Abstract

In the current age Intrusion detection is an interest in and challenging area. As there are now a few exploration works are as of now done and the outcome change is in advancement. In this paper a hybrid approach has been proposed which is based on association rule mining and Selective Iteration based Particle Swarm Optimization (SIPSO). The NSL-KDD dataset is used. First normal and attack nodes are separated. Then normal node is checked for suspicious behavior. Then association rule mining is applied to form the associated for the next preprocessing. Then we apply SIPSO to check the threshold value obtained for the different intrusion types. If it is passed the threshold velocity assigned, then it will be categorized as the specific attack. We have considered a Denial of Service (DoS), User to Root (U2R), Remote to User (R2L) and Probing (Probe) attacks in this research work. The results show the improvement in detection as compared to the previous method.
Selective Iteration based Particle Swarm Optimization (SIPSO) for Intrusion Detection System


16. Li Han, "Using a Dynamic K-means Algorithm to Detect Anomaly Activities", Seventh International Conference on Computational Intelligence and Security, 2011.

17. Z. Muda, W. Yassin, M.N. Sulaiman, N.I. Udzir, "Intrusion Detection based on K-Means Clustering and Naïve Bayes Classification", 7th International Conference on IT in Asia (CITA), 2011.


24. Description of Kyoto University Benchmark Data
http://www.takakura.com/Kyoto_data/BenchmarkData-Description-v3.pdf

Index Terms

Computer Science
Security

Keywords

Association rule mining, SIPSO, DoS, U2R, R2L, Probe