1.

Record Nr.	UNINA990008569600403321
Autore	Moiso, Francesco
Titolo	Natura e cultura nel primo Fichte / Francesco Moiso
Pubbl/distr/stampa	Milano : Mursia, ©1979
Descrizione fisica	353 p. ; 23 cm
Collana	Biblioteca di Filosofia , Ricerche ; 5
Disciplina	193
Locazione	FLFBC
Collocazione	P.1 8D FICH/S 6
Lingua di pubblicazione	Italiano
Formato	Materiale a stampa
Livello bibliografico	Monografia

2.

Record Nr.	UNINA9911047817803321
Autore	Zheng Zhirun
Titolo	Perturbation Based Privacy in Crowdsensing / / by Zhirun Zheng, Zhetao Li, Xuemin Shen
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2026
ISBN	3-031-95052-6
Edizione	[1st ed. 2026.]
Descrizione fisica	1 online resource (264 pages)
Collana	Wireless Networks, , 2366-1445
Altri autori (Persone)	LiZhetao ShenXuemin
Disciplina	004.6
Soggetti	Computer networks Data protection - Law and legislation Wireless communication systems Mobile communication systems Computer Communication Networks Privacy Wireless and Mobile Communication
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia

Nota di contenuto

Chapter 1 -- 1.1 An Overview of Crowdsensing -- 1.1.1 Evolutionary Path of Crowdsensing -- 1.1.2 Architecture and Characteristics of Crowdsensing -- 1.1.3 Applications of Crowdsensing -- 1.2 Privacy Challenges in Crowdsensing -- 1.2.1 Privacy Leakage -- 1.2.2 Data Privacy vs. Data Utility -- 1.2.3 Data Privacy vs. Data Poisoning -- 1.3 Aim and Organization of Monograph -- Chapter 2 Perturbation-based Privacy Preservation -- 2.1 Classical Privacy Notions -- 2.1.1 Differentially Privacy -- 2.1.2 Identifiability -- 2.1.3 Mutual-Information Privacy -- 2.2 Relations between Privacy Notions -- 2.2.1 Differentially Privacy vs. Identifiability -- 2.2.2 Differentially Privacy vs. Mutual-Information Privacy -- 2.2.3 Identifiability vs. Mutual-Information Privacy -- 2.3 Summary -- Chapter 3 Semantic-Aware Trajectory Privacy Preservation in Crowdsensing -- 3.1 Problem Statement and Basic Concepts -- 3.1.1 Problem Statement -- 3.1.2 Basic Concepts -- 3.2 Privacy and Utility Metrics -- 3.2.1 Data Privacy Metric -- 3.2.2 Semantic Privacy Metric -- 3.2.3 Semantic-Aware Trajectory Utility Metric -- 3.3 Semantic-Aware Privacy Mapping Mechanism -- 3.3.1 Constructing Optimization Model -- 3.3.2 Solving Optimization Model -- 3.3.3 Computational Complexity -- 3.4 Privacy Analysis -- 3.5 Performance Evaluation -- 3.5.1 Simulation Settings -- 3.5.2 Simulation Results -- 3.6 Summary and Further Reading -- Chapter 4 Pricing-Aware Location Privacy Preservation in Crowdsensing -- 4.1 Problem Statement and Basic Concepts -- 4.1.1 Problem Statement -- 4.1.2 Basic Concepts -- 4.2 Utility Loss Metrics 4 4.2.1 Adaptive Supply and Demand Aware Grid -- 4.2.2 Dynamic Pricing Utility Metric -- 4.2.3 Ride-Matching Utility Metric -- 4.3 Pricing-Aware Privacy Mapping Mechanism -- 4.3.1 Constructing Optimization Model -- 4.3.2 Solving Optimization Model -- 4.3.3 Computational Complexity -- 4.4 Privacy Analysis -- 4.5 Performance Evaluation -- 4.5.1 Simulation Settings -- 4.5.2 Simulation Results -- 4.6 Summary and Further Reading -- Chapter 5 Data Poisoning Attacks and Defenses to LDP-based Crowdsensing -- 5.1 Problem Statement and Basic Concepts -- 5.1.1 Problem Statement -- 5.1.2 Basic Concepts -- 5.2 Data Poisoning Attacks Hidden behind the LDP Noise -- 5.2.1 LDP-based Privacy-Preserving Truth Discovery Methods -- 5.2.2 Formulating Optimal Data Poisoning Attacks -- 5.2.3 Finding Optimal Data Poisoning Attacks -- 5.3 Countermeasures: Designing Optimal Defenses -- 5.3.1 Formulating Optimal Countermeasures -- 5.3.2 Finding Optimal Countermeasures -- 5.4 Computational Complexity and Limitations of Attacks and Defenses -- 5.4.1 Computational Complexity of Attacks and Defenses -- 5.4.2 Limitations of Attacks and Defenses -- 5.5 Performance Evaluation -- 5.5.1 Simulation Settings -- 5.5.2 Simulation Results -- 5.6 Summary and Further Reading -- Chapter 6 Data Poisoning Attacks and Defenses to CDP-based Crowdsensing -- 6.1 Problem Statement and Basic Concepts -- 6.1.1 Problem Statement -- 6.1.2 Basic Concepts -- 6.2 Formulating Game Model between Attacks and Defenses -- 6.2.1 Zero-Sum Stackelberg Game -- 6.2.2 Unveiling the Normal Behavior of Workers -- 6.3 Finding Optimal Data Poisoning Attacks and Defenses -- 6.3.1 Defense Strategy for Defenders -- 6.3.2 Attack Strategy for Attackers -- 6.3.3 Local Minimax Point of Defenders-Attackers Interaction -- 6.4 Computational Complexity and Limitations of Attacks and Defenses -- 6.4.1 Computational Complexity of Attacks and defenses -- 6.4.2 Limitations of Attacks and Defenses 5 6.5 Performance Evaluation -- 6.5.1 Simulation Settings -- 6.5.2 Simulation Results -- 6.6 Summary

	and Further Reading -- Chapter 7 Conclusion and Future Works -- 7.1 Conclusion -- 7.2 Future Works.
Sommario/riassunto	This book investigates perturbation-based privacy in crowdsensing systems. The authors first present an explicit overview of crowdsensing systems and privacy challenges and briefly discuss how the noise added by perturbation-based privacy-preserving techniques could inevitably degrade data quality and facilitate the success of data poisoning attacks on crowdsensing. The authors then give a comprehensive review of classical privacy notions for perturbation-based privacy-preserving techniques and theoretically analyze the relations between these privacy notions. The next four chapters conduct a series of studies on privacy preservation in crowdsensing systems from three dimensions of data privacy, data utility and data poisoning. Finally, the book explores open issues and outlines future research directions for perturbation-based privacy preservation in crowdsensing systems. Advanced-level students majoring in the areas of network security, computer science and electrical engineering will find this book useful as a secondary text. Professionals seeking privacy-preserving solutions for crowdsensing systems will also find this book useful as a reference.