

Contents

1	Introduction	1
1.1	Motivation	1
1.2	Contributions	3
1.3	Outline	6
2	Car-to-X Communication: System Architecture and Applications	9
2.1	C2X System Architecture	10
2.1.1	Components and Communication Channels	11
2.1.2	Forwarding Types	12
2.1.3	Message Types	13
2.2	Car-to-X Applications and Use Cases	15
2.2.1	Cooperative Road Safety	15
2.2.2	Cooperative Traffic Efficiency	18
2.2.3	Cooperative Local Services	19
3	Application Layer Security: Public Key Infrastructure	21
3.1	Motivation	21
3.1.1	Security Motivation	22
3.1.2	Privacy Motivation	24
3.2	Security and Privacy Objectives	25
3.2.1	Security Objectives	26
3.2.2	Privacy Objectives	27
3.3	Security Protection	28
3.3.1	Cryptographic Message Signing	28
3.3.2	Cryptographic Message Verification	29
3.4	Privacy Protection	31
3.5	Public Key Infrastructure	34
3.5.1	PKI Architectural Overview	34
3.5.2	PKI Management Protocols	35
3.5.3	PKI Implementation	42
3.6	Conclusion	44
4	Facility Layer Security: Mobility Data Verification	45
4.1	Motivation	45
4.2	Related Work	48
4.2.1	Mobility Verification Approaches	48
4.2.2	Mobility Verification Frameworks	49
4.2.3	Assessment	50
4.3	Mobility Data Verification Framework	51
4.3.1	Path Prediction	52

4.3.2	Sensor-based Verification	59
4.3.3	Maneuver Recognition	62
4.4	Evaluation Results	72
4.4.1	Implementation	72
4.4.2	Common Traffic Scenarios	72
4.4.3	Dynamic Traffic Scenarios	76
4.5	Conclusion	78
5	Network Layer Security: Group Privacy Protocols	81
5.1	Motivation	82
5.1.1	Privacy Measure based on Driver Entropy	82
5.1.2	Privacy Measure based on Traceability	85
5.1.3	Privacy Level of Simple Pseudonym Changes	86
5.2	Related Work	87
5.2.1	Mix Zones	87
5.2.2	Situational Mix Zones	87
5.2.3	Cryptographic Mix Zones	91
5.3	Privacy Protocol Objectives	96
5.4	System Requirements	97
5.4.1	Spatial Synchronization	97
5.4.2	Temporal Synchronization	99
5.5	Group Establishment Protocol I: C2CGE.1	99
5.5.1	Initial Group Definition	99
5.5.2	Key Fragment Distribution	100
5.5.3	Group Key Generation	101
5.5.4	Anonymous Message Exchange	102
5.5.5	Implementation	102
5.6	Group Establishment Protocol II: C2CGE.2	105
5.6.1	Initial Group Definition	106
5.6.2	Key Fragment Distribution	107
5.6.3	Group Key Calculation	107
5.6.4	Anonymous Message Exchange	108
5.6.5	Implementation	109
5.7	Group Management	110
5.7.1	Group Join	110
5.7.2	Group Interference	111
5.7.3	Group Disjoin	113
5.8	Evaluation Results	113
5.8.1	Protocol Verification	114
5.8.2	Protocol Comparison	119
5.8.3	Simulation Setup	122
5.8.4	Temporal Behavior Evaluation	123
5.8.5	Privacy Evaluation	124
5.9	Conclusion	129
6	Physical Layer Security: Secure Car-to-X Beamforming	131
6.1	Motivation	132
6.1.1	Congestion Avoidance	132

6.1.2	Privacy Enhancements	133
6.1.3	Security Enhancements	134
6.2	Related Work	134
6.2.1	IEEE 802.11p	134
6.2.2	Car-to-X Antenna System Design	135
6.2.3	Physical Security with Antennas	136
6.3	Secure Car-to-X Beamforming Design Flow	137
6.3.1	Design Flow	138
6.3.2	Simulation and Evaluation Tool Chain	140
6.4	Secure C2X Beamforming Algorithm I: Antenna Array	142
6.4.1	Use Case Requirements	143
6.4.2	Antenna Pattern Model	144
6.4.3	Beamforming Algorithm	150
6.5	Secure C2X Beamforming Algorithm II: sim ^{TD} Antenna	153
6.5.1	Use Case Requirements	154
6.5.2	Antenna Pattern Model	154
6.5.3	Beamforming Algorithm	154
6.6	Evaluation Results	160
6.6.1	SCBM Metric	161
6.6.2	Beamforming Evaluation	167
6.7	Conclusion	167
7	Conclusions and Perspectives	169
	Appendix	171
A	Network Layer Security: Situational Mix Zone Detection	171
B	Side View to Privacy	175
	Bibliography	179