Proposed Title: Design and Validation of Security Protocols in Hybrid Wireless Mesh Networks 1. Introduction Wireless mesh network is a self-healing, self-organizing and self-configuring network capable of establishing and maintaining mesh connectivity in a network. It promises lower cost, lower power consumption and improved reliability. Because of its many advantages, WMNs have gained widespread use in many applications and hence have emerged as the key technology for the next generation wireless networking. Some applications of WMNs include home broadband network, enterprise networking, security surveillance systems in military, vehicle network and etc. 2. Existing Issues and Research However, there remain some open research issues that impede the wide-scale deployment of WMNs especially in the area of security: 1) WMNs are vulnerable to physical attacks which give rise to serious internal threats within the network which make the issues of authentication, integrity and confidentiality even more challenging than conventional wireless networks. 2) Some of the nodes in WMNs are characterized by low battery power and limited computational abilities. Therefore, they are not suitable for intensive computations. 3) Communication within WMNs is via multi-hop transmission and therefore intermediate nodes during relaying can modify mutable fields like the hop count, TTL, metric in the routing element before forwarding and re-broadcasting them. This poses a threat. These are some of the open issues and I would like to investigate these issues and to suggest methods or algorithms to improve the security levels of WMNs. 3. Project Objectives This project will examine the security issues involved in the deployment of WMNs and to research and develop suitable protocols to enhance the performance of routing protocol in the network. Network Simulator (NS-3) will be used to simulate the scenario of the above.