21st CENTURY RENAISSANCE ENGINEERS
REVOLUTIONIZING ENGINEERING

TENNESSEE TECH UNIVERSITY

COLLEGE OF ENGINEERING

SEMINAR ANNOUNCEMENT

“Efficient Security and Privacy-Preserving Protocols/Schemes for Multihop Wireless Networks”

Presenter: Mohamed M. E. A. Mahmoud

Abstract

In multihop wireless networks, the mobile nodes should relay others' packets to enable many useful applications and enhance the networks deployment and performance. However, selfish nodes do not relay others’ packets because they consume the nodes’ resources without direct benefits. Moreover, malicious nodes will launch denial-of-service attacks by dropping the packets they are supposed to relay. These attacks will degrade the network availability and may cause the multihop communications to fail. In order to consider these security issues, we use payment and trust systems with a secure routing protocol. The payment system charges the nodes that send packets and rewards those relaying packets. The system can stimulate the selfish nodes to relay packets and enforce fairness. The trust system evaluates the nodes’ competence and reliability in relaying packets in terms of multi-dimensional trust values. The routing protocol can make smarter routing decisions by establishing routes through those highly trusted nodes having sufficient energy to minimize the packet dropping probability. We have also developed several approaches to ensure the security and efficiency of the payment and trust systems.

In addition, due to the broadcast nature of radio transmission and multihop packet relay, attackers can receive the communication packets and investigate them to infer sensitive information, such as the nodes’ locations and the users’ communication activities. We will briefly talk about our works in preserving users’ privacy in hybrid ad hoc network and preserving source nodes’ location privacy in sensor networks.

In the second part of the seminar, we will talk about our current and future works in securing smart power grid communication network. Smart grid integrates information technology, digital communications, sensing and control technologies into the power system to enhance the grid’s reliability and service quality. However, the security of the smart grid’s communication network is the most concern in widely deploying this new technology. Attackers will exploit any security flaw to attack the communication protocols, e.g., by injecting false information and modifying/replaying the disseminated messages which may cause the instability of the whole power grid or even result in devastating widespread blackouts. Moreover, smart meters will provide near real-time information about the consumers electricity usage. These data can be used by the attackers to invade the consumers’ privacy. For example, these data can reveal the consumers’ daily routines such as

whether they spend the week end in home and when they sleep, get up, leave to work, return from work, cook, etc. We will talk about the security and privacy violation issues in smart grid. We will also discuss why securing the smart grid communication is a challenge.

About the Speaker

Dr Mahmoud received PhD degree from the University of Waterloo, Ontario, Canada, in April 2011. From May 2011 to May 2012, he worked as a postdoctoral fellow in the Broadband Communications Research group - University of Waterloo. From August 2012 to July 2013, he worked as a visiting scholar in University of Waterloo, and a postdoctoral fellow in Ryerson University - Toronto. From August 2013 to present, Dr Mahmoud works as an assistant professor in Department Electrical and Computer Engineering, Tennessee Tech University. The research interests of Dr. Mahmoud include security and privacy preserving schemes for smart grid communication network, mobile ad hoc network, sensor network, and delay-tolerant network. Dr. Mahmoud has received MITACS-PDF award, Canadian national award. He has also received the competitive NSERC-PDF award, Canadian national award. He won the prestigious Best Paper Award from IEEE International Conference on Communications (ICC'09), Dresden, Germany, 2009. Dr. Mahmoud is the first author for more than twenty three papers published in IEEE conferences and journals, and recenty he publsihed a book in Springer Briefs in Computer Science titled "*Security for Multihop Wireless Networks*". Dr Mahmoud serves as an Associate Editor in Springer journal of peer-to-peer networking and applications, and as a technical program committee member and reviewer for several IEEE conferences and journals. For more information, you are welcome to visit his website http://iweb.tntech.edu/mmahmoud/ .

Date: December 3, 2013
Time: 12 P.M. – 1 P.M.
Bring your own lunch; beverages and snacks to be provided.
Location: Prescott 225