

An Indian-Australian research partnership

Data integrity and intrusion detection in wireless sensor networks

Project number: IMURA0037

Monash University supervisors: Dr Ahmet Sekercioglu and Professor Bala Srinivasan

Monash University contact: Dr Ahmet Sekercioglu and Professor Bala Srinivasan
srini@infotech.monash.edu.au

IITB supervisors: Professor D Manjunath

IITB contact: Professor D Manjunath; Email: dmanju@ee.iitb.ac.in

The problem

Wireless sensor networks (WSNs) are emerging as cost effective solutions to many security critical applications such as remote monitoring of strategic installations covering large geographical areas, pollution control and disaster recovery. Their ability of self-organisation, built-in redundancy and operational capabilities without needing human intervention make WSNs suitable for such remote monitoring applications. But the unattended operation of WSNs and limited processing capabilities of the individual nodes make them vulnerable to a variety of security attacks, especially disruption of information flow or data corruption. For wired or wireless ad-hoc networks, there exist several automated systems for maintaining their functional integrity. Unfortunately, these strategies are not directly applicable to WSNs since ad-hoc networks are not as resource constrained as WSNs.

The project

This project aims to develop distributed algorithms for detecting anomalous activity in information flow patterns in large-scale sensor networks. These algorithms will be used as building blocks of an integrated system for intrusion detection, attack isolation and fully automated response for assuring WSN survivability and information flow continuity. Initially, the project will only focus on detecting and recovering from routing attacks. Routing is an essential component of a WSN and is critical for reliable delivery of data to monitoring stations, and is considered as the most vulnerable component of the software architecture of WSN. The initial project focus will be only for detection of anomalous activities. It involves in developing analytical models, and experimental studies at developing algorithms for detection of anomalous activities. Algorithms will be developed to build model of normal traffic behaviour, and then use this model to detect abnormal traffic patterns. It is hoped that the model is able to detect attacks patterns that have not previously been seen and also has the potential to apply to a wide range of routing protocols. The performance of the model will be evaluated by simulating routing attacks in wireless sensor networks.