ABSTRACT

With the increase in the deployment of the network systems there is a significant increase in the intensity and complexity of the network attacks. Intrusions are the activities that violate the security policy of the system, and intrusion detection is the process to identify such intrusions. Basically three approaches exist for such detection, signature-based, classification based and anomaly based approach. Recently, Entropy-based approaches are also being employed in anomaly detection. DDoS is special kind of attack wherein the victim's system is flooded with traffic packets. In this work we study the existing intrusion detection systems developed using entropy-metrics. We use basic entropy on a flow-header feature (e.g. Source IP) to determine whether the traffic is normal or anomalous. We further study and analyze the effect of extended entropy to determine the different attack classes present in the dataset. We performed the experimental study on the CAIDA dataset.