Abstract

In computer and network security, standard approaches to intrusion detection and response attempt to detect and prevent individual attacks. However, it is not the attack but rather the attacker against which our networks must be defended. To do this, the information that is being provided by intrusion detection systems (IDS) must be gathered and then divided into its component parts such that the activity of individual attackers is made clear. Our approach to this involves the application of Bayesian methods to data being gathered from distributed IDS. With this we hope to improve the capabilities for early detection of distributed attacks against infrastructure and the detection of the preliminary phases of distributed denial of service (DDOS) attacks.

Keyword : Bayesian, IDS,DDOS