Apr 8th, 11:00 AM - 12:00 PM

Unsupervised Learning to Improve Intrusion Detection

Daniel H. Garrette
Illinois Wesleyan University

Jinqiao Yu, Faculty Advisor
Illinois Wesleyan University

Oral Presentation O13.2

UNSUPERVISED LEARNING TO IMPROVE INTRUSION DETECTION

Daniel H. Garrette and Jinqiao Yu*
Computer Science Department, Illinois Wesleyan University

The purpose of an intrusion detection system is to determine when a computer or computer network is under attack. Intrusion detection systems take many forms. Anomaly detection techniques seek to determine what is "out of the ordinary" and to mark it as intrusive. Because of the huge amounts of network traffic that exist on any network, it is an extremely difficult task to label traffic as either normal or anomalous. Therefore many experts see a need for anomaly detection techniques that do not require labeled data. One approach to accomplishing this goal is to build clusters of network traffic. This works by dumping huge amounts of network traffic into a grid and letting a computer group the data. It can then be inferred that the data in larger groups constitute normal traffic and the data in smaller groups constitute anomalous traffic. It is the goal of this research project to improve the accuracy of this form of anomaly detection.