A Reconfigurable Antenna Based Solution for Device Authentication in Wireless Networks

**Technology Summary:** Large scale proliferation of wireless technology coupled with the increasingly hostile information security landscape creates a serious need for effective security measures. The fundamental broadcast nature of wireless data transmission aggravates the situation by introducing multiple avenues for attack and penetration into a network. While several established protection mechanisms such as cryptography based techniques and wireless intrusion prevention systems exist, each method has its own weaknesses and is susceptible to failure under different circumstances. Drexel researchers have devised a novel device authentication scheme that utilizes the capabilities of reconfigurable antennae to provide a robust additional layer of security against attacks that are based on spoofing transmitter identities, as well as man-in-the-middle attacks. This method shows marked improvement in intruder detection rates, as well as providing a precise guideline on how to choose a reconfigurable antenna and the number of modes in order to achieve the required level performance in a given environment.

**Applications:**
- Device authentication in wireless network security

**Advantages:**
- **Effectiveness:** high intruder detection rates at low false alarm rates. It has been shown that the effectiveness of the device fingerprint can be increased significantly with the addition of extra antenna modes.
- **Security:** Enforcing security at the lowest layer provides a robust extra level of security and helps the upper level layers to better handle spoofing and man-in-the-middle attacks.
- **Efficiency:** Reconfigurable antennas are mainly incorporated in wireless devices for their ability to increase spectral efficiency. Applying them for security provides meaningful additional returns on the extra costs incurred in incorporating such antennas.

**IP Status:** International Application Pending: PCT/US2012/054205

**Commercialization Opportunities:** Drexel University is seeking partners interested in the further development of these technologies and commercialization of both the software and patent pending algorithms.
Inventor(s): Prathaban Mookiah, Kapil R. Dandekar, John MacLaren Walsh, Rachel Greenstadt,

Relevant Publication(s):

Drexel Technology ID: 11-1327D

Contact Information

For Technical Information: For Intellectual Property and Licensing Information:

Kapil Dandekar, PhD Paul Dougherty
Professor, Electrical and Computer Licensing Manager
Engineering Office of Technology Commercialization
Associate Dean for Research and The Left Bank
Graduate Studies 3180 Chestnut Street, Suite 104
College of Engineering Philadelphia, PA 19104
3141 Chestnut St – 7-209 Phone: 1-215-571-4290
Philadelphia, PA 19104 Email: pdougherty@drexel.edu

Phone: 215-895-2004
Email: dandekar@coe.drexel.edu