J Supercomput (2013) 64:661–663
DOI 10.1007/s11227-013-0953-4

Trust, security and privacy for pervasive applications

Guojun Wang · Wanlei Zhou · Laurence T. Yang

Published online: 25 April 2013

Pervasive computing, or ubiquitous computing, has evolved into an active research area, as a result of the tremendous advances in a broad range of technologies, including wireless networking, mobile and distributed computing, sensor systems, RFID technology, etc. Pervasive computing, which enables users to obtain information and services anytime and anywhere, could have a wide range of applications, such as healthcare, homecare, intelligent transportation, and environmental monitoring. However, it is quite difficult for pervasive applications to satisfy trust, security and privacy requirements, due to their ability to gather sensitive information and change the environment via actuating devices autonomously.

This special section aims at presenting a collection of high quality research papers that report the latest research achievements in trust, security and privacy for pervasive applications, and providing a forum to present and discuss emerging ideas and trends in this highly challenging field. In this special section, we selected 8 papers out of 37 total submissions, which demonstrate some novel works in this field. A detailed overview of the selected works is given below.

The first paper, "A Holistic Approach Examining RFID Design for Security and Privacy," [1] presents a holistic approach to ensure security and privacy for Radio

G. Wang (✉)
School of Information Science and Engineering, Central South University, Changsha, 410083, China
e-mail: csgjwang@csu.edu.cn

W. Zhou
School of Information Technology, Deakin University, 221 Burwood Highway, Burwood, Victoria 3125, Australia
e-mail: wanlei@deakin.edu.au

L.T. Yang
Department of Computer Science, Francis Xavier University, Antigonish, NS, B2G 2W5, Canada
e-mail: ltyang@stfx.ca

Frequency Identification (RFID) systems. The proposed approach adopts a practical realization of a secure passive (battery-less) RFID tag, and integrates the ultra-low-power Advanced Encryption Standard (AES) design together with a novel random number generator. The experimental results show that the proposed holistic approach can provide a strong security guarantee with very low power, very low number of cycles, and very low area for achieving the required performance within the stringent constraints imposed by passive RFIDs.

The second paper, "Secure Localization and Location Verification in Wireless Sensor Networks: A Survey," [2] presents a survey on secure localization and location verification in wireless networks. To provide a comprehensive review on the security of sensor locations, this survey describes the attacks against localization and location verification, classifies and describes existing solutions to such attacks, and provides quantitative performance comparison of typical secure localization algorithms by simulations.

The third paper, "Requirements and Design for Neutral Trust Management Framework in Unstructured Networks," [3] designs a neutral trust management framework for MANETs, to ensure that users could obtain services free from discrimination or interference. In the proposed framework, the neutrality requirements, objectiveness, fairness and variegation have been naturally included into the requirements of trust management, trust propagation, calculation and enforcement. The performance analyses show that neutrality can be achieved under the location-dependent attack of free-rider in MANETs.

The fourth paper, "Dynamic Camouflage Event based Malicious Node Detection Architecture," [4] presents the Dynamic Camouflage Event-based malicious Node Detection Architecture (D-CENDA) for detecting malicious nodes in the sensor networks. D-CENDA improves CENDA by using dynamic feedback from the network in the form of sensor node usage for event detection and packet propagation. By adopting a multiphase approach, D-CENDA can not only detect intrusions but also identify the malicious nodes and the type of attacks, with reduced overhead and less false positive rate.

The fifth paper, "ADVS: A Reputation-based Model on Filtering SPIT over P2P-VoIP Networks," [5] proposes a novel Anti-Distributed Voice Spam scheme (ADVS) against SPam over Internet Telephony (SPIT) for the distributed and self-organized VoIP networks. ADVS presents a proper reputation model which evaluates end-users' past behaviors and accumulates other users' referrals for detecting and filtering spam calls. The experimental results show that ADVS can detect spam calls accurately and stably.

The sixth paper, "User Requirements-Aware Security Ranking in SSL Protocol," [6] proposes a secret exchange algorithm for the Secure Socket Layer (SSL) handshake protocol. The proposed algorithm uses the batch RSA decryption with a unique certificate to speed up the SSL session initialization, and optimizes the batch size by using a constrained model that integrates the user-perceived quality into secure web server design. Evaluation results show that the proposed algorithm works well for heavily loaded web servers that handle many concurrent SSL sessions.

The seventh paper, "Detection of Blackhole Attack in a Wireless Mesh Network using Intelligent Honeypot Agents," [7] proposes an intelligent honeypot-based system to detect blackhole attackers in Wireless Mesh Networks (WMNs). The proposed system utilizes the topological knowledge from the mobile honeypot agents to detect spurious route advertisements. The simulation results show that the proposed honeypot-based system has a high detection rate and a low false positive rate.

The eighth paper, "VectorTrust: Trust Vector Aggregation Scheme for Trust Management in Peer-to-Peer Networks," [8] proposes a trust-vector–based trust management scheme (VectorTrust) for aggregation of distributed trust scores in Peer-to-Peer (P2P) networks. By leveraging a Bellman–Ford algorithm, VectorTrust can provide fast and lightweight trust score aggregation in decentralized P2P network without a centralized server. The analysis and simulation results demonstrate that VectorTrust converges faster and involves less complexity than most existing trust schemes.

In conclusion, this special section on trust, security and privacy for pervasive applications gives insight into the recent research results in the broader trust, security, and privacy community. This special section also provides certain guidelines for academic and industry advances, and these accomplishments are regarded as a basis towards future research directions, and vital commercial applications.

This special section has obtained help and instructions from all participants. We would like to express our great appreciation to Prof. Hamid R. Arabnia, the Editor-in-Chief of this journal, for his suggestions and encouragements all through the stages, and to all anonymous reviewers who spent their precious time in reviewing the papers, and offering good advice or recommendations, which greatly helped us to select the best papers into this special section. We also thank all authors who submitted their papers to this special section.

Finally, we hope you will find the papers in this special section useful.

References

1. Good T, Benaissa M (2010) A holistic approach examining RFID design for security and privacy. J Supercomput. doi:10.1007/s11227-010-0497-9
2. Zeng Y, Cao J, Hong J, Zhang S, Xie L (2010) Secure localization and location verification in wireless sensor networks: a survey. J Supercomput. doi:10.1007/s11227-010-0501-4
3. Li R, Li J (2010) Requirements and design for neutral trust management framework in unstructured networks. J Supercomput. doi:10.1007/s11227-010-0502-3
4. Pongaliur K, Xiao L, Liu AX (2010) Dynamic camouflage event based malicious node detection architecture. J Supercomput. doi:10.1007/s11227-010-0508-x
5. Wang F, Wang FR, Huang B, Yang LT (2011) ADVS: a reputation-based model on filtering SPIT over P2P-VoIP networks. J Supercomput. doi:10.1007/s11227-010-0545-5
6. Qi F, Tang Z, Wang G, Wu J (2011) User requirements-aware security ranking in SSL protocol. J Supercomput. doi:10.1007/s11227-010-0546-4
7. Prathapani A, Santhanam L, Agrawal DP (2011) Detection of blackhole attack in a wireless mesh network using intelligent honeypot agents. J Supercomput. doi:10.1007/s11227-010-0547-3
8. Zhao H, Li X (2011) VectorTrust: trust vector aggregation scheme for trust management in peer-to-peer networks. J Supercomput. doi:10.1007/s11227-011-0576-6