Chapter 18

Intrusion Detection and Prevention on Flow of Big Data Using Bacterial Foraging

Khaleel Ahmad
Maulana Azad National Urdu University, India

Gaurav Kumar
Swami Vivekananda Subharti University, India

Abdul Wahid
Maulana Azad National Urdu University, India

Mudasir M. Kirmani
Sher-e-Kashmir University of Agricultural Science and Technology of Kashmir, India

ABSTRACT

Rapid connectivity and exchange of information across the globe with extension of computer networks during the past decade has led to security threats in network communication and has become a critical concern for network management. It is necessary to retain high security measures to ensure safe and trusted communication across the network. Diverse soft-computing-based methods have been devised in the past for the perfection of intrusion detection systems on host-based and host-independent systems. This chapter discusses the flow-based anomaly detector for intrusion in network by self-learning process with characteristics of bacterial foraging approach. This approach handles the network-flow and attack on network traffic in an automated fashion. This approach works on host-independent systems and on stream of network rather than payload length where data behavior of flow in network is analyzed. This model provides a cataloging of attacks and resistance mechanism techniques to avoid intrusion.

INTRODUCTION

Today we are reliant on computer expertise in one form or the other due to increasing use of Information Technology in different sectors. However, different risk are associated with usage of technology which has given rise to need for emergence of new domain of security issues like network attacks, network flow, security alarm, Denial of Service, Trojan horse etc. Network attacks have increased along with ruthlessness over the past few years and its affect on financial and economic has led to losses. Network security is the high priority challenge for the researchers and developers in the Information Technology domain. Different intrusion detection systems have been

DOI: 10.4018/978-1-4666-6559-0.ch018
put in place by different organization and one of the reliable approach is aggregated traffic metrics is used for ensuring safety to mitigate the impact of threats. These approaches are categorizes as host-based, host independent and with usability on high speed networks. Dorothy Denning was the first person to propose an intrusion detection model in 1987 (Denning, 1987) as available in the published material.

After 1987, people operating within the field of network security however haven’t been able to get substantial results. A number of tools are available in the market like antivirus, firewall, etc. however; these tools don’t wrap all security risks as reported in 2009(Roesch, 2009). The main work of intrusion detection system (IDS) is to recognize the infringement in network and it collects different parameter of network based on traffic and collects information which is analyzed to detect any attack and generates an alert for possible attack. Many institute like Epsilon providing email marketing, Sony’s online entertainment services, professional engineering society suffered from intrusion in network and it has resulted in huge financial losses in 2011(Rashid, 2012). In March 2013, one of the largest cyber attacks which slowed down global Internet services and led to almost standstill of the global internet services. Online security organization “Kaspersky Lab” released a statement on the attacks which was evaluated at 300 Gigabits per second and confirmed as major distributed Denial of Service (DDoS) attacks (Reuters, 2013). The presence Denial of Services threat has led to huge financial and professional losses to different organization which make it necessary to have effective, efficient and secure design security infrastructure of network.

Although with the probability of occurrence of intrusion in the network being high, its detection and prevention technology has been developed and is in its infancy stage due to which it does not provide absolute defense system against the intrusion threats.

The security application enterprises are facing number of challenges in developing intelligent IDS to track behaviors of suspicions applications in order to categorize and recognize attacks by their archetypal effects without raising large number of false alarms. Therefore, intruder knowledge and attacker interest is to be devised for their identification. Attacker sophistication and intruder knowledge according to their growth in the past year has been increasing with the time is shown in Figure 1.

With the emergence of flow based IDS which can be instrumental in overall network security architecture resulting in an automated mechanism & protection system which works against a broad class of attacks to eliminate false alarm. This approach is seen as a primer approach in intrusion detection as it provides solution based on behavior of network rather than packet. Flows are frequently used for network monitoring, permitting to acquire a real time impression of the traffic status. Intrusion detection concern about the dynamic collection, examination of data set and this is extracted and corresponding data logs are generated. These are mainly defined by signature-based intrusion detection (Ilgun, Kemmerer & Porras, 1995), (Lindqvist & Porras, 1999), the composed data set is verified against recognized attack, characteristics available in database but this does not stop researchers to develop system to deal with new intrusions and known attacks.

For an anomaly detection (Javitz & Valdes, 1994), normal activities of network are tracked using different tools wherein a training process is verified against current behavior of network to detect any momentous divergence from the normal activity. A training method in anomaly-based intrusion detection determines characteristics of normal activity of network. The network is moni-