# SEMINAR NOTICE:

# Efficient Security and Privacy-Preserving Protocols for Multi-hop Wireless Networks


*Mohamed Mahmoud*

Postdoctoral fellow with the Centre for Wireless Communications at University of Waterloo (Ontario – Canada)


**TIME & LOCATION:**

**Illinois:**
**Wednesday, January 4 at 7:30 p.m.**
**Coordinated Science Lab - Room 238**
**ADSC Videoconference Room**

**Singapore:**
**Thursday, January 5 at 9:30 a.m.**
**@ ADSC - Level 8, Fusionopolis, Connexis North**


## Abstract:

In mobile ad hoc and multihop cellular networks, the mobile nodes should relay others' packets for enabling new applications and enhancing the networks' deployment and performance. However, selfish nodes do not relay others' packets because it consumes their resources without benefits and malicious nodes may drop packets to launch denial-of-service attacks, which degrade the network availability and cause multihop communications to fail. In the first part of our talk, we will give a brief overview to our works on securing mutihop wireless networks. We combine payment/trust systems and a trust-based and energy-aware routing protocol for securing the network and establishing stable routes. The payment system charges the nodes that send packets and rewards those relaying packets. Since a trusted party may not be involved in the communication sessions, the nodes compose proofs of relaying packets, called receipts, and submit them to an offline trusted party to update their credit accounts. The payment system can stimulate the selfish nodes to relay packets and enforce fairness by rewarding the nodes that relay more packets. It can also discourage message-overloading attack and regulate message transmission because the nodes pay for relaying their messages. The trust system evaluates the nodes' competence/reliability in relaying packets in terms of multi-dimentional trust values. Our trust system maintains multi-dimensional trust values for each node instead of a single trust value to better predict the node's future behavior, and thus make smarter routing decisions. The nodes that frequently drop packets, break routes, or are not active in relaying packets have low trust values and are avoided in routing. The nodes that consistently drop packets are identified as packet-dropping attackers and excluded from the network. Based on the nodes' trust values, we develop two routing protocols to direct traffic through those highly trusted nodes having sufficient energy to minimize the probability of breaking the route, and thus boosting the network performance in terms of end-to-end packet delay, packet delivery ratio, throughput, etc. By this way, the integration of trust and payment punishes the nodes that break routes or report incorrect energy capability by reducing their future earnings.


## Biosketch:

**Mohamed Elsalih Mahmoud** received PhD degree from the University of Waterloo (Ontario - Canada), Department of Electrical and Computer Engineering, in April 2011 under the supervision of Prof. Xuemin (Sherman) Shen. He is currently postdoctoral fellow with the Centre for Wireless Communications, University of Waterloo, under the supervision of Prof. Sherman (Xuemin) Shen (University of Waterloo) and Prof. Xiaodong Lin (University of Ontario Institute of Technology). He is also a member of the Broadband Communications Research Group. Dr. Mahmoud is the first author for more than twenty papers published in major IEEE conferences and journals, including IEEE INFOCOM conference and IEEE Transactions on Vehicular Technology, Mobile Computing, and Parallel and Distributed Systems. He won the prestigious Best Paper Award from IEEE International Conference on Communications (ICC'09), Dresden, Germany, 2009. The research interests of Dr. Mahmoud include wireless network security, mobile ad hoc and multihop cellular wireless networks, wireless sensor networks, delay-tolerant wireless networks, users and location privacy-preserving schemes, trust-based and energy-aware routing protocols, anonymous and secure routing protocols, cooperation incentive mechanisms, micropayment systems, trust and reputation systems, and applied cryptography.