Quantum Cryptography for Secure Communication in IEEE 802.11 Wireless Networks

Shirantha Wijesekera

Faculty of Information Sciences and Engineering

University of Canberra ACT 2601

A thesis submitted in fulfilment of the requirements of the

Degree of Doctor of Philosophy

June 2011

Abstract

IEEE 802.11 is the Wireless Local Area Networks (WLAN) standard developed by the IEEE LAN/MAN Standards Committee. WLANs are increasingly deployed by businesses, government and SOHO users as they offer many advantages to customers with mobility, flexibility and convenience. Wi-Fi is a trademark of the Wi-Fi Alliance that has been used with certified products that belong to a class of WLANs based on the IEEE 802.11 standards. WLANs have become one of the widely used communication systems in the world. It is estimated that there are over 4,00,000 hotspots and millions of Wi-Fi users across the world as of now.

Since there are no boundaries in wireless networks, they are more vulnerable to security threats than their wired counterparts. It is possible for an attacker to snoop on confidential communications or modify them to gain access to the wireless networks more easily. Therefore, providing secure communication for wireless networks has become one of the prime concerns. IEEE has made amendments to the initial release of 802.11 standard with the 2004 release of 802.11i, since the former version was found to having security weaknesses in the way it handles authentication and privacy.

Quantum Key Distribution (QKD), based on quantum cryptography, offers the promise of unconditional security. QKD enables two parties to distribute a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages.

This research implements a novel method of integrating QKD to distribute the secret key in WLANs. IEEE 802.11i standard uses a *4 way handshake* procedure to distribute the key used to encrypt the data communication. In this research, instead of using the 4 way handshake procedure, QKD based key distribution for IEEE 802.11 has been implemented targeting the Counter mode with CBC-MAC Protocol (CCMP) of the Robust Security Network Association (RSNA). Necessary communication flows of existing IEEE 802.11 protocol have been indentified and modified. These modifications are done in such a way that only some of the selected fields of the existing protocol have been used to carry QKD specific information. Existing frame formats are not changed, keeping the overall modifications to a minimum. The

resulting QKD based novel protocol offers unconditional security to the wireless networks with the use of key distributed via QKD.

The key distribution process splits into two main communication channels. Firstly, it uses quantum channel to transmit the photons where both parties interpret each photon to a bit (0 or 1) depending on the bases and polarisation used. Secondly it uses classical channel, in this case it is the existing wireless channel, to retrieve the final secured key.

Further, a number of possible extensions to IEEE 802.16 (WiMax) and also possibility of merging with IEEE 802.21 standard are also discussed. Several possible enhancements of this research are presented. One such enhancement is the use of Multi Agent Systems (MAS) to deploy the same solution with better control and more efficiently.

Acknowledgements

First and foremost I would like to thank Associate Professor Xu Huang for supervision and support over the course of my PhD program. His selfless perseverance, consistent attention to my work and many insightful comments has been a great aid to me in completing this research. He has been instrumental in providing me the guidance through his academic experience which was always there when I needed. This research would never have taken shape without his support.

I would also like to express my humble gratitude to Professor Dharmendra Sharma for his supervision, inspiration and kindness right throughout this research which has been invaluable to me.

I am extremely grateful to my previous supervisors Assistant Professor Bala Balachandran, Dr Sajal Palit, Dr Adrian Whichello for their support towards my studies.

I am indebted to emeritus Professor Paul Edwards for his supervision, enthusiasm and inspiration given to me during the initial stage of this research. I would also like to thank him for granting me CATQER top up scholarship.

I must also thank the IT support staff for their timely interventions to resolve my network issues.

I am heartily thankful to administration staff of ISE, specially Serena Chong, Coral Suthern and Kylie Reece for their support given to me in many ways.

I am grateful for University of Canberra for choosing me for a RTS scholarship, which was an invaluable aid to me in completing my PhD.

Last, but not least, I would like to thank my wife and daughter for their support and understanding right throughout the course of my studies.

List of Acronyms

ACK	Acknowledgement
AES	Advanced Encryption Standard
AK	Authorisation Key
ANonce	random or pseudo-random value generated by the Access Point
AP	Access Point
APD	Silicon Avalanche Photodiode
ARP	Address Resolution Protocol
B92	QKD protocol developed by C. H. Bennett in 1992
BB84	QKD protocol developed by Bennett and Brassard 1984
BS	Base Station
BSS	Basic Service Set
CA	Certificate Authority
CCMP	Counter mode with CBC-MAC Protocol
CR	Cognitive Radio
CTS	Clear to Send
DES	Data Encryption Standard
DoS	Denial of Service
DS	Distribution System
EAP-AKA	EAP for UMTS Authentication and Key Agreement)
EAPOL	Extensible Authentication Protocol over LAN
EAP-SIM	EAP for GSM Subscriber Identity
EAP-TLS	EAP Transport Layer Security
EAP-TTLS	EAP-Tunnelled Transport Layer Security
ECC	Elliptic Curve Cryptography
ESS	Extended Service Set
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GTK	Group Temporal Key
IBSS	Independent Basic Service Set
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers

IPsec	Internet Protocol Security
IV	Initialization Vector
KCK	Key Confirmation Key
KEK	Key Encryption Key
L2TP	Layer 2 Tunnelling Protocol
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control
MAS	Multi Agent System
MIC	Message Integrity Check
MIMO	Multiple-Input Multiple-Output
MLME	MAC Sublayer Management Entity
NAT	Network Address Translation
NIC	Network Interface Controller
P2P	Peer to Peer
PHY	Physical layer
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PKM	Privacy Key Management
PMK	Pairwise Master Key
PPTP	Point-to-Point Tunnelling Protocol
PRF	Pseudo Random Function
PTK	Pairwise Transient Key
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
Q-Key	Quantum Key
Qubit	Quantum Bit
RADIUS	Remote Authentication Dial In User Service
RSA	Rivest-Shamin-Adleman
RSN	Robust Security Networks
RSNA	Robust Security Network Association
RTS	Request to Send
SAID	Security Association IDs
SARG04	QKD protocol (derived from BB84)

SNonce	random or pseudo-random value generated by the Station
SS	Subscriber Station
SSID	Service Set Identifier
SSL	Secure Sockets Layer protocol
TEK	Traffic Encryption Keys
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
TSN	Transition Security Network
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over IP
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Networks
WMAN	Wireless Metropolitan area networks
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPAN	Wireless Personal Area Networks

Nomenclature:

- **IEEE 802.1X** standard provides authentication mechanism to clients accessing the IEEE 802.11 wireless network. IEEE 802.1X uses three main parties of its architecture: *Authenticator*, *Supplicant* and *Authentication Server***.** These entities have been referred to in the network documentation by various other terms as well.

  Widely used terms for the *Authenticator* are: *Access Point* (AP), *Base Station* (BS) etc.

  Widely used terms for the *Supplicant* are: *Station* (STA), *Client, Subscriber Station* (SS) etc.

  For consistency, throughout this thesis, these entities have been referred as **AP** (*Authenticator*) and **STA** (*Supplicant*).

  Also for simplicity, the functionalities of the *Authentication Server* has been assumed to be implemented within the AP.

- **Wi-Fi** is the industry standard for products as defined by the Wi-Fi Alliance and conforming to IEEE 802.11 standard. Because of the relationship with the underlying standards, the term Wi-Fi is often used as a synonym for IEEE 802.11 technology. Further IEEE 802.11i standard specifies security mechanisms for wireless networks done as an amendment to the original IEEE 802.11. Throughout this thesis, the term **Wi-Fi** has also been referred as **IEEE 802.11** and **IEEE 802.11i**.

.

Table of Contents

List of Tables

List of Figures