Abstract

Now security is considered as a major issue in networks, since the network has extended dramatically. Therefore, intrusion detection systems have attracted attention, as it has an ability to detect intrusion accesses effectively. These systems identify attacks and react by generating alerts or by blocking the unwanted data/traffic. The proposed system includes fuzzy logic with a data mining method which is a class-association rule mining method based on genetic algorithm. Due to the use of fuzzy logic, the proposed system can deal with mixed type of attributes and also avoid the sharp boundary problem. Genetic algorithm is used to extract many rules which are required for anomaly detection systems. An association-rule-mining method is used to extract a sufficient number of important rules for the user's purpose rather than to extract all the rules meeting the criteria which are useful for misuse detection. Experimental results with KDD99 Cup database from MIT Lincoln Laboratory show that the proposed method provides competitively high detection rates compared with crisp data mining.

References

- Mabu S., Chen C., Shimada K., "An Intrusion-Detection Model Based on Fuzzy
- Lee W. and Stolfo S., "Data Mining Approaches for Intrusion Detection," Computer Science Department Columbia University.
- Desheng F., Zhou S., Guo P., "Research on a Distributed Network Intrusion Detection System Based on Association Rule Mining," The 1st International Conference
Design of Intrusion Detection System using Fuzzy Class-Association Rule Mining based on Genetic Algorithm


Index Terms

Computer Science

Artificial Intelligence
Keywords
Data Mining  Intrusion Detection System (IDS)  Genetic Algorithm (GA)  Network Security  Fuzzy Logic