International Journal of Scientific Research in Computer Science & Engineering
Technical Paper Vol-1, Issue-5 ISSN: 2320-7639

Online Intrusion Alert Aggregation with Generative Data Stream Modeling

Ramchandar Durgam[1]* and R.V.Krishnaiah[2]

[1]*M.Tech Dept of CSE, DRK College of Engineering and Technology, Hyderabad, A.P, India
[2]PG Coordinator, Dept. of CSE, DRK Group of Institutions, Hyderabad, A.P, India

Available online at www.isroset.org

Abstract: Security plays an important role in IT systems. Intrusion detection systems can be used to ensure security in a network. The existing IDSs (Intrusion Detection Systems) such as Firewall, Snort provide huge number of alerts as they monitor the network flows. Since the number of alerts is plenty, the network administrator might be confused to know exact problem. This will delay indecision making in the presence of any security threats. As it takes more time to understand the alerts when they are more number, the network administrator needs to spend some time to make effective decisions. In this paper, we proposed a framework which aggregates alerts and generates few Meta alerts. These Meta alerts can be understood by the network personnel quickly and take decisions immediately. A data stream version of maximum likelihood approach is used in the framework. The experimental results revealed that the framework is very useful and can be used in the real world networks.

Index Terms – IDS, Online Intrusion Detection, Probabilistic Model, Online Intrusion Detection, Alert Aggregation