Intrusion detection system with data mining approach: a review

ABSTRACT

Despite of growing information technology widely, security has remained one challenging area for computers and networks. Recently many researchers have focused on intrusion detection system based on data mining techniques as an efficient strategy. The main problem in intrusion detection system is accuracy to detect new attacks therefore unsupervised methods should be applied. On the other hand, intrusion in system must be recognized in realtime, although, intrusion detection system is also helpful in off-line status for removing weaknesses of network's security. However, data mining techniques can lead us to discover hidden information from network's log data. In this survey, we try to clarify: first,the different problem definitions with regard to network intrusion detection generally; second, the specific difficulties encountered in this field of research; third, the varying assumptions, heuristics, and intuitions forming the basis of erent approaches; and how several prominent solutions tackle different problems.

Keyword: Data mining; Intrusion detection; Clustering; Classification