Geometric Structure Based Feature Transformation for Network Anomaly Detection System

Publisher: IEEE

A.S Aneetha **All Authors**

Abstract:
Due to development of new internet connected devices, the attack surface has also been increased for the cyber intruders. The evolution of theses cyber intruders poses a ... **View more**

Metadata

Abstract:
Due to development of new internet connected devices, the attack surface has also been increased for the cyber intruders. The evolution of theses cyber intruders poses a critical challenge for designing of detection mechanisms especially in network devices. Intrusion detection system is one such approach with the ability of detecting dynamic and unknown attacks. In this work, network anomaly detection system is developed using Mahalanobis distance-based detection mechanism with heron's triangle area based transformed features. The KDD Cup'99 network dataset is utilized to analysis the performance of the system. It contains four different attack types such as DoS, Probe, R2L and U2R. The model has achieved very high detection rate for Normal and U2R classes with false alarm rates of 1.53% and 6.66% respectively. The detection rates are more than 99.53%, 99.7% and 98% for Probe, DoS and R2L classes along with 0.09%, 0.66% and 0.2% false alarm rates respectively.

Published in: 2023 12th International Conference on Advanced Computing (ICoAC)

Date of Conference: 17-19 August 2023 **DOI:** 10.1109/ICoAC59537.2023.10249601

Date Added to IEEE *Xplore*: 19 September 2023 **Publisher:** IEEE

ISBN Information: **Conference Location:** Chennai, India

Contents

In recent years due to pandemic situation, there is an exponential growth of computer devices and a network technology, made the network security has become most significant in cyber systems. Many network intrusion detection systems are available to detect the attacks of known signatures, whereas there is a great challenge in detecting new born or zero-day attacks. Development of efficient Intrusion Detection Systems (IDS) to provide real time dynamic security for all internet connect devices and network technologies assumes greater importance [1]. An intrusion detection system consists of relevant security features capable of adapting themselves for the changing environment based on their learning ability of events from time to time. IDS is categorized into signature and anomaly detection, where signature has the ability of detecting known intrusion patterns whereas anomaly is capable of detection zero-day attacks [2].