1. Record Nr. UNISA996550557903316

Autore	Butun Ismail
Titolo	Low-Power Wide-Area Networks: Opportunities, Challenges, Risks and Threats [[electronic resource] /] / edited by Ismail Butun, Ian F. Akyildiz
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2023
ISBN	3-031-32935-X
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (225 pages)
Altri autori (Persone)	AkyildizIan F
Disciplina	004.67
Soggetti	Computer networks Wireless communication systems Mobile communication systems Computer networks - Security measures Cooperating objects (Computer systems) Computer Communication Networks Wireless and Mobile Communication Mobile and Network Security Cyber-Physical Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Part I Preliminaries,DesignPrinciplesandChallengesofLPWANs -- 1. Theoretical Landscape of LPWANs -- 2. IDS and IPS in LPWAN (LoRaWAN, Sigfox, and NB-IoT) -- Part II Challenges, Opportunities, Risks and Threats in LPWANs -- 3. Pervasive LPWAN connectivity through LEO Satellites: tradingoff reliability, throughput, latency, and energy efficiency -- 4 Energy Saving as a Security Threat in LPWAN and Internet of Things -- Part III Cyber Security Aspects and Applications of LPWANs -- 5 Analysis of LPWAN: Cyber-Security Vulnerabilities and Privacy Issues in LoRaWAN, Sigfox, and NB-IoT -- 6 Applications of LPWANs.
Sommario/riassunto	This book offers the most suitable methods of applying Low-Power Wide-Area Network (LPWAN) technology to conceptual works and/or research studies. For instance, existing IoT protocols such as CoAP and MQTT are complemented by LPWAN to provide better service quality

(QoS) to enable the notion of "sensor as a service" to endpoint users which is demonstrated in this book. LPWAN is a new enabling technology for IoT, filling the gap that existed between the legacy network technologies (WLAN, LAN, PAN) in terms of power, range, and data rates. It is also an alternative solution to implementations of IoT via cellular (4G/5G/6G) technologies, as it operates on the ISM band and also provides long-term battery life. Due to the several advantages, it brings, LPWAN raises high enthusiasm for many stakeholders of IoT. However, there still exist many research challenges to be tackled within this technology. As such this book aims at shedding light on those research problems. Moreover, practical users can also benefit from this book: Emergency response teams can leverage IoT systems with the extended communications-range capability provided by LPWAN technology. Moreover, machine-to-machine (M2M) and thing-to-thing (T2T) communications also benefit from this notion, as well as the Social IoT (SIoT) concept, owing to the “low-power” consumption advantage that is brought up by LPWAN technologies, e.g., 10 years battery lifetime projection for the LoRaWAN end-devices is very promising. Eventually, this proposed book aims at covering all aspects of LPWANs, from A to Z, theoretical aspects, hardware platforms and technologies, along with applications, opportunities, and, finally, challenges. Cyber-attacks and incidences are on the rise within the last decade, especially cases in large corporates and critical infrastructures have shown that cybersecurity should become one of the important pillars of computer network infrastructures as well as any kind of relevant technology being introduced. As such, cybersecurity is bringing attention not only from practitioners and academicians but also from other parties such as media, politicians, etc. Eventually, to reflect this important point of view, this book includes three chapters to investigate various aspects of LPWAN cybersecurity. Researchers working in wireless communications technologies and advanced-level students taking courses in electrical engineering or computer science will benefit from this book as a reference. Professionals working within this related field will also want to purchase this book.