Chapter XLVIII
Modeling Intrusion Detection with Self Similar Traffic in Enterprise Networks

Cajetan M. Akujuobi
Prairie View A&M University, USA

Nana K. Ampah
Prairie View A&M University, USA

ABSTRACT

Most of the existing networks (e.g., telecommunications, industrial control, enterprise networks etc.) have been globally connected to open computer networks (Internet) in order to decentralize planning, management and controls in business. Most of these networks were originally designed without security considerations, thereby making them vulnerable to cyber attacks. This has given rise to the need for efficient and scalable intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) to secure existing networks. Existing IDSs and IPSs have five major limitations, which prevent them from securing networks absolutely. It has been proven that the right combination of security techniques always protects networks better. This approach used change in Hurst parameter and a signal processing application of wavelets (i.e., multi-resolution technique) to develop an IDS. The novelty of our proposed IDS technique presented in this chapter lies in its efficiency and ability to eliminate most of the limitations of existing IDSs and IPSs, thereby ensuring high level network protection.

INTRODUCTION

Telecommunications networks form the major part or the foundation of all business enterprise networks, which may include a combination of local area networks (LANs), metropolitan area networks (MANs), wide area networks (WANs), and remote LAN access connectivity. Business enterprise networks are the main targets for hackers due to the fact that most financial transactions

(i.e., E-commence) take place online and the networks also handle vast amounts of data and other resources (Satti & Garner, 2001). Handling transactions online is on the increase everyday because it makes life easier for both the customers as well as the enterprises offering services (Tront & Marchany, 2004). Business enterprise networks also have lots of bandwidth, which is very attractive to hackers because they take advantage of that by using those networks as launching pads to attack others (Tront & Marchany, 2004; Janakiraman, et. al., 2003). It therefore becomes very difficult for the IDSs and IPSs at the receiving end to detect and prevent hackers, since the packet header information will indicate legitimate senders. This is the main reason why most IPSs are easily bypassed by hackers (Tront & Marchany, 2004). Intrusion prevention, which is a proactive technique, prevents attacks from entering the network. Unfortunately, some of the attacks still bypass the IPSs. Intrusion detection, on the other hand, detects attacks only after they have entered the network.

The increasing use of Internet for various economic activities coupled with the complex and dynamic nature of network security management has given rise to numerous attacks on the network itself as well as any other networks connected to it. There is also a rapid increase in the daily use of data networks for research and development collaborations with respect to rapidly changing technologies. Securing information on data networks has therefore become a very difficult task considering the diverse types and number of intrusions being recorded daily. The situation has necessitated drastic research work in the area of network security, especially in the development of IDSs and IPSs intended to detect and prevent all possible attacks on a given network. The development of IDSs and IPSs has therefore acquired increasing commercial importance (Janakiraman, et. al., 2003; Akujuobi & Ampah, 2007; Akujuobi, et. al., 2007). Although attacks are generally assumed to emanate from outside a given network, the most dangerous attacks actually emanate from the network itself. Those are really difficult to detect, since most users of the network are assumed to be trusted people. There is no existing security technique that guarantees total security for a given network, so the best approach frequently used is to implement several layers of techniques.

As a second line of defense, a combination of IDS techniques is required to back-up the existing IPSs. This has been a difficult task for network administrators mainly due to the availability of different types of IDSs on the market. These IDSs use either anomaly-based or signature-based detection techniques. Anomaly detection techniques detect both known and unknown attacks, but signature-based detection techniques detect only known attacks. The main approaches of anomaly detection techniques are statistical, predictive pattern generation, neural networks, and sequence matching and learning. The main approaches of signature-based detection techniques are expert systems, keystroke monitoring, model-based, state transition analysis, and pattern matching (Biermann, et. al., 2001). This chapter also investigates the negative effects of designing, planning and managing telecommunication networks, industrial control networks, and business enterprise networks with special emphases on issues like effectiveness, efficiency and reliability without considering proper security planning, management and constraints.

These networks have become vulnerable due to their recent connectivity to open networks with the intention of establishing decentralized management and remote control (Chunmei, et. al., 2004; Chi-Ho & Kwong, 2005; Amanullah, et. al., 2005). Cyber attacks on control systems for power, water, oil/gas, chemical, paper and agriculture businesses recorded in the past included denial of service attacks. Some confirmed cyber attacks included intentionally opening valves resulting in discharge of millions of liters of sewage, opening breaker switches, tampering with boiler control