

Contents

1	Motivation, Objectives and Organisation of the Thesis	1
1.1	Motivation	1
1.2	Objectives of the Thesis	2
1.3	Structure of the Thesis	2
2	Related Work	5
2.1	Introduction	5
2.2	Overview of the IEEE 802.11 Standard	6
2.2.1	Network Architecture	6
2.2.2	Physical Level	6
2.2.3	Summary	7
2.3	Community Networks	7
2.3.1	Examples of Wireless Community Networks	8
2.3.2	How a Wireless Community Network works	9
2.4	Information and Communication Technologies in Developing Countries.	12
2.4.1	The Digital Divide	13
2.4.2	Causes of the Digital Divide	14
2.4.3	Old Solutions for New Problems	15
2.5	Mesh Networks	15
2.6	Mobile Ad hoc Networks	16
2.7	Routing Protocols	17
2.7.1	Basic Routing Techniques	17
2.7.2	Classification of Routing Protocols	18
2.7.3	Routing in Ad hoc Networks	18
2.7.4	Why different protocols?	20
2.7.5	The Optimised Link-State Routing Protocol (OLSR)	20
2.7.6	Ad hoc On-Demand Distance Vector Routing (AODV)	24
2.7.7	Other Protocol specifically used in Mesh Networking: B.A.-T.M.A.N.	25
2.8	Security on MANETs and Wireless Mesh Networks	26
2.8.1	Challenges	26
2.8.2	Routing disruption attacks	27
2.8.3	Watchdogs	28

CONTENTS

2.9	Methodology Used to Evaluate MANET and Mesh Networks Proposals	28
2.9.1	Importance of Evaluation in Research	29
2.9.2	Simulators	29
2.9.3	Emulators	30
2.9.4	Main Differences between Simulators and Emulators	32
3	<i>Castadiva</i>: a MANET Emulator	33
3.1	Introduction	33
3.2	Objectives of <i>Castadiva</i>	34
3.3	Architectural Overview	34
3.4	<i>Castadiva</i> 's Implementation Details	36
3.4.1	Wireless Nodes' Software	37
3.4.2	Main Application	39
3.5	Performance Evaluation and Validation of <i>Castadiva</i>	48
3.5.1	Evaluation of <i>Castadiva</i> with a Static Scenario	48
3.5.2	Evaluation of <i>Castadiva</i> with a Mobile Scenario	51
3.6	Assessing the performance of videoconferencing in MANETS with <i>Castadiva</i>	54
3.6.1	Static Scenario	54
3.6.2	Dynamic Scenario	59
3.7	Summary	62
4	An Architecture supporting Web-based Services and Authentication	63
4.1	Introduction	64
4.2	Objectives of <i>RuralNet</i>	65
4.3	The <i>RuralNet</i> System Architecture	65
4.3.1	Technologies Used	67
4.4	<i>RuralNet</i> 's Basic Functionality	67
4.4.1	Controlling the Access to <i>RuralNet</i>	67
4.4.2	The <i>RuralNet</i> Interface Implementation	71
4.5	<i>RuralNet</i> for Developing Countries	74
4.5.1	Using Multiple Internet Connectivities	74
4.5.2	Scalability	74
4.5.3	Services without Internet Connectivity	74
4.6	Evaluation	75
4.6.1	Evaluation with one client	76
4.6.2	Interactions among different clients	76
4.6.3	Round-trip time	78
4.7	<i>Maya</i> : Our Mesh Networks Management Tool	80
4.7.1	Implementation and Functionality	80
4.7.2	The Wireless Router Enabling/Disabling problem	81
4.7.3	Network Parameters Setup	82
4.7.4	Security Issues	83
4.7.5	UDP Message Issues	83
4.7.6	Evaluation	84

4.8	Deploying <i>RuralNet</i> in Mozambique	87
4.8.1	Why we chose Mozambique as our scenario?	87
4.8.2	Objectives in Mozambique	88
4.8.3	Deploying <i>RuralNet</i>	89
4.8.4	Scenario	89
4.8.5	Infrastructure	91
4.8.6	Final result	92
4.9	Summary	92
5	Security Improvements for Community Wireless Networks	95
5.1	Introduction	96
5.1.1	Black holing Ad hoc Networks	96
5.2	Objectives to achieve	97
5.3	Watchdog-based Intrusion Detection Systems (IDS)	97
5.3.1	Watchdogs and their Importance for MANETs IDSs	97
5.3.2	Design Approach	98
5.3.3	Implementation Trade-offs	100
5.3.4	Countermeasures proposed	101
5.3.5	Evaluation of our watchdog using <i>Castadiva</i>	102
5.3.6	Evaluation using ns-2	106
5.3.7	Detected drawbacks of the watchdog mechanism	109
5.4	Adapting Bayesian Filters to IDS of MANETs: The Bayesian Watchdog	110
5.4.1	Bayesian Filtering.	110
5.4.2	Why Bayesian Filters?	111
5.4.3	Assumptions	111
5.4.4	Bayesian Filtering Adapted for our IDS	112
5.4.5	Watchdog Reputation Rating	113
5.4.6	Implementation trade-offs	113
5.5	Evaluation	115
5.5.1	Static Scenario	115
5.5.2	Dynamic Scenario	116
5.6	Comparison between the Bayesian Watchdog and the Standard Watchdog	119
5.7	Summary	120
6	Conclusions, Publications and Future Work	123
6.1	Conclusions	123
6.2	Publications Related with this Thesis	125
6.2.1	<i>Castadiva</i>	125
6.2.2	<i>RuralNet</i>	126
6.2.3	Standard Watchdog and Bayesian Watchdog	127
6.3	Future Work	128
	Bibliography	131

List of Figures

2.1	Internet penetration on the world.	12
2.2	Internet Users.	13
2.3	Global digital divide.	14
2.4	Example of a mesh network.	16
2.5	Illustration of the multi-point relay concept for node N	22
2.6	Steps for a black hole attack.	27
3.1	Schema of <i>Castadiva</i> 's architecture.	35
3.2	Scenario definition with <i>Castadiva</i>	36
3.3	<i>Castadiva</i> 's physical network.	37
3.4	Software components for <i>Castadiva</i>	38
3.5	Example of a scenario with four nodes.	38
3.6	Application control menu.	40
3.7	Scenario definition with <i>Castadiva</i>	41
3.8	Node configuration interface.	42
3.9	Mobility implementation.	43
3.10	Traffic declaration window.	44
3.11	External traffic declaration.	44
3.12	Example of how to add external traffic injection.	45
3.13	Random Simulation window.	46
3.14	Execution Planner.	46
3.15	New Protocol Window.	47
3.16	Mobility Plugins Designer.	48
3.17	Scenario used for evaluation purposes.	49
3.18	Performance comparison between <i>Castadiva</i> and ns-2 in a static scenario using CBR/UDP traffic (left) and FTP/TCP traffic (right). Routing disabled.	49
3.19	Performance comparison between <i>Castadiva</i> with ns-2 in a static scenario. Using CBR/UDP traffic (left) and FTP/TCP traffic (right). Routing enabled.	50
3.20	Packet loss due to the proximity of the devices in an emulation (left) and capacity of an ad hoc network compared with <i>Castadiva</i> (right).	51
3.21	Result comparison of <i>Castadiva</i> with ns-2 without routing.	52
3.22	Result comparison of <i>Castadiva</i> with ns-2 for UDP (left) and TCP (right) traffic with routing.	53

LIST OF FIGURES

3.23	Comparison of <i>Castadiva</i> and ns-2 at different node speeds with both UDP (left) and TCP (right) traffic. Routing disabled.	53
3.24	Comparison of <i>Castadiva</i> and ns-2 using OLSR at different node speeds with both UDP (left) and TCP (right) traffic.	54
3.25	Topology for evaluating video traffic delivery.	55
3.26	Average data rate generated (left) and packet loss ratio (right) for different numbers of hops.	56
3.27	Cumulative distribution function for the inter-packet generation interval and inter-packet arrival interval in a scenario with one hop (left) and ten hops (right).	56
3.28	Testing a videocall when both webcams point to screen with a movie.	57
3.29	Screenshot of the videocall with a scenario of one hop (left) and ten hops (right).	58
3.30	Cumulative distribution function for the throughput in a scenario with different hops (left) and packet loss rate in different scenarios (right).	58
3.31	Cumulative distribution function for the inter-packet generation interval and inter-packet arrival interval in a scenario with one hop (left) and ten hops (right).	59
3.32	Evaluation of the ping sessions in different scenarios.	59
3.33	Throughput and packet losses with a standard videocall in a scenario with mobility.	61
3.34	Throughput and packet losses with a movie in a scenario with mobility.	61
4.1	The <i>RuralNet</i> system architecture.	66
4.2	Relationship among <i>RuralNet</i> 's software components.	68
4.3	Typical captive portal connection scheme.	68
4.4	<i>RuralNet</i> presentation screen.	69
4.5	TC queue hierarchy.	71
4.6	<i>RuralNet</i> interface.	73
4.7	Accessing <i>RuralNet</i> with a mobile phone.	73
4.8	<i>RuralNet</i> connected to another <i>RuralNet</i> system.	75
4.9	Documents in <i>RuralNet</i>	75
4.10	Connection speed for one client.	77
4.11	Download speed for the 4 clients under analysis.	77
4.12	Download speed when the bandwidth towards the FTP server is limited to 1024 Kb/s.	78
4.13	Download speed when the bandwidth towards the FTP server is limited 256 Kb/s.	79
4.14	Evaluation of the distribution network.	79
4.15	<i>Maya</i> 's management interface.	81
4.16	Format of the management UDP messages.	84
4.17	Comparison of the latency associated to <i>Maya</i> 's management tasks when varying the number of hops.	85
4.18	Overhead of management tasks requiring UDP messages, SSH connections and key exchanges when varying the number of TCP flows, at different hop distances.	86

LIST OF FIGURES

4.19 UDP message arrival probability.	87
4.20 Diffusion of Technology.	88
4.21 Region of Nampula	89
4.22 Selected schools of Nacala.	90
4.23 Infrastructure of a school.	91
4.24 Distance between the <i>RuralNet</i> nodes.	92
4.25 In order: deploying an antenna for <i>RuralNet</i> (left up), one of our members with an antenna (right up), a classroom of the school (left bottom), and one of our router before being installed (right bottom).	93
4.26 In order: An antenna deployed for <i>RuralNet</i> (left up), another antenna (right up), one of our members installing an access point (left bottom), one of the schools of the project (right bottom).	94
5.1 The watchdog technique.	98
5.2 Experimental setup: A watchdog in <i>RuralNet</i>	103
5.3 Throughput with different levels of noise.	104
5.4 Network's throughput affected by noise.	104
5.5 Relation between the minimum <i>tolerance threshold</i> needed to avoid false positives using OLSR and AODV.	105
5.6 False Negative interval when the <i>tolerance threshold</i> is set to 50% (up) and relation between the time needed for detecting an attacker and the number of packets forwarded previously when using different values of the <i>devaluation</i> option (bottom).	106
5.7 Probability of an attack when varying the number of nodes and the percentage of attackers.	107
5.8 Attacks detected by the watchdog when changing the mobility of a scenario.	107
5.9 Number of false positives generated (up) and false positive ratio (bottom) when changing the mobility of a scenario.	108
5.10 False positives due to watchdogs timeouts.	109
5.11 Example of a reputation function.	114
5.12 Actual detections and false positives in a static scenario.	116
5.13 Percentage of (a) actual attacks detected and (b) false positives for different tolerance threshold and for different devices' speed.	117
5.14 Percentage of (a) actual attacks detected and (b) false positives for different fading values and different mobility speeds.	118
5.15 Attacks detected (up) and false positives produced (bottom) when varying the neighbour timeout.	119
5.16 Attacks detected (up) and false positives produced (bottom) when varying the neighbour timeout.	120
5.17 Comparison between both watchdogs with different degrees of mobility: detections (up) and false positives (bottom).	121
6.1 Detecting cooperative attacks.	129

List of Tables

2.1	Comparative of existing emulators.	31
3.1	Iptables rules: example of usage in <i>Castadiva</i> 's framework.	39
3.2	Default OLSR parameter values.	52
3.3	OpenWRT parameters values for the OLSR protocol.	55
3.4	OLSR values used for the mobility scenarios.	60
3.5	Percentage of the simulation time when a route between both laptops exists.	60
4.1	Coordinates of each node deployed in Nacala.	90

List of Algorithms

3.1	Iptables rules to emulate when a node goes out of range between seconds 15 and 35.	43
4.1	User disconnection from <i>RuralNet</i>	70
4.2	Connection speed of each user using <i>RuralNet</i>	72
4.3	OnReceivingaBroadcast() function of the <i>Maya</i> tool.	82
4.4	ApplyNetworkConfiguration() function of the <i>Maya</i> tool.	83
5.1	Isolating a malicious node.	102
5.2	Selecting an alternative route.	102
5.3	Pseudocode of the bayesian algorithm for predicting <i>black hole</i> attacks.	113

