Mining Fuzzy Associate Rules for Anomaly Detection

Xiong Ping, Zhu Tianqing, Huang Tianshu
School of Electron and Information, Wuhan University, WuHan 430079.China
Email: zhutq@126.com **Tel**.: 027-62034306

ABSTRACT

In this paper, we describe the technology of mining fuzzy associate rules. An approach is presented that the fuzzy sets of each transaction's attributes is divided and calculated as separate attributes in mining fuzzy associate rules. The process of applying the approach for anomaly detection is discussed in detail. Using experiments on network traffic analysis, the feasibility of applying the mining fuzzy associate rules in intrusion detection is validated. Finally, we establish response mechanism according to the similarity of rule sets.

Keywords: Anomaly Detection, Data Mining, Fuzzy Associate Rules.