Announcing the Final Examination of Baber Aslam for the degree of Doctor of Philosophy

Time & Location: December 19, 2011 at 10:00 AM in HEC 356
Title: Networking and Security Solutions for VANET Initial Deployment Stage

Vehicular ad hoc network (VANET) is a special case of mobile networks, where vehicles equipped with computing/communicating devices are the mobile wireless nodes. Vehicular networks have hybrid architecture; it is a combination of both infrastructure and infrastructure-less architectures. The direct vehicle to vehicle (V2V) communication is infrastructure-less or ad hoc in nature; vehicles traveling within communication range of each other form an ad hoc network. Whereas the vehicle to infrastructure (V2I) communication has infrastructure architecture; vehicles communicate with other vehicles/wired nodes through access points (known as road side units RSUs) deployed along the road. To provide various services to vehicles, RSUs are generally connected to other RSUs and to the Internet. The success of VANET depends on existence of pervasive roadside infrastructure and sufficient number of smart vehicles. Most of the VANET applications and services are based on either one or both of these requirements. A fully matured VANET will have pervasive roadside network and enough vehicle density to enable VANET applications. But, the initial deployment stage of VANET will be characterized by lack of pervasive roadside infrastructure and low market penetration of smart vehicles.

It will be economically infeasible to initially install a pervasive and fully networked roadside infrastructure. Low market penetration will result in insufficient number of smart vehicles to enable V2V communication, thus causing failure of services and applications that depend on V2V. There will be, therefore, a need to optimally place the limited number of roadside units to provide best service to smart vehicles. Further, due to non-availability of pervasive connectivity to certification authorities and dynamic locations of each vehicle, it will be difficult and expensive to have security solutions based on some central certificate management authority.

Due to economical considerations the installation of roadside infrastructure will take a long time and will be incremental thus resulting in a heterogeneous infrastructure with non-consistent capabilities. Similarly, smart vehicles will also have varying degree of capabilities. This will result in failure of applications and services that have very strict requirements on V2I or V2V communications. Routing protocols that either depend on infrastructure or fully connected V2V network will also fail.

We have proposed several solutions to overcome the challenges that will be faced during initial deployment stage of VANET: 1) a VANET architecture that can provide services with limited number of heterogeneous roadside units and smart vehicles with varying capabilities, 2) a back-end connectivity solution that provides connectivity between Internet and smart vehicles without requiring pervasive roadside infrastructure or large number of smart vehicles, 3) a security architecture that does not depend on pervasive roadside infrastructure or a fully connected V2V network, 4) optimization solutions for placement of limited number of RSUs within a given area to provide best possible service to smart vehicles, and 5) a routing protocol that can route message without need of a pervasive and fully connected network or a large number of smart vehicles or guaranteed location/trajectory information from smart vehicles.

Major: Computer Science

Educational Career:
Bachelor's of Electrical Engineering (Telecommunication), BS, 1997, National University of Sciences and Technology, Pakistan
Master's of Computer Science, MS, 2009, University of Central Florida, USA

Committee in Charge:
Changchun Zou, Chair, EECS
Chung-Ching Wang, Statistics
Damla Turgut, EECS
Mostafa Bassiouni, EECS
Approved for distribution by Changchun Zou, Committee Chair, on November 30, 2011.

The public is welcome to attend.