ABSTRACT

Intrusion Detection systems are now an essential component in the overall network and data security arsenal. With the rapid advancement in the network technologies including higher bandwidths and ease of connectivity of wireless and mobile devices, the focus of intrusion detection has shifted from simple signature matching approaches to detecting attacks based on analyzing contextual information which may be specific to individual networks and applications. As a result, anomaly and hybrid intrusion detection approaches have gained significance. However, present anomaly and hybrid detection approaches suffer from three major setbacks; limited attack detection coverage, large number of false alarms and inefficiency in operation.

As computer technology evolves and the threat of computer crimes increases, the apprehension and pre-emption of such violations become more and more difficult and challenging. Most system security mechanisms are designed to prevent unauthorized access to system resources and data. To date, it appears that completely preventing breaches of security is unrealistic. Therefore, we must try to detect these intrusions as they occur so that actions may be taken to repair the damage and prevent further harm. Over the years, intrusion detection has become a major area of research in computer science and various innovative methods have been applied to these systems.

In the last five years, the information revolution has finally come of age. More than ever before, we see that the Internet has changed our lives. The possibilities and opportunities are limitless; unfortunately, so too are the risks and likelihood of malicious intrusions. Intruders can be classified into two categories: outsiders and insiders. Outsiders are intruders who approach
your system from outside of your network and who may attack your external presence (ie. deface web servers, forward spam through e-mail servers, etc.) They may also attempt to go around the firewall and attack machines on the internal network. Insiders, in contrast, are legitimate users of your internal network who misuse privileges, impersonate higher privileged users, or use proprietary information to gain access from external sources.

Another approach to intrusion detection is called anomaly detection. Anomaly based systems basically attempt to map events to the point where they “learn” what is normal and then detect an anomaly that might indicate an intrusion. Anomaly detection techniques assume that all intrusive activities are necessarily anomalous. This means that if we could establish a normal activity profile for a system, we could, in theory, flag all system states that vary from the established profile by statistically significant amounts as intrusion attempts. The main issues in anomaly detection systems thus becomes the selection of threshold levels so that the system does not flag anomalous activities that are non-intrusive nor fail to flag intrusive activities that are not anomalous. Anomaly detection systems are computationally expensive because of the overhead of keeping track of, and possibly updating, several system profile metrics.

In this thesis, we address these three issues by introducing efficient intrusion detection frameworks and models which are effective in detecting a wide variety of attacks and which result in very few false alarms. Additionally, using our approach, attacks can not only be accurately detected but can also be identified which helps to initiate effective intrusion response mechanisms in real-time. Experimental results performed on the benchmark KDD 1999 data set and two additional data sets collected locally confirm that layered conditional random fields are particularly well suited to detect attacks
at the network level and user session modeling using conditional random fields can effectively detect attacks at the application level.

In this research, a new PSO based intrusion detection system is developed for reliable and efficient IDS that will timely and accurately detect intrusions is challenging. Based on results we find that the PSO is converging very fast. Since time is a significant factor in a real-time process and the fitness function is guided by a set of rules, fast convergence is affordable and desirable in our case. The results show that the proposed PSO based system has found a good solution and can therefore efficiently work as an excellent filter to detect attacks.

Additionally, another IDS are for security systems that can identify attempted or ongoing attacks on a computer system or network. In this chapter a new differential evolution algorithm based intrusion detection system is developed for reliable and efficient IDS that will timely and accurately detect intrusions is challenging. Based on results we find that the differential evolution algorithm is converging very fast. Since time is a significant factor in a real-time process and the fitness function is guided by a set of rules, fast convergence is affordable and desirable in our case. The results show that the proposed PSO based system has found a good solution and can therefore efficiently work as an excellent filter to detect attacks.

Using our user session modeling approach based on conditional random fields also results in early attack detection. This is desirable since intrusion response mechanisms can be initiated in real-time thereby minimizing the impact of an attack.