1. Record Nr. UNINA9911047714703321

Autore	Lu Weidang
Titolo	Secure Communications in Unmanned Aerial Vehicle-Enabled Mobile Edge Computing Systems / / by Weidang Lu, Yu Ding, Huimei Han, Guanjun Xu
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2026
ISBN	981-9696-11-9
Edizione	[1st ed. 2026.]
Descrizione fisica	1 online resource (139 pages)
Collana	SpringerBriefs in Computer Science, , 2191-5776
Altri autori (Persone)	DingYu HanHuimei XuGuanjun
Disciplina	004.0151
Soggetti	Computer science Data protection Electronic digital computers - Evaluation Models of Computation Security Services System Performance and Evaluation
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	"Chapter 1. Overview of Unmanned Aerial Vehicle – Mobile Edge Computing Systems" -- "Chapter 2 PLS-based Secure communications for UAV-enabled MEC Systems" -- "Chapter 3 RIS-Based Secure Communications for UAV-Enabled MEC Systems" -- "Chapter 4 DRL-Based Secure Communications for UAV-Enabled MEC Systems" -- "Chapter 5 Online-Based Secure Communications for UAV-Enabled MEC Systems" -- "Chapter 6 Conclusions and Future Research".
Sommario/riassunto	With the rapid evolution of wireless communication technologies, emerging applications like autonomous driving, telemedicine, and virtual reality are becoming integral to modern life. These advancements have significantly increased computing demands and coverage requirements, posing challenges for traditional systems and resource-constrained devices. Unmanned aerial vehicle-assisted mobile edge computing (UAV-assisted MEC) offers an innovative solution, enabling rapid deployment of communication infrastructure and

providing efficient computing services for devices. However, the openness and broadcast nature of UAV communications make them highly susceptible to security threats. The book "Secure Communications in Unmanned Aerial Vehicle-Enabled Mobile Edge Computing Systems" explores advanced strategies to secure data transmission in UAV-enabled MEC systems. Furthermore, this book provides a detailed exploration of how physical-layer security techniques can be effectively employed to enhance secure communications within these complex systems. Aimed at researchers, engineers, and professionals in the fields of secure communications, MEC, and UAV technology, the book addresses the growing demand for resilient security frameworks that can handle the dynamic and real-time nature of UAV operations. It offers vital insights for anyone involved in the development of next-generation wireless networks, making it an indispensable reference for those tackling security challenges in UAV-enabled MEC systems. The content covers advanced theoretical insights and technical analysis, offering a comprehensive range of methods to strengthen security in UAV-enabled MEC systems. Key topics include secure offloading strategies, communication modes, edge learning, deep reinforcement learning, reconfigurable intelligent surface, and multiple UAVs collaboration. Additionally, the book delves into physical-layer security techniques such as artificial noise generation and cooperative jamming. These methods aim to safeguard sensitive information from eavesdroppers and secure communication channels at the physical layer. Alongside these security-focused techniques, the book also covers essential optimization strategies, including trajectory optimization, resource allocation under adversarial conditions, which collectively enhance secure performance in UAV-enabled MEC systems.