

# Research Statement

Minho Shin (mhshin@cs.dartmouth.edu)

## I. OVERVIEW

My research interest is in the design, implementation, and performance evaluation of wireless networks and its security mechanisms. Wireless networks are becoming more and more dynamic in its scale, mobility, and diversity of technologies. I have focused on “studying the impact of dynamics on wireless network system and design methods for support of reliability, performance, and security.” Especially, I have been interested in building systems that achieve both security and performance and understanding trade-off between them.

My approach is to *decentralize* system functionalities to distributed entities to achieve reliability and efficiency without sacrificing security. Centralized approaches for the design of systems and security mechanisms fail to satisfy new system needs spurred by the dynamics of wireless networks. Although decentralization can effectively adapt the system to dynamic environments, the benefit of decentralization comes with price. One of my research question is what is the price of decentralization and how it trade-offs with benefit.

## II. PAST AND CURRENT

### **Impact of Mobility on Performance and Security**

In wireless networks, mobility is a major drive for network dynamics. In infrastructured networks such as Wireless LANs (WLANs) or cellular networks, *hand-off* mechanism deals with the limitation of radio coverage against user mobility. The inevitable disruption of connection challenges the performance of delay-sensitive applications such as Voice over IP. Through in-depth measurement study and analysis, I identified the major bottleneck of hand-off as the process (*i*) to discover next AP (up to 400 ms) and (*ii*) to authenticate the user for new connection (up to 800 ms). To address the bottleneck, I and my colleagues proposed *Neighbor Graphs*, a distributed data structure representing a directed graph that captures user mobility.

To expedite AP-discovery, I designed a fast AP-discovery algorithm that optimizes the set of probed channels and the waiting time for each channel [1]. Experimental study in a real WLAN network showed that proposed algorithm reduces AP-discovery latency down to 50ms. For long authentication latency, we proposed and implemented a decentralized solution, Proactive Key Distribution and Caching with neighbor graphs[2], and a centralized proactive key distribution scheme based on neighbor graphs, that works with 802.11i wireless security standard [3]. Combination of our fast AP-discovery and authentication scheme could reduce 1.2 second hand-off latency down to around 50 ms. We evaluated our scheme on a testbed of around 40 custom built APs (Soekris NET4521/OpenBSD) with precise measurements of hand-off latencies using two laptops connected for time synchronization. The proactive key distribution scheme is incorporated as recommended practice into the IEEE 802.11i and IEEE 802.11f standards.

I expanded the concept of Neighbor Graphs to Hierarchical Neighbor Graph for inter-domain hand-off problem such as hand-off between WLAN and 3G[4]. EAP-TLS for WLAN and AKA for 3G are assumed for authentication protocol. I also worked on inter-provider hand-off by policy-based dynamic roaming agreements[5].

### **Impact of Diversity on Performance and Reliability**

Abundant wireless spectrum can boost up the communication performance in multi-radio multi-hop wireless networks, such as Mobile Ad hoc Networks and Wireless Mesh Networks. Although each wireless node can have multiple radio interfaces, the number of interfaces at each node is not necessarily the same. The question is how much we can, in a decentralized way, improve network performance in terms of throughput and delay when nodes are capable of simultaneous access to different number of wireless channels. We showed that channel assignment for optimal performance is NP-hard even for simple cases. Distributed channel assignments can partition the network; when nodes independently choose their channels, neighboring nodes may not have common channels and it can lead to a network partition. I and my colleagues proposed a distributed channel assignment algorithm called SAFE (Skeleton Assisted partition FrEe) [6]. SAFE algorithm guarantees the network connectivity by keeping edges of a spanning subgraph. Packet level simulations show that SAFE significantly improves network throughput and delay comparably with the best prior centralized scheme which jointly considers routing and channel assignment. Further, we designed semi-definite programming algorithms [7], [8].

### **Impact of Scale on Reliability and Security**

Multi-hop wireless networks such as wireless mesh networks and sensor networks require efficient lookup services for reliable system operation. The lack of infrastructure, however, makes the centralized lookup fail to scale in multi-hop wireless networks. For example, in a citywide wireless mesh network, centralized authentication methods fail to scale due to a high volume of user access and inherent vulnerability of wireless links. The decentralization of user authentication, however, faces a challenge of key discovery; how to find the location of user keys. Motivated from the user authentication problem in wireless mesh networks, my dissertation work aims to provide efficient and scalable distributed lookup services for multi-hop wireless networks. A loosely-structured scheme Valley-Walk strategically places object copies and locates them efficiently only with a minimal local structure. The Valley-Walk finds target objects in near-optimal hop counts with a moderate number of copies (e.g., 10% the network size) stored in the network. Without a global structure, however, Valley-Walk fails to guarantee the low cost search with a small number of copies. A tightly-structured scheme RIGS (Ring Interval Graph Search) realizes a Distributed Hash Table (DHT) in multi-hop wireless networks. Experimental study shows the limitations of existing DHTs in multi-hop wireless networks due to its independence of underlying topology. Unlike DHT, RIGS constructs a search structure Ring Interval Graph such that queries are forwarded only to local neighbors. RIGS guarantees successful object lookup with near-optimal performance.

### **Highly Dynamic System: Vehicular Ad hoc Network**

Vehicular Ad hoc Network (VANET) is one of the most dynamic wireless network due to high mobility and constant change in network size. To date, however, no single simulation tool can comprehensively simulate a VANET-based transportation system. As a basis for further research, I built a realistic VANET simulation framework by integration of a transportation simulator (Paramics) and communications network simulator (QualNet). For simulation integrity, two simulators constantly synchronize their simulation states such as time, vehicle positions, and inter-vehicle communications. As a case study, I performed simulation experiments on a simple but intelligent traffic information system on a real road network with real traffic history. In the experiments, each vehicle with special equipment spreads their past travel time information throughout the network (by flooding) so that receiving equipped vehicles can analyze traffic situation ahead and adjust their shortest-time travel path. Results show that our simulation framework takes at most 1.5 times longer than the simulated time with high traffic loads, and it is up to 100 times shorter with

low traffic. Fast and reliable information dissemination was observed even with low market penetration of 1%. Intelligent routing with traffic information reduced travel time of VANET-capable vehicles by up to 10 % with market penetration of 5 % [9].

### III. FUTURE DIRECTION

I am interested in continuing to study the dynamics of wireless networks, especially with Sensor Networks, Wireless Mesh Networks, and Vehicular Ad hoc Networks. I envision that every network converges into one hybrid massive network which constructs an intelligent system from which people benefit for most aspect of life, if not all. I intend to research on an integrated system of wireless mesh network, vehicular ad hoc network, and sensor network, which eventually converges to a giant intelligent system.

#### **Metropolitan Wireless Mesh Networks**

Wireless Mesh Network is popular for building mobile wireless connection service in wide area such as metropolitan area. The system is going to face a number of users with different properties such as types of device, session length and frequency, security capability, and types of applications. During peak usage, thousands of users may request access to the network for short period. To maintain reliable, efficient, and secure system, we need to address many research issues: efficient but secure user authentication, adaptive radio resource allocation, seamless hand-off for moving users, and accommodation of heterogeneous user devices. I primarily intend to expand and combine my previous research work to help design a reliable and practically efficient wireless mesh network for metropolitan area.

#### **Intelligent Wireless Sensing System for Metropolitan Area**

I am also interested in building an infrastructure for the wireless intelligent system in metropolitan area by integration of wireless mesh network, VANET, and people-centric sensor network. People-centric sensor networks leverage the mobile phones carried by people in an urban area to sense urban environment and human activity. Combined with VANET and wireless mesh network, we can build effective intelligent systems such as urban disaster response system, smart traffic information system, as well as a urban social network. Especially I am interested in security matters in such systems, for instance, access control to sensing resource; who can assign sensing commands and who can access sensing results.

### REFERENCES

- [1] M. Shin, A. Mishra, and W. Arbaugh, "Improving the latency of 802.11 hand-offs using neighbor graphs," *Mobisys, Boston, MA*, 2004.
- [2] A. Mishra, M. Shin, and W. Arbaugh, "Context caching using neighbor graphs for fast handoffs in a wireless network," *IEEE conference Infocom, Hong Kong*, 2004.
- [3] A. Mishra, M. Shin, J. Nick L. Petroni, T. C. Clancy, and W. Arbaugh, "Pro-active key distribution using neighbor graphs," *Wireless Communications Magazine*, Feb. 2004.
- [4] M. Shin, J. Ma, A. Mishra, and W. Arbaugh, "Wireless network security and interworking," *The Proceedings of IEEE on Cryptography and Security*, 2005.
- [5] Z. J. Fu, M. Shin, J. C. Strassner, N. Jain, V. Ram, S. Upadhyaya, and W. A. Arbaugh, "Aaa for spontaneous roaming agreements in heterogeneous wireless networks," *ATC, Hong Kong, China*, 2007.
- [6] M. Shin, S. Lee, and Y. Kim, "Distributed channel assignment for multi-radio wireless networks," *MASS, Vancouver, Canada*, Oct. 2006.
- [7] C. Kari, Y.-A. Kim, S. Lee, A. Russell, and M. Shin, "Soft edge coloring," *APPROX, Princeton, NJ*, 2007.
- [8] H. Dinh, Y.-A. Kim, S. Lee, M. Shin, and B. Wang, "Sdp-based approach for channel assignment in multi-radio wireless networks," *Dial M-POMC*, 2007.
- [9] H. Kim, M. Shin, B. Nam, and D. Lovell, "An integrated transportation and communication simulation framework for vehicular ad hoc network applications," *Transportation Research Board*, 2008.