Abstract:
The notion of inflicting higher costs on an attacker has appeared in isolated instances in various areas of computer science. This talk will introduce a recent approach for designing distributed algorithms which formalizes the concept of imposing prohibitive resource costs on an attacker.

As an example, we consider a scenario where Alice wishes to transmit information to Bob over a communication channel that is vulnerable to disruption by an attacker. There is a cost for accessing the channel (sending, listening, or disrupting) and this cost is measured in terms of network resources such as computational power, bandwidth, or energy. This communication problem abstracts many types of conflict in networks.

For example, in wireless sensor networks, where both the correct and the attacking devices are battery powered, energy is a scarce resource. In this setting, we will see randomized algorithms that guarantee that either (1) communication is quickly achieved, or (2) the attacking devices rapidly deplete their energy supply in attempting to thwart Alice and Bob. In the latter case, the attackers may delay communication for a time, but they are quickly rendered bankrupt and unable to launch further attacks on the system. These results are joint work with Jared Saia (University of New Mexico), Valerie King (University of Victoria), Seth Gilbert (National University of Singapore), and Seth Pettie (University of Michigan).

Bio:
Maxwell Young earned his Ph.D. in computer science at the University of Waterloo (Canada). Before joining the Department of Computing at Drexel University, he was a Research Fellow at the National University of Singapore, and later a Postdoctoral Fellow in the Department of Electrical Engineering and Computer Science at the University of Michigan, Ann Arbor. His research interests include security and distributed computing.