EURASIP Journal on
Wireless Communications and Networking
a SpringerOpen Journal

EDITORIAL Open Access

Introduction to advances in trust, security, and privacy for wireless networks

Yulei Wu[1*], Félix Gómez Mármol[2] and Ahmed Al-Dubai[3]

In recent years, wireless networks have become one of the most influential technological accomplishments and pervaded our daily lives in forms of mobile telephony and wireless computing. Due to their rapid development and widespread applications, trust, security, and privacy issues in wireless networks have become very important topics. As a result, there is a grand challenge to build wireless systems and networks in which various applications allow users to enjoy more comprehensive services while preserving trust, security, and privacy at the same time. The accepted papers in this special issue deal with a wide range of important aspects and challenging issues of trust, security, and privacy techniques for wireless networks, and the contents are built on analytical modelling, and experimental and simulation studies. The contributions of these papers are outlined below.

In intelligent transportation systems, the cooperation between vehicles and the roadside units is essential to bring these systems to fruition. Vehicular *ad hoc* networks (VANETs) are a promising technology to enable communications among vehicles, and between vehicles and roadside units. Eiza et al. propose in their work entitled 'Investigation of routing reliability of vehicular *ad hoc* networks' a new vehicular reliability model to facilitate reliable routing in VANETs. Simulation experiments demonstrate that the proposed reliable routing outperforms significantly the well-known *ad hoc* on-demand distance vector (AODV) routing protocol in terms of better delivery ratio and less link failures while maintaining a reasonable routing control overhead.

Wormhole attack is one of the most severe security threats in wireless mesh networks that can disrupt majority of routing communications when strategically placed. In the paper entitled 'WRSR: wormhole-resistant secure routing for wireless mesh networks', Matam and Tripathy present a wormhole-resistant secure routing (WRSR) algorithm that detects the presence of wormhole during route discovery process and quarantines it. The most attractive features of the WRSR include its ability to defend against all forms of wormhole (hidden and Byzantine) attacks without relying on any extra hardware like Global Positioning System, synchronized clocks or timing information, and computational intensive traditional cryptographic mechanisms.

Due to an unorganized and decentralized infrastructure, cooperative mobile *ad hoc* networks (CO-MANETs) are vulnerable to attacks initiated on relays. Yu et al. propose in 'Security and quality of service (QoS) co-design in cooperative mobile *ad hoc* networks' a game theoretic approach to quantitatively analyze the attack strategies of the attacker in order to make a rational decision on relay selection and the authentication parameter adaptation to reach a trade-off between security and QoS in CO-MANETs. Simulation results demonstrate the effectiveness of the proposed approach for security and QoS co-design in CO-MANETs.

Indirect trust computation based on recommendations forms an important component in trust-based access control models for pervasive environments. It can provide the service provider the confidence to interact with unknown service requesters. In the paper entitled 'A mechanism for detecting dishonest recommendation in indirect trust computation', Iltaf et al. propose a defense mechanism for filtering out dishonest recommendations based on a measure of dissimilarity function between the two subsets. The simulation results show that the proposed approach can effectively filter out the dishonest recommendations based on the majority rule.

Cooperative relaying with orthogonal frequency division multiple access (OFDMA) has recently emerged as a promising technology to achieve virtual spatial diversity in wireless networks, which has been adopted in the fourth-generation mobile communication standard. Wang et al. present in 'Joint subcarrier and power allocation for physical layer security in cooperative OFDMA networks' a

* Correspondence: wuyulei@cstnet.cn
[1]Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190, China
Full list of author information is available at the end of the article

joint subcarrier and power allocation algorithm to improve the physical layer security in cooperative OFDMA networks, where several source-destination pairs and one untrusted relay are involved. Numerical results show that the proposed algorithm can effectively improve the system sum secrecy rate, and the convergence performance is also desirable.

With the development of mobile networks, propagation characteristics and defense mechanisms of the virus have attracted increasing research attention. Cai et al. present a work entitled 'Virus propagation power of the dynamic network' where they introduce a new way to assess and restrain virus propagation by proposing the concepts of propagation power and propagation structure under the dynamic changes of network topology. This study offers a feasible approach for quantifying the risk of virus infection in the network community which is valuable for designing and optimizing the virus defense systems.

Wireless body area networks (WBANs) are formed by using tiny health monitoring sensors on the human body in order to collect and communicate human personal data. With the work entitled 'Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications', Ali and Khan propose and evaluate an energy-efficient cluster-based key management scheme for WBANs that takes into account the available resources of a node during the whole life cycle of key management. The performance comparison of the proposed cluster-based key management scheme and low-energy adaptive clustering hierarchy (LEACH)-based key agreement scheme show that the proposed mechanism is secure, more energy-efficient, and provides better network lifetime.

Firewalls are network devices dedicated to analyzing and filtering traffic in order to separate network segments with different levels of trust and are usually placed on the network perimeter. In a wireless multihop network, the concept of perimeter is hard to identify, and the firewall function must be implemented on every node together with routing. Maccari and Cigno, in 'Waterwall: a cooperative, distributed firewall for wireless mesh networks,' propose a novel concept of firewall in which every node filters the traffic only with a portion of the whole rule set in order to reduce its computational burden for wireless mesh networks. Even if some errors are committed at each hop, the results show that the filtering efficiency measured for the whole network can achieve the desired precision, with a positive effect on available network resources.

Rapid growth in Internet usage and diverse military applications have led researchers to think of intelligent systems that can assist users and applications in getting services by delivering the required quality of service in networks. Sannasi et al. present in 'Intelligent feature selection and classification techniques for intrusion detection in networks: a survey' a survey on intelligent techniques for feature selection and classification for intrusion detection in networks based on intelligent software agents, neural networks, genetic algorithms, neuro-genetic algorithms, fuzzy techniques, rough sets, and particle swarm intelligence. In addition, the authors propose two new algorithms, namely intelligent rule-based attribute selection algorithm for effective feature selection and intelligent rule-based enhanced multiclass support vector machine for efficient classification.

Acknowledgements
We would like to express our deep thanks to the Editor-in-Chief, Professor Luc Vandendorpe, for providing us the opportunity to host this special issue in *EURASIP Journal on Wireless Communication Networking*. We also thank all the authors who submitted their contributions to this special issue for publication consideration. Last but not the least, we are thankful for the thoughtful work of the many reviewers who provided invaluable evaluations and recommendations.

Author details
[1]Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190, China. [2]NEC Laboratories Europe, Heidelberg 69115, Germany. [3]School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, UK.

Received: 27 November 2013 Accepted: 2 December 2013
Published: 17 December 2013

doi:10.1186/1687-1499-2013-287
Cite this article as: Wu *et al.*: Introduction to advances in trust, security, and privacy for wireless networks. *EURASIP Journal on Wireless Communications and Networking* 2013 **2013**:287.