0.1 Abstract

With a burgeoning number of IoT devices penetrating into all aspects of our lives, seemingly endless privacy-related concerns are surfacing. To embrace the convenience brought by IoT devices, privacy consideration should be incorporated into the core design of IoT solutions, where customers have more control over what information can be inferred about them and what data is collected about them. We model the sensor network with decentralized detection framework, where each sensor make a local decision based on its observation of hypotheses, and transmit the local decision to the fusion center. The fusion center make inferences based on the received sensor decisions. In this thesis, we aim to find privacy mapping at each sensor to distort sensor observations before send to the fusion center, such that privacy is protected, while still enabling the fusion center to make accurate detection of the public hypothesis.

Firstly, we consider protecting information privacy of private hypothesis without assuming knowledge of joint distribution of the sensor observations and hypotheses. Here, we call a hypothesis a public hypothesis if its inference or detection is to be achieved by a sensor network specifically designed for this purpose, whereas we call a hypothesis a private hypothesis, if its true state is not authorized to be detected or inferred from the observations about it. We introduce the concept of an empirical normalized risk, which provides a theoretical guarantee for the network to achieve information privacy for the private hypothesis with high probability when the number of training samples is large. We develop iterative optimization algorithms to determine an appropriate privacy threshold and the best sensor privacy mappings, and show that they converge. Finally, we extend our approach to the case of a private multiple hypothesis.

Secondly, we consider protecting information privacy of a set of private hypotheses with known joint distribution of the sensor observations and hypotheses. We consider the fact that privacy concern is usually not about a single hypothesis, small deviation from a nominal private hypothesis should also be kept private from the fusion center. We find a representative private hypothesis, which is the easiest to detect among the set of private hypotheses. We propose an algorithm, by protecting the information privacy of the representative private hypothesis, the information privacy of the set of private hypotheses is protected. We consider the two cases where the number of sensors is finite and infinite respectively.

Finally, we discuss the relationship between various privacy metrics proposed in the literature. We divide the privacy metrics into inference privacy and data privacy. Here, data privacy refers to the concealment of sensors raw

observation from the fusion center, while reducing the disclosure of private states of the object to the fusion center is inference privacy. We show that inference and data privacy are in general not equivalent. We propose methods to protect both inference and data privacy in decentralized detection, by incorporating local differential privacy (data privacy) and information privacy (inference privacy) metrics. We consider both case with and without the known prior knowledge of the sensor observations distribution.

List of my Publications

[1] M. Sun, W. P. Tay, and X. He. Toward information privacy for the internet of things: A nonparametric learning approach. *IEEE Transactions on Signal Processing*, 66(7):1734–1747, April 2018.

[2] Meng Sun and Wee Peng Tay. Privacy-preserving nonparametric decentralized detection. In *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, pages 6270–6274, Shanghai, 2016.

[3] Xin He, Wee Peng Tay, and Meng Sun. Privacy-aware decentralized detection using linear precoding. In *Proc. IEEE Sensor Array and Multichannel Signal Processing Workshop*, pages 1–5, Rio de Janeiro, 2016.

[4] Meng Sun and Wee Peng Tay. Inference and data privacy in iot networks. In *Proc. IEEE Int. Workshop Signal Processing Advances*, Sapporo, 2017.