NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

PH.D DEFENCE - PUBLIC SEMINAR

Title: **Securing Multi-channel Wireless Networks against Malicious Behavior**

Speaker: Mr Zheng Chaodong

Date/Time: 27 August 2015, Thursday, 10:00 AM to 11:30 AM

Venue: MR1, COM1-03-19

Supervisor : Dr Seth Gilbert, Assistant Professor, School of Computing

ABSTRACT:

Wireless networks are becoming increasingly popular over the last two decades, and there is no doubt this trend will continue. The key advantage of wireless networks is that they utilize radio waves to transmit information over the air, hence allowing related devices to communicate in a cordless manner. Nevertheless, the open and shared nature of wireless networks' communication medium also makes them more vulnerable to various malicious behavior. These malicious behavior include, but are not limited to, jamming, spoofing, and sybil attacks.

Sybil attacks refer to the situation in which malicious users dishonestly generate large numbers of fake identities, and inject them into the network to gain unfair advantage over honest users, or to conduct other hostile activity. Compared with jamming and spoofing attacks, sybil attacks relatively new, and are not so well-studied, especially in the environment of wireless networks. In this thesis, we focus on the topic of how to effectively thwart sybil attacks in multi-channel wireless networks, and at the same time tolerate other malicious behavior as well.

We first consider centralized multi-channel wireless networks, in which one central and trusted base station exists. The problem is to enforce fairness when multiple users are downloading data from the base station. In particular, without special care, malicious users can commence a sybil attack by simulating many fake identities, and hence obtain a large and unfair portion of the total bandwidth. To counter such behavior, we propose a protocol named SybilCast. SybilCast limits the number of fake identities, and in doing so, it ensures that each honest user gets at least a constant fraction of its fair share of the bandwidth. As a result, each honest user can complete his or her data download in asymptotically optimal time. A key aspect of this protocol is balancing the rate at which new identities are admitted and the maximum number of fake identities that can co-exist, while keeping the overhead low.

We then consider a more challenging scenario: ad hoc multi-channel wireless networks, where no central base stations exist. The problem in this setting is for each user to learn the identities of the other users, even though they have no prior knowledge of the number of other users or their identities. To solve this problem, several new anti-sybil algorithms are described and analyzed. They guarantee each honest user accepts a set of trusted and unforgeable identities that include all other honest users and a bounded number of fake identities. The proposed algorithms provide trade-offs between time complexity and sybil bounds. It is also worth noting that these algorithms solve, as subroutines, two problems of independent interest in this anonymous wireless setting: Byzantine consensus and network size estimation.

It is worth noting that all the above mentioned algorithms are randomized algorithms that can only guarantee correctness with high probability. Towards the end of the thesis, we study if such small chance of error is inevitable. In particular, we focus on the problem of counting and node discovery, and show that in some adversarial environments, even without sybil attacks, it is impossible to guarantee to solve these problems: chance of error may exist, or the algorithm may never terminate.