Abstract

Intrusion detection is an emerging area of research in the computer security and networks with the growing usage of internet in everyday life. An Intrusion Detection is an important in assuring security of network and its different resources. Intrusion detection attempts to detect computer attacks by examining various data records observed in processes on the network. Recently data mining methods have gained importance in addressing network security issues, including network intrusion detection. Intrusion detection systems aim to identify attacks with a high detection rate and a low false positive. Here, we are going to propose Intrusion Detection System using data mining technique: Support Vector Machine (SVM). Support vector machine-based intrusion detection methods are increasingly being researched because it can detect novel attacks. But solving a support vector machine problem is a typical quadratic optimization problem, which is influenced by the feature dimensions and number of training samples. In this paper how the support vector machines are used for intrusion detection are described and finally proposed a solution to the intrusion detection system.
references

- V. N. Vapnik. The nature of statistical learning theory. Springer Verlag, New York. NY, 1995
- B. Schölkopf, Estimating the support of a high-dimensional distribution, Neural Computation 13 (2001) 1443–147
A Survey on SVM Classifiers for Intrusion Detection

- Hsu, C., Lin, C., “A comparison on methods for multi-class support vector machines,” Technical report, Department of Computer Science and Information Engineering, National Taiwan University, Taipei, Taiwan, (2001)

Index Terms

Computer Science
Security
Keywords
   Kernel functions  soft margins  Multi class SVM