Securing and Enhancing Routing Protocols for Mobile Ad hoc Networks

Manel Guerrero Zapata

Submitted in partial fulfilment of the requeriments for
the degree of Doctor of Philosophy
Doctorate in Computer Architecture and Technology
Computer Architecture Department (DAC)

Tutor: Dr. Jorge García Vidal

Technical University of Catalonia
Universitat Politècnica de Catalunya

Barcelona, March 2006

ABSTRACT

MANET (Mobile and Ad hoc NETworks) are networks in which nodes are mobile and link connectivity might change all the time. In this kind of networks routing, security and key management are important and complex problems. The problem of routing has been properly addressed by the research community. Nevertheless, the research in security and key management has been posponed or relegated to a second term.

This research work tries to give a solution to the needs in security for MANET networks using as a base a pre-existing routing protocol: Ad Hoc On-Demand Vector Routing (AODV). The selection of AODV is because the author of this research work is one of the contributors to AODV (so he knows perfectly how it works) and because it seemed that it would be the one that could more easily accommodate the needed modifications. The proposed solution in an extension to AODV called Secure AODV (SAODV).

In addition to the security proposal, this research work includes an enhancement to AODV that allows to use shorter routes, which will result in lower end-to-end delays, and longer battery life of the network nodes.

Contents

1 Overview 13

1.1 Background 13

1.1.1 MANET 13

1.1.2 AODV 14

1.2 SAODV 14

1.2.1 SAODV hash chains 15

1.2.2 SAODV digital signatures 15

1.3 SAKM 15

1.3.1 Delayed Verification 16

1.4 Short Cut Detection 16

2 Contributions 17

2.1 Publications 17

2.2 Conferences 19

2.3 Internet drafts 20

2.4 Other Contributions 21

2.5 Brief Future Research Plan 22

3 Ad hoc On-Demand Distance Vector Routing 23

3.1 Introduction 23

3.2 AODV 23

3.3 AODV Message Formats 27

4 Secure Ad hoc On-Demand Distance Vector 29

4.1 Introduction 29

4.2 Related Work 29

4.3 Security Requirements 32

4.4 Securing Ad hoc Protocols 33

4.5 Security flaws of AODV 34

4.6 Securing AODV 35

4.6.1 SAODV hash chains 36

4.6.2 SAODV digital signatures 38

4.6.3 SAODV error messages 39

4.6.4 When a node reboots 40

4.6.5 Analysis 41

4.7 Other routing protocols 43

4.8 Secure AODV Extensions 44

5 Simple Ad hoc Key Management 51

5.1 Introduction 51

5.2 Generation of the IP address for SAODV 53

5.3 New fields in the SAODV messages 54

5.4 Duplicated IP Address Detection 55

5.4.1 Duplicated IP Address Detection for SAODV 56

5.4.2 Network Leaders 57

5.5 Delayed Verification of Signatures 57

5.5.1 Revised Security Requirements 58

5.5.2 Achieving Delayed Import Authorization 58

5.5.3 SAODV with Delayed Verification 59

5.6 Simulation Results 61

5.7 Analysis 64

5.8 SAODV Duplicate Address Detection Messages 65

6 Shortcut Detection and Route Repair 69

6.1 Introduction 69

6.2 Related Work 70

6.3 Shortcut Detection 71

6.3.1 Shortcut Routes 71

6.3.2 Shortcut Requests . . . 72
6.3.3 Shortcut Replies . . . 72
6.3.4 One-Hop Shortcuts . . . 72
6.3.5 Two-Hop Shortcuts . . . 73
6.3.6 Other Kind of Shortcuts . . . 74
6.4 Route Repair . . . 75
6.5 AODV-SDR . . . 79
6.6 Simulation Results . . . 82

7 A Concluding Remark 87

8 Acknowledgments 89

9 Appendix: Publications 97

List of Figures

3.1 Mobility in Routing 24

3.2 Route Request 25

3.3 Route Reply 26

3.4 Route Error 27

3.5 Route Request (RREQ) Message Format 28

3.6 Route Reply (RREP) Message Format 28

3.7 Route Error (RERR) Message Format 28

3.8 Route Reply Acknowledgment (RREP-ACK) Message Format 28

4.1 RREQ (Single) Signature Extension 44

4.2 RREP (Single) Signature Extension 45

4.3 RREQ Double Signature Extension 46

4.4 RREP Double Signature Extension 46

4.5 RERR Signature Extension 46

4.6 RREP-ACK Signature Extension 46

5.1 SAODV daemon 60

5.2 SAODV daemon with a routing middleware 61

5.3 Simulation Results 63

5.4 Duplicated Address (DADD) Detected Message 65

5.5 New Address (NADD) Notification Message 66

5.6 New Address Acknowledgment (NADD-ACK) Message 67

6.1 One-hop Shortcut Detection 73

6.2 Two-hop Shortcut Detection 74

6.3 Three-hop Shortcut 75
6.4 Propagation of SREQs 77
6.5 Simple Repaired Route Discovery 78
6.6 Repaired Route Discovery with Additional Forwarding by neighbors 79
6.7 Shortcut Request (SREQ) Message Format 80
6.8 Shortcut Reply (RREP) Message Format 81
6.9 Changing speed 84
6.10 Changing area 85
6.11 Changing protocol 86

List of Tables

4.1 Possible values of the Hash Function field 36
4.2 RREQ and RREP Signature Extension Fields 45
4.3 RREQ Double Signature Extension Fields 47
4.4 RREP Double Signature Extension Fields 48
4.5 RERR and RREP-ACK Signature Extension Fields 49

5.1 Possible values of the Signature Method field 55
5.2 Times for a Compaq iPAQ 3670 62
5.3 Duplicated Address (DADD) Detected Message Fields 65
5.4 New Address (NADD) Notification Message Fields 66
5.5 New Address Acknowledgment (NADD-ACK) Message Fields 67

6.1 Shortcut Request Message Fields 80
6.2 Shortcut Reply Message (RREP with the 'S' flag) Fields . . . 81