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

Efficiency 45 -- 2.5 Concluding Remarks 47 -- References 47 -- 3 ECPP: EFFICIENT CONDITIONAL PRIVACY PRESERVATION PROTOCOL 51 -- 3.1 Introduction 51 -- 3.2 System Model and Problem Formulation 52 -- 3.2.1 System Model 52 -- 3.2.2 Design Objectives 54 -- 3.3 Proposed ECPP Protocol 55 -- 3.3.1 System Initialization 55 -- 3.3.2 OBU Short-Time Anonymous Key Generation 56 -- 3.3.3 OBU Safety Message Sending 62 -- 3.3.4 OBU Fast Tracking Algorithm 63 -- 3.4 Analysis on Conditional Privacy Preservation 64 -- 3.5 Performance Analysis 66 -- 3.5.1 OBU Storage Overhead 66 -- 3.5.2 OBU Computation Overhead on Verification 66 -- 3.5.3 TA Computation Complexity on OBU Tracking 68 -- 3.6 Concluding Remarks 69 -- References 69 -- 4 PSEUDONYM-CHANGING STRATEGY FOR LOCATION PRIVACY 71.
4.1 Introduction 71 -- 4.2 Problem Definition 73 -- 4.2.1 Network Model 73 -- 4.2.2 Threat Model 74 -- 4.2.3 Location Privacy Requirements 75 -- 4.3 Proposed PCS Strategy for Location Privacy 75 -- 4.3.1 KPSD Model for PCS Strategy 75 -- 4.3.2 Anonymity Set Analysis for Achieved Location Privacy 79 -- 4.3.3 Feasibility Analysis of PCS Strategy 85 -- 4.4 Performance Evaluation 86 -- 4.5 Concluding Remarks 89 -- References 89 -- 5 RSU-AIDED MESSAGE AUTHENTICATION 91 -- 5.1 Introduction 91 -- 5.2 System Model and Preliminaries 93 -- 5.2.1 System Model 93 -- 5.2.2 Assumption 93 -- 5.2.3 Problem Statement 94 -- 5.2.4 Security Objectives 95 -- 5.3 Proposed RSU-Aided Message Authentication Scheme 96 -- 5.3.1 Overview 96 -- 5.3.2 Mutual Authentication and Key Agreement between RSUs and Vehicles 96 -- 5.3.3 Hash Aggregation 98 -- 5.3.4 Verification 99 -- 5.3.5 Privacy Enhancement 100 -- 5.4 Performance Evaluation 101 -- 5.4.1 Message Loss Ratio 102 -- 5.4.2 Message Delay 102 -- 5.4.3 Communication Overhead 104 -- 5.5 Security Analysis 105 -- 5.6 Concluding Remarks 106 -- References 107 -- 6 TESLA-BASED BROADCAST AUTHENTICATION 109 -- 6.1 Introduction 109 -- 6.2 Timed Efficient and Secure Vehicular Communication Scheme 110 -- 6.2.1 Preliminaries 110 -- 6.2.2 System Formulation 112 -- 6.2.3 Proposed TSVC Scheme 113 -- 6.2.4 Enhanced TSVC with Nonrepudiation 118 -- 6.2.5 Discussion 123 -- 6.3 Security Analysis 129 -- 6.4 Performance Evaluation 129 -- 6.4.1 Impact of Vehicle Moving Speed 131 -- 6.4.2 Impact of Vehicle Density 132 -- 6.5 Concluding Remarks 134 -- References 134 -- 7 DISTRIBUTED COOPERATIVE MESSAGE AUTHENTICATION 137 -- 7.1 Introduction 137 -- 7.2 Problem Formulation 138 -- 7.2.1 Network Model 138 -- 7.2.2 Security Model 139 -- 7.3 Basic Cooperative Authentication Scheme 140 -- 7.4 Secure Cooperative Authentication Scheme 141 -- 7.4.1 Evidence and Token for Fairness 142 -- 7.4.2 Authentication Proof 145 -- 7.4.3 Flows of Proposed Scheme 146 -- 7.5 Security Analysis 147.
7.5.1 Linkability Attack 147 -- 7.5.2 Free-Riding Attack without Authentication Efforts 147 -- 7.5.3 Free-Riding Attack with Fake Authentication Efforts 148 -- 7.6 Performance Evaluation 148 -- 7.6.1 Simulation Settings 148 -- 7.6.2 Simulation Results 149 -- 7.7 Concluding Remarks 150 -- References 151 -- 8 CONTEXT-AWARE COOPERATIVE AUTHENTICATION 153 -- 8.1 Introduction 153 -- 8.2 Message Trustworthiness in VANETs 156 -- 8.3 System Model and Design Goal 159 -- 8.3.1 Network Model 159 -- 8.3.2 Attack Model 159 -- 8.3.3 Design Goals 160 -- 8.4 Preliminaries 160 -- 8.4.1 Pairing Technique 160 -- 8.4.2 Aggregate Signature and Batch Verification 160 -- 8.5 Proposed AEMAT Scheme 161 -- 8.5.1 System Setup 161 -- 8.5.2 Registration 162 -- 8.5.3 SER Generation and Broadcasting 162 -- 8.5.4 SER Opportunistic Forwarding 162 -- 8.5.5 SER Aggregated Authentication 163 -- 8.5.6 SER Aggregated

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.