

Contents

Contents	xi
List of Tables	xvii
List of Figures	xix
Acronyms	xxiv
1 Introduction	1
2 Evaluation of ad hoc routing protocols	7
2.1 Introduction	8
2.2 Routing protocols	11
2.3 Key aspects behind the evaluation of ad hoc routing protocols	15
2.3.1 Evaluation platforms	15
2.3.1.1 Model-based evaluation	15
2.3.1.2 Prototype-based evaluation	16
2.3.1.3 Emulation-based evaluation	17
2.3.1.4 Summary	18
2.3.2 Recreating the environment characteristics	19
2.3.3 Measures considered during evaluation	20

CONTENTS

2.4	Towards a resilience evaluation framework for ad hoc routing protocols	22
2.4.1	The benefits of fault injection	22
2.4.1.1	Faults related to resources limitations	24
2.4.1.2	Faults derived from the nature of the wireless communication medium	25
2.4.1.3	Faults boosted by the mobility of nodes	26
2.4.1.4	Challenges behind to the absence of infrastructure	27
2.4.1.5	Summary	27
2.4.2	Usefulness of resilience measures	29
2.4.3	Discussion	31
2.5	Conclusions	32
3	A novel methodology to evaluate the resilience of ad hoc routing protocols	35
3.1	Introduction	36
3.2	Experiments configuration	39
3.2.1	Network profile definition	40
3.2.2	Execution profile	40
3.2.2.1	Workload	41
3.2.2.2	Faultload	41
3.2.3	Measures definition	44
3.2.4	Configuration of the experimental campaign	45
3.3	Experiments execution	47
3.3.1	Proposed architecture	47
3.3.2	Experimental procedure	50
3.3.3	Golden run execution	51
3.3.4	Fault injection execution	51
3.3.4.1	F1: Signal attenuation	51

CONTENTS

3.3.4.2	F2: Ambient noise	52
3.3.4.3	F3: Battery extenuation	52
3.3.4.4	F4: Traffic peak	53
3.3.4.5	F5: Sink hole attack	53
3.3.4.6	F6: Tampering attack	54
3.3.4.7	F7: Replay attack	55
3.3.4.8	F8: Selective forwarding attack	56
3.3.4.9	F9: Jellyfish attack	56
3.3.4.10	F10: Flooding attack	57
3.3.4.11	F11: Neighbours saturation	57
3.3.4.12	F12: Sequence number replay	58
3.4	Analysis of results	59
3.5	Conclusions	60
4	A tool to support our methodology	63
4.1	Introduction	63
4.2	Architectural overview	65
4.3	Experiments definition	67
4.3.1	Experiments campaign	68
4.3.2	Network profile	69
4.3.3	Execution profile	70
4.4	Execution of experiments	72
4.4.1	Initialisation	72
4.4.2	Visibility of nodes	72
4.4.3	Execution of the routing protocol	74
4.4.4	Execution of the workload	74
4.4.5	Execution of the faultload	76
4.4.5.1	Injection nodes instrumentation	76

CONTENTS

4.4.5.2	Fault injection	79
4.5	Analysis of results	82
4.5.1	Performance measures computation	83
4.5.2	Resources consumption measures computation	85
4.5.3	Resilience measures computation	86
4.5.4	Measures report delivery	89
4.6	Tool features	90
4.7	Conclusions	91
5	Exploitation of REFRAHN	93
5.1	Introduction	93
5.2	Experimental resilience evaluation	94
5.2.1	Routing protocol targets	95
5.2.2	Experimental testbed	96
5.2.3	Network profile configuration	97
5.2.4	Execution profile configuration	99
5.2.4.1	Workload	99
5.2.4.2	Faultload	100
5.2.5	Number and duration of experiments	100
5.2.6	Considerations about the measures selection	101
5.2.7	Analysis of results	101
5.2.7.1	Performance analysis	101
5.2.7.2	Resilience analysis	103
5.2.7.3	Resources consumption analysis	104
5.2.8	Summary	105
5.3	Vulnerability discovery	106
5.3.1	Accepting routing protocol packets with a replayed sequence number	107

CONTENTS

5.3.2	Establishing links with a reduced number of actions	108
5.3.3	Incorrect management of the neighbour lists of routing protocols	110
5.3.4	Conclusions	113
5.4	Resilience benchmarking	114
5.4.1	Measures aggregation approaches	116
5.4.2	Logic Score of Preferences	117
5.4.3	Experimental consideration of the case study	120
5.4.3.1	Measures selection	122
5.4.3.2	Fine-grained experimental results	122
5.4.3.3	Definition of criterion functions	124
5.4.3.4	Aggregation of scores	126
5.4.4	Hierarchical ranking of results	127
5.4.4.1	Ranking per global quality	127
5.4.4.2	Ranking per characteristic	128
5.4.4.3	Ranking per fault type	129
5.4.4.4	Summary	129
5.4.5	Conclusions	129
5.5	Fine tuning	131
5.5.1	Experimental considerations of the case study	132
5.5.2	Parameterisation of fault detection mechanisms	132
5.5.2.1	Watchdog: a mechanism to detect packet loss	132
5.5.2.2	Problem pathology	134
5.5.2.3	Parameterisation proposal	136
5.5.3	Parameterisation of handshaking mechanisms	138
5.5.3.1	Limitations of a MD5 handshaking mechanism	138
5.5.3.2	Parameterisation Proposal	139

CONTENTS

5.5.4	Conclusions	141
5.6	Design of new fault tolerance mechanisms	142
5.6.1	Experimental considerations of the case study	143
5.6.1.1	Proactive routing protocols under study	143
5.6.1.2	Ambient noise characterisation	144
5.6.1.3	Experiment setup	145
5.6.1.4	Impact of ambient noise	147
5.6.1.5	Tuning the routing protocol configuration	150
5.6.2	Link-quality-based adaptive replication of packets . . .	155
5.6.2.1	Analytical overview of the technique	155
5.6.2.2	Implementation of the algorithm	157
5.6.2.3	Assessing the adaptive replication of packets	159
5.6.3	Conclusions	162
5.7	Conclusions	162
6	Conclusions	165
6.1	Future work	168
6.1.1	Future research	168
6.1.2	Future development and empirical work	171
6.2	Dissemination of this thesis	173
6.2.1	Journals	173
6.2.2	Indexed conferences	173
6.2.3	Other papers	175
6.2.4	Awards	177
6.3	Projects supporting this thesis	177
	References	179