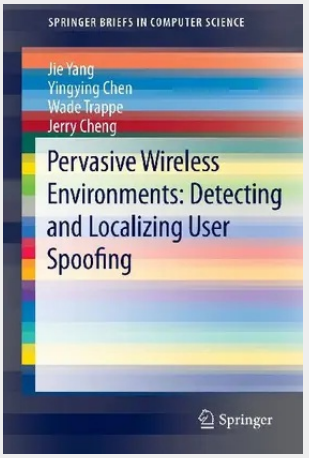
Yang / Chen / Trappe

Pervasive Wireless Environments: Detecting and Localizing User Spoofing



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.

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.

53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783319073552
Medium: Buch
ISBN: 978-3-319-07355-2
Verlag: Springer
Erscheinungstermin: 14.07.2014
Sprache(n): Englisch
Auflage: Erscheinungsjahr 2014
Serie: SpringerBriefs in Computer Science
Produktform: Kartoniert
Gewicht: 1358 g
Seiten: 72
Format (B x H): 155 x 235 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)