False Alarm Rate Reduction using Hybrid Model in Network Anomaly Detection

Network based intrusion causes predominantly to reveal network and service vulnerabilities. And that is why network based intrusion detection system execute thoroughly packet inspection. For faster execution with better detection accuracy, of the overall procedure while facing new dataset, we are representing a hybrid intrusion detection system in this paper. The hybridized algorithms are Triangle Inequality based k-means clustering algorithm and k-nearest neighbor classifier. Basically a combination of clustering and classification algorithms is studied in this paper. The dataset we used is the refined version of KDD’99 dataset and it is NSL KDD dataset. Some ingrained problems are solved in NSL KDD dataset. This paper work mainly focuses on the reduction of the false alarm rate. But the system is capable of detecting U2R, R2L, probe and Dos with high accuracy.

References

Index Terms

Computer Science Security

Keywords

Hybrid intrusion detection system, data mining, Triangle Inequality based k-means, k nearest neighbor, NSL-KDD dataset, accuracy, false alarm rate.