1. Record Nr. UNINA9910861087203321

Autore	Parkinson Simon
Titolo	Deception in Autonomous Transport Systems : Threats, Impacts and Mitigation Policies
Pubbl/distr/stampa	Cham : , : Springer International Publishing AG, , 2024 ©2024
ISBN	3-031-55044-7
Edizione	[1st ed.]
Descrizione fisica	1 online resource (196 pages)
Collana	Wireless Networks Series
Altri autori (Persone)	NikitasAlexandros VallatiMauro
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Contents -- Introduction -- 1 Setting the Scene -- 2 Organization -- 3 Target Audience -- References -- Part I Smart Cities, Policies, and Ethics -- Ethical Dilemmas in Autonomous Driving: Philosophical, Social, and Public Policy Implications -- 1 Introduction -- 2 The Trolley Problem -- 3 Self-Sacrifice? -- 4 The Responsibility Question -- 5 State and Public Policy for AVs -- 6 Conclusion -- References -- Smart Cities: Concept, Pillars, and Challenges -- 1 Introduction -- 2 Building Intelligence: The Journey to Smart Cities -- 2.1 Smart Governance -- 2.2 Smart Environment -- 2.3 Smart Communications -- 2.4 Smart Mobility -- 2.5 Citizen Participation -- 2.6 Smart Living -- 3 Transformative Phases in Urban Landscapes -- 4 Smart in the Making: From Concept to Reality -- 5 Conclusion and Take-Home Message -- 5.1 Reflections and Implications -- 5.2 The Bottom Line -- References -- The Connected and Autonomous Vehicle Trade-Off: Functional Benefits versus Security Risks -- 1 Introduction -- 2 Literature Review -- 2.1 Defining the Terminology of CVs, AVs, and CAVs -- 2.2 Cyber-Physical Systems (CPSs) -- 2.3 The Levels of Automation -- 2.4 Benefits of CAVs -- 2.4.1 Improving Highway Safety -- 2.4.2 Alleviating Traffic Congestion -- 2.4.3 Reducing Air Pollution -- 2.4.4 Improving the Fuel Economy -- 2.4.5 Beneficial Impact on Public Health -- 2.4.6 Improving Travel Behavior -- 2.5 Risks Associated with CAVs -- 2.5.1 Cyber Security -- 2.5.2 Privacy -- 2.5.3

Legislation -- 2.5.4 Other Risks -- 3 Conclusion -- References -- Connected and Autonomous Vehicles and Infrastructure Needs: Exploring Road Network Changes and Policy Interventions -- 1 Introduction -- 2 Future Urban Road and Autonomous Vehicles. Do They Fit? -- 3 Infrastructure for Connected Autonomous Vehicles in Cities. Are We Ready? Potentials and Risks.
3.1 Are Our Cities Ready to Welcome Connected and Autonomous Vehicles? -- 3.2 Which Are the Issues Hindering a Full-Scale Adoption of CAVs? -- 3.3 Further Developments Required for Adoption -- 3.3.1 Technology -- 3.3.2 Safety -- 3.3.3 Regulation -- 3.3.4 Infrastructure -- 4 Policies and Interventions -- 4.1 Integrating CAVs in Urban Road Environments Through Street Classification -- 4.2 Setting a Complete Framework of Policies and Interventions -- 5 Conclusions -- References -- Part II AI Applications for Smart Transport and Mobility -- Centralized Intelligent Traffic Routing in the Light of Disobedience of Drivers -- 1 Introduction -- 2 Problem Formulation -- 3 Discrepancies Between Global and Individual Costs -- 4 Route Assignment as a Normal Form Game -- 5 Disobedience of Drivers -- 6 Toward Fairness of Centralized Vehicle Routing Systems -- 6.1 Toward the Concept of Fairness -- 6.2 Toward Considering Fairness in Routing -- 6.3 Different Costs Among Vehicles/Drivers -- 7 Discussion -- 8 Conclusion -- References -- Detecting Abnormal Vehicle Behavior: A Clustering-Based Approach -- 1 Introduction -- 2 Literature Review -- 3 Methodology -- 3.1 Data Generation and Preprocessing -- 3.2 Unsupervised Machine Learning Algorithms -- 4 Results and Discussion -- 5 Conclusion -- References -- AI Approaches on Urban Public Transport Routing -- 1 AI Approaches on Urban Public Transport Routing -- 1.1 Traditional Network Route Design -- 1.1.1 Fuel Bus Routing Design -- 1.1.2 Electric Bus Routing Design -- 1.2 Smart Public Transport System -- 1.2.1 Conventional Bus Service -- 1.2.2 Flexible Demand-Responsive Service -- 1.3 Intelligent Public Transport with CAVs -- 1.3.1 Impact of AV Technology -- 1.3.2 Impact of CV Technology -- 1.4 Issues and Challenges -- 1.4.1 Limitations of AI Algorithm -- 1.4.2 Issues of an AI-Based Transportation System.
1.4.3 Challenges of CAVs -- References -- Part III Cyber Security for Deceitful Connected and Autonomous Vehicles -- Cyber Threat Intelligence Analysis for Situational Understanding in Autonomous Transport Systems -- 1 Introduction -- 2 A Primer in Cyber Threat Intelligence Analysis -- 2.1 Cyber Kill Chain -- 2.2 The Diamond Model -- 3 Technology-Centered Analysis of Threats in Autonomous Transport Systems -- 4 Intelligence-Driven Situational Understanding: A Case Study -- 5 Conclusions -- References -- Interaction Attacks as Deceitful Connected and Automated Vehicle Behavior -- 1 Introduction -- 2 Driving Automation, Cyberattacks, and Deception -- 3 Control, Feedback, and Fakes -- 4 Interaction Attacks -- 5 A Case Study -- 6 Interaction Attacks as Deceitful CAV Behavior -- References -- Securing Vehicle-to-Drone (V2D) Communications: Challenges and Solutions -- 1 Introduction -- 2 Fundamentals of V2D Communications -- 2.1 Use Cases and Applications -- 2.1.1 Traffic Management and Optimization -- 2.1.2 Last-Mile Delivery and Logistics Operations -- 2.1.3 Emergency Response -- 2.1.4 Infrastructure Inspection -- 2.1.5 Cooperative Navigation -- 2.2 Key Components in V2D Communications -- 2.2.1 Onboard Vehicle Systems -- 2.2.2 Drone Systems -- 2.2.3 Communication Protocols -- 2.2.4 Data Exchange Formats -- 2.2.5 Positioning and Navigation Technologies -- 2.2.6 Data Processing and Decision-Making -- 2.2.7 Security and Privacy Measures -- 3 V2D-Driven Enhanced Perception -- 4 Security and Privacy Issues in V2D -- 4.1 Threat Landscape in V2D Communications

-- 4.2 Authentication and Authorization Issues -- 4.3 Privacy Concerns in V2D Communications -- 5 Example Scenarios of Compromised Security in V2D -- 5.1 Unauthorized Access to Traffic Monitoring Drones -- 5.2 Drone Package Tampering in Last-Mile Delivery -- 5.3 Jamming in Surveillance and Security.
6 Key Security Solutions for V2D Communications -- 6.1 AI-Driven Solutions -- 7 Concluding Remarks -- References -- The Use of GPS Spoofing Attacks in Location Deception -- 1 Introduction -- 2 GPS Workings -- 2.1 GPS Signals -- 2.2 Determining Position -- 2.3 Signal Strength -- 3 GPS Spoofing -- 4 GPS Attacks and Detection and Prevention -- 4.1 Attacks -- 4.2 Detection and Prevention Techniques -- 5 How Spoofing Facilitates CAV Deception -- 6 Conclusion -- References.