The Thirteenth IEEE International Workshop on Managing Ubiquitous Communications and Services, 2016 - Program

Opening remarks

S1: Managing Data and Information

An Intelligent SDP Discovery Scheme Using Knowledge-based Adaptive Probing
Heesuk Son and Dongman Lee (Korea Advanced Institute of Science and Technology, Korea)

Natural Language Search of Sensor Data
Keyi Zhang and Alan Marchiori (Bucknell University, USA)

Integrating Quality of Information with Pragmatic Assistance
James H Edwards (Pennsylvania State University, USA); Taylor Cassidy (US Army Research Laboratory, USA); Geeth Ranimai de Mel (IBM Research, United Kingdom); Tom La Porta (Pennsylvania State University, USA)

Session discussion

Morning Coffee

S2: Managing IoT Applications

Device Group Management in Constrained Networks
Maria Ines Robles (Aalto University & Ericsson Research, Finland); Domenico D’Ambrosio (Università degli Studi di Napoli Federico II, Italy); Jaime Jimenez Bolonio (Ericsson, Spain); Miika K.T. Komu (Ericsson Research, Finland)

Pushing SDN to the End-Host, Network Load Balancing Using OpenFlow
Anees Al-Najjar (University of Queensland, Australia); Siamak Layeghy (The University of Queensland, Australia); Marius Portmann (University of Queensland, Australia)

Linked models @ runtime to ease the administration of pervasive applications
Philippe Lalanda (Grenoble University, France); Stéphanie Chollet (LIG, France); Catherine Hamon (Orange, France)

Session discussion
Lunch

K: Keynote

First part of this talk will discuss how the community is converging towards the IoT vision having worked in wireless sensor networking and Machine-2-Machine (M2M) communication. This will follow a general discussion of security challenges in IoT. Finally I will discuss some results from an ongoing project on security of bodyworn devices. Wireless bodyworn sensing devices are becoming popular for fitness, sports training and personalized healthcare applications. Securing the data generated by these devices is essential if they are to be integrated into the current health infrastructure and employed in medical applications. In this talk, I will discuss a mechanism to secure data provenance for these devices by exploiting symmetric spatio-temporal characteristics of the wireless link between two communicating parties. Our solution enables both parties to generate closely matching ‘link’ fingerprints, which uniquely associate a data session with a wireless link such that a third party, at a later date, can verify the links the data was communicated on. These fingerprints are very hard for an eavesdropper to forge, lightweight compared to traditional provenance mechanisms, and allow for interesting security properties such as accountability and non-repudiation. I will present our solution with experiments using bodyworn devices in scenarios approximating actual device deployment.

A Changing Landscape: Securing the Internet of Things (IoT)
Sanjay Jha (University of NSW, Australia)

S3: Models and Architectures for Managing Ubiquitous Communications

A Study on the Optimization of the Uplink Period Using Machine Learning in the Future IoT Network
Jae Seong Jang, Young Lak Kim and Jin Hyo Park (SKtelecom, Korea)

Towards Programmable and Scalable IoT Infrastructures for Smart Cities
Andreea Ancuta Corici and Ronald Steinke (Fraunhofer FOKUS, Germany); Thomas Magedanz (Fraunhofer Institute FOKUS / TU Berlin, Germany); Louis Coetzee (CSIR, South Africa); Dawid Oosthuizen (CSIR, Germany); Buhle Mkhize (CSIR, South Africa); Marisa Catalan (i2CAT Foundation, Spain); Jacint Castells Fontelles (I2CAT, Spain); Josep Paradells (UPC, Spain); Ranjan Shrestha (Fraunhofer FOKUS, Germany); Daniel Nehls (Technische Universität Berlin & FOKUS Fraunhofer, Germany); Bjoern Riemer (Technische Universität Berlin, Germany)

Session discussion

Afternoon Tea

W: Interactive Working Session

This session will foster an interactive discussion with all participants on a current issue in managing ubiquitous communications and systems.