Preface

With the recent advances in communication and computer networks, network-based applications are rapidly growing. New Internet or network-based applications are constantly introduced and quickly accepted by the society. Internet or network-based systems are used in many areas such as communications, data transfer or sharing, equipment control or monitoring, remote control or remote presence, entertainment media and military operations.

Many business sectors are dependent on the services provided by computer networks. The financial sector shows an increasing demand for reliable and secure network-based services. The growing demand for e-banking, e-business and online trading in stock markets are some examples of this high demand.

The industrial sector is using a computer network for the distributed networking and applications where coordination between sophisticated systems is needed to run a plant or a service in a coordinated way. Here, systems operating separately and located in remote locations can be controlled to operate as one plant.

Network security has been known to be mainly about encryption/decryption for a long time. In the past decade network security has gradually but surely moved towards securing the network environment rather than the transferred data. In the past decade research interest in intrusion detection experienced a rapid growth.

The increased interest on the intrusion detection together with prevention and response proves that protecting the data either in storage or during transfer is necessary but not sufficient for the security of a network. It should be noted that encryption technologies consume a large portion of the available processing power.

With the wide spread Internet usage and the ever growing dependency of every aspect of our life on the Internet, malicious activities on the Internet have increased significantly. Security of the networks and the Internet affects the industrial and economical growth of any society and ignoring this issue will have a significant negative impact on all aspects of the society. To make the situation even worse, the privacy issue has made the use of the networks, especially the Internet something to worry about.
Introduction and the wide spread of the wireless networks in different types made the situation even worse. The concern is due to the fact that sending the information via waves through the air leaves the data with no protection. In the wired network, communication environment is a closed environment where the service provider is responsible for its protection. However, in the wireless environment the service provider has no responsibility in this regard. Problem with wireless communication security can be even tougher than the wired network.

The introduction of the wireless network and free Wi-Fi or wireless Internet access zones in some cities may ease hit and run scenarios for the attackers such as Wardriving and may become a source for new problems. Therefore, wireless network security is one of the greatest concerns.

Privacy of the network users is also an important concern. Many researchers have focused their research on improving privacy on the Net. Nevertheless, this issue is still unsolved and data collection from the network users and in particular Internet users is an ongoing problem.

Threats on data and privacy in computer networks force network security officers to look for prevention and response methods. Response can be found in two forms; one in cyberspace and the other in the form of legal responses. Both aspects are research areas where researchers are looking for ways to make a malicious act difficult to do or to make it lose its attractiveness by the legal consequences that it may bring. Here it would be nice to mention that the legal system in many countries still suffer from the lack of clear laws and legal procedures for cyber crime.

Some technologies are driven by the need for them even though the scientific society does not show enough interest in them. Honey pots are one example of these technologies. One guess is that, since this area has no theoretical concept and justification for publication can be difficult, researchers might not find it interesting enough to invest in.

Honey pots use deception techniques and they are merely a deception, tracking and data collection system. Nevertheless, in the past few years the number of papers published in this area has increased. Honey pots have proven to be effective and implemented technologies in them are getting more and more sophisticated. Intruders are concerned and anti-honey pot technology is gaining momentum as well.

Viruses and worms are also a serious concern for the people responsible for the security of the networks. Execution of these codes can disrupt the operation of the targeted systems and is the first step to gain control over a computer or a network.

Nowadays, Botnets are attracting much attention, and recruiting Bots and gaining access to other computers can be a valuable asset. Selling the collected information, processing power, and the power to coordinate DDoS attacks can be worth millions of dollars.
Finally, it would feel nice to work in a cyberspace where user feels safe and protected instead of being secured by different types of safes and locks e.g. Encryption/Decryption technologies. To reach there, researchers are working hard finding new ways to detect the malicious acts over the Internet and computer networks, but so are the hackers. Only the future will prove which one will be winner. For the time being, no real end can be imagined for this conflict.

The audience for this book will include but not be limited to scholars and industry experts. Network administrators and security officers may also find the book interesting. The intention was to select chapter reporting research in the area of interest of the audience of the book.

Selected chapters mainly present works reporting experimental results as proof for the effectiveness of the proposed method of approach. There is one chapter explaining the data collection method for intrusion detection where it presents a survey on the methods applied in this area.

Chapters are sorted in such a way that they address data collection methods for intrusion detection followed by several reported works in the area of intrusion detection. One of the major problems in intrusion detection is the size of the problem and the time constraint for it. The Intrusion Detection System (IDS) should be designed in such a way that the calculations needed for detection of the intrusion attempts can be performed in a timely manner.

If IDS cannot meet the time constraints set by the bandwidth of the network it is operating on, its operation in real time will not be possible. Once the network traffic is not processed fast enough, the IDS will have two options, one is to slow down the traffic and two is to start sampling the traffic (packet dropping), neither one is desired. Improving the efficiency of the calculations for the IDS monitored network parameters should be selected carefully and implemented methods should be optimized. Large number of parameters may improve the accuracy of the detection and reduce the detection speed. There should be a balance between the accuracy required and the computation cost for the detection. Using feature selection methods makes it possible to reach to such a balance. This issue is addressed in the second part of the book where curse of dimensionality is a major concern.

Chapters in the first section are as follows:

**Chapter 1** talks about data collection methods for intrusion detection and provides detailed explanations about data collection mechanism components. It provides useful hints and guidelines for mechanism selection and deployment.

**Chapter 2** uses an auto-reclosing technique applied on long rural power lines together with multi-resolution techniques to develop an IDS that helps to keep IPS up to date. The proposed method can block SYN-flood attacks, distributed denial of service attacks (DDoS) based on SYN-flood attacks, and helps to improve the limitations of existing IDSs and IPSs.
Chapter 3 introduces a peer-to-peer based intrusion detection system called Komondor and it is based on the Kademlia system. The proposed system is composed of independent software instances running on different hosts organized into a peer-to-peer network. The goal of the chapter is to explain modifications and enhancements made on the Kademlia.

Chapter 4 reports a work where entropy-based behavioral traffic profiles are used for anomaly-based intrusion detection. The proposed method is based on the Method of Remaining Elements (MRE) as its core.

Chapter 5 targets one of the important security concerns in the world, i.e. Botnets. It reports an analysis of botnets detecting intrusion attempts more effectively and without relying on any specific protocol, characteristics of bots such as synchronism and network load within specific time windows are analyzed.

Chapter 6 aims on the NGN and addresses the security issue in SIP protocol. The main security concern in the reported work is the DoS attack on SIP. It proposes a combination of the specification- and anomaly-based intrusion detection techniques to detect the attack.

The main concern in the chapters in the second section is to improve the performance of the detection by increasing its speed while keeping its accuracy around the same value.

Chapter 7 presents a work where the Principal Component Analysis (PCA) is applied on the DARPA’99 dataset for feature selection and to reduce the dimensionality of the sampled dataset. Here, the intension is to increase the speed of the detection process by reducing the complexity and dimensionality of the problem without significant decrease in the detection accuracy.

Chapter 8 reports a case study of anomaly detection in large and high-dimensional network connection data streams using Stream Projected Outlier deTector (SPOT) to detect anomalies from data streams using subspace analysis. The dataset used in this work is the 1999 KDD CUP dataset.

Chapter 9 reports a work where Weighted PCA (WPCA) is applied on the DARPA99 dataset for feature extraction. A difference is reported in the accuracy of the result when the number of features is limited, the number of classes is large, and population of classes is unbalanced.

Peyman Kabiri
Iran University of Science and Technology, Iran