ERCIM "ALAIN BENSOUSSAN"
FELLOWSHIP PROGRAMME

Scientific Report

First name / Family name	Naveen Kumar Dasanadoddi Venkategowda
Nationality	India
Name of the *Host Organisation*	NTNU-Norwegian University of Science and Technology
First Name / family name of the *Scientific Coordinator*	Stefan Werner
Period of the fellowship	01/10/2017 to 30/09/2018

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

Wireless sensor networks (WSN) are ubiquitous with wide spread use in safety-critical applications such as smart grids, environmental monitoring, infrastructure, transportation etc. WSNs consist of sensor nodes having sensing, computations, communication and power components distributed over a geographical area to observe the phenomena of interest. In a generic WSN, multiple sensors distributed over a geographical area observe a source process and these observations are processed and shared with the neighbouring nodes in case of a distributed WSN or transmitted to fusion center in case of a centralized WSN over a wireless communication network. The sensors accomplish various tasks such as monitoring/inference activities, for e.g., source parameter estimation and event detection.

However, these networks are vulnerable to threats due to use of open wireless communication networks and physical tampering of the sensor nodes. Unlike conventional data security, attacks on WSN influence the physical processes and have significant impact on the environment, national security, and loss of property. Incidents such as the attack on Ukraine's power-grid, StuxNet attack on an industrial infrastructure, Sentinel UAV capture have shown the risk and far-reaching effects of the attacks on economy and safety. Hence, developing solutions to mitigate the threat and assure safe operation of WSN is imperative. The attacks can be broadly categorized into 1) denial

of service where adversaries block the communication between different agents, 2) false data injection where adversaries add malicious data by physically tampering the sources or by hacking the communication channels, and 3) loss of privacy when adversaries gain unauthorized access to private and sensitive data.

Conventional security deals only with the integrity of data and does not consider the effects of the attacks on the physical systems. The security protocols are limited to securing the networks through authentication techniques that prevent impersonation and access control that restricts mala fide entities accessing the network. Though such protocols enhance the security and form a first line of defence, they can be breached and are not perfect due to hidden software and hardware vulnerabilities, design flaws, human error, among many other factors. In summary, the existing research in security mainly focuses on preventive mechanisms and do not address the recovery and operability of WSN under attacks.

Therefore, the central theme of our research is to develop signal processing and communication techniques that enable WSN to survive and continuously function under the attacks. In particular, we investigate signal processing and communication schemes to guarantee privacy such that the global objective of WSN is achieved while the adversary is unable to acquire or learn sensitive information.

We consider the decentralized estimation setting in a WSN where the sensor nodes transmit their observations of the source to the fusion center that estimates the parameter of interest. The observation noise and the noisy fading wireless channel between the sensors and fusion center degrades the estimation accuracy. However, transceivers can be designed to minimize these ill effects by utilizing the knowledge of channel state information and sensor observation model information. Precoding enables us to exploit the multiple access channel to coherently combine the transmissions from the sensor nodes over the channel, and thus leading to diversity and array gain, which enhance the estimation accuracy. However, the local sensor information and the sensor measurements are sensitive and must be protected from leaking to unauthorized agents. Conventional cryptographic security solutions are prohibitively demanding in resources to employ them in WSNs. Hence, we studied low complex algorithms for physical layer security and privacy in WSNs.

In many applications the sensors might be unwilling to share their observation models and CSI due to privacy and security concerns. For instance, in radar sensor networks the observation matrices contain sensitive information such as codes, timing, and location that cannot be revealed to other entities. In these scenarios, it is imperative that the network designs the precoders and the fusion rule with information privacy requirements i.e. without sharing the CSI, observations or observation models directly. For such networks, we propose an iterative distributed algorithm to compute the precoders and fusion rule while protecting the privacy of the sensor nodes. As the minimum mean square error estimation framework results in a intractable objective function, we derive an upper bound on the optimal error that is used to optimize the WSN. To ensure information privacy, we employ alternating direction method of multipliers and privacy-preserving average consensus to solve the dual of the error minimization problem in a distributed manner. In this approach, at each iteration, the sensor nodes update their precoder and share the local perturbed dual variable to their neighbouring nodes. We prove that the proposed algorithm is privacy-preserving and derive limits on privacy guaranteed for the sensor nodes. In addition, since the agents in WSN have stringent computational, energy, real-time operational constraints, the proposed data processing algorithms are designed to have low computational complex and consume minimal resources.

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

[1] N. K. D. Venkategowda and S. Werner, "Privacy-preserving distributed precoder design for decentralized estimation," *in proceedings of 2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP),* Nov. 2018, pp. 1–5.

Abstract: We study privacy-preserving precoder design for decentralized estimation in wireless sensor networks where the sensor nodes want their local information such as the channel state information, observation matrices, and observation covariance matrices to be private. We propose a distributed algorithm with closed form expressions to design the precoders and fusion rule that minimize the estimation error by exchanging messages which do not reveal the local information. We derive the privacy limits offered by the proposed algorithm and prove that the algorithm is privacy-preserving. Simulation results illustrate the trade-off between privacy and estimation accuracy of the proposed algorithm.

[2] C. Gratton, N. K. D. Venkategowda, R. Arablouei, and S. Werner, "Distributed ridge regression with feature partitioning," *in proceedings of 2018 Asilomar Conference on Signals, Systems and Computers,* Oct. 2018, pp. 1–5.

Abstract: We develop a new distributed algorithm to solve the ridge regression problem with feature partitioning of the observation matrix. The proposed algorithm, named D-Ridge, is based on the alternating direction method of multipliers (ADMM) and estimates the parameters when the observation matrix is distributed among different agents with feature (or vertical) partitioning. We formulate the associated ridge regression problem as a distributed convex optimization problem and utilize the ADMM strategy to iteratively obtain a solution. Numerical results demonstrate that the D-Ridge algorithm converges faster in comparison to the diffusion approach.

[3] N. K. D. Venkategowda and H. B. Mishra, "Optimal energy transmission for decentralized detection in wireless powered sensor networks," *in proceedings of 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall),* Aug. 2018, pp. 1–5.

Abstract: In this paper, we study energy transmission for decentralized detection in wireless powered sensor networks (WPSN) in which the sensor nodes are powered by harvesting the radio frequency signals transmitted from dedicated energy access points (E-AP). We present a joint design of the transmit covariance matrices at E-APs and sensor precoders to minimize the probability of error. To this end, we maximize the error exponents by employing Dinkelbach's method and semidefinite relaxation. We present an iterative algorithm to solve the relaxed problem and prove that the relaxation is tight. Simulation results demonstrate that the proposed design results in a superior detection performance in comparison to the conventional techniques.

III – ATTENDED SEMINARS, WORKHOPS, CONFERENCES

1. Telenor-NTNU AI Lab tutorial series on deep reinforcement learning 24 October to 21 November 2017.
2. NTNU-Institute of Statistical Mathematics, Tokyo joint workshop on Sustainability and Machine Learning, 04-05 June 2018.
3. Short course on multiuser detection by Prof. Ralf Muller, Friedrich-Alexander Universitat Erlangen-Nurnberg during 08-09 August 2018 at NTNU.
4. Short course on multiuser large scale analysis by Prof. Ralf Muller, Friedrich-Alexander Universitat Erlangen-Nurnberg during 09-10 August 2018 at NTNU.
5. Asilomar Conference on Signals, Systems and Computers, Pacific Grove, USA, from 28-31 October 2018.

IV – RESEARCH EXCHANGE PROGRAMME (REP)

From 24/09/2018 to 28/09/2018, I visited VTT Technical Research Centre of Finland, Helsinki and was hosted by Senior Scientist Pirkko Kuusela. During this visit, I presented my research on privacy in distributed estimation in wireless sensor networks and held discussions with the members of Big data Industrial Applications group to explore potential avenues for collaboration. The research exchange program helped me network with scientists at VTT sharing similar research interests and build collaborative partnerships.