1.	Record Nr.	UNINA9910337562103321
	Autore	Jiang Jiaojiao
	Titolo	Malicious Attack Propagation and Source Identification [[electronic resource] /] / by Jiaojiao Jiang, Sheng Wen, Bo Liu, Shui Yu, Yang Xiang, Wanlei Zhou
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
	ISBN	3-030-02179-3
	Edizione	[1st ed. 2019.]
	Descrizione fisica	1 online resource (192 pages)
	Collana	Advances in Information Security, , 1568-2633 ; ; 73
	Disciplina	005.8
	Soggetti	Data protection Computer communication systems Electrical engineering Security Computer Communication Networks Communications Engineering, Networks
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	1 Introduction -- 2 Preliminary of Modeling Malicious Attack Propagation -- 3 User Influence in the Propagation of Malicious Attacks -- 4 Restrain Malicious Attack Propagation -- 5 Preliminary of Identifying Propagation Sources -- 6 Source Identification Under Complete Observations: A Maximum Likelihood (ML) Source Estimator -- 7 Source Identification Under Snapshots: A Sample Path Based Source Estimator -- 8 Source Identification Under Sensor Observations: A Gaussian Source Estimator -- 9 Comparative Study and Numerical Analysis -- 10 Identifying Propagation Source in Time-varying Networks -- 11 Identifying Multiple Propagation Sources -- 12 Identifying Propagation Source in Large-scale Networks -- 13 Future Directions and Conclusion.
	Sommario/riassunto	This book covers and makes four major contributions: 1) analyzing and surveying the pros and cons of current approaches for identifying rumor sources on complex networks; 2) proposing a novel approach to identify rumor sources in time-varying networks; 3) developing a fast

approach to identify multiple rumor sources; 4) proposing a community-based method to overcome the scalability issue in this research area. These contributions enable rumor source identification to be applied effectively in real-world networks, and eventually diminish rumor damages, which the authors rigorously illustrate in this book. In the modern world, the ubiquity of networks has made us vulnerable to various risks. For instance, viruses propagate throughout the Internet and infect millions of computers. Misinformation spreads incredibly fast in online social networks, such as Facebook and Twitter. Infectious diseases, such as SARS, H1N1 or Ebola, have spread geographically and killed hundreds of thousands people. In essence, all of these situations can be modeled as a rumor spreading through a network, where the goal is to find the source of the rumor so as to control and prevent network risks. So far, extensive work has been done to develop new approaches to effectively identify rumor sources. However, current approaches still suffer from critical weaknesses. The most serious one is the complex spatiotemporal diffusion process of rumors in time-varying networks, which is the bottleneck of current approaches. The second problem lies in the expensively computational complexity of identifying multiple rumor sources. The third important issue is the huge scale of the underlying networks, which makes it difficult to develop efficient strategies to quickly and accurately identify rumor sources. These weaknesses prevent rumor source identification from being applied in a broader range of real-world applications. This book aims to analyze and address these issues to make rumor source identification more effective and applicable in the real world. The authors propose a novel reverse dissemination strategy to narrow down the scale of suspicious sources, which dramatically promotes the efficiency of their method. The authors then develop a Maximum-likelihood estimator, which can pin point the true source from the suspects with high accuracy. For the scalability issue in rumor source identification, the authors explore sensor techniques and develop a community structure based method. Then the authors take the advantage of the linear correlation between rumor spreading time and infection distance, and develop a fast method to locate the rumor diffusion source. Theoretical analysis proves the efficiency of the proposed method, and the experiment results verify the significant advantages of the proposed method in large-scale networks. This book targets graduate and post-graduate students studying computer science and networking. Researchers and professionals working in network security, propagation models and other related topics, will also be interested in this book.