



**Illinois Wesleyan University**  
**Digital Commons @ IWU**

---

John Wesley Powell Student Research  
Conference

2006, 17th Annual JWP Conference

---

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*

Follow this and additional works at: <https://digitalcommons.iwu.edu/jwprc>

---

Garrette, Daniel H. and Yu, Faculty Advisor, Jinqiao, "Unsupervised Learning to Improve Intrusion Detection" (2006). *John Wesley Powell Student Research Conference*. 2.  
<https://digitalcommons.iwu.edu/jwprc/2006/oralpres13/2>

This Event is protected by copyright and/or related rights. It has been brought to you by Digital Commons @ IWU with permission from the rights-holder(s). You are free to use this material in any way that is permitted by the copyright and related rights legislation that applies to your use. For other uses you need to obtain permission from the rights-holder(s) directly, unless additional rights are indicated by a Creative Commons license in the record and/ or on the work itself. This material has been accepted for inclusion by faculty at Illinois Wesleyan University. For more information, please contact [digitalcommons@iwu.edu](mailto:digitalcommons@iwu.edu).

©Copyright is owned by the author of this document.

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.