Peer-to-Peer Netw. Appl. (2014) 7:213–214
DOI 10.1007/s12083-013-0237-z

PPNA special issue on "the green, reliability and security of machine-to-machine communications"

Xu Li · Xiaodong Lin · Wenye Wang · Nathalie Mitton

Received: 6 September 2013 / Accepted: 10 September 2013 / Published online: 26 September 2013

Machine-to-machine communications is an emerging technology that realizes a system of networks, wireless or wired, possibly distributed across the world, for transmitting events captured by low-end machines such as sensors and smart meters to high-end applications and/or personal appliances, where the events are translated into meaningful information. It embraces several major research fields including wireless sensor networks, vehicular networks, smart grid and RFID, emerging as a promising approach to enabling ubiquitous computing environment. Unlike current world-scale human-centric 3G wireless networks, M2M communication network is characterized by the absence of direct human intervention and the rapid increase in size and is therefore imposed with unique requirements.

With ever-decreasing cost of deployment of M2M communication devices and access to public wireless data networks, and also thanks to its potential to support a large number of ubiquitous characteristics and achieving better cost efficiency, M2M communications has quickly become a market-changing force for a wide variety of real-time monitoring applications, such as remote patient monitoring, smart homes, utility management, environmental monitoring and industrial automation. However, the flourishing of M2M communications still hinges on fully understanding and managing the existing GRS challenges, i.e., Green (energy efficiency), Reliability and Security. This special issue includes six state-of-the-art contributions on the GRS aspects of M2M communications.

The first paper entitled "An Attack-and-Defence Game for Security Assessment in Vehicular Ad Hoc Networks" by Suguo Do, Xiaolong Li, Junbo Du, Haojin Zhu points out that existing risk analysis solutions fail to consider the attack and defense costs and gains in vehicular networks, and thus cannot appropriately model the mutual interaction between the attacker and defender. The authors propose a game theoretical approach for security assessment in Vehicular Ad Hoc Networks (VANETs). They consider both of the rational attacker and defender, and adopt the attack-defense tree to model the attacker's potential attack strategies and the defender's corresponding countermeasures. To take the attack and defense costs into consideration, they introduce Return On Attack and Return on Investment to represent the potential gain from launching an attack or adopting a countermeasure in vehicular networks. They investigate the potential strategies of the defender and the attacker by modeling it as an attack-defense game. A detailed analysis on its Nash Equilibrium is provided.

The second paper entitled "A Social Network Approach to Trust Management in VANETs" by Zhen Huang, Sushmita Ruj, Marcos Cavenaghi, Milos Stojmenovic, and Amiya Nayak presents several limitations of current trust management schemes in VANETs and proposes ways to counter them. The authors identify that the problem of information cascading and oversampling, which commonly arise in social networks, adversely affects trust management schemes in VANETs. They show that simple voting for decision-making leads to oversampling and gives incorrect results in VANETs. To overcome this problem, they propose a new voting scheme, where each vehicle has different voting weight according to its distance from the event. The vehicle that is closer to the event possesses higher weight.

X. Li (✉)
Huawei Technologies Canada, Ottawa, ON K2K 3J1, Canada
e-mail: easylix@gmail.com

X. Lin
University of Ontario Institute of Technology,
Oshawa, ON L1H 7K4, Canada

W. Wang
North Carolina State University, Raleigh, NC 27695, USA

N. Mitton
Inria Lille - Nord Europe, Villeneuve d'Ascq 59650, France

The third paper entitled "PaderMAC: Energy-efficient Machine to Machine Communication for Cyber-physical Systems" by Marcus Autenrieth and Hannes Frey presents a new MAC protocol, called PaderMAC, for wireless sensor networks, where the routing decision on the next hop node is made by the receiver as opposed to the senser naming the recipient explicitly in a state of the art mac protocol X-MAC. This work specifies the PaderMAC protocol, explains the implementation of the protocol using TinyOS and the MAC layer architecture (MLA), describes a contribution to the MLA which is useful also for other MAC layer implementations, and presents the results of a testbed and theoretical performance study.

In wireless sensor networks, sensor nodes close to the sink consume more energy than others because they are burdened with heavier relay traffic destined for the sink and trend to die early, forming energy holes. It has a serious impact on network lifetime. The forth paper entitled "On Mitigating Hotspots to Maximize Network Lifetime in Multi-hop Wireless Sensor Network with Guaranteed Transport Delay and Reliability" by Anfeng Liu, Deyu Zhang, Penghui Zhang, Guohua Cui, and Zhigang Chen proposes three optimization algorithms to mitigate such energy holes and prolong network lifetime for adaptive Mary Phase Shift Keying (MPSK) based wireless sensor networks, while transport delay and reliability can be still guaranteed. Extensive simulation studies show that the algorithms do considerably prolong the network lifetime.

IEEE 802.15.4 standard was proposed for low power wireless personal area networks. The fifth paper entitled "Uncoordinated Coexisting IEEE 802.15.4 Networks for Machine to Machine Communications" by Chao Ma, Jianhua He, Hsiao-Hwa Chen and Zuoyin investigates the problem of reliable communications in uncoordinated coexisting IEEE 802.15.4 networks. The authors address the problem in three typical scenarios and propose an analytic model to reveal how performance of coexisting 802.15.4 networks may be affected by uncoordinated operations. The analytic model is validated through simulation. It is observed that uncoordinated operations may lead to a significant degradation of system performance in M2M applications. With the analytic model, the authors also study the performance limits of 802.15.4 networks, and the conditions under which coordinated operations may be necessary.

In VANETs, reliable transmission and privacy of vehicles are two important issues, which are addressed in the last paper entitled "Identity Privacy-based Reliable Routing Method in VANETs" by Di Wu, Xiaojing Wang, Limin Sun, Yan Ling and Dongxia Zhang. The paper proposes an Identity Privacy-based Reliable Routing method (IPRR). This method divides the message transferring model into an uploading process and a downloading process. The uploading process has four stages, including connection establishment, gaming, detecting process and message sending process. In the four stages, a dynamic ID scheme is used to protect identity privacy. During communications, a game model, based on the reliability and the frequency of contacts, is engaged to accomplish reliable transmission. Simulation results show that the proposed routing method can not only increase message delivery ratio, but also reduce the end-to-end delay and the overhead ratio of the network.

In closing, we would like to thank all the authors who have submitted their research work to this special issue. We would also like to acknowledge the contribution of many experts in the field who have participated in the review process and provided helpful suggestions to the authors on improving the content and presentation of the papers. We would also like to express our gratitude to the Editor-in-Chief, Dr. Xuemin Shen, for his support and help in bringing forward this special issue. We hope you will enjoy the papers in the special issue.