Institute for Integrated and Intelligent Systems (IIIS) is pleased to present the SEMINAR on “Securing Wireless Mess Networks”

Steve Glass - ICT PhD student & NICTA

**Time**  10.00am - 11.00am  
**Date**  20th March 2009  
**Venue**  G23 1.21 Gold Coast campus Griffith University.

**Abstract:** Wireless Mesh Networks (WMNs) offer improved utility and lower infrastructure costs than is the case for conventional infrastructure wireless networks. As with mobile ad hoc networks (MANETs) a WMN will use a multi-hop routing strategy to extend the wireless service area across a large geographical space. The WMNs avoids the low performance and difficult management of a MANET by the presence of a high-speed back-haul network. The back-haul network uses dedicated high-bandwidth wireless routers to optimize network performance and provide gateways to the wired Internet and other wireless services. Ensuring the security of a WMN requires special care. The large service area presents many locations from which an adversary may monitor or attack the network. Multi-hop routing strategies present new threats in which an outsider can render much of the whole network inoperational. In this talk we will discuss the threats posed to the security of WMNs and the work we are undertaking to secure WMNs against attack using modified MAC layer protocols.