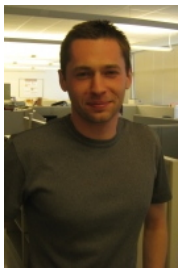
DREXEL UNIVERSITY
Cybersecurity Institute

Research project profile: **secure wireless symmetric key generation** and **protocol-aware reactive jamming of wireless signals**

Investigators	Danh Nguyen	Ph.D. student	Dept. of ECE	Drexel University
	Cem Sahin	Ph.D. student	Dept. of ECE	Drexel University
	Boris Shishkin			LMCO-ATL
	Naga Kandasamy	Associate Professor	Dept. of ECE	Drexel University
	Kapil Dandekar	Professor	Dept. of ECE	Drexel University


D. Nguyen


C. Sahin


B. Shishkin


N. Kandasamy


K.R. Dandekar

Research summary – secure wireless symmetric key generation: Our algorithm, which is designed for orthogonal frequency-division multiplexing (OFDM) systems, collects channel state information (CSI) data to extract randomness from the wireless channel. We start by sending packets that contain dummy or non-confidential data back and forth between two legitimate users. For each received packet, the nodes extract CSI and store them inside a matrix. Within the matrix, each column corresponds to the subcarrier index and the rows indicate the packet number. We call this collection of individual CSI measurements the channel trend information (CTI). CTI is used to determine the overall fading trend of each data subcarrier. The confidence constant, N, is set by the user and indicates the number of agreeing ones or zeroes required before a secret bit can be locked. These secret bits are then concatenated to form a secret key. The value of N also determines the number of dummy packets that needs to be transmitted before the key generation takes place. Apart from transmitting packets with dummy data, our algorithm provides secrecy as it does not leak any sensitive information.

Research summary – protocol-aware reactive jamming of wireless signals: We develop a software-defined radio (SDR) framework for real-time reactive adversarial jamming in wireless networks. The system consists of detection and RF response infrastructure, implemented in the FPGA of a USRP N210 and designed to function with the open source GNU Radio SDR library. The framework can be used to implement a fast turnaround reactive jamming system capable of timely RF response within *80ns* of signal detection. Our framework also allows for full control and feedback from the FPGA hardware to the GNU Radio-based cognitive radio backend, making it applicable to a wide range of preamble-based wireless communication schemes. Using this platform, we demonstrate real-time reactive jamming capabilities in both WiFi (802.11g) and mobile WiMAX (802.16e) networks and quantify jamming performances by measuring the network throughput using the iperf software tool. The results indicate that our system works reliably in real time as a reactive jammer.

Publications related to this research project include:

[1] Danh Nguyen, Cem Sahin, Boris Shishkin, Nagarajan Kandasamy, and Kapil R. Dandekar. A real-time and protocol-aware reactive jamming framework built on software-defined radios. *Proceedings of the ACM SIGCOMM Software Radio Implementation Forum (SRIF)*, Chicago, IL, August 2014.

[2] Nikhil Gulati, Rachel Greenstadt, Kapil R. Dandekar, and John M. Walsh. GMM based semi-supervised learning for channel-based authentication scheme. *Proceedings of the 7th IEEE Fall Vehicular Technology Conference (VTC)*, Las Vegas, NV, September 2013.

[3] Prathaban Mookiah and Kapil R. Dandekar. A reconfigurable antenna-based solution for stationary device authentication in wireless networks. *Hindawi International Journal of Antennas and Propagation*, 2012.

This research is partially supported by the following grants:

[1] Steven Weber (PI), Kapil R. Dandekar, Spiros Mancoridis, and Harish Sethu. TTP: Medium: Securing the Wireless Philadelphia Network. *National Science Foundation Secure and Trustworthy Cyberspace Program (NSF-SaTC)*, CNS-1228847, September, 2012 – August, 2016. $1,080,800.

[2] Kapil R. Dandekar (PI), Rachel Greenstadt, and John MacLaren Walsh. A framework for wireless network security based on reconfigurable antennas. *National Science Foundation Networking Technology and Systems (NeTS) Program*, CNS-1028608, September, 2010 – August, 2014. $359,506.