Lalitha Sankar, Wade Trappe,
Kannan Ramchandran,
H. Vincent Poor,
and Mérouane Debbah

Signal Processing for Cybersecurity and Privacy

Information technology and electronic communications have been rapidly applied to many spheres of human activity, including commerce, medicine, and social networking, resulting in huge volumes of data flowing across our networks to and from computers, where they are analyzed and deposited into databases for later retrieval. In this context, keeping data secure from malicious external adversaries (the security problem) and limiting the leakage of personal data (the privacy problem) are important problems with tremendous societal impact.

Traditionally, data security is ensured via cryptographic techniques. However, emerging systems require security and privacy mechanisms at all levels, from transmission to storage to access, which thus requires information protection techniques beyond traditional cryptography. The aim of this special issue of *IEEE Signal Processing Magazine* is to examine information security and privacy methods that complement traditional cryptographic services. The articles chosen survey the challenges associated with achieving security and privacy in both communications networks as well as distributed systems and identify signal processing approaches to protect information. Throughout this special issue are articles covering security and privacy, and thus it is worthwhile to differentiate between the two as privacy and security are related and often conflated. However, there are distinct differences: while the focus in security problems is on keeping data safe from malicious and illegitimate users, the privacy problem is concerned with curtailing inadvertent leakage or inference of correlated private information during a legitimate information transaction.

This special issue seeks to provide a venue for ongoing research on the signal and information processing approaches to the security and privacy problems. We received a total of 34 manuscripts, out of which eight high-quality articles were selected for publication after rigorous peer reviews. At a high level, the articles can be categorized as being focused on signal processing approaches to

- achieve secrecy at the physical layer of communication networks
- secure access control and identification via biometrics
- address security challenges in large distributed networks
- assure information privacy in data networks, databases, and more broadly, big data across applications.

We begin by focusing on the signal processing challenges for securing physical layer communications. Traditionally, the cryptographic approach to confidential communications between two entities, Alice and Bob, in the presence of an eavesdropper, Eve, exploits an advantage that Alice and Bob have over Eve (their sharing of an encryption key) to enable secrecy. In many communication settings, it is possible to find other sources of advantage that Alice and Bob share over Eve. For example, when Alice and Bob share a channel that is better than their opponent, they can make use of this advantage through proper coding to guarantee they can secretly share information that Eve cannot understand. Research in this area has explored the fundamental theory behind secret dissemination in wireless systems and several observations have emerged: 1) the fading process experienced in a typical wireless scenario is very special and can serve to enhances the ability to secretly communicate when compared to less harsh communication scenarios and 2) the broadcast nature of the wireless medium can be used to create interference that harms an adversary's ability to eavesdrop. We include three physical layer security articles.

The first contribution focuses on enhancing secure communications over the wireless medium. In this article, "Cooperative Security at the Physical Layer," by Bassily et al., the authors focus on guaranteeing confidentiality against eavesdropping attacks in which an unauthorized entity aims to intercept an ongoing wireless communication session and provide a comprehensive summary of recent advances in the area of physical layer security that guarantee confidentiality by using cooperative techniques unique to the wireless medium. These cooperative techniques consist of carefully designed coding and signaling schemes that harness the properties of the physical layer.

Hong et al. provide a signal processing framework to enhance secrecy at the physical layer level for multiantenna systems in the second article, "Enhancing Physical-Layer Secrecy in Multiantenna Wireless Systems." The signal processing framework involves two phases: a channel estimation phase and a data transmission phase. The channel estimation phase ensures that the channel is better estimated at the destination than at the eavesdropper. The data transmission phase uses signal processing techniques related to beamforming and precoding to enhance the signal quality at the destination while limiting the signal strength at the eavesdropper. The two phases in

Digital Object Identifier 10.1109/MSP.2013.2264854
Date of publication: 20 August 2013

combination enable a more favorable secrecy channel.

The third article focuses on constructive mechanisms to enable physical layer security. In "Coding for Secrecy" by Harrison et al., the authors discuss code constructions for physical layer security. Their approach is inspired by the success of coding schemes such as low-density parity check codes in resolving errors or discrepancies that occur between two parties. The authors present a variety of code constructions that provide information-theoretic confidentiality guarantees along with error-correcting capabilities over noisy channels.

As electronic information sources grow, the problem of ensuring secure access to the data becomes imperative. In "Secure Biometrics," by Rane et al., the authors focus on this problem using biometrics. Biometrics are attractive because they make use of inherent properties of individuals to identify them and thus need not be remembered like passwords and are not easily lost or forged. At the same time, biometrics are fundamentally noisy and irreplaceable. There are always slight variations among the measurements of a given biometric, and unlike passwords or identification numbers, biometrics are derived from physical characteristics that cannot easily be changed. The proliferation of biometric usage raises critical privacy and security concerns that, due to the noisy nature of biometrics, cannot be addressed using cryptography. In their article, the authors discuss the tradeoffs between biometric security and the privacy of the biometric itself and present an overview of an emerging class of methods known as "biometric template protection" that address these concerns.

Advances in communication and device technology have given rise to the use of sophisticated sensors for data collection and monitoring in a variety of applications and networks including critical infrastructure networks such as the electric grid. Distributed sensors can enable fine-grained monitoring, inference, and control over multiple time scales and are essential for guaranteeing reliability. Ensuring that the data from these sensors are not corrupted by malicious adversaries is the topic of the article "Distributed Inference in the Presence of Byzantine Data" by Vempaty et al. The article provides an overview of the state of the art in distributed inference in the presence of such attacks involving corrupt insiders (Byzantines) who operate maliciously by falsifying data, but continue to operate within the context of the application/protocol at hand. The authors detail the effect of such attacks on critical networks such as the electric grid and discuss mitigating strategies.

Yet another domain rife with privacy and security challenges is that of network traffic monitoring. Recent work has shown that it is possible to infer a significant amount of sensitive information in a communication flow by examining the contextual information contained in the timing between packets, even if the underlying communication flow is encrypted. In "Preventing Timing Analysis in Networks," Kadloor et al., focus on addressing security and privacy breaches associated with the temporal patterns underlying network traffic. This article surveys techniques that limit the ability of an adversary to engage in statistical inference using timing information. The techniques presented draw heavily upon information-theoretic and signal processing methods to smoothly adjust the tradeoff between the penalties associated with introducing false traffic and the privacy gains associated with obfuscation methods.

Guaranteeing privacy of individuals and organizations whose data is stored in distributed repositories requires tools quite different from security methods to protect contextual information from being gleaned by potential insider inference. There have been a number of privacy models and privacy-preserving data analysis algorithms to answer these challenges. One such recent framework is differential privacy, introduced and developed by the theoretical computer sciences community that enables quantifying the exposure (privacy) of any record in a database. This framework has lent itself to develop privacy-guaranteed approaches to learning and inference on the data. In "Signal Processing and Machine Learning with Differential Privacy," Sarwate and Chaudhuri survey the area of differential privacy signal processing and machine learning.

Electronic data sources exist to be used and have tremendous value (utility) to their users and collectors; on the other hand, they raise important privacy concerns, leading to a tension between privacy and utility. Modeling both utility and privacy explicitly for any application can enable understanding the tradeoff between the two conflicting goals.

The final article, "The Role of Signal Processing in Meeting Privacy Challenges," by Sankar et al., surveys privacy-utility tradeoff and motivates an information-theoretic framework with signal processing solutions to the tradeoff problem. The article surveys the application of the framework via a number of case studies to illustrate concretely how signal processing can be harnessed to provide data privacy.

In closing, we would like to thank all of the authors who submitted their manuscripts to this special issue and the reviewers who provided valuable reviews in a timely manner. Thanks are also extended to Rebecca Wollman for her professional assistance in the article review and publication process. Finally, we thank Dr. Fulvio Gini, *IEEE Signal Processing Magazine's* area editor of special issues, for his guidance and help throughout the process.

As digital interactions and electronic information sources become pervasive, the privacy and security challenges across a number of domains will continue to rise, some with tremendous social costs. While there have been many rigorous research efforts in the last few years toward understanding these challenges, the articles in this special issue offer many avenues for future research with obvious practical relevance. We are confident that this nascent field will continue to flourish both in theory and in practice. [SP]