1. Record Nr. UNINA9910830597903321

Autore	Lin Xiaodong
Titolo	Vehicular ad hoc network security and privacy / / Xiaodong Lin, Rongxing Lu
Pubbl/distr/stampa	Hoboken [New Jersey] : , : IEEE Press/Wiley, , [2015] [Piscataqay, New Jersey] : , : IEEE Xplore, , [2015]
ISBN	1-119-08216-1 1-119-08215-3 1-119-08214-5
Descrizione fisica	1 online resource (237 p.)
Collana	IEEE press series on information and communication networks security IEEE Press series on information & communication networks security
Disciplina	388.312
Soggetti	Vehicular ad hoc networks (Computer networks)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references at the end of each chapters and index.
Nota di contenuto	List of Figures xi -- List of Tables xv -- Acronyms xvii -- Preface xix -- 1 INTRODUCTION 1 -- 1.1 Background 1 -- 1.2 DSRC AND VANET 2 -- 1.2.1 DSRC 2 -- 1.2.2 VANET 3 -- 1.2.3 Characteristics of VANET 6 -- 1.3 Security and Privacy Threats 7 -- 1.4 Security and Privacy Requirements 8 -- 1.5 Challenges and Prospects 9 -- 1.5.1 Conditional Privacy Preservation in VANETs 9 -- 1.5.2 Authentication with Efficient Revocation in VANETs 10 -- 1.6 Standardization and Related Activities 11 -- 1.7 Security Primitives 13 -- 1.8 Outline of the Book 17 -- References 17 -- 2 GSIS: GROUP SIGNATURE AND ID-BASED SIGNATURE-BASED SECURE AND PRIVACY-PRESERVING PROTOCOL 21 -- 2.1 Introduction 21 -- 2.2 Preliminaries and Background 23 -- 2.2.1 Group Signature 23 -- 2.2.2 Bilinear Pairing and ID-Based Cryptography 23 -- 2.2.3 Threat Model 23 -- 2.2.4 Desired Requirements 24 -- 2.3 Proposed Secure and Privacy-Preserving Protocol 25 -- 2.3.1 Problem Formulation 25 -- 2.3.2 System Setup 27 -- 2.3.3 Security Protocol between OBUs 29 -- 2.3.4 Security Protocol between RSUs and OBUs 38 -- 2.4 Performance Evaluation 41 -- 2.4.1 Impact of Traffic Load 43 -- 2.4.2 Impact of Cryptographic Signature Verification Delay 43 -- 2.4.3 Membership Revocation and Tracing

Trustworthiness 165 -- 8.6 Security Discussion 168 -- 8.6.1 Collusion Attacks 168 -- 8.6.2 Privacy Protection of Witnesses 168 -- 8.7 Performance Evaluation 169 -- 8.7.1 Transmission Cost 169 -- 8.7.2 Computational Cost 169 -- 8.8 Concluding Remarks 170 -- References 170 -- 9 FAST HANDOVER AUTHENTICATION BASED ON MOBILITY PREDICTION 173 -- 9.1 Introduction 173 -- 9.2 Vehicular Network Architecture 175 -- 9.3 Proposed Fast Handover Authentication Scheme Based on Mobility Prediction 176 -- 9.3.1 Multilayer Perceptron Classifier 176 -- 9.3.2 Proposed Authentication Scheme 178 -- 9.4 Security Analysis 183 -- 9.4.1 Replay Attack 183 -- 9.4.2 Forward Secrecy 183 -- 9.5 Performance Evaluation 184 -- 9.6 Concluding Remarks 185 -- References 186 -- Index 187.

Sommario/riassunto

Unlike any other book in this area, this book provides innovative solutions to security issues, making this book a must read for anyone working with or studying security measures. Vehicular Ad Hoc Network Security and Privacy mainly focuses on security and privacy issues related to vehicular communication systems. It begins with a comprehensive introduction to vehicular ad hoc network and its unique security threats and privacy concerns and then illustrates how to address those challenges in highly dynamic and large size wireless network environments from multiple perspectives. This book is richly illustrated with detailed designs and results for approaching security and privacy threats. Additional features of this book include: . An introduction to standardization and industry activities as well as government regulation in secure vehicular networking. Eight novel secure and privacy-preserving schemes for vehicular communications. Explorations into interdisciplinary methods by combining social science, cryptography, and privacy enhancing technique The authors have taken a non-traditional method toward securing communications, allowing for new research directions in security and privacy in VANETs, which will be helpful to students, researchers, and IT practitioners.