Editorial

Francesco Benedetto*

SP4TE – Signal Processing for
Telecommunications and Economics Lab,
University of ROMA TRE,
Via Vito Volterra 62, 00146 Rome, Italy
Email: francesco.benedetto@uniroma3.it
*Corresponding author

Arno Wacker

Applied Information Security,
Kassel University,
Pfannkuchstr. 1, 34121 Kassel, Germany
Email: arno.wacker@uni-kassel.de

With the proliferation of many innovative data communications services such as social networks, cloud computing, location-based service, and internet of things, security and privacy issues become more and more demanding and challenging. In addition, wireless physical layer secrecy has attracted much attention in recent years due to the broadcast nature of the wireless medium and its inherent vulnerability to eavesdropping. While recently published works on physical layer secrecy focus on the information-theoretic aspect, with this special issue we look specifically at the signal processing aspects of secure physical layer communications.

Our intent is to collect into this *IJMNDI* special issue relevant research contributions from academics and industry professionals in the signal processing area, as well from practitioners and engineers working on the security and privacy aspects of data communications and computer networks. It will also serve these scientific communities by presenting the state-of-the-art in signal processing methodologies and computer network security and fostering future research in this emerging area. This goal is herein pursued through the presentation of six articles as described below.

In the first paper, entitled 'Statistically-enhancing the diagnosis of packet losses in WSNs' by Tedeschi et al., the authors analyse an important class of adverse events in wireless sensor networks, namely packet losses, that can be caused by either misbehaving nodes, or attacks focused on the wireless links. Understanding the underlying cause is critical for effective response measures to restore network functionality. This work introduces a method that, exploiting resident metrics, such as the received signal strength indicator (RSSI) and the link quality indicator (LQI), profiles the wireless links between the nodes using, to accurately diagnose the root causes of the losses. In addition, the authors introduces a statistical model for determining optimal system thresholds based on the variances of RSSI and LQI, and also supporting individual per-link thresholds. The validation of the results is performed through real sensor data showing the accuracy of the model for underlying the causes of packet losses in wireless sensors networks.

In the second paper, entitled 'Specific buffer-aided full duplex relaying over LTE advanced networks' by Vijayarani and Nithyanandan, the security aspects of the full duplex relaying (FDR) technique are investigated. In particular, this emerging technique is used to transmit and receive simultaneously at the same frequency for enhancing the attainable spectral efficiency in long-term evolution advanced (LTE-A) network. However, since in case of FDR both transmission and reception are happening in same orthogonal channels, the increase in buffer length and higher delay deteriorates the system quality of service (QoS). To achieve both spectral efficiency and QoS, full duplex relay with separate buffers for receiving and re-transmitting is proposed in this paper, while keeping the security aspects into account. The optimal trusted relay selection scheme is incorporated for maximising the security with effective signal-to-interference and noise ratio, which significantly improves the relaying transmission and further tabu search-based metaheuristic algorithm is used for dealing with the trusted relay selection problem.

The third paper, 'From multilevel security to multiple independent levels of security/safety: the evolution illustrated through a novel cross-domain architecture' by Liguori, focuses on the so-called multiple independent levels of security/safety. In particular, multilevel security represents one of the toughest problems that security engineers are still facing, due to the fact that it is difficult to manage securely information at different classification levels on the same electronic device or network. It concerns wired and wireless communications, from personal area and wireless sensor networks to wide area and satellite networks. The problem becomes even more critical when

users with various clearance, privileges, and roles need to operate simultaneously on these security-motley data. This work discusses the evolution that drove the multilevel security into this new paradigm, highlighting the benefits and the drawbacks of the former together with the improvement of the latter and its open issues. A novel cross-domain solution is then presented as the thread in-between the two approaches.

The fourth paper of this special issue is 'Design of 3rd order cascaded multi-bit sigma delta modulator for ADC using internal feedback' by Sonika et al., and investigates the design of a new third order cascaded multi-bit sigma delta modulator for analogue to digital converter. The idea of the proposed architecture is to create extra feedback paths around the modulator to reduce errors, and hence to enhance the security of the system. The authors propose an improved version of cascaded multi-bit sigma delta modulator along with a third order cascaded low distortion ADC architecture to overcome these problems. Simulation results are finally provided to verify the superiority of both the proposed modulators.

The fifth paper, 'Decentralised trust-management inspired by ant pheromones' by Edenhofer et al., focuses on computational trust that is now increasingly utilised to select interaction partners in open technical systems consisting of heterogeneous, autonomous agents. Current approaches rely on centralised elements for managing trust ratings (i.e., control and provide access to aggregated ratings). Here, the authors propose a novel, decentralised trust mechanism inspired by the nestmate recognition system in ants. More precisely, the concept of recognition pheromones, which stick to the agents and cannot be removed or counterfeit, is turned into algorithmic logic and interaction protocols. They conclude their work by demonstrating the potential benefit by using simulations of the grid scenario.

The last paper of this special issue, entitled 'Simulating cheated results acceptance rates for gossip-based volunteer computing', by Kopal et al., discusses two different methods to estimate the dissemination rates of cheated results for decentralised distribution algorithms designed for volunteer computing networks. The authors first define gossip-based protocols and present a short taxonomy that is based on data sizes for categorisation of distribution algorithms. Then, they show three different distribution algorithms that are suitable for volunteer computing based on gossip-based protocols. Finally, to minimise the amount of needed cheat detection computations they either use simulations with the help of cellular automatons and a mathematical model to estimate the dissemination rates of cheated results.

Great thanks go to all of the authors for submitting their papers to this special issue and to all the reviewers for spending invaluable efforts to evaluate the submissions. The guest editors would also like to thank the Editor-in-Chief (EiC), Prof. Dr. M. Bartolacci, along with the Inderscience Publisher staff for their gentle assistance during the review and decision processes. Finally, we hope this special issue will be of interest for the readers and it may provide useful insights for achieving significant improvements in the field of signal processing, security and privacy for mobile/wireless and computer networks.