Abstract

An Intrusion Detection System (IDS) is a software or hardware tool used to detect unauthorized access of a computer system or network. A wireless IDS performs this task exclusively for the wireless network. These systems monitor traffic on your network looking for and logging threats and alerting personnel to respond. An IDS usually performs this task in two ways, with either signature-based or anomaly based detection. Almost every IDS today is at least in part signature-based. This means that known attacks can be detected by looking for these signatures. The other approach is anomaly-based systems. These are not often implemented, mostly because of the high amount of false alarms. It detects traffic which deviates from what it considers normal an alert is generated. The traditional IDS system is not work well for wireless network, but the wireless network is more vulnerable than a wired network. A major problem with current IDS that employs Bayesian network is they give a series of false alarms in system environment modification. There are two types of false alarms in determining the any deviations from normal pattern: false positive and false negative. The main goal is to keep these alarms as low as possible. So a BN is used to build automatic intrusion detection system based on signature recognition. The goal is to recognize signatures of known attacks, match the
Intrusion Detection System using Bayesian Approach for Wireless Network

observed behavior with those known signatures, and signal intrusion when there is a match. IDS must be able to adapt to these changes. The goal is to provide a framework for an adaptive intrusion detection system that uses Bayesian network

References


Index Terms

Computer Science Wireless
Keywords
Intrusion Detection System  Bayesian Network  Directed Acyclic Graph  K2