Chapter 3
Cross-Layer Based Intrusion Detection and Prevention for Network

Reema Kumari
Galgotias University, India

Kavita Sharma
National Institute of Technology Kurukshetra, India

ABSTRACT

Day by day technologies for mobile computing growing rapidly and its network security changed according to their need. The attacker always trying to learn some new techniques to break those security walls of the wireless network. To prevent our network from attacker various defense techniques are used. Firewalls and encryption are used to prevent our network from malware but it is not sufficient for protecting the networks. Many researchers implement new architecture and techniques or mechanism that protect and detect malicious node and their activity over the network that is intrusion detection system (IDS). IDS provides security wall and it provides network security as well as it has continuously monitored and taken appropriate action against the threat. In this Chapter, we are trying to explain some network attack that is resolved or detect through intrusion detection system by exploiting the technology or information that available across different layers of the protocol stack in order to improve the accuracy of detection.

BACKGROUND

The meaning of intrusion is "…any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource…" (Heady et al. 1990). In the wired network, there are no vulnerabilities but when we talk about wireless network then in each step and each ways attacker is ready for attack. Firewall and encryption software is used to protect our system but it is no longer sufficient for network security. Therefore, we need to develop a new architecture and mechanism that protect our wireless network. Internet worm called Code Red that infects many Windows-based server machines in 2001. To prevent our wireless network from this type of worm attacks, many companies trust on firewalls. It protects an

DOI: 10.4018/978-1-5225-4100-4.ch003

internal network of intranet (Zhang, Lee, & Huang, 2003). Wireless network does not have the underlying infrastructure. Its infrastructure continuously changes according to their node movement. Many hosts connect at a time and make their own topology or infrastructure. These networks create a number of vulnerable network attacks. The wireless network does not communicate directly, it communicates through the intermediate node. To detect and provide the security we need to complement traditional security mechanism with efficient intrusion detection system. Intrusion detection system (IDS) is used to prevent our network. An ID is continuously monitoring our network and warns or detect if any suspicious behavior of the network is occurring (Mishra, Nadkarni, & Patcha, 2004). Wireless sensor network is mainly composed of sensor sink and sensor nodes. The main advantage of the sensor network is self-organizing and self-healing. It mainly used in such areas where wired networks are impossible. There are various applications of wireless sensor networks, which is detecting changed the climate, monitoring habitats, monitoring environment and it is used in military applications and surveillance. Nevertheless, there is one problem in WSN's, WSN nodes are always exposed their physical security attacks. To prevent such type of attacks, WSN proposed various security mechanisms such as key exchange, authentication, and secure routing. However, these security mechanisms are not capable to ensure security at all level, if not eliminate all security attacks. One possible solution having to address a wide range of security attacks in WSNs that is Intrusion Detection System (IDS) (Ananthakumar, Ganediwal, & Kunte, 2015).

INTRODUCTION

Cross layer-based intrusion, detection system utilizes information across the layers; it effectively identifies intrusion over the network. Before detecting malicious node on the network, first, it performs multi-level detection on multiple layers. The main objective of adopting cross-layer design is, 1) Detecting attack at multi-level of the protocol layer; 2) Exploiting information so that energy and congestion; and 3) It detects intrusion more accurately on multiple layers.

1. **Detecting Intrusion:** It detects intrusion on two levels that is level-1 detection and level-2 detection. The two levels are using two methods i.e.
    a. **CIDS-1:** Information is obtained through detecting DoS attacks at one layer and it is shared on another layer.
    b. **CIDS-2:** In this attack, multiple detections of a DoS is detected on the same layer.
2. **CIDS (Cross-Layer Based Intrusion Detection)-1:** It is level-1 detection method. It detects malicious node from different layers. In addition, level 2 detects truly malicious nodes in the network.
3. **CIDS (Cross-Layer Based Intrusion Detection)-2:** It is the second method for detection; 2-level detection occurs at the same layer. It is similar to the first method. In level-1 detection, only passive monitoring is done but in level-2 detection, detection is applied on the same layer (Thamilarasu, Balasumbramanian, Mishra, & Sridhar, 2005).

Cross-layer-based prevention technique is used for securing multi-path routing (CLDASR). This approach is used for dropping the malicious packet and enhances the performance of authentication and prevention. In authentication method, when any source wants to send data packets, then it generates a hash value to encrypt data or packet with destination private key. If intermediate node receive packet