Modeling Malicious Network Packets with Generative Probabilistic Graphical Models

Ashe Magalhaes, Gene Lewis

Motivation

A **cyber enterprise** is an elaborate web of applications, software, storage, and networking hardware that can see up to a megabit of network traffic per second. The problem of detecting malicious network packets in such a system can be addressed by modeling a controller of the host and Intrusion Detection System as a Markov Decision Process. To boost the resiliency of this **MDP controller**, we explore generative probabilistic graphical models of network packets to better characterize **attack types**.

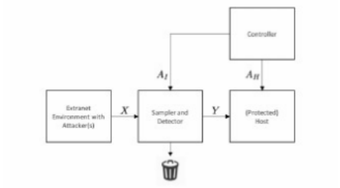
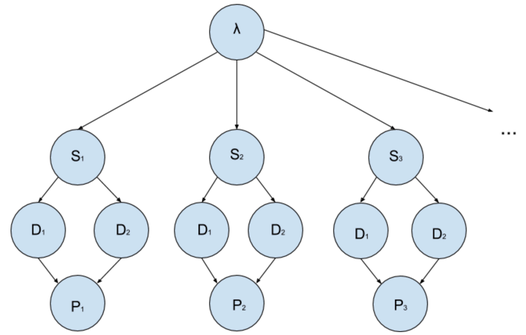


Fig. 1. Example of MDP Controller. Controller has actions A_I and A_H. Action A_I encodes the action space of the IDS (i.e. whether to pass or drop a packet). Action A_H encodes the action space of the host (i.e. whether to wait for a packet or reset).

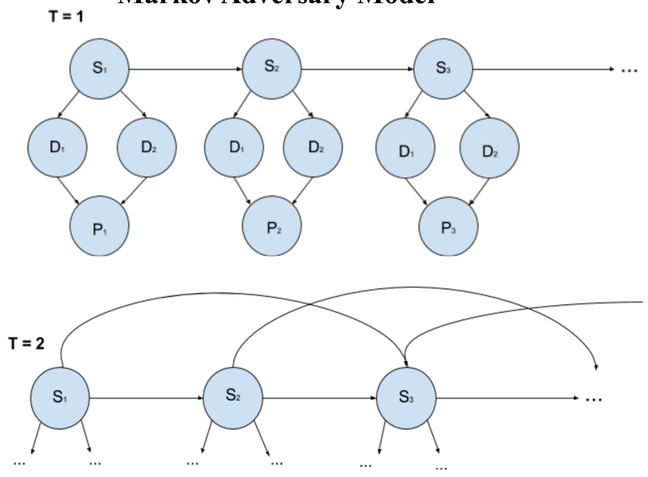
Generative Adversary Models

Naïve Bayes Adversary Model

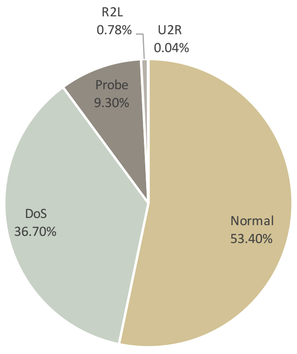


S_i – adversary state
D_j – packet generation network
P_i – generated packet

Markov Adversary Model



NSL-KDD Dataset



Total Examples: 120,000

Each packet is annotated with **40 distinct features**, ranging from duration of connection to protocol type to total number of failed logins.

DoS attack: denial-of-service; attempt to make a machine or network resource unavailable to its intended users

Probe attack: attack in which the hacker scans a machine or a networking device in order to determine vulnerabilities

R2L attack: remote-to-user; user sends packets to a machine over the internet, which s/he does not have access to in order to expose the machines vulnerabilities

U2R attack: user-to-root; hacker starts off on the system with a normal user account and attempts to abuse vulnerabilities in the system in order to gain super user privileges

Experimental Results