Department of Mathematics, Statistics and Computer Science
St. Francis Xavier University
Presents

Key Management in Heterogeneous Wireless Sensor

by

Dr. Sajid Hussain
Jodrey School of Computer Science
Acadia University

Friday, November 28th, 2008 @ 2:15 in AX23A

We propose a key management scheme based on random key predistribution for heterogeneous wireless sensor networks (HSNs). As large-scale homogeneous networks suffer from high costs of communication, computation, and storage requirements, the HSNs are preferred because they provide better performance and security solutions for scalable applications in dynamic environments. We consider hierarchical HSN consisting of a small number high-end sensors and a large number of low-end sensors. To address storage overhead problem, we incorporate a key generation process, where instead of generating a large pool of random keys, a key pool is represented by a small number of generation keys. For a given generation key and a publicly known seed value, a keyed-hash function generates a key chain; these key chains collectively make a key pool. As dynamic network topology is native to WSNs, the proposed scheme allows dynamic addition and removal of nodes. We evaluate the computation and storage costs of two keyed-hash algorithms for key chain generation, HMAC-SHA1 and HMACMD5, using Crossbow's MicaZ motes. Further, for collusion resistance, we update the key ring after initial deployment and generate new key rings by using one-way hash function on nodes' IDs and initial key rings. The proposed key management scheme outperforms the previous random key predistribution schemes by: a) considerably reducing the storage requirement, b) providing more resiliency against node capture and collusion attacks.

Refreshments will be served before the talk in AX24A