Mining network data stream for intrusion detection through combining SVMs with Selective K-Medoids and StreamKM++ clustering algorithms

Every day, huge volumes of network data are continuously generated as streams, which need to be analyzed online as they arrive. Streaming data can be considered as one of the main sources of what is called big data. Mining data streams and big data have received a lot of attention over the last decade. Beside the precautionary operations used for achieving security in communication networks, intrusion detection is one of the most essential things for security infrastructures in network environments, and it is widely used in detecting, identifying and tracking the intruders. Capabilities of intrusion detection technologies have great importance with the performance of intrusion detection system (IDS). Many IDS has been designed and implemented using various techniques like data mining approches. This paper investigates the problem of existing normal data mining Techniques which is not efficient enough for mining network data stream for intrusion detection. In this paper, we introduce a new hybrid machine learning classification algorithm to classify data stream that is applied to real-time network intrusion detection. Our new approach combines supervised learning and unsupervised learning methods to take the advantages of both while avoiding their weaknesses. This paper proposes a new hybrid classification algorithm which incrementaly models a data stream. In the proposed algorithm, k-clustering approaches collaborate directly with SVMs to reduce training time and increase detection accuracy. Our algorithm is implemented in java platform and evaluated using a standard benchmark NSL-KDD data set that is new version of KDD99. The experimental results show that the proposed intrusion detection algorithm performs high predictive detection accuracy and fast running time.

Data stream mining, Active Learning, Intrusion Detection System, Hybrid Classification, LASVM, K-clustering

https://www.civilica.com/Paper-ICCEIT01-ICCEIT01_072.html
این صفحه به معنای تاییدیه نمایه سازی مقاله در پایگاه استنادی سپویلیکا می‌باشد. در هر لحظه به منظور تایید اصلاحات این گواهی می‌توانید وضعیت ثبت مقاله را از طریق لینک فوق به صورت آینه کنترل نمایید.