1.	Record Nr.	UNINA9910298989003321
	Autore	Yang Jie
	Titolo	Pervasive Wireless Environments: Detecting and Localizing User Spoofing / / by Jie Yang, Yingying Chen, Wade Trappe, Jerry Cheng
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2014
	ISBN	3-319-07356-7
	Edizione	[1st ed. 2014.]
	Descrizione fisica	1 online resource (79 p.)
	Collana	SpringerBriefs in Computer Science, , 2191-5768
	Disciplina	005.8
	Soggetti	Computer security Computer communication systems Computers Application software Systems and Data Security Computer Communication Networks Information Systems and Communication Service Information Systems Applications (incl. Internet)
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Description based upon print version of record.
	Nota di bibliografia	Includes bibliographical references at the end of each chapters.
	Nota di contenuto	Introduction -- Feasibility of Launching User Spoofing -- Attack Detection Model -- Detection and Localizing Multiple Spoofing Attackers.-Detecting Mobile Agents Using Identity Fraud -- Related Work -- Conclusions and Future Work.
	Sommario/riassunto	This Springer Brief provides a new approach to prevent user spoofing by using the physical properties associated with wireless transmissions to detect the presence of user spoofing. The most common method, applying cryptographic authentication, requires additional management and computational power that cannot be deployed consistently. The authors present the new approach by offering a summary of the recent research and exploring the benefits and potential challenges of this method. This brief discusses the feasibility of launching user spoofing attacks and their impact on the wireless and sensor networks. Readers are equipped to understand several system models. One attack detection model exploits the spatial correlation of received signal

strength (RSS) inherited from wireless devices as a foundation. Through experiments in practical environments, the authors evaluate the performance of the spoofing attack detection model. The brief also introduces the DEMOTE system, which exploits the correlation within the RSS trace based on each device's identity to detect mobile attackers. A final chapter covers future directions of this field. By presenting complex technical information in a concise format, this brief is a valuable resource for researchers, professionals, and advanced-level students focused on wireless network security.