Abstract

Security is becoming a critical part of organizational information systems and security of a computer system or network is compromised when an intrusion takes place. In the field of computer networks security, the detection of threats or attacks is nowadays a critical problem to solve. Intrusion Detection Systems (IDS) have become a standard component in network security infrastructures and is an essential mechanism to protect computer systems from many attacks. In recent years, intrusion detection using data mining have attracted researchers more and more interests. Different researchers propose a different algorithm in different categories. Classifier construction is another research challenge to build an efficient intrusion detection system. KDDCup 1999 intrusion detection dataset plays a key role in fine tuning intrusion detection system and is most widely used by the researchers working in the field of intrusion detection. This paper presents an overview of intrusion detection, KDDCup's 99 dataset and detailed analysis of classification techniques used in intrusion detection.
Classification Techniques for Intrusion Detection – An Overview

- Chen M. S., Han J and Yu Philip S., Data Mining: An Overview from a Database Perspective, IEEE Transactions on Knowledge and Data Engineering, vol. 8, No. 6, 1996, pp. 866-883.
- Fayyad, Gregory Piatetsky-Shapiro, Padhraic Smyth, From Data Mining to Knowledge Discovery in Databases, American Association for Artificial Intelligence, 1996, pp. 37-54.
- Huy Anh Nguyen, Deokjai Choi, Application of Data Mining to Network Intrusion
- Shelly Xiaonan Wu, Wolfgang Banzhaf, The use of computational intelligence in intrusion

Index Terms

Computer Science
Artificial Intelligence

Keywords
Intrusion Detection classification KDDCup