A NEW APPROACH BASED ON HONEYBEE GUARDING SYSTEM TO IMPROVE INTRUSION DETECTION SYSTEM

by

GHASSAN AHMED ALI

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

2011

ACKNOWLEDGEMENTS

The PhD journey has certainly been a learning experience, on many levels, and there are many people who have had an impact in one way or another. Although this thesis represents an achievement that bears my name, it would not have been possible without help of others who I would to thank. First, and for most, I thank Allah for all his blessings and guidance. I thank Him for bestowing health upon me to be able to think and for opening the way to gain knowledge.

I am grateful to my parents for being there for me, for their prayers, for their love and care, for teaching me those good things comes with hard work.

I sincerely thank my wife for her great encouragement and understanding during these years of my study. I am so grateful for unconditional love, patience, time, and support to finish this research. I still remember her voice: "Oh!! Ghassan work hard, focus!!". She didn't go around and lost a lot in order to untiring help during my difficult moments. Thank you so much my lovely wife.

I would like to express my sincere thanks and deepest gratefulness to my supervisor Dr. Amar Jantan for his supervision, encouragements, guidance, insightful criticism, and for all of his help during my research work and preparation this thesis.

I express my special thanks to School of Computer Sciences for all facilities and support to achieve this research.

I am deeply thankful to my closest friends and my pillars of support Rasmi, Abdulghani, Fazli, and Izham for their help and support during my thesis preparation.

To the Souls of all "Shahids in Al-Tagheer Squares" in My Country

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACO	Ant Colony Optimisation
AI	Artificial Intelligence
AIS	Artificial Immune System
ANN	Artificial Neural Network
BA	Bees Algorithm
BN	Bayesian Network
DARPA	Defence Advanced Research Projects Agency
DP	Desirable-Present
DDoS	Distributed Denial of Service
DoS	Denial of Service
DT	Decision Tree
ENN	Evolutionary Neural Network
FN	False Negative
FNR	False Negative Rate
FP	False Positive
FPR	False Positive Rate
GA	Genetic Algorithm
GP	Genetic Programming
HMM	Hidden Markov Model
HN	Hidden Neurons
IDS	Intrusion Detection System
KBS	Knowledge Based System
KDD	Knowledge Discovery and Data mining
LVQ	Learning Vector Quantization
MLP	Multi Layer Perception
MSE	Mean of Squared Errors
NB	Naive Bayes
NeGPAIM	Next Generation Proactive Identification Model
NN	Neural Network
PAIM	Proactive Identification Model
PSO	Particle Swarm Optimization
RBF	Radial Basis Function
ROC	Receiver Operator Curve
SVM	Support Vector Machine
TNR	True Negative Rate
TN	True Negative
TPR	True Positive Rate
TP	True Positive
TTL	Time To Live
UA	Undesirable-Absent

SATU PENDEKATAN BARU MENGGUNAKAN SISTEM PENGAWALAN LEBAH-MADU UNTUK PENAMBAHBAIKAN SISTEM PENGESANAN PENCEROBOHAN

ABSTRAK

Serangan yang semakin meningkat terhadap rangkaian dalam pelbagai cara yang canggih mendapat perhatian daripada pihak keselamatan rangkaian. Sistem pengesanan penerobohan (intrusion detection system, IDS) digunakan untuk mengenal pasti atau membezakan antara pengguna yang sah (legitimate incomer) dengan peneroboh. Masalah utama IDS adalah untuk mengkelaskan pengguna yang masuk dan mengelompokkannya dalam kumpulan tertentu berdasarkan sifat khususnya. Di samping itu, terdapat juga kesukaran dalam membezakan antara paket yang sah dengan paket peneroboh. Oleh itu, suatu model khusus diperlukan untuk meningkatkan proses pengelasan dalam usaha memperoleh suatu keputusan yang tepat. Justeru, mekanisme gera dalam IDS hendaklah ditingkatkan agar mesej yang dihantar untuk sesuatu tindakan adalah tepat. Secara amnya, kebanyakan sistem pengesan yang sedia ada hanyalah bertindak menyerang tanpa terlebih dahulu membuat sebarang pengesanan. Hal ini menyebabkan banyak serangan yang dilakukan adalah salah.

Kami mencadangkan satu pendekatan baru yang mana telah diilhamkan dari konsep lebah madu di alam semula jadi untuk mengatasi masalah mengenal pasti dan pengklasifikasian IDS. Di sini, kami menyiasat sistem koloni lebah madu serta mekanismc perlindungan dan pengesanan mereka untuk meningkatkan pengesan IDS supaya menjadi sistem IDS yang lebih baik untuk pengesanan dalam rangkaian. Jenis

yang berbeza untuk pengesan IDS dan penyelesaian semasa telah diselidiki dan sifat-sifat mereka serta ciri-ciri telah ditetapkan secara am. Kemudian, kami meniru dan mengadaptasikan sistem lebah madu sebagai suatu pendekatan baru dalam IDS. Hasilnya, kami mendapati Jaringan Saraf (Neural Network) yang dilatih oleh " Algoritma Lebah" ini dapat mempelajari corak serangan melalui set data terlatih malah ia juga dapat mengesan corak serangan di dalam set data ujian yang disediakan. Tambahan pula, Jaringan Saraf (Neural Network) dapat mengesan tindak balas janggal berdasarkan model tindakan normal yang telah dilatih untuk mengesan sebarang gangguan baru dalam masa nyata.

IDS yang dicadangkan dinilai menggunakan set data DARPA KDD 99 dan eksperimen menunjukkan bahawa prestasi pendekatan yang dicadangkan boleh mengesan penerobohan baru dan mengurangkan gera-palsu. Justeru, adaptasi pengesanan lebah-madu dan sistem ketahanan merupakan suatu pengetahuan baru yang boleh membantu sistem lain, contohnya IPS, antivirus, atau sistem ketahanan untuk meniru teknik AI dalam melaksanakan fungsi mereka.

A NEW APPROACH BASED ON HONEYBEE GUARDING SYSTEM TO IMPROVE INTRUSION DETECTION SYSTEM

ABSTRACT

Increasing of network attacks with sophisticated forms has made the network security concern a significant necessity for such a network. The intrusion detection system (IDS) used to identify the legitimate incomer from an intruder. The main problem in an intrusion detection system is to identify incoming network packet, then assign it to a selective group based on specific characteristics. In addition, it is also difficult to distinguish between intruder packet and valid packet that lead to the need of a certain model to improve classification process in order to get a correct decision for proper action. Furthermore, the mechanism of alert notification in IDS should be improved to provide more accuracy in conveying the exact message for suitable action rather than disturbing the user. In general, most of the existing systems detect general and only known attack. Therefore, a lot of malicious attack intrudes without any detection.

A new approach, which has been inspired from the honeybee in nature, is proposed to overcome such identification and classification problems of IDS. We investigate the honeybee colony system as well as their protection system and detection mechanism to get an improvement approach for IDS detector in order to enhance IDS system for better intrusion detection. The different type of IDS detector and current solution are explored and their attributes as well as features and needs are generalized.

Then, the good features and attributes of the honeybee system are imitated and adopted to produce a new approach to be employed in IDS.

The neural network, which is trained by Bees Algorithm, is used to learn patterns of attacks given in training dataset and use these patterns to find specific attacks in test dataset. Moreover, the trained neural network detects anomalous behaviors based on the trained normal behavior model in order to train the detector in real-time to detect new intrusions.

The proposed IDS is evaluated by using DARPA KDD 99 dataset and experiments show that the performance of the proposed approach can detect novel intrusions and reduce false alarms. Furthermore, the adaptation of the honeybee detection and defense system itself is a new knowledge that can also help other systems such as IPS, antivirus, or even defense system to imitate the AI techniques in performing their functions.

CHAPTER ONE

INTRODUCTION

1.1 Problem Overview

Researches in computer security technologies remain obsession for many years of improvement and growth. However, it still needs a lot of hard work to settle the critical security problems. According to the 2010 Cyber Security Watch Survey (CSO, 2010), the number of security incidents continues to increase faster than companies' defenses. Within the reports, the outsider attacks are the main threats of cybercrime in general. However, more costly incidents are caused by the insider.

Certain techniques are used to secure data, such as firewall, encryption etc. Nevertheless, most defense systems are still susceptible to attacks and intrusions. For example, firewall acts as the first line of defense to protect sensitive data. However, the firewall merely reduces exposure rather than monitors or eliminates vulnerabilities in computer systems. Furthermore, as stated by Ghosh et al. (1998), firewall unable to detect novel attacks. At the same time, the encryption adds an extra burden on hosts or applications. Therefore, the need of a detecting system to detect intrusion attempts from attacking the whole system is a very critical issue.

The intrusion detection is a set of methods and techniques that are used to detect malicious attacks. It is a mechanism normally deployed to solve the problem of recognizing intruder's attempt. According to Denning (1987), the intrusion detection system (IDS) is a framework that acts against intrusions and inform administrator to respond. The main concern of IDS is to monitor the traffic state by looking for unauthorized usage, denial of services, and anomalous behavior. The key in IDS is to

detect intrusions. The idea is that if it is not possible to prevent attacks, at least it may be possible to detect these attacks. Then once detected, it can be in some way to prevent the attacks as claimed by Benjamin (2007). The IDS aims to support the essential security issues via scrutinizing every entry and then feedback the user regarding the systems' situation. It acts as the "second line of defense" inside the network and it is need as another wall to protect network systems. The IDS gives a clear picture of the threats that is faced by the system and provides an ability to see all the network traffic.

The concept of intrusion detection was born with Anderson's paper in 1980 (Anderson, 1980). Since then, several researches published and many technologies improved the intrusion detection system to its current state. Figure 1 shows the timelines of the significant works on early state of IDS.

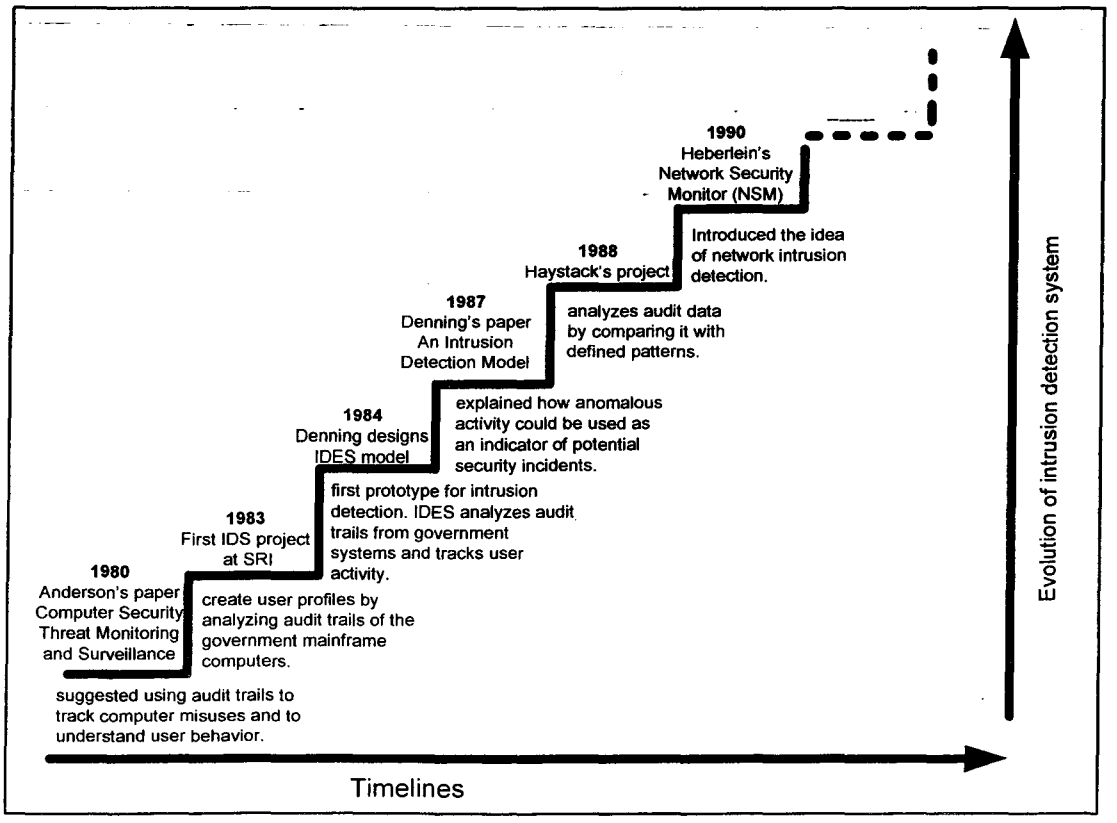

Figure 1.1: The Evolutions of IDS on Early Stage.

The main problem that arises when deploying intrusion detection system has led to the generation of excessive amount of false alarms. In addition, IDS fails, in many situations, to meet a high detection rate and not capable to detect unknown intrusions. These two cases are because of the difficulty that IDS faces to determine whether such action is either a malicious or a normal. Both of these weaknesses significantly reduce the benefit of IDS and make the area of IDS an attractive and open research field.

In general, the criterion for evaluating the efficiency of IDS is the capability to detect novel attacks, while minimizing the false alarms. The previous approaches on intrusion detection such as (Sarafijanovic S. and Boudec J., 2003), (Abadeh M.S. and Habibi J. , 2007), and (Özyer et al., 2007) focus on improving detection accuracy and restraining false alarms. Among these approaches and methods which spread in the IDS researches are artificial intelligence techniques such as the social insects' behavior approaches due to the nature and suitability of problem identification in social insects to the problem of intrusion detection.

A great deal of successful research in the field of computer security has been inspired by biological systems as stated by Meisel et al. (2009). Many researchers such as (Rains, 2008) and (Srinoy, 2007) have argued that social insects' behavior system provides us with a powerful metaphor that can be applied to solve the problems in intrusion detection system

The crossover between the behavior of social insects and computer science is declared by Bonabeau et al. (1999) as "any attempt to design algorithms or distributed problem-solving devices inspired by the collective behavior of social

insect colonies and other animal societies''. From studying how social insects perform tasks, it can be figured out such model to be used as a basis for developing, either by tuning the model parameters beyond the natural relevant range or by adding natural features to the model as it has suggested in (Ghassan et al., 2008; 2009; 2011).

The ability to recognize and detect intrusion is critical to the maintenance of social insect colonies integrity which recommended in (Ghassan et al., 2009), as well as (GH Lai et al., 2008), and (Mukkamala et al., 2002). However, many proposed methods can only be applied in specific cases where such attacks are known. This means that the system has to know the attack to be able to detect it. In our case, we lean on natural honeybee, which faced the analogous security problems. Honeybees survive in difficult environments and different levels of threats to security. These threats motivate bees to detect and respond quickly on any aggressive acts that may attack the colony as mentioned by Couvillon (2008). A lot of work has been carried out such as by Horridge (1999) and Breed (2004), which try to understand and extract the key mechanisms through how the natural bee guarding system can achieve its detection and protection capabilities.

The detection system in honeybee which keeps the colony safe would be the basis of the main framework of this research. Figure 1.2 depicts the areas in our work. We concern on discrimination between innocuous and the intrusion by capturing the intrusion ones based on some techniques, which have been inspired from the nestmate-recognition system in honeybee.

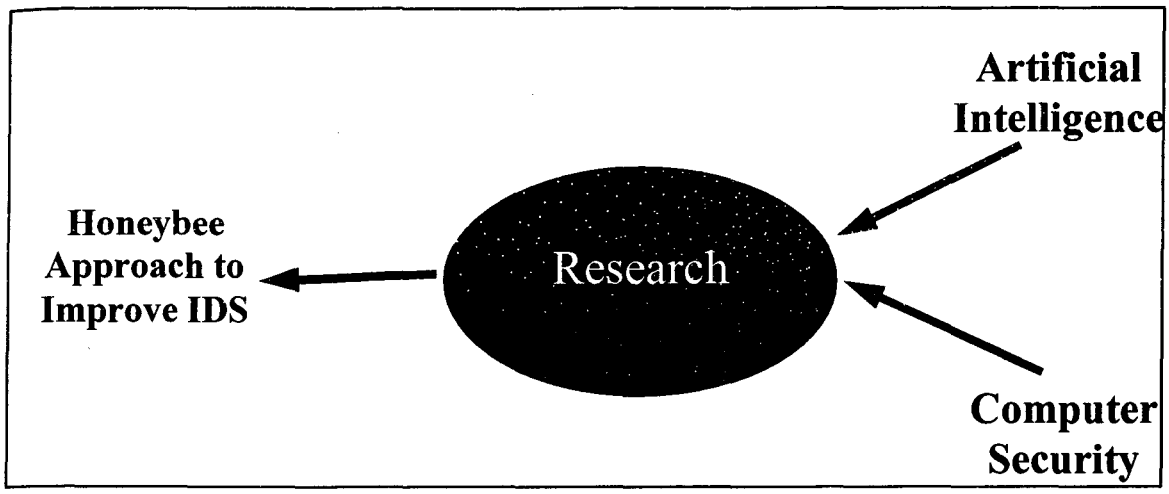

Figure 1.2: Research Areas.

The methods Undesirable-Absent (UA), Desirable–Present (DP), and Filtering-Decision (FD) that honeybee guard uses in nature in order to filter the incomer are applied to the IDS. Further details about these methods will be indicated in Chapter 3.

1.2 Research Motivation

IDS technology has become an essential part of defense in computer network security infrastructure. However, according to Sobh (2006), a failure of IDS to detect novel attacks and the increase of false alerts are the major problems in most of the network-based IDS detector. Moreover, the intruder might try to take advantage of the false alarms to hide an attack to locate and exploit vulnerability on the system. Ultimately, this will help the attacker to control the function of the security detector due to the high volume of fake attacks such that a massive DoS attack to defer detector function.

Bakar et al., (2005), Abraham et al. (2007), and Shafi et al. (2009) declared that the high volume of false alerts is a very time consuming task for network security

analysts to determine whether it is an attack or not. As a result, a remarkable effect of the analysis at higher stages is occurred. Hence, there is a need for efficient IDS detector for tuning alerts to minimize false alarms.

The intrusion detection processes require comprehensive and sophisticated techniques to be employed for proper intrusion detection and response. Particularly, the network intrusion detection problem requires adaptive and intelligent systems, which are able to work in different environments. Thus, it is an advantage to use several computing techniques and approaches for the problem of intrusion detection. This study is conducted to prove the hypothesis that the detection's deficiency of IDS detector can be improved by supplementing a defense-in-depth strategy at a detector level to alleviate higher level of analysis operations.

1.3 Goal and Scope

This study proposed a new approach, which emulated the Honeybee guard approach in nature for improving the IDS detection accuracy and performance. The ultimate goal is to develop an IDS system which is capable to address IDS shortcomings to some extent and able to detect various attack types.

In this thesis, the focus is on hybrid intrusion detection system utilizing both anomaly and misuse detection aspects. The proposed approach takes the advantages of both modules. *Undesirable-Absent* detector is responsible for detecting pre-defined attacks based on their attack signatures. Neural network trained by Bees Algorithm is used to learn the patterns of attacks given in training dataset and these patterns are used to find specific attacks in test dataset. *Desirable-Present* detector is responsible

for detecting anomalous behaviors based on the trained normal behavior model. A neural network trained by Bees Algorithm is used to build a normal behavior model. The *Filtering Decision* is used to train the *Undesirable-Absent* detector in real-time to detect new intrusions.

This dissertation advances current knowledge in intrusion detection by providing insights into how the combination of knowledge will achieve success in an intrusion detection system. From the widest scope, firstly, we combine social insects and network security knowledge. Then, we combine *Undesirable-Absent* and *Desirable-Present* detectors. At the technique level, we also combine neural network and Bees Algorithm. In addition, deploying such detection approach will provide a multilevel checking on legitimate activities. Each level of the proposed approach has a method to detect the unwanted activities, which will increase the efficiency and give wider coverage of detection. Furthermore, we will see that the proposed hybrid in such levels give better performance over individual alone by reducing the false alarm rate to an acceptable level and enhancing detection accuracy, thus guaranteeing the proposed approach to be applied in practice.

1.4 Objectives

This thesis demonstrates the analysis of HoneybeeGuard effectiveness which is inspired from the behavior of the honeybee in nature. It introduces an approach to solve the intrusion detection problem. The main objectives of this study are:

1. To formalize and figure out an approach based on honeybee guarding system of intrusion detection that would be the basis frame for the model of intrusion detection system, originally initialized here.

2. To design a new detection approach on the way to improve the intrusion detection using a well-trained neural network by the bees algorithm and hybrid module intrusion detection.
3. To implement the proposed system and evaluate the effectiveness of the approach in increasing the detection accuracy and performance.

1.5 Methodology

In this study, we use Artificial Intelligence (AI) techniques in order to take the advantages of the new approach to improve the IDS. According to Kabiri et al., (2005) and Servin et al., (2008), the concept of using AI to solve the two IDS problems is very efficient. The generalization of AI makes possible decreases of false alarms as well as increases the accuracy of an intrusion detection process.

One of the important requirements for the technique to support the proposed approach is the ability of learning. Besides that, this technique is supposed to distinguish different characteristics after some level of training. Thus the neural network has been chosen to be the main component of the model because of the many features that neural network poses such as the ability of learning, generalizing attributes even with noisy data, and the capability of classifying patterns effectively. These features can be further used to improve detection and reduce false alarms in the intrusion detection system.

Nevertheless, the neural network alone cannot take the complete advantages of the proposed approach because it has some drawbacks such as a computational complexity, its convergence of the learning process is slow, and difficulty of

parameter settings. Therefore, many global optimization techniques have been proposed to train a neural network to tackle these problems and enhance learning efficiency such as Particle Swarm Optimization suggested by Srinoy et al. (2007) and Genetic Algorithms proposed by Hua et al. (2009).

In this research, an alternative method based on the Bees Algorithm (BA) is proposed to be used in training neural network. BA is a new optimization algorithm that imitates the natural foraging behavior of bees. It was proposed by Pham et al. (2006) and has been successfully applied to different optimization problems including the training of neural networks for wood defect identification by Pham et al. (2006) and control chart pattern recognition by Pham et al. (2007), which shows better results than other methods. To the best of our knowledge, the construction of training neural network by BA to improve the performance of an intrusion detection system has not been addressed in the literature. Here, the bees algorithm extends to classification and demonstrates its effectiveness in intrusion detection.

We train the system with different types of attacks data and model different types of attack signatures under different phases. Figure 1.3 on the next page, shows the proposed system overview. The performance of the proposed IDS is evaluated by using KDD 99 dataset, which is the popular benchmark dataset used by IDS researchers. After the training phase, the neural network will be able to make the distinction between both normal and anomalous and then within anomalous between different attack classes. Once the neural network is trained, it can be used to classify new data sets whose input/output associations are similar to those that characterize the training data set.

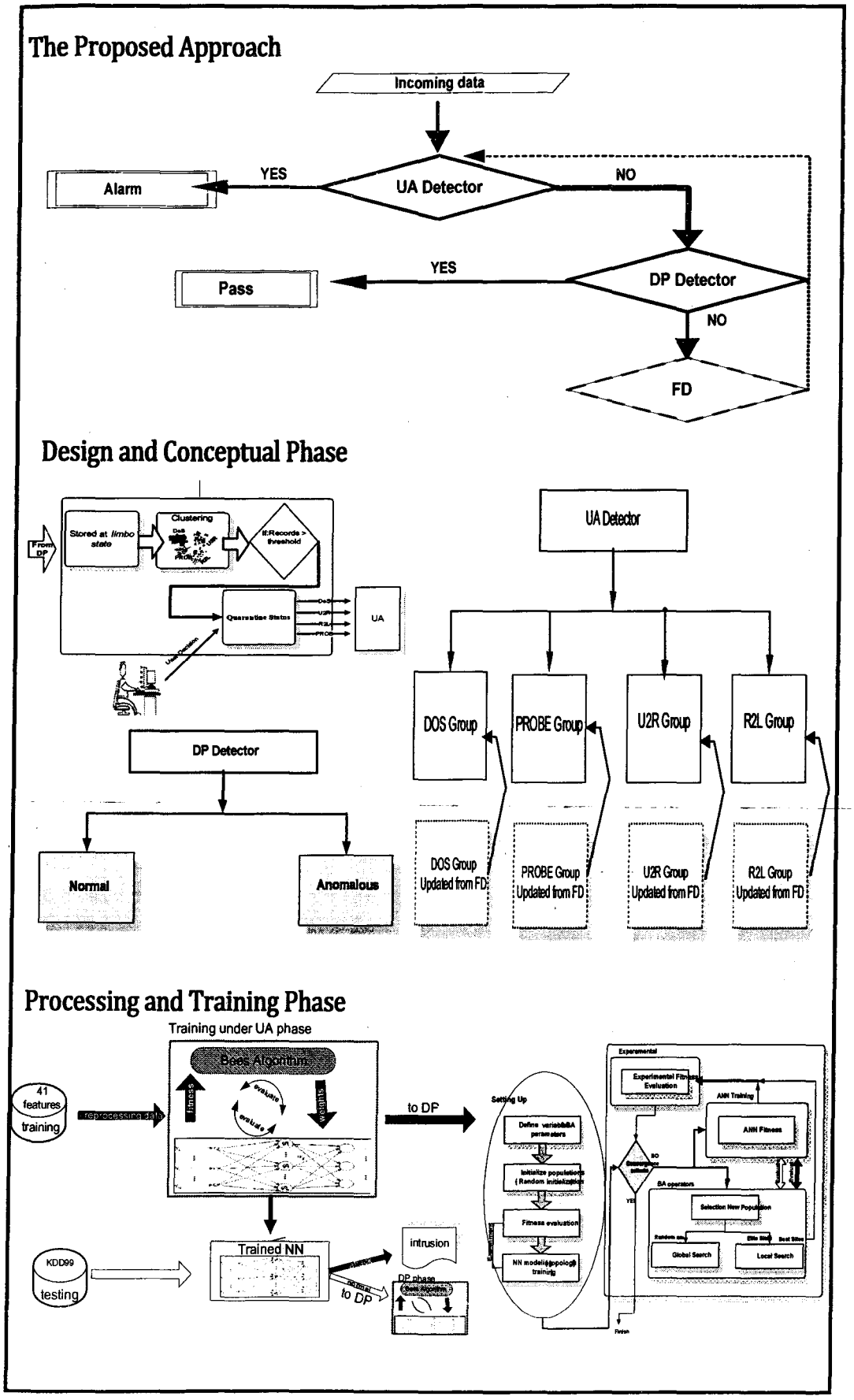

Figure 1.3: General System Overview

1.6 Contributions of the Study

The main contribution made by this thesis is about emulating the nestmate-recognition system, which inspired from the natural honeybee to improve the detection accuracy and reduce the false alerts. The contributions are illustrated as follows:

1. Defining a new approach based on natural honeybee to eliminate anomalous network data using the most significant features of the packet.
2. Building an *Undesirable-Absent* detector to detect the known intrusions accurately. This detector contains a neural network which trains by the bees algorithm. The training aims to filter out the incoming packet that poses the undesirable characteristics.
3. Building a *Desirable-Present* detector to filter out the abnormal data and detect the novel attacks. This detector also contains the neural network trains by the bees algorithm but under desirable characteristics.
4. Designing the *Filtering Decision* method, to enhance the *Undesirable-Absent* detector's functionalities and performance. The *Filtering Decision* clusters the data which filters out from the *Desirable-Present* detector, and uses these data to train the *Undesirable-Absent* classifier.

1.7 Thesis Outline

The next Chapter (2) describes the background and literature review for understanding the proposed work. Chapter 3 presents the honeybee approach of detection in detail, components, properties, and features of approach. The approach is then applied to the domain of an intrusion detection system. The design of the system is offered in Chapter 4. Further details, evaluation of the dataset, testing and

discussion of the proposed system in the context of network IDS are described in chapter 5. In Chapter 6, general discussion and directions for future work are discussed. Finally, Chapter 7 presents the conclusion. Figure 1.4 shows the structure of the thesis.

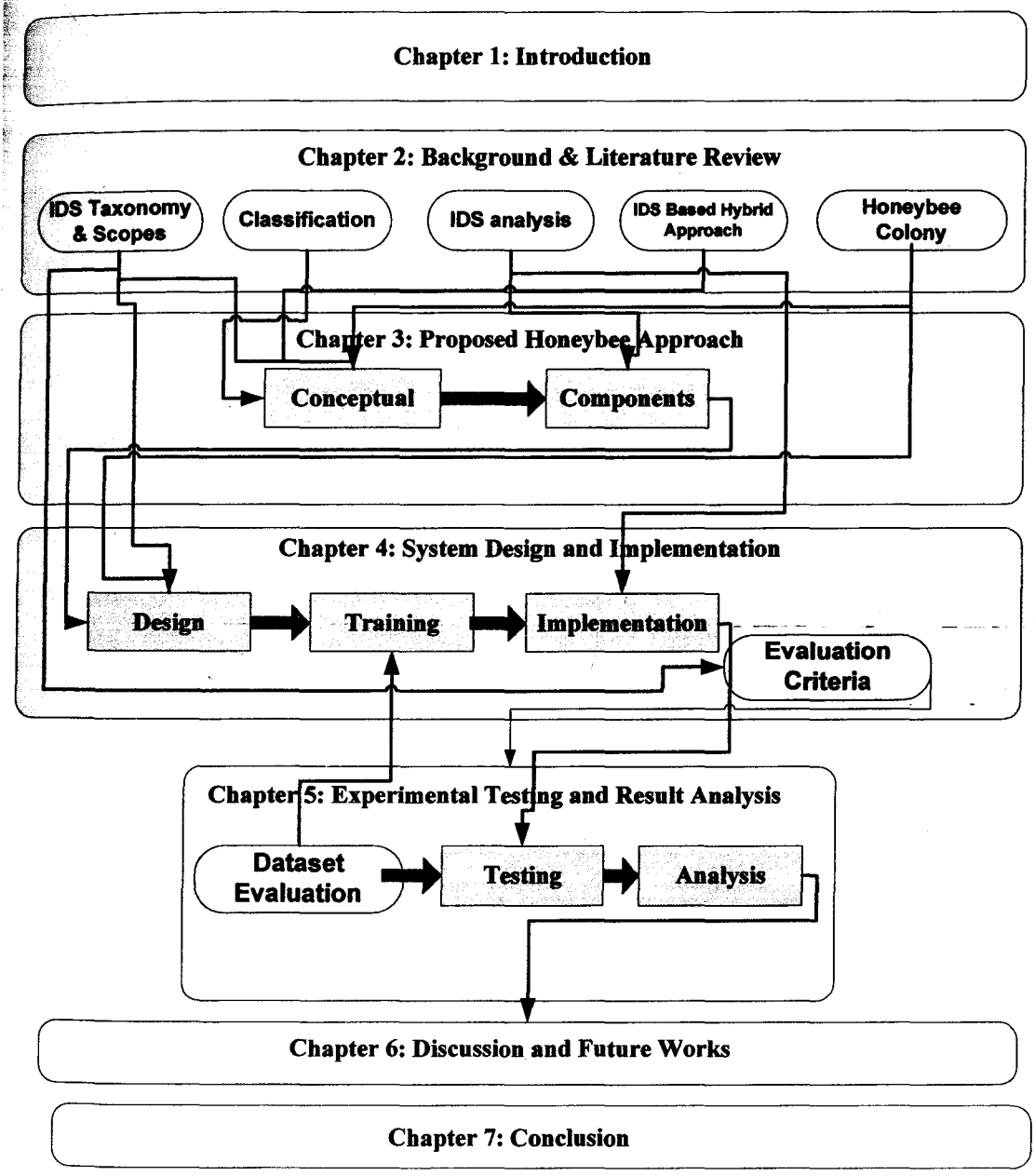

Figure 1.4: Thesis Outline

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The aim of this chapter is to provide a literature review of this thesis. The chapter will state previous works related to the research area. It starts giving a basic concept of the most important network security technologies, i.e. IDS. Here, the focus will be on the detection issue, thus others issues such as response or prevent will not be investigated.

The literature review presented here focuses on two parts: the first is to present a comprehensive survey on research contributions that investigate utilization of Artificial Intelligence (AI) methods in building intrusion detection models. The second aim is to define existing research challenges, and to highlight promising new research directions. The scope of the survey is the core methods of AI, which encompasses artificial neural networks and bees algorithm. Figure 2.1 on the next page clarifies the hierarchy of this chapter and gives general view of how this chapter is organized and arranged. It is used as a guideline throughout this chapter.

From Figure 2.1 we can notice the main areas of the research literature review and the overlap between the elements of the research. Each level represents as a section in this chapter and provides an overview of the works with related problems. Moreover, an overview of research performed in this area is given and evaluated for each section. This evaluation leads to the statement of the goal of this thesis.

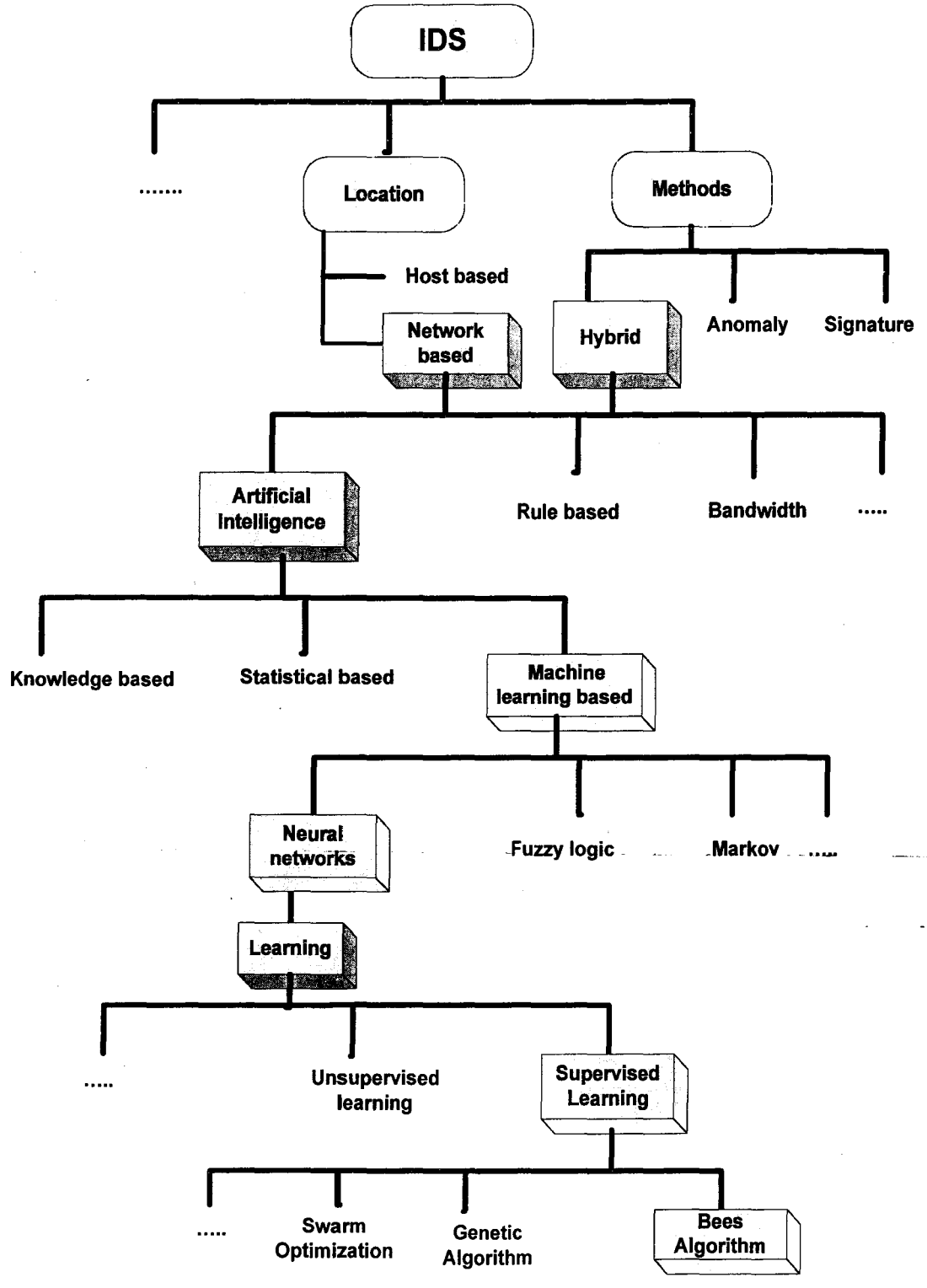

Fig. 2.1: The Literature Survey and Related Work

2.2. Intrusion Detection System (IDS)

2.2.1. Overview

An intrusion is any set of actions that attempt to compromise confidentiality, integrity, and availability of a resource. Intrusion detection is declared by Ghorbani et al. (2009) and Simson (1996) as the process of monitoring computer networks and systems for violations of security. An Intrusion Detection System (IDS) is a computer system that monitors the system and the activity in the computers and the networks in order to detect abnormal or suspicious activity. In case of detecting intrusion, IDS alerts the system or network administrator to take an appropriate action. As stated by Sobh (2006), IDS does not usually perform any action to prevent intrusions when an attack is detected; its main function is to alert the system administrators. IDS role is more reactive than proactive (Sobh, 2006). In other words, IDS plays the role of an informant rather than defender and does not attempt to stop an intrusion when it occurs but alert a system security officer that a potential security violation is occurring.

In the early 1980s, Anderson stated that an intrusion attempts to: access information, manipulate information, and/or render a system unreliable or unusable (Anderson, 1980). Figure 2.2 on the next page shows scenario of these intrusion attempts. The figure shows that the intrusion attempts target the information sources to break into or performs an action not legally allowed. Recent researches such as Fida and Khaled (2010), Ghorbani (2009), and Sobh (2006) declare that the intruder also attempts to create false information or to alter or destroy sensitive information and service availability to prevent legitimate users from using resources.

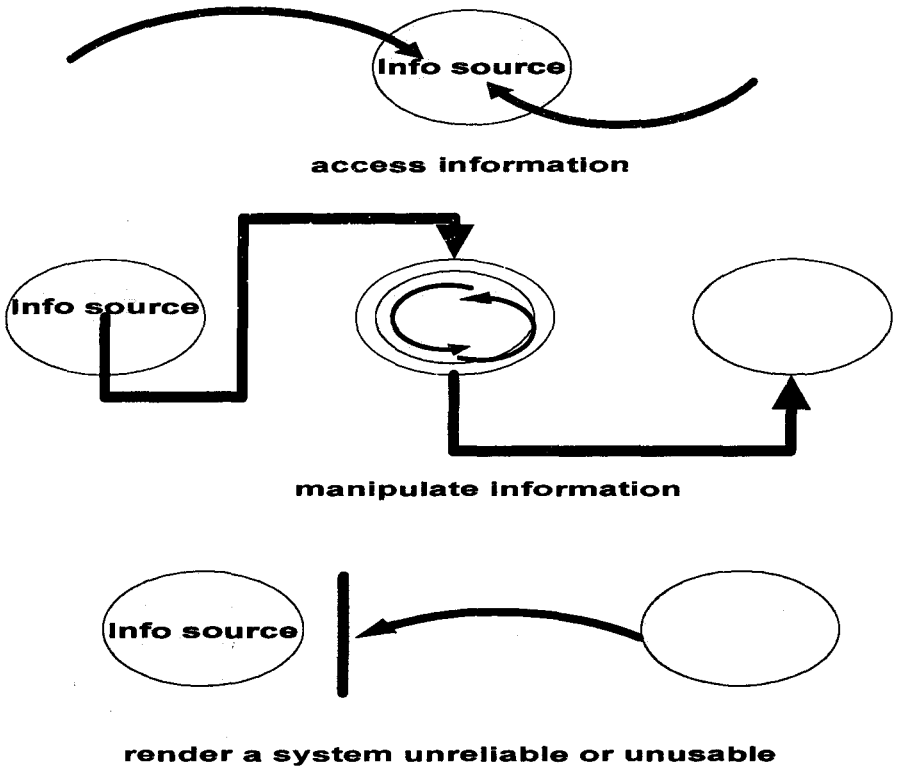

Fig. 2.2: Example of Intrusion Attempts.

The work of Shahbaz et al. (2007) state that the most effective way to detect these intrusions is through accurate identification of an attacker. More awareness of attacker characterizations will help to detect abnormal activities and intrusion attempts. Thus, the detection mechanism should be more concerned on the properties of the intrusion. We believe the best way to make good generalization accuracy is by determining the intrusion characteristics. The identification of attack features is an important step toward making a detector performs efficiently. However, even if this is an important step in the right direction, it is still necessary to manage alerts for the correct intrusion detection.

2.2.2 The Base-Rate Fallacy and Detection Deficiency of IDS

An IDS aims to discriminate between intrusion attempts and normal activities. In doing so, however, an IDS can introduce classification mistakes. Research performed by Paxson (2008) and Stallings (2010) showed that a potential IDS should detect a substantial percentage of intrusions and keep the false alarm rate at reasonable level. The nature of probabilities involved in the detection processes caused difficulty to get a complete rate of detection with a low rate of false alarms, this effect called base-rate fallacy which has been described by Axelsson (1999). The author stated that there is a natural trade-off between detecting all malicious events and missing anomalies.

Generally, there are many situations corresponding to the relation between the result of the detection for an analyzed event ("normal" *vs.* "intrusion") and its actual nature ("innocuous" *vs.* "malicious") as follows:

- True: The state of intrusion detection system is appropriate.
- False: The state of intrusion detection system is not appropriate.
- Positive: The system is alerting (either true or false).
- Negative: The system is not alarming (either true or false).
- True positive (TP): An alert is generated in condition that should be alarmed.
- False positive (FP): An alert is generated in condition that should not be alarmed.
- True negative (TN): An alert is not generated in condition that should not be alarmed.
- False negative (FN): An alert is not generated in condition that should be alarmed.

It is clear that low FP and FN rates, together with high TP and TN rates, will result in good efficiency values. However, which component of the trade-off is more important is a case-specific decision, and ideally, we would want to optimize both components. Furthermore, this proposed research will focus on the tradeoff between the ability to detect new attacks and the ability to generate a low rate of false alarms. In addition, we will investigate various mechanisms that suppress the false alerts and improve the coverage of detection of the IDS detector.

Below are the surveys of current solutions that tried to overcome this critical problem i.e. minimize the false alerts and increase the detection rate of IDS detector base on methods derived from computational artificial intelligence.

2.2.3 Current Solutions

In general, deploying IDS detector would result many benefits such as reducing the false alert and increasing the detection accuracy. Moreover, most of the previous surveys indicate the important of detector to assist the security necessity and needs. In 1999, Debar (1999) described IDS as a detector which processes the incoming information from the system. The information contains the knowledge of the detection technique, the status of the system, and the audit knowledge about the system activities. Figure 2.3 on the next page shows the simple architecture of intrusion detection system as described by Debar (1999). The figure shows the detector as central part of IDS which filters out unnecessary information from the audit trial and presents the probabilities of such events. These probabilities are then evaluated to make a decision that such action may consider as an intrusion.

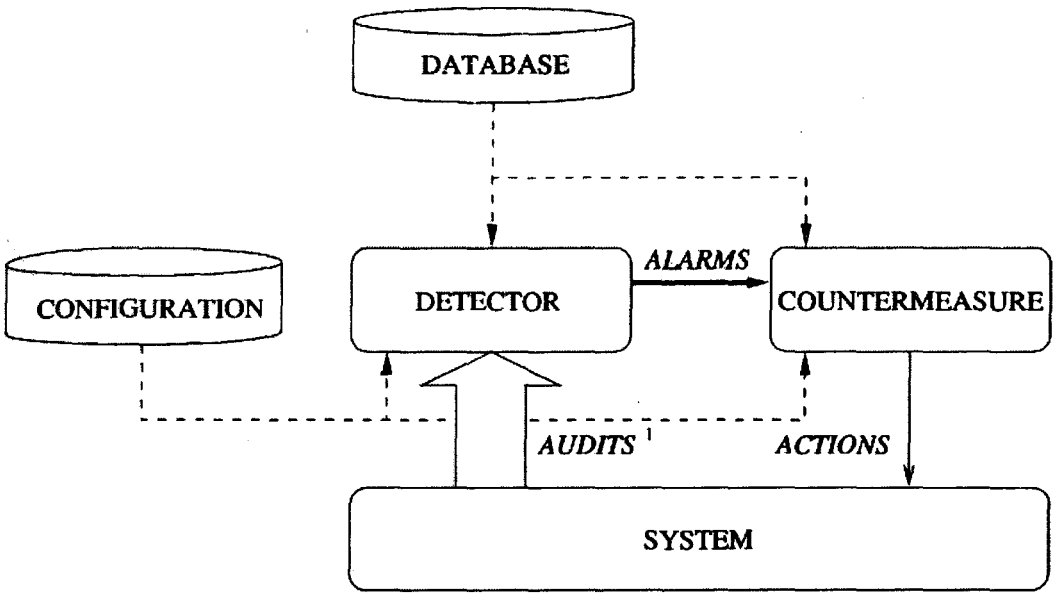

Figure 2.3: A Simple Intrusion Detection System (Debar, 1999).

Many researchers also construct a general structure of IDS and its components. For example, Sobh (2006) categorizes intrusion detection elements according to its assumptions and components. The author specified that the detector should be positioned as the heart of IDS component. Figure 2.4 on the next page indicates the location of the detector and the overall IDS components as suggested by Sobh (2006). Sobh (2006) and Debar (1999) emphasized the important of the detector in the structure of IDS. In particular, Debar (1999) focused more on the important of the detector role in synthetic view of the security-related actions taken by users whereas Sobh (2006) discussed detector activities in more details.

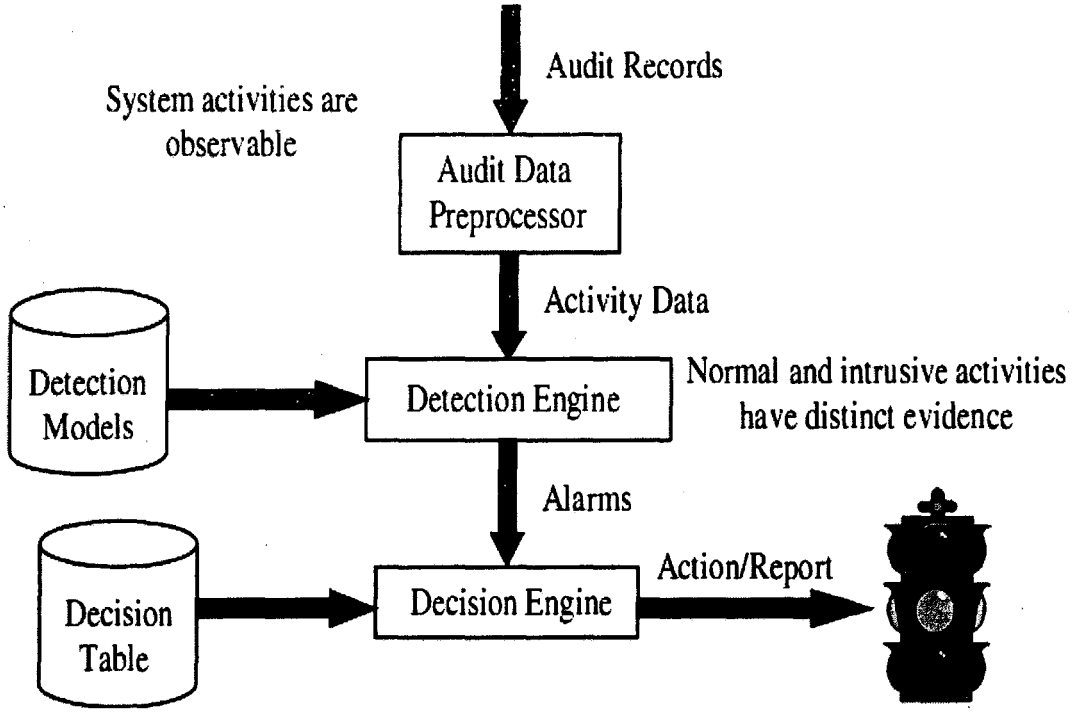

Figure 2.4: Intrusion Detection System Components (Sobh, 2006)

In general, there is diversity on the IDS roles and classification. IDS is classified into many classifications based on attributes, process, or methods. In the next section we will discuss in details the classification and taxonomy of IDS in order to have a better understanding and complete background.

2.2.4 Intrusion Detection System Taxonomy

Recent studies on IDS taxonomy have demonstrated the important of having a good taxonomy of IDS in order to specify the area and to determine the scope. However, not all taxonomies are fully agreed upon. Moreover, most of the studies are similar in

contents. One reason for that is the use of different terms but referring to the same concepts. Certain standard taxonomies are summarized in Table 2.1.

Table 2.1 presents summary of current works on IDS taxonomies and its classification based. For example, Debar (1999) developed taxonomy which classify intrusion systems according to their detection method, behaviour on detection, audit source location, or usage frequency. The taxonomy was later extended to include additional issues of IDS such as detection paradigm and vulnerability consideration as described by Debar et al., (2000).

Table 2.1: Previous Works of IDS Taxonomy

Author	**Classification Based**		
(Debar et al., 1999)	behavior-based	knowledge-based	
(Axelsson, 2000)	anomaly	signature	signature inspired
(Almgren et al., 2003)	reference model type	reference model generation process	
	reference model updating strategy		
(Sobh, 2006)	types of intruders	detection behaviors	
	detection approaches	detection techniques	
(Shelly et al., 2010)	detection method	response to intrusion	audit data source

Many researchers claim that previous studies on IDS taxonomy are not strong enough when it comes to more systematic taxonomic approach. For example, Axelsson (2000) presented a new taxonomy in terms of detection principle and

operational aspects of IDS. The author focused more on the need of effective detectors, which were divided into three groups anomaly, signature, and signature-inspired. Moreover, author reviewed in his work a number of surveyed systems and analyses these prototypes in order to develop the classification problem. The need of an effective detector is also stated by Almgren (2003). Moreover, the author attempted to form a taxonomy which concerned on the detection component of IDS. The suggested taxonomy framework by the author identifies and classifies more attacks with a wide variety of characteristics relevant for detection purposes.

Generally, IDS can also be categorized into two categories: Network-based IDS (NIDS) and Host-based IDS (HIDS). According to Filip (2002), when the intrusion detection product looks in network traffic for the patterns, it is called NIDS. Typically, NIDS processes system activities based on network data and decide whether these activities are normal or intrusion. On the other hand, IDS is called HIDS when the intrusion detection product logs the event driven on specific host. The HIDS scans resources on the hosts' machines for security related information such as file system modification logs. Figure 2.5 (a) on the next page shows the NIDS location where Figure 2.5 (b) shows the location of HIDS. The strengths of NIDS is due to its faster response and notification compared to HIDS counterpart. An intrusion may attack the low level services before HIDS can react. In addition, NIDS verifies both packet payload and headers, which provide the ability to detect the attacks that HIDS may miss. Finally, in (Filip, 2002), the author stated that one of the effective techniques to detect the intrusion is by looking at the packet header across the network using NIDS. Furthermore, the engine of NIDS is difficult to attack directly, whereas in HIDS the attacker can threat all system services, including the HIDS itself.

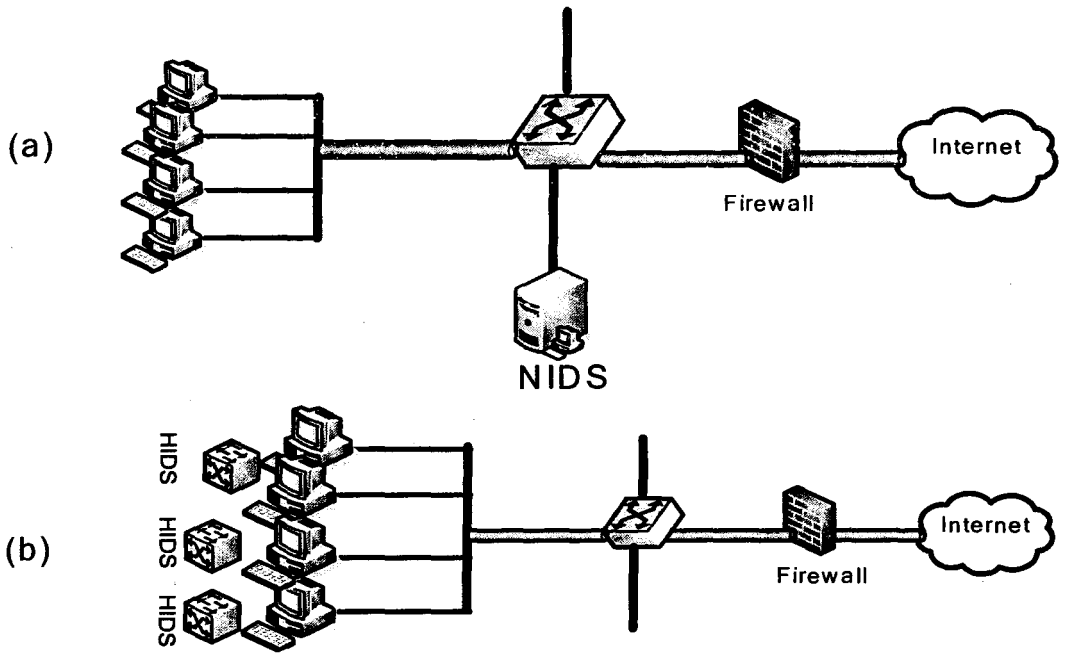

Figure 2.5: (a) NIDS Location (b) Location of HIDS

Finally, one of the popular taxonomy was proposed by Sobh (2006). This taxonomy is summarized in Figure 2.6 on the next page. The figure shows general categorization of IDS according to intruder type, detection behavior, and detection techniques suggested by Sobh (2006). It is also classifying IDS to four classifications based on the type of intruder, detection behavior, detection approach, and system types. The classification of detection approaches is divided into two approaches: anomaly detection and misuse detection. We add a hybrid detection approach to the taxonomy for more clarification. The additional hybrid detection is filled with white color as it can be seen in the figure.

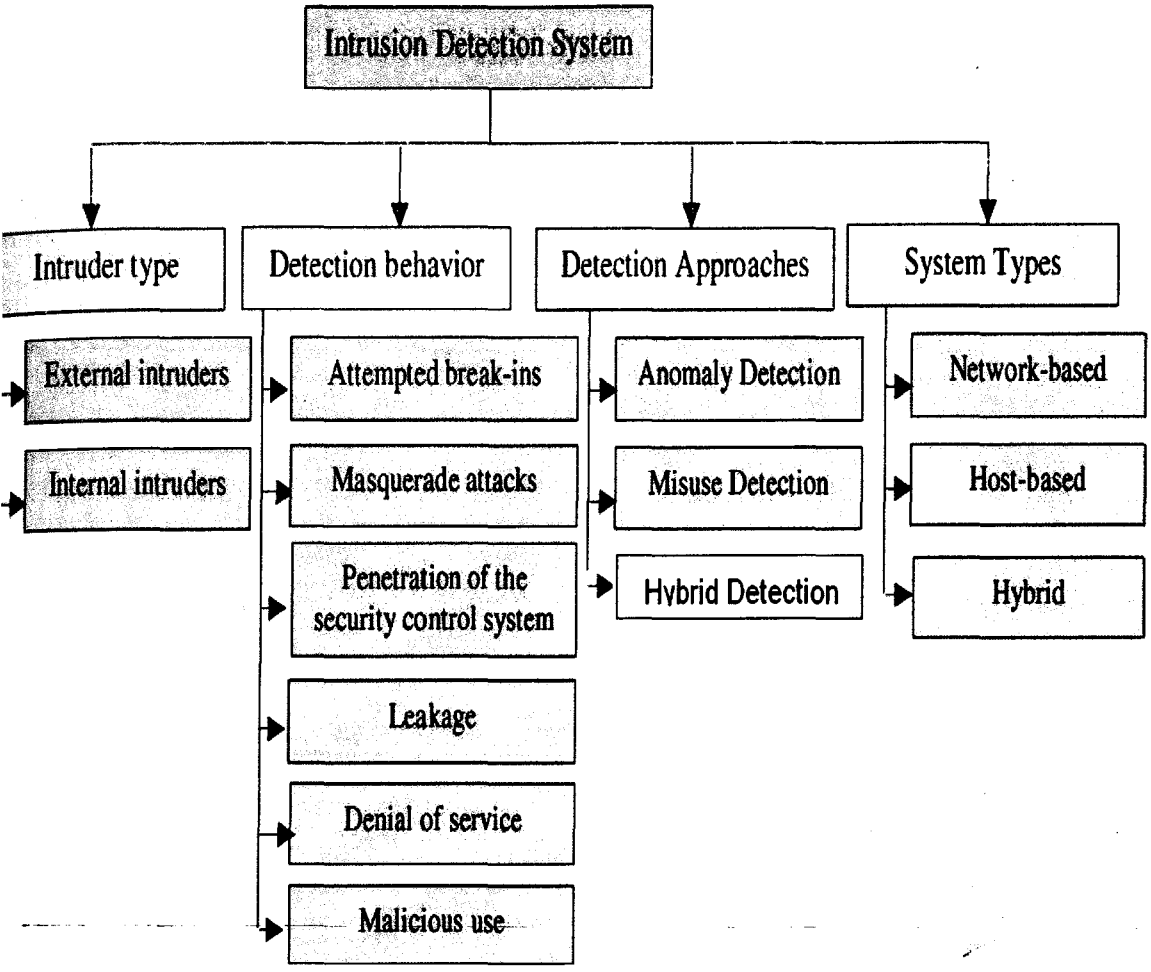

Figure 2.6: Classification of Intrusion Detection System Methods

The hybrid intrusion detection techniques consist of a misuse detection component as well as an anomaly detection component. By combining both techniques into a single hybrid system IDS will get benefits of both approaches. One of the advantages of this hybrid approach is that the chances of one approach to detect intrusions missed by the other one will increase. More discussion about each detection approach will be followed in the next section.