Wireless Pers Commun (2014) 75:1587–1589
DOI 10.1007/s11277-014-1649-7

Special Issue on Advances in Trust, Security and Privacy for Wireless and Mobile Networks

Yulei Wu · Ryan Ko · Ahmed Al-Dubai

Published online: 20 February 2014

The advances in wireless communication technologies and mobile devices have provided cost-effective platforms and environments for people to have better and ubiquitous interpersonal communications. The trust, security and privacy issues in such an environment have drawn significant attention recently from both academia and industry. The accepted papers in this special issue are devoted to the most recent developments and research addressing related theoretical and practical aspects on trust, security and privacy for wireless and mobile networks, and the contents are built on analytical modelling, experimental and simulation studies. The contributions of these papers are outlined below.

People-centric sensing (PCS) is an emerging and promising paradigm of sensor networks, but faces severe security problems due to the strong connectivity and homogeneous applications. Lu et al. propose a novel behavioural signature generation system, called SimBehavior, to generate lightweight behavioural signature for malware detection in PCS. Unlike malware detection using behaviour graph which is NP-Complete, the proposed SimBehavior is efficient and suitable for malware detection in PCS. The experimental results show that SimBehavior can extract behavioural signatures effectively which can be used to detect new malware samples in PCS efficiently.

Security and privacy protection have been the primary concerns in pushing towards the success of wireless mesh networks. In order to defend against the internal attacks and to achieve better security and privacy protection, Lin et al. propose a role based privacy-aware secure routing protocol (RPASRP), combining a new dynamic reputation mechanism with the role based multi-level security technology and a hierarchical key management protocol. Simulation results show that the proposed RPASRP implements the security and privacy

Y. Wu (✉)
Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190, China
e-mail: wuyulei@cstnet.cn

R. Ko
Department of Computer Science, University of Waikato, Hamilton 3240, New Zealand

A. Al-Dubai
School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, UK

protection against the inside attacks more effectively and performs better than the classical hybrid wireless mesh protocol in terms of packet delivery ratio and average route length.

Vehicular ad hoc networks (VANETs) are implemented to support a wide variety of distributed applications starting from safety services such as collision avoidance systems down to commercial services such as context-aware advertisement and file sharing. Wahab, Otrok and Mourad address the problem of cooperation among vehicles in VANET using QoS-OLSR protocol in the presence of selfish nodes, and propose a Dempster–Shafer based Tit-for-Tat strategy to improve the decision and regulate the cooperation in the vehicular networks. Simulation results prove that the Dempster–Shafer based strategy is able to maintain the survivability of the vehicular networks in the presence of high mobility and packet collisions with minimal time and overhead.

With the rise of smart phones, laptops, and tablets, which all utilize wireless networks for connectivity to the Internet, the effect of attacks on wireless security has become much larger and more significant. Liu et al. investigate the trends within security usage in wireless networks and discover wireless security threats that are freely available to download. The overall findings display the fact that wireless security can be improved using encryption. The findings are then used to produce recommendations that present the most appropriate countermeasures to the threats found.

Indirect trust computation based on recommendations play an important role in trust based access control models. Iltaf et al. present an effective model for indirect trust computation, which is capable of identifying dishonest recommendations. The proposed model has been compared with other existing evolutionary recommendation models, and the results show that the model is more accurate in measuring the trustworthiness of unknown entity.

Accountability requires that any entity in a computer and network system should be held responsible for its own action in order to assure the accountability of the entire system. Without assuring accountability, there might be no effective solution to find out the source and reason of the disclosing of the sensitive data. Fu and Xiao propose a flow-net scheme to record all the events and their relations through the collaboration of the nodes in a network, which can accomplish accountability and detect attacks in networks. The authors then present two methods to analyze the accountability of a network via the users' accepted overhead called Q-Accountable Logging by Overhead and the flow-net record depth called P-Accountable Logging, respectively.

The scarcity of energy and the difficulty of recharging in ad hoc networks make selfish nodes a common problem in the selection of multi-point relay (MPR) nodes in a cluster-based QOLSR network. Moati et al. present an MPR selection mechanism considering the selfishness during the election and selection process by using the reputation system that motivates the nodes to participate the selection of MPRs. In addition, the authors propose a hierarchal cooperative watchdog detection model for the cluster-based QOLSR to avoid the misbehaviour of nodes after being selected/elected. Simulation results show that the novel cluster-based QoS-OLSR model can give incentive to nodes to behave normally without sacrificing the quality of service of the network.

The concept of federation has been proposed as a technology to bridge different trust domains, allowing user identity information to be shared in order to improve usability. Cabarcos et al. present IdMRep, the first completely decentralized reputation-based mechanism which makes dynamic federation a reality. Initial experiments demonstrate its accuracy as well as an assumable overhead in scenarios with and without malicious nodes.

Data access control within smart grids is a challenging issue because of the environmental noise and interferences. Wu et al. propose a dedicated data access control scheme that is able to enforce fine-grained access control and resist against the corruptions implied by the

noisy channels and the environmental interferences. Extensive simulation results show the efficiency and feasibility of the proposed scheme in terms of error correcting capability and energy consumption.

A two-tiered architecture with resource-rich master nodes at the upper tier and resource-poor sensor nodes at the lower tier is expected to be adopted in large-scale sensor networks. In a hostile environment, adversaries are more motivated to compromise the master nodes to break the authenticity and completeness of query results. Ma et al. study the problem of verifiable fine-grained top-k queries in two-tiered sensor networks, and propose a novel verification scheme, which is named verification scheme for fine-grained Top-k queries (VSFTQ). Both theoretical analysis and simulation results show that the proposed VSFTQ can ensure high probability of detecting forged and/or incomplete query results, and significantly decrease the amount of verification information when compared with existing schemes.

Acknowledgments We would like to express our deep thanks to the Editor-in-Chief, Professor Ramjee Prasad, for providing us with the opportunity to host this special issue in Wireless Personal Communications. We also thank all the authors who submitted their contributions to this Special Issue for publication consideration. Last but not least, we thank the thoughtful work of the many reviewers who provided invaluable evaluations and recommendations.