

Copyright is owned by the Author of the thesis. Permission is given for a copy to be downloaded by an individual for the purpose of research and private study only. The thesis may not be reproduced elsewhere without the permission of the Author.

Encryption Key Management in Wireless Ad Hoc Networks

A thesis presented in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy in Computer Science

at Massey University, Auckland, New Zealand

Alastair Jon Nisbet

2010

Abstract

Communication is an essential part of everyday life, both as a social interaction and as a means of collaboration to achieve goals. Networking technologies including the Internet have provided the ability to communicate over distances quickly and effectively, yet the constraints of having to be at a computer connected to a network access point restricts the use of such devices. Wireless technology has effectively released the users to roam more freely whilst achieving communication and collaboration, and with worldwide programs designed to increase laptop usage amongst children in developing countries to almost 100%, an explosive growth in wireless networking is expected. However, wireless networks are seen as relatively easy targets for determined attackers. Security of the network is provided by encrypting the data when exchanging messages and encryption key management is therefore vital to ensure privacy of messages and robustness against disruption.

This research describes the development and testing through simulation of a new encryption key management protocol called SKYE (Secure Key deploYment & Exchange) that provides reasonably secure and robust encryption key management for a mobile ad hoc network. Threshold cryptography is used to provide a robust Certificate Authority providing certificate services to the network members using Public Key Infrastructure. The protocol is designed to be used in an environment where communications must be deployed quickly without any prior planning or prior knowledge of the size or numbers of the potential members. Such uses may be many and varied and may include military, education or disaster recovery where victims can use the protocol to quickly form ad hoc networks where other communication infrastructure has failed. Many previous protocols were examined and several key

features of these schemes were incorporated into this protocol along with other unique features. These included the extensive tunability of the protocol allowing such features as increasing the number of servers that must collaborate to provide services and the trust level that must exist along a certificate chain before a request for a certificate will be accepted by a server. The locations of the servers were carefully selected so that as these parameters were altered to increase security, performance remained high. For example, when two servers were required for certificate issuance, a certificate request would succeed 92% of the time. By doubling the servers required and therefore considerably increasing resilience against attack of the certificate authority, this figure dropped only moderately to 78%. The placement of the servers proved to be a critical parameter and extensive experiments were run to identify the best placements for servers with the various parameters chosen.

Simulations show that the protocol performs effectively in a developing and constantly changing network where nodes may join and leave the network frequently and where many of the members may be mobile. The many tunable parameters of the protocol ensure that it is useful in a variety of applications and has unique features making it effective and efficient in a highly dynamic network environment.

Acknowledgements

I would like to thank the many people who have provided encouragement and advice during the time that this research was undertaken. Thanks to my supervisor Dr Mohammed Rashid who provided enthusiastic supervision that ensured the research continued its course towards completion. His knowledge, advice and encouragement during difficult times were a source of inspiration.

Thanks also to my co-supervisor Dr Fakhrul Alam who provided advice and support with the technical aspects of this research and to the School of Engineering and Applied Science at Massey University that provided resources and facilities required to complete the research.

I am very grateful to my previous supervisor Dr Ellen Rose who provided a wealth of knowledge and experience to ensure the research took an unfaltering path during her time as my supervisor.

The completion of this thesis is a testament to the unwavering support of my wife, Ruth who provided many years of support whilst I undertook a lifelong ambition. To her I will be eternally grateful.

This thesis is dedicated to my wife and our two wonderful little children, Thomas and Skye who have suffered the trials and tribulations of Doctoral research at times as much as me. Thank you to my wonderful family.

Table of Contents

Abstract	i
Acknowledgements	iii
List of Figures	viii
List of Tables	x
List of Publications	xi
Abbreviations and Acronyms	xii
1 Introduction	1
1.1 Introduction	1
1.2 Statement of the Problem	4
1.3 Research Methodology	6
1.4 Motivation	8
1.5 Contribution of the Thesis	11
1.6 Thesis Structure	13
2 Mobile Ad Hoc Networks Security and Key Management	16
2.1 Introduction	16
2.2 Mobile Ad Hoc Networks	16
2.3 Wireless Networking Topologies	21
2.3.1 Infrastructure Mode	21
2.3.2 Ad Hoc Mode	24
2.4 Wireless Protocols	28
2.5 Wireless Network Security	37
2.5.1 Wireless Network Attacks	37
2.5.1.1 Access Control List Avoidance	38
2.5.1.2 Denial of Service (DOS)	39
2.5.1.3 Denial of Service with Frequency Jamming	39
2.5.1.4 Address Resolution Protocol (ARP) Cache Poisoning	40
2.5.1.5 Eavesdropping	42
2.5.1.6 Man in the Middle (MTM)	42
2.5.1.7 Replay Attack	43
2.5.1.8 Spoofing	44
2.5.1.9 WiFi Protected Access Password Discovery	45
2.5.2 Standards Based Security Solutions	47
2.5.2.1 Wired Equivalent Privacy (WEP)	47

	2.5.2.2 Weaknesses in WEP	52
	2.5.2.3 WiFi Protected Access (WPA)	56
	2.5.2.4 Michael	58
	2.5.2.5 Defeating Replays: IV Sequence Enforcement	59
	2.5.2.6 Defeating Weak Key Attacks: Key Mixing	59
	2.5.2.7 Defeating Key Collision Attacks: Rekeying	60
	2.5.2.8 WiFi Protected Access 2 (WPA2)	62
	2.5.3 Non-Standards Based Security Solutions	66
	2.6 Summary	68
3	Cryptography in Mobile Ad Hoc Networks	69
	3.1 Introduction	69
	3.2 Background	70
	3.3 Encryption	72
	3.3.1 Symmetric Encryption	75
	3.3.2 Asymmetric Encryption	79
	3.4 Threshold Cryptography	82
	3.5 Identity Based Cryptography	83
	3.6 Summary	85
4	Literature Review	87
	4.1 Introduction	87
	4.2 Encryption Key Exchange	89
	4.3 Contributory Schemes	90
	4.4 Distributive Asymmetric Schemes	93
	4.5 Distributive Symmetric Schemes	101
	4.6 Conclusion	110
5	Design of the Key Management Scheme	111
	5.1 Introduction	111
	5.2 Key Features of the Design	113
	5.3 Design Steps for the Proposed Protocol	118
	5.4 Summary	131
6.	Performance Simulation of the Scheme	132
	6.1 Introduction	132
	6.2 Justification of Software Choice	133

6.2.1 Simulation Software Choices	133
6.3 Simulation Environment	137
6.4 Simulation Parameters	142
6.4.1 Blind versus Informed Requests	142
6.2.1 Percentage of Servers	143
6.4.3 Servers Required Rule	144
6.4.4 Trust Threshold	144
6.4.5 Node Growth Rate	145
6.4.6 Node Leave Rate	146
6.4.7 Node Mobility Model	146
6.4.8 Node Pause Time	147
6.4.9 Malicious Node Percentage	148
6.4.10 Malicious Message Threshold	149
6.4.11 Accusation Ejection Threshold and Timeout	149
6.4.12 Communication Distance	150
6.5 Simulations	150
6.5.1 Simulation Metrics	151
6.5.1.1 Measures	153
6.5.1.2 Input Parameters	153
6.6 Conclusion	155
7 Comparisons and Discussion of Results	157
7.1 Introduction	157
7.2 Blind versus Informed Request	163
7.3 Servers Required	165
7.3.1 Conclusion for Servers Required	168
7.4 Mobility	168
7.4.1 Speed	169
7.4.2 Conclusion for Speed	171
7.4.3 Percentage Mobile	171
7.4.4 Conclusion for Percentage Mobile	173
7.4.5 Percentage of Servers	173
7.4.6 Conclusion for Percentage of Servers	178
7.5 Server Rules	179
7.5.1 Server Rule Results: Not Updated	181
7.5.2 Server Rule Results: Updated	190
7.5.3 Most Updated Server Rule	191

7.5.4	Conclusion for Most Updated Server Rule	196
7.5.5	Least Updated Server Rule	198
7.5.6	Conclusion for Least Updated Server Rule	204
7.6	Comparisons With Other Protocols	205
7.7	Experimental Verification Scenario	208
7.8	Conclusion	210
8	Conclusions and Future Work	214
8.1	Introduction	214
8.2	Conclusions	214
8.3	Future Work	218
9	References	220
10	Appendices	
	Appendix 1: Lookup Tables for Mobility	226
	Appendix 2: Lookup Tables for Server Percentage	229
	Appendix 3: Server Location Comparisons	231

List of Figures

2.1	A Wireless mesh network	17
2.2	Ad Hoc network with a base station	19
2.3	Ad Hoc network extending range	20
2.4	Wireless network in infrastructure mode	22
2.5	Basic ad hoc network	24
2.6	North American operating channels: non-overlapping	32
2.7	North American operating channels: overlapping	32
2.8	WEP data unit	49
2.9	WEP encipherment	50
2.10	Authentication request and response	51
2.11	TKIP encapsulation	62
2.12	IEEE 802.1X architecture	64
3.1	Direct symmetric key exchange using Diffie-Hellman key exchange	75
3.2	Symmetric key exchange using a KDC	76
3.3	A successful request for Alice to communicate with Bob	81
4.1	Categorisation of KMS schemes	89
5.1	Wireless networks example – 4 servers required	127
6.1	MANET simulators used in research	133
6.2	Example OPNET Simulation	134
6.3	Example NS-2 Simulation	135
6.4	Example GloMoSim output	135
6.5	Random waypoint mobility model	147
6.6	Baseline simulation results	152
7.1	Simulation at 200, 400 and 600 seconds for 3 servers required	158
7.2	Results for 3 servers required with 20% mobility at 10-20kmh vs Trust	160
7.3	Network grid with 8 nodes	162
7.4	Certificate success – Informed Request vs Blind Request	164
7.5	Certificate success for 1 – 5 servers required vs Trust and static	166
7.6	Average hops for 1 – 5 servers required vs Trust	167
7.7	Certificate success: 1–5 servers vs Trust and 20% mobile at 40-50 kmh	169
7.8	Certificate success: 1–5 servers vs Trust and mobile up to 100 kmh	170
7.9	Certificate success: 1–5 servers vs Trust and 50% mobile at 40-50kmh	172

7.10	Certificate success: 1–5 servers vs Trust and static with 10% servers	174
7.11	Certificate success for 1 – 5 servers vs Trust and static with 50% servers	175
7.12	Certificate success: 1–5 servers vs trust and static with 100% servers	176
7.13	Average hops: 1–5 servers vs Trust and static with 100% servers	177
7.14	Static network with 1 and 2 servers required	182
7.15	Static network with 3, 4 and 5 servers required	183
7.16	Certificate success: 3, 4 and 5 servers with 20% mobile at 40-50kmh	185
7.17	Hops required for 3, 4 and 5 servers – static network	187
7.18	Hops required for 4 servers – 20% mobile at 40-50kmh	188
7.19	Hops required for 5 servers – 20% mobile at 40-50kmh.	189
7.20	Typical network server placement Most Updated vs Least Updated rule	190
7.21	Example of Most rule Updated with 5 servers required – 22 hops	191
7.22	Success rate: Most vs Most Updated with 1 and 2 servers required	192
7.23	Most rule vs Most Updated rule with 3, 4 and 5 servers required	194
7.24	Least server rule with five servers required – 30 hops	198
7.25	Success rate: Random / Most vs Least Updated 1 and 2 servers required	200
7.26	Success rate: Most rule vs Least Updated rule: 3, 4 and 5 servers required	201
7.27	Server role exchanges for Most Updated rule vs Least Updated rule	203

List of Tables

1.1	The six aspects of security in a network	4
2.1	Rate-dependant parameters	30
2.2	Valid operating channels	30
2.3	Wireless network attack tools	38
2.4	Network attacks	47
2.5	Standards based encryption methods	65
3.1	Basic fields of an IETF X.509 v3 Digital Certificate	80
4.1	Characteristics of key exchange and contributory schemes	93
4.2	Characteristics of distributive asymmetric schemes	101
4.3	Characteristics of distributive symmetric schemes	110
5.1	Comparison of protocol features	119
5.2	Benefits and drawbacks of features	120
6.1	Simulation environment	137
6.2	Simulation fixed parameters	138
6.3	Simulation variable parameters	141
6.4	Simulation runs	151
6.5	Initial experiment variable parameters	152
7.1	Network graphics legend	157
7.2	Static versus mobile network certificate issuance efficiency	171
7.3	Average hops & success Percentage for a certificate 10% to 100% servers – 3 servers required	177
7.4	Average hops – Random / Most v Most Updated server rule	195
7.5	Average server role exchanges for Most Updated rule: 1-5 servers	196
7.6	Average hops – Random / Most v Least Updated server rule	202
7.7	Average server role exchanges – Least Updated rule: 1-5 servers	203
7.8	Recommended default settings for SKYE	212

List of Publications

Nisbet, A. J. *Wireless Networks in Education – A New Zealand Perspective*.

Proceedings of the IIMS Postgraduate Conference 2004, Massey University, Auckland, 2004.

Nisbet, A.J. *An Improved Encryption Key Management System for IEEE 802.16 Mesh*

Mode Security Using Simulation. Proceedings of the Fifth New Zealand Computer Science Research Student Conference, Waikato University, Hamilton, 2007.

Nisbet, A.J. Rashid M.A., *A Scalable & Tunable Encryption Key Management System*

for Mobile Ad Hoc Networks. Proceedings of the 2009 International Conference on Wireless Networks, Las Vegas, USA, 2009.

Nisbet, A.J, Rashid M.A, Alam, F. *The Quest for Optimum Server Location Selection in*

Mobile Ad Hoc Networks Utilising Threshold Cryptography. Proceedings of the 7th International Conference on International Technology: New Generations. Las Vegas, USA, 2010.

Nisbet, A.J, Rashid M.A. *Performance Evaluation of Secure Key Deployment and*

Exchange Protocol for MANETs. Accepted for International Journal of Secure Software Engineering (IJSSE), 2010.

Abbreviations and Acronyms

AAA	Authentication Authorisation and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
AS	Access Server
BPSK	Binary Phase Shift Keying
BSS	Basic Service Set
CA	Certificate Authority
CCK	Complimentary Code Keying
CCM	Clear Channel Assessment under MAC
CPU	Central Processing Unit
CRC	Cyclic Redundancy Checksum
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
DBPSK	Differential Binary Phase Shift Keying
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DQPSK	Differential Quadrature Phase Shift Keying
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol Over LAN
ETSI	European Telecommunications Standards Institute
ERP	Extended Rate PHY
IBSS	Independent Basic Service Set
IC	Integrity Check
ICV	Integrity Check Value
ID	Identity
IEEE	Institute of Electronics and Electrical Engineers
IP	Internet Protocol
IPSec	Internet Protocol Security
IV	Initialisation Vector

FCC	Federal Communications Commission
FH	Frequency Hopping
GHz	Gigahertz
ISM	Industrial Scientific and Medical
KDC	Key Distribution Centre
KGS	Key Generation Server
KM	Key Management
KMS	Key Management Service
L2F	Layer 2 Forwarding
LAN	Local Area Network
MAC	Media Access Control
MANET	Mobile Ad Hoc Network
Mbps	Mega bits per second
MIC	Message Integrity Check
MIMO	Multiple Input Multiple Output
MPDU	MAC Packet Data Unit
MSDU	MAC Service Data Unit
MTM	Man in The Middle
NAS	Network Access Server
OFDM	Orthogonal Frequency Division Multiplexing
PBCC	Packet Binary Convolutional Coding
PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PHY	Physical Layer
PKI	Public Key Infrastructure
PMK	Pre-shared Master Key
PPTP	Point To Point Tunnelling protocol
PRNG	Pseudo Random Number Generator
PSK	Pre-Shared Key
PTK	Pre-shared Temporal Key
PTMP	Point to Multi Point
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying

RADIUS	Remote Access Dial In User Service
RFMon	Radio Frequency Monitor Mode
RTS/CTS	Request to Send / Clear to Send
STA	Station
TGT	Ticket Granting Ticket
TKIP	Temporal Key Integrity Protocol
TTP	Trusted Third Party
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WiMax	Worldwide Interoperability for Microwave Access
WPA	WiFi Protected Access
XOR	Exclusive Or