

1. Record Nr.	UNINA9910829807103321
Autore	Benarous Leila
Titolo	Security in vehicular networks : focus on location and identity privacy / / Leila Benarous, Salim Batim, and Abdelhamid Mellouk
Pubbl/distr/stampa	Hoboken, NJ : , : John Wiley & Sons, Inc., , [2022] ©2022
ISBN	1-394-17261-3 1-394-17259-1
Descrizione fisica	1 online resource (265 pages)
Disciplina	388.312
Soggetti	Vehicular ad hoc networks (Computer networks) Intelligent transportation systems - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Title Page -- Copyright Page -- Contents -- Preface -- List of Acronyms -- Introduction -- Chapter 1. Vehicular Networks -- 1.1. Introduction -- 1.2. Motivation by numbers -- 1.3. Evolution -- 1.4. Architecture -- 1.5. Characteristics -- 1.6. Technical challenges and issues -- 1.7. Wireless technology -- 1.8. Standards -- 1.8.1. IEEE WAVE stack -- 1.8.2. ETSI standards -- 1.8.3. The 3GPP standard -- 1.9. Types -- 1.9.1. The autonomous vehicle (self-dependent) -- 1.9.2. VANET -- 1.9.3. Vehicular clouds -- 1.9.4. Internet of vehicles -- 1.9.5. Social Internet of vehicles -- 1.9.6. Data named vehicular networks -- 1.9.7. Software-defined vehicular networks -- 1.10. Test beds and real implementations -- 1.11. Services and applications -- 1.12. Public opinion -- 1.13. Conclusion -- Chapter 2. Privacy and Security in Vehicular Networks -- 2.1. Introduction -- 2.2. Privacy issue in vehicular networks -- 2.2.1. Types -- 2.2.2. When and how it is threatened? -- 2.2.3. Who is the threat? -- 2.2.4. What are the consequences? -- 2.2.5. How can we protect against it? -- 2.3. State- of-the-art location privacy-preserving solutions -- 2.3.1. Non- cooperative change -- 2.3.2. Silence approaches -- 2.3.3. Infrastructure-based mix-zone approach -- 2.3.4. The cooperation approach (distributed mix-zone) -- 2.3.5. Hybrid approach -- 2.4. Authentication issues in vehicular networks -- 2.4.1. What is being

authenticated in vehicular networks? -- 2.4.2. Authentication types -- 2.4.3. How does authentication risk privacy? -- 2.5. Identity privacy preservation authentication solutions: state of the art -- 2.6. Conclusion -- Chapter 3. Security and Privacy Evaluation Methodology -- 3.1. Introduction -- 3.2. Evaluation methodology -- 3.2.1. Security -- 3.2.2. Privacy -- 3.3. Conclusion -- Chapter 4. The Attacker Model -- 4.1. Introduction -- 4.2. Security objectives. 4.3. Security challenges -- 4.4. Security attacker -- 4.4.1. Aims -- 4.4.2. Types -- 4.4.3. Means -- 4.4.4. Attacks -- 4.4.5. Our attacker model -- 4.5. Conclusion -- Chapter 5. Privacy-preserving Authentication in Cloud-enabled Vehicle Data Named Networks (CVDNN) for Resources Sharing -- 5.1. Introduction -- 5.2. Background -- 5.2.1. Vehicular clouds -- 5.2.2. Vehicular data named networks -- 5.3. System description -- 5.4. Forming cloud-enabled vehicle data named networks -- 5.5. Migrating the local cloud virtual machine to the central cloud -- 5.6. Privacy and authentication when using/providing CVDNN services -- 5.6.1. The authentication process -- 5.6.2. The reputation testimony -- 5.7. The privacy in CVDNN -- 5.8. Discussion and analysis -- 5.8.1. The privacy when joining the VC -- 5.8.2. Privacy while using the VC -- 5.9. Conclusion -- Chapter 6. Privacy-preserving Authentication Scheme for On-road On-demand Refilling of Pseudonym in VANET -- 6.1. Introduction -- 6.2. Network model and system functionality -- 6.2.1. Network model -- 6.2.2. The system functionality -- 6.3. Proposed scheme -- 6.4. Analysis and discussion -- 6.4.1. Security analysis -- 6.4.2. Burrows, Abadi and Needham (BAN) logic -- 6.4.3. SPAN and AVISPA tools -- 6.5. Conclusion -- Chapter 7. Preserving the Location Privacy of Vehicular Ad hoc Network Users -- 7.1. Introduction -- 7.2. Adversary model -- 7.3. Proposed camouflage-based location privacy-preserving scheme -- 7.3.1. Analytical model -- 7.3.2. Simulation -- 7.4. Proposed hybrid pseudonym change strategy -- 7.4.1. Hypothesis and assumptions -- 7.4.2. Changing the pseudonyms -- 7.4.3. The simulation -- 7.5. Conclusion -- Chapter 8. Preserving the Location Privacy of Internet of Vehicles Users -- 8.1. Introduction -- 8.2. CE-IoV -- 8.3. Privacy challenges -- 8.4. Attacker model. 8.5. CLPPS: cooperative-based location privacy-preserving scheme for Internet of vehicles -- 8.5.1. Simulation -- 8.5.2. Comparative study and performance analysis -- 8.6. CSLPPS: concerted silence-based location privacy-preserving scheme for Internet of vehicles -- 8.6.1. The proposed solution -- 8.6.2. Simulation results -- 8.6.3. Comparative study performance analysis -- 8.7. Obfuscation-based location privacy-preserving scheme in cloud-enabled Internet of vehicles -- 8.7.1. The proposition -- 8.7.2. Study of feasibility using game theoretic approach -- 8.7.3. The simulation -- 8.7.4. Analytical model -- 8.7.5. Comparative study -- 8.8. Conclusion -- Chapter 9. Blockchain-based Privacy-aware Pseudonym Management Framework for Vehicular Networks -- 9.1. Introduction -- 9.2. Background -- 9.2.1. Public key infrastructure (PKI) -- 9.2.2. Vehicular PKI -- 9.2.3. Blockchain technology -- 9.2.4. Blockchain of blockchains -- 9.3. Related works -- 9.3.1. Blockchain-based PKI -- 9.3.2. Privacy-aware blockchain-based PKI -- 9.3.3. Monero -- 9.3.4. Blockchain-based vehicular PKI -- 9.4. Key concepts -- 9.4.1. Ring signature -- 9.4.2. One-time address -- 9.5. Proposed solution -- 9.5.1. General description -- 9.5.2. Registration to the blockchain -- 9.5.3. Certifying process -- 9.5.4. Revocation process -- 9.5.5. Transaction structure and validation -- 9.5.6. Block structure and validation -- 9.5.7. Authentication using blockchain -- 9.6. Analysis -- 9.7. Comparative study -- 9.8. Conclusion -- Conclusion -- References -- Index --

EULA.

---