Abstract

Intrusion-detection systems (IDS) which were essential in computer security because of difficulties in ensuring the information systems are security free. Literature has numerous intrusion detection approaches for network security. IDS efficiency was based on the ability to differentiate between normal and harmful activity. Hence, it becomes crucial to achieve better detection rates and lower false alarm rates in IDS. Automated/adaptive detection systems
should secure the system handling present and possible threats in the future. Features extracted from network traffic by the IDS, classify the record/connection as either an attack or normal traffic. So, feature selection has a major role in IDS performance. This paper adopts a feature selection using the Fisher Score. Artificial Immune Systems (AIS) based IDS to detect and defend against harmful, unknown invaders is proposed. Evaluation of security detection mechanisms is done through the KDD-cup dataset.

References

Index Terms

- Computer Science
- Security

Keywords

- Intrusion Detection System (ids)
- Kdd Cup 99 Dataset
- Fisher Score For Feature Selection
- Artificial Immune Systems (ais)