ABSTRACT

Intrusion is any set of event that threaten the availability, integrity, and confidentiality of network resources, such as user account, file system, system kernel, etc. To prevent this event happens, intrusion detection system (IDS), a system for observing and analyzing a computer's event is an intrusion or not , is built. One of IDS category is anomaly detection. This category detects intrusion event based on data profile. An event is detected as intrusion if it's characteristic is different from common data profile. Clustering is one way to observe data profile. There's a lot of clustering algorithm proposed for anomaly detection on IDS, one of them is CLIQUE Partitioning (CP). CP is the combination of grid-based clustering and density-based clustering technique. CP divides dataspace into subspace and searches cluster in every subspace. Testing is done to analyze system's performance based on computational time, completeness, and false alarm. CP algorithm shows good performance from completeness point of view (94.59%) and false alarm rate (2.54%). From computational time, CP shows good performance based on the amount of tuple (the escalation of the quantity of tuple is linear with the escalation of computational time), but the performance is not too good from the quantity of feature side (the escalation of the quantity of tuple is exponential with the escalation of computational time).

Keywords : *anomaly detection, IDS, CLIQUE Partitioning, subspace, cluster*