# Department of Computer Science

## Computer Science Seminar

## Talk is Cheap: How to Efficiently Communicate When Your Network is Under Attack

## by

## Dr. Maxwell Young

Date: February 3, 9:30 a.m.  
Place: E2-304 EITC

Abstract

How can we protect large-scale decentralized systems from anonymous attackers with access to substantial computational and network resources? For example, both wireless sensor networks and peer-to-peer networks represent compelling paradigms for massive data collection, storage, and retrieval; however, from a security perspective, the absence of any reliable admission control or trusted central authority leaves these networks particularly vulnerable to malicious behaviour. In such settings, establishing performance guarantees is a challenging task requiring the design of new protocols that are resilient to a wide range of assaults on the system. In this talk, I will discuss two recent results from this area that address the fundamental problem of establishing secure and reliable communication between network participants in the presence of a powerful attacker.

The first result addresses the domain of wireless sensor networks where denial-of-service (DoS) attacks can be launched by ``jamming'' the communication medium. This is a well-documented threat that puts at risk all manner of potential applications such as those for battlefield monitoring, airport security, and disaster management. In this setting, I will discuss novel protocols that exploit the economics of energy usage in wireless sensor networks in order to mitigate DoS attacks and ultimately guarantee communication.

The second portion of my talk will focus on peer-to-peer networks. Specifically, I will address the issue of securely routing messages in a distributed hash table (DHT) when a large fraction of the peers in the network can collude and execute attacks aimed at derailing critical network operations. For example, peers controlled by an attacker may maliciously reroute or discard network traffic, corrupt stored data, or advertise false content; such actions are yet another form of DoS attack that can render the network unusable. Here, I will present routing protocols for DHTs that can tolerate such events while yielding both asymptotic and practical improvements over all previous work in terms of the required communication overhead.

This speaker is a candidate for a tenure-track position in the Department of Computer Science.