Sensor Netw Data Commun 2015, 3:2
http://dx.doi.org/10.4172/2090-4886.C1.003

OMICS International
conferenceseries.com

International Conference and Business Expo on
Wireless Communication & Network
September 21-23, 2015 Baltimore, USA

Are beacons creepy? Are beacons enabling a connection for better services and systems?

Steve Hegenderfer
Bluetooth Special Interest Group, USA

Beacons are small, inexpensive wireless devices that broadcast radio signals to smart devices, but placing several those in a certain area chance an entire experience. Just take a look at how beacons have already changed the way people can shop. When you go to your local grocery store, you get turn-by-turn directions to the products you need, reminders for items you left off your list, and coupons tailored specifically to you. Sounds helpful, right? But it also sounds a little creepy. Beacon technology is being deployed across retail stores and sports, providing personalized micro-location based notifications such as in the grocery store example. However, the beacons have the potential to change more than just customer service and retail. Beacons can improve the quality of life – from better health care and access, education, and agricultural infrastructure scenarios to handle valuable resources. For example, Beacons can be implemented to monitor and manage irrigation systems in developing countries that will let people, and nations, better understand and make efficient use of their water supplies. As a wireless trade association with more than 24,000 members, the Bluetooth SIG is in a unique position to discuss the potential and challenges of beacons as a disruptive wireless technology across different industries, countries, and uses cases for different peoples and cultures. This session will explore beacons - their privacy and security concerns, and how they will impact the human interaction with our health, education, and resources.

shegenderfer@bluetooth.com

Connected vehicles, communications and security infrastructure

Tarek Saadawi
City University of New York, USA

Today's modern cars are pervasively computerized and controlled by a heterogeneous combination of digital components, referred to as Electronic Control Units, ECUs. Each vehicle may have between 20 to 100 ECUs. With the deployment of the wireless technology, the vehicle of the future will potentially be vulnerable to cyber-attacks and precautions need to be implemented early. Cyber-attacks on connected cars and connected trucks that are largely computer controlled can bring chaos to the roads. This talk will address the WAVE (Wireless Access Vehicular Environment) standard, recent pilot projects and the connected vehicle wireless infrastructure vulnerability. We will discuss also the denial of service attacks on the WAVE technology, how to detect such attack, and how to mitigate its effect on the communications infrastructure.

saadawi@ccny.cuny.edu