AN EFFECTIVE ATTACK SCENARIO CONSTRUCTION MODEL BASED ON TWO-TIER FEATURE SELECTION AND COARSE GRAIN CLEANING

TAGWA AHMED MOHAMMED ALHAJ

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

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

DECEMBER 2018

This thesis is dedicated…

To my parents, **Ahmed and Awatif,** for their endless love, support and whose good examples have taught me to work hard for the things that I aspire to achieve. To my husband, **Hani,** for his continuous support and the inspiration throughout the journey.

To my Brothers and Sisters, **Raja, Mohammed, Abdullah, Fatin, Yasir** and **Amar** for their words of encouragement to keep on striving to complete this research.

ACKNOWLEDGEMENT

First and foremost, I thank Allah S.W.T, the Most Merciful for giving me, the strength and persistence to complete this research. I would like to sincerely thank my main supervisor **Dr. Maheyzah Md Siraj** for her guidance and support throughout this study. It has been an honour to be her first Ph.D. student. I appreciate all her contributions of time, ideas, and funding to make my Ph.D. experience productive and stimulating. As for my co-supervisor **Dr. Anazida Zainal**, special thanks for her encouragement and support. I am grateful for her guidance and the opportunities she has afforded me. She is incredibly organized and a great problems solver. My deepest gratitude also extends to all my family members who have provided assistance continues support and endless love. Last but not least to all my friends and lab members, thank you for your understanding and encouragement in my many, many moments of crisis. Your friendship makes my life a wonderful experience.

ABSTRACT

Attack Scenario Construction (ASC) via Alert Correlation (AC) is important to reveal the strategy of attack in terms of steps and stages that need to be launched to make the attack successful. Previous works on AC used two approaches which are Structural-based Alert Correlation (SAC) that clusters the alerts features to reveal a list of attack steps, and Casual-based Alert Correlation (CAC) which classifies the alerts based on the cause-effect relationship. However, major limitations of previous works have been found to have false and incomplete correlations due to inaccurate attack step identification based on different set of features, infiltration of raw alerts and failure to identify the sequence of attack stages. Therefore, an ASC model was developed to select significant features and to discover the complete correlations. Firstly, this research designed a two-tier feature selection using Information Gain (IG) for optimal accuracy on attack steps identification. Secondly, preserving the alerts using coarse grain cleaning for accurate attack stages identification was carried out. Finally, an effective attack scenario model to discover a complete relationship among alerts by identifying and mapping the related alerts was constructed. The model was successfully experimented using two types of datasets which are DARPA2000 and ISCX2012. The Completeness and Soundness of the model were measured to evaluate the overall correlation effectiveness. The existing works achieved 76% average completeness in comparison to the proposed model which achieved 100% completeness resulting in a 24% improvement. With regard to soundness measurement, the existing work scored 83.055% soundness while the proposed model soundness reached 100%, which has a 16.9% improvement. The findings has shown that this research is significant to Security Analyst (SA) for designing responsive and preventive mechanisms which are effective and reliable in protecting and securing computer networks.

ABSTRAK

Pembinaan Senario Serangan (ASC) melalui Korelasi Amaran (AC) adalah penting untuk mendedahkan strategi serangan dari segi langkah dan peringkat yang perlu dilancarkan untuk membuat serangan itu berjaya. Kerja-kerja terdahulu dalam AC menggunakan dua pendekatan iaitu Korelasi Amaran berdasarkan Struktural (SAC) yang mengelompokkan ciri amaran untuk mendedahkan senarai langkah serangan dan Korelasi Isyarat berasaskan Kasual (CAC) yang mengklasifikasikan peringatan berdasarkan hubungan sebab-akibat. Walau bagaimanapun, kekangan utama kajian terdahulu didapati mempunyai korelasi palsu dan tidak lengkap disebabkan oleh ketepatan pengenalan langkah serangan tidak tepat berdasarkan set ciri yang berbeza, penyusupan amaran mentah dan kegagalan untuk mengenal pasti urutan peringkat serangan. Oleh itu, model ASC telah dibangunkan untuk memilih ciri-ciri penting dan menemui korelasi yang lengkap. Pertama, kajian ini mencadangkan pemilihan ciri dua peringkat menggunakan Pengumpulan Maklumat (IG) untuk ketepatan optimum mengenai langkah-langkah pengesanan serangan. Kedua, memelihara amaran dengan menggunakan pembersihan butiran kasar untuk mengenal pasti tahap serangan tepat yang telah dicadangkan. Akhir sekali, model senario serangan yang berkesan untuk mencari hubungan yang lengkap di kalangan amaran dengan mengenal pasti dan memetakan isyarat yang berkaitan telah dibina. Model ini telah berjaya dieksperimen dengan menggunakan dua jenis dataset iaitu DARPA2000 dan ISCX2012. Kesempurnaan dan keberkesanan model diukur untuk menilai keberkesanan korelasi secara keseluruhan. Kajian sedia ada mencapai kesempurnaan purata 76% berbanding dengan model yang dicadangkan yang mencapai kesempurnaan 100% yang menghasilkan peningkatan sebanyak 24%. Berkenaan dengan pengukuran keberkesanan, kerja sedia ada memberikan 83.055% keberkesanan sementara model yang dicadangkan mencapai 100%, yang membawa kepada peningkatan sebanyak 16.9%. Dapatan ini menunjukkan bahawa kajian ini penting kepada Penganalisis Keselamatan (SA) untuk mereka bentuk mekanisme responsif dan pencegahan yang berkesan dan boleh dipercayai dalam melindungi dan menjamin rangkaian komputer.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

AA	-	AutoAssociator
AC	-	Alert Correlation
ACC	-	Accuracy
ACM	-	Alert Correlation Matrix
AFB	-	Air Force Base
AIRS	-	Artificial Immune Recognition System
AR	-	Accuracy Rate
ASC	-	Attack Scenario Construction
CAC	-	Causal-based Alert Correlation
CAML	-	Correlated Attack Modelling Language
CC	-	Coordination Center
CV	-	Cross Validation
DAG	-	Directed Acyclic Graph
DDoS	-	Distributed Denial of Services
DMZ	-	Demilitarized Zone
DoS	-	Denial of Service
EC	-	Event Correlations
EM	-	Expectation Maximization
EWSs	-	Early Warning Systems
fp	-	False Positives
FTP	-	File Transfer Protocol
GCT	-	Granger Causality Test
GRBF	-	Gaussian Radial Basis Function
HAC	-	Hybrid-based Alert Correlation
HMM	-	Hidden Markov Model
IC	-	Intrusion Correlation

IDMEF	-	IDMEF Intrusion Detection Message Exchange Format
IDS	-	Intrusion Detection System
IG	-	Information Gain
IP	-	Internet Protocol
IPCAEMP	-	IUR, PCA, EM, Post-clustering model
IPCALM	-	IUR, PCA, LM model
IUR	-	Improved Unit Range
LAMDBA	-	Language Model Database for Detection of Attacks
LM	-	Levenberg-Marquardt
MAE	-	Mean Absolute Error
MLP	-	Multilayer Perceptron
NIDS	-	Network-based IDS
ODF	-	Optimal Decision Function
PCA	-	Principal Component Analysis
PS	-	Percentage Split
Rc	-	Completeness
Rs	-	Soundness
SAC	-	Structural-based Alert Correlation
SMTP	-	Simple Mail Transfer Protocol
SOM	-	Self-Organizing-Maps
StAC	-	Statistical Alert Correlation
STAT	-	State Transition Analysis Technique
STATL	-	State Transition Attack Language
SVM	-	Support Vector Machine
TIAA	-	Tool for Intrusion Alert Analysis
tn	-	True Negatives
tp	-	True Positives
UR	-	Unit Range
XML	-	Extended Markup Language

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Problem Background

With the advent of new technologies and various services provided in the context of computer networks, a considerably large volume of information is now being generated. The main challenge in this area is the provision of network protection services against various threats and vulnerabilities (Ramaki *et al.,* 2015). Information Assurance and Security (IAS) is an important research area in network security and distributed information. IAS makes all efforts to protect and secure information.

The studies on prevention, detection and forensic aspect of computer network attacks have long been researched. Encryption, Virtual Private Network (VPN) and firewalls are examples of some prevention techniques (Kavousi and Akbari, 2014). However, these techniques reduce exposure rather than monitor or eliminate vulnerabilities in computer systems (Ghosh *et al*., 1998). It is important to have a detecting and monitoring network which can protect information in the networks, including detection of intrusions by security sensors and responding toward them. Therefore, these challenges have motivated various security-related research studies to propose new solutions that might not be manageable by conventional security approaches.

Network Intrusion Detection System (NIDS) is a monitoring tool used to monitor and protect networks from attack. The main goal of NIDS is to monitor system environments and detect network threats (Wang and Chiou, 2016). NIDS generate huge amount of low level intrusion alerts, which makes it difficult to analysis the alerts from these large datasets (Yao *et al.,* 2016; Shittu *et al*., 2015). Alert analysis is an essential part of the tasks of Security Analyst (SA) in order to describe the level of significance of an attack. It recognizes the plans or the strategies of intrusions and thereby infers the goal of the attacker. The majority of the research contributions in alert analysis focus, on the attack scenario construction to extract attack intelligence (Yao *et al*., 2016).

The attack scenario elicits the steps and actions taken by the intruder to breach the system. In practice, an attack scenario consists of a number of attack stages, and an attack stage contains a list of attack steps. For example, according to Ning *et al.,* (2002) in Distributed Denial of service (DDoS) attacks, the attacker has to install the DDOS daemon programs before instructing the daemons to launch an attack. In other words, an attacker has to reach a certain stage before launching some other attacks steps. In more details, Siraj (2013) described the relationship between the real attack scenarios, steps and stages: attack scenario is composed of a series of attack stages. The attack stages contain at least one attack step. An attack step will create several network events. The NIDS determines if a network event can be classified as an intrusion. If the NIDS identifies a network event as an intrusion, then an alert is produced and recorded as shown in Figure 1.1.

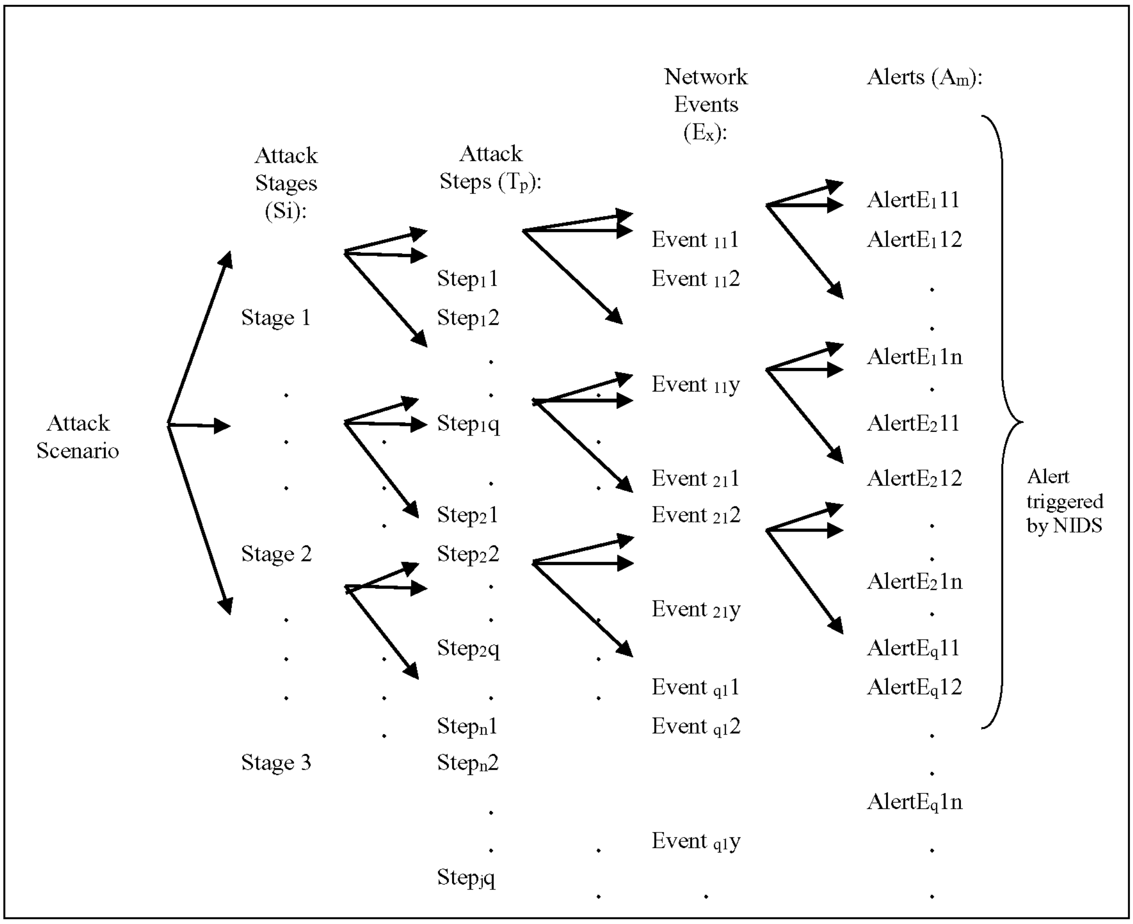

Figure 1.1: The relationship of attack steps and attack stages in attack scenario.

In Figure 1.1, the set of j attack stages in a multi-stage network is represented by $Si = \{S_1, S_2, \ldots, S_i, \ldots, S_j\}$. Each S_i is composed of q attack steps that reflect the goals of the attacker. T_p, where $p = 1, 2, \ldots, q$ and $T_p \subseteq S_i$, expresses an Attack Step. Every T_p adds to y network events that will be assessed by the NIDS to determine if any intrusive patterns are present.

NIDS identified intrusions is expressed as E_x, where $x = 1, 2, \ldots, y$ and $E_x \subseteq T_p \subseteq S_i$. When an E_x occurs, the NIDS will create n alerts to describe the intrusion. Alerts are expressed as A_m, where $m = 1, 2, \ldots, n$ and $A_m \subseteq E_x \subseteq T_p \subseteq S_i$. Alert sets are produced and recorded for the SA. SA's use these unlabelled low level alerts to examine and understand the attack scenario even though there is no prior knowledge about the underlying cause of the alert.

Understanding the attack scenario allows the SA to identify the compromised resources, spot the system vulnerabilities, and determine the intruder objectives and the attack severity (Saad and Traore, 2013). However, the Security Analyst (SA) cannot capture the logical steps or scenarios behind these attacks. Thus, the attacks scenarios cannot be recognized and identified directly from the alerts as occurring due to the following causes:

i. The SA is overwhelmed with a huge number of alerts (alert flooding) most of which are redundant (duplicate), false positives, or irrelevant. The organizations use heterogeneous and cooperative NIDSs in order to provide a global view of intrusion activities, and offer better network protection (Yao *et al.,* 2016).
ii. NIDSs trigger alerts independently in low-level information that describe individual attack steps and are not designed to recognize the attack plans or discover multistage attack scenarios. Therefore, identifying the scenario of attack directly from these alerts is unmanageable due to problems with detailing a low level of information (Li and Tian, 2010; GhasemiGol *et al.,* 2016).

Therefore, in order to take appropriate responses and design adequate defensive and preventive scenarios these low level alerts must be structured adequately and mapped into meaningful attack scenarios (Li and Tian, 2010; Saad and Traore, 2013).

At the core of the attack scenario construction process is the Alert Correlation (AC), which takes a set of alerts produced by one or more NIDSs as input and generates a high-level view of occurring or attempted intrusions (Saad and Traore, 2013). It is defined as a process that contains multiple components with the purpose of analyzing alerts and can provide a high-level insight on the security state of the network under surveillance (GhasemiGol and Ghaemi-Bafghi, 2015). It finds and discovers the relationships among unrelated alerts and their attributes that reveal the behavior of the attacker by finding similarity or causality between the alerts (Saad and Traore, 2013).

In the alert similarity relationship, certain relations and associations between the alerts have been discovered based on structure or physical properties of alerts. It is named as Structural-based Alert Correlation (SAC). The amount of alerts is reduced by clustering them based on their attributes or features (Salah *et al.,* 2013). Furthermore, a pattern of attack steps can be identified by grouping and clustering the alerts based on proper similarity features. Previous researchers (Siraj, 2013; Elshoush, 2014; Bateni *et al*., 2013; Shittu *et al*., 2015) selected different features based on their knowledge, experience and data sources and grouping the alerts based on the similarity of these features. However, the selection of different features led to inconsistence clustering performance and less accuracy of identification of attack steps. In addition, the causal relationships between alerts cannot be detected in this category, because it simply works on an attribute level.

Meanwhile, the causality relationship which known as Causal-based Alert Correlation (CAC) has two main aspects to construct the attack scenario in literature. Few works defined the causality by identifying which alerts cause an attack stage for a multi-stage network attack (Mathew *et al*., 2005; Siraj, 2013). Their idea closely related to a classification problem because it attempts to classify the alerts into the corresponding class/ stages. Siraj (2013) predicted the membership of each alert into the predetermined classes or attack stages. However, a large number of alerts are deleted and filtered out through the improvement of alerts quality. Such regressive cleaning of data may loss important alert that may help in the attack stage identification.

In the second aspect, most of the existing works (Zhu and Ghorbani, 2006; Marchetti, 2011; Soleimani and Ghrobani, 2012; Huang *et al.,* 2012; Saad and Traore, 2013; Ramaki *et al.,* 2015) tend to find the causality for Attack Scenario Construction (ASC) using three categories , which are: Scenario-based; Rule based; and machine learning-based. In Scenario-based, some attack scenario template are predefined. Whenever a new alert is received, it is compared with the existing scenarios and then added to the most likely candidate scenario (Salah *et al*., 2010). There are huge numbers of correlation languages related to the specification of attack scenarios have been proposed to implement well defined scenarios (Salah *et al.,* 2010). This approach works with the hypothesis of that alerts that belonging to one problem have similar attributes values. The alerts that contribute to the construction of a predefined scenario should be correlated. The main advantage of this approach is that it is able to accurately detect well-documented attacks derived from the libraries. But if it is a novel attack, the method will fail to detect the intrusion (Chahira and Kemei, 2016). However, the limitation of this approach is the need for more complete and comprehensive scenario libraries; the time and cost required to build and maintain them are the main concerns.

Rule-based approaches are one of the main categories used by many researchers (Ning *et al.,* 2004; Ding, 2007; Saad and Traore,2012). The knowledge is implemented as conditional, if-then rules. The events when they come are matched with these set of rules (Salah *et al.,* 2010). Each rule contains two main expressions which are formulas of predicate calculus linked by an implication connective (=>). The left side of the rule contains a prerequisite (pre-conditions) that must exist for an attack to be finished. The right side which is consequences (post-conditions) presents the action to be executed if the rule is applicable. They are the effects that remain after an attack has occurred. Exact and partial are two types of rules matching. In exact rule matching, the left side of the rule should be matched before specifying which action should be triggered. Meanwhile in partial matching, the action is determined if some, but not all, of these conditions are satisfied. This approach does not require profound understanding of the underlying architectural and operational principles of a system. In addition, it is modularized, and easy to maintain when deploy on small systems. However, it cannot enumerate and encode all possible rules of an individual attack. In addition, the conditions of an attack should not be mistaken for the necessary existence of an earlier attack.

Machine learning-based employs a different learning algorithm on training data-set and uses knowledge-based data derived from human experts to identify attack scenarios on intrusion patterns and relationships among alerts. Some relation rules or patterns will be created from correlation relationships that satisfy some statistical criteria. This involves pair-wise comparisons between alerts since every two alerts might be similar and therefore can be correlated (Sadoddin *et al.,* 2009). In this case, the repeated comparisons between alerts will lead to a huge computational overload especially in large scale networks. This approach requires a lengthy initial period of training (Mahboubian *et al.*, 2012). Moreover, the risk of overfitting the model can result in a poor attack scenario construction. Also, some of machine learning techniques are not fully automated and required, as a result, significant human supervision. (Ahmed, 2014).

Finally, from the above argument and discussion, the processing of hidden, missing, and false relationships, has largely been ignored by most of this approaches because they deal with raw alerts and do not take into account the sequence and order of the attack (Saad and Traore, 2013). In addition, redundant relationship has been generated due to different attempts of attack by using different parameters until the host is compromised. Therefore, limitations motivate this research to construct an effective attack scenario model by identifying accurate attack steps and stages. In addition, the purpose of the proposed model is to provide alert analysis that can discover complete relationships among alerts. Such transition of motivation is summarized in Figure 1.2.

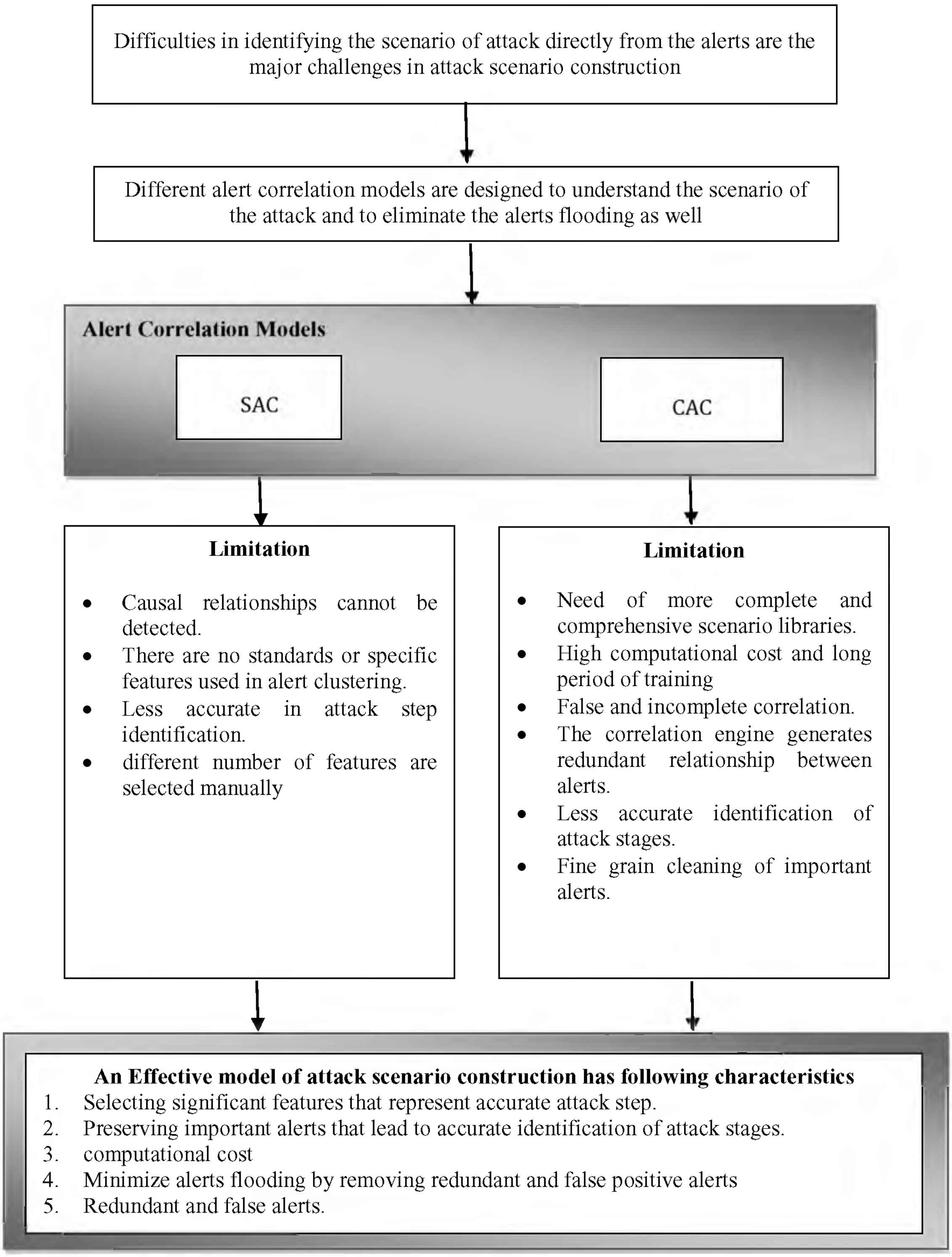

Figure 1.2: Motivation of this research

1.2 Problem Statement

Unidentified the attack scenario directly from the alerts is the main issue of alert analysis. Most of the existing attack scenario construction models have false, redundant and incomplete relationships because they are dealing with redundant and irrelevant alerts and did not take into account the sequence and order of attack stages. Therefore, in order to take suitable responses and design sufficient defensive and preventive scenarios low level alerts information must be structured, mapped into meaningful attack scenarios and an effective attack scenario construction model is needed.

Thus, the main research question is:
How to discover complete relationship among known and new alerts patterns in order to identify the logical correlation behind the attack by constructing the attack scenario?

The research hypothesis is as follows:
Complete alert relationships among alerts could be discovered by considering an accurate identification of attack steps, stages and effective attack scenario construction.

The following are the supporting research questions that will be addressed:

i. How accurate attack steps from the alerts can be identified?
ii. How accurate attack stages can be identified?
iii. How an effective attack scenario can be constructed?

1.3 Research Aim

The aim of this research is to propose an effective attack scenario construction model that can discover complete relationships among known and new alerts and offer optimal performance for identification of the logical correlation behind the attack.

1.4 Research Objectives

The objectives of this research are:

i. To identify accurate attack steps by selecting significant features from the alerts.
ii. To identify an accurate attack stages by preserving important alerts and filtering redundant and false alerts.
iii. To construct an effective attack scenarios construction model that can discover complete relationships among alerts by identifying and mapping the related alerts.

1.5 Research Significant

The research is important and significant from theoretical and practical perspectives. The rationale and motivation for this research are as follows:

i. In a structural-based alert correlation method, alerts are clustered and grouped based on similarity of features to identify the list of attack steps. This research focuses on selecting significant features that could represent accurate attack steps.
ii. The attacks become more complex and more frequent (higher intensity) which lead to more vulnerability of computer networks.

Therefore, timely and accurate classification of alerts has long been a subject of research and continues to be pursued so as to identify which alerts cause an attack stage for multi-stage network attacks.

iii. Identifying the attack plan at early stage of alert analysis would stop the attack from escalating and damaging the network.

iv. Construct an effective attack scenario model that provides a complete relationship among the alerts give to SA complete view of attack intention.

v. NIDSs generated huge amount of useless low-level alerts unless they are analyzed.

1.6 Research Contributions

This section discusses the contributions of this research. The main contribution of this research is the proposal of construction an effective attack scenario model. It identifies and maps the related alerts into a relevant attack scenario. Other specific contributions are:

i. Identify accurate attack steps. It is aimed to group and cluster the alerts based on the appropriate features.

ii. Identify accurate attack stages. It is intended to predict the membership of each new alert into predetermined classes or attack stages and identify accurate attack stages.

1.7 Definition of Terms

Alert	-	A notification of the occurrence of specific events that match the signatures or deviates from normal activities

Attack Steps	-	Steps involved in an attack stage
Attack Stages	-	Stages involved in the attack strategy
Attack Scenario	-	A complete attack launched by an attacker which consists of attack steps and attack stages.
Event	-	A low-level entity used by NIDS to detect the sign of an attack; for example, network traffic or network packet
Structural-based	-	Certain relations and associations between the alerts have been discovered based on structure or physical properties of alerts
Causal-based	-	Correlating alerts based on their causes
Alert correlation	-	A process that contains multiple components with the purpose of analyzing alerts and can provide a high-level insight on the security state of the network under surveillance.
Intra stages	-	Finds the similarity between alerts inside a single stage
Inter stages	-	Finds the alert similarity between multiple stages
Attack graph	-	Directed graph with nodes and edges that show the overall scenario of an attack

1.8 Organization of the thesis

The thesis is structured into seven chapters as presented in Figure 1.3 below.

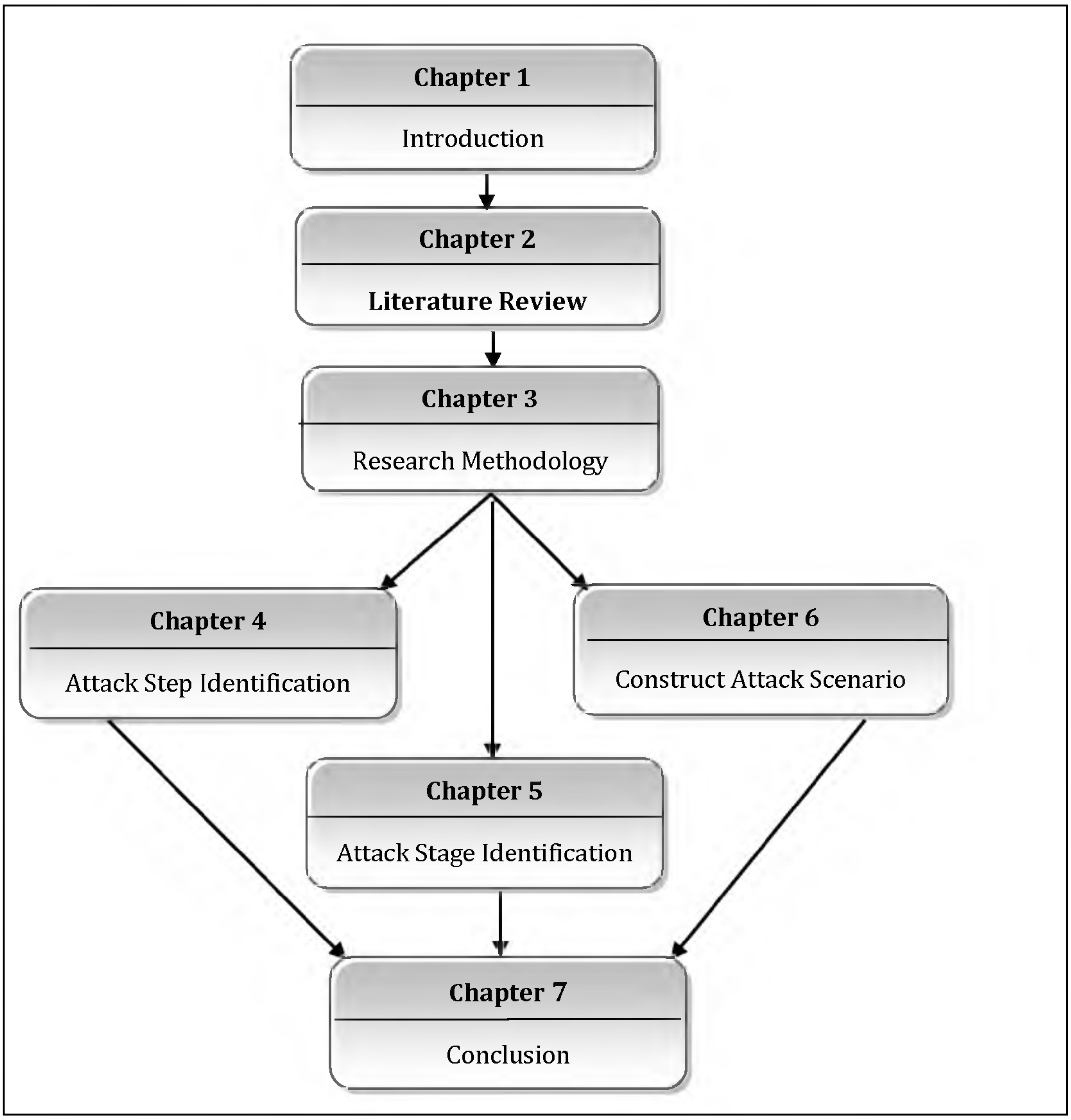

Figure 1.3: Thesis Organization

Chapter 1 is an introduction to the research. Chapter 2 provides background information and a review of related literature that led to the formulation of the research problem. Chapter 3 describes the research methodology. Chapter 4 addresses the identification of the attack steps. Chapter 5 focuses on the attack stage identification. Chapter 6 presents an effective attack scenario model. Finally, Chapter 7 concludes the thesis with lists of contributions and suggestions for future work.

REFERENCES

Ahmadian Ramaki, A. and Rasoolzadegan, A. (2016). Causal knowledge analysis for detecting and modeling multi-step attacks. *Security and Communication Networks,* 9(18), 6042-6065. doi:10.1002/sec.1756.

Ahmadian Ramaki, A. and Rasoolzadegan, A. (2017). Causal Knowledge Analysis for Detecting and Modeling. *Security and Communication Networks,* 9(18).

Ahmadinejad, S.H. and Jalili, S. (2009). Alert correlation using correlation probability estimation and time windows. In *International Conference on Computer Technology and Development,* 170-175. doi:10.1109/ICCTD.2009.22.

Ahmed, A.A. and Zaman, N.a.K. (2017). Attack Intention Recognition: A Review. *International Journal of Network Security,* 19(2), 244-250. doi: 10.6633/IJNS.201703.19(2).09.

Ahmed, A.A., Jantan, A. and Wan, T.-C. (2016). Filtration model for the detection of malicious traffic in large-scale networks. *Computer Communications,* 82, 59-70. doi:10.1016/j.comcom.2015.10.012.

Ahmed, S. S. (2014). *Intrusion Alert Analysis Framework Using Semantic Correlation.* (Doctoral dissertation). University of Victoria, Canada.

Al-Mamory, S.O. and Zhang, H. (2007). A survey on IDS alerts processing techniques. In *Proceeding of the 6th WSEAS international conference on information security and privacy, Spain,* 69-78.

Al-Mamory, S.O. and Zhang, H. (2009). Intrusion detection alarms reduction using root cause analysis and clustering. *Computer Communications,* 32(2), 419-430. doi:10.1016/j.comcom.2008.11.012.

Alserhani, F. (2013). A framework for multi-stage attack detection. In *IEEE Electronics, Communications and Photonics Conference (SIECPC),* 1-6. doi:10.1109/SIECPC.2013.6550973.

Alserhani, F., Akhlaq, M., Awan, I.U., Cullen, A.J. and Mirchandani, P. (2010). MARS: multi-stage attack recognition system. In *IEEE International Conference on Advanced Information Networking and Applications*, 753-759. doi:10.1109/AINA.2010.57.

Alserhani, F.M. (2016). Alert correlation and aggregation techniques for reduction of security alerts and detection of multistage attack. *International Journal of Advanced Studies in Computers, Science and Engineering,* 5(2), 1.

Alshammari, R., Sonamthiang, S., Teimouri, M. and Riordan, D. (2007). Using neuro-fuzzy approach to reduce false positive alerts. In *IEEE Fifth Annual Conference on Communication Networks and Services Research,* 345-349. doi:10.1109/CNSR.2007.70.

Ammar, A. (2015). A decision tree classifier for intrusion detection priority tagging. *Journal of Computer and Communications.* 3(04), 52 -58. doi:10.4236/jcc.2015.34006.

Anbarestani, R., Akbari, B. and Fathi, F. (2012). An iterative alert correlation method for extracting network intrusion scenarios. In *20th Iranian Conference on Electrical Engineering (ICEE),* 684-689. doi:10.1109/IranianCEE.2012.6292441.

Anderson, J.P. (1980). *Computer security threat monitoring and surveillance.* Technical report, James P. Anderson Company, Fort Washington, Pennsylvania.

Bahrbegi, H., Navin, A.H., Ahrabi, A.a.A., Mirnia, M.K. and Mollanejad, A. (2010). A new system to evaluate GA-based clustering algorithms in Intrusion Detection alert management system. In *IEEE Second World Congress on Nature and Biologically Inspired Computing (NaBIC),* 115-120. doi:10.1109/NABIC.2010.5716289.

Bai, H., Wang, K., Hu, C., Zhang, G. and Jing, X. (2011). Boosting performance in attack intention recognition by integrating multiple techniques. *Frontiers of Computer Science in China,* 5(1), 109-118. doi:10.1007/s11704-010-0321-y

Bateni, M. and Baraani, A. (2014). An Architecture for Alert Correlation Inspired By a Comprehensive Model of Human Immune System. *International Journal of Computer Network and Information Security,* 6(12), 47. doi:10.5815/ijcnis.2014.12.06.

Bateni, M., Baraani, A. and Ghorbani, A. (2013a). Using Artificial Immune System and Fuzzy Logic for Alert Correlation. *IJ Network Security,* 15(1), 160-174.

Bateni, M., Baraani, A., Ghorbani, A. and Rezaei, A. (2013b). An ais-inspired architecture for alert correlation. *International Journal of innovative Computing, Information & Control,* 9(1), 231-255.

Bhatt, P., Yano, E.T. and Gustavsson, P. (2014). Towards a framework to detect multi-stage advanced persistent threats attacks. In IEEE *8th International Symposium on Service Oriented System Engineering (SOSE),* 390-395. doi:10.1109/SOSE.2014.53.

Bolon-Canedo, V., Sanchez-Marono, N. and Alonso-Betanzos, A. (2011). Feature selection and classification in multiple class datasets: An application to KDD Cup 99 dataset. *Expert Systems with Applications,* 38(5), 5947-5957. doi:10.1016/j.eswa.2010.11.028.

Bul'ajoul, W., James, A. and Pannu, M. (2015). Improving network intrusion detection system performance through quality of service configuration and parallel technology. *Journal of Computer and System Sciences,* 81(6), 981-999. doi:10.1016/j.jcss.2014.12.012.

Chahira, J.M. and Kemei, P.K (2016). A Review of Intrusion Alerts Correlation Frameworks. *International Journal of Computer Applications Technology and Research,* 5 (4), 226 -233, doi:10.7753/IJCATR0504.1009.

Chandrashekar, G. and Sahin, F. (2014). A survey on feature selection methods. *Computers & Electrical Engineering,* 40(1), 16-28. doi:10.1016/j.compeleceng.2013.11.024.

Che, T., Ma, J., Li, N. and Wang, C. (2015). A Security Quantitative Analysis Method For Access Control Based on Security Entropy. *IJ Network Security,* 17(5), 517-521.

Cipriano, C., Zand, A., Houmansadr, A., Kruegel, C. and Vigna, G. (2011). Nexat: A history-based approach to predict attacker actions. In ACM *Proceedings of the 27th Annual Computer Security Applications Conference*, 383-392.

Cuppens, F. (2001). Managing Alerts in a Multi-Intrusion Detection Environment. In *Seventeenth Annual Computer Security Applications Conference,* 22. doi:10.1109/ACSAC.2001.991518.

Cuppens, F. and Miege, A. (2002). Alert correlation in a cooperative intrusion detection framework. In *Proceedings IEEE Symposium on Security and Privacy,* 202-215. doi:10.1109/SECPRI.2002.1004372.

Cuppens, F. and Ortalo, R. (2000). Lambda: A language to model a database for detection of attacks. In *International Workshop on Recent Advances in Intrusion Detection*, 197-216. Springer, Berlin, Heidelberg.

Davis, J.J. and Clark, A.J. (2011). Data preprocessing for anomaly based network intrusion detection: A review. *Computers & Security,* 30(6), 353-375. doi:10.1016/j.cose.2011.05.008.

Debar, H. and Wespi, A. (2001). Aggregation and correlation of intrusion-detection alerts. In *International Workshop on Recent Advances in Intrusion Detection*, 85-103. Springer, Berlin, Heidelberg.

Denning, D.E. (1987). An intrusion-detection model. In *IEEE Transactions on Software Engineering,* 13(2), 222-232. doi:10.1109/TSE.1987.232894.

Dua, S. and Du, X. (2016). *Data mining and machine learning in cybersecurity.* CRC Press.

Ebrahimi, A., Navin, A.H.Z., Mirnia, M.K., Bahrbegi, H. and Ahrabi, A.a.A. (2011). Automatic attack scenario discovering based on a new alert correlation method. In *IEEE International Systems Conference (SysCon),* 52-58. doi:10.1109/SYSCON.2011.5929072.

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. doi:10.3233/JCS-2002-101-204.

Elshoush, H.T. and Osman, I.M. (2013). *Intrusion alert correlation framework: an innovative approach*. In *IAENG Transactions on Engineering Technologies,* 405-420. Springer, Dordrecht.

Elshoush, H.T.I. (2014). Reducing the Correlation Processing Time by Using a Novel Intrusion Alert Correlation Model. *International Journal of Advanced Computer Science and Applications*, 132-141.

Faraji Daneshgar, F. and Abbaspour, M. (2016). Extracting fuzzy attack patterns using an online fuzzy adaptive alert correlation framework. *Security and Communication Networks,* 9(14), 2245-2260. doi:10.1002/sec.1483.

Farhadi, H., Amirhaeri, M. and Khansari, M. (2015). Alert correlation and prediction using data mining and HMM. *The ISC International Journal of Information Security,* 3(2). 77-101. doi:10.22042/isecure.2015.3.2.3.

GhasemiGol, M. and Ghaemi-Bafghi, A. (2015). E-correlator: an entropy-based alert correlation system. *Security and Communication Networks,* 8(5), 822-836. doi:10.1002/sec.1039.

GhasemiGol, M., Ghaemi-Bafghi, A. and Takabi, H. (2016). A comprehensive approach for network attack forecasting. *Computers & Security,* 58, 83-105. doi:10.1016/j.cose.2015.11.005.

Ghosh, A.K., Wanken, J. and Charron, F. (1998). Detecting anomalous and unknown intrusions against programs. In *Proceedings 14th Annual Computer Security Applications Conference,* 259-267. doi:10.1109/CSAC.1998.738646.

Gupta, B.B., Joshi, R.C. and Misra, M. (2012). ANN Based Scheme to Predict Number of Zombies in a DDoS Attack. *IJ Network Security,* 13(3), 216-225.

Han, J. and Fu, Y. (1994). Dynamic Generation and Refinement of Concept Hierarchies for Knowledge Discovery in Databases. *KDD Workshop*. 157-168.

Hebb, D.O. (1949). The first stage of perception: Growth of the assembly. *The Organization of Behavior.* 60-78. New York: Wiley.

Huang, C.-J., Hu, K.-W., Cheng, H., Chang, T.-K., Luo, Y.-C. and Lien, Y.-J. (2012). Application of type-2 fuzzy logic to rule-based intrusion alert correlation detection. *Int J Innov Computing Inform and Control,* 8(4), 2865-2874.

Julisch, K. (2001). Mining alarm clusters to improve alarm handling efficiency. In *IEEE Proceedings 17th Annual Computer Security Applications Conference,* 12-21. doi:10.1109/ACSAC.2001.991517.

Julisch, K. (2003). Clustering intrusion detection alarms to support root cause analysis. *ACM transactions on information and system security (TISSEC),* 6(4), 443-471. doi:10.1145/950191.950192.

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

Kamarudin, M.H., Maple, C., Watson, T. and Safa, N.S. (2017). A New Unified Intrusion Anomaly Detection in Identifying Unseen Web Attacks. *Security and Communication Networks,* 2017. doi:10.1155/2017/2539034.

Karim, M.R., Ahmed, C.F., Jeong, B.-S. and Choi, H.-J. (2013). An efficient distributed programming model for mining useful patterns in big datasets. *IETE Technical Review,* 30(1), 53-63. 10.4103/0256-4602.107340.

Kavousi, F. and Akbari, B. (2012). Automatic learning of attack behavior patterns using Bayesian networks. In *6th International Symposium on Telecommunications (IST)*, 999-1004. doi:10.1109/ISTEL.2012.6483132.

Kavousi, F. and Akbari, B. (2014). A Bayesian network-based approach for learning attack strategies from intrusion alerts. *Security and Communication Networks,* 7(5), 833-853. doi:10.1002/sec.786.

Kenaza, T. and Aiash, M. (2016). Toward an efficient ontology-based event correlation in SIEM. *Procedia Computer Science,* 83, 139-146. doi:10.1016/j.procs.2016.04.109.

Kim, G., Lee, S. and Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications,* 41(4), 1690-1700. doi:10.1016/j.eswa.2013.08.066.

Kim, Y.-H. and Park, W.H. (2014). A study on cyber threat prediction based on intrusion detection event for APT attack detection. *Multimedia tools and applications,* 71(2), 685-698. doi:10.1007/s11042-012-1275-x.

Kruegel, C., Robertson, W. and Vigna, G. (2004). Using alert verification to identify successful intrusion attempts. *Praxis der Informationsverarbeitung und Kommunikation,* 27(4), 219-227. doi:doi.org/10.1515/PIKO.2004.219.

Kumar, M., Siddique, S. and Noor, H. (2009). Feature-based alert correlation in security systems using self organizing maps. *SPIE Defense, Security, and Sensing*, 7344, 734404. doi:10.1117/12.820000.

Lafram, I., Berbiche, N. and El Alami, J. (2017). A Random Forest Estimator Combined With N-Artificial Neural Network Classifiers to Optimize Network Intrusion Detection. *International Journal of Applied Engineering Research,* 12(16), 5835-5843.

Lagzian, S., Amiri, F., Enayati, A. and Gharaee, H. (2012). Frequent item set mining-based alert correlation for extracting multi-stage attack scenarios. In *6th International Symposium on Telecommunications (IST),* 1010-1014. doi:10.1109/ISTEL.2012.6483134.

Lee, C.-C., Liu, C.-H. and Hwang, M.-S. (2013). Guessing Attacks on Strong-Password Authentication Protocol. *IJ Network Security.* 15(1), 64-67.

Lee, K., Kim, J., Kwon, K.H., Han, Y. and Kim, S. (2008). DDoS attack detection method using cluster analysis. *Expert Systems with Applications,* 34(3), 1659-1665. doi:10.1016/j.eswa.2007.01.040.

Li, W. and Tian, S. (2010). An ontology-based intrusion alerts correlation system. *Expert Systems with Applications,* 37(10), 7138-7146. doi:10.1016/j.eswa.2010.03.068.

Li, W., Zhi-Tang, L., Dong, L. and Jie, L. (2007a). Attack scenario construction with a new sequential mining technique. In *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing,* 872-877. doi:10.1109/SNPD.2007.395.

Li, Y., Xue, Y., Yao, Y., Zhao, X., Liu, J. and Zhang, R. (2016). An attack pattern mining algorithm based on fuzzy logic and sequence pattern. In *4th International Conference on Cloud Computing and Intelligence Systems (CCIS)*, 234-238. doi:10.1109/CCIS.2016.7790260.

Li, Z., Zhang, A., Li, D. and Wang, L. (2007b). Discovering novel multistage attack strategies. In *International Conference on Advanced Data Mining and Applications*, 45-56. Springer, Berlin, Heidelberg.

Liang-Min, W. and Jian-Feng, M. (2005). Two-stage algorithm for correlating the intrusion alerts. *Wuhan University Journal of Natural Sciences,* 10(1), 89-92. doi:10.1007/BF02828624.

Liao, H.-J., Lin, C.-H.R., Lin, Y.-C. and Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications,* 36(1), 16-24.

Lin, Z., Li, S. and Ma, Y. (2010). Real-time intrusion alert correlation system based on prerequisites and consequence. In *6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM),* 1-5. doi:10.1109/WICOM.2010.5601285.

Ma, J., Li, Z.-T. and Li, W.-M. (2008). Real-time alert stream clustering and correlation for discovering attack strategies. In *Fifth International Conference on Fuzzy Systems and Knowledge Discovery,* 379-384. doi:10.1109/FSKD.2008.522.

Maggi, F. and Zanero, S. (2007). On the use of different statistical tests for alert correlation–short paper. In *International Workshop on Recent Advances in Intrusion Detection*, 167-177. Springer, Berlin, Heidelberg.

Maggi, F., Matteucci, M. and Zanero, S. (2009). Reducing false positives in anomaly detectors through fuzzy alert aggregation. *Information Fusion,* 10(4), 300-311. doi:10.1016/j.inffus.2009.01.004.

Mahboubian, M., Udzir, N.I., Subramaniam, S. and Hamid, N.a.W.A. (2012). An alert fusion model inspired by artificial immune system. In *International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, 317-322. doi:10.1109/CyberSec.2012.6246083.

Mahoney, M.V. and Chan, P.K. (2003). An analysis of the 1999 DARPA/Lincoln Laboratory evaluation data for network anomaly detection. In *International Workshop on Recent Advances in Intrusion Detection*, 220-237. doi:10.1007/978-3-540-45248-5_13.

Man, D., Yang, W., Wang, W. and Xuan, S. (2012b). An alert aggregation algorithm based on iterative self-organization. *Procedia Engineering,* 29, 3033-3038. doi:10.1016/j.proeng.2012.01.435.

Man, D.-P., Li, X.-Z., Yang, W., Wang, W. and Xuan, S.-C. (2012a). A Multi-step Attack Recognition and Prediction Method Via Mining Attacks Conversion Frequencies. I.J. Wireless and Microwave Technologies, 2, 20-25. doi:10.5815/ijwmt.2012.02.04.

Marchetti, M., Colajanni, M. and Manganiello, F. (2011). Framework and models for multistep attack detection. *International Journal of Security and Its Applications,* 5(4), 73-90.

Mathew, S., Britt, D., Giomundo, R., Upadhyaya, S., Sudit, M. and Stotz, A. (2005). Real-time multistage attack awareness through enhanced intrusion alert clustering. In *IEEE Military Communications Conference,* 1801-1806.

Mcculloch, W.S. and Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. *The bulletin of mathematical biophysics,* 5(4), 115-133. doi:10.1007/BF02478259.

Meng, G., Liu, Y., Zhang, J., Pokluda, A. and Boutaba, R. (2015). Collaborative security: A survey and taxonomy. *ACM Computing Surveys (CSUR),* 48(1), doi:10.1145/2785733.

Michel, C. and Mé, L. (2001). Adele: an attack description language for knowledge-based intrusion detection. In *IFIP International Information Security Conference*, 353-368. doi:10.1007/0-306-46998-7_25.

Minsky, M. and Papert, S. (1969). Perceptrons. Cambridge, MA:MIT Press

Mirheidari, S.A., Arshad, S. and Jalili, R. (2013). Alert correlation algorithms: A survey and taxonomy. In *Cyberspace Safety and Security,* 183-197. doi:10.1007/978-3-319-03584-0_14.

Mohamed, A.B., Idris, N.B. and Shanmugum, B. (2012). Alert correlation using a novel clustering approach. In *International Conference on Communication Systems and Network Technologies*, 720-725. doi:10.1109/CSNT.2012.212.

Morin, B. and Debar, H. (2003). Correlation of intrusion symptoms: an application of chronicles. In *International Workshop on Recent Advances in Intrusion Detection,* 94-112. doi:10.1007/978-3-540-45248-5_6.

Mudzingwa, D. and Agrawal, R. (2012). A study of methodologies used in intrusion detection and prevention systems (IDPS). In *Proceedings of IEEE Southeastcon,* 1-6. doi: 10.1109/SECon.2012.6197080.

Navarro, J., Deruyver, A. and Parrend, P. (2018). A systematic survey on multi-step attack detection. *Computers & Security,* 76, 214-249. doi:10.1016/j.cose.2018.03.001.

Nguyen, T.H., Luo, J. and Njogu, H.W. (2014). Improving the management of IDS alerts. *International Journal of Security and Its Applications,* 8(3), 393-406.

Ning, P. and Xu, D. (2002). A*dapting query optimization techniques for efficient intrusion alert correlation.* North Carolina State University: Center for Advanced Computing and Communication.

Ning, P. and Xu, D. (2003). Learning attack strategies from intrusion alerts. In *Proceedings of the 10th ACM conference on Computer and communications security,* 200-209. doi:10.1145/948109.948137.

Ning, P. and Xu, D. (2010). Toward automated intrusion alert analysis. *Network Security,* 175-205. doi:10.1007/978-0-387-73821-5_8.

Ning, P., Cui, Y. and Reeves, D.S. (2002a). Analyzing intensive intrusion alerts via correlation. In *International Workshop on Recent Advances in Intrusion Detection*, 74-94. doi:10.1007/3-540-36084-0_5.

Ning, P., Cui, Y. and Reeves, D.S. (2002b). Constructing attack scenarios through correlation of intrusion alerts. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 245-254. doi:10.1145/586110.586144.

Ning, P., Cui, Y., Reeves, D.S. and Xu, D. (2004). Techniques and tools for analyzing intrusion alerts. In *ACM Transactions on Information and System Security (TISSEC),*7(2), 274-318. doi:10.1145/996943.996947.

Ning, P., Peng, P., Hu, Y. and Xu, D. (2003). *TIAA: A visual toolkit for intrusion alert analysis.* North Carolina State University. Center for Advanced Computing and Communication.

Park, W. and Ahn, S. (2017). Performance comparison and detection analysis in Snort and Suricata environment. *Wireless Personal Communications,* 94(2), 241-252. doi:10.1007/s11277-016-3209-9.

Pietraszek, T. (2004). Using adaptive alert classification to reduce false positives in intrusion detection. In *International Workshop on Recent Advances in Intrusion Detection*, 102-124. doi:10.1007/978-3-540-30143-1_6.

Pietraszek, T. and Tanner, A. (2005). Data mining and machine learning—towards reducing false positives in intrusion detection. *Information security technical report,* 10(3), 169-183. doi:10.1016/j.istr.2005.07.001.

Qin, X. and Lee, W. (2007). Discovering novel attack strategies from INFOSEC alerts. In *Data Warehousing and Data Mining Techniques for Cyber Security,* 109-157. doi:10.1007/978-0-387-47653-7_7.

Ramaki, A.A., Amini, M. and Atani, R.E. (2015a). RTECA: Real time episode correlation algorithm for multi-step attack scenarios detection. *Computers & Security,* 49, 206-219. doi:10.1016/j.cose.2014.10.006.

Ramaki, A.A., Khosravi-Farmad, M. and Bafghi, A.G. (2015b). Real time alert correlation and prediction using bayesian networks. In *12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, 98-103. doi:10.1109/ISCISC.2015.7387905.

Ren, H., Stakhanova, N. and Ghorbani, A.A. (2010). An online adaptive approach to alert correlation. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, 153-172. doi:10.1007/978-3-642-14215-4_9.

Rosenblatt, F. (1958). The perceptron: A probabilistic model for information storage and organization in the brain. *Psychological Review,* 65(6), 386 - 408. doi:10.1037/h0042519.

Saad, S. and Traore, I. (2012a). Extracting attack scenarios using intrusion semantics. In *International Symposium on Foundations and Practice of Security*, 278-292. doi:10.1007/978-3-642-37119-6_18.

Saad, S. and Traore, I. (2012b). Heterogeneous Multi-sensor IDS Alerts Aggregation using Semantic Analysis. *Journal of Information Assurance & Security,* 7(2), 79-88.

Saad, S. and Traore, I. (2013). Semantic aware attack scenarios reconstruction. *Journal of Information Security and Applications,* 18(1), 53-67. doi:10.1016/j.jisa.2013.08.002.

Sadighian, A., Fernandez, J.M., Lemay, A. and Zargar, S.T. (2014). Ontids: A highly flexible context-aware and ontology-based alert correlation framework. In *Foundations and Practice of Security,* 161-177. Springer.

Sadoddin, R. and Ghorbani, A.A. (2009). An incremental frequent structure mining framework for real-time alert correlation. *Computers & Security,* 28(3), 153-173. doi:10.1016/j.cose.2008.11.010.

Salah, S., Maciá-Fernández, G. and Díaz-Verdejo, J.E. (2013). A model-based survey of alert correlation techniques. *Computer Networks,* 57(5), 1289-1317. 10.1016/j.comnet.2012.10.022.

Salim, L.F. and Mezrioui, A. (2007). Improving the quality of alerts with correlation in intrusion detection. *International Journal of Computer Science and Network Security,* 7(12), 210-215.

Sallay, H. and Bourouis, S. (2015). Intrusion detection alert management for high-speed networks: current researches and applications. *Security and Communication Networks,* 8(18), 4362-4372. doi:10.1002/sec.1366.

Sallay, H., Ammar, A., Saad, M.B. and Bourouis, S. (2013). A real time adaptive intrusion detection alert classifier for high speed networks. In *IEEE 12th International Symposium on Network Computing and Applications*, 73-80. doi:10.1109/NCA.2013.16.

Santos, O., Kampanakis, P. and Woland, A. (2016). *Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP.* Indianapolis, USA: Cisco Press.

Saurabh, S. and Sairam, A.S. (2016). Increasing Accuracy and Reliability of IP Traceback for DDoS Attack Using Completion Condition. *IJ Network Security,* 18(2), 224-234.

Shimamura, M. and Kono, K. (2006). Using attack information to reduce false positives in network ids. In *11th IEEE Symposium on Computers and Communications,* 386-393. doi:10.1109/ISCC.2006.165.

Shittu, R., Healing, A., Ghanea-Hercock, R., Bloomfield, R. and Rajarajan, M. (2015). Intrusion alert prioritisation and attack detection using post-correlation analysis. *Computers & Security,* 50, 1-15. doi:10.1016/j.cose.2014.12.003.

Siraj, M.M., Maarof, M.A. and Hashim, S.Z. (2009). Intelligent alert clustering model for network intrusion analysis. *Int. J. Advance. Soft Comput. Appl,* 1(1), 1-16.

Smith, R., Japkowicz, N., Dondo, M. and Mason, P. (2008). Using unsupervised learning for network alert correlation. In *Conference of the Canadian Society for Computational Studies of Intelligence*, 308-319. doi:10.1007/978-3-540-68825-9_29.

Soleimani, M. and Ghorbani, A.A. (2012). Multi-layer episode filtering for the multi-step attack detection. *Computer Communications,* 35(11), 1368-1379. doi:10.1016/j.comcom.2012.04.001.

Tan, Z., Jamdagni, A., He, X., Nanda, P. and Liu, R.P. (2011). Denial-of-service attack detection based on multivariate correlation analysis. In *International Conference on Neural Information Processing,* 756-765. doi:10.1007/978-3-642-24965-5_85.

Templeton, S.J. and Levitt, K. (2001). A requires/provides model for computer attacks. In *Proceedings of the 2000 workshop on New security paradigms*, 31-38. doi:10.1145/366173.366187.

Thanthrige, U.S.K., Samarabandu, J. and Wang, X. (2016). Intrusion Alert Prediction Using a Hidden Markov Model. *arXiv preprint arXiv:1610.07276.*

Tjhai, G.C., Furnell, S.M., Papadaki, M. and Clarke, N.L. (2010). A preliminary two-stage alarm correlation and filtering system using SOM neural network and K-means algorithm. *Computers & Security,* 29(6), 712-723. doi:10.1016/j.cose.2010.02.001.

Treinen, J.J. and Thurimella, R. (2006). A framework for the application of association rule mining in large intrusion detection infrastructures. *International Workshop on Recent Advances in Intrusion Detection*, 1-18. doi:10.1007/11856214_1.

Ullah, I. and Mahmoud, Q.H. (2017). A filter-based feature selection model for anomaly-based intrusion detection systems. In *IEEE International Conference on Big Data,* 2151-2159. doi:10.1109/BigData.2017.8258163.

Ussath, M., Cheng, F. and Meinel, C. (2016a). Automatic multi-step signature derivation from taint graphs. In *IEEE Symposium Series on Computational Intelligence (SSCI),* 1-8. doi:10.1109/SSCI.2016.7850076.

Ussath, M., Cheng, F. and Meinel, C. (2016b). Event attribute tainting: A new approach for attack tracing and event correlation. In *IEEE/IFIP Network Operations and Management Symposium (NOMS),* 509-515. doi:10.1109/NOMS.2016.7502851.

Valdes, A. and Skinner, K. (2001). Probabilistic alert correlation. In *International Workshop on Recent Advances in Intrusion Detection,* 54-68. doi:10.1007/3-540-45474-8_4.

Valeur, F., Vigna, G., Kruegel, C. and Kemmerer, R.A. (2004). Comprehensive approach to intrusion detection alert correlation. In *IEEE Transactions on Dependable and Secure Computing,* 1(3), 146-169. doi:10.1109/TDSC.2004.21.

Vasan, K.K. and Surendiran, B. (2016). Dimensionality reduction using Principal Component Analysis for network intrusion detection. *Perspectives in Science,* 8, 510-512. doi:10.1016/j.pisc.2016.05.010.

Viinikka, J., Debar, H., Mé, L. and Séguier, R. (2006). Time series modeling for IDS alert management. In *Proceedings of the 2006 ACM Symposium on Information, computer and communications security*, 102-113. doi:10.1145/1128817.1128835.

Wang, L., Liu, A. and Jajodia, S. (2006). Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts. *Computer communications,* 29(15), 2917-2933. doi:10.1016/j.comcom.2006.04.001.

Wang, L.-M., Ma, J.-F. and Zhan, Y.-Z. (2004). Enhancing the content of the intrusion alerts using logic correlation. In *Content Computing,* 137-142. doi:10.1007/978-3-540-30483-8_17.

Xian, M. and Zhang, Y. (2016). A privacy-preserving multi-step attack correlation algorithm. In *IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC),* 1389-1393. doi:10.1109/IMCEC.2016.7867441.

Xiao, M. and Xiao, D. (2007). Alert verification based on attack classification in collaborative intrusion detection. In *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing,* 739-744. doi:10.1109/SNPD.2007.216.

Xu, D. and Ning, P. (2004). Alert correlation through triggering events and common resources. In *20th Annual Computer Security Applications Conference*, 360-369. doi:10.1109/CSAC.2004.5.

Xu, D. and Ning, P. (2006). *Correlation analysis of intrusion alerts*. Springer.

Yan, Y., Qian, Y., Sharif, H. and Tipper, D. (2012). A survey on cyber security for smart grid communications. *IEEE Communications Surveys and tutorials,* 14(4), 998-1010.

Yang, Y. and Pedersen, J.O. (1997). A comparative study on feature selection in text categorization. *Icml*, 412-420.

Yao, Y., Wang, Z., Gan, C., Kang, Q., Liu, X., Xia, Y. and Zhang, L. (2016). Multi-source alert data understanding for security semantic discovery based on rough set theory. *Neurocomputing,* 208, 39-45. doi:10.1016/j.neucom.2015.12.127.

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(3), 632-654. doi:10.1016/j.comnet.2006.05.008.

Zainal, A., Maarof, M.A. and Shamsuddin, S.M. (2006). Feature selection using rough set in intrusion detection. In *Tencon IEEE Region 10 Conference*, 1-4. doi:10.1109/TENCON.2006.344210.

Zakaria, Z., Isa, N.a.M. 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,* 4(2), 170-173.

Zali, Z., Hashemi, M.R. and Saidi, H. (2012). Real-time attack scenario detection via intrusion detection alert correlation. *In 9th International ISC Conference on Information Security and Cryptology*, 95-102. doi:10.1109/ISCISC.2012.6408197.

Zhang, A.-F., Li, Z.-T., Li, D. and Wang, L. (2007). Discovering novel multistage attack patterns in alert streams. *International Conference on Networking, Architecture, and Storage*, 115-121. doi:10.1109/NAS.2007.20.

Zhang, Y., Luo, X. and Luo, H. (2016). A multi-step attack-correlation method with privacy protection. *Journal of Communications and Information Networks,* 1(4), 133-142. doi:10.1007/BF03391586.

Zhang, Y., Xiao, S., Zhuang, X. and Peng, X. (2008). Using cluster and correlation to construct attack scenarios. *International Conference on Cyberworlds*, 471-476. doi:10.1109/CW.2008.94.

Zhao, D., Traore, I., Sayed, B., Lu, W., Saad, S., Ghorbani, A. and Garant, D. (2013). Botnet detection based on traffic behavior analysis and flow intervals. *Computers & Security,* 39, 2-16. doi:10.1016/j.cose.2013.04.007.