

TRUST ENHANCED SECURITY
FRAMEWORK FOR MOBILE AD HOC
WIRELESS NETWORKS

By

Venkatesan Balakrishnan

A THESIS SUBMITTED TO MACQUARIE UNIVERSITY

FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

DEPARTMENT OF COMPUTING

NOVEMBER 2010



MACQUARIE
UNIVERSITY
FACULTY OF SCIENCE

© Venkatesan Balakrishnan, 2010.

Typeset in L^AT_EX 2_ε.

Except where acknowledged in the customary manner, the material presented in this thesis is, to the best of my knowledge, original and has not been submitted in whole or part for a degree in any university.

Venkatesan Balakrishnan

Acknowledgements

I am very thankful to *Prof. Vijayaraghavan Varadharajan*, without whom I would have never reached to this stage of my professional career. I am grateful to him for his guidance and also his motivational talks during those hard moments. I thank him for sharing his knowledge and vision on a variety of thought-provoking topics, ranging from technical to philosophical that have added a new dimension to my thought process. I would like to express my gratitude to *Dr. Udaya Tupakula*, who provided valuable technical insights into my research work and, therefore been a significant factor for its progression. I dedicate all my publications to him, especially to his efforts in reviewing all the draft versions and constantly emerging out with suggestions for improvements, until those drafts were published. I appreciate *Ms. Andrina Brennan* for her kindness and the difference she made to my research work by saving innumerable hours that would have been lost in administration works. I would like to thank *Defence Signals Directorate (DSD), Australia* for supporting this research work.

I am thankful to *Dr. Sarath Indrakanti*, who inspired me with his research dedication and for sharing his research experience and working with me during those countless long nights. I would like to thank *Dr. Vijayakrishnan Pasupathinathan* for his stimulating technical discussions and being there whenever I invited him for a short-break from research work. My research implementation would have not met the deadlines without the contributions from *Phillip Lucs*. I am very grateful to him for bringing many years of his industrial experience in software engineering and, working countless nights and weekends with me during his Bachelors Honours degree. I am very thankful

to *Dr. Venkatakrishnan Balasubramanian Appiah* for his motivational speeches on various topics and helping me to get the casual academic teaching role that supported my financial requirements. I thank *Dilshan Jayarathna, Adam Shah, Suresh Mulavineth* and *Richard Miller* for providing the technical resources and supplying with Gigabytes of storage space for my simulation logs, in particular, during those days when Gigabytes of storage space was expensive. I appreciate *Dr. Marie Elisabeth Gaup Moe* from NUST, Norway for sharing her knowledge on MANETs that support anonymous communications. *Mark Bazant*, who was my Team Lead at CSC deserves a loud appreciation for accommodating my leave and time-in-lieu requests without which the thesis writing would have been further delayed. I am thankful to the thesis proof-reader, *Tony Roberts* for his quick responses, regardless of the time of the day or night and, polishing this thesis within a short notice. I would also like to thank the thesis reviewers for their time and effort in reviewing this thesis and providing valuable comments and feedbacks.

To all the well-wishers, who have supported me all these years. Foremost thanks goes to *Rajesh Udayamurthy* and *Ramya Rajesh* for being kind, supportive and caring to me during those solitary days of my research degree. My ex-flatmate, *Jayachandra Rao* stands out among all the hearts that enabled me to transform a research idea into this well-researched thesis work. I am very grateful for his generosity that took care of all house-keeping activities and provided cooked food regardless of the time of the day or night. I dedicate this thesis to him for his selfless nature and all the care that he has showered during my stay with him. I am very grateful and thankful to my mentors, *Dr. Archana Parashar* and *Dr. M Vasudevacharya* for their support, love and guidance for all these years, without which none of the significant accomplishments and progressions would have happened during the last eight years of my life. To my loveable parents and adorable brothers, who have been wonderful, selfless and been a platform to make all my dreams come true. And to my admirable wife, who is always there for me. Finally, to the fundamental physical forces in this universe that manifested this insignificant agglomeration of atoms and molecules to reach a significant achievement during its lifetime.

List of Publications

Book Chapters

- V. Balakrishnan, V. Varadharajan, and U. K. Tupakula, *Trust Management in Mobile Ad hoc Networks*. Handbook of Wireless Ad hoc and Sensor Networks, Springer (London), 2009.
- V. Balakrishnan, V. Varadharajan, and U. K. Tupakula, *Security and Authentication*. Mobile Wireless Networks: Integrated Service Issues, Wiley-Blackwell, 2009.
- V. Balakrishnan, V. Varadharajan, U. K. Tupakula, and P. Lucs, *SMRTI:: Secure MANET Routing with Trust Intrigue*. Mobile Intelligence: Mobile Computing and Computational Intelligence, John Willey & Sons, Inc., 2010.
- V. Balakrishnan, V. Varadharajan, and U. K. Tupakula, *Security in Mobile Ad-hoc Networks*. Handbook of Communication Networks and Distributed Systems, World Scientific (Singapore) (*Accepted for publication*).

Conference Proceedings

- V. Balakrishnan, V. Varadharajan, and U. K. Tupakula, *Subjective Logic Based Trust Model for Mobile Ad-hoc Networks*. Proceedings of the 4th ACM International Conference on Security and Privacy in Communication Networks (SecureComm 2008), Istanbul, Turkey, September 2008.

-
- V. Balakrishnan, V. Varadharajan, U. K. Tupakula, and P. Lucs, *TEAM: Trust Enhanced Security Architecture for Mobile Ad-hoc Networks*. Proceedings of the 15th IEEE International Conference on Networks (ICON 2007), Adelaide, Australia, pp. 182-187, November 2007.
 - V. Balakrishnan, V. Varadharajan, U. K. Tupakula, and P. Lucs, *Trust Integrated Cooperation Architecture for Mobile Ad-hoc Networks*. Proceedings of the 4th IEEE International Symposium on Wireless Communication Systems (ISWCS 2007), Trondheim, Norway, pp. 592-596, October 2007.
 - V. Balakrishnan, V. Varadharajan, U. K. Tupakula, and M. E. Gaup Moe, *Mitigating Flooding Attacks in Mobile Ad-hoc Networks Supporting Anonymous Communications*. Proceedings of the 2nd IEEE International Conference on Wireless Broadband and Ultra Wideband Communication (AusWireless 2007), Sydney, Australia, pp. 29-34, August 2007.
 - V. Balakrishnan, V. Varadharajan, U. K. Tupakula, and P. Lucs, *Trust and Recommendations in Mobile Ad hoc Networks*. Proceedings of the 3rd International Conference on Networking and Services (ICNS 2007), Athens, Greece, pp. 64-69, June 2007.
 - V. Balakrishnan, V. Varadharajan, P. Lucs, and U. K. Tupakula, *Trust Enhanced Secure Mobile Ad hoc Network Routing*. Second IEEE International Symposium on Pervasive Computing and Ad Hoc Communications (PCAC 2007), Proceedings of the 21st IEEE International Conference on Advanced Information Networking and Applications Workshops(AINAW 2007), Niagara Falls, Canada, pp. 27-33, May 2007.
 - V. Balakrishnan, V. Varadharajan, and U. K. Tupakula, *Fellowship: Defense against Flooding and Packet Drop Attacks in MANET*. Proceedings of the 10th IEEE/IFIP Network Operations and Management Symposium (NOMS 2006), Vancouver, Canada, pp. 1-4, April 2006.

- V. Balakrishnan, and V. Varadharajan, *Fellowship in Mobile Ad hoc Networks*. Proceedings of the 1st IEEE International Conference on Security and Privacy in Communications Networks (SecureComm 2005), Athens, Greece, pp. 225-227, September 2005.
- V. Balakrishnan, and V. Varadharajan, *Packet Drop Attack: A Serious Threat to Operational Mobile Ad hoc Networks*. Proceedings of the International Conference on Networks and Communication Systems (NCS 2005), Krabi, Thailand, pp. 89-95, April 2005.
- V. Balakrishnan, and V. Varadharajan, *Designing Secure Wireless Mobile Ad hoc Networks*. Proceedings of the 19th IEEE International Conference on Advanced Information Networking and Applications (AINA 2005), Taipei, Taiwan, pp. 5-8, March 2005.

Abstract

The advent of wireless communication and the proliferation of handheld devices have significantly advanced the growth of nomadic communications. Capability of these handheld mobile devices to self-organise themselves on fly in the absence of an infrastructure and to extend their communications beyond their wireless radio range have potentially led to the development of Mobile Ad hoc Networks (MANET). Security is one of the most indispensable research areas and plays a central role in determining the success of civilian and commercial mobile ad hoc networks. Unfortunately, mobile nodes struggle to enlist trusted intermediaries for communication with various destinations since trusted intermediaries are a prerequisite to keep those communications alive and free from active attacks. Although few integrated security systems exist for the MANETs, a two-layered (prevention and detection-reaction systems) trust-enhanced security architecture is yet to be seen for the MANETs to the best of our knowledge. The two-layered approach is so required for the prevention and detection-reaction systems to complement each other to deliver a trustworthy, secure, and an operational routing layer amidst the inherent issues.

Therefore this thesis, (a) *focuses on the systematic study of the security threats and attacks and, adversaries in the MANETs and accordingly the analysis of the strength of solutions that have been proposed within different categories of security systems*, (b) *proposes novel techniques to meet the shortcomings of proposed security solutions and thence to develop a realistic two-layered **Trust Enhanced security Architecture***

*for the MANETs (**TEAM**). These novel techniques include, (a) an obligation-based **fellowship** model to motivate cooperation among the mobile nodes, (b) **Secure MANET Routing with Trust Intrigue (SMRTI)** that resolves the limitations harboured by related trust models and capitalises all the evidence that are available within the limitations of the MANET for making better routing decisions and, (c) a new secure routing protocol known as **Scasec**. Furthermore, fellowship model is extended to defend flooding attacks in the MANETs that support anonymous communications. Similarly, SMRTI is extended to incorporate subjective logic with a focus to resolve the notion of uncertainty in the trust relationships established between newly-joining and existing mobile nodes. Finally, the better performance results of all these proposed techniques are demonstrated using varied simulation scenarios.*

Contents

Acknowledgements	v
List of Publications	vii
Abstract	xi
List of Figures	xxi
List of Tables	xxv
List of Acronyms	xxix
List of Symbols	xxxiii
1 Introduction	1
1.1 State of Art	2
1.2 Proposed Approach	5
1.3 Thesis Overview	6
2 Related Work	13
2.1 Introduction	13
2.2 Attacks and Adversaries	16
2.2.1 Passive Attacks	16
2.2.2 Active Attacks	17

2.2.3	Security Concepts	19
2.3	Anonymous Secure Routing in MANET	20
2.4	Secure Routing in MANET	22
2.4.1	Authenticated Routing for Ad-hoc Networks (ARAN)	22
2.4.2	Secure Ad-hoc On-demand Distance Vector (SAODV)	23
2.4.3	Ariadne	24
2.4.4	Secure Routing Protocol (SRP)	26
2.4.5	Building Secure Routing out of an Incomplete Set of Security Association (BISS)	27
2.5	Key Management in MANET	29
2.5.1	Partially-Distributed Public-Key System	29
2.5.2	Completely-Distributed Public-Key System	31
2.5.3	Identity-based Public-Key System	31
2.5.4	Transitive-Chain based Public-Key System	32
2.5.5	Limitations	32
2.6	Incentive and Game-theory based Systems	33
2.7	Reputation and Trust Management Systems	35
2.7.1	Concepts – Trust and Reputation	36
2.7.2	Components of Trust Management Systems	37
2.7.3	Significance in the MANET	38
2.7.4	State of the Art	39
2.7.5	Limitations	46
2.8	Motivation and Security Requirements	52
2.9	Conclusion	55
3	Fellowship: Mitigating Packet Drop and Flooding Attacks	57
3.1	Introduction	57
3.2	Adversary Model	60
3.3	Fellowship Model	62
3.3.1	Fundamental Concepts	62

3.3.2	Overview of Components	64
3.3.3	Data Structures	65
3.3.4	System Design	67
3.3.5	System Operation	83
3.4	Simulation	88
3.4.1	Simulator Overview	88
3.4.2	Additional Tools	92
3.4.3	Simulation Setup	92
3.4.4	Simulation Results – Packet Drop Attack	95
3.4.5	Simulation Results – Flooding Attack	102
3.5	Limitations	109
3.5.1	Pure MANET	109
3.5.2	Preventive Vs Reactive Approach	110
3.5.3	Formal Basis	110
3.5.4	Resource as Metrics	111
3.6	Conclusion	111
4	SMRTI: Secure MANET Routing with Trust Intrigue	115
4.1	Introduction	115
4.2	Proposed Approach	116
4.2.1	Evidence of Trustworthiness	117
4.2.2	Evidence-to-Opinion Mapping	118
4.2.3	Trust Decisions	119
4.3	Architectural Design	120
4.3.1	Detection Layer	120
4.3.2	Reaction Layer	121
4.4	System Operation	122
4.4.1	Sequence Number Update	123
4.4.2	Route Recording	125
4.4.3	Route Selection	126

4.4.4	Route Pruning	126
4.4.5	Packet Propagation	128
4.4.6	Sensitive Communications	129
4.4.7	Route Maintenance	131
4.5	Reaction Component	132
4.5.1	Trust-evaluation Module	132
4.5.2	Trust-over-reputation Module	134
4.6	Detection Component	134
4.6.1	Direct Reputation	135
4.6.2	Observed Reputation	137
4.6.3	Recommended Reputation	139
4.7	Reputation-update	144
4.8	Limitations	147
4.8.1	Extension to the Pure MANET	148
4.8.2	Limitations on Promiscuous Monitoring	148
4.8.3	Constrained Defence against Route Reply Modification	151
4.8.4	Limited Availability of Observed and Recommended Evidence	153
4.8.5	Initial Arbitrary Reputations	155
4.9	Conclusion	156
5	Performance Analysis of SMRTI	159
5.1	Introduction	159
5.2	Adversary Model	160
5.2.1	Route Discovery Disruption	160
5.2.2	Data Flow Disruption	163
5.2.3	Route Maintenance Disruption	165
5.2.4	Gratuitous Detour Attack	165
5.3	Simulation Setup	167
5.3.1	General Simulation Parameters	169
5.3.2	Extensions and Options in DSR	169

5.3.3	Simulation Parameters for SMRTI	170
5.3.4	Simulation Scenarios	171
5.3.5	Performance Metrics	172
5.4	Simulation Results	173
5.4.1	Scenario I	173
5.4.2	Scenario II	178
5.4.3	Scenario III	182
5.4.4	Scenario IV	184
5.4.5	Analysis of Selective Behaviours	187
5.4.6	Discussion	190
5.5	Conclusion	191
6	Trust Integrated Cooperation Architecture for MANET	195
6.1	Introduction	195
6.2	Background	197
6.2.1	Fellowship Model	197
6.2.2	SMRTI Model	199
6.3	Interface Integration	199
6.3.1	Elimination of Contribution-share (η)	200
6.3.2	Amendments to Rate-limitation Component	200
6.3.3	Amendments to Enforcement Component	203
6.3.4	Amendments to Restoration Component	203
6.4	System Operation	204
6.5	Conclusion	206
7	TEAM: Trust Enhanced Security Architecture for MANET	207
7.1	Introduction	207
7.2	Pure MANET – Preventive Mechanisms	208
7.3	SMG: Scalable Multi-service Key Management	209
7.3.1	System Initialisation	210
7.3.2	Encryption-Decryption Process	211

7.3.3	Discussion	212
7.4	Scasec: Secure Routing in Managed MANET	213
7.4.1	Route Request (RREQ) Propagation in Scasec	215
7.4.2	Route Reply (RREP) Propagation in Scasec	217
7.4.3	Secure Data Flow using Scasec	218
7.4.4	Discussion	219
7.5	TEAM	221
7.5.1	Interface Integration	221
7.5.2	System Operation	223
7.6	Conclusion	226
8	Mitigating Flooding Attacks in Anonymous Communications	229
8.1	Introduction	229
8.2	Anonymous Secure Routing (ASR) Protocol	231
8.3	Analysis	234
8.4	Adapted Fellowship Model	235
8.4.1	System Operation	237
8.5	Simulation	239
8.5.1	Simulation Setup	239
8.5.2	Simulation Results	242
8.6	Conclusion	244
9	SL-SMRTI: Subjective Logic based SMRTI	245
9.1	Introduction	245
9.2	SMRTI – Overview	247
9.3	Subjective Logic and MANET	248
9.3.1	Overview of Subjective Logic	248
9.3.2	Subjective Logic tailored for MANET	253
9.4	Architecture of SL-SMRTI	265
9.4.1	Formal Representation of SL-SMRTI	265
9.4.2	System Operation	266

9.4.3	Trust Evaluation	272
9.4.4	Direct Opinion	273
9.4.5	Observed-Opinion	274
9.4.6	Recommended Opinion	275
9.5	Adversary Model	277
9.5.1	Modification of Route Request	278
9.5.2	Modification of Route Reply and Route Error	281
9.5.3	SL-SMRTI's Effect on Adversary Model	284
9.6	Simulation	285
9.6.1	Simulation Parameters	286
9.6.2	Simulation Scenarios	288
9.6.3	Simulation Results	289
9.6.4	Discussion	292
9.7	Limitations	294
9.7.1	Synonymous with SMRTI	294
9.7.2	Contrast with SMRTI	295
9.7.3	Limitations of Subjective Logic	296
9.8	Conclusion	297
10	Conclusion	303
10.1	Further Work	307
A	UML Design Diagrams	311
A.1	Fellowship: Class Diagrams	311
A.2	Fellowship: Sequence Diagrams	312
A.3	SMRTI: Class Diagrams	313
A.4	SMRTI: Sequence Diagrams	313
A.5	DSR and CBR Generator	315
A.6	Class and Sequence Diagrams	315

B Code Snippets	365
B.1 Fellowship Implementation	365
B.2 SMRTI Implementation	382
C Analysis Scripts	423
D Scalable Multi-service Group Key Management	453
D.1 Encryption-Decryption Process in SMG	453
D.1.1 Encryption	454
D.1.2 Decryption	455
References	457

List of Figures

2.1	Components of Envisaged Trust Enhanced Security Architecture. . . .	54
3.1	Components of Fellowship Model.	64
3.2	Interaction among Fellowship, Malicious and Selfish Nodes.	84
3.3	Constituents and Extensions to a Mobile Node.	88
3.4	Performance of Fellowship and DSR-MAC Nodes against Packet Droppers.	98
3.5	Performance of Fellowship and DSR-MAC Nodes against Flooders.	103
4.1	Evidence Collection and Formulation.	117
4.2	Process of Making Trust based Decisions.	118
4.3	Architecture of SMRTI.	119
4.4	Adaptation of DSR to Record Valid Sequence Number.	123
4.5	Adaptation of DSR to Handle Route Modification Attacks.	127
4.6	Adaptation of DSR to Propagate Trustworthy Packets.	130
4.7	Adaptation of DSR to Defend Against Falsified Route Error.	131
4.8	Reputation-capture: Evidence Collection for Direct Reputation.	135
4.9	Reputation-capture: Evidence Collection for Observed Reputation.	137
4.10	Reputation-capture: Evidence Collection for Recommended Reputation.	141
4.11	Reputation-update: Effect of Mobility on Reputations.	145
4.12	RTS/CTS Defence against Receiver and Ambiguous Collisions.	149
4.13	Constrained Defence against Route Reply Modification Attack.	152

5.1	Route Discovery and Data Flow Attacks.	162
5.2	Route Maintenance and Gratuitous Detour Attacks.	164
5.3	Mobile Node – SMRTI and Adversary Extensions.	166
5.4	Performance of SMRTI Nodes against Adversaries and V_{max}	174
5.5	Performance of SMRTI Nodes against Pause Time and Node Density	180
5.6	Analysis of Selective Behaviours.	188
6.1	Integrated Architecture of SMRTI and Fellowship.	204
7.1	Route Discovery using Scasec.	214
7.2	Scasec Defence against Route Discovery related Attacks.	220
7.3	Trust Enhanced Secure Architecture for MANET.	222
8.1	Route Discovery Cycle in ASR Protocol.	232
8.2	Performance of ASR-MAC and fellowship-extended nodes.	242
9.1	Visualisation of Subjective Opinions.	250
9.2	Formulation of Overall Recommended Opinion.	262
9.3	Route Discovery in AOMDV.	269
9.4	Insertion of Modified RREQ.	279
9.5	Insertion of Fabricated RERR.	282
9.6	Insertion of Fabricated Gratuitous RREP.	283
9.7	Performance of TME and AOMDV Nodes against Adversaries.	290
10.1	TEAM and Related Security Areas in the MANET.	308
A.1	Class Diagram of the Fellowship Model (<i>Left</i>).	316
A.2	Class Diagram of the Fellowship Model (<i>Right</i>).	317
A.3	Class Diagram of the Fellowship’s Data Structures.	318
A.4	Class Diagram of the Fellowship’s Enforcement Component.	319
A.5	Class Diagram of the Fellowship’s Rate-limitation Component.	320
A.6	Sequence Diagram for Processing a Packet by Rate-limitation.	321

A.7	Sequence Diagram for the Interactions between the Rate-limitation and Enforcement (<i>Left</i>).	322
A.8	Sequence Diagram for the Interactions between the Rate-limitation and Enforcement (<i>Right</i>).	323
A.9	Sequence Diagram for the Channel Availability Computation by Rate-limitation.	324
A.10	Sequence Diagram for the Computations at the Restoration Component	325
A.11	Sequence Diagram for Processing the Acknowledgement and Duplicates by the Enforcement (<i>Left</i>).	326
A.12	Sequence Diagram for Processing the Acknowledgement and Duplicates by the Enforcement (<i>Right</i>).	327
A.13	Sequence Diagram for Updating the Contributions	328
A.14	Class Diagram of the SMRTI Model (<i>Top</i>).	330
A.15	Class Diagram of the SMRTI Model (<i>Bottom</i>).	331
A.16	Class Diagram of the Trust and Reputation Structures of the SMRTI. .	332
A.17	Class Diagram for the Data Interfaces.	333
A.18	Class Diagram for the Data Structures.	334
A.19	Sequence Diagram for Determining the Trust of a Context by the SMRTI (<i>Top</i>).	336
A.20	Sequence Diagram for Determining the Trust of a Context by the SMRTI (<i>Bottom</i>).	337
A.21	Sequence Diagram for the Trust Evaluation of a Packet by the SMRTI.	338
A.22	Sequence Diagram for the Trust Evaluation of a Node by the SMRTI. .	339
A.23	Sequence Diagram for Capturing the Direct Reputation of a Next-hop (<i>Top</i>).	340
A.24	Sequence Diagram for Capturing the Direct Reputation of a Next-hop (<i>Bottom</i>).	341
A.25	Sequence Diagram for Capturing the Observed Reputation of a Next-hop (<i>Top</i>).	342

A.26 Sequence Diagram for Capturing the Observed Reputation of a Next-hop (<i>Bottom</i>).	343
A.27 Sequence Diagram for Traversing the Observed Reputation's Packet Buffer (<i>Top</i>).	344
A.28 Sequence Diagram for Traversing the Observed Reputation's Packet Buffer (<i>Bottom</i>).	345
A.29 Sequence Diagram for Capturing the Recommended Reputation (<i>Top</i>).	346
A.30 Sequence Diagram for Capturing the Recommended Reputation (<i>Bottom</i>).	347
A.31 Sequence Diagram for Matching a Duplicate with a Buffered Packet (<i>Top</i>).	348
A.32 Sequence Diagram for Matching a Duplicate with a Buffered Packet (<i>Bottom</i>).	349
A.33 Sequence Diagram for locating the Reputation of a Mobile Node.	350
A.34 Sequence Diagram Changing the Reputation in the Absence of Evidence.	351
A.35 Sequence Diagram for Counting Duplicate Packets in a Packet Buffer.	352
A.36 Sequence Diagram for Dumping the Contents of a Packet Table.	353
A.37 Sequence Diagram for Dumping the Contents of a Reputation Table.	354
A.38 Sequence Diagram for Purging an Expired Packet from a Buffer.	355
A.39 Sequence Diagram for Storing a Packet in a Buffer (<i>Left</i>).	356
A.40 Sequence Diagram for Storing a Packet in a Buffer (<i>Bottom</i>).	357
A.41 Sequence Diagram for Assigning Weights to Various Participants during a Trust Evaluation.	358
A.42 Class Diagram showing Association between the DSR and SMRTI.	360
A.43 Class Diagram showing the Design, Associations, Aggregations, and Re- lationships of CBR Generator.	361
A.44 Sequence Diagram for the CBR Traffic Generation.	362
A.45 Sequence Diagram for the Inner Working of CBR Traffic Generator.	363

List of Tables

2.1	Secure Route Discovery using ARAN.	23
2.2	Secure Route Discovery using SAODV.	24
2.3	Secure Route Discovery using Ariadne.	25
2.4	Secure Route Discovery using SRP.	27
2.5	Secure Route Discovery using BISS.	28
3.1	Instance of Contribution-list's Attributes	76
3.2	Parameters for Fellowship Model	77
3.3	Simulation Parameters for NS2, MAC, Fellowship and Adversary	93
5.1	Simulation Parameters for NS2, DSR, SMRTI, and Adversary	168
7.1	Route Request Broadcast in Scasec.	216
7.2	Route Reply Unicast in Scasec.	217
8.1	Threshold Parameters for Rate-limitation	237
8.2	Simulation Parameters for NS2, Fellowship and Adversary	240
9.1	Simulation Parameters for NS2, AOMDV, SL-SMRTI and Adversary	287

Listings

B.1	Mac-802-11.cc	367
B.2	Wireless-phy.cc	372
B.3	Monitor.cc	373
B.4	RateLimitation.cc	375
B.5	Enforcement.cc	376
B.6	Restoration.cc	378
B.7	EnforcementVisitor.cc	379
B.8	CommitmentElement.cc	379
B.9	CommitmentStore.cc	380
B.10	MacPacketStore.cc	381
B.11	DsrAgent.cc	384
B.12	Path.cc	405
B.13	PlugInTrust.cc	406
B.14	DirectReputation.cc	410
B.15	DirectVisitor.cc	411
B.16	ObservedReputation.cc	413
B.17	ObservedVisitor.cc	414
B.18	RecommendedReputation.cc	416
B.19	ReputationStore.cc	417
B.20	ReputationElement.cc	418
B.21	PacketStore.cc	418

B.22 SRElement.cc	419
B.23 WeightStore.cc	420
B.24 PacketCountVisitor.cc	420
B.25 PrintVisitor.cc	420
C.1 CbrGen.py	425
C.2 NS2Scenario.tcl	428
C.3 NS2Batch.sh	433
C.4 TraceParser.py	436
C.5 Latency.py	443
C.6 LatencyGraph.py	444
C.7 PacketDeliveryRatio.py	445
C.8 PacketDeliveryRatioGraph.py	447
C.9 SuccessfulRouteDiscovery.py	449
C.10 SuccessfulRouteDiscoveryGraph.py	450
C.11 CompressNamTr.py	451

List of Acronyms

The following list of acronyms is neither exhaustive nor exclusive, but presents the key acronyms used in this thesis.

ACK	<i>Acknowledgement</i>
ANODR	<i>Anonymous On-demand Routing</i>
AODV	<i>Ad-hoc On-demand Distance Vector</i>
ARAN	<i>Authenticated Routing for Ad-hoc Networks</i>
ARM	<i>Anonymous Routing Protocol for MANET</i>
ARP	<i>Address Resolution Protocol</i>
ASR	<i>Anonymous Secure Routing</i>
BISS	<i>Building Secure Routing out of an Incomplete Set of Security Association</i>
CA	<i>Centralised Authority</i>
CAR	<i>Chain-based Anonymous Routing</i>
CBR	<i>Constant Bit Rate</i>
CCS	<i>Credit Clearance Service</i>

CONFIDANT	<i>Cooperation of Nodes: Fairness in Dynamic Ad-hoc Networks</i>
CREQ	<i>Certificate Request</i>
CTS	<i>Clear to Send</i>
DCF	<i>Distributed Coordination Function</i>
DoS	<i>Denial of Service</i>
DSR	<i>Dynamic Source Routing</i>
DSSS	<i>Direct Sequence Spread Spectrum</i>
FIFO	<i>First in First out</i>
HMAC	<i>Message Authentication Code</i>
IDS	<i>Intrusion Detection System</i>
IFQ	<i>Interface Queue</i>
MAC	<i>Medium Access Layer</i>
MANET	<i>Mobile Ad hoc Networks</i>
MOCA	<i>Mobile CA</i>
NAV	<i>Network Allocation Vector</i>
NS2	<i>Network Simulator 2</i>
PDA	<i>Personal Digital Assistant</i>
PDR	<i>Packet Delivery Ratio</i>
PGP	<i>Pretty Good Privacy</i>
PKG	<i>Public Key Generator</i>
PPM	<i>Packet Purse Model</i>

PTM	<i>Packet Trade Model</i>
QoS	<i>Quality of Service</i>
RERR	<i>Route Error</i>
RREP	<i>Route Reply</i>
RREQ	<i>Route Request</i>
RTS	<i>Request to Send</i>
SAODV	<i>Secure Ad-hoc On-demand Distance Vector</i>
SCASEC	<i>Scalable Multi-service Group Key based Secure Routing Protocol</i>
SEKM	<i>Secure and Efficient Key Management</i>
SL-SMRTI	<i>Subjective Logic based SMRTI</i>
SMG	<i>Scalable Multi-service Group Key Management</i>
SMRTI	<i>Secure MANET Routing with Trust Intrigue</i>
SRD	<i>Successful Route Discovery</i>
SRP	<i>Secure Routing Protocol</i>
TEAM	<i>Trust Enhanced Security Architecture for MANET</i>
TORA	<i>Temporally-Ordered Routing Algorithm</i>
TRR	<i>Trust Recommendation Request</i>
TTL	<i>Time to Live</i>
UML	<i>Unified Modeling Language</i>
VANET	<i>Vehicular Ad hoc Networks</i>

List of Symbols

The following list of symbols is neither exhaustive nor exclusive, but highlights the symbols used in our models for the sake of completeness.

M	Notation for a message
T	Notation for trust metric
P	Set of positive evidence
N	Set of negative evidence
R	Representation of a route
x	Notation for a preposition
f	Notation for communication flow
p	Total number of positive evidence
n	Total number of mobile nodes (elsewhere) Total number of negative evidence (Chapter 9)
E	Set of events (route request, route reply, route error, <i>etc.</i>)
l	Cardinality of sensitivity levels (elsewhere) Interval count for which recommendation is absent (Chapter 9)

k	Interval count for which mobile nodes are out of communication
$\mathcal{A}, \mathcal{B}, \mathcal{C}$	Representation of mobile nodes
$K(\mathcal{A})$	Notation for data keying matrix
$S(\mathcal{A})$	Matrix for managing the communication groups
RR	Representation of, direct, observed, or recommended reputation
$Bandwidth(\mathcal{A})$..	Physical channel bandwidth of \mathcal{A}
$pos(event)$	Positive value for a benign behaviour
$neg(event, action)$	Negative value for a malicious action
$p^{\mathcal{A}}, q^{\mathcal{A}}$	Large primes of \mathcal{A}
P_k	Notation for a packet k
$K_{\mathcal{S}-session}$	Session key generated by \mathcal{S}
r_1, r_2, r_3	Notation for a sensitivity levels
$K_{\mathcal{SD}}$	Shared secret between \mathcal{S} and \mathcal{D}
$s^{\mathcal{A}}$	Notation for \mathcal{A} 's master secret key
$T_{\mathcal{I}}, U_{\mathcal{I}}$	Random numbers generated by \mathcal{I}
t_0	Network deployment time period
R_0	Notation for the initial reputation
V_{max}	Maximum velocity of a mobile node
$C_{\mathcal{A}-Contribution}$..	\mathcal{A} 's battery energy for other nodes
$C_{\mathcal{A}-Self}$	\mathcal{A} 's battery energy for self operations

$PK_{\mathcal{I}}$	One-time public key generated by \mathcal{I}
$n_{\mathcal{I}}$	All nodes in the network excluding \mathcal{I}
$\mathbb{R}_{\mathcal{I}}$	Set of trust relationships held between \mathcal{I} and $n_{\mathcal{I}}$
$\mathbb{R}_{\mathcal{I}\mathcal{J}}$	Represents the trust relationship between \mathcal{I} and \mathcal{J}
S_i	A segment within the reputation range $[-1, +1]$
CG_1, CG_2, CG_3	Communication groups based on sensitivity level
a_x	Base rate that optimistically views uncertainty as belief for x
u_x	Belief that is neither committed to the truth nor falsehood of x
$HMAC_{SK^S}(M)$	HMAC of M using SK^S
$K_{SD}(M)$	Encryption of M using K_{SD}
$\{M\}_{PK_{\mathcal{I}}}$	Encryption of M using $PK_{\mathcal{I}}$
$E_{\mathcal{A}}(t_0)$	Battery energy of \mathcal{A} at t_0
$E_{\mathcal{A}}(P_k)$	\mathcal{A} 's battery energy to transmit P_k
$H_1(\mathcal{I})$	Notation for a one-way function
$T_{\mathcal{I}}Flow_f(t_{a+1})$..	\mathcal{I} 's trustworthiness for f at $t_{(a+1)}$
$T_{\mathcal{I}}Route_R(t_{a+1})$..	\mathcal{I} 's trustworthiness for R at $t_{(a+1)}$
$T_{\mathcal{I}}Node_{Src}(t_a)$..	\mathcal{I} 's trustworthiness for node Src at t_a
$E(\omega_x)$	Probability expectation value of an opinion
$P_{pub}^{\mathcal{A}}$	Notation for \mathcal{A} 's public key
$\mathbb{G}_1^{\mathcal{A}}$	Notation for \mathcal{A} 's additive group

$\mathbb{G}_2^{\mathcal{A}}$	Notation for \mathcal{A} 's multiplicative group
$S_{\mathcal{I}}^{\mathcal{A}}$	Notation for \mathcal{A} 's participant key to \mathcal{I}
$CG_k^{\mathcal{A}}$	Notation for \mathcal{A} 's CG_k with sensitivity level k
$S_{\mathcal{M}k}^{\mathcal{A}}$	Denotes whether or not \mathcal{A} considers \mathcal{M} for $CG_k^{\mathcal{A}}$
$SK_k^{\mathcal{A}}$	\mathcal{A} 's session secret key for f that belongs to $CG_k^{\mathcal{A}}$
$Auth_k^{\mathcal{A}}$	\mathcal{A} 's authorisation for nodes that belong to $CG_k^{\mathcal{A}}$
\odot	Fading operator
\oplus	Consensus operator
\otimes	Discounting operator
\geq	Comparison operator
θ	Length of S_i
σ	Merit factor
λ	Demerit factor
Δ	Threshold-limit
η	Contribution-share
χ	Contribution-common
μ	Redemption threshold
ρ	Negotiation threshold
ν	Transmission threshold
Θ	Frame of discernment

α, β	Beta PDF parameters
ϕ	Count of new neighbours
γ	Relative weight (Chapter 9) Packet forwarding ratio (elsewhere)
δ	Reputation decay (or) growth factor
∇	Evidence-to-opinion mapping operator
τ	Reception threshold (elsewhere) Average duration taken for f (Chapter 9)
Ω	Set of opinions (direct, observed and recommended)
σ	Contains timestamps of opinion initialisation or last revision
δ_n	Name of a cluster
b_x	Belief that x is true
d_x	Disbelief that x is false
Δ_c	Threshold-limit for a context
Δ_r	Threshold-limit for derived recommendations
$\beta_{\mathcal{J}}$	\mathcal{J} 's weight in the route during trust evaluation
ω_x	Binomial subjective opinion about the truth of x
δ_t	Represents the type of relationship in a cluster-based MANET
${}^A\eta_{\mathcal{I}}$	\mathcal{A} 's contribution-share for \mathcal{I}
${}^A\tau_{\mathcal{I}}$	\mathcal{A} 's reception threshold for \mathcal{I}
${}^A T_{\mathcal{I}}$	\mathcal{A} 's blacklist timestamp for \mathcal{I}

$\mathcal{I}_{\mathcal{A}}^{recp}$	\mathcal{I} 's reciprocate reception for \mathcal{A}
$A\nu_{\mathcal{J}}$	\mathcal{A} 's transmission threshold for \mathcal{J}
$A\gamma_{\mathcal{J}}$	\mathcal{A} 's packet forwarding ratio for \mathcal{J}
$A\beta_{\mathcal{J}}$	Total count of packets transmitted to \mathcal{J} by \mathcal{A}
$A\alpha_{\mathcal{J}}$	Total count of packets forwarded by \mathcal{J} on behalf of \mathcal{A}
$A\omega_{\mathcal{B}}^m$	\mathcal{A} 's opinion (of type m) on \mathcal{B}
$A b_{\mathcal{B}}^m$	\mathcal{A} 's belief (with respect to m) on \mathcal{B}
$A d_{\mathcal{B}}^m$	\mathcal{A} 's disbelief (with respect to m) on \mathcal{B}
$A u_{\mathcal{B}}^m$	\mathcal{A} 's ignorance (with respect to m) on \mathcal{B}
$\omega_x^{\mathcal{A}}$ or $\omega(\mathcal{A} : x)$	\mathcal{A} 's opinion on x
$\omega_x^{\mathcal{R}:\mathcal{S}}$	$\omega_{\mathcal{S}}^{\mathcal{R}}$ discounts $\omega_x^{\mathcal{S}}$
$\omega_x^{\mathcal{P}\diamond\mathcal{Q}}$	Consensus opinion of $\omega_x^{\mathcal{P}}$ and $\omega_x^{\mathcal{Q}}$
$\omega_{\mathcal{I}\mathcal{J}}^{RR}(t_a)$	\mathcal{I} 's reputation of type RR for \mathcal{J} at t_a
$\omega_{\mathcal{I}\mathcal{J}}^{Direct}(t_a)$	\mathcal{I} 's accrued direct reputation for \mathcal{J} at t_a
$\omega_{\mathcal{I}\mathcal{J}}^{Observed}(t_a)$	\mathcal{I} 's accrued observed reputation for \mathcal{J} at t_a
$\omega_{\mathcal{I}\mathcal{J}}^{Rec}(t_a)$	\mathcal{I} 's accrued recommended reputation for \mathcal{J} at t_a
$\gamma_{\mathcal{I}\mathcal{J}}^{RR}$	RR 's weight in the trust evaluation of \mathcal{I} for \mathcal{J}