A SITUATION ASSESSMENT AND PREDICTION MECHANISM FOR NETWORK SECURITY SITUATION AWARENESS

by

LEAU YU BENG

Thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy

July 2016

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest gratitude to my supervisor, **Dr. Selvakumar Manickam** for giving me full support and faithfulness in all guidance and commitments upon on effort from the early stages of this study through to the completion of this thesis. His wide knowledge and understanding have been invaluable to me especially in giving constructive comments and advice throughout this study.

My sincere heartfelt gratitude to my parents, **Leau Chuan Keow** and **Quek Kim Choo**, brother, **Leau Yu Chia** and my lovely son, **Darren Leau Jin Khang** for their endless love, help and encouragement during this study period especially when I have endured a periods of frustration. Word cannot truly express how much I owe you all.

I would like to convey my appreciation to all the **academic staffs** in National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia for their dedication and persistent support. Besides that, the **administration and support staffs** in NAv6 deserve a high mention for keeping everything running smoothly. As does my funding body, the **Ministry of Higher Education (MOHE)**, Malaysia and **Universiti Malaysia Sabah (UMS)** for awarding me a scholarship to pursuit this study.

Finally, collective and individual acknowledgments are also owed to my **friends** and **colleagues** in NAv6 who have helped and supported me over these years.

Thank you.

Leau Yu Beng

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AHP	Analytical Hierarchy Process
AGVK-NESSIP	Adaptive Grey Verhulst-Kalman Network Security Situation Prediction
AGV-NESSIP	Adaptive Grey Verhulst Network Security Situation Prediction
AGO	Accumulating Generation Operation
AP	Average Priority
ARMA	Autoregressive-Moving-Average
AS	Alert Score
ASSE	Asset Security Situation Entropy
AT	Asset Threat
AW	Asset Weight
BPNN	Back Propagation
CERT	Computer Emergency Response Team
CPU	Central Processing Unit
CSOC	Cyber Security Operations Centre
CSV	Comma Separated Value
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial of Service
DNS	Domain Name System
DOS	Denial of Service
EDGF	Equal Dimensions Grey Filling
E-NESSAS	Entropy-based Network Security Situation Assessment
ESN	Echo State Network

ESX	Elastic Sky X
EVM	Eigenvector Method
GM(1,1)	First-order One-variable Grey Model
HTML	Hypertext Markup Language
IAGO	Inverse Accumulated Generation Operation
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
LAN	Local Area Network
MAPE	Mean Absolute Percentage Error
MySQL	My-Structured Query Language
NAv6	National Advanced IPv6 Centre
NESSAP	Network Security Situation Assessment and Prediction
NESSAS	Network Security Situation Assessment
NESSIP	Network Security Situation Prediction
NSSA	Network Security Situation Awareness
OS	Operating System
PHP	Hypertext Preprocessor
PSO	Particle Swarm Optimization
RI	Risk Index
RIAC	Real-time Intrusion Alert
RMSD	Root Mean Square Deviation
RPE	Relative Percentage Error
RS	Risk State

R2L	Remote to User Attack
SA	Situation Awareness
SCE	Sony Computer Entertainment
SCGM	System Cloud Grey Model
SJTU	Shanghao Jiaotong University
SVM	Support Vector Machine
UK	United Kingdom
US	United States
U2R	User to Root Attack
VMFS	Virtual Machine File System

MEKANISMA PENILAIAN DAN PERAMALAN SITUASI BAGI KESEDARAN SITUASI KESELAMATAN RANGKAIAN

ABSTRAK

Percubaan menceroboh rangkaian telah mencecah tahap yang membimbangkan. Laporan Keselamatan *Cisco* 2014 menunjukkan bahawa 50,000 pencerobohan rangkaian telah dikesan dan 80 juta permintaan sesawang yang mencurigakan telah disekat setiap hari. Oleh itu, Sistem Pencegahan Pencerobohan (*IPS*) telah dipilih sebagai mekanisma pertahanan dalam organisasi. Walau bagaimanapun, *University of South Wales* melaporkan bahawa tujuh IPS berjenama gagal mengesan dan menyekat 34% - 49% serangan dalam aplikasi berasaskan sesawang. Ketepatan *IPS* boleh dipertingkatkan sekiranya situasi rangkaian dipertimbangkan dalam penyekatan percubaan pencerobohan. Pengetahuan mengenai situasi keselamatan rangkaian semasa dan yang akan datang adalah diperlukan sebelum sebarang langkah berjaga-jaga diambil. Penilaian dan peramalan situasi merupakan antara dua fasa utama dalam Kesedaran Situasi Keselamatan Rangkaian. Model penilaian yang sedia ada tidak mengambil kira faktor kos sebagai kriteria penilaian. Lebih-lebih lagi, terdapat kekurangan garis panduan piawaian digunakan untuk menentukan kepentingan aset rangkaian. Dalam peramalan, melatih pengesan pembelajaran sendiri adalah susah disebabkan data yang tidak lengkap dan mencukupi. Tambahan pula, model Grey Pembolehubah-tunggal Peringkat-pertama (*GM(1,1)*) adalah tidak sesuai untuk meramal urutan rawak yang tidak pegun. Sebagai tambahan, urutan janaan min menjejaskan ketepatan model dengan ralat kelewatan. Oleh itu, tesis

ini mempersembahkan satu mekanisma penilaian dan peramalan situasi keselamatan rangkaian yang mencadangkan skim penilaian situasi berdasarkan Entropi untuk menilai status keselamatan rangkaian semasa dengan bantuan Proses Hierarki Analisis dan memperkenalkan juga skim penyesuaian peramalan situasi berdasarkan Grey Verhulst dan Penapisan Kalman untuk meramal situasi keselamatan yang akan datang. Mekanisma yang dicadangkan terdiri daripada empat modul, (1) Penyediaan Data menyediakan amaran dalam format yang betul, (2) Normalisasi Data mengumpul amaran berdasarkan ciri-cirinya dan menghapuskan amaran yang berlebihan, (3) Penilaian Situasi Keselamatan Rangkaian Berasaskan Entropi (*E-NESSAS*) menilai keseluruhan situasi keselamatan rangkaian dengan mempertimbangkan kriteria ketara dan tidak ketara dan (4) Peramalan Penyesuaian Situasi Keselamatan Rangkaian *Grey Verhulst-Kalman* (*AGVK-NESSIP*) meramal situasi keselamatan rangkaian yang akan datang berdasarkan data situasi semasa dan lama. Keberkesanan rangka kerja telah dinilai dengan mengunakan empat set data iaitu *DARPA 1999, LLDOS 1.0, LLDOS 2.0.2* dan *NAv6 2015*. Penemuan menunjukkan bahawa *E-NESSAS* dapat menilai situasi keselamatan rangkaian secara menyeluruh dengan konsep Entropi. Sementara itu, *AGVK-NESSIP* dapat menyediakan ketepatan ramalan yang tinggi dalam kesemua set data dengan purata ketepatan sebanyak 79.61%. Berbanding dengan model sedia ada yang lain, *AGVK-NESSIP* telah menunjukkan peningkatan sebanyak 15.5% dari segi ketepatan peramalan. Keputusan jelas mendedahkan bahawa mekanisma yang dicadangkan dapat menilai situasi keselamatan semasa secara bersistematik dengan *E-NESSAS* dan dapat meramal situasi dengan lebih tepat dengan *AGVK-NESSIP* tanpa mengira selang masa dan tingkah laku urutan data.

A SITUATION ASSESSMENT AND PREDICTION MECHANISM FOR NETWORK SECURITY SITUATION AWARENESS

ABSTRACT

Network intrusion attempts have reached an alarming level. Cisco's 2014 Security Report indicated that 50,000 network intrusions were detected and 80 million suspicious web requests were blocked daily. Hence, Intrusion Prevention System (IPS) had been chosen as a defence mechanism in many organizations. However, the University of South Wales reported that seven big-brand IPS had failed to detect and block 34% - 49% of attacks in web-based applications. The accuracy of IPS can be improved if the network situation is also considered in preventing intrusion attempts. Knowledge about current and incoming network security situation is required before any precaution can be taken. Situation assessment and prediction are two main phases of Network Security Situation Awareness. The existing assessment models do not consider cost factor as an assessment criterion. Moreover, there has been a lack of standard guidelines to determine the importance of network assets. On prediction, training self-learning detectors are difficult due to incomplete and insufficient data. Furthermore, First-order One-variable grey model (GM(1,1)) has not been suitable to predict non-stationary random sequence. In addition, mean generation sequence depresses the model precision with delay error. Hence, this thesis presents a network security situation assessment and prediction mechanism that proposes an Entropy-based situation assessment scheme to assess current network security status with the aid of the Analytical Hierarchy Process and the introduction of an adaptive situation

prediction mechanism based on Grey Verhulst and Kalman Filtering is proposed so as to predict the incoming security situation. The proposed mechanism consists of four modules, (1) *Data Preparation* which prepares the alerts in proper format, (2) *Data Normalization* which groups alerts based on their features and to eliminate redundant alerts, (3) *Entropy-based Network Security Situation Assessment (E-NESSAS)* which assesses entire network security situation by considering tangible and intangible criteria and (4) *Adaptive Grey Verhulst-Kalman Network Security Situation Prediction (AGVK-NESSIP)* which predicts incoming network security situation based on current and historical situation data. The effectiveness of the mechanism is evaluated using four datasets, i.e. DARPA 1999, LLDOS 1.0, LLDOS 2.0.2 and NAv6 2015 dataset. The findings demonstrated that E-NESSAS assessed more comprehensively network security situation by using Entropy concept. Meanwhile, AGVK-NESSIP provided high predictive accuracy in all datasets with an average accuracy of 79.61%. Compared with other existing models, AGVK-NESSIP has shown an improvement of 15.5% in terms of prediction accuracy. The results clearly revealed that the proposed mechanism could assess current security situation systematically by E-NESSAS and was able to predict the situation more accurately by AGVK-NESSIP regardless of the time intervals and behaviour of the data sequence.

CHAPTER 1
INTRODUCTION

1.1 Background and Motivation

In this globalization era, the Internet has become an important part of our lives offering convenient services and information sharing. The number of Internet users worldwide has mushroomed to reach 3.17 billion which is almost 40% of the world population in 2015 (International Telecommunication Union, 2015). Unfortunately, the immense popularity of the Internet and prevalent use of online applications has made the Internet a breeding ground for malware and cyber criminals. The local area networks (LANs) are the building blocks of the Internet. LAN is crucial for computing operations within the boundaries of the organization. Since LAN is also connected to the Internet, it is vulnerable to infiltration and attacks from outside the organization.

In 2014, Symantec had encountered a 40% increase in phishing attacks compared to previous year, 2013 (Symantec, 2015). Meanwhile, Arbor Network had also revealed that Distributed Denial of Service (DDoS) attack was the most frequently observed threat in an enterprise with an average of 21 attacks in a month. The situation became worse when more than 33% of organizations had their intrusion prevention system devices experience failure during the attack (Anstee et al., 2015). This phenomenon brings serious challenges and problems to network security

The number of incidents is also rising. For example, in Malaysia, the published incident statistics for year 2014 indicate that 11918 cases were reported to MyCERT with different types of attacks such as denial of service, intrusion attempt, malicious codes, spamming and etc (Malaysia Computer Emergency Response Team, 2015). An

information security breaches survey conducted by PricewaterhouseCoopers on United Kingdom (UK)'s businesses discovered that 90% and 74% of large and small organizations respectively had a security breach in the year 2014 and it caused losses of £1.46 million - £3.14 million average in the year (PricewaterhouseCoopers, 2015). Figure 1.1 illustrates the network security landscape which consists of promising online applications, new emerging network threats, current alarming situation and main components in situational awareness.

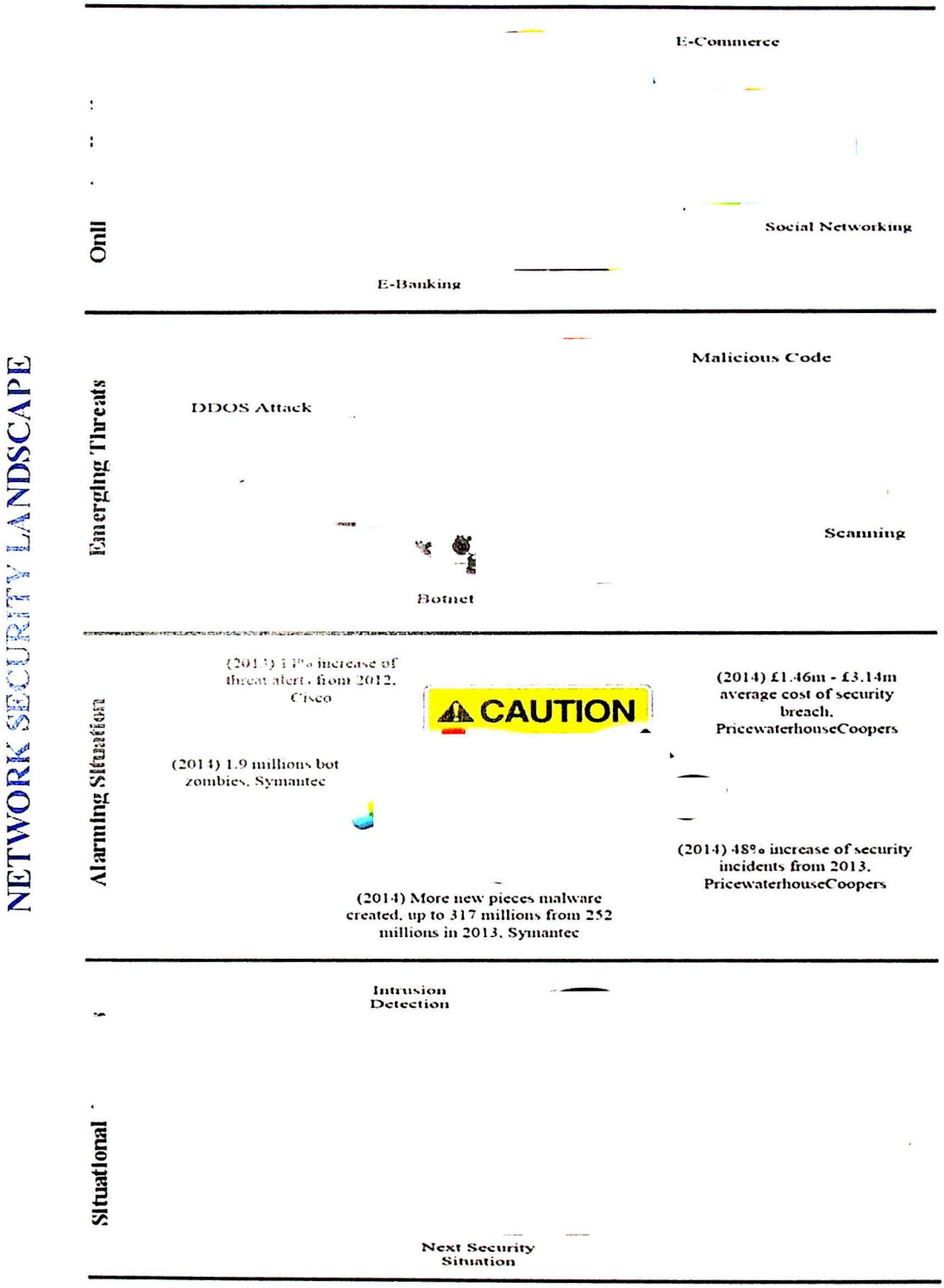

Figure 1.1: Network Security Landscape

Due to the rising number of threats, detection alone is no longer able to provide an organization a reliable network. Prevention before an incident occurs should be in place. In 2011, a massive hacking of Sony's PlayStation Network caused Sony Computer Entertainment (SCE) Europe Limited to lose millions of dollars while the site was down for a month. The company was unaware that the attack exploited a known vulnerability in the application server to plant software that was used to access the database server even though their detection mechanisms were in use (Williams, 2011). Consequently, millions of users' personal data were leaked in the incident and company was fined US$395,775 by the Information Commissioner's Office in United Kingdom (Goodin, 2011). After the incident, Sony decided to apply the security monitoring system to help guard and prevent against future attacks by spotting unusual network activity. As preventing an incident requires careful analysis and planning, network security communities are constantly on the alert to monitor the current and incoming security situation in their networks before any precautions could be taken. Coincidentally, security situation assessment and prediction capabilities were considered the main components in situation awareness by Endsley (Endsley, 1988a) when he introduced the concept of situation awareness in 3-hierarchical phases to the world.

1.2 Network Security Situation Awareness

Situation awareness is defined as the observation of changing critical factors in a complex global network within a time and space interval, the understanding of those factors mean according to the operator's goals and the projection of their status in next interval (Endsley, 1988a).

In general, situation awareness can be divided into three stages which are event detection, current situation assessment and future situation prediction (Endsley, 1995b). These stages can be adapted in Network Security Situation Awareness (NSSA) and represent the awareness level as Figure 1.2.

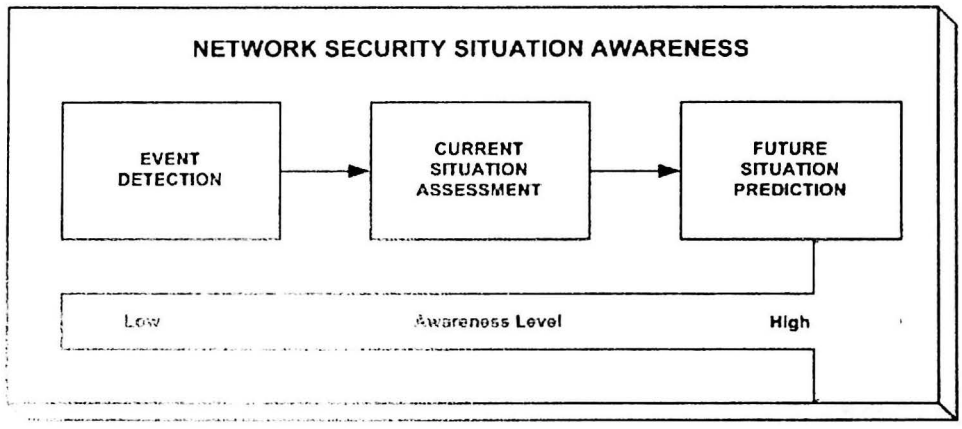

Figure 1.2: The Concept Model of Network Security Situation Awareness

Stage 1: Event Detection is a basic process of situation awareness. This stage is mainly to identify the abnormal and malicious activity in the network and translates them into logical format.

Stage 2: Current Situation Assessment is a process to evaluate the security situation of the entire network by using the information obtained from the detected alerts in the previous stage.

Stage 3: Future Situation Prediction is aimed to forecast the future network security tendency according to the current and historical network security situation status.

In 1999, the concept was first introduced in cyberspace (Bass and Gruber, 1999) and gradually spread to various areas such as computer network security. In other words, the concept of NSSA actually originated from the classical situation

In general, situation awareness can be divided into three stages which are event detection, current situation assessment and future situation prediction (Endsley, 1995b). These stages can be adapted in Network Security Situation Awareness (NSSA) and represent the awareness level as Figure 1.2.

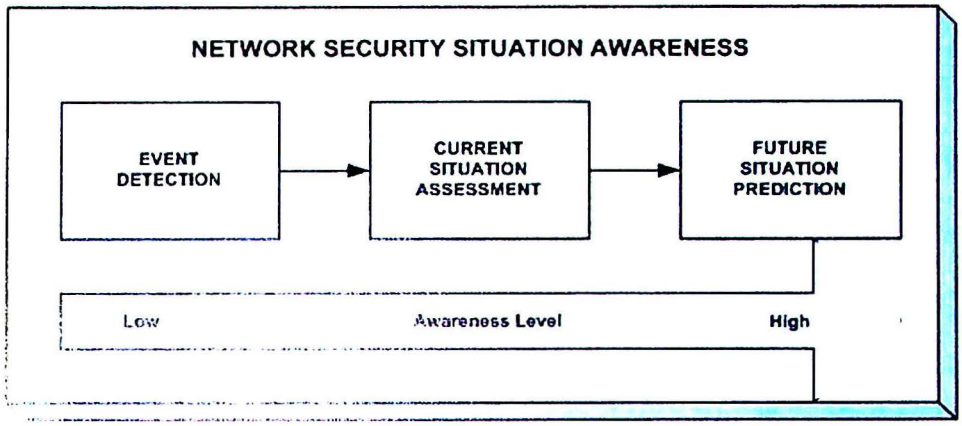

Figure 1.2: The Concept Model of Network Security Situation Awareness

Stage 1: Event Detection is a basic process of situation awareness. This stage is mainly to identify the abnormal and malicious activity in the network and translates them into logical format.

Stage 2: Current Situation Assessment is a process to evaluate the security situation of the entire network by using the information obtained from the detected alerts in the previous stage.

Stage 3: Future Situation Prediction is aimed to forecast the future network security tendency according to the current and historical network security situation status.

In 1999, the concept was first introduced in cyberspace (Bass and Gruber, 1999) and gradually spread to various areas such as computer network security. In other words, the concept of NSSA actually originated from the classical situation

awareness concept (Durso and Gronlund, 1999). Based on Sheng-Hui Chien et al, a network security situation can be referred to as that which extends to network devices that have been compromised (Chien and Ho, 2012). In the computer network, NSSA can be defined as the forecasting of future network security trend by integrating and assessing all the suspicious packets captured by intrusion detection systems (IDSs) keen to exploit the stability of the network. The governments, enterprises and other stakeholders are seeking appropriate strategies with this kind of capability to manage their information and control system. For instances, the Australia Government established a Cyber Security Operations Centre (CSOC) within the Department of Defense to provide a 24/7 cyber situation awareness capability to facilitate operational responses to cyber security events of national importance (Australia Attorney-General's Department, 2009). In United States (US), President Barack Obama sealed a strategy plan to share situational awareness of network vulnerabilities and risks among the public and private sector networks and to work with other countries (between government and industries) in order to expand the international network in building a greater global situation awareness and incident response (The White House, 2011). The United Kingdom (UK) Cyber Security Strategy clearly stated that they will continue to improve their detection and analysis of sophisticated cyber threats especially in the UK's critical national infrastructure as well as to pool knowledge and situational awareness when appropriate with their partners across all businesses to build a genuinely national response (The Cabinet Office, 2011). One of the main responsibilities of The German National Cyber Response Centre is to alert the crisis management staff whenever the cyber security situation reaches the level of an imminent or already occurred crisis (Federal Ministry of the Interior, 2011). In Malaysia, the National Cyber Security Policy addressed the need to develop effective

cyber security incident reporting mechanisms capable of disseminating vulnerability advisories and threat warnings in a timely manner so as to strengthen the National Computer Emergency Response Teams (CERTs) in monitoring the situation of critical national information infrastructure (MOSTI, 2012). From the effort of aforementioned countries in their strategic planning, it obviously reflected a concerted concern that NSSA is very much in demand at the top level of cyber security strategic plan.

Unfortunately, there are serious challenges to assess and to present a comprehensive security situation in a network. Firstly, it requires high human intervention especially in collecting all kinds of data and analyzing them in multi dimensions (Endsley, 1988b, Bass, 1999, Bass, 2000, Ticha and Ranchin, 2006). Secondly, there is a need to have standardized procedures to estimate network security situation (Endsley, 1995b, Tadda et al., 2006, Zhuo et al., 2008). Thirdly, a lack of methodologies to construct all-inclusive insight of current security situation in a network (Salerno et al., 2005, Smets, 2007, Tadda, 2008). Lastly, to forecast precisely and effectively the next incoming trend of network security situation is a difficult task (Flagg et al., 2007, Wang et al., 2008, Erbacher et al., 2010, Erbacher, 2012).

1.3 Definition

1.3.1 Intrusion Alert

Intrusion Alert is a kind of user notification which is used to warn the security administrator regarding an intruder activity after being detected by a detection engine. An alert consists of several information lines which represent its features (El-Taj et al., 2010). There are some common features in alert detection engines log as below (Karim et al., 2013). Figure 1.3 presents the structure of a probing attack alert.

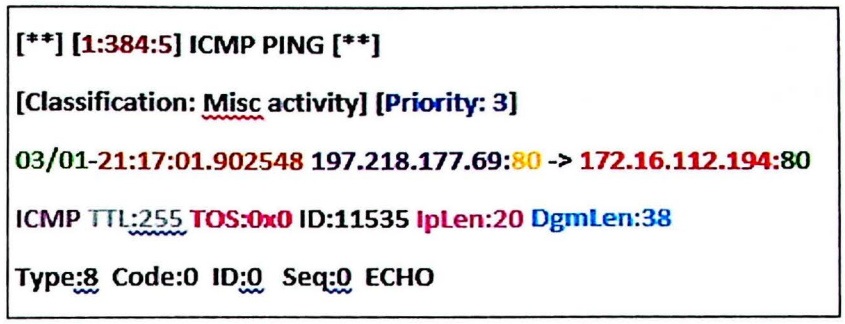

Figure 1.3: Example of the Structure of an Alert

- ID: Unique identifier for alert type
- Date: Date of occurrence
- Time: Time of occurrence
- IP Source: Internet Protocol address of attacker
- Port Source: Port Source of attacker
- IP Destination: Internet Protocol address of victim
- Port Destination: Port Destination of victim
- TTL: Time to live
- IpLen: Size of Internet Protocol header in bytes
- DgmLen: Size of packet in bytes
- Protocol: The protocol used
- Priority: Priority of the alert
- TOS: Type of service

1.3.2 Network Asset

Network Asset is a device which provides a service in a network. It can vary from hardware (e.g. server, switch, router, host and printer) to software (e.g. operating system (OS) and application).

1.3.3 Intrusion Prevention System (IPS)

Intrusion Prevention System is a pre-emptive technology that examines network traffic to identify the malicious packets embedded in it, log information about these suspicious packets and to respond to them before any damage on the network assets.

1.3.4 Intrusion Detection System (IDS)

Intrusion Detection System is an application designed to inspect all inbound and outbound network activities, detects possible intrusion such as computer attack and traffic anomalies, and alerts the administrator upon detection. Basically IDS can be categorized into two detection mechanisms based on their functionality, Misuse Detection System and Anomaly Detection System as shown in Figure 1.4.

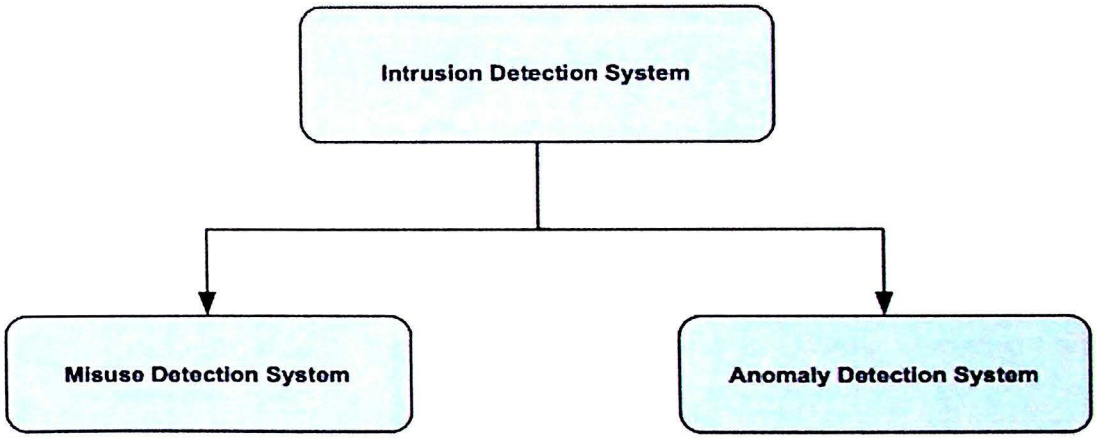

Figure 1.4: Types of Intrusion Detection System

1.4 Problem Statements

Network intrusion attempts have been on the rise. According to Cisco's 2014 Annual Security Report, there have been 50,000 network intrusions which were detected and 80 million suspicious web requests were blocked every day (Cisco, 2014). Due to this,

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) have become common threat detection mechanisms in many companies (Anstee et al., 2015). Unfortunately, there are some shortcomings with these mechanisms.

- IDS can detect malicious activities afterwards but the damage of the compromised system might have been done. It is unable to predict the future network security situation and take remedial action before the incident happens.
- Countering attacks in an IPS with a complete list of responses is insufficient. Surprisingly, in a study done by University of South Wales in 2013 on nine big-brand IPS systems, they found that seven out of nine failed to detect and block 34% - 49% attacks that target vulnerabilities in web-based application (Xynos et al., 2013). Moreover, direct response to particular attacks without any assessment on alerts itself as well as in the entire network will create a lot of false positive and false negative notification.

Hence, network security situation assessment and prediction are important practices to provide useful information to the network administrator in order to be ready with proper action to take so as to minimize the probability of the entire network being vulnerable to attacks. However, some drawbacks in existing assessment and prediction methods have been addressed in this research.

- Lack of standard guidelines to assign the weight of devices in the network. As different network devices play different roles in a network such as a server and printer, the negligence of considering the differences of their importance in the network is inappropriate.
- Based on our best knowledge, no single study exists which adequately considers the cost factor such as damage and response costs in the assessment.

Most of them solely consider the importance of assets, severity of attacks and their likelihood of occurrence.

- Constructing a complete logical relationship template of the alerts from multiple sources and training a set of self-learning and tolerance detectors in relationship analysis and artificial immune methods respectively are laborious tasks.
- The difficulty of making assumptions of all the possible states and transition especially in a heterogeneous network in order to build a complete Markov prediction model and small-scaled data as less input information tends to slow the convergence in machine learning method. Besides that, a bulk of training data is required to gain fit parameters and establish self-learning neurons.
- Data of network situation are uncertainty and incomplete in certain circumstances. Grey theory, particularly First-order One-variable grey model (GM(1,1)) is suitable to provide short-term prediction with this characteristic of small data without any training required. Regrettably, the method is only limited to linear time series and it is not suitable for non-stationary random sequence. In addition, the generation sequence with mean is only suitable for small time interval and it depresses the model precision with delay error.

1.5 Research Aim and Hypothesis

The aim of this research is to present and develop a mechanism to address the network security situation assessment and prediction processes in order to provide the network administrator the current and incoming network status as reference for his/her decision making. After discussing the problems faced by our community especially in situation assessment and prediction, we present the hypothesis of this research:

A mechanism for network security situation assessment and prediction capable of evaluating the current security situation in an organization's network by assessing the security threats against every affected network asset and forecasting incoming security situation based on current and previous security situation.

1.6 Research Questions and Objectives

As mentioned earlier, there is a need to develop a novel mechanism for assessing the current security situation and predicting the incoming situation based on current and previous security situation in which detected intrusion alerts were obtained. With this in mind, some of the research questions presented are:

i. How to assess the security situation in a network?

ii. How to predict the incoming security situation in a network?

iii. How good our mechanism is?

To achieve our aim in answering all the aforementioned research questions, the following specific objectives are defined:

1. To propose an Entropy-based network security situation assessment scheme to assess current security status of a network with the aid of the Analytical Hierarchy Process (AHP).
2. To design an adaptive Grey Verhulst-Kalman prediction scheme to forecast the incoming network security situation.
3. To verify and validate the performance in the aspect of accuracy of the proposed mechanism by implementing a novel prototype with benchmark datasets.

1.7 Research Scope

The research mechanism covers only two main realms in Network Security Situation Awareness (NSSA) which are Network Security Situation Assessment (NESSAS) and Network Security Situation Prediction (NESSIP). The performance of the proposed mechanism is evaluated by implementing a mechanism prototype in an offline environment. Three benchmark datasets, DARPA 1999, LLDOS 1.0 and LLDOS 2.0.2 and a generated intrusion dataset which simulated the National Advanced IPv6 Centre (NAv6) have been used to verify and validate the accuracy performance of the proposed mechanism in terms of its Relative Percentage Error (RPE), Mean Absolute Percentage Error (MAPE) and Root Mean Square Deviation (RMSD).

The mechanism is limited to IPv4 network which is subjected to malicious attacks and the suspicious alerts are only detected by Snort as an intrusion detection system in this research. Some assumptions have been made as below:

- All detected alerts from intrusion detection system in the network are true and reliable.
- The loss of intangible aspects can be relatively measured as the impacts of an attack in aspects of confidentiality, integrity and availability according to the business policy.

The discussion on alerts filtering, classification and normalization are not in in-depth discussion in this thesis. The computational cost incurred for the proposed mechanism is also not considered in this research.

1.8 Research Methods

In order to achieve the main objectives as stated in Section 1.6, all the accomplishments taken in this research can be divided into five important phases. Figure 1.5 illustrates a comprehensive research method of this dissertation.

In the first phase, research is focused on exploring and understanding the concept of Network Security Situation Awareness (NSSA), formulating the problems in NSSA and then defining the research objectives and scopes. The key activity in this phase is to identify the problems existing in NSSA such as the completeness of criteria concerned in the assessment stage and also the rate of precision in prediction stage. From the addressed problems, research objectives and scope have been defined clearly.

In the second phase, literature of some assessment and prediction techniques have been reviewed in order to discover their requirements and core concept practiced in the process. Based on that, these assessment and prediction techniques have been grouped into different categories. The strengths and limitations of each category have been identified before the module design starts.

In the third phase, based on the information explored and gathered in previous phases, current network security assessment and future network security prediction modules have been designed. The design of proposed modules are theoretical trial and error research. This design starts with developing an initial situation assessment algorithm and time-interval prediction algorithm and then integrating them to form a network security situation assessment and prediction mechanism. The process of modification is done continuously until the proposed mechanism achieves the objectives of this research.

In the fourth phase, a prototype of the mechanism has been developed in order to implement the proposed assessment and prediction modules. The purpose is to

assess the performance in the aspect of precision of the proposed mechanism. Three evaluation metrics, Relative Percentage Error (RPE), Mean Absolute Percentage Error (MAPE) and Root Mean Square Deviation (RMSD) have been calculated with benchmark datasets, Defense Advanced Research Projects Agency (DARPA) 1999 and 2000 as well as National Advanced IPv6 Centre (NAv6) 2015 dataset.

In the last phase, the results gained from previous phase have been compared with other existing techniques and justification has been made from the evaluation process. Then, the deliverables of each phase have been finalized and documented.

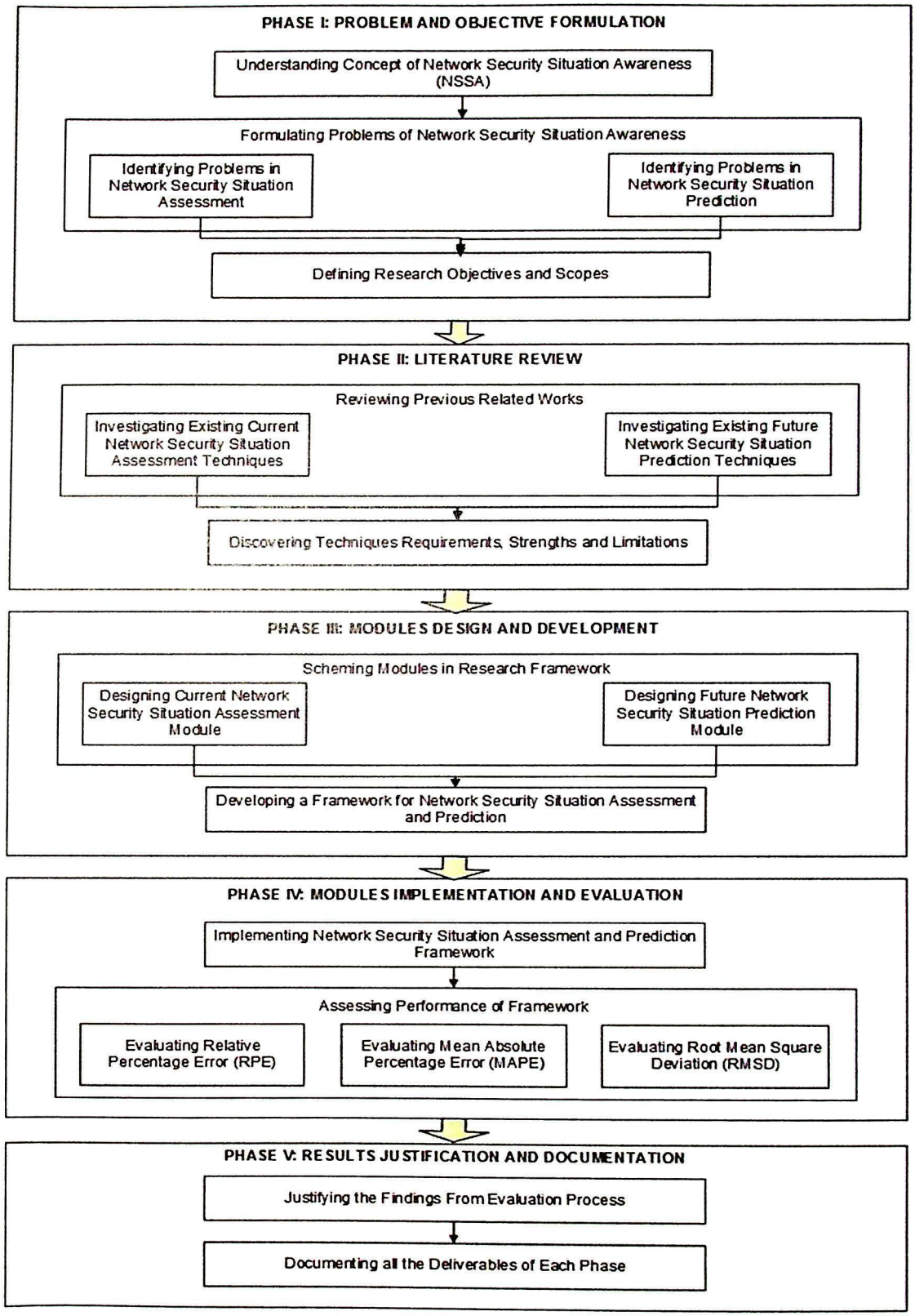

Figure 1.5: Research Methods

1.9 Research Contribution

The roles of IDSs in network security and its weaknesses have been briefly discussed. As mentioned in Section 1.3.4, there are two types of IDSs which are misuse-based and anomaly-based. Both have their own advantages and disadvantages in detecting intrusion alerts. The main shortcomings of IDSs are their inability to provide the useful information such as security situation of the entire network to the administrator and only has the ability to detect the malicious activities after the incident while any loss or damage have already been done. These limitations have increase the interest of researchers to look for new alternatives to gain information about the current security situation as well as incoming security status in the whole network. This information will be helpful for the network administrator in making good decisions and to take more appropriate response towards the malicious attacks before further exploitation to the network in future. Therefore, this research has presented two main contributions as listed below:

- An Entropy-based Network Security Situation Assessment scheme with the aid of the AHP which consider tangible and intangible criteria on every single asset in the network.
- A novel Adaptive Grey Verhulst-Kalman Prediction scheme to forecast the incoming network security situation while taking into account both initial predicted value and its predicted error based on historical records.

1.10 Chapter Organization

This thesis is organized into six chapters as follows.

Chapter 1 presents some facts of network incidents which has caused our community to be in a dilemma presently and an introduction to a brief background of

Network Security Situation Awareness concept. The problem statements, objectives and contribution of the research are clearly defined in this chapter.

Chapter 2 describes the nature of intrusion attack and the attacks types. This chapter also explains the history and concept of Network Security Situation Awareness in detail. Some existing network security situation assessment and prediction works are studied and grouped into three categories. The strengths and limitations of each category are highlighted.

Chapter 3 illustrates the proposed overall mechanism in overall which consists of four phases. To demonstrate the design and architectures in each phase, the methodology steps are sequentially and clearly explained with the aid of detailed flowcharts.

Chapter 4 depicts the implementation details of the proposed mechanism. Several scenarios with different datasets were executed in the developed prototype of proposed mechanism as well as existing methods in grey prediction.

Chapter 5 covers in-depth analysis of the proposed mechanism performance based on the results obtained through the experiments. Statistical metrics for evaluating the accuracy of the proposed prediction mechanism are mentioned. For each dataset, the results of comparison between the proposed prediction mechanism and other grey prediction methods are included.

Chapter 6 summarizes the whole discussion and provides the conclusion of the research covered in this thesis. Some recommended future directives are also discussed in this chapter.

CHAPTER 2
LITERATURE REVIEW

2.1 Introduction

In recent years, network has penetrated and essentially been integrated into our lives and work in providing convenient services such as information sharing, resource accessing and etc. However, new security challenges are constantly emerging while people are sharing their resources in this convenient condition. In a Data Breach Investigation Report 2014, it stated that there have been 63,437 security incidents recorded from 50 organizations from around the world in 2013. These network attacks intruded into different industries such as the public sector, finance institution, manufacturing, healthcare and etc (Verizon, 2014). The number of network intrusion attacks have reached an alarming level and begun to threaten internet users in their daily activities.

2.2 The Nature of Intrusion Attack

A network intrusion attack is an event that compromises the network stability or the security of information that is stored in computers connected to it. These events might include attempts to destabilize the whole network, gain unauthorized access to files or privileges as well as simple mishandling and misuse of software (Portnoy, 2000). The chronology of an intrusion attack can be presented in a risk-time curve as Figure 2.1. Initially, the host is in a normal state without any suspicious incidents. Then, the attackers begin preparation by finding out as much as possible about the target. The technique such as port scanning is used to gather the network information such as standard ports or services that are running and responding, types and version of

applications and also the operation system installed on the target system (Pfleeger and Pfleeger, 2002). In this state, the system's availability will be affected and the likelihood of an attack will increase. Therefore, the accumulated curve of risk index grows gradually. Although the number of attempts is huge in this situation, the severity of attacks is still low. Once significant network information has been collected, attackers start to identify and realize the potential vulnerable services and security level of the target. Then they will adopt some hacking techniques or plant the malwares which are a higher severity of attack on the target so as to evade detection and countermeasures. The system performance will now be seriously affected. These intrusion behaviours grow the risk index more rapidly and the curve becomes steep. The risk index reaches its limitation when the target is exploited and the curve becomes smooth again. In a nutshell, the variation of the situation which makes the curve of accumulated risk index with time behaves in an S-shape will be repeated when a new intrusion occurs in the network.

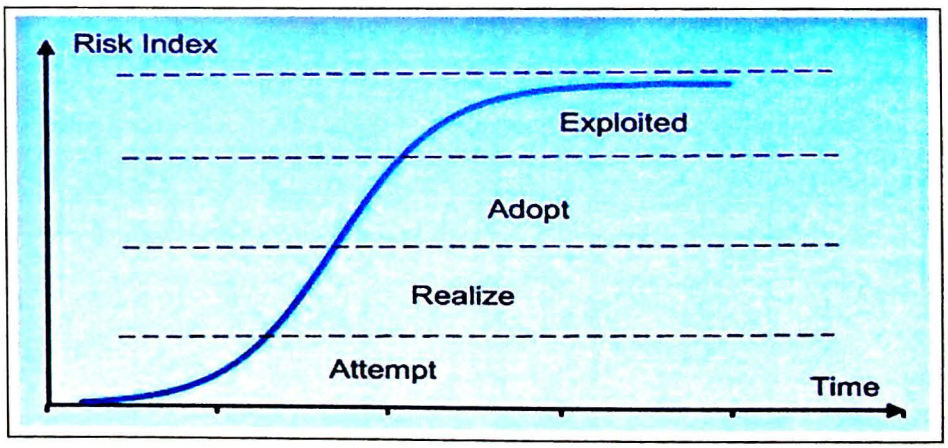

Figure 2.1: The Chronology of an Intrusion Attack

2.3 Types of Network Attacks

Basically, network attacks can be grouped into four main categories. There are Probing Attack, Denial of Service Attack (DoS), Remote to User Attack (R2L) and User to Root Attack (U2R) (Tavallaee et al., 2009, Paliwal and Gupta, 2012, Dastanpour and Mahmood, 2013, Siddiqui and Naahid, 2013, Revathi and Malathi, 2014).

2.3.1 Probing / Scanning Attack

Probing Attack is an attack in which the attacker tries to gather information of network devices such as the host by scanning the network. The intention of this attack is to determine the vulnerabilities of a targeted machine in order to circumvent its security controls during the system compromise process. This probing attack contains some attacks such as Portsweep, Satan, Nmap, Ipsweep and others.

2.3.2 Denial-of-Service Attack (DoS)

Denial-of-Service Attack is an attack in which the penetrator attempts to make a machine or network unavailable in terms of busying and overloading some computing and memory resources for its intended users. It causes the machine to fail to handle legitimate requests and hence denying user access to it. Apache, Smurf, Neptune, Ping of Death, Land Attack, Teardrop Attack and etc are some examples of DoS attack.

2.3.3 Remote to User Attack (R2L)

Remote to User Attack is an attack in which the hacker is able to send packets to a machine over a network although he does not have an authorized account to access it. The unauthorized access from a remote machine such as local or known user in the

machine allows the hacker to expose the machine vulnerabilities and exploit its privilege. Some of the R2L attacks are Multihop, Imap, Warezclient, Spy, Sendmail Dictionary Xnsnoop and etc.

2.3.4 User to Root Attack (U2R)

User to Root Attack is an attack in which the intruder starts to access the machine with an ordinary user account which might be gained by social engineering, dictionary attack or password sniffing. It enables the intruder to exploit and abuse the vulnerabilities in the machine and gain local super user (root) privileges on it. Buffer Overflow, Perl and Rootkit are some instances of U2R attack.

2.4 The Evolution of Network Security Situation Awareness (NSSA)

The concept of Situation Awareness (SA) was first introduced in the aviation and aerospace realms throughout the research which were the focus on human factors. Its objective is to ensure the necessary information is readily accessible and understood by various levels of decision makers and analysts by providing them in an abstract visual format. In 1987, Emerson and his group had defined SA as the crew's knowledge in both internal and external state of the aircraft as well as the operating environment (Emerson et al., 1987). It is the knowledge of current and near-term disposition of both friendly and enemy forces within a volume of airspace (Hamilton, 1987). SA seems like an internal model of the world around the pilot at any point of time (Endsley, 1988b). The pilot has to understand and integrate the factors which will contribute to the safe flying of the aircraft under normal or non-normal conditions (Regal et al., 1988, Vidulich, 1995). Based on Taylor's point of view, SA was probably the pre-requisite state of knowledge in making adaptive decisions especially in

uncertainty situations (Taylor, 1990). The continuous perception of pilots and the aircraft in relation to the dynamic environment of flight, threats, mission and the ability to foresee enabled them to execute their tasks based on that perception (Carroll, 1992, McMillan, 1994). In 1995, from the human factors' perspective, Endsley agreed that SA provides the primary basic for subsequent decision making and performance in the operation of complex and dynamic systems which has a narrow space of time. Ongoing and up-to-date analysis of the environment is essential to accomplish the tasks. The operator needs to quickly perceive relevant information from the environment, integrate them in conjunction with task goals and forecast the events and system states in future (Endsley, 1995a). A model of SA in dynamic decision making has also been introduced as Figure 2.2.

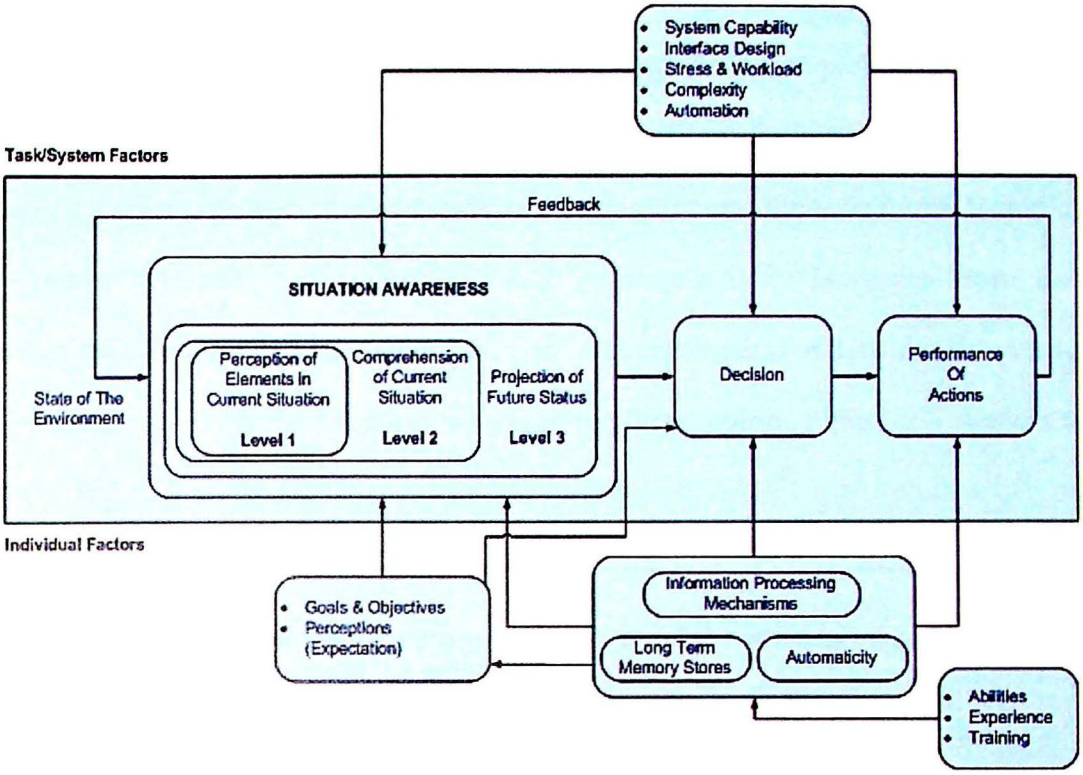

Figure 2.2: Endsley's Model of Security Awareness in Dynamic Decision Making (adapted from (Endsley, 1995b))

Detect, integrate and interpret data as well as predict the incoming situation are main components in many real world conditions in which the data may be spread throughout the visual field and is frequently noisy (Green et al., 1995). To firmly expand upon their perspective of SA, Endsley and her group have illustrated SA into three hierarchical phases which begins with Perception, followed by Comprehension in the next level and the highest level which is Projection (Endsley et al., 1998). Perception classifies information about the status, attributes and dynamics of relevant elements within the environment into understood representation. It is the basic building blocks which will be provided to comprehend and project in forming a correct picture of the situation. Comprehension of the situation includes how people integrate multiple pieces of information, interpret them in terms of their relevance to an individual's