Cluster based Statistical Anomaly Intrusion Detection for Varied Attack Intensities

International Journal of Computer Applications
© 2011 by IJCA Journal

Number 1 - Article 1

Year of Publication: 2011

Authors:

M. Thangavel
Dr. P. Thangaraj

Abstract

In today's Internet paradigm, the type of intrusion attacks becomes crucial in presenting effective improvement to anomaly intrusion attacks. Anomaly Traffic hacker attacks combined with traditional network intruders was a serious threat to network security. The existing work on intrusion detection and prevention of traffic attacks take much time, before which the intruder is spread across the network. The sensing mechanism in addition to rejection of an attack against
intruders and keeps no record of the cause of the attack and its effects. In same time the actual happening of the attack detection method was left over unnoticing. This motivates to develop an effective attack mechanism of the cluster based anomaly intrusion detection.

Reference

- F. Autrel and F. Cuppens, “Using an intrusion detection alert similarity operator to aggregate and fuse alerts,” in 4th Conference on Security and Network Architectures, Batz sur
Cluster based Statistical Anomaly Intrusion Detection for Varied Attack Intensities

Mer, France, 2005, pp. 312–322.

Index Terms

Computer Science
Security

Key words

Network Traffic
Anomaly Intrusion Detection
Traffic Statistics
Cluster Data Streams