having k-1 items, and deleting those that contain a subset that is not large (where large refers to support above minimum support). Frequent sets of items with minimum support form the basis for deriving association rules with minimum confidence. For A=> B to hold with confidence C, C% of the transactions having A must also have B.

The apriori algorithm pseudo code is explained below:

C_k: Candidate itemset of size k
L_k: frequent itemset of size k

L_1= {frequent items};
for (k= 1; Lk!=∅; k++) **do begin**
  C_{k+1}= candidates generated from L_k;
  for each transaction t in database do
    increment the count of all candidates in C_{k+1}
    that are contained in t
    L_{k+1}= candidates in C_{k+1} with min_support
  end
return $\cup_k L_k$;

3.2.3. Improving the Apriori Algorithm

The apriori algorithm has some recognised limitations (Han,2000;Goswami,2010):

1. It may need to generate a huge number of candidate sets. For example, if there are 10^4 frequent 1-itemsets, the apriori algorithm will need to generate more than 10^7 candidate 2-itemsets and accumulate and test their occurrence frequencies.
2. This algorithm needs to repeatedly scan the database and check a large set of candidates by pattern matching. Hence the apriori algorithm can be inefficient when mining longer patterns.
3. The apriori algorithm does not consider the order of items in item sets. In the false alert reduction problem, each IDS alert is an item sequence the appearance of current item may depend on any item before it and it does not depend on the item after it. More-over many items can occur repeatedly.

In the next stage of my research (after submitting mini thesis), I will improve the apriori algorithm for root cause analysis in order to achieve a better performance. Essentially there are three important proposal about how to improve the performance of the apriori algorithm (Al-Mamory,2009):

1. Reduce passes over the transaction database
2. Shrink the number of possible candidates
3. Facilitate the support counting of the candidates

3.2.4. The results of Root Cause Analysis module

The results of root cause analysis module are the feature set of false positive alerts which then will be investigated by security analyst. The security analyst has three important tasks:

1. The security analyst investigates the feature set of false positives to discover root causes
2. The security analyst checks the network environment or devices that trigger the false positive alerts (e.g. router configuration, network printer setting, DNS server configuration, a broken router interface, etc.)
3. The security analyst updates the new IDS filters for the discovered problems.

3.3. Outlier Detection Module

The goal of Outlier Detection module is to find the outliers among a large number of IDS alerts. I am interested in using the FP-Outlier method proposed by (He, 2005) for outlier detection problem because the authors claim that their approach is able to handle two common problems. Firstly, the existing techniques detect outliers using the distance of points in the full dimension space. These approaches are not appropriate for discovering outliers in a high dimensional space, especially in the field of intrusion detection which produces million alerts per day and each alert has more than twenty attributes. Furthermore, these algorithms have a high computational cost. Secondly, most outlier detection approaches are focused only on identifying outliers, however in real applications the reasons why the identified outliers are abnormal also needs to be explained.

3.3.1. FP-Outlier Algorithm

The FP-outlier algorithm (He, 2005) detects outliers by discovering the frequent itemsets. Since the frequent itemsets discovered by the association rule algorithm reflect the common patterns in the dataset, it is reasonable and intuitive to regard as outliers those data points which contain infrequent patterns. In other words, if a data object contains more frequent patterns, it means that this data object is unlikely to be an outlier because it possesses the common features of the dataset. Those infrequent patterns that are contained in few data objects can be used as descriptions of outliers.

3.3.2. FP-Outlier Pseudo code

(He, 2005) define a measure called FPOF (Frequent Pattern Outlier Factor) to identify outlier objects and proposed an algorithm (FindFPOF) to extract them from the data. FPOF is used to determine the degree of an item deviation.

1. Mining the set of frequent patterns on database using an association rule algorithm with a given minimum support.
2. For every transaction in the database, the value of FPOF is computed.
3. Sort the items in the ascending order based on their FPOF values.
4. The top-n FP-outliers are output with their corresponding top-k contradict frequent patterns.

4. Conclusion and Future Work

4.1. Conclusions

In this research, I propose a FARS design based on the outlier detection approach. The proposed system will be able to reduce IDS alerts efficiently as well as analyze the root cause of false alerts. In the first stage, I will use the apriori algorithm for mining frequent IDS alerts and the FP-Outlier algorithm to detect outliers which represent possibly real attacks or intrusions. In the next stage, I will modify and improve the apriori algorithm in order to achieve an improved better performance. Furthermore, I will also evaluate the performance of the FP-Outlier algorithm and compare with several other outlier detection approaches. The robustness of the proposed system will be evaluated not only using various simulated intrusion data sets, but also on real network traffic generated inside the University of Southampton

4.2. Future Work

I have a plan to develop a prototype of my proposed False Alert Reduction System (FARS) within the next six months as explained in the table below.

Table 1. The proposed time schedule for the next six months

No	Activity	13	14	15	16	17	18
		Oct 10	Nov 10	Dec 10	Jan 11	Feb 11	Mar 11
1	False Alert Reduction System (FARS) Design						
2	Data Mining and Log Analysis Tools Experiment						
3	Root Cause Analysis Module Development						
4	Outlier Detection Module Development						
5	Prototype System Integration						
6	Evaluation of Prototype System						
7	Mini Thesis						

1. FARS Design

The FARS design as seen in Figure 3.1 and Figure 3.2 will be extended. The new diagrams will define exactly how the outliers will be calculated and then evaluated using threshold values. The FARS design will be revised and improved in month 16 during the prototype system evaluation. The revised design will focus on an improved performance and lower human intervention handle false positives alerts.

2. Data Mining Tools and Log Analysis Tools Experiment

I will use WEKA (java-based data mining tools) to develop my FARS design. The WEKA tools provide various data mining algorithms such as classification, clustering, association rules and visualization. WEKA has an apriori algorithm module but it will require modification in order able to handle a very large and high-dimensional dataset such as that generated by IDS alerts. Unfortunately, WEKA does not provide any outlier detection algorithms such as FP-Outlier. I propose to develop java codes for outlier detection methods and hopefully this will become one of my contributions to the WEKA community world-wide.

There are two interesting log analysis tools which are relevant to my proposed system, they are SLCT (Simple Log Correlation Tools) and LogHound. These are both tools which developed by Risto Vaarandi in the 'C' Language and are designed for assisting network/system administrators in extracting knowledge from event logs. SLCT employs a data clustering algorithm for analyzing textual event logs while LogHound implement apriori

algorithms for discovering frequent patterns from event logs. I anticipate that studying and exploring various tools such as WEKA, SLCT, LogHound, etc. will enrich my proposed design and develop the system more efficiently.

3. Prototype development, integration and evaluation

Starting from month 13, I will develop Java code for Root Cause Analysis based on the apriori algorithm and also an outlier detection method using FP-Outlier method. After that I will integrate both modules as a prototype of my FARS design which I will then evaluate. The performance of the proposed FARS will be evaluated using three different measurements: *reduction rate*, *completeness* and *soundness*. Reduction rate measures how many alerts can be filtered by the system, the completeness evaluates how well the system can detect true alerts and the soundness measures how correctly the alerts are recommended. The results from this prototype development will be reported in my mini thesis and also will be submitted as a conference paper.

After submitting my mini thesis, I will continue to develop my FARS design using an improved apriori algorithm and improved FP-Outlier methods designed to achieve an improved performance in terms of a lower reduction rate, higher level of completeness and overall soundness.

Bibliography

Abdulrahman Alharby, Hideki Imai, IDS false alert reduction using continuous and discontinuous patterns, *Computer Science, Springerlink 3531*, pages 192-205, 2005

Alfonso Valdes, Keith Skinner, Probabilistic Alert Correlation, In *Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection*, pages 54-68, 2001

Alshammari R, Sonamthiang S, Teimouri M, Riordan D, Using neuro-fuzzy approach to reduce false positive alerts, In *CNSR '07: Proceedings of The Fifth Annual Conference on Communication Networks and Services Research,* Washington DC, USA: IEEE Computer Society, pages 345–34, 2007

Christopher Kruegel, Fredrik Valeur, Giovanni Vigna, *Intrusion Detection and Correlation, Challenges and Solution*, Springer Science and Business Media Inc, USA, 2005

Fu Xiao, Shi Jin, Xie Li, A Novel Data Mining-based method for alert reduction and analysis, *Journal of Networks*, VOL. 5, No. 1, January 2010

Georgios P. Spathoulas, Sokratis K. Katsikas, Reducing false positives in intrusion detection systems, *Journal on Computer & Security 29*, pages 35-44, 2010

Goswami D.N., Anshu C., An Algorithm for Frequent Mining based on Apriori, In *(IJCSE) International Journal on Computer Sciences and Engineering*, Vol. 02, No. 04, pages 942-947, 2010

Jiawei Han, Jian Pei, Yiwen Yin, Runying Mao, Mining Frequent Patterns without Candidate Generation, In *International Proceeding of the 2000 ACM SIGMOD*, Dallas, pages 1–12, 2000

Klaus Julisch, Clustering intrusion detection alarms to support root cause analysis, *ACM Trans. Inf. Syst. Secur.*, 6(4):443-471, 2003

Lippmann RP, Fried DJ, Graf I, Haines JW, Kendall KR, Mc Clung D, et al., Evaluating intrusion detection systems: the 1998 DARPA off-line intrusion detection evaluation, In *DARPA Information Survivability Conference and Exposition*, 2000. DISCEX '00. Proceedings, vol. 2; 2000b. p. 12–26. IEEE Computer Society, 2000.

Rakesh Agrawal, Ramakrishnan Srikant, Fast algorithms for mining association rules in large databases, in *VLDB'94, Proceedings of 20th International Conference on Very Large Data Bases*, pages 487–499, 1994

Reza Sadoddin, Ali Ghorbani, Alert Correlation Survey: Framework and Techniques, In *Proceedings of the 4th Annual Conference on Privacy, Security and Trust (PST)*, pages 6-15, 2006

Risto Vaarandi, Real-time Classification of IDS Alerts with Data Mining Techniques, In *Proceedings of the 2009 IEEE MILCOM Conference,* ISBN: 978-1-4244-5239-2, 2009

Safaa O. Al-Mamory, Hongli Zhang, Intrusion detection alarms reduction using root cause analysis and clustering, *Computer Communications 32*, pages 419–430, 2009

Tadeusz Pietraszek, Using Adaptive Alert Classification to Reduce False Positives in Intrusion Detection, In *RAID '04: Proc. 7th Symposium on Recent Advances in Intrusion Detection*, Volume 3224 of LNCS., Springer, pages 102-124, 2004

Urko Zurutuza , Roberto Uribeetxeberria, Intrusion Detection Alarm: A Survey, In *Proceedings of the IADAT International Conference on Telecommunications and Computer Networks*, pages 1-3, 2004

Wang Taihua, Gua Fan, Associating IDS alerts by an improved apriori algorithm, In *2010 Third International Symposium on Intelligent Information Technology and Security Informatics*, pages 478-482, 2010

Xinzhou Qin, Wenkee Lee, Discovering Novel Attack Strategies from INFOSEC Alerts, In *Proceedings of The 9th European Symposium on Research in Computer Security* (ESORICS 2004) , Sophia Antipolis, France, September 2004.

Zengyou He, Xiaofei Xu, Joshua Z. Huang, Shengcun Deng, FP-Outlier: Frequent Pattern Based Outlier Detection, Computer Science and Information System, 2(1), pages 103-118, 2005