

SECURE ROUTING IN WIRELESS SENSOR NETWORKS

ECE Scholarly Paper Presentation

Srividya Shanmugham

Scholarly Paper Advisor: Dr. Jens-Peter Kaps

Graduate Advisor: Dr. Brian L. Mark

March 20, 2009, 3.00 P.M

STII, Room 230A

Department of Electrical & Computer Engineering

George Mason University

ABSTRACT

Wireless sensor networks (WSN) is an emerging area that has a wide spectrum of critical applications like battlefield surveillance, emergency disaster relief systems. Sensor devices are designed to be limited in their resources. Therefore they are simple to build, economically viable and can be deployed to closely interact with their environment. They perform in-network processing to reduce the load of raw data by aggregating useful information. These characteristics of sensor networks pose unique challenges for routing data securely over wireless communication channels. Traditional security techniques cannot be adopted easily. Security in WSNs can be properly addressed only by integrating secure data transmission into the routing process itself. In this presentation we outline different routing attacks in WSN and discuss how various sensor network routing protocols breakdown in the face of those attacks. We then list a set of attributes that would make a routing protocol more secure. Finally we study a new protocol called Secure Sensor Network Routing Protocol that was designed to be resilient to routing attacks and analyze the strength of its security.