1. Record Nr. UNINA9910779062903321

Autore	Angrist Michele Penner <1970->
Titolo	Party building in the modern Middle East [[electronic resource] /] / Michele Penner Angrist
Pubbl/distr/stampa	Seattle, : University of Washington Press, 2006
ISBN	0-295-80112-3
Descrizione fisica	1 online resource (257 p.)
Collana	Publications on the Near East
Disciplina	324.20956
Soggetti	Political parties - Middle East Authoritarianism - Middle East Middle East Politics and government 1979-
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	pt. 1. Explaining party system characteristics -- pt. 2. The impact of party systems on regime formation.

2. 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 --

3.3.1. Definition of intelligent radio -- 3.3.2. Motivations for using intelligent radio in the IoT -- 3.3.3. Challenges in using intelligent radio in the IoT -- 3.4. Conclusion -- 3.5. References -- 4. Optimizing the Energy Consumption of IoT Devices -- 4.1. Introduction -- 4.2. Energy optimization -- 4.2.1. Definitions -- 4.3. Optimization techniques for energy consumption -- 4.3.1. The A* algorithm -- 4.3.2. Fuzzy logic -- 4.4. Energy optimization in the IoT -- 4.4.1. Characteristics of the IoT -- 4.4.2. Challenges in energy optimization. 4.4.3. Research on energy optimization in the IoT -- 4.5. Autonomous energy optimization framework in the IoT -- 4.5.1. Autonomous computing -- 4.5.2. Framework specification -- 4.6. Proposition of a self-optimization method for energy consumption in the IoT -- 4.6.1. Fuzzy logic model -- 4.6.2. Decision-making algorithm -- 4.6.3. Evaluating energy self-optimization in the IoT -- 4.7. Conclusion -- 4.8. References -- 5. Toward Intelligent Management of Service Quality in the IoT: The Case of a Low Rate WPAN -- 5.1. Introduction -- 5.2. Quick overview of the IoT -- 5.2.2. Technologies for the IoT -- 5.2.3. IoT and quality of service -- 5.3. IEEE 802.15.4 TSCH approach -- 5.4. Transmission scheduling -- 5.4.1. General considerations -- 5.4.2. Scheduling in the literature -- 5.5. Routing and RPL -- 5.5.1. Routing -- 5.5.2. RPL -- 5.5.3. Multipath -- 5.6. Combined approach based on 802.15.4 TSCH and multipath RPL -- 5.6.1. Automatic Repeat reQuest -- 5.6.2. Replication and Elimination -- 5.6.3. Overhearing -- 5.7. Conclusion -- 5.8. References -- 6. Adapting Quality of Service of Energy-Harvesting IoT Devices -- 6.1. Toward the energy autonomy of sensor networks -- 6.1.1. Energy harvesting and management -- 6.1.2. State-of-the-art energy managers -- 6.2. Fuzzyman: use of fuzzy logic -- 6.2.1. Design of Fuzzyman -- 6.2.2. Evaluating Fuzzyman -- 6.2.3. Conclusion -- 6.3. RLMan: using reinforcement learning -- 6.3.1. Formulating the problem of managing the harvested energy -- 6.3.2. RLMan algorithm -- 6.3.3. Evaluation of RLMan -- 6.3.4. Conclusion -- 6.4. Toward energy autonomous LoRa nodes -- 6.4.1. Multisource energy-harvesting architecture -- 6.4.2. Applying energy management to LoRa nodes -- 6.5. Conclusion -- 6.6. References -- 7. Adapting Access Control for IoT Security -- 7.1. Introduction -- 7.2. Defining security services in the IoT.
7.2.1. Identification and authentication in the IoT -- 7.2.2. Access control in the IoT -- 7.2.3. Confidentiality in the IoT -- 7.2.4. Integrity in the IoT -- 7.2.5. Non-repudiation in the IoT -- 7.2.6. Availability in the IoT -- 7.3. Access control technologies -- 7.4. Access control in the IoT -- 7.4.1. Research on the extension of access control models for the IoT -- 7.4.2. Research on adapting access control systems and technologies for -- 7.5. Access control framework in the IoT -- 7.5.1. IoT architecture -- 7.5.2. IoT-MAAC access control specification -- 7.6. Conclusion -- 7.7. References -- 8. The Contributions of Biometrics and Artificial Intelligence in Securing the IoT -- 8.1. Introduction -- 8.2. Security and privacy in the IoT -- 8.3. Authentication based on biometrics -- 8.3.1. Biometrics -- 8.3.2. Biometric techniques -- 8.3.3. The different properties of biometrics -- 8.3.4. Operating a biometric system -- 8.3.5. System performances -- 8.4. Multifactor authentication techniques based on biometrics -- 8.4.1. Multifactor authentication -- 8.4.2. Examples of multifactor authentication approaches for securing -- 8.4.3. Presentation of the approach of Sammoud et al. (2020c) -- 8.5. Authentication techniques based on biometrics and machine learning -- 8.5.1. Machine learning algorithms -- 8.5.2. Examples of authentication approaches based on biometrics and -- 8.5.3. Authentication approaches based on ECG and machine learning -- 8.6. Challenges and limits -- 8.6.1. Quality of biometric

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.

3. Record Nr. UNIORUON00056696

Autore	AKAMATSU Toshihide
Titolo	Shinran / Akamatsu Toshihide; Nihon rekishi gakkai
Pubbl/distr/stampa	Tokyo, : Yoshikawa kobunkan, 1961
Descrizione fisica	371 p. ; 19 cm
Classificazione	GIA IV
Soggetti	Giappone - Biografie
Lingua di pubblicazione	Giapponese
Formato	Materiale a stampa
Livello bibliografico	Monografia