Intelligent Intrusion Detection in Computer Networks using Swarm Intelligence

Abstract

Swarm Intelligence is inspired by the collective behaviour of many individuals. It is coordinated using decentralized control and self-organization. The individual simplicity and their complex group behaviours can outperform the vast majority of individual members when solving problems and making decisions. During recent years, the number of attacks on networks has dramatically increased and consequently, interest in network intrusion detection has increased among the researchers. In this research paper, a software architecture is modelled and implemented which uses Ant Colony Optimization (ACO), ACO is combined with Non-Negative Matrix Factorization method for classifying a computer network behaviour as a sequence of system calls.

References

2. Tony Bradley. Introduction to intrusion detection systems (ids).
20. Tashish Thomas. Types of intrusion detection systems (ids).


Index Terms

Computer Science

Security

Keywords

Ant Colony Optimization, Meta-heuristics, Anomaly-based Intrusion Detection System, Non-Negative Matrix Factorization