International Journal of Distributed Sensor Networks, 3: 135–136, 2007

ISSN: 1550-1329 print/1550-1477 online
DOI: 10.1080/15501320701252771

Taylor & Francis
Taylor & Francis Group

Introduction to the Special Issue on Sensor Networks, Ubiquitous and Trustworthy Computing

The first IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC2006) was held in Taiwan on June 5–7, 2006. SUTC2006 is an international forum for researchers to exchange information regarding advancements in the state of the art and practice of sensor networks, ubiquitous and trustworthy computing, as well as to identify the emerging research topics and define the future of sensor networks, ubiquitous and trustworthy computing. The technical program of SUTC2006 consists of invited talks, paper presentations, and panel discussions.

SUTC2006 covers broad and diverse topics, which include

- Sensor network architecture and protocols
- Operating systems
- Routing protocols
- Data storage
- Ubiquitous computing and Ad Hoc networking
- Ubiquitous intelligence and smart spaces
- Embedded chips, sensor, and actuator
- Self-adaptive and self-healing systems
- Topology construction and coverage maintenance
- Energy and mobility management
- Context and location aware applications
- Data gathering, fusion, and dissemination
- Distributed coordination algorithms
- Complexity analysis of algorithms
- QoS, security, privacy, reliability, and social issues
- Trust establishment, negotiation, and management
- Authentication and access control
- Intrusion detection and tolerance
- Design and programming methodologies for wireless systems
- Formal methods for analysis of wireless systems
- Performance evaluation and modeling of mobile and wireless networks
- Simulation languages and systems for wireless systems
- Testing and debugging techniques for wireless systems
- Personal area networks
- Database management systems and mobile computing
- User interface technologies
- Applications of wireless sensor networks

A total of 215 papers were submitted to the conference by researchers all over the world. All the submitted papers were reviewed by three or four reviewers. The technical program committee selected 52 papers. The acceptance rate is 24%. From the 52 papers, 5 best papers were selected and extended to appear in this special issue.

The first paper by Ou, Hsiao, Chiang, and King presents a distributed overlay formation protocol to deal with the scalability and functional complexity of a non-homogeneous

architecture of future-generation wireless sensor networks. Through simulation, authors compare their protocol with two overlay formation protocols, one that generates a fully connected topology and the other a minimum spanning tree. The results show that our protocol can achieve better performance both in message latency and energy consumption.

The second paper by Xu and Lee proposes an efficient and accurate algorithm for in-network data compression, called delay-tolerant trajectory compression (DTTC) to support a broad class of movement trajectories using two proposed techniques, DC-compression and SW-compression, and an efficient trajectory segmentation scheme, which are designed for improving the trajectory compression accuracy at less computation cost. Authors analyze the underlying cluster-based infrastructure and mathematically derive the optimum cluster size, aiming at minimizing the total communication cost of DTTC algorithm. Simulation results show that DTTC exhibits superior performance in terms of accuracy, communication cost and computation cost and soundly outperforms DPR with all types of movement trajectories.

The third paper by Ren, Yu, Kwiat, and Tsai presents a coordination model that contains three active entities: actors, roles and coordinators. Actors abstract the system's functionalities while roles and coordinators statically encapsulate coordination constraints and dynamically propagate these constraints among themselves and onto the actors. A software system's attack-tolerance and survivability in open hostile environments are enhanced through appropriate constraint propagations and constraint enforcements. The survivable feedback loops presented in the model resist the contamination of the system by faulty elements and thereby protect the whole system from being broken down by single failures.

The fourth paper by Panja, Medria, and Bhargava describes a group key management protocol for hierarchical sensor networks where instead of using pre-deployed keys, each sensor node generates a partial key dynamically using a function. They have implemented this protocol using MICA2 motes and have experimentally analyzed the time and energy consumption in broadcasting partial keys and the group key under two sensor routing protocols (Tiny-AODV and Tiny-Diffusion). They found out that the obtained results are very close to the observations made using the simulator.

The fifth paper by Liu, Ngan, and Ni attempts to answer a fundamental but practical question: "how should we deploy these nodes?" Through their study, they exhibit the weakness of the uniform distribution by disclosing the fatal Sink routing-hole problem. To address this problem, authors propose a non-uniform, power-aware distribution scheme. The analysis and simulation results show that the Power-aware deployment scheme can significantly improve the long-termed network connectivity and service quality.

Jeffrey J. P. Tsai
Guest Editor