

Contents

Preface	vii
1 Introduction	1
1.1 Book Overview	3
2 Centralized Multi-user Key Management	7
2.1 Basic Multicast Information Theory	7
2.2 Overview of Multicast Key Management	11
2.3 Requirements for Centralized Group Key Management	13
2.4 Basic Polynomial Interpolation Scheme	15
2.4.1 Resistance to Attack	17
2.4.2 Anonymity Reduces Communication Overhead	18
2.5 Extending to a Scalable Protocol	19
2.5.1 Basic Protocol Primitives	21
2.5.2 Advanced Protocol Operations	23
2.6 Architectural Considerations	26
2.6.1 Optimization of Tree Degree for Communication	26
2.6.2 Binomial Occupancy Model	30
2.6.3 Communication Overhead	32
2.6.4 Computational Complexity	35
2.7 Chapter Summary	36
3 Group Key Agreement Techniques in Heterogeneous Networks	39
3.1 Introduction	39

3.2	Group DH Overview	41
3.3	Conference Trees and the Butterfly Scheme	43
3.4	Computational Considerations	49
3.4.1	Minimizing Total Cost	49
3.4.2	Budget Constraints	51
3.4.3	Combined Budget and Cost Optimization	54
3.5	Efficiency and Feasibility Evaluation	56
3.5.1	Comparison of Total Cost	56
3.5.2	Feasibility Comparison	58
3.6	System Sensitivity to False Costs	62
3.6.1	Sensitivity to Approximate Costs	62
3.6.2	Sensitivity to Costs from Untrustworthy Users	64
3.7	Chapter Summary	68
4	Optimizing Rekeying Costs in Group Key Agreement	71
4.1	Join-Exit Tree for Reducing Latency in Key Agreement Protocols	72
4.1.1	Time-efficiency Measurement	72
4.1.2	Join-Exit Tree (JET) Topology	73
4.1.3	The Join Tree Algorithm	74
4.1.4	The Exit Tree Algorithm	80
4.1.5	Performance Analysis	83
4.2	Optimizing Rekeying Cost	85
4.2.1	Performance Metric Review	85
4.2.2	PFMH Key Tree Structure and Basic Procedures	87
4.2.3	PACK: an PFMH tree-based contributory group key agreement	97
4.2.4	Performance Evaluation and Comparison	107
4.2.5	Contributory Group Key Agreement with Key Validation	109
4.3	Chapter Summary	110
5	Optimizing Multicast Key Management for Cellular Multicasting	113
5.1	Targeting Property of Rekeying Messages	114
5.2	Topology-aware Key Management	115
5.3	Topology-aware Key Management in Cellular Wireless Network	115
5.3.1	Key Tree Design	116
5.3.2	Performance Metrics	117
5.3.3	Handoff Schemes for TMKM Tree	118
5.4	Performance Analysis	122
5.5	Separability of the Optimization Problem	126
5.6	Optimizing TMKM Tree Design	127
5.6.1	Dynamic membership model	128
5.6.2	ALX tree structure	129

5.6.3	User subtree design	132
5.6.4	BS subtree design	133
5.6.5	SH subtree design	134
5.7	Performance Evaluation	136
5.7.1	One-SH systems	136
5.7.2	SH subtree design methods	139
5.7.3	Multiple-SH systems	140
5.8	Chapter Summary	142
6	Key Management and Distribution for Securing Multimedia Multicasts	143
6.1	A Basic Key Management Scheme	145
6.1.1	Key Refreshing	146
6.1.2	Member Join	147
6.1.3	Member Departure	147
6.2	Distribution of Rekeying Messages for Multimedia	148
6.2.1	Media-Independent Channel	150
6.2.2	Media-Dependent Channel	152
6.3	An Improved Rekeying Message Format	155
6.3.1	Basic Message Form	156
6.3.2	Security Analysis of Residue-based Method	157
6.3.3	Achieving Scalability	163
6.4	System Feasibility Study	166
6.5	Extensions to Multilayered Services	169
6.6	Chapter Summary	170
7	Hierarchical Access Control for Multi-Group Scenarios	175
7.1	Hierarchical Access Control: Problem Formulation	176
7.1.1	System description	176
7.1.2	Security requirements	177
7.1.3	Data encryption and hierarchical key management	178
7.2	Centralized Multi-group Key Management Scheme	179
7.2.1	Independent key trees for hierarchical access control	179
7.2.2	Multi-group key management scheme	179
7.3	Performance Measures and Analysis	184
7.3.1	Storage overhead	185
7.3.2	Rekey overhead	188
7.4	Simulations and Performance Comparison	189
7.4.1	Statistical dynamic membership model	189
7.4.2	Performance with different group size	191
7.4.3	Scalability	192
7.4.4	Performance with different transition probability	192
7.4.5	Simulation of multi-service applications	196
7.5	Contributory Multi-group Key Management	196
7.6	Related Work	199

7.7	Chapter Summary	200
8	Protecting Membership Information in Secure Multicasting	203
8.1	GDI Disclosure in Centralized Key Management Schemes	204
8.1.1	Attack 1: Estimation of $J(t_0, t_1)$ and $L(t_0, t_1)$ from rekeying-message format	205
8.1.2	Attack 2: Estimation of the group size from the rekeying-message-size	206
8.1.3	Attack 3: Estimation of group size based on key IDs	208
8.1.4	Discussion on three attacks	211
8.1.5	GDI vulnerability in prevalent key management schemes	212
8.2	Defense Techniques	213
8.3	Optimization	218
8.3.1	The leakage of GDI	218
8.3.2	Communication Overhead	220
8.3.3	System Optimization	221
8.4	Simulations	221
8.5	GDI Disclosure and Protection in Contributory Key Management Schemes	223
8.5.1	Fully and Partially Contributory Key Management Schemes	226
8.5.2	GDI Disclosure in Contributory Key Management Schemes	227
8.5.3	The Cost of Preventing GDI leakage	227
8.5.4	More on GDI Leakage Problem	228
8.6	Chapter Summary	228
9	Reducing Delay and Enhancing DoS Resistance in Multicast Authentication	231
9.1	Background Literature and TESLA	232
9.1.1	Related Work	232
9.1.2	TESLA Overview	234
9.1.3	Examination of Trust in TESLA	235
9.2	Staggered TESLA: Multi-Grade Multicast Authentication	236
9.2.1	Format of the Packet	237
9.2.2	Multi-Grade Source Authentication	238
9.3	Reduced-Delay Multicast Authentication Schemes	243
9.3.1	Staggered TESLA with Proximity Protection	243
9.3.2	Distributed Key Distributors	245
9.4	Buffer Requirements and Tradeoffs	246
9.5	Simulations and Performance Analysis	251
9.5.1	Simulations on Multi-Grade Authentication	251
9.5.2	Performance Analysis of Staggered TESLA	252
9.5.3	Impact of the Locations of Adversaries	255

9.5.4	Simulation on Reducing Authentication Delay	260
9.6	Conclusion	262
10	An Authentication Service for Sensor and Ad Hoc Networks	265
10.1	Introduction	265
10.1.1	Hierarchical Sensor Network	266
10.2	TESLA and TESLA Certificates	268
10.2.1	TESLA Certs	269
10.3	Overview of the Authentication Framework	270
10.4	Certificates	272
10.4.1	Initial Certs	272
10.4.2	Runtime Certs	273
10.5	Certificate Renewal	274
10.5.1	Access Point	274
10.5.2	Sensor Node	274
10.6	Entity Authentication	275
10.6.1	Access Point	275
10.6.2	Forwarding Nodes	275
10.6.3	Sensor Nodes	276
10.7	Roaming and Handoff	277
10.7.1	Forwarding Nodes	277
10.7.2	Sensor Nodes	277
10.8	Data Origin Authentication	278
10.8.1	Sending Sensor Data in Weak Mode	278
10.8.2	Sending Sensor Data in Assured Mode	279
10.9	Evaluation	280
10.9.1	Security Analysis	280
10.9.2	Performance Analysis	281
10.10	Conclusion	282
	References	287
	Index	301