

---

# Contents

---

<b>Preface</b> . . . . .	xi
<b>List of Acronyms</b> . . . . .	xiii
<b>Introduction</b> . . . . .	xix
<b>Chapter 1. Vehicular Networks</b> . . . . .	1
1.1. Introduction . . . . .	1
1.2. Motivation by numbers . . . . .	2
1.3. Evolution . . . . .	3
1.4. Architecture . . . . .	4
1.5. Characteristics . . . . .	5
1.6. Technical challenges and issues . . . . .	6
1.7. Wireless technology . . . . .	7
1.8. Standards . . . . .	7
1.8.1. IEEE WAVE stack . . . . .	8
1.8.2. ETSI standards . . . . .	9
1.8.3. The 3GPP standard . . . . .	9
1.9. Types . . . . .	10
1.9.1. The autonomous vehicle (self-dependent) . . . . .	10
1.9.2. VANET . . . . .	11
1.9.3. Vehicular clouds . . . . .	11
1.9.4. Internet of vehicles . . . . .	12
1.9.5. Social Internet of vehicles . . . . .	14
1.9.6. Data named vehicular networks . . . . .	15
1.9.7. Software-defined vehicular networks . . . . .	15

---

1.10. Test beds and real implementations . . . . .	16
1.11. Services and applications . . . . .	17
1.12. Public opinion . . . . .	19
1.13. Conclusion . . . . .	20
<b>Chapter 2. Privacy and Security in Vehicular Networks . . . . .</b>	<b>21</b>
2.1. Introduction . . . . .	21
2.2. Privacy issue in vehicular networks . . . . .	22
2.2.1. Types. . . . .	23
2.2.2. When and how it is threatened? . . . . .	24
2.2.3. Who is the threat? . . . . .	24
2.2.4. What are the consequences? . . . . .	24
2.2.5. How can we protect against it? . . . . .	25
2.3. State-of-the-art location privacy-preserving solutions . . . . .	28
2.3.1. Non-cooperative change . . . . .	28
2.3.2. Silence approaches . . . . .	28
2.3.3. Infrastructure-based mix-zone approach . . . . .	28
2.3.4. The cooperation approach (distributed mix-zone) . . . . .	36
2.3.5. Hybrid approach . . . . .	36
2.4. Authentication issues in vehicular networks . . . . .	49
2.4.1. What is being authenticated in vehicular networks? . . . . .	49
2.4.2. Authentication types . . . . .	50
2.4.3. How does authentication risk privacy? . . . . .	51
2.5. Identity privacy preservation authentication solutions: state of the art . . . . .	52
2.6. Conclusion . . . . .	54
<b>Chapter 3. Security and Privacy Evaluation Methodology . . . . .</b>	<b>55</b>
3.1. Introduction . . . . .	55
3.2. Evaluation methodology . . . . .	58
3.2.1. Security . . . . .	58
3.2.2. Privacy . . . . .	66
3.3. Conclusion . . . . .	74
<b>Chapter 4. The Attacker Model . . . . .</b>	<b>75</b>
4.1. Introduction . . . . .	75
4.2. Security objectives. . . . .	76
4.3. Security challenges . . . . .	78
4.4. Security attacker . . . . .	79
4.4.1. Aims . . . . .	80
4.4.2. Types. . . . .	80
4.4.3. Means . . . . .	81
4.4.4. Attacks . . . . .	82

4.4.5. Our attacker model . . . . .	85
4.5. Conclusion . . . . .	90
<b>Chapter 5. Privacy-preserving Authentication in Cloud-enabled Vehicle Data Named Networks (CVDNN) for Resources Sharing . . . . .</b>	<b>91</b>
5.1. Introduction . . . . .	91
5.2. Background. . . . .	92
5.2.1. Vehicular clouds . . . . .	92
5.2.2. Vehicular data named networks . . . . .	94
5.3. System description. . . . .	94
5.4. Forming cloud-enabled vehicle data named networks . . . . .	95
5.5. Migrating the local cloud virtual machine to the central cloud . . . . .	97
5.6. Privacy and authentication when using/providing CVDNN services . . . . .	97
5.6.1. The authentication process . . . . .	98
5.6.2. The reputation testimony . . . . .	100
5.7. The privacy in CVDNN. . . . .	102
5.8. Discussion and analysis . . . . .	103
5.8.1. The privacy when joining the VC . . . . .	103
5.8.2. Privacy while using the VC . . . . .	106
5.9. Conclusion . . . . .	106
<b>Chapter 6. Privacy-preserving Authentication Scheme for On-road On-demand Refilling of Pseudonym in VANET . . . . .</b>	<b>109</b>
6.1. Introduction . . . . .	109
6.2. Network model and system functionality . . . . .	111
6.2.1. Network model . . . . .	111
6.2.2. The system functionality . . . . .	113
6.3. Proposed scheme. . . . .	114
6.4. Analysis and discussion. . . . .	119
6.4.1. Security analysis . . . . .	119
6.4.2. Burrows, Abadi and Needham (BAN) logic . . . . .	124
6.4.3. SPAN and AVISPA tools . . . . .	126
6.5. Conclusion . . . . .	129
<b>Chapter 7. Preserving the Location Privacy of Vehicular Ad hoc Network Users . . . . .</b>	<b>131</b>
7.1. Introduction . . . . .	131
7.2. Adversary model. . . . .	133
7.3. Proposed camouflage-based location privacy-preserving scheme . . . . .	133
7.3.1. Analytical model . . . . .	135
7.3.2. Simulation . . . . .	136
7.4. Proposed hybrid pseudonym change strategy . . . . .	141

---

7.4.1. Hypothesis and assumptions . . . . .	141
7.4.2. Changing the pseudonyms . . . . .	142
7.4.3. The simulation . . . . .	145
7.5. Conclusion . . . . .	148
<b>Chapter 8. Preserving the Location Privacy of Internet of Vehicles Users . . . . .</b>	<b>151</b>
8.1. Introduction . . . . .	151
8.2. CE-IoV . . . . .	153
8.3. Privacy challenges . . . . .	156
8.4. Attacker model . . . . .	157
8.5. CLPPS: cooperative-based location privacy-preserving scheme for Internet of vehicles . . . . .	158
8.5.1. Simulation . . . . .	159
8.5.2. Comparative study and performance analysis . . . . .	163
8.6. CSLPPS: concerted silence-based location privacy-preserving scheme for Internet of vehicles . . . . .	166
8.6.1. The proposed solution . . . . .	166
8.6.2. Simulation results . . . . .	167
8.6.3. Comparative study performance analysis . . . . .	169
8.7. Obfuscation-based location privacy-preserving scheme in cloud-enabled Internet of vehicles . . . . .	171
8.7.1. The proposition . . . . .	171
8.7.2. Study of feasibility using game theoretic approach . . . . .	173
8.7.3. The simulation . . . . .	174
8.7.4. Analytical model . . . . .	177
8.7.5. Comparative study . . . . .	178
8.8. Conclusion . . . . .	180
<b>Chapter 9. Blockchain-based Privacy-aware Pseudonym Management Framework for Vehicular Networks . . . . .</b>	<b>181</b>
9.1. Introduction . . . . .	181
9.2. Background . . . . .	183
9.2.1. Public key infrastructure (PKI) . . . . .	183
9.2.2. Vehicular PKI . . . . .	185
9.2.3. Blockchain technology . . . . .	185
9.2.4. Blockchain of blockchains . . . . .	190
9.3. Related works . . . . .	191
9.3.1. Blockchain-based PKI . . . . .	191
9.3.2. Privacy-aware blockchain-based PKI . . . . .	191
9.3.3. Monero . . . . .	191
9.3.4. Blockchain-based vehicular PKI . . . . .	192

---

9.4. Key concepts . . . . .	192
9.4.1. Ring signature . . . . .	192
9.4.2. One-time address . . . . .	194
9.5. Proposed solution . . . . .	195
9.5.1. General description . . . . .	195
9.5.2. Registration to the blockchain . . . . .	196
9.5.3. Certifying process. . . . .	196
9.5.4. Revocation process . . . . .	197
9.5.5. Transaction structure and validation . . . . .	197
9.5.6. Block structure and validation . . . . .	200
9.5.7. Authentication using blockchain. . . . .	201
9.6. Analysis . . . . .	202
9.7. Comparative study. . . . .	206
9.8. Conclusion . . . . .	206
<b>Conclusion</b> . . . . .	211
<b>References</b> . . . . .	215
<b>Index</b> . . . . .	229