Abstract

Detecting intrusions in a network is one of the major functionalities that cannot be overlooked. Even though the intrusion detection systems in networks tend to perform their best, the other side is always ahead conjuring new attacks every time. Further, detecting an attack earlier or at least as soon as the attack has occurred is the only way to counter it. Detecting it at a later point in time proves to be useless. But the current systems available are not able to live up to the needs of the real time scenario. This paper presents an Ant Colony Optimization based intrusion detection system that uses agents to perform the process of detection, storage and monitoring. The network is not considered as a whole, instead, it is divided into clusters and detection is performed on the nodes within the cluster alone. Hence the workload of the detection system is reduced considerably, providing faster results. Another added advantage is that all the agents can run in parallel, hence parallelized detection becomes possible. Experiments were carried out using multi core CPUs and many core GPUs and the comparison shows that the CPUs shows twice the increase in performance when compared to single core machines, while GPUs show thrice the increase in performance when compared to multi core CPUs.

Index Terms

Computer Science  
Security

Keywords

Intrusion detection; Parallelized ACO; Clustering; Cluster Head Selection; Agent based IDS