Guest Editorial: Special Issue on Security and Privacy of Distributed Algorithms and Network Systems

I. Introduction

THE integration of computation, communication, and control technologies has led to the widespread emergence of large scale engineering systems. These network systems are deployed in numerous fields, including electric and smart grids, transportation and smart cities, health-care and manufacturing, and so forth. Due to the rapid growth in number of geographically deployed units, such as sensors, computers and controllers, traditional centralized control and optimization algorithms may not be efficient, robust, or even applicable at all. Instead, distributed control and optimization algorithms offer a promising and desirable approach to operate and guarantee the well functioning of network systems. They have the advantage of being flexible, scalable, robust, and efficient. However, due to their very nature, distributed algorithms are particularly vulnerable to cyber and physical attacks. Security and privacy issues of distributed control and optimization algorithms are critical in network systems and, if not addressed properly, can result in critical economic losses and even threats to human safety.

Due to the above scenario, recently there has been rapidly growing scientific and industrial interest in security and privacy of distributed algorithms in network systems. While many scientific disciplines have contributed to security and privacy, the control systems community seems to have ignored these issues although it has been consistently engaged in the development of theories, tools, and practices for the design and operation of network systems. The aim of this special issue is to provide a window into the recent developments of the fundamentals and applications of security and privacy of distributed algorithms in network systems.

II. Issue at a Glance

This special issue is expected to link recent theoretical developments in security and privacy of distributed control and optimization algorithms in network systems with practical technological applications. In response to the call for papers, we have received 45 submissions, out of which 10 full papers and 10 technical notes were selected for the special issue after a rigorous peer review process. The selected papers cover a broad range of topics, all centered around the use of tools and methods from the systems and control perspective to address security and privacy issues of distributed algorithms in network systems. The first fundamental cornerstone for building an insight into security and privacy of network systems lies in proper attack models. Then, developing efficient intrusion detection methods becomes critical to identify and locate the attacks. Based on that, one core goal is to design resilient estimation and control algorithms to enhance the privacy and security of network systems. When the results are satisfactorily evaluated in terms of specific metrics, the theoretical tools and techniques can be finally applied to real industrial systems to further improve their performance. Within this broad overview, we organized the accepted papers into five main categories in this special issue: attack modeling, intrusion detection, resilient and privacy-preserving estimation and control, security metrics of estimation and control, and applications.

A. Attack Modeling

The attack surface refers to all the components of the system that can be exploited by an attacker. These include software, hardware, and network protocols. The attack surface of network systems has been enlarged due to the wide usage of communication and computation technologies. Attack modeling is to document attacks in a structured and reusable form, so that they can be used to develop more secure and survivable network systems. Four of the papers address challenges related to such attack modeling of network systems. The paper by Lu and Yang studies malicious attacks against distributed control systems, which can worsen estimation performance by compromising partial communication links. It is shown that the existence of perfect attacks is caused by the null-space of the system, and an effective attack mechanism is designed accordingly. Meanwhile, if the capability of the attacker is restricted, i.e., the number of compromised communication links is limited, both off-line and on-line nonperfect attack strategies are developed, where the on-line attacker uses the system measurements to enlarge the attacks' influence. He *et al.* investigate how random and impulsive sequential attacks affect the stability of a class of Lipschitz-type nonlinear systems in networked environments. With available expectations of impulsive instants and gains, sufficient conditions are derived to ensure almost sure stability based on Doob's martingale convergence theorem. Stealthy actuator signal attacks are modeled for stochastic control systems in the paper by Fang *et al.*, where the attack detector applies a hypothesis test on the innovation of the Kalman filter. It is shown that the attack can keep stealthy by limiting achievable false alarm probability and the detection probability below a

Digital Object Identifier 10.1109/TAC.2020.3004329

certain threshold. Given a specific level of stealthiness, sufficient conditions on attacks and the upper bound of system degradation are also obtained. Gan *et al.* study the optimal attack scheduling problem against state estimation over a two-hop relay network, where both channel selection and limited energy of attacks are considered to maximize the effect of attacks. For the time-varying dropout rate, the problem is formulated as a mixed-integer programming problem and a dynamic energy dispatch algorithm is developed to approach the optimal attack scheduling. Meanwhile, for the time-invariable dropout rate, an analytical expression of the optimal attack is obtained.

B. Intrusion Detection and Defense

Effective detection is crucial for establishing resilience control, attack identification, and isolation for network systems. Reacting to and recovering from an attack is greatly contingent on reliable, timely attack detection. Five papers are devoted to intrusion detection and defense problems for network systems. The paper by Liu *et al.* considers a replay attack detection problem for a linear time-invariant system by watermarking technology, where system parameters are required to be identified online. A physical watermarking scheme is proposed to detect replay attacks by using a random input as a watermark. The tradeoff between control performance and intrusion detection is achieved optimally by solving a watermark signal design optimization problem. Anguluri *et al.* study the relationship between centralized and decentralized detectors against exogenous attacks by processing measurements at different locations for interconnected systems. It is shown that the decentralized detector can outperform the centralized one if the system and the attack systems are appropriately designed, which is caused by the fundamental nature of the hypothesis testing attack detection problem. The paper by Mao *et al.* investigates novel attack strategies and the corresponding detection schemes for multiagent control systems under zero dynamics attacks. This article focuses on how to deal with stealthy attacks for the dynamic switching topology-based scenario. First, combining zero dynamic attack strategies with stealthy topology attacks, the stealthiness of attacks is analyzed and the detectability is obtained. Then, a strategic topology switching algorithm is proposed to detect the attack through a Luenberger observer while the privacy requirements are met. Peng and Sun develop a switching-like event-triggered control strategy for network control systems under malicious denial of service attacks, where communication efficiency can be improved and the desirable control performance is maintained. A time-delay system model is obtained to characterize the system performance and security in a unified way. In the paper by Barboni *et al.*, how to distributedly detect covert attacks for large-scale interconnected linear systems is addressed, where bounded processes and measurement disturbances are considered. Based on decentralized and distributed observers, a local detection strategy is proposed. A sufficient condition ensures that covert attacks are detectable by the proposed strategy when only one neighbor subsystem is manipulated by the attacks. Moreover, upper bound of detection time and estimation errors are analyzed thoroughly.

C. Resilient and Privacy-Preserving Estimation and Control

Resilience is an important system property. It reflects the ability to contain the maximum impact of an attack and to operate as close to normal as possible. Privacy disclosure may cause attack surface disclosure and thus property losses. Therefore, designing resilient and privacy-preserving estimation and control strategies is crucial to ensure system security against malicious attacks. Six papers deal with the problem of resilience and privacy preservation for estimation and control in network systems. In the paper by Wang and Wang, a new pulse-based mechanism is proposed to improve the synchronization resilience of pulse-coupled oscillators under general connection topologies. It is shown that the proposed mechanism ensures perfect synchronization of legitimate oscillators under stealthy Byzantine attacks and the resilience property is even achieved when the initial phases of legitimate oscillators are widely distributed in a half circle. Su and Shahrampour study the problem in which multiagents collaboratively estimate system parameters, while an unknown subset of agents suffer Byzantine attacks. A computationally-efficient algorithm is proposed that utilizes coordinate-wise trimmed means against Byzantine agents. Given mild technical assumptions, normal agents can estimate the true parameters asymptotically and finite-time convergence is also ensured with a high probability. In the paper by Lee *et al.*, a distributed median solver-based state estimation method is proposed, which is resilient to malicious sensor attacks. The paper by Hadjicostis and Dominguez-Garcia deals with the privacy of distributed average under directed topologies in the presence of curious but not malicious nodes. Conflictingly, initial states of all nodes have integer values, which makes the weights set and all operations challenging to be solved. A homomorphic-encryption-based ratio consensus is shown to be able to perform integer operations to ensure all node' states converging to average while initial states can be preserved. Furthermore, a secure and privacy-preserving dynamic controller design problem for linear time-invariant systems is considered in the paper by Murguia *et al.* To solve the problem, Pailier's encryption is applied to the outputs and the states of the controllers and the states are also reset periodically to avoid overflow and underflow within the encryption domain. Next, stability of the closed-looped system is analyzed. Kawano and Cao study a differentially private controller design problem, where the relationship between input observability and privacy requirements is analyzed and dynamic privacy-preserving controllers are designed for classic tracking control problems.

D. Security Metrics of Estimation and Control

Security metrics are to characterize system properties and performance in the presence of malicious attacks. They play a key role in designing survivable control and estimation strategies for network systems. Two papers address the security metric development for network systems. The paper by Ren *et al.* introduces a new performance metric for secure state estimation with Byzantine sensors. The new metric quantifies the asymptotic decay rate for the probability that an estimation error is larger than a given threshold. With this metric, an optimal estimator is developed. When sensors are homogeneous, an optimal estimator is proposed for every threshold. In the paper by Milošević *et al.*, a new actuator security index is developed to localize and protect vulnerable actuators in a networked control system. It is shown that the index can be increased by placing additional sensors for small-scale systems. To deal with NP-hardness and sensitivity of the index computation, a robust index is proposed to overcome any system realization, which can be computed in polynomial time. The robust index optimization problem for the placement of two sensors is formulated and analyzed to have submodular structure, and thus can be computed suboptimally in polynomial time.

E. Applications

There are many network systems applications to be investigated where distributed algorithms play a key role. Three papers are devoted explicitly to applications, specifically, power systems and transaction systems. Gallo *et al.* propose a distributed scheme to detect cyber-attacks for linear large-scale systems with its application to dc microgrids. In the detection scheme, a Luenberger observer together with a bank of unknown-input observers is placed at each subsystem. Conditions are derived to ensure the detection/nondetection of attacks. It is also shown that there exist some classes of undetectable attacks using modules independently and the detection property can be improved by using modules simultaneously. Wu *et al.* investigate false data injection attacks in cyber-physical power systems, where the attack is established based on partial feedback of generator frequencies to destabilize the system with a minimum cost. A location-fixed attack planning problem and a location switching attack design problem are formulated as switched control problems. Explicit solutions for a diagonal partial feedback matrix as well as convexified switching variables are derived by quadratic and fractional programming. In the paper by Ferraro *et al.*, a directed acyclic graphs (DAG)-based distributed ledger is modified for transaction-based applications. This article focuses on establishing fluid models of the IOTA DAG behavior and includes Monte-Carlo-inspired tip selection algorithms leading to the a partial-differential-equation-based approximation of tangle. Then, a new tip selection algorithm is developed to ensure that all transactions are validated in finite time.

III. Conclusion

In this special issue, many novel methods based on control theory and optimization are developed to furnish the essential tools to address security and privacy concerns in distributed algorithms and network systems. Results range from initial attack modeling to final practical applications, where each part is critical and plays a key role in enhancing high and stringent performance of future cyber–physical coupling and smart network systems.

Because practical network systems are complex, there are some other related topics that are not covered in this special issue. For example, how to make group decisions under both security and privacy constraints as well as self-healing and self-recovery remains open. Also, considering the tight integration of layered communication networks and dynamical physical coupling, it is desirable and challenging to solve security and privacy issues in a more systematic way. Moreover, security and privacy issues in high-dimensional systems, machine learning, multisystem cooperation as well as their applications are also worth further exploration. Previous achievements and current challenges point to a very fruitful future for systems and control theoretic research in the field of secure and privacy-preserving distributed algorithms in network systems.

Acknowledgment

The guest editors would like to thank all the authors, for their submissions, and a large number of reviewers, who carefully and timely scrutinized and evaluated the many papers submitted.

Zhiyong Chen, *Guest Editor*
School of Electrical Engineering and Computing
The University of Newcastle
Callaghan, NSW 2308, Australia

Fabio Pasqualetti, *Guest Editor*
Department of Mechanical Engineering
University of California
Riverside, CA 92521 USA

Jianping He, *Guest Editor*
Department of Automation
Shanghai Jiao Tong University
Shanghai 200240, China

Peng Cheng, *Guest Editor*
College of Control Science and Engineering
Zhejiang University
Hangzhou 310027, China

Harry L. Trentelman, *Guest Editor*
Johann Bernoulli Institute for Mathematics and
Computer Science
University of Groningen
9712 CP Groningen, The Netherlands

Francesco Bullo, *Guest Editor*
Department of Mechanical Engineering
University of California
Santa Barbara, CA 93106 USA