Abstract

Sherif Fahmy

A hybrid entropy-based DoS attacks detection system for software defined networks (SDN): a proposed trust mechanism

Software defined networks are an emerging category of networks in which the data plane and control plane are separated. This separation of planes opens the door for designing sophisticated routing algorithms that would overwhelm the computing power of traditional networking nodes. In this paper, we consider the possibility of introducing node trust into the routing problem. There are many ways for measuring node trust. However, in this paper, we focus on denial of service attacks. We develop a hybrid method for detecting denial of service attacks and incorporate this information in routing decisions so that nodes that are part of a botnet can be quickly identified and excluded from the network. The proposed method is flexible enough to allow nodes that have been suspected of participating in a denial of service attack to be “rehabilitated” if they cease their malicious behavior. The technique is also able to detect the start of a second attack while another one is on-going. Our results indicate that the proposed method for detecting denial of service attacks performs better than non-hybrid techniques.