Signature-based anomaly intrusion detection using integrated data mining classifiers

ABSTRACT

As the influence of Internet and networking technologies as communication medium advance and expand across the globe, cyber attacks also grow accordingly. Anomaly detection systems (ADSs) are employed to scrutinize information such as packet behaviours coming from various locations on network to find those intrusive activities as fast as possible with precision. Unfortunately, besides minimizing false alarms; the performance issues related to heavy computational process has become drawbacks to be resolved in this kind of detection systems. In this work, a novel Signature-Based Anomaly Detection Scheme (SADS) which could be applied to scrutinize packet headers' behaviour patterns more precisely and promptly is proposed. Integrating data mining classifiers such as Naive Bayes and Random Forest can be utilized to decrease false alarms as well as generate signatures based on detection results for future prediction and reducing processing time. Results from a number of experiments using DARPA 1999 and ISCX 2012 benchmark dataset have validated that SADS own better detection capabilities with lower processing duration as contrast to conventional anomaly-based detection method.

Keyword: Anomaly detection system; Naïve Bayes; Packet header; Random forest