Perspectives on Probabilistic Graphical Models

DONG LIU

Doctoral Thesis in Electrical Engineering
Stockholm, Sweden 2020

Devision of Information Science and Engineering
TRITA-EE XXXX KTH, School of Electrical Engineering and and Computer Science
ISSN .... SE-100 44 Stockholm
ISBN .... SWEDEN

Akademisk avhandling som med tillstånd av Kungl Tekniska högskolan framlägges till offentlig granskning för avläggande av teknologie doktorsexamen i Elektroteknik onsdag den 13 september 2017 klockan 13.15 i F3, Lindstedtsvägen 26, Stockholm.

Tryck: Universitetsservice US AB

To my beloved

Abstract

Sammanfattning

Acknowledgements

Contents

Acronyms and Notations

Notations

X	random variable
x	realization of the random variable X
$\mathcal{X}$	alphabet of the random variable X
X_i^k	random sequence $(X_i, \ldots, X_k)$
x_i^k	realization of the random sequence X_i^k
$\mathcal{X}_i^k$	alphabet of the random sequence X_i^k
X^k	random sequence $(X_1, \ldots, X_k)$
x^k	realization of the random sequence X^k
$\mathcal{X}^k$	alphabet of the random sequence X^k
$X_i^{k\backslash n}$	random sequence $(X_i, \ldots, X_{n-1}, X_{n+1}, \ldots, X_k)$
$x_i^{k\backslash n}$	realization of the random sequence $X_i^{k\backslash n}$
$\mathcal{X}_i^{k\backslash n}$	alphabet of the random sequence $X_i^{k\backslash n}$
$X^{k\backslash n}$	random sequence $(X_1, \ldots, X_{n-1}, X_{n+1}, \ldots, X_k)$
$x^{k\backslash n}$	realization of the random sequence $X^{k\backslash n}$
$\mathcal{X}^{k\backslash n}$	alphabet of the random sequence $X^{k\backslash n}$
$\|\| \cdot \|\|$	set cardinality
f_X	p.d.f. of the continuous random variable X
p_X	p.m.f. of the discrete random variable X
$\mathcal{N}(\mu, \sigma^2)$	normal distribution with mean μ and variance σ^2

$\mathrm{D}(\cdot\|\|\cdot)$	Kullback-Leibler divergence
$\mathrm{D}_\tau(\cdot\|\|\cdot)$	τ-th order Rényi divergence
$\mathrm{C}(\cdot,\cdot)$	Chernoff information
$\mathrm{E}[\cdot]$	expectation
$\partial\cdot$	boundary of a closed set
$\hat{\partial}\cdot$	upper boundary of a two-dimensional closed set
$\check{\partial}\cdot$	lower boundary of a two-dimensional closed set
$\log(\cdot)$	natural logarithm

Chapter 1

Introduction

Motivate the research in probabilistic models.

1.1 Motivations

1.2 Thesis Outline

Chapter 2

Background

Background on probabilistic graphical models

2.1 Directed and Undirected graphs

.

2.2 Dealing with latent variables

Chapter 3

An alternative view of belief propagation

Content:

1. α Belief Propagation as Fully Factorized Approximation, GlobalSIP 2019.
2. α Belief Propagation for Approximate Bayesian Inference, under review.

3.1 α belief propagation

3.2 Convergence study

3.3 Experimental results

Chapter 4

Region-based Energy Neural Network Model

work in Region-based Energy Neural Network for Approximate Inference, under, review

4.1 Region-based graph and energy

4.2 RENN model for Approximate Inference

4.3 RENN model for markov random field training

4.4 Experimental results

Chapter 5

Powering the expectation maximization method by neural networks

content: Neural Network based Explicit Mixture Models and Expectation-maximization based Learning, under review

5.1 Normalizing flow

5.2 expectation maximization of neural network based mixture models

5.3 An alternative construction method

5.4 Experiments

Chapter 6

Powering Hidden Markov Model by Neural Network based Generative Models

content:

1. Powering Hidden Markov Model by Neural Network based Generative Models, ECAI 2020
2. Antoine Honore, Dong Liu, Hidden Markov Models for sepsis detection in preterm infants, ICASSP, 2020

6.1 Hidden Markov Model

6.2 GenHMM

6.3 Application to phone recognition

6.4 Application to sepsis detection in preterm infants

Chapter 7

An implicit probabilistic generative model

content: Entropy-regularized Optimal Transport Generative Models, ICASSP 2019

7.1 Modeling data without explicit probabilistic distribution

7.2 Employing EOT for modeling

7.3 Experimental results

Chapter 8

Conclusion and Discussions

Bibliography

[1] URL `http://www.eugdpr.org/`.

[2] T. C. Aysal and K. E. Barner. Sensor data cryptography in wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 3(2): 273–289, 2008.

[3] R. F. Barber and J. C. Duchi. Privacy and statistical risk: Formalisms and minimax bounds. eprint arXiv:1412.4451.

[4] R. S. Blum, S. A. Kassam, and H. V. Poor. Distributed detection with multiple sensors: Part II - Advanced topics. *Proceedings of the IEEE*, 85(1):64–79, 1997.

[5] Z. Cao, J. Hu, Z. Chen, M. Xu, and X. Zhou. Feedback: Towards dynamic behavior and secure routing for wireless sensor networks. In *Proceedings of AINA 2006*, pages 160–164, 2006.

[6] C. Dwork. Differential privacy. In *Proceedings of ICALP 2006*, pages 1–12, 2006.

[7] G. Giaconi, D. Gündüz, and H. V. Poor. Smart meter privacy with an energy harvesting device and instantaneous power constraints. In *Proceedings of ICC 2015*, pages 7216–7221, 2015.

[8] S. Goel and R. Negi. Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications*, 7(6):2180–2189, 2008.

[9] D. Gündüz and J. Gómez-Vilardebó. Smart meter privacy in the presence of an alternative energy source. In *Proceedings of ICC 2013*, pages 2027–2031, 2013.

[10] X. Guo, A. S. Leong, and S. Dey. Estimation in wireless sensor networks with security constraints. *IEEE Transactions on Aerospace and Electronic Systems*, PP(99):1–1, 2017.

[11] H. Jeon, J. Choi, S. W. McLaughlin, and J. Ha. Channel aware encryption and decision fusion for wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 8(4):619–625, 2013.

[12] H. Jeon, D. Hwang, J. Choi, H. Lee, and J. Ha. Secure type-based multiple access. *IEEE Transactions on Information Forensics and Security*, 6(3):763–774, 2011.

[13] Z. Ji, Z. C. Lipton, and C. Elkan. Differential privacy and machine learning: A survey and review. eprint arXiv:1412.7584.

[14] P. Kairouz, S. Oh, and P. Viswanath. The composition theorem for differential privacy. In *Proceedings of the 32nd International Conference on Machine Learning*, pages 1–10, 2015.

[15] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda. Privacy for smart meters: Towards undetectable appliance load signatures. In *Proceedings of SmartGridComm 2010*, pages 232–237, 2010.

[16] K. Kittichokechai, T. J. Oechtering, and M. Skoglund. Secure source coding with action-dependent side information. In *Proceedings of ISIT 2011*, pages 1678–1682, 2011.

[17] J. Le Ny and G. J. Pappas. Differentially private filtering. *IEEE Transactions on Automatic Control*, 59(2):341–354, 2014.

[18] F. Li, B. Luo, and P. Liu. Secure information aggregation for smart grids using homomorphic encryption. In *Proceedings of SmartGridComm 2010*, pages 327–332, 2010.

[19] S. Li, A. Khisti, and A. Mahajan. Structure of optimal privacy-preserving policies in smart-metered systems with a rechargeable battery. In *Proceedings of SPAWC 2015*, pages 375–379, 2015.

[20] Z. Li and T. J. Oechtering. Privacy on hypothesis testing in smart grids. In *Proceedings of ITW 2015 Fall*, pages 337–341, 2015.

[21] D. Liu, P. Ning, S. Zhu, and S. Jajodia. Practical broadcast authentication in sensor networks. In *Proceedings of MobiQuitous 2005*, pages 118–129, 2005.

[22] S. Marano, V. Matta, and P. K. Willett. Distributed detection with censoring sensors under physical layer secrecy. *IEEE Transactions on Signal Processing*, 57(5):1976–1986, 2009.

[23] M. Mhanna and P. Piantanida. On secure distributed hypothesis testing. In *Proceedings of ISIT 2015*, pages 1605–1609, 2015.

[24] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin. Private memoirs of a smart meter. In *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, pages 61–66, 2010.

[25] V. Nadendla. Secure distributed detection in wireless sensor networks via encryption of sensor decision. Master's thesis, Louisiana State University, 2009.

[26] V. S. S. Nadendla, H. Chen, and P. K. Varshney. Secure distributed detection in the presence of eavesdroppers. In *Proceedings of ASILOMAR 2010*, pages 1437–1441, 2010.

[27] S. Schmidt, H. Krahn, S. Fischer, and D. Wätjen. A security architecture for mobile wireless sensor networks. In *Proceedings of the First European Conference on Security in Ad-hoc and Sensor Networks*, pages 166–177, 2005.

[28] A. Smith. Privacy-preserving statistical estimation with optimal convergence rates. In *Proceedings of the Fourty-Third Annual ACM Symposium on the Theory of Computing*, pages 813–822, 2011.

[29] R. Soosahabi, M. Naraghi-Pour, D. Perkins, and M. A. Bayoumi. Optimal probabilistic encryption for secure detection in wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 9(3):375–385, 2014.

[30] F. Sultanem. Using appliance signatures for monitoring residential loads at meter panel level. *IEEE Transactions on Power Delivery*, 6(4):1380–1385, 1991.

[31] O. Tan, D. Gündüz, and H. V. Poor. Increasing smart meter privacy through energy harvesting and storage devices. *IEEE Journal on Selected Areas in Communications*, 31(7):1331–1341, 2013.

[32] E. Tekin. The Gaussian multiple access wire-tap channel: Wireless secrecy and cooperative jamming. In *Proceedings of ITA 2007*, pages 404–413, 2007.

[33] J. N. Tsitsiklis. Decentralized detection. In *Proceedings of Advances in Statistical Signal Processing*, pages 297–344, 1993.

[34] H. L. van Trees. *Detection, Estimation, and Modulation Theory, Part I.* Wiley-Interscience, 2001.

[35] D. Varodayan and A. Khisti. Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage. In *Proceedings of ICASSP 2011*, pages 1932–1935, 2011.

[36] P. K. Varshney. *Distributed Detection and Data Fusion.* Springer-Verlag New York, Inc., 1996.

[37] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui, and K. P. Chow. Security issues and challenges for cyber physical system. In *Proceedings of GreenCom-CPSCom 2010*, pages 733–738, 2010.

[38] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8): 1355–1387, 1975.

[39] L. Yang, X. Chen, J. Zhang, and H. V. Poor. Optimal privacy-preserving energy management for smart meters. In *Proceedings of INFOCOM 2014*, pages 513–521, 2014.

[40] J. Yao and P. Venkitasubramaniam. On the privacy-cost tradeoff of an in-home power storage mechanism. In *Proceedings of Allerton 2013*, pages 115–122, 2013.

[41] J. Yao and P. Venkitasubramaniam. The privacy analysis of battery control mechanisms in demand response: Revealing state approach and rate distortion bounds. In *Proceedings of CDC 2014*, pages 1377–1382, 2014.