Institute for Integrated and Intelligent Systems (IIIS) and
School of Information and Communication Technology (ICT)

is pleased to present the Seminar on

“Substantiating Anomalies In Wireless Networks Using Group Outlier Scores”

Elankayer Sithirasenan  BScEng (Perad’ya), MSoftEng(Griff) - IIIS/ICT
PhD Student

Time 10.00am - 11.00am
Date 24th April 2009
Venue G23 1.21 Gold Coast campus Griffith University.

Abstract: Huge amounts of network traces can be collected from today’s busy computer networks. Analyzing these traces could pave the way to detect unusual conditions and/or other anomalies. Presently, due to the lack of effective substantiating mechanisms intrusion detection systems often exhibit numerous false positives or negatives. The efficiency of a network intrusion detection system (NIDS) depends very much on detecting and effectively validating the detected anomalies. Furthermore, most NIDSs do not have proven mechanisms that will easily accommodate legitimate dynamic changes. Achieving dynamic adaptation in real time has been a long standing desire for effective intrusion detection and prevention. Real time detection of outliers is a feasible option to substantiate anomalies in large data sets, leading to effective intrusion detection and prevention. In this context we propose and investigate a novel mechanism to detect intruders and to classify security threats using group outliers. Our system monitors for timing and/or behavioural anomalies and uses outlier based techniques to substantiate the anomaly. In this paper we introduce the concept of Group Outlier Score (GOS) and its use in substantiating security threats in wireless networks. We have tested the concept on our experimental wireless networking environment. The analysis of the results reveals that with a threshold value of 1.2 for GOS our system demonstrates optimum performance.