1. Record Nr. UNINA9910830981303321

Titolo	Intelligent security management and control in the Iot / / edited by Mohamed-Aymen Chalouf
Pubbl/distr/stampa	Hoboken, New Jersey : , : John Wiley & Sons, Incorporated, , [2022] ©2022
ISBN	1-394-15603-0 1-394-15601-4 1-394-15602-2
Descrizione fisica	1 online resource (314 pages)
Collana	Sciences. Networks and communications. Network management and control
Disciplina	004
Soggetti	Internet of things - Security measures Internet of things - Control
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cover -- Half-Title Page -- Title Page -- Copyright Page -- Contents -- 1. Multicriteria Selection of Transmission Parameters in the IoT -- 1.2. Changing access network in the IoT -- 1.3. Spectrum handoff in the IoT -- 1.4. Multicriteria decision-making module for an effective spectrum handoff in the IoT -- 1.4.1. General architecture -- 1.4.2. Decision-making flowchart -- 1.4.3. Performances evaluation -- 1.5. Conclusion -- 1.6. References -- 2. Using Reinforcement Learning to Manage Massive Access in NB-IoT Networks -- 2.1. Introduction -- 2.2. Fundamentals of the NB-IoT standard -- 2.2.1. Deployment and instances of use -- 2.2.2. Transmission principles -- 2.2.3. Radio resource random access procedure -- 2.3. State of the art -- 2.4. Model for accessing IoT terminals -- 2.5. Access controller for IoT terminals based on reinforcement learning -- 2.5.1. Formulating the problem -- 2.5.2. Regulation system for arrivals -- 2.6. Performance evaluation -- 2.7. Conclusion -- 2.8. References -- 3. Optimizing Performances in the IoT: An Approach Based on Intelligent Radio -- 3.1. Introduction -- 3.2. Internet of Things (IoT) -- 3.2.1. Definition of the IoT -- 3.2.2. Applications of the IoT -- 3.2.3. IoT challenges -- 3.2.4. Enabling technologies in the IoT -- 3.3. Intelligent radio --

data -- 8.6.2. Non-revocability of biometric data -- 8.6.3. Security of biometric systems -- 8.7. Conclusion -- 8.8. References -- 9. Dynamic Identity and Access Management in the IoT: Blockchain-based Approach -- 9.1. Introduction -- 9.2. Context -- 9.2.1. Intelligent identity and access management -- 9.2.2. Blockchain.
9.3. Blockchain for intelligent identity and access management -- 9.3.1. A new architecture integrating blockchain -- 9.3.2. The different benefits -- 9.4. Challenges -- 9.4.1. Scaling up -- 9.4.2. Blockchain security -- 9.4.3. Energy consumption -- 9.4.4. Definition of consensus algorithms based on artificial -- 9.5. Conclusion -- 9.6. References -- 10. Adapting the Security Level of IoT Applications -- 10.1. Introduction -- 10.2. Definitions and characteristics -- 10.2.1. Definitions -- 10.2.2. Characteristics -- 10.3. IoT applications -- 10.4. IoT architectures -- 10.5. Security, trust and privacy protection in IoT applications -- 10.5.1. General remarks -- 10.5.2. Security services -- 10.5.3. Communication security -- 10.5.4. Trust -- 10.5.5. Privacy -- 10.6. Adapting the security level in the IoT -- 10.6.1. Context-awareness -- 10.6.2. Context-aware security -- 10.6.3. Context-aware security architecture and privacy protection -- 10.7. Conclusion -- 10.8. References -- 11. Moving Target Defense Techniques for the IoT -- 11.1. Introduction -- 11.2. Background -- 11.2.1. Brief chronology of Moving Target Defense -- 11.2.2. Fundamental technical and taxonomic principles of MTD -- 11.3. Related works -- 11.3.1. Surveys on MTD techniques -- 11.3.2. Frameworks for IoT systems linked to the concept of MTD -- 11.4. LMTD for the IoT: a qualitative survey -- 11.4.1. Data: MTD mechanism against side-channel channel attacks -- 11.4.2. Software -- 11.4.3. Runtime environment -- 11.4.4. Platform: diversifying by reconfiguring the IoT node firmware -- 11.4.5. Networks -- 11.4.6. Section summary -- 11.5. Network components in the IoT: a vast domain for MTD -- 11.5.1. Physical layer -- 11.5.2. Link layer -- 11.5.3. OSI network layer -- 11.5.4. Transport layer -- 11.5.5. Application layer -- 11.5.6. Section summary -- 11.6. An MTD framework for the IoT.
11.6.1. Proposition: components -- 11.6.2. Instantiation: UDP port hopping -- 11.7. Discussion and avenues for future research -- 11.8. Conclusion -- 11.9. References -- List of Authors -- Index -- EULA.

Sommario/riassunto

The Internet of Things (IoT) has contributed greatly to the growth of data traffic on the Internet. Access technologies and object constraints associated with the IoT can cause performance and security problems. This relates to important challenges such as the control of radio communications and network access, the management of service quality and energy consumption, and the implementation of security mechanisms dedicated to the IoT. In response to these issues, this book presents new solutions for the management and control of performance and security in the IoT. The originality of these proposals lies mainly in the use of intelligent techniques. This notion of intelligence allows, among other things, the support of object heterogeneity and limited capacities as well as the vast dynamics characterizing the IoT.