HYBRID OF STRUCTURAL-CAUSAL AND STATISTICAL MODEL FOR INTRUSION ALERT CORRELATION

MAHEYZAH BINTI MD. SIRAT @ MD. SIRAJ

UNIVERSITI TEKNOLOGI MALAYSIA

HYBRID OF STRUCTURAL-CAUSAL AND STATISTICAL MODEL FOR INTRUSION ALERT CORRELATION

MAHEYZAH MD. SIRAT @ MD. SIRAJ

A thesis submitted in fulfilment of the requirements for the award of the degree of Doctor of Philosophy (Computer Science)

Faculty of Computing
Universiti Teknologi Malaysia

FEBRUARY 2013

This thesis is dedicated especially for…

My beloved & supported husband
Erwan Najhan

My kindest parents & in-laws
Md. Siraj & Mortasiah
Othman & Fatimah

My adorable & lovely daughters
Eirdyna Najihah
Eywani Nadhirah
Effah Nafeesah
Einsyeerah Nasuha

ACKNOWLEDGEMENTS

Alhamdulillah, praise to the Almighty Allah S.W.T. With only His consent and blessing that this thesis can be completed. I would like to express my warm appreciations and thanks to all people who have assisted and motivated me during the research study. I personally want to thank my supervisor *Prof. Dr. Mohd. Aizaini Maarof,* for his support and guidance on helping me finished up the research and thesis. His perpetual energy and enthusiasm had motivated me to complete this study. As for my co-supervisor *Assoc. Prof. Dr. Siti Zaiton Mohd Hashim*, special thanks for her sincere concern and assistant throughout my study. I also would like to thank *Prof. Dr. Ajith Abraham* and *Asst. Prof. Dr. Hussain Kettani* for their valuable comments and ideas during my proposal at the early stage of my study. Not forgotten to the respected evaluators and chairman (*Prof. Dr. Md. Yazid Mohd. Saman, Prof. Dr. Abd. Hanan Abdullah, Assoc. Prof. Dr. Mazleena Salleh* and *Assoc. Prof. Dr. Subariah Ibrahim*) who have given me constructive comments during viva voce and towards submission of the thesis. My deepest gratitude goes to my dearest family and friends for their undying support and endless love. They are my true inspiration in achieving all my dreams. Last but not least, thanks to Faculty of Computing, Universiti Teknologi Malaysia (UTM) and Ministry of Higher Education (MoHE) for giving me the opportunity to further my doctorate. I wished all the best for all of us and may Allah bless us always. Ameen.

ABSTRACT

The evolutions of computer network attacks have urged many organizations to install multiple Network Intrusion Detection Systems (NIDSs) for complete monitoring and detection of intrusions. Such solution produces enormous number of alerts due to repeated and false positive alerts. This contributes to low quality alerts and makes manual Alert Correlation (AC) tedious, labour intensive and error prone. Besides that, alerts are also unformatted, unlabelled and unstructured. Thus, the actual attack strategy cannot be recognized. The existing AC models have few limitations. They only provide single type of correlation and rely on a large number of static predetermined rules to correlate alerts. Consequently, alerts are not being correlated completely and rules need to be manually updated regularly. Therefore, this research proposes a new automated Hybrid-based AC (HAC) model that provides complete correlation in terms of structural, causal and statistical. The purpose is to improve the quality of alerts as well as to recognize the attack strategy through alerts patterns. To accomplish this, it hybridizes Improved Unit Range (IUR), Principal Component Analysis (PCA), Expectation Maximization (EM) algorithm, Levenberg-Marquardt (LM) Backpropagation algorithm and statistical correlation tests to optimally recognize the known and new steps and stages of an attack strategy. New post-clustering algorithms are proposed and become part of the hybridization to filter out the low quality alerts. HAC is successfully experimented using DARPA 2000 benchmark dataset onto signature-based RealSecure Version 6.0 NIDSs. The experimental results validate that HAC optimally correlate the alerts with 98.72% of correlation completeness (R_c) and 3.45 seconds of execution time. This shows that HAC is effective and practical in providing complete correlation even on high dimensionality, large scaled and low quality dataset.

ABSTRAK

Evolusi dalam serangan rangkaian komputer menyebabkan banyak organisasi menggunapakai pelbagai Sistem Pengesan Pencerobohan Rangkaian (NIDSs) untuk pemantauan dan pengesanan pencerobohan yang sempurna. Penyelesaian ini menghasilkan sebilangan besar amaran yang disebabkan oleh amaran yang berulang dan palsu. Ini menyumbang kepada amaran berkualiti rendah dan membuatkan korelasi amaran (AC) secara manual merumitkan, meletihkan dan terdedah ralat. Selain itu, amaran juga adalah dalam bentuk tidak seragam, tidak berlabel dan tidak teratur. Oleh itu, strategi serangan sebenar tidak dapat dikenalpasti. Model-model AC sedia ada terdapat beberapa kekangan. Ia menawarkan hanya satu jenis korelasi dan bergantung kepada banyak penentuan peraturan statik untuk mengkolerasi amaran. Akibatnya, amaran tidak dapat dikorelasi secara menyeluruh dan peraturan perlu kerap dikemaskini secara manual. Oleh yang demikian, penyelidikan ini mencadangkan automasi model AC baru berasaskan hibrid (HAC) yang menawarkan kolerasi menyeluruh dari segi struktur, sebab dan statistik. Tujuannya adalah untuk menambahbaik kualiti amaran dan juga mengenalpasti strategi serangan melalui corak amaran. Bagi mencapai hasrat ini, ia menghibridkan *Improved Unit Range* (IUR), *Principal Component Analysis* (PCA), algoritma *Expectation Maximization* (EM), algoritma *Levenberg-Marquardt* (LM) *Backpropagation* dan ujian korelasi statistik bagi mengenalpasti secara optimum langkah dan peringkat yang telah diketahui mahupun baru bagi sesebuah strategi serangan. Algoritma *post-clustering* juga dicadangkan bersama penghibridan untuk menapis keluar amaran berkualiti rendah. HAC berjaya diuji menggunakan set data bertanda-aras DARPA 2000 ke atas RealSecure Versi 6.0 NIDSs. Hasil ujian menentusahkan HAC berjaya mengkolerasi amaran secara optimum dengan keseluruhan korelasi (R_c) sebanyak 98.72% selama 3.45 saat masa perlaksanaan. Ini menunjukkan bahawa ia berkesan dan praktikal dalam menyediakan kolerasi secara menyeluruh walaupun ke atas set data yang berdimensi tinggi, berskala besar dan berkualiti rendah.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ANN	-	Artificial Neural Networks
AC	-	Alert Correlation
Acc	-	Accuracy
ACS	-	Alert Correlation System
ADeLe	-	A Language Driven Alert Correlation
AI	-	Artificial Intelligent
AR	-	Accuracy Rate
BayesNet	-	Bayesian Networks
BFA	-	Bacterial Foraging Algorithm
BPANN	-	Backpropagation Artificial Neural Networks
c	-	Correlation coefficients
CA	-	Clustering Accuracy
CAC	-	Causal-based Alert Correlation
CE	-	Clustering Error
CPN	-	Colored Petri Net
DAG	-	Directed Acyclic Graph
DDoS	-	Distributed Denial of Service
DMZ	-	Demilitarized Zone
EM	-	Expectation Maximization
F1	-	F-measure
FCM	-	Fuzzy C-means
GA	-	Genetic Algorithm
GCI	-	Granger Causality Index
GCT	-	Granger Causality Test
GN	-	Gauss-Newton
HCPN	-	Hidden Colored Petri Net
HAC	-	Hybrid-based Alert Correlation

HIDS	-	Host-based Intrusion Detection System
HIPS	-	Host-based Intrusion Prevention System
ICA	-	Independent Component Analysis
IDPS	-	Intrusion Detection and Prevention System
IPCAEMP	-	IUR, PCA, EM, Post-clustering model
IPCALM	-	IUR, PCA, LM model
IPEMPoLS	-	IUR, PCA, EM, Post-clustering, LM, Statistical correlation tests model
IUR	-	Improved Unit Range
k-CV	-	*k* Cross Validation
LAMDBA	-	Language Model Database for Detection of Attacks
LM	-	Levenberg Marquardt
LVQ	-	Learning Vector Quantization
MSE	-	Mean Squared Error
NIDS	-	Network-based Intrusion Detection System
NIPS	-	Network-based Intrusion Prevention System
P	-	Precision
PC	-	Principle Component
PCA	-	Principle Component Analysis
PSO	-	Particle Swarm Optimization
R'	-	Recall
RBF	-	Radial Basic Function
R_c	-	Correlation completeness
ROC	-	Receiver Operating Characteristics
SA	-	Security Analyst
SAC	-	Structural-based Alert Correlation
SCG	-	Scaled Conjugate Gradient
SD	-	Standard Deviation
SLA	-	Supervised Learning Algorithm
SOM	-	Self-organizing Map
StAC	-	Statistical-based Alert Correlation
STATL	-	State/transition-based Attack Description Language
TBF	-	Token Bucket Filter
TIAA	-	Tool for Intrusion Alert Analysis

tn	-	True negative
tp	-	True positive
ULA	-	Unsupervised Learning Algorithm
UR	-	Unit Range
XML	-	Extended Markup Language

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Protecting information in organizations is crucial due to continuous increase of network attacks (Axelsson, 1999; Allen *et al.*, 2000; Zhu and Ghorbani 2005). In effect, the Information Assurance and Security (IAS) becomes an important research field in networked and distributed information sharing environments. IAS involves all efforts and methods to protect and secure information whether in memory, processing or in the network transactions. Finding the effective way to protect information systems, networks and sensitive data within the critical information infrastructure is challenging even with the most advanced technology and trained professionals (Kruegel *et al.*, 2005).

The implementation of Intrusion Detection and Prevention System (IDPS) is one of the effective ways on protecting the information on a secured network (Mudzingwa and Agrawal, 2012). It provides a unified platform to monitor the status of a network and to prevent the attack from damaging the network via appropriate respond mechanism. IDPS consists of three domains: Intrusion Detection (ID), Alert Correlation (AC) and Intrusion Prevention (IP). Briefly, ID detects intrusion whether in a host or network and triggers the alerts; AC processes and analyzes the alerts for discovering the relationships among them and finally IP suggests suitable respond plan towards the detected intrusion for preventing information and resources loss in the network.

This research focuses on AC due to practitioners are still performing manual alert analysis which is tedious, time-consuming and error prone (Valeur *et al.*, 2004; Julisch and Dacier, 2002). As mentioned in Pouget and Dacier (2003), the automation of alert analysis can be performed by correlation. Therefore, Alert Correlation (AC) defines an automated process that finds and discovers the relationships among unrelated alerts (Bateni *et al.*, 2012) and their attributes. Such relationships are crucial to reveal the behaviour of the attacker (in terms of attack strategy) that would be useful in determining reasonable precautions in future.

In a real attack scenario, an *Attack Strategy* comprises several of *Attack Stages* whereby each of them may contain one or more *Attack Steps*. Each attack step will produce a number of *Network Events* that shall be detected by NIDSs to decide whether it is an intrusion or not. If it is, *Alerts* will be triggered and logged. This scenario is illustrated in Figure 1.1. In general, these terms can be defined as follows.

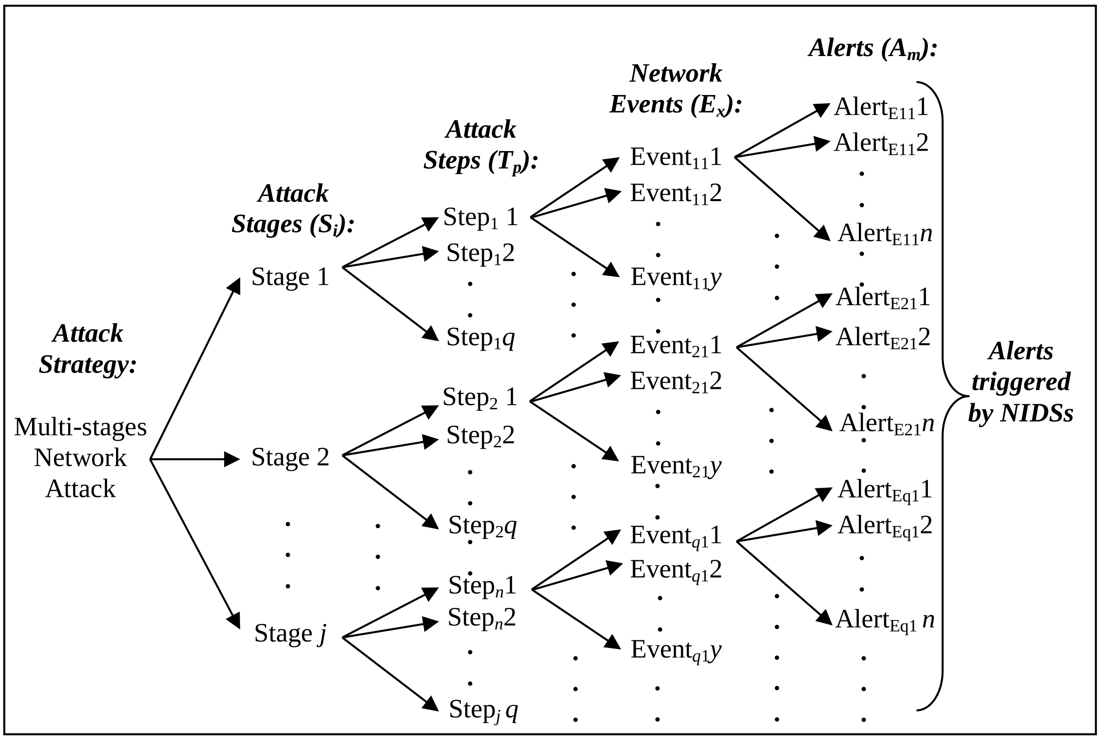

Figure 1.1: The real network attack scenario

There is a set of j attack stages denoted as $S_i = \{S_1, S_2, \ldots, S_i, ..., S_j\}$ in a multi-stages network attack. Each S_i contains q attack steps based on the attacker's goal. An attack step is denoted as T_p, where $p = 1, 2, ..., q$ and $T_p \subseteq S_i$. For every T_p, it contributes to y network events which their values will be evaluated by NIDSs for any intrusion pattern. A network event (which positively identified as intrusion) is denoted as E_x, where x = 1, 2, ..., y and $E_x \subseteq T_p \subseteq S_i$. For any E_x occurred in the network, NIDSs will generate n alerts to report the details on intrusion detected. An alert is denoted as A_m, where m = 1, 2, ..., n and $A_m \subseteq E_x \subseteq T_p \subseteq S_i$. Set of alerts A_m are logged and reported to SA for correlation process. SA can only rely on these enormous and unlabelled alerts in order to understand and study the attack strategy providing no prior knowledge or information on the causes of the alerts. This makes AC research challenging and thus, worth to be explored and appreciated.

1.2 Problem Background

Regarding to Mudzingwa and Agrawal (2012), Debar *et al.* (2004) and Allen *et al.* (2000), the most applied solution among organizations in order to optimally monitor and detect intrusions or threats in the network is the installation of multiple Network-based Intrusion Detection Systems (NIDSs). Such environment produces a diversity of alerts format. Worst, the number of alerts generated are huge and overwhelm. Even for a short period of time, the amount of alerts is enormous. Nevertheless, AC is important to recognize the attack strategy of an attacker that contains list of attack steps and stages. Generally, there are two major issues that are needed to be considered in conducting AC research.

First, alerts are in low quality in terms of high redundancy and dimensionality, false positives and invalid alerts. Such alerts can degrade the effectiveness of a correlation model or system. This is agreed by Sadoddin and Ghorbani (2009), Smith *et al.* (2008), Yu and Frinche (2007), Xu (2006), Bakar and Belaton (2005) and Ning *et al.* (2004). Even if the best NIDS implemented, the Security Analyst (SA) has to be assured that the alerts are free from low quality alerts to produce an accurate analysis results. This issue is caused by several problems:

1) *Low performance of NIDSs*. NIDSs generates many false positive alerts since normal activities are mistakenly regard as intrusions (Lee *et al.*,

2006; Wang *et al.*, 2006; Pietraszek and Tanner, 2005; Valeur *et al.*, 2004; Julisch and Dacier, 2002; Allen *et al.*, 2000).

2) *Attackers launch intensive attacks simultaneously towards multiple hosts in the network* (Zhu and Ghorbani, 2005). Such scenario could confuse the NIDSs and produce false positives. It also increases the redundancy of alerts.

3) *Organizations tend to implement multiple (either homogenous or heterogeneous) NIDSs in their networks*. As a result, SA is overwhelm with enormous number of high-dimensionality alerts (Perdisci *et al.*, 2006; Cuppens and Miege, 2002; Dain and Cunningham, 2001).

Second, the attack strategy cannot be recognized and determined directly from the alerts. Knowledge about attack strategy is important to SA to design effective response mechanisms in order to prevent the attacks from damaging the networks. This issue is caused by the following problems:

1) *Alerts that are generated by multiple NIDS are in diverse format and represented by low level information* (Valeur *et al.*, 2004). Hence, revealing the attack strategy directly from such raw alerts is unmanageable (Tedesco and Aickelin, 2006; Debar *et al.*, 2007).

2) *Continuous development of new network attacks*. Since the networks are vulnerable to the attacks and methods used by the attackers are getting more sophisticated (Zhu and Ghorbani, 2005), this has contributes to new attack strategy and new pattern of detected alerts.

Clearly, those AC problems need to be addressed for discovering useful knowledge from the alerts in terms of attack steps and stages involved in the attack strategy (Smith *et al.,* 2008; Pietraszek, 2006). Such knowledge discovery is important to the SA for developing precise and effective response and preventive mechanisms, so that organizations can avoid the intrusions from happening or escalating since true actions can be activated at earlier stage.

1.3 Research Motivation

Based on literature, previous AC models can be classified into three categories based on the criteria or approach used for finding relationships among alerts:

1) *Structural-based AC (SAC)*: Alerts are correlated based on similarity of attributes. Similarity index or function is used to determine the degree of relationships. Although it can discover known group of alerts or attack steps, Ning *et al.*, (2004) and Pietraszek (2006) claimed that it cannot discover the causal relationships among alerts.

2) *Causal-based AC (CAC)*: The correlation is emphasized on recognizing which alerts cause an attack stage for a multi-stages network attack. In this category, it can be classified into three groups:

    a) *Using attack modeling languages*. Each attack stage needs to be specified, precisely in the model. But, it is only applicable to known attack stages (Sadoddin and Ghorbani, 2006) and heavily dependent to the SA expert knowledge. It also unable to determine correlation when the alerts are unseen/new. A few examples are State/transition-based Attack Description Language (STATL) by Eckmann *et al.* (2000), Language Model Database for Detection of Attacks (LAMDBA) by Cuppens and Ortalo (2000) and A Language Driven Alert Correlation (ADeLe) by Totel *et al.* (2004).

    b) *Using predefined knowledge and rules*. As in Templeton and Levitt (2000) and Ning *et al.* (2004), they have to define the knowledge about correlating alerts based on series of rules at the early stage of the system development. It requires frequent manual updating and large database (Qin, 2005). Thus, such solution is less practical to be adopted.

c) *Using supervised learning*. Correlation of alerts is determined by learning from the collected alerts. Researches by Dain and Cunningham (2001), Qin (2005) and Smith *et al.*, (2008) have showed that they can discover correlations of unseen alerts.

3) *Statistical-based AC (StAC)*: Works under this category correlate alerts based on statistical model to discover the relationships statistically. But, as discussed in Maggi and Zanero (2007), good performance strongly depends on good parameters setting which is very difficult to estimate.

The existing works that used single approach can be referred as single correlation models. The limitation of such models is it offers only one type of correlation. The alert analysis is incomprehensive and may lead to improper response. Moreover, Lewis (1999) and Pouget and Dacier (2003) have mentioned that there is no single model that is best suited to manage the dynamic problems of AC. Since the field of AC is relatively young which just started in 2000, there is no significant precedent to guide the AC research in a clear way (Smith *et al.*, 2008).

Those arguments have motivated this research that is to offer multiple types of correlations (SAC, CAC and StAC) into a model. It is known as Hybrid-based Alert Correlation (HAC) where all advantages from single correlation models can be combined. The purpose is to provide comprehensive alert analysis that can discover complete relationships among unrelated alerts. In addition, HAC is proposed to overcome the weaknesses in the previous works which need enormous predefined rules at the early stage of development, recognize only known alerts and require manual parameters setting. Therefore, the taxonomy on research motivation that also summarizes the explanation in Section 1.1 until 1.3 is given in Figure 1.2.

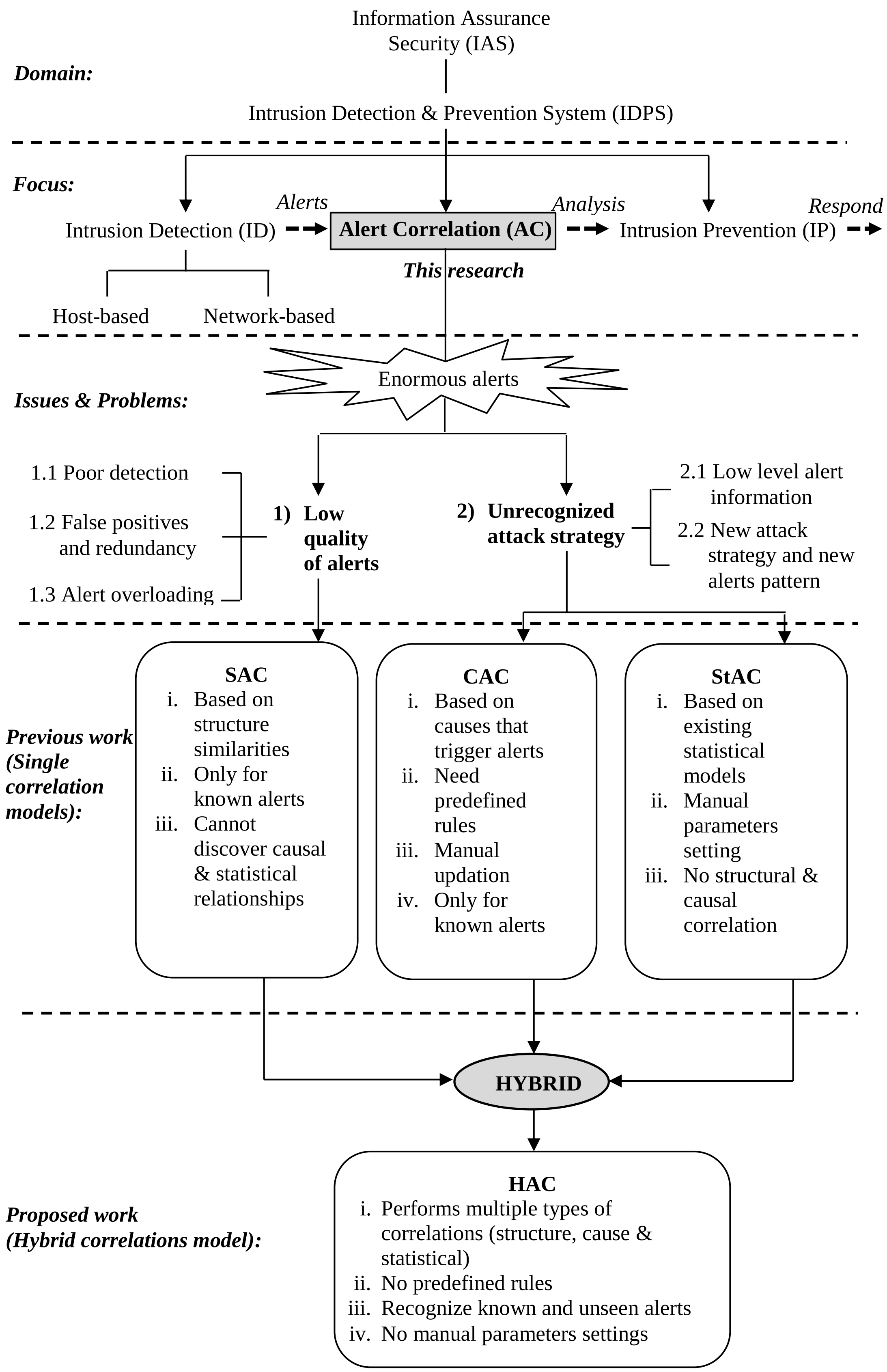

Figure 1.2: Taxonomy on research motivation

1.4 Problem Statement

In order to comply with the requirement of discovering complete relationships among alerts from multiple NIDSs, a more practical and effective AC model is needed. This is to address the problems of low quality alerts and unrecognized attack strategy as well as to overcome the limitations of existing works. Indeed, complete discovery on alert relationships can lead to effective respond and preventive mechanisms. Thus, the main research question is:

How to discover complete relationship with optimal performance among known and unseen/new alerts generated by multiple NIDSs in order to improve the quality of alerts and recognize attack strategy?

Based on this question, several supporting research questions are:

1) What defines complete relationship?
2) What are the aspects of correlations need to be performed?
3) How to measure completeness in the correlation?
4) How to define optimal performance?
5) How to identify the low quality alerts in order to improve quality?
6) How to learn the pattern of known alerts?
7) How to recognize the pattern of unseen alerts?
8) What are the elements of attack strategy in order to recognize it?

Complete relationship is the key factor of this research. Therefore, it is crucial to determine its definition and measurement. Since alert relationships can be achieved by performing correlation, completeness should include all possible aspects of correlations that known and unseen alerts should be correlated together. In this case, the aspects are in terms of structural, causal and statistical. Each correlation is measured independently and the product of all produces the correlation completeness (Ning *et al.*, 2004; Hussain *et al.*, 2005). More importantly, the performance of correlation completeness must be optimal to show the effectiveness of the proposed model.

1.5 Research Goal

Providing the above problem statement, the research goal is:

To propose an alert correlation (AC) model that can discover complete relationships and offer optimal performance among known and unseen/new alerts generated by multiple NIDSs for improved quality of alerts and recognized attack strategy.

In order to achieve the goal, the research hypothesis is:

"If alert relationships are discovered by hybridizing structural, causal and statistical correlations, then relationships among known and unseen/new alerts generated by multiple NIDSs can be revealed completely and performed optimally."

1.6 Research Objectives

In order to achieve the goal, three research objectives are required:

1) To enhance the Structural-based AC (SAC) model using unsupervised learning algorithm for improving the quality of alerts and identifying attack steps.

2) To enhance the Causal-based AC (CAC) model using supervised learning algorithm for recognizing membership of attack stages.

3) To design a Hybrid-based AC (HAC) model by hybridizing structural, causal and statistical correlations for optimizing correlation completeness and determining attributes dependency strength.

1.7 Research Scopes

The scope of this study is restricted to below limitations:

1) An offline DARPA 2000 attack scenario specific dataset (Haines, 2000) is used to validate and evaluate the proposed correlation models. It is the only freely available benchmark dataset that is widely used by other researchers in AC area as well for examples Smith *et al.*(2008), Yu and Frincke (2007), Wang *et al.* (2006), Tedesco and Aickelin (2006), Zhu and Ghorbani (2005), Ning *et al.*(2004) and Pouget and Dacier (2003).
2) This research focuses on analyzing the alerts that are generated by four RealSecure 6.0 NIDSs, as a guidance to design an appropriate responsive mechanism. The design of the responsive mechanism is excluded.
3) Verification of false positive alerts and invalid alerts is based on the freely available signature files extracted from RealSecure Signatures Reference Guide Version 6.0 (Internet Security Systems, 2000).
4) The improvement in the quality of alerts is referred to elimination or deletion of false positive alerts, invalid alerts and redundant alerts.
5) The identification of attack strategy is referred to identification of the attack steps and recognition of attack stages.

1.8 Research Framework

A brief operational framework on conducting this research is depicted in Figure 1.3. The details on the framework, flowcharts, plan and measurements are presented in Chapter 3. The research is conducted by four phases:

1) *Alert Formatting and Representation*. The raw alerts are formatted into a unified standard format called Intrusion Detection Message Exchange Format (IDMEF). Then, they are represented in numerical using Internet Protocol (IP) Obscuring technique and scaled based on Improved Unit Range (IUR).

2) *Enhanced Structural-based Alert Correlation*. It discovers the relationship among alerts based on their attributes using Expextation Maximization (EM) unsupervised learning algorithm to reveal the attack steps. Principal Component Analysis (PCA) is implemented to reduce the alerts dimensionality and optimize the performance. As to improve the alerts quality, post-clustering algorithms are proposed.
3) *Enhanced Causal-based Alert Correlation*. It adopts Levernberg-Marquardt (LM) supervised learning algorithm to discover the relationships among alerts based on their causes to recognize the attack stages. PCA is implemented to investigate whether it can improve the model's performance as well.
4) *Proposed Hybrid-based Alert Correlation*. It hybridizes IUR, PCA, EM, post-clustering, LM and statistical correlation tests to boost the overall correlation performance and measure the dependency strength among alert attributes.

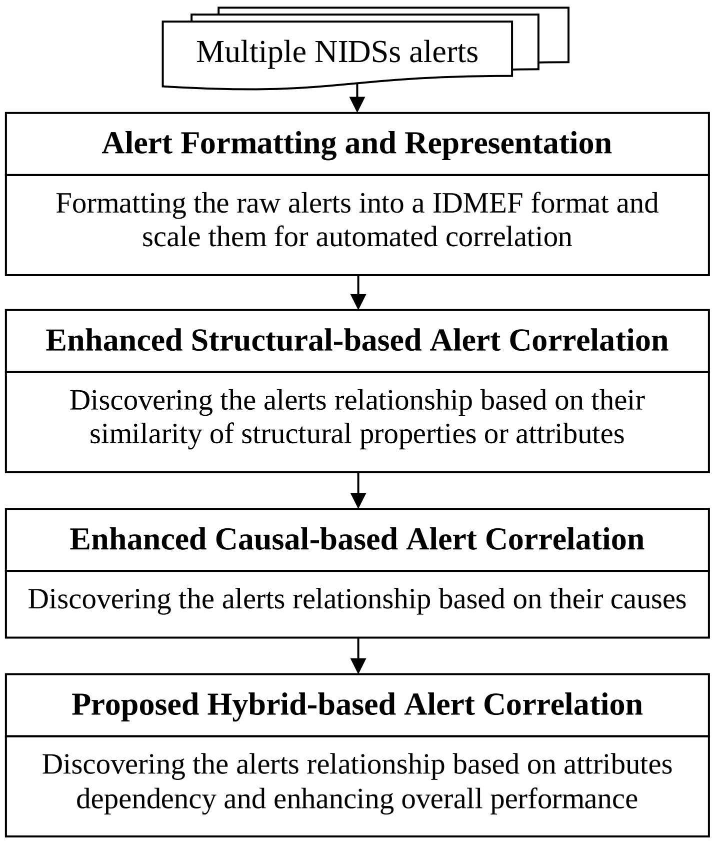

Figure 1.3: Design phases in this research

1.9 Research Contributions

The summary of research contributions is illustrated in Figure 1.4. It shows the top-down contributions from the *philosophy* aspect until the *model design*. Advanced and new correlation models are proposed to accomplish the philosophy of "providing a complete and optimal alert correlation". The specific contributions are:

1) The enhanced SAC model called IPCAEMP. It aims to improve the quality of alerts and reveal the list of attack steps by clustering the common alerts.
2) The enhanced CAC model called IPCALM. It recognizes the memberships of several attack stages of a network attack.
3) The proposed HAC model called IPEMPoLS. It hybridizes the artificial intelligent-based machine learning and statistical techniques to optimize the performance of the overall correlation and estimate the alerts attribute dependency. Details on the research contributions and suggested future works are provided in Chapter 8. The list of publications that support this research is provided in Appendix A.

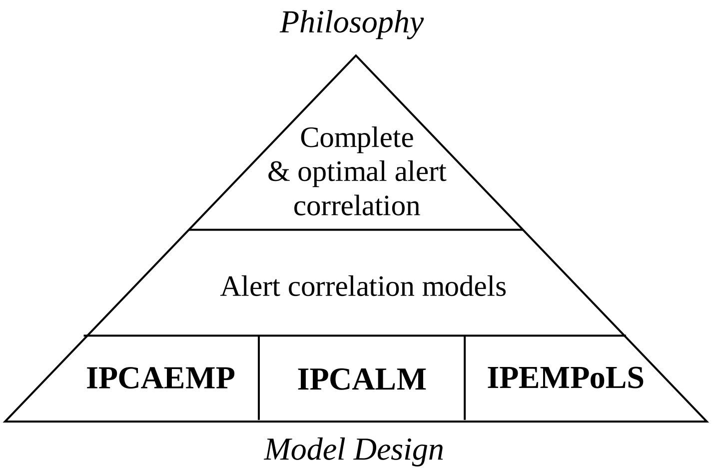

Figure 1.4: Top-down summary of research contributions

1.10 Research Significance

1) Alerts generated by multiple NIDSs are meaningless unless they are analyzed through correlations. The knowledge extracted from the correlations give a significant impact to the SA to investigate, design and develop an accurate and appropriate responsive mechanism.
2) Analyzing intrusion alerts is challenging (Manganaris *et al.,* 2000), particularly due to the large amount of alerts produced by NIDSs. Minimizing the SA intervention with the automation of AC would certainly reduce the burden of SA.
3) Updating rules frequently to discover attack strategy like in Ning *et al.* (2004) is less practical and required high costs (due to large database and labour intensive). Thus, a HAC model that has the capability of learn in order to recognize known and new alerts is more practical and cost saving.
4) Discovering the attacker strategy at early stage of alert analysis would stop the attack from escalating and damaging the network.
5) A complete AC that offers a comprehensive analysis through optimal relationships discovery of alerts could benefit SA to identify the steps and stages of a multi-stages network attack.

1.11 Organization of the Thesis

This chapter serves as an essential introduction to the research. Chapter 2 surveys the area of AC research in terms of issues, existing models and techniques. Chapter 3 explains in detail the method and framework on designing and measuring HAC performance. Chapter 4 presents the initial work of the research that is formatting and representing the alerts. Chapter 5 discusses the design and validation on IPCAEMP. Chapter 6 deals with IPCALM design and its relevant validation. Chapter 7 explains the proposed IPEMPoLS. The last chapter concludes the thesis and provides a unified discussion of research contributions and further researches.

1.12 Definition of Terms

Alert – a notification of the occurrence of specific events that matches the signatures (in signature-based NIDS) or deviates from normal activities (for anomaly-based NIDS).

Alert correlation – multi steps process that receives raw alerts as input and acts as a platform to manage and understand the alerts.

Attack graph – is a relational/causal graph or Directed Acyclic Graph (DAG) that represents the causal relationship between attacks to reveal attack strategy. Edges represent action and nodes represent system's state.

Attack steps – steps involved in an attack stage. Technically, it represents the clusters produced by clustering in IPCAEMP.

Attack stages – stages involved in the attack strategy. Technically, it represents the classes defined by classification in IPCALM.

Attack strategy – a complete attack launched by attacker which consists of attack steps and attack stages.

DDoS – stand for Distributed Denial of Service. It referred to an attack which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

Event – is a low level entity that used by NIDS to detect the sign of attacks, for examples network traffic or network packet.

False positive – an alert that is not supposed to be reported by NIDS, typically because of flawed traffic modeling or weak rules/signatures/ anomalies specified.

Known alert – a labelled alert that has class information based on previous data or domain experts knowledge. It is usually used for training the machine learning algorithm.

Unseen/new alert – an unlabelled alert that has no class information. It is usually used for validation and testing the machine learning algorithm.

REFERENCES

Abraham, A., Corchado, E. and Corchado, J. M. (2009). Hybrid Machine Learning. *International Journal of Neurocomputing*. 72(13-15): 2729-2730.

Alander, J.T. (1994). *Indexed Bibliography of Genetic Algorithms and Neural Networks.* University of Vaasa: Technical Report.

Alba, E. and Chicano, J. F. (2004). Training Neural Networks with GA Hybrid Algorithms. http://www.lcc.uma.es/~eat/pdf/gecco04f.pdf (Accessed: 8 October 2007).

Allen, J., Christie, A., Fithen, W., McHugh, J., Pickel, J. and Stoner, E. (2000). *State of the Practice of Intrusion Detection Technologies*. Carnegie Mellon University: Technical Report.

Al-Mamory, S. O. and Zhang, H. L. (2007). A Survey on IDS Alerts Processing Techniques. *6th WSEAS International Conference on Information Security and Privacy*.

Alshammari, R., Sonamthiang, S., Teimouri, M. and Riordan, D. (2007). Using Neuro-Fuzzy Approach to Reduce False Positives Alerts. *IEEE Fitth Annual Conference on Communication Networks and Services Research (CNSR07)*. 345-349.

Amoroso, E. (1999). *Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response*. Intrusion.Net Books.

Anderson, J. P. (1980). *Computer Security Threat Monitoring and Surveillance*. James P. Anderson Co., Fort Washington, PA: Technical Report.

Ariela, G., Engquistb, B., Tanushevb, N. M. and Tsaib, R. (2011). Gaussian Beam Decomposition of High Frequency Wave Fields Using Expectation–Maximization. *Journal of Computational Physics.* 230(6): 2303-2321.

AT & T Labs. (2000). Graphviz - Open Source Graph Drawing Software. http://www.research.att.com/sw/tools/graphviz (Accessed: 2 August 2007).

Axelsson, S. (1999). *Research in Intrusion-detection Systems: A Survey*. Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden: Technical Report TR 98-17.

Axelsson, S. (2000). The Base-rate Fallacy and Its Implications for the Difficulty of Intrusion Detection. *ACM Transactions on Information and System Security*. 3(3): 186–205.

Bakar, A. N. and Belaton, B. (2005). Towards Implementing Intrusion Alert Quality Framework. *Proceedings of the First International Conference on Distributed Frameworks for Multimedia Applications (DFMA'05)*, Washington: IEEE, 198-205.

Bakar, A. N., Belaton, B. and Samsudin, A. (2005). False Postives Reduction via Intrusion Alert Quality Framework. *Networks*, 2005. Jointly held with the 2005 IEEE 7th Malaysia International Conference on Communication.

Balcerek, B., Szurgot, B., Uchro´nski, M. and Waga, W. (2011). ACARM-ng: Next Generation Correlation Framework. M. Bubak, T. Szepieniec, and K. Wiatr (Eds.): PL-Grid 2011. *LNCS 7136 Springer-Verlag Berlin Heidelberg*. 114-127.

Baldacchino, T., Anderson, S. R. and Kadirkamanathan, V. (2012). Structure Detection and Parameter Estimation for NARX Models in a Unified EM Framework. *Automatica*. 48(5): 857-865.

Batbayar, B. and Yu, X. (2008). An Improved Levenberg-Marquardt Learning Algorithm for Neural Networks Based on Terminal Attractors. *Proceedings of International Symposium on Systems and Control in Aerospace and Aeronautics*. 1-4.

Bateni, M., Baraani, A. and Ghorbani, A. (2012). Alert Correlation using Artificial Immune Recognition System. *International Journal of Bio-Inspired Computation*. 4(3): 155-166.

Bellowin, S. M. (1993). Packets Found on an Internet. *Computer Communications Review*. 23(3): 26-31.

Bezdek, J. C. (1981). *Pattern Recognition with Fuzzy Objective Function Algorithms*. New York: Plenum Press.

Bloedorn, E., Hill, B., Christiansen, A., Skorupka, C., Talbot, L. and Tivel, J. (2000). *Data Mining for Improving Intrusion Detection*. MITRE Corporation: Technical Report.

Bluman, A. G. (2008). *Elementary Statistics A Step by Step Approach*. Fourth Edition. Singapore: McGraw Hill.

Boer, R.C. (2002). *A Generic Architecture for Fusion-based Intrusion Detection*

Systems. Erasmus University Rotterdam: Master Thesis.

Bonissone, P. (2002). Hybrid Soft Computing for Classification and Prediction Applications. *Proceedings of 1st International Conference on Computing in an Imperfect World (Soft-Ware 2002).*

Bonissone, P. P. (2000). Hybrid Soft Computing Systems: Where Are We Going?. *Proceedings of the 14th European Conference on Artificial Intelligence (ECAI 2000),* Berlin Germany. 739-746.

Bonissone, P. P., Chen, Y. T., Goebel, K. and Khedkar, P.S. (1999). *Proceedings of the IEEE Hybrid Soft Computing Systems: Industrial and Commercial Applications.* 87(9): 1641-1667.

Bonissone, P. P., Khedkar, P.S., and Chen, Y. T. (1996). Genetic Algorithms for Automated Tuning of Fuzzy Controllers, A transportation Application. *Proceedings of Fifth IEEE Int. Conf. on Fuzzy Systems (FUZZ-IEEE'96).* 674-680.

Bonissone, P.P. and Cheetham, W. (1997). Financial Applications of Fuzzy Case-Based Reasoning to Residential Property Valuation. *Proceedings Sixth Int. Conf. On Fuzzy Systems (FUZZ-IEEE'97).* 37-44.

Bonissone, P.P., Cheetham, W., Golibersuch, D. and Khedkar, P.S. (1998). Automated Residential Property Valuation: An Accurate and Reliable Based on Soft Computing. *Soft Computing in Financial Engineering*, R. Ribeiro, H. Zimmermann, R.R. Yager, and J.Kacprzyk, Eds., Heidelberg, Germany: Physica-Verlag (Springer-Verlag).

Bouzida, Y. (2006). *Principal Component Analysis for Intrusion Detection and Supervised Learning for New Attack Detection*. Ecole Nationale Sup´erieure des T´el´ecommunications de Bretagne: PhD Thesis.

Bradley, P. S., Fayyad, U., Reina, C. (1998). *Scaling EM (Expectation-Maximization) Clustering to Large Databases*. Technical Report. Microsoft Research Redmond, WA 98052, USA.

Broderick, J. (1998). IBM Outsourced Solution. http://www.infoworld.com/cgi-bin/displayTC.pl?/980504sb3-ibm.htm (Accessed: 6 June 2007).

Brugger, S. T. and Chow, J. (2005). *An Assessment of the (1999) DARPA IDS Evaluation Dataset Using Snort*. University of California, Davis, Department of Computer Science, Davis, CA: Technical Report CSE-2007-1.

Carey, N., Clark, A. and Mohay, G. (2002). IDS Interoperability and Correlation

Using IDMEF and Commodity Systems. *Proceedings of the International Conference on Information and Communications Security (ICICS 2002).* 252-264.

Carson, C., Belongie, S., Greenspan, H. and Malik, J. (2002). Blobworld: Image Segmentation Using Expectation-Maximization and Its Application to Image Querying. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 24(8): 1026 - 1038.

CERT (1999). Results of the Distributed-systems Intruder Tool Workshop. http://www.cert.org/reports/dsit_workshop.pdf (Accessed: 4 June 2008).

Chan, Z. S. H. and Kasabov, N. (2004). Gene Trajectory Clustering with a Hybrid Genetic Algorithm and Expectation Maximization Method. *Proceedings of 2004 IEEE International Joint Conference onNeural Networks*. 1669 - 1674.

Chattopadhyay, S. (2006). Anticipation of Summer Monsoon Rainfall over India by Artificial Neural Network with Conjugate Gradient Descent Learning. http://arxiv.org/abs/nlin/0611010 (Accessed: 9 July 2009).

Chen, L. and Man, H. (2003). Discriminant Analysis of Stochastic Models and Its Application to Face Recognition. *IEEE International Workshop on Analysis and Modeling of Faces and Gestures*. 5-11.

Cheng, J., Greiner, R., Kelly, J., Bell, D. and Liu, W. (2002). Learning Bayesian Networks from Data: An Information-theory Based Approach. *Artificial Intelligence*. 137: 43–90.

Clarke, E., Grumberg, O. and Peled, D. (2000). *Model Checking*. MIT Press.

Clifton, C. and Gengo, G. (2000). Developing Custom Intrusion Detection Filters Using Data Mining. *Military Communications International Symposiums (MILCOM2000)*. 440-443.

Cooper, G. F. and Herskovits, E. (1991). A Bayesian Method for Constructing Bayesian Belief Networks from Databases. *Proceedings of the Seventh Conference on Uncertainty in Artificial Intelligence*.

Corchado, E., Abraham, A. and Carvalho, A. (2010). Hybrid Intelligent Algorithms and Applications. *International Journal of Information Sciences*. 180(14): 2633-2634.

Cover, T. and Thomas, J. (1991). *Elements of Information Theory*. John Wiley.

Cuppens, F. (2001). Managing Alerts in a Multi-intrusion Detection Environment. *17th Annual Computer Security Applications Conference*, New Orleans, USA.

22–31.

Cuppens, F. (2005). Using an Intrusion Detection Alert Similarity Operator to Aggregate and Fuse Alerts. *Proceedings of the 4th Conference on Security and Network Architectures*.

Cuppens, F. and Miege, A. (2002). Alert Correlation in a Cooperative Intrusion Detection Framework. *Proceedings of the IEEE Symposium on Security and Privacy*. 202-215.

Cuppens, F. and Ortalo, R. (2000). Lambda: A Language to Model a Database for Detection of Attacks. *Proceedings of Recent Advances in Intrusion Detection, 3rd International Symposium, (RAID 2000)*. 197-216.

Cuppens, F., Autrel, F., Mie`ge, A. and Benferhat, S. (2002). Correlation in an Intrusion Detection Process. *Internet Security Communication Workshop (SECI'02).* 153–172.

Dain, O.M. and Cunningham, R. K. (2001). Fusing a Heterogeneous Alert Stream into Scenarios. *Proceedings of the 2001 ACM Workshop on Data Mining for Security Applications*. 1-13.

Deb, N., Chakraborty, M. and Chaki, N. (2011). A State-of-the-Art Survey on IDS for Mobile Ad-Hoc Networks and Wireless Mesh Networks. *Communications in Computer and Information Science*. 203: 169-179.

Debar, H., Curry, D. and Feinstein, B. (2007). The Intrusion Detection Message Exchange Format (IDMEF). http://www.ietf.org/rfc/rfc4765.txt (Accessed: 7 December 2007).

Debar, H. and Wespi, A. (2001). Aggregation and Correlation of Intrusion–detection Alerts. *Proceedings of the 4th International Symposium on Recent Advances in Intrusion detection (RAID2001)*. 87–105.

Dempster, A. P., Laird, N. M. and Rubin, D. B. (1977). Maximum likelihood from in-complete data via the EM algorithm. *Journal of the Royal Statistical Society: Series B*. 39(1): 1–38.

Do, C. B., and Batzoglou, S. (2008). What is the Expectation Maximization Algorithm? *Nature Biotechnology*. 26: 897-899.

Dua, S. and Du, X. (2011). *Data Mining And Machine Learning In Cybersecurity*. USA: Taylor and Francis Group, LLC.

Duda, R., Hart, P. and Stork, D. (2001). *Pattern Classification 2nd Edition.* New York: John Wiley and Sons.

Dunn, J. C. (1973). A Fuzzy Relative of the ISODATA Process and its Use in Detecting Compact Well-separated Custers. *Journal of Cybernetics.* 3: 32-57.

Dvurecenskij, A. and Pulmannova, S. (1989). A Signed Measure Completeness Criterion. *Letters in Mathematical Physics*. 17: 253-261.

Eckmann, S.T., Vigna, G. and Kemmerer, R.A. (2002). Statl: An attack Language for State-based Intrusion Detection. *Journal of Computer Security.* 10 (1-2)*:* 71-103.

Elshoush, H. T. and Osman, I. M. (2011). Alert Correlation in Collaborative Intelligent Intrusion Detection Systems-A survey. *Applied SoftComputing*. In Press.

Eschelbeck, G. and Krieger, M. (2003). *Eliminating Noise From Intrusion Detection Systems*. Information Security Technical Report. 8(4): 26-33.

Foo, B., Glause, M. W., Howard, G. M., Wu, Y. S., Bagchi, S. and Spafford, E. H. (2007). *Intrusion Response System: A Survey*. Purdue University: Center for Education and Research in Information Assurance and Security (CERIAS).

Friedman, N., Nachman, I. and Peer, D.(1999). Learning Bayesian Network Structure from Massive Datasets: The Sparse Candidate Algorithm. *Proceedings of the 15th Conference on Uncertainty in Artificial Intelligence*.

Gardner, R. D. and Harle, D. A. (1996). Methods and Systems for Alarm Correlation. *Proceedings of GLOBECOM*, London. 136–140.

Geib, C. and Goldman, R. (2001). Plan Recognition in Intrusion Detection Systems. *DARPA Information Survivability Conference and Exposition (DISCEX)*. 46–55.

Gevers, M. R. and Anderson, B. D. O. (1981). Representations of Jointly Stationary Stochastic Feedback Processes. *International Journal of Control*. 33: 777–809.

Goldman, R. P., Heimerdinger, W., Harp, S., Geib, C. W., Thomas, V. and Carter, R. (2001). Information Modeling for Intrusion Report Aggregation. *Proceedings of the DARPA Information Survivability Conference and Exposition II (DISCEX-II).* 329–342.

GraphViz (1999). An Open Source Graph Generator. http://www.research.att.com/sw/tools/graphviz (Accessed: 5 November 2007).

Guerrero, R. D. (2010). Auto- and Cross-Correlation-Functions as Entanglement Quantifiers in Semiconductor Microcavities. *Mesoscale and Nanoscale Physics.* arXiv:1010.3318 (Accessed: 4 February 2011).

Hagan, T. and M. Menhaj, M. (1994). Training Feedforward Networks with the

Marquardt Algorithm. *IEEE Transactions Neural Networks*. 5(6): 989-993.

Haines, J. W. (2000). DARPA 2000 Intrusion Detection Evaluation Datasets. Lincoln Laboratory, Massachusetts Institute of Technology. http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/2000data.html (Accessed: 5 May 2007).

Haines, J., Ryder, D. K., Tinnel, L. and Taylor, S. (2003). Validation of Sensor Alert Correlators. *IEEE Security and Privacy.* 1(1): 46–56.

Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P. and Witten I. H. (2009). The WEKA Data Mining Software: An Update. SIGKDD Explorations. 11(1). http://www.cs.waikato.ac.nz/ml/weka/ (Accessed: 6 March 2007).

Han, J., Cai, Y. and Cercone, N. (1992). Knowledge Discovery in Databases: An Attribute-Oriented Approach. *Proceedings 18th International Conference on Very Large Databases (VLDB).* 547-559.

Han, J., Cai, Y. and Cercone, N. (1993). Data-Driven Discovery of Quantitative Rules in Relational Databases. *IEEE Transactions on Knowledge and Data Engineering*, 5(1). 29-40.

Hätälä, A., Särs, C., Addams-Moring, R., and Teemupekka, V., (2004). Event Data Exchange and Intrusion Alert Correlation in Heterogeneous Networks. *Proceeding of the 8th Colloquium for Information Systems Security Education West Point*, New York.

Hawickhorst, B. A., Zahorian, S. A. and Rajagopal, R. (2009). A Comparison of Three Neural Network Architectures for Automatic Speech Recognition. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.134.5674 (Accessed: 28 November 2011).

Hayter, A. J. (2002). *Probability and Statistics for Engineers and Scientists*. Duxbury Press.

Heckerman, D., Meek, C. and Cooper, G. F. (1999). A Bayesian Approach to Causal discovery, in *Book of Computation, Causation, and Discovery.* C. Glymour and G.Cooper Editors: MIT Press.

Heslop, D., Dekkers, M. J., Kruiver, P. P (2002). Analysis of Isothermal Remanent Magnetization Acquisition Curves Using the Expectation–Maximization Algorithm. *Geophysical Journal International*. 148(1): 58-64.

Hesse, W., Moller, E., Arnold, M., Witte, H. and Schack, B. (2003). Investigation of Time-variant Causal Interactions Between Two Eeg Signals by Means of the

Adaptive Granger Causality. *Brain Topography*. 15: 265–266.

Huang, C. J., Hu, K. W., Chen, H. M., Chang, T. K., Luo, Y. C. and Lien, Y. J. (2012). Applicatopn of Type-2 Fuzzy Logic to Rule-based Intrusion Alert Correlation Detection. *International Journal of Innovative Computing, Information and Control*. 8(4): 2865-2874.

Hussain, T., Awais, M. M. and Shamail, S. (2005). A Fuzzy Based Approach to Measure Completeness of an Entity-Relationship Model. *Proceedings of the 24th International Conference on Perspectives in Conceptual Modeling*. 410-422.

Ilgun, K., Kemmerer, R. and Porras, P. (1995). State Transition Analysis: A Rule-based Intrusion Detection System. *IEEE Transactions on Software Engineering*. 21 (3): 181-199.

Internet Security Systems (2000). RealSecure Sensor Network. http://www.iss.net/products_services/enterprise_protection/rsnetwork/sensor.php (Accessed: January 2007).

Internet Security Systems (2001). RealSecure Signatures Reference Guide Version 6. http://xforce.iss.net (Accessed: 10 June 2008).

Jakobson, G. and Weissman, M. D. (1993). *Alarm Correlation*. IEEE Network Magazine. 52–59.

Janecek, A. G. K., Gansterer, W. N., Demel, M. A. and Ecker, G. F. (2008). On the Relationship Between Feature Selection and Classification Accuracy. *JMLR: Workshop and Conference Proceedings*. 4: 90-105.

Jantzen, J. (1998). *Neurofuzzy Modelling*. Department of Automation, Technical University of Denmark: Technical Report No. 98-H-874.

Japkowicz, N. and Smith, R. (2005). *Autocorrel II: Unsupervised Network Event Correlation*. University of Ottawa, Canada: Technical Report.

Jha, S., Sheyner, O. and Wing, J.M. (2002). Two Formal Analyses of Attack Graphs. *Proceedings of the 15th IEEE Computer Security Foundations Workshop*. 49-63.

Jolliffe, I. T. (2002). *Principal Component Analysis*. Third Edition. New York: Springer Verlag.

Jones, E. R. (2004). *An Introduction to Neural Networks*. USA: Visual Numerics, Inc.

Jukić, V. D. (2011). Partial Spectral Analysis of Hydrological Time Series. *Journal* *of Hydrology*. 400(1–2): 223-233.

Julisch, K. (2000). Dealing With False Positives in Intrusion Detection. *The 3th Workshop on Recent Advances in Intrusion Detection*, October 2000.

Julisch, K. (2001). Mining Alarm Clusters to Improve Alarm Handling Efficiency. *Proceedings of the 17th ACSAC*. 12–21.

Julisch, K. (2003). *Using Root Cause Analysis to Handle Intrusion Detection Alarms*. University of Dortmund, Germany: PhD Thesis.

Julisch, K. (2003a). Clustering intrusion detection alarms to support root cause analysis. *ACM Transactions on Information and System Security (TISSEC)*. 6(4): 443-471.

Julisch, K. and Dacier, M. (2002). Mining Intrusion Detection Alarms for Actionable Knowledge. *Proceedings of the 8th ACM International Conference on Knowledge Discovery and Data Mining*. 366-375.

Kabiri, P. and Ghorbani, A. A. (2005). Research on Intrusion Detection and Response: A Survey. *International Journal of Network Security*. 1(2): 84-102.

Kabiri, P. and Ghorbani, A. A. (2007). A Rule-based Temporal Alert Correlation System. *International Journal of Network Security*. 5(1): 66-72.

Kaufmann, R. K. and Stern, D. I. (1997). Evidence for Human Influence on Climate from Hemispheric Temperature Relations. *Nature*. 388: 39-44.

Kayacik, H.G. and Zincir-Heywood, A.N. (2003). A Case Ctudy of Three Open Source Security Management Tools. *Proceedings of 8th IFIP/IEEE International Symposium on Integrated Network Management*. 101-104.

Kermani, B. G., Schiffman, S. S. and Nagle, H. T. (2005). Performance of the Levenberg–Marquardt Neural Network Training Method in Electronic Nose Applications. *Sensors and Actuators*. 110:13-22.

Kiatpanichagij, K. and Afzulpukar, N. (2009). Use of Supervised Discretization with PCA in Wavelet Packet Transformation-based Surface Electromyogram Classification. *Biomedical Signal Processing and Control*. 4(2) : 127-138.

Kohn, A. F. (2006). Autocorrelation and Crosscorrelation Methods. http://www.leb.usp.br/andfkohn/EBME_2006_electronic_version.pdf (Accessed: 26 April 2009).

Kohonen, T. (1998). The Self-organizing Map. *Neurocomputing*. 21(1-3). 1-6.

Kohonen, T. (2001). *Self-Organizing Maps: Series in Information Sciences.* Third Extended Edition. Berlin: Springer.

Kohonen, T., Hynninen, J., Kangas, J. and Laaksonen, J. (1996). *SOM PAK: The Self-Organizing Map Program Package*. Helsinki University of Technology: Technical Report.

Kollias, S., and Anastassiou, D. (1989). An Adaptive Least Squares Algorithm for the Efficient Training of Artificial Neural Networks. *IEEE Transactions Circuits System*. 36(8): 1092-1101.

Korn, G. A. and Korn, T. M. (2000). *Mathematical Handbook for Scientists and Engineers: Definitions, Theorems, and Formulas for Reference and Review*. Dover Publications.

Kruegel, C., Robertson, W. and Vigna, G. (2004). Using Alert Verification to Identify Successful Intrusion Attempts. *Practice in Information Processing and Communication (PIK)*. 27(4): 219-227.

Kruegel, C., Valeur, F. and Vigna, G. (2005). *Intrusion Detection and Correlation, Challenges and Solution*. USA: Springer Science Business Media Inc.

Kumar, M., Siddique, S., and Noor, H. (2009). Feature-based Alert Correlation in Security Systems. *Proceedings of Data Mining, Intrusion Detection, Information Security and Assurance and Data Networks Security*.

Lee, S., Chung, B., Kim, H., Lee, Y., Park, C. and Yoon, H. (2006). Real-time Analysis of Intrusion Detection Alerts via Correlation. *Journal of Computers and Security*. 25: 169-183.

Lee, W., Stolfo, S. J. and Mok, K. W. (1999). A Data Mining Framework for Building Intrusion Detection Models. *Proceedings of the 1999 IEEE Symposium on Security and Privacy*. 608-618.

Lee, W., Stolfo, S.J., Chan, P.K., Eskin, E., Fan, W., Miller, M., Hershkop, S. and Junxin, Z. (2001). Real Time Data Mining-based Intrusion Detection. *Proceedings of the DARPA Information Survivability Conference & Exposition II (DISCEX '01)*. 89 - 100.

Levenberg, K. (1944). A Method for the Solution of Certain Problems in Least Squares. *Quart. Applied Math*. 2: 164-168.

Lewis, L. (1993). A Case-based Reasoning Approach to the Resolution of Faults in Communications Networks. *Integrated Network Management III.* North-Holland, Amsterdam. 671–681

Lewis, L. (1999). *Service level Agreements for Enterprise Networks*. Artech House: Norwood, MA. 158-190.

Li, R., Zhao, Y., Zhang, F. and Song, L. (2007). *Rough Sets in Hybrid Soft Computing Systems*. Advanced Data Mining and Applications. Lecture Notes in Computer Science. Springer Berlin / Heidelberg. 35-44.

Li, W., Li, Z., Jie, L. and Yao L. (2006). A Novel Algorithm SF for Mining Attack Scenarios Model. *IEEE International Conference on e-Business Engineering (ICEBE'06*). 55-61.

Lippmann, R., Webster, S. and Stetson, D. (2002). The Effect of Identifying Vulnerabilities and Patching Software on the Utility of Network Intrusion Detection. *Proceedings of the Recent Advances in Intrusion Detection (RAID2002).* Springer Verlag*:* Lecture Notes in Computer Science. 2516: 307–326.

Long, J., Schwartz, D. and Stoecklin, S. (2006). Distinguishing False from True Alerts in Snort by Data Mining Patterns of Alerts. *Conference on Data Mining, Intrusion Detection, Information Assurance and Data Networks Security*. Florida, USA. 6241: 1-10.

MacQueen, J. B. (1967). Some Methods for Classification and Analysis of Multivariate Observations. *Proceedings of 5th Berkeley Symposium on Mathematical Statistics and Probability*. 1: 281-297.

Madhu, S. N., Rajasree, R., Jisha J., and Wilscy, M. (2008). Expectation-Maximization with Distance Measure for Color Image Segmentation. *IEEE Region Colloquium and the Third ICIIS*. 1-5.

Maggi, F. and Zanero, S. (2007). *On the Use of Different Statistical Tests for Alert Correlation*. Springer-Verlag: Lecture Notes Computer Science. 4637: 167-177.

Maggi, F., Matteucci, M. and Zanero, S. (2009). Reducing False Positives in Anomaly Detectors Through Fuzzy Alert Aggregation. *Information Fusion*. 10(4): 300-311.

Mahoney, M.V. and Chan, P.K. (2003). *An Analysis of the 1999 Darpa/Lincoln Laboratory Evaluation Data for Network Anomaly Detection*. Springer-Verlag: Lecture Notes in Computer Science. 2820: 220–237.

Man, D., Yang, W., Wang, W. and Xuan, S. (2012) . An Alert Aggregation Algorithm Based on Iterative Self-Organization. *Procedia Engineering.* 29: 3033-3038.

Manganaris, S., Christensen, M., Zerkle, D., and Hermiz, K. (2000). A Data Mining Analysis of RTID Alarms. *Journal of Computer Networks.* 34: 571–577.

Marchetti, M., Colajanni, M. and Manganiello, F. (2011). Framework and Models for Multistep Attack Detection. *International Journal of Security and Its Applications*. 5(4): 73-92.

Marquardt, D. (1963). An Algorithm for Least Squares Estimation of Non-linear Parameters. *Jurnal Industrial Applied Math*. 431-441.

MathWorks (2008). MATLAB: The Languange of Technical Computing. http://www.mathworks.com (Accessed: 2 Jan 2007).

McClelland, J.L. and Rumelhart, D.E. (1986). *Parallel Distributed Processing: Explorations in the Microstructure of Cognition*. USA: The MIT Press.

McHugh, J. (2000). Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory. *ACM Transactions Information System Security*. 3(4): 262–294.

McHugh, J., Christie, A. and Allen, J. (2000). *Defending Yourself: The Role of Intrusion Detection Systems*. http://www.cert.org/archive/pdf/IEEE_IDS.pdf (Accessed: 27 September 2007).

Meyer, J. A. (1996). *Artificial Life and the Animat Approach to Artificial Intelligence*. Artificial Intelligence, 2nd edition, Handbook of Perception and Cognition. New York: Academic Press. 325–354.

Ming-Yang Sua, Gwo-Jong Yub, and Chun-Yuen Lin (2009). A real-time network intrusion detection system for large-scale attacks based on an incremental mining approach. Computers & Security Volume 28, Issue 5, July 2009, Pages 301-309.

Mirikitani, D. and Nikolaev, N. (2008). Recurrent Expectation Maximization Neural Modeling. *Proceedings of International Conferences on Computational Intelligence for Modelling, Control and Automation*. 674-679

Mitra, S., Choudhury, T. R. and Ferrara, A. (2010). Reionization Constraints using Principal Component Analysis. http://arxiv.org/abs/1011.2213 (Accessed: 23 August 2011).

Mizuta, S., Sato, T., Lao, D., Ikeda, M. and Shimizu, T. (2001). Structure Design of Neural Networks using Genetic Algorithms. *Complex Systems*. 13: 161–175.

Mohamed, A. B., Idris, N. B., and Shanmugum, B. (2012). An Operational Framework for Alert Correlation using a Novel Clustering Approach. *International Journal of Computer Applications*. 54(12).

Moller (1993). A Scaled Conjugate Gradient Algorithm for Fast Supervised

Learning. *Neural Networks*. 6(4): 525-533.

Morin, B., Me, L., Debar, H. and Ducassé, M. (2002). M2D2: A Formal Data Model for IDS Alert Correlation. *5th International Symposium in Recent Advances in Intrusion Detection (RAID2002). 115-127.*

Mudzingwa, D. and Agrawal, R. (2012). A study of Methodologies used in Intrusion Detection and Prevention Systems (IDPS). *Proceedings of IEEE Southeastcon*. 1-6.

Munjal, G. and Kaur, S. (2006). Comparative Study of ANN for Pattern Classification. *Proceedings of the 8th WSEAS International Conference on Mathematical Methods and Computational Techniques in Electrical Engineering*.

Munkres, J. (1957). Algorithm for the Assignment and Transportation Problem. *Journal of SIAM*. 5(1): 32-38.

Munshi, D., Heavens, A., Cooray, A. and Valageas, P. (2011). Secondary Non-Gaussianity and Cross-correlation Analysis. *Monthly Notices of the Royal Astronomical Society*. 414(4): 3173-3197.

Nauck, D., Nauck, U. and Kruse, R. (1999). NEFCLASS for JAVA - New Learning Algorithms. *Proceedings of 18th International Conference of the North American Fuzzy Information Processing Society (NAFIPS)*. 472-476.

Ning, P. (2002). TIAA: A Toolkit for Intrusion Alert Analysis, http://discovery.csc.ncsu.edu/software/correlator/ (Accessed: March 2007).

Ning, P. and Xu, D. (2003). Learning Attack Strategies From Intrusion Alerts. *Proceedings of the 10th ACM Conference on Computer and Communication Security*. 200-209.

Ning, P., Cui, Y., Reeves, D. and Xu, D. (2004). Techniques and Tools for Analyzing Intrusion Alerts. *ACM Transactions on Information and System Security (TISSEC)*. 2: 274-318.

Norton, M. and Roelker, D. (2004). *Snort 2.0 Rule Optimizer*. Sourcefire Network Security White Paper, April 2004.

Olson, D. L. and Delen, D. (2008). *Advanced Data Mining Techniques*. Springer ISBN 3540769161. 138.

Ordonez, C. and Cereghini, P. (2000) SQLEM: fast clustering in SQL using the EM algorithm. *ACM SIGMOD Record*. 29(2): 559 - 570.

Orozco, J., Carlos, A. and García, R. (2003). Applying Scaled Conjugate Gradient for the Classification of Infant Crying. *European Symposium on Artificial Neural Networks*. 349-354.

Palm, W.J. (2005). *Introduction to Matlab 7 for Engineers*. Singapore: McGraw Hill.

Paxson, V. (1999). Bro: A System for Detecting Network Intruders in Real-Time. *Computer Networks* 31(23-24): 2435-2463.

Pchelp (1999). *How to Obscure Any URL*. Available at: http://www.pc-help.org/obscure.htm

Pearl, J. (1988). *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Morgan Kaufmann Publishers, Inc.

Pearl, J. (2000). *Causality: Models, Reasoning, and Inference*. Cambridge University Press.

Perdisci, R., Giacinto, G. and Roli, F. (2006). Alarm Clustering for Intrusion Detection Systems in Computer Networks. *Engineering Applications of Artificial Intelligence.* 19: 429-438.

Pickett, J. P. (2000). *The American Heritage Dictionary of the English Language*. Boston: Houghton Mifflin Company.

Pietraszek, T. (2004). *Using Adaptive Alert Classification to Reduce False Positives in Intrusion Detection*. Recent Advances in Intrusion Detection (RAID2004). Springer-Verlag: Lecture Notes in Computer Science. 3324: 102-124.

Pietraszek, T. (2006). *Alert Classification to Reduce False Positives in Intrusion Detection*. Albert-Ludwigs-Universit¨at Freiburg im Breisgau, Germany: PhD Thesis.

Pietraszek, T. and Berghe, C. V. (2005). *Defending Against Injection Attacks Through Context-sensitive String Evaluation*. Recent Advances in Intrusion Detection (RAID2005). Springer-Verlag: Lecture Notes in Computer Science. 3858: 124–145.

Pietraszek, T. and Tanner, A. (2005). *Data Mining and Machine Learning – Towards Reducing False Positives in Intrusion Detection*. Information Security Technical Report, 10 (3).

Poppi, S. (2004). Snort IDMEF output Plug-In. http://sourceforge.net/projects/snort-idmef/ (Accessed: 12 June 2007).

Porras, P. A., Fong, M. W. and Valdes, A. (2000). A Mission-impact Based Approach to INFOSEC Alarm Correlation. *Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection 2000 (RAID2000)*. 95–

114.

Pouget, F. (2003). *Alert Correlation*. Institut Eurecom Sophia Antipolis, France: Research Report RR-03-094.

Pouget, F. and Dacier, M. (2003). *Alert Correlation: Review of the State of the Art*. Institut Eurecom Sophia Antipolis, France: Research Report RR-03-093.

Ptacek, T. H. and Newsham, T. N. (1998). *Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection*. Secure Networks Inc.: Technical Report.

Putratama, L. A., Muhayyatin, U. and Kaloko, B. S. (2012). Forecasting of PDRB in Jember, East Java using Levenberg Marquardt Method. *Journal of Academic Research International*. 2(1): 30-34.

Qin, X. (2005). *A Probabilistic-based Framework for INFOSEC Alert Correlation*. Georgia Institute of Technology, USA: PhD Thesis.

Qin, X. and Lee, W. (2003). Statistical Causality Analysis of INFOSEC Alert Data. *Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection 2003 (RAID2003)*. 73–93.

Qin, X. and Lee, W. (2004). *Discovering Novel Attack Strategies from INFOSEC Alerts*. 9th European Symposium on Research Computer Security (ESORICS 2004). Springer-Verlag: Lecture Notes in Computer Science. 3193: 439–456.

Qiu, C., Zuo, X., Wang, C., Wu, J. and Zhang, T. (2010). An Urban Traffic Speed Fusion Method Based on Principle Component Analysis and Neural Network. *Proceedings of the 2010 International Joint Conference on Neural Network.* 1-7.

Qualys, QualysGuard Vulnerability Assessment (2003). http://www.qualys.com/?page=services/qg/how. (Accessed: 8 January 2008).

Rahejaa, A. and Dhawan, A. P. (2000). Wavelet-based Multiresolution Expectation Maximization Image Reconstruction Algorithm for Positron Emission Tomography. *Computerized Medical Imaging and Graphics*. 24(6): 359-376.

Ranum, M. J. (2003). *False Positives: A User's Guide to Making Sense of IDS Alarms*. ICSA Labs IDSC.

Riordan, J., Zamboni, D. and Duponchel, Y. (2005). *Billy Goat, an Accurate Worm-detection System (revised version)*. IBM Zurich Research Laboratory: *Technical Report*.

Roesch, M. (1999). Snort: Lightweight Intrusion Detection for Networks. *Proceedings of Usenix 13th Systems Administration Conference (LISA 99)*, Usenix Association.

Roschke, S., Cheng, F. and Meinel, C. (2010). A Flexible and Efficient Alert Correlation Platform for Distributed IDS. *Proceedings of the 4th International Conference on Network and System Security (NSS).* 24-31.

Rosipal, R. and Girolami, M. (2001). An Expectation-Maximization Approach to Nonlinear Component Analysis. *Neural Computation*. 13(3): 505-510.

Roweis, S. and Ghahramani, E. (1999). A Unifying Review of Linear Gaussian Models.*Computation and Neural Systems.* California Institute of Technology.

Rumelhart, D. E., Hinton, G. E. and Williams, R. J. (1986). Learning Representations by Back-propagating Errors. *Nature*. 323: 533-536.

Sabahi and Movaghar (2011). Intrusion Detection: A Survey. *Proceeding of 3rd Int Conf on Systems and Networks Communications (ICSNS 08).* 23-26.

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

Sadoddin, R. and Ghorbani, A. A. (2009). An Incremental Frequent Structure Mining Framework for Real-time Alert Correlation. *Computers and Security*. 28(3-4): 153- 173.

Sahu, S. and Shandilya, S. K. (2010). A Comprehensive Survey on Intrusion Detection in MANET. *International Journal of Information Technology and Knowledge Management*. 2(2): 305-310.

Sakhnov, K., Verteletskaya, E., and Simak, B. (2011). Echo Delay Estimation Using Algorithms Based on Cross-correlation. *Journal of Convergence Information Technology*. 6(4): 1-11.

Saric, A. and Xiao, J. (2011). Efficient Levenberg-Marquardt Minimization of the Cross-entropy Error Function. *Proceedings of the 2011 International Joint Conference on Neural Networks.* 1-8.

Schneier, B. (1999). *Modeling Security Threats*. Dr. Dobb's Journal.

Sekar, R., Guang, Y., Verma, S. and Shanbhag, T. (1999). A High-performance Network Intrusion Detection System. *ACM Conference on Computer and Communications Security.* Kent Ridge Digital Labs: Singapore. 8-17.

Sendi, A. S., Dagenais, M., Jabbarifar, M. and Couture, M. (2012). Real Time Intrusion Prediction based on Optimized Alerts with Hidden Markov Model. *Journal of Networks*. 7(2): 311-321.

Shankar, U. and Paxson, V. (2001). Active Mapping: Resisting NIDS Evasion

Without Altering Traffic. *Proceedings of the IEEE Symposium on Security and Privacy*. Oakland, California. 44-62.

Sheyner, O. (2004). *Scenario Graphs and Attack Graphs*. Carnegie Mellon University: PhD Thesis.

Sheyner, O. and Wing, J.M. (2004). Tools for Generating and Analyzing Attack Graphs. *Proceedings of Workshop on Formal Methods for Components and Objects*. 344-371.

Sheyner, O., Haines, J., Jha, S., Lippmann, R. and Wing, J. M. (2002). Automated Generation and Analysis of Attack Graph. *Proceedings of the 2002 IEEE Symposium on Security and Privacy (S&P'02)*. 273-284.

Shlens, J. (2003). *A Tutorial on Principal Component Analysis*. www.snl.salk.edu/~shlens/pca.pdf (Accessed: 4 Jan 2008).

Siraj, A. and Rayford, B. V. (2005). Multi-level Alert Clustering for Intrusion Detection Sensor Data. *Annual Meeting of the North American Fuzzy Information Processing Society (NAFIPS 2005)*. 748-753.

Siraj, A. and Rayford, B. V. (2007). Alert Correlation with Abstract Incident Modeling in a Multi-Sensor Environment. *International Journal of Computer Science and Network Security*. 7(8): 8-19.

Smith, R., Japkowicz, N., Dondo, M., and Mason, P. (2008). Using Unsupervised Learning for Network Alert Correlation. *Springer-Verlag: Lecture Notes of Artificial Intelligent. 5032*: 308-319.

Snort (2007). Snort - A Lightweight Intrusion Detection for Networks. http://www.snort.org (Accessed: 2 January 2008).

Sommer, R. and Paxson, V. (2003). Enhancing Byte-level Network Intrusion Detection Signature With Context. *Proceedings of the 10th ACM Conference on Computer and Communication Security*. Washington DC, USA. 262-271.

Spirtes, P., Glymour, C. and Scheines, R. (1993). *Causation, Prediction, and Search*. New York: Springer-Verlag NY, Inc.

Stakhanova, N., Basu, S. and Wong, J. (2007). A Taxonomy of Intrusion Response Systems. *International Journal Information and Computer Security*. 1(1/2): 169-184.

Stallman, R. (1989). GNU General Public License. http://www.gnu.org/copyleft/gpl.txt. (Accessed: 20 February 2008).

Steinder, M. and Sethi A. S. (2004). A Survey of Fault Localization Techniques in

Computer Networks. *Science of Computer Programming.* 53: 165-194.

Stevens (2003). Partial and Semipartial Correlations. Technical report. pages.uoregon.edu/stevensj/MRA/partial.pdf (Accessed: 19 April 2009).

Swiler, L., Phillips, C., Ellis, D. and Chakerian, S. (2000). Computer-attack Graph Generation Tool. *Proceedings of the DARPA Information Survivability Conference and Exposition*.

Sy, J. P. Sy, Taylor, J. M. G. and Cumberland, W. G. (1997). A Stochastic Model for the Analysis of Bivariate Longitudinal AIDS Data. *Biometrics*. 53(2): 542-555.

Takeda, K. and Takefuii, Y. (2001). Pakemon - A Rule Based Network Intrusion Detection Svstem. *International Journal of Knowledge-Based Intelligent Engineering Systems*. 5(4): 240-246.

Tanoto, Y., Ongsakul, W. and Marpaung, C.O.P. (2011). Levenberg-Marquardt Recurrent Networks for Long-Term Electricity Peak Load Forecasting. *TELKOMNIKA.* 9(2): 257-266.

Tedesco, G. and Aickelin, U. (2006). Data Reduction in Intrusion Alert Correlation. *WSEAS Transactions on Computers.* 5(1): January 2006.

Templeton, S.J. and Levitt, K. (2000). A Requires/Provides Model for Computer Attacks. *Proceedings of the 2000 Workshop on New Security Paradigms*. 31-38.

Timm, K. (2001). *Strategies to Reduce False Positives and False Negatives in NIDS*. SecurityFocus Article. http://www.securityfocus.com/infocus/1463 (28 September 2007).

Tjhai, G. C., Funnel, S. M., Papadaki, N. and Clarke, L. (2010). A preliminary Two-stage Alarm Correlation and Filtering System using SOM Neural Network and K-means Algorithm. *Proceedings of Computers and Security*. 712-723.

Toosia, A. N. and Mohsen, K. (2007). A New Approach to Intrusion Detection Based on an Evolutionary Soft Computing Model using Neuro-Fuzzy Classifiers. *Computer Communications*. 30(10): 2201-2212.

Totel, E., Vivinis, B. and Mé, L. (2004). A language driven IDS for event and alert correlation. *IFIP International Federation for Information Processing*. 208-224.

Tsai, A., Zhang, J. and Willsky, A. S. (2001). Expectation-Maximization Algorithms for Image Processing Using Multiscale Models and Mean- field Theory, with Applications to Laser Radar Range Profiling and Segmentation. *Optical Engineering*. 40(7): 1287-1301.

Turner, A. (2000). Tcpreplay. http://tcpreplay.synfin.net/trac/ (Accessed: 18 June

2007).

Turner, J. (2000). New Directions in Communications (or which way to the information age?). *IEEE Communications Magazine*. 24(10): 8-15.

Valdes A. and Skinner, K. (2000). Blue Sensors, Sensor Correlation, and Alert Fusion. *Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID 2000).*

Valdes A. and Skinner, K. (2001). Probabilistic Alert Correlation. *Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID2001).* 54-68.

Valeur, F., Mutz, D. and Vigna, G. (2005). A Learning-based Approach to the Detection of SQL Attacks. *Proceedings of the Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA).* Vienna, Austria.

Valeur, F., Vigna, G. and Kruegel, C., (2004). A Comprehensive Approach to Intrusion Detection Alert Correlation. *IEEE Transactions on Dependable and Secure Computing.* 1(3): 146-169.

Walker, C. L. F., Perin, J., Aryee, M. J., Pinto, C. B. and Black, R. E. (2012). Diarrhea Incidence in Low- and Middle-income Countries in 1990 and 2010: A Systematic Review. *BMC Public Health.* doi:10.1186/1471-2458-12-220.

Wang, J. X., Wang, Z. Y. and Dai, K. (2006). Intrusion Alert Analysis Based on PCA and the LVQ Neural Network. *Proceedings of the International Conference on Neural Information (ICONIP 2006)*. 217-224.

Wang, L., Liu, A. and Jajodia, S. (2006). Using Attack Graphs for Correlating, Hypothesizing, and Predicting Intrusion Alerts. *Computer Communications*. 29(15): 2917-2933.

Warfield, S., Zou, K. and Wells, W. (2002). Validation of Image Segmentation and Expert Quality with an Expectation-Maximization Algorithm. Lecture Notes in Computer Science. Springer Berlin / Heidelberg. Volume 2488/2002. 298-306.

Wasserman, L. (2004). *All of Statistics: A Concise Course in Statistical Inference*. Springer.

Wei, C. C. (2012). RBF Neural Networks Combined with Principal Component Analysis Applied to Quantitative Precipitation Forecast for a Reservoir Watershed during Typhoon Periods. *Journal of Hydrometeor*. 13: 722-734.

Werbos, P. J. (1988). Back-propagation: Past and future. *Proceeding of the International Conference on Neural Networks*. 1: 343-354.

Wilamowski, B.M. and Yu, H. (2010). Improved Computation for Levenberg–Marquardt Training. *IEEE Transactions on Neural Networks.* 21(6): 930-937.

Wilamowski, B.M., Iplikci, S., Kaynak, O. and Efe, M.O. (2001). An algorithm for fast convergence in training neural networks. *Proceedings of the IEEE International Joint Conference on Neural Networks.* 3: 1778-1782.

Wing, J. M. (2005). Scenario Graphs Applied to Security. *Proceedings of Workshop on Verification of Infinite State Systems with Applications to Security*. Timisoara, Romania. Summary paper.

Witten, I. H. and Frank, E. (2000). WEKA *Data Mining: Practical Machine Learning Tools and Techniques with Java Implementations*. Morgan Kaufmann Publishers.

Wu, J., Chen, J., Zhang, X. and Chen, J. (2010). The Segmentation of Brain MR Images Using Reformative Expectation-Maximization Algorithm. *International Journal of Image and Graphics (IJIG).* 10(2): 289-297.

Wu, P., Bhatnagar, R., Epshtein, L., Bhandaru, M. and Shi, Z. (1998). Alarm Correlation Engine (ACE). *Proceedings Network Operation and Management Symposium (NOMS'98)*. New Orleans, LA. 733-742.

Xiang, G., Dong, X. and Yu, G. (2005). Correlating Alerts with a Data Mining Based Approach. *Proceedings of the 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'05).* 341-346.

Xiaoqiang, Z., Zhongliang, Z. and Pingzhi, F. (2007). *Journal of Electronics (China)*. 24(5): 679-685.

Xiou, M. and Xiou, D. (2007). Alert Verification Based on Attack Classification in Collaborative Intrusion Detection. *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007)*. 739-744.

Xu, D. (2006). *Correlation Analysis of Intrusion Alerts.* North Carolina State University, USA: PhD Thesis.

Yang, Q., Deng, B., Lu, W., Shen, F., Chen, R., Wang, Y., Du, G., Yan, F., Xiao, T. and Xu, H. (2012). Fast and Accurate X-ray Fluorescence Computed Tomography Imaging with the Ordered-subsets Expectation Maximization Algorithm. *Journal of Synchrotron Radiation.* 19: 210-215.

Ye, N., Giordano, J., Feldman, J. and Zhong, Q. (1998). Information Fusion Techniques for Network Intrusion Detection. *IEEE Information Technology*

Conference, Information Environment for the Future. 117-120.

Yu, D. and Frincke, D. (2004). A Novel Framework for Alert Correlation and Understanding. *International Conference on Applied Cryptography and Network Security (ACNS).* Springer Verlag: Lecture Notes Computer Science. 3089: 452-466.

Yu, D. and Frincke, D. (2005). Alert Confidence Fusion in Intrusion Detection Systems with Extended Dempster–Shafer Theory. *Proceedings of ACMSE 2005.*

Yu, D. and Frincke, D. (2007). Improving the Quality of Alerts and Predicting Intruder's Next Goal with Hidden Colored Petri-Net. *Computer Networks.* 51: 632-654.

Zadeh, L. A. (1994). Soft Computing and Fuzzy Logic. *IEEE Software.* 11(6): 48-56.

Zakaria, Z., Isa, N. and Suandi, S. A. (2010). A Study on Neural Network Training Algorithm for Multiface Detection in Static Images. *World Academy of Science, Engineering and Technology*.

Zhai, Y. (2006). *Integrating Multiple Information Resources to Analyze Intrusion Alerts*. North Carolina State University, USA: PhD Thesis.

Zhu, B. and Ghorbani, A. A. (2005). Alert Correlation for Extracting Attack Strategies. *International Journal of Network Security.* 3(2): 259-270.

Zurutuza, U. and Uribeetxeberria, R. (2004). Intrusion Detection Alarm Correlation: A Survey. *Proceedings of the IADAT International Conference on Telecommunications and Computer Networks.*