A SECURE WIRELESS NETWORK ARCHITECTURE PROPOSAL TO BE USED BY GOVERNMENTS IN CASE OF EMERGENCY SITUATIONS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF INFORMATICS
OF
THE MIDDLE EAST TECHNICAL UNIVERSITY

BY

MUSTAFA AKSOY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF INFORMATION SYSTEMS

SEPTEMBER 2007

Approval of the Graduate School of Informatics

_____

Prof.Dr. Nazife BAYKAL
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

_____

Assoc.Prof.Dr. Yasemin YARDIMCI
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____

Prof.Dr. Nazife BAYKAL
Supervisor

Examining Committee Members

Assoc.Prof.Dr. Y.Murat ERTEN	(TOBB ETU, CENG)	_____
Prof.Dr. Nazife BAYKAL	(METU, II)	_____
Dr. Ali ARİFOĞLU	(METU, IS)	_____
Dr. Erhan EREN	(METU, IS)	_____
Dr. Altan KOÇYİĞİT	(METU, IS)	_____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name : Mustafa AKSOY

Signature : _____

ABSTRACT

A SECURE WIRELESS NETWORK ARCHITECTURE PROPOSAL TO BE USED BY GOVERNMENTS IN CASE OF EMERGENCY SITUATIONS

AKSOY, Mustafa
MS, Department of Information Systems
Supervisor: Prof. Dr. Nazife BAYKAL

September 2007, 74 pages

Since wireless network technology has advanced swiftly and dropped in price, it became a widely used networking option among numerous organizations and even single home users. In spite of their widespread usage by private sector, wireless networks are still undesired alternative for the governments due to security concerns. Although wireless networks possessed lots of proven and documented security flaws at first, with the latest researches and developments this condition ameliorated by the time and wireless networks became much more robust to various security attacks. In this thesis, a secure wireless network architecture that will allow exchange of unclassified information, using 802.11 (Wi-fi) and 802.16 (WIMAX), will be proposed that could be established by governments in case of emergency situations, namely natural disasters or wars, where cable infrastructure becomes unavailable.

Keywords: WLAN, WMAN, 802.16, 802.11, Wireless Security

öz

OLAĞANÜSTÜ DURUMLARDA RESMİ KURUMLAR TARAFINDAN
KULLANILABİLECEK GÜVENLİ BİR KABLOSUZ AĞ MİMARİ ÖNERİSİ

AKSOY, Mustafa
Yüksek Lisans, Bilişim Sistemleri Bölümü
Tez Danışmanı: Prof. Dr. Nazife BAYKAL

Eylül 2007, 74 sayfa

Kablosuz ağ teknolojisi, hızlı gelişiminden ve fiyatlarının düşmesinden dolayı pek çok kuruluş ve hatta ev kullanıcıları arasında yaygın olarak kullanılan bir ağ seçeneği haline gelmiştir. Özel sektör tarafından yaygın kullanımına rağmen, güvenlik endişelerinden dolayı kablosuz ağlar, resmi kurumlar tarafından halen tercih edilmeyen bir alternatif konumundadır. Kablosuz ağlar, ilk başlarda pek çok güvenlik açıklarına sahip olmalarına rağmen, son zamanlardaki araştırma ve geliştirmelerle bu durum zamanla iyileşmiş ve kablosuz ağlar saldırılara karşı çok daha dirençli hale gelmiştir. Bu tezde, resmi kurumlar tarafından, kablo altyapısının elverişsiz hale geldiği doğal afet ve savaşlar gibi olağanüstü durumlarda, 802.11 (Wi-fi) ve 802.16 (WIMAX) kullanılarak tesis edilebilecek ve gizlilik derecesi olmayan bilgilerin değişimini sağlayacak güvenli bir kablosuz ağ mimarisi önerilecektir.

Anahtar Sözcükler: WLAN, WMAN, 802.16, 802.11, Kablosuz Ağ Güvenliği

To My Beloved Family…

ACKNOWLEDGEMENTS

First of all I would like to express sincere appreciation to Prof. Dr. Nazife BAYKAL who has shown the courtesy of accepting to be my advisor in spite of her excessively busy schedule. I also owe her my gratitude for her invaluable support and guidance with her exceptionally modest attitude.

And I will always be grateful to Dr. Altan KOCYIGIT and Dr. Omer DELIALIOGLU who made me love computer networking more than ever.

I offer cordial thanks to my wife, Gonul, and to my daughter, Oyku, for their faith in me and for their understanding and support during my entire study.

TABLE OF CONTENTS

ABSTRACT iv
ÖZ v
DEDICATION vi
ACKNOWLEDGEMENTS vii
TABLE OF CONTENTS viii
LIST OF TABLES x
LIST OF FIGURES xi
LIST OF ABBREVIATIONS xiii
CHAPTER
1. INTRODUCTION 1
1.1 Background 1
1.2 Problem Definition 2
1.3 Research Goal 3
1.4 Research Method 3
1.5 Research Limitations 3
1.6 Thesis Organization 3
2. OVERVIEW OF IEEE 802.11 STANDARD 5
2.1 802.11 Network Architecture 6
2.2 802.11 Physical Layer 8
2.3 802.11 MAC Layer 9
2.4 802.11 Security 11
2.4.1 WEP 11
2.4.2 WPA 14
2.4.3 802.11i (WPA2) 19
3. OVERVIEW OF IEEE 802.16 STANDARD 25
3.1 802.16 Network Architecture 26
3.2 802.16 Physical Layer 28
3.3 802.16 MAC Layer 29

3.4 802.16 Security 31
3.4.1 Authentication and Key Management 32
3.4.2 Data Encryption 34
4. SECURE WIRELESS NETWORK ARCHITECTURE PROPOSAL 36
4.1 Rationale for a New Security Architecture 37
4.2 New Security Architecture 40
4.2.1 WLAN Architecture 41
4.2.2 WMAN Architecture 45
4.2.3 Certificate Management 46
5. SECURITY AND PERFORMANCE ANALYSIS 50
5.1 Security Analysis 51
5.1.1 WLAN Security Analysis 51
5.1.2 WLAN Threat Analysis 52
5.1.3 WMAN Security Analysis 53
5.1.4 WMAN Threat Analysis 54
5.2 Performance analysis 54
5.2.1 Analysis of Certificate Management 55
5.2.2 Analysis of Authentication Scheme 56
5.2.3 Modification Requirements 59
6. CONCLUSIONS 62
6.1 Synopsis of the Proposal 62
6.2 Pros and Cons 63
6.3 Future Work 64
BIBLIOGRAPHY 65
APPENDICES
A. PAE STATE MACHINE IN STA 69
B. PAE STATE MACHINE IN AP 70
C. CERTIFICATE MANAGEMENT PROCESS FLOW DIAGRAM 71
D. CERTIFICATE MANAGEMENT SCENARIOS 72

LIST OF TABLES

Table 1. Comparison of 802.11 Standards 6
Table 2. 802.11 Physical Layer Properties..... 9
Table 3. IEEE 802.16 Standards 25
Table 4. 802.16 Physical Layer Specifications.....28
Table 5. EAPOL Frame Format.....41
Table 6. RSA Packet Format.....42
Table 7. Certificate Exchange Message Format 47
Table 8. Authentication Message Flow on WLAN without AS 57
Table 9. Authentication Message Flow on WMAN without AS 57
Table 10. Authentication Message Flow on WLAN with AS.....57
Table 11. Authentication Message Flow on WMAN with central AS 58
Table 12. Scenario 1 – Certificate renewal of STA.....72
Table 13. Scenario 2 – Certificate renewal of AP 73
Table 14. Scenario 3 – Certificate renewal of BS 73
Table 15. Scenario 4 – Certificate renewal of SS 74

LIST OF FIGURES

Figure 1. Overview of IEEE 802 Network Standards 2
Figure 2. IEEE 802.11 Mapped to the OSI Reference Model 5
Figure 3. Basic Service Set 7
Figure 4. Extended Service Set 7
Figure 5. Independent Basic Service Set 7
Figure 6. 802.11 CSMA/CA 10
Figure 7. 802.11 Generic MAC Frame 10
Figure 8. Overview of Encryption and Decryption with RC4 12
Figure 9. WEP Authentication 13
Figure 10. 802.1x Framework 15
Figure 11. A typical 802.1x message flow with EAP-TLS 16
Figure 12. TKIP Key Hierarchy 17
Figure 13. 4-Way Handshake 18
Figure 14. Group Key Handshake 18
Figure 15. AES-CCMP Key Hierarchy 19
Figure 16. CBC-MAC 20
Figure 17. AES Counter Mode 21
Figure 18. CCMP Encrypted 802.11 MAC Frame 21
Figure 19. RSN IE Format 21
Figure 20. RSNA Establishment 22
Figure 21. IEEE 802.16 Protocol Stack 26
Figure 22. A Single 802.16 Cell 27
Figure 23. 802.16 Mesh Topology 27
Figure 24. 802.16 Applications 28
Figure 25. Dynamic Adaptive Modulation 29
Figure 26. ATM CS PDU Format 29
Figure 27. 802.16 MAC PDU Format 30
Figure 28. PKMv2 RSA Based Authorization 32

Figure 29. PKMv2 EAP Authorization 33
Figure 30. 802.16 Encryption Process 34
Figure 31. 802.16 Data Key Exchange 34
Figure 32. Typical Network Topology with 802.11 and 802.16 36
Figure 33. Network Topology Option with Multiple AS 37
Figure 34. Network Topology Option with Single AS 38
Figure 35. UDP Segment Carrying RADIUS Data 38
Figure 36. STA-AS Message Exchange with EAP-TLS 39
Figure 37. Authentication Load vs. Number of Clients on WMAN 39
Figure 38. Overview of the New Security Architecture 40
Figure 39. RSA Authentication 43
Figure 40. Certificate Management Messages 55
Figure 41. Authentication Load on WLAN 58
Figure 42. Authentication Load on WMAN 59
Figure 43. Proposed Security Architecture 62
Figure 44. PAE State Machine in STA 69
Figure 45. PAE State Machine in AP 70
Figure 46. Certificate Management Process Flow Diagram 71

LIST OF ABBREVIATIONS

AAA	: Authentication, Authorization, and Accounting
ACK	: Acknowledgement
AK	: Authorization Key
AKID	: Authorization Key ID
AP	: Access Point
ARPANET	: Advanced Research Projects Agency Network
AS	: Authentication Server
ASF	: Alerting Standards Forum
AES	: Advanced Encryption Standard
BR	: Bandwidth Request
BS	: Base Station
BSID	: Base Station ID
BSS	: Basic Service Set
CA	: Certificate Authority
CBC-MAC	: Cipher Block Chaining Message Authentication Code
CCM	: Counter-Mode/CBC-MAC Protocol (802.16e)
CCMP	: Counter-Mode/CBC-MAC Protocol (802.11i)
CEM	: Certificate Exchange Message
CI	: CRC Indicator
CID	: Connection Identifier
CLP	: Cell Loss Priority
CPE	: Customer Premises Equipment
CRC	: Cyclic Redundancy Check
CSMA/CD	: Carrier Sense Multiple Access/Collision Detection
CSMA/CA	: Carrier Sense Multiple Access/Collision Avoidance
CTS	: Clear to Send
DIFS	: Distributed Inter-Frame Space
DL	: Downlink
DoS	: Denial of Service
DS	: Distribution System
DSL	: Digital Subscriber Line

DSSS : Direct Sequence Spread Spectrum
EAP : Extensible Authentication Protocol
EAPOL : EAP over LAN
EBSS : Extended Basic Service Set
EC : Encryption Control
EKS : Encryption Key Sequence
FBWA : Fixed Broadband Wireless Access
FCC : Federal Communications Commission
FCH : Frame Control Header
FCS : Frame Check Sequence
FDD : Frequency Division Duplexing
FDM : Frequency Division Multiplexing
FEC : Forward Error Correction
FHSS : Frequency Hopping Spread Spectrum
GKEK : Group Key Encryption Key
GSA : Group Security Association
GTEK : Group Traffic Encryption Key
GTK : Group Temporal Key
HCS : Header Check Sequence
HR : High Rate
HT : Header Type
IBSS : Independent Basic Service Set
IE : Information Element
IEEE : Institute of Electrical and Electronics Engineers
IR : Infrared
ISM : Industrial, Scientific and Medical
IV : Initialization Vector
KEK : Key Encryption Key
LAN : Local Area Network
LLC : Logical Link Control
LOS : Line of Sight
MAC : Medium Access Control
MAC CPS : MAC Common Part Sublayer
MAC CS : Service Specific Convergence Sublayer
MAN : Metropolitan Area Network
MBWA : Mobile Broadband Wireless Access
MIC : Message Integrity Code
MIMO : Multiple-Input/Multiple-Output
MSK : Master Session Key
NAV : Network Allocation Vector

OFDM : Orthogonal Frequency Division Multiplexing
OFDMA : Orthogonal Frequency Division Multiple Access
O/S : Open System
PACP : Port Access Control Protocol
PAE : Port Access Entity
PAK : Primary Authorization Key
PAN : Personal Area Network
PDA : Personal Digital Assistant
PEAP : Protected EAP
PDU : Protocol Data Unit
PHY : Physical Layer
PKCS : Public Key Cryptography Standard
PKM : Privacy Key Management
PLCP : Physical Layer Convergence Procedure
PMD : Physical Medium Dependent
PMK : Pairwise Master Key
PN : Packet Number
PRNG : Pseudo Random Number Generator
PSK : Pre-shared Key
PTI : Payload Type indicator
PTK : Pairwise Transient Key
QAM : Quadrature Amplitude Modulation
QoS : Quality of Service
QPSK : Quadrature Phase-Shift Keying
RADIUS : Remote Authentication Dial In User Service
RC4 : Rivest Cipher 4
RFC : Request for Comments
RN : Random Number
RSA : Rivest Shamir Adleman
RSN : Robust Security Network
RSNA : Robust Security Network Associations
RTS : Request to Send
SA : Security Association
SAID : Security Association ID
SAP : Service Access Point
SHA : Secure Hash Algorithm
SIFS : Short Inter-Frame Space
SNAP : Subnetwork Access Protocol
SNR : Signal Noise Ratio
SOFDMA : Scalable Orthogonal Frequency Division Multiple Access

SS	: Subscriber Station
SSL	: Secure Socket Layer
STA	: Wireless Station
TAG	: Technical Advisory Group
TCS	: Transmission Convergence Sublayer
TDD	: Time Division Duplexing
TEK	: Traffic Encryption Key
TKIP	: Temporal Key Integrity Protocol
TLS	: Transport Layer Security
TSC	: TKIP Sequence Counter
TTLS	: Tunneled TLS
UDP	: User Datagram Protocol
UL	: Uplink
VCI	: Virtual Channel Identifier
WEP	: Wired Equivalent Privacy
Wi-fi	: Wireless Fidelity
WIMAX	: Worldwide Interoperability for Microwave Access
WLAN	: Wireless LAN
WMAN	: Wireless MAN
WPA	: Wireless Protected Access
WPAN	: Wireless PAN
WRAP	: Wireless Robust Authenticated Protocol

CHAPTER 1

INTRODUCTION

1.1 Background

The history of wireless communications extends back to 19th century. In 1885, Heinrich Hertz generated and transmitted radio waves. After then in 1896, Guglielmo Marconi achieved to send telegraph signals across the Bristol Channel over a distance of 1.75 miles. Just five years later in 1901, again Marconi successfully sent signals across the Atlantic, a distance of 2100 miles. Public use of radio began in 1907 and Edwin Armstrong invented the FM radio in 1933. Packet data technology was developed in the mid-1960s and was put into practical application in the ARPANET. Initiated in 1970, the ALOHANET, based at the University of Hawaii, was the first large-scale packet radio project.

The main standards in the wireless data networks are: 802.11, which stands for Wireless Local Area Network (WLAN), and 802.16 which describes Wireless Metropolitan Are Network (WMAN). These two wireless network standards are usually known by two acronyms: Wireless Fidelity (Wi-fi) to be a symbol of WLAN, and Worldwide Interoperability for Microwave Access (WIMAX) to be a symbol of WMAN.

Wi-fi came up as a result of the decision taken by the Federal Communications Commission (FCC) in 1985 to open several bands of the wireless spectrum for use without a government license. In 1990, a new IEEE committee was set up to develop a standard for wireless LANs. 802.11 Wireless Local Area Networks standard published in 1997. IEEE started studies on Broadband Wireless Access

in 1999, and published the 802.16 Broadband Wireless Access (WMAN) standard in 2002.

In spite of their rapid growth, flexible nature and low price, wireless technologies still have some disadvantages. Security is a major drawback of top priority. Because of using the space as the transmission media, wireless networks are open to eavesdropping and jamming and they need quite more attention than their wired equivalents.

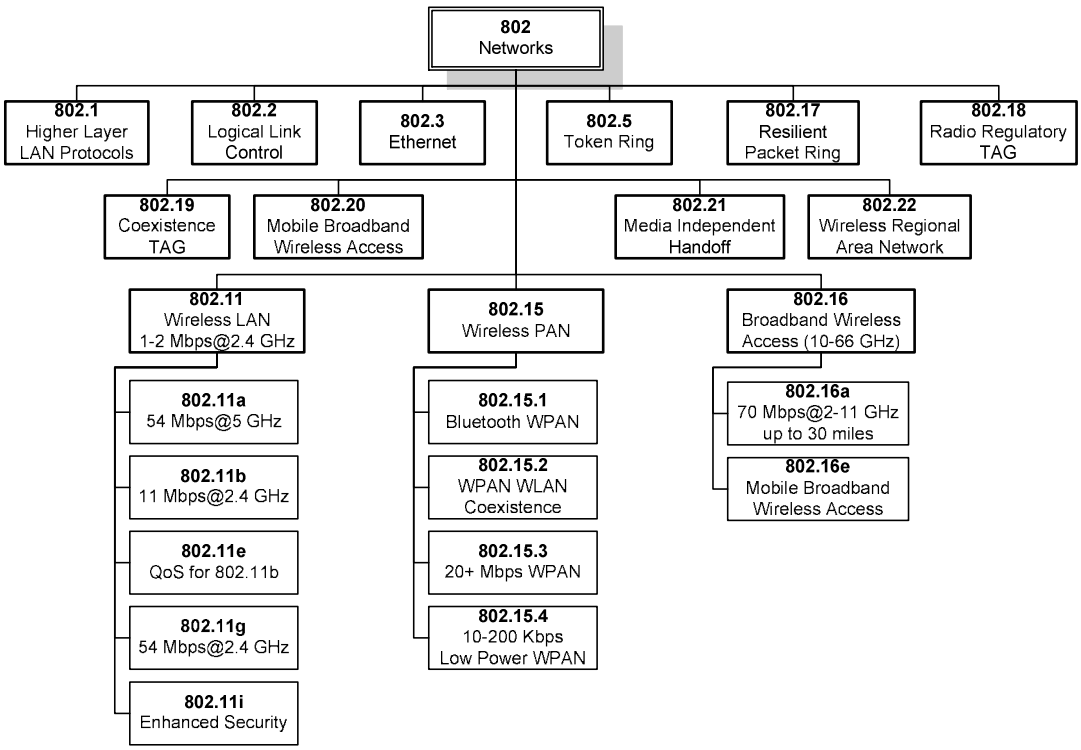


Figure 1. Overview of IEEE 802 Network Standards

1.2 Problem Definition

Vulnerable nature of wireless networks combined with the security flaws of foremost standards makes it an undesired technology for the governments with plenty of classified information to exchange. However, in case of emergency situations like wars, quakes, floods etc. when the cable infrastructures becomes unavailable, governments will most be in need of a data network to keep going their activities. Besides, it is also evident that emergency situations are such conditions that information becomes very precious. Recent researches on wireless network security resulted in new products with new security features that make wireless networks much more robust to various attacks. The problem

that will be addressed in this thesis is providing governments secure wireless network architecture for exchanging classified information that can be used in emergency situations.

1.3 Research Goal

The main goal of this thesis is to propose secure wireless network architecture for the governments that will provide the exchange of unclassified information using 802.11 and 802.16 with some minor changes aiming to improve manageability and efficiency.

1.4 Research Method

An inductive method is followed during the preparation of this thesis. During the research, literature study is done, mostly through Internet, IEEE, and ACM, where latest news about the protocol was announced. Ratified RfCs and standards are used.

1.5 Research Limitations

Because of the financial restrictions researches are at the theoretical level and no laboratory experiments or other practical research methods are used.

1.6 Thesis Organization

Chapter 1

Chapter 1 contains thesis objectives and organization and also a brief history and explanation about wireless communication and wireless security.

Chapter 2

Chapter 2 is an overview of 802.11 Wireless LAN Standard especially from the security point of view. Known vulnerabilities are discussed in this chapter.

Chapter 3

Chapter 3 is an overview of 802.16 Broadband Wireless Access Standard especially from the security point of view. Known vulnerabilities are discussed in this chapter.

Chapter 4

This chapter contains the rationale for secure wireless network architecture proposal and proposal itself.

Chapter 5

Security and performance analysis of the proposed architecture will be presented in this chapter.

Chapter 6

This chapter will provide a synopsis of the proposal, conclusions derived from the overall study, and future work.

CHAPTER 2

OVERVIEW OF IEEE 802.11 STANDARD

The IEEE 802.11 standard is the member of the 802 family which consists of several specifications about LAN technologies. 802.11 specifies the interface between a wireless client and a base station or access point, as well as among wireless clients. The standard addresses both the Physical (PHY) and Media Access Control (MAC) layers and is similar in most respects to the IEEE 802.3 Ethernet standard. The 802.11 standard deals particularly with:

- Specifications required for an 802.11 device to operate either in a peer-to-peer fashion or integrated with an existing wired LAN
- Operation within overlapping 802.11 WLANs and mobility
- MAC level access control and data delivery services to upper layers
- Physical layer signaling techniques and interfaces
- Privacy and security

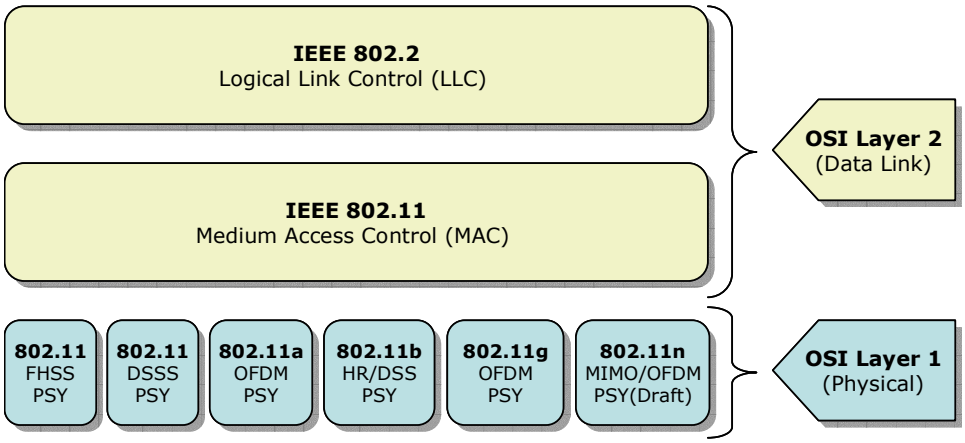


Figure 2. IEEE 802.11 Mapped to the OSI Reference Model

802.11 products were initially released in 1997. Infrared (IR), Frequency Hopping Spread Spectrum (FHSS), and Direct Sequence Spread Spectrum (DSSS) were being used at the physical layer. IR has never been widely used and the data rate was limited up to 2 Mbps which is quite slow compared to current WLAN technologies. 802.11 working group continued its studies and released the new standards 802.11a and 802.11b in 1999. While 802.11a uses Orthogonal Frequency Division Multiplexing (OFDM) and operates on 5 GHz frequency band with 54 Mbps maximum speed, 802.11 b uses high rate DSSS at the 2.4 GHz frequency band (S-band ISM) providing a data rate of 11 Mbps. In 2003, 802.11g was released. This standard works at the same frequency band with 802.11b but uses OFDM and provides a speed of 54 Mbps. IEEE is still working on 802.11n. The real data throughput of this draft standard is estimated to reach a theoretical 540 Mbps. 802.11n is being constructed on previous 802.11 standards by adding Multiple-Input/Multiple-Output (MIMO). By benefiting from MIMO, using multiple transmitter and receiver antennas is being considered to allow for increased data throughput.

Table 1. Comparison of 802.11 Standards

Standard	Frequency Band	Speed (Max)	Range (Indoor)	Release Date
802.11 (Legacy)	2.4 GHz	2 Mbps	-	1997
802.11a	5 GHz	54 Mbps	30 m	1999
802.11b	2.4 GHz	11 Mbps	50 m	1999
802.11g	2.4 GHz	54 Mbps	30 m	2003
802.11n	2.4 GHz or 5 GHz	540 Mbps	50 m	Draft

2.1 802.11 Network Architecture

802.11 is based on a cellular approach where each cell is called a Basic Service Set (BSS). There are two operational modes: Infrastructure Mode and Ad Hoc Mode. In Infrastructure Mode wireless stations (STA) communicate with each other through a base station called Access Point (AP) which is typically connected to a wired network called Distribution System (DS). In Ad Hoc Mode wireless stations communicate directly with each other, without using an AP. Possible architectures are BSS, Extended BSS (EBSS), and Independent BSS (IBSS).

In BSS there is an AP and one or more wireless stations. The stations do not communicate directly other stations. They communicate with the AP, and the AP forwards the frames to the destination stations.

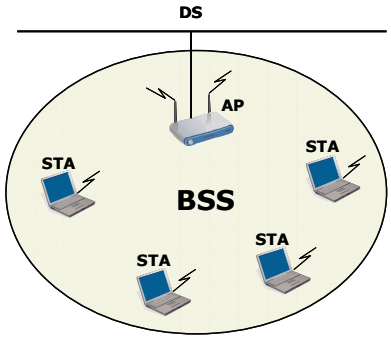


Figure 3. Basic Service Set

A number of BSSs connected via a DS is called ESS.

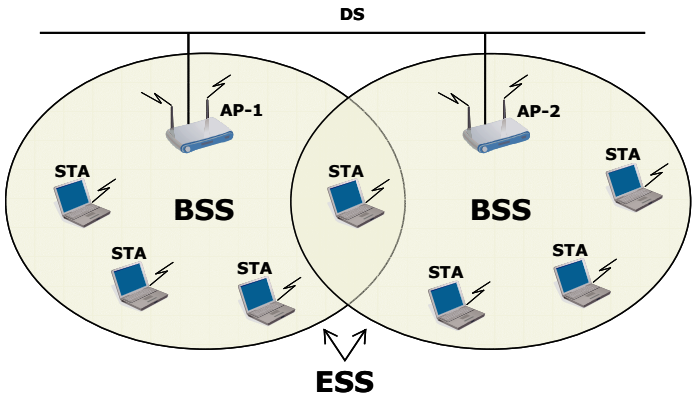


Figure 4. Extended Service Set

In an IBSS, there is no AP and wireless stations communicate with each other directly.

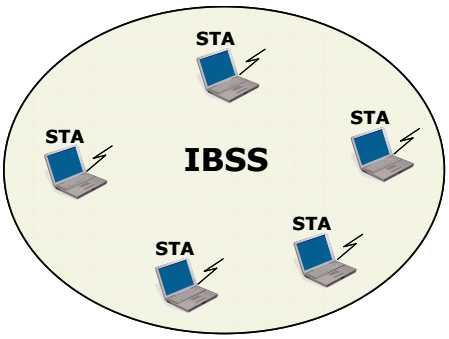


Figure 5. Independent Basic Service Set

2.2 802.11 Physical Layer

Physical layer comprises of two sublayers: Physical Layer Convergence Procedure (PLCP) and Physical Medium Dependent (PMD). PLCP is the interface between PMD and MAC. PLCP adds its own header to the frame and PMD is responsible for transmitting the bits it received from PLCP.

In the initial revision of the 802.11, three physical layers were standardized:

- Frequency-hopping spread-spectrum (FHSS) radio PHY
- Direct-sequence spread-spectrum (DSSS) radio PHY
- Infrared light (IR) PHY

Although IR is a physical layer standard, no products have been created based on it. In 1999 two more physical layers were added to the standard:

- Orthogonal Frequency Division Multiplexing (OFDM) PHY
- High-Rate Direct Sequence (HR/DSSS) PHY

As it can be inferred from above that there are three spread-spectrum techniques used in 802.11:

- FHSS is a technique in which data signal is modulated with a narrow band carrier signal jumping randomly from one frequency to another according to a hopping code within a specified frequency range. It reduces interference.
- DSSS is achieved by spreading the narrowband radio signal to a wider frequency band. Although it requires more power, it is more reliable. HR/DSSS is the advanced version of DSSS defined by 802.11b. HR/DSSS uses complementary code keying technique which enables it to achieve faster data rates.
- OFDM is similar to frequency division multiplexing (FDM) but it achieves higher throughput by using several overlapping but do not interfering channels. Separating overlapping channels is accomplished with the help of complex mathematical relationship called orthogonality.

802.11 specifications according to their physical layer properties are listed below.

Table 2. 802.11 Physical Layer Properties

Standard	Frequency Band	Modulation Technique	Speed (Max)
802.11	2.4 GHz	FHSS DSSS	2 Mbps
802.11a	5 GHz	OFDM	54 Mbps
802.11b	2.4 GHz	HR/DSSS	11 Mbps
802.11g	2.4 GHz	OFDM	54 Mbps
802.11n (Draft)	2.4 GHz or 5 GHz	OFDM/MIMO	540 Mbps

2.3 802.11 MAC Layer

The 802.11 MAC Layer works on any physical layer and controls the transmission of frames in the air as well as the interaction with the wired network. Access to the medium is provided through coordination functions. For contention-based access Distributed Coordination Function (DCF) and for contention-free access Point Coordination Function (PCF) is used. While PCF is used only in infrastructure networks, DCF can be used for both infrastructure and ad hoc modes.

802.11 is similar to Ethernet with some little exceptions. While Ethernet uses the Carrier Sense Multiple Access/Collision Detection (CSMA/CD) as the network contention protocol, 802.11 uses the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). Collision detection is not possible in 802.11 because of two reasons: one is the need for full duplex radios (transmitting and receiving simultaneously) which will increase the price; the other is that it is not possible for the stations to hear each other all the time. In order to deal with the collision problem a collision avoidance mechanism is established. To avoid collisions following steps are applied:

- To see whether the line is busy the station uses first the real and then the virtual carrier sensing. In the real one it listens to the medium for any activity and in the virtual one it uses the Network Allocation Vector (NAV) to calculate whether the medium is in use or not.

- If the medium is idle for an amount of time that is equal to or greater than Distributed Inter-Frame Space (DIFS) the station can begin to send.
- It initially sends a Request to Send (RTS) frame to the AP to allocate the channel indicating the time needed for the transmission of the data and ACK packets.
- When AP receives the RTS frame, it responds with a Clear to Send (CTS) frame after waiting for an amount of time that is equal to Short Inter-Frame Space (SIFS). The frame contains the duration field which indicates the time needed for the whole transaction.
- After receiving the CTS frame, the station sends the data packet after waiting for a SIFS.
- After receiving the data packet, AP sends an ACK frame after waiting for a SIFS.
- On the receipt of the ACK packet, the station understands that no collision occurred.

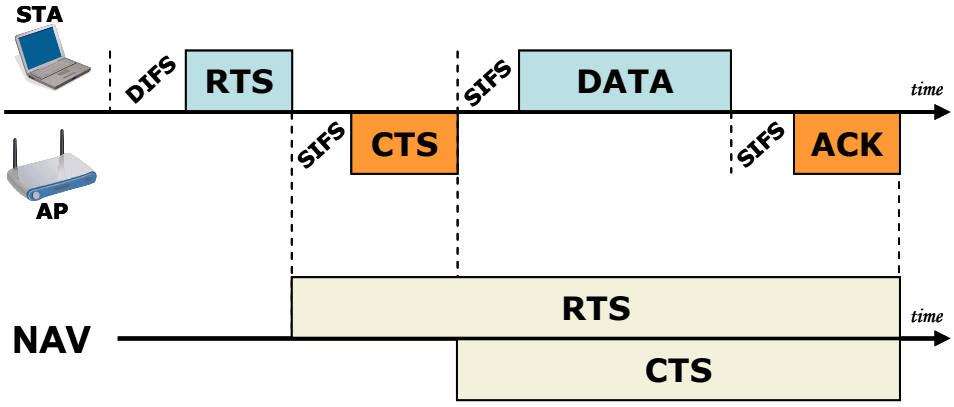


Figure 6. 802.11 CSMA/CA

The generic format of a MAC frame and description of the fields is shown below.

Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	FCS
2	2	6	6	6	2	6	0-2312	4

Figure 7.802.11 Generic MAC Frame

- **Frame Control** : Protocol, type, power management, WEP etc. control information.
- **Duration / ID** : Duration for data frames and ID for control frames.

- **Address 1** : Source address.
- **Address 2** : Address of the final destination.
- **Address 3** : Address of the wireless station that will process the frame.
- **Sequence Control** : Fragmentation and discarding duplicate frames.
- **Address 4** : Address of the wireless station that transmitted the frame.
- **Data** : Higher layer payload.
- **FCS** : Frame Check Sequence for error detection.

There are three general types of frames. Data Frames are used for carrying protocols and data from higher layers within the frame body. Control Frames, and Management Frames carry specific control and management information in the frame body. While Management Frames (Authentication, Association Request, Beacon, Probe Request etc.) enables stations to establish and maintain communications, Control Frames (RTS, CTS, ACK) are used to control access to the media.

2.4 802.11 Security

When 802.11 standard was initially introduced in 1997, it didn't comprise any security features and organizations that implement WLAN need to find out their own security solutions to protect their WLANs. In 1999, 802.11 task group developed Wired Equivalent Privacy (WEP) security mechanism which would provide authentication and privacy for the WLANs. When it is proved that WEP is not secure any more, in late 2002 the Wi-Fi Alliance developed and announced an intermediate security solution, which is called Wi-fi Protected Access (WPA), until 802.11i task group is done with the new 802.11i standard. WPA was a partial implementation of 802.11i and the full implementation was called WPA2. WPA2 was ratified by IEEE in 2004 and became mandatory by 1 March 2006.

2.4.1 WEP

WEP is designed to provide confidentiality, access control and data integrity. While confidentiality is achieved by using encryption, access control is achieved by means of an authentication mechanism requiring the usage of a shared key on both ends. CRC-32 checksum is used by receiver and the transmitter to assure the integrity of the transmitted data.

WEP uses RC4 (Rivest Cipher 4) algorithm for encryption. RC4 is well known and widely used stream cipher algorithm which also used in SSL (Secure Socket Layer). RC4 generates a long stream of pseudorandom bytes which is known as the Initialization Vector (IV). Then the IV is processed with the shared secret key through a function. The output of this function is the keystream. The last step is to XOR the plaintext with the keystream to produce the ciphertext. Original WEP standard is a 64-bit system in which he IV is 24 bit and shared key is 40 bit. Although the key length was insufficient at the beginning because of the export restrictions of the US government, 256-bit systems, with 24-bit IV and 232-bit shared key, are available currently.

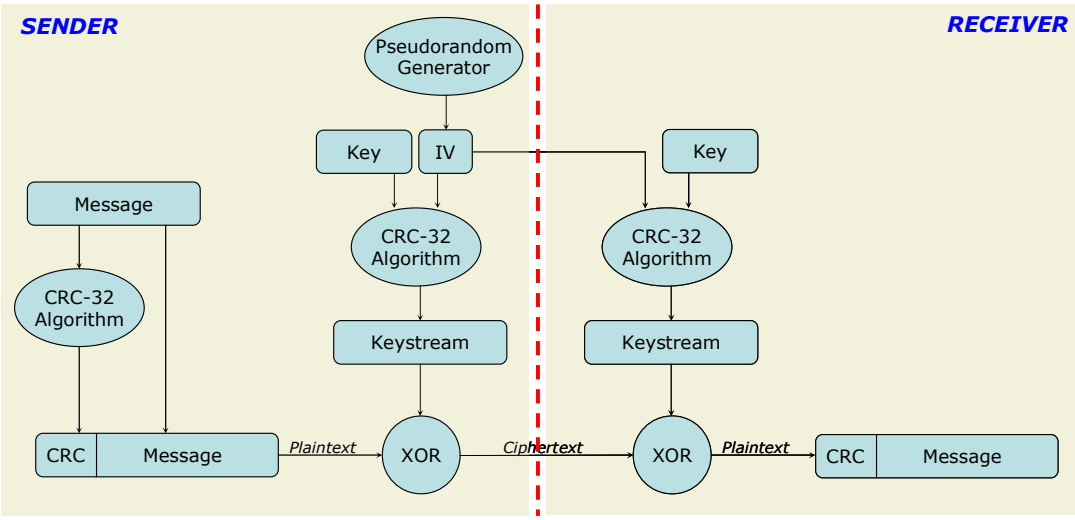


Figure 8. Overview of Encryption and Decryption with RC4

It is important to know that the IV is sent in an unencrypted form to the receiver. As soon as the receiver receives the message it produces the key stream using the IV attached to the message. After decrypting the ciphertext with the keystream it calculates the checksum and compares it with the checksum attached to the message.

Although it was initially designed to meet the security requirements of wireless users, in a few years WEP proved to be insufficient in providing security that is equivalent to wired networks as its name implies. While it provides some sort of security to stop casual sniffers, it takes only 15 minutes for an experienced hacker to crack the WEP keys in a busy network [1]. A number of security vulnerabilities are identified by some researchers [2-6] and these vulnerabilities can be summarized as follows:

• **Small key size:** Original WEP uses 40-bit keys which makes the protocol vulnerable to brute force attacks. Later the key size is increased to 104 bits to increase the resistance, which is known as WEP2. In fact, plenty of flaws in its whole design make WEP vulnerable at any key size [2].

• **Lack of key management:** WEP uses single and static shared key throughout the network. Key distribution is done manually and there is no lifetime for the keys. This makes it painful job for the system administrators to update the current keys with the new ones. At the same time using a key for a long period of time makes the attacker's job easier by giving him/her abundant data to analyze.

• **Poor authentication:** WEP provides two authentication mechanisms; open system authentication and shared key authentication. In open system authentication anyone who requests authentication is authenticated. In shared key authentication the initiator sends an authentication request and the responder replies with a challenge text. Upon receiving the challenge, the initiator encrypts it with the shared key and sends it back to the responder. The responder then decrypts this frame, validates its integrity, and compares the challenge text with the one it has sent already.

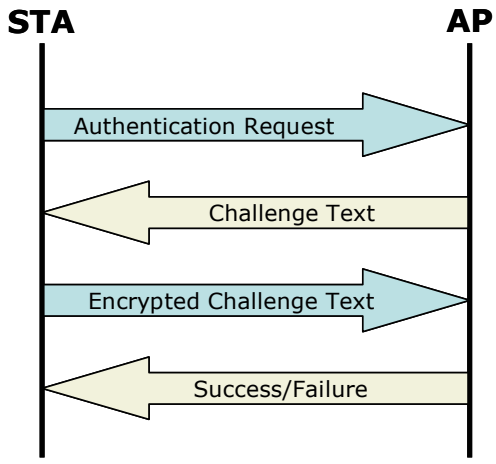


Figure 9. WEP Authentication

An attacker having the second and third frames can easily discover the shared key by XORing challenge text with the encrypted challenge text. This made the shared key authentication cause more harm than good and forced people use open authentication.

Another weakness of the WEP is that it doesn't provide mutual authentication. The stations are authenticated to APs but the APs are not authenticated to the stations which make the network open to rouge AP attacks.

- **Usage of CRC for integrity:** Since CRC is linear and lacks cryptography, by using a form of induction; a key dictionary can be generated by simply knowing enough specific plaintext [7].

- **Repetition of IV values:** As mentioned above, IV is used to derive the keystream by combining it with the shared secret key. 24 bits is allocated for IV which means 2^{24} different keystreams. Although it seems enough, on a busy network it is a matter of seconds to have frames with the same IV values. Knowing that;

$$C_1 \text{ XOR } C_2 = P_1 \text{ XOR } P_2$$

an attacker can decrease the number of possibilities and with some further analysis can even recover the plaintext and the key stream without knowing any of the plaintext in advance [2].

2.4.2 WPA

WPA is developed as a standards-based, interoperable, and interim security solution for WLANs until the 802.11i (or WPA2) standard is ratified. It has some improved security features which addresses all known security weakness of WEP. It is designed as a software upgrade and requires no additional hardware. It is also forward and backward compatible [8].

WPA uses 802.1x standard [9] with one of the Extensible Authentication Protocol (EAP) types [10] for authentication and Temporal Key Integrity Protocol (TKIP) for encryption. It also replaces CRC-32 with Message Integrity Check (MIC) for data integrity.

As mentioned above WPA uses 802.1x with one of the EAP types. 802.1x is a port-based network access mechanism which can be used by both wired and wireless networks. In 802.1x, port represents the association between station and AP. 802.1x defines three main components: supplicant, authenticator, and authentication server (AS). In wireless networks; supplicant is the wireless station, authenticator is the AP, and AS is a third party entity provides authentication service to the authenticator which typically uses Remote

Authentication Dial In User Service (RADIUS) or DIAMETER. RADIUS is an authentication, authorization, and accounting (AAA) protocol and DIAMETER is the successor of RADIUS.

The supplicant communicates with the AS via the authenticator. Between supplicant and the authenticator EAP over LAN (EAPOL) protocol is used for communication. AS uses "EAP over RADIUS" for its communication with the authenticator. Dual port mechanism is used within authenticators: controlled port and uncontrolled port. Uncontrolled port is used to pass EAP traffic between supplicants and AS. This port allows only EAP packets and filters the others. When the authentication process succeeds, authenticator opens the controlled port to let the supplicant access to the network.

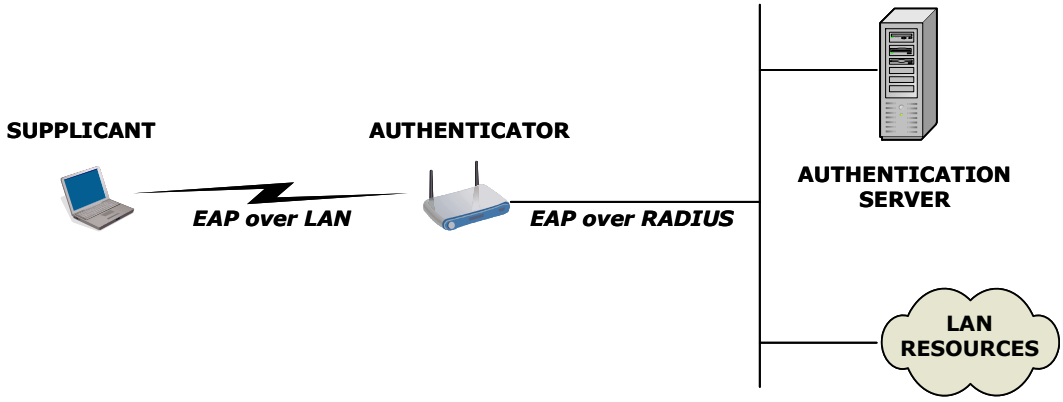


Figure 10. 802.1x Framework

Based on EAP, 802.1x can use different types of authentication mechanisms. Most common authentication methods are listed below:

- **EAP-MD5:** Uses one-way hash function. User only needs to type user name and password. It is considered to be more vulnerable than other authentication methods.

- **EAP-TLS (EAP-Transport Layer Security):** Based on TLS and requires both supplicant and AS have valid certificates. After negotiation phase, an encrypted TLS tunnel is established and used for the exchange of session keys.

- **EAP-TTLS (EAP Tunneled TLS):** An extension of EAP-TLS. Requires only AS possessing a valid certificate. User is required to enter user name and password. Since users are not needed to have a certificate it is more manageable than EAP-TLS.

• **PEAP (Protected EAP):** Almost identical to EAP-TTLS. PEAP can only use EAP protocols (e.g. EAP-MS-CHAP-V2), while EAP TTLS can use both EAP and non-EAP protocols (e.g. PAP, CHAP, EAP-MS-CHAP-V2).

In EAP, users can use digital certificates, user names and passwords, smart cards, secure IDs, tokens, or any other identity credentials suitable for them to authenticate themselves to the network. A typical message flow in 802.1x with EAP-TLS is shown in Figure 11.

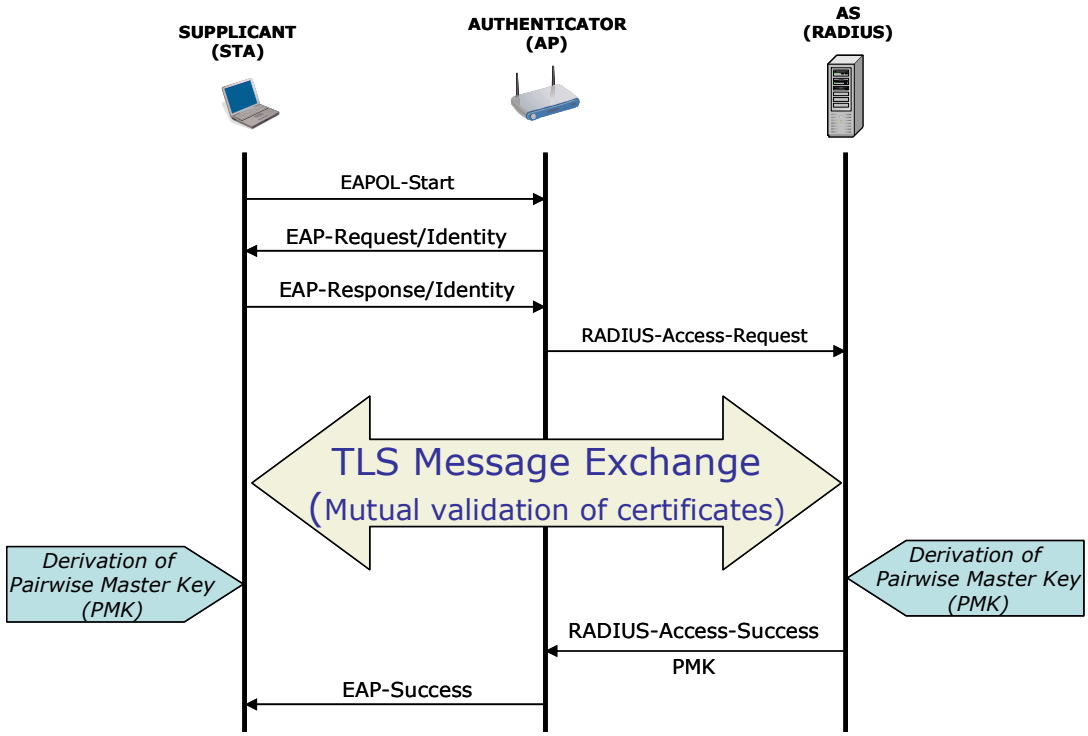


Figure 11. A typical 802.1x message flow with EAP-TLS

As mentioned above, WPA uses TKIP for message protection. Its primary objective is to provide solutions to the known vulnerabilities of WEP using the existing WLAN devices with software upgrades. Bound with this constraint, TKIP does not provide perfect solutions but can be a cure for the current insecure WLANs that are using WEP.

TKIP continues to use RC4 for encryption with some changes. While the key length is increased from 40 to 128 bits, the size of the IV is increased from 24 to 48 bits as well. It also replaces the usage of single static key with a dynamically generated and distributed key management mechanism. The key hierarchy used in TKIP provides approximately 500 trillion possible keys to be used on a single

data packet [8]. TKIP also includes message integrity code (MIC), known as Michael, to provide the integrity of the packets. Randomness is guaranteed by seeding the 8-byte MIC by the MIC key and TKIP Sequence Counter (TSC).

Creation of the temporal keys for encryption and integrity comes after PMK is derived by both STA and AS and is sent to AP by AS. Temporal keys are grouped in two ways: Pairwise Transient Key (PTK) and Group Temporal Key (GTK). PTK is used for unicast traffic and GTK is used for broadcast/multicast traffic. PTK is derived from PMK, nonce created by AP (ANonce), nonce created by STA (SNonce), MAC address of AP, and MAC address of STA. 512-bit long PTK comprises of Data Encryption Key (128 bits), Data Integrity Key (128 bits), EAPOL-Key Encryption Key (128 bits), and EAPOL-Key Integrity Key (128 bits). GTK is derived from Group Master Key (256-bit random number created by AP), Group nonce (GNonce), and MAC address of AP. 256-bit long GTK comprises of Group Encryption Key (128 bits) and Group Integrity Key (128 bits). Creation and distribution of the group keys are done through the secure channel created by pairwise keys between AP and STA. Key hierarchy established by TKIP is shown in Figure 12.

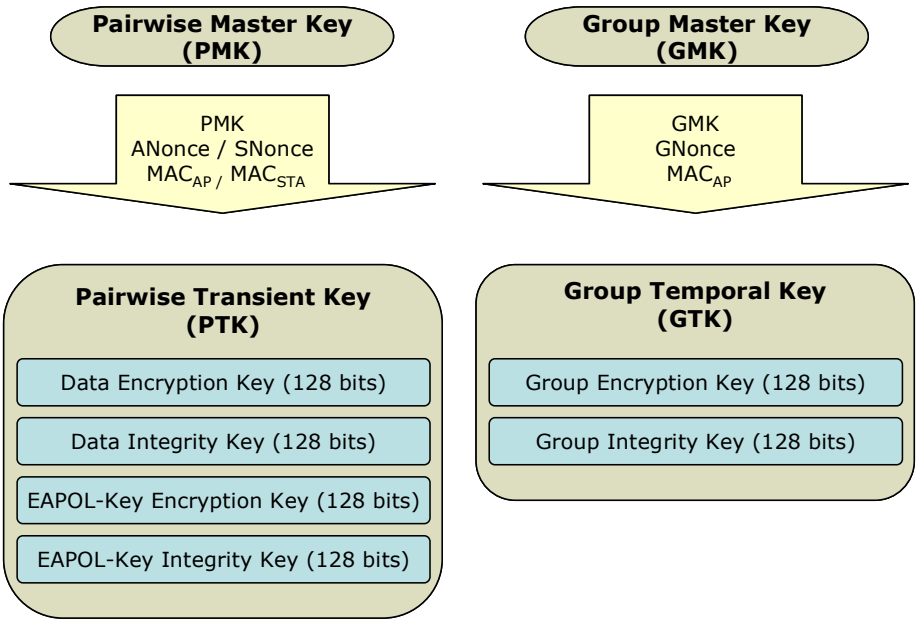


Figure 12. TKIP Key Hierarchy

Data Encryption Key is used for encrypting unicast frames, Data Integrity Key is used for calculating the MIC for unicast frames, EAPOL-Key Encryption Key is used for encrypting EAPOL-Key messages, EAPOL-Key Integrity Key is used for

calculating the MIC for EAPOL-Key messages, Group Encryption Key is used for encrypting broadcast/multicast frames, and finally Group Integrity Key is used for calculating the MIC for broadcast/multicast frames. The generation of the temporal keys relies on a number of message exchanges between AP and STA which is known as 4-way handshake (Figure 13). While group key handshake is used for GTK generation, GTK can also be generated during four-way handshake if needed (Figure 14). 4-way handshake and group key handshake are done using EAPOL-Key frames.

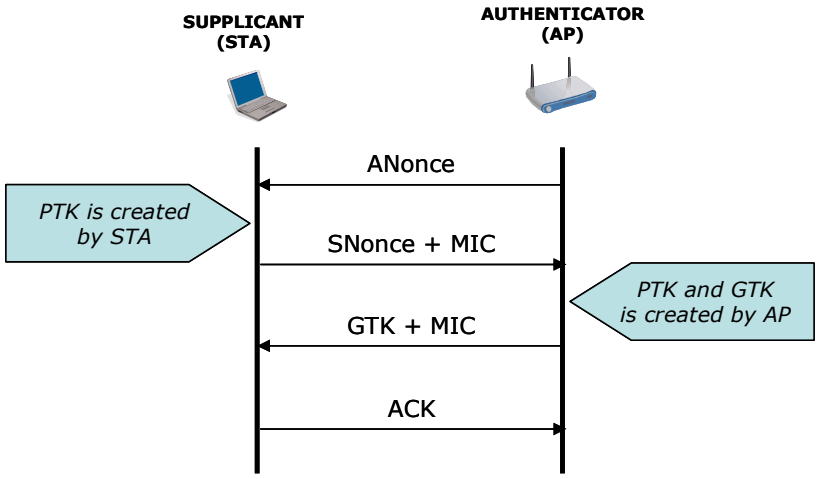


Figure 13. 4-Way Handshake

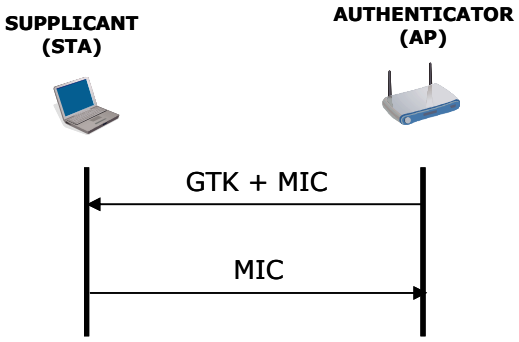


Figure 14. Group Key Handshake

As it is mentioned above, WPA was developed as an interim security solution until the ratification of the 802.11i standard. Keeping in mind that WPA was designed to operate on current WLAN devices with no hardware change, it can be said that although it is pretty much secure than WEP, it still have some weaknesses stemming from the constraints reflected to its design.

2.4.3 802.11i (WPA2)

Ratified in 24 June 2004, IEEE 802.11i standard [11] is designed to provide enhanced security to WLANs. It is backward and forward compatible which means it supports WEP, WPA, and WPA2. The aim of the standard is to define a robust security network (RSN) that allows only the creation of robust security network associations (RSNA) between the devices in compliance with the standard.

Two security frameworks are defined in the standard: RSN and pre-RSN. Networks that only allow RSNA are called RSN and networks that allow pre-RSNA are called pre-RSN. The main difference between RSNA and pre-RSNA is that in RSNA 4-way handshake is used in authentication/association phase. Since pre-RSN framework is for backward compatibility, RSN which provides enhanced security will be discussed in detail here.

Like WPA, 802.11i also uses 802.1x with one of the EAP types for authentication with an exception that in an RSN, usage of an EAP type that supports mutual authentication is compulsory. That is why EAP-MD5 cannot be used in an RSN. For key management an RSN depends on 802.1x and 4-way handshake which is described in 2.4.2. Key hierarchy is very similar to that of TKIP as shown in Figure 15. In 802.11i, the number of keys used is less than the number of keys used in TKIP because of the fact that the encryption protocol (AES-CCMP) used in 802.11i combines the encryption and integrity processes.

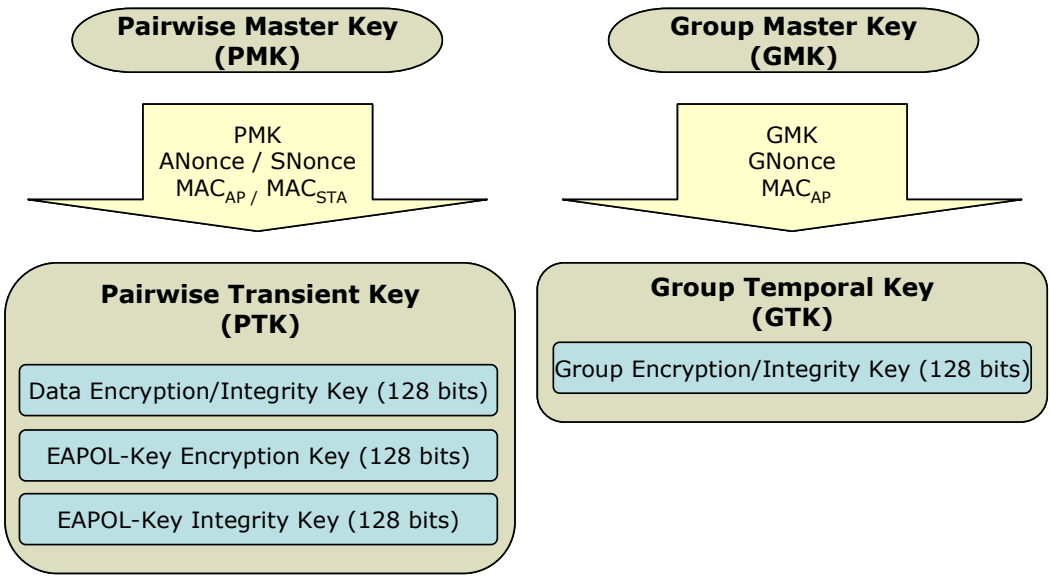


Figure 15. AES-CCMP Key Hierarchy

802.11i also offers a security solution for networks without an AS. This solution, which is potentially vulnerable to offline dictionary attacks [13], depends on the usage of pre-shared keys (PSK) and will not be discussed here.

802.11i supports three cryptographic algorithms: TKIP, Wireless Robust Authenticated Protocol (WRAP) and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). CCMP is mandatory in an RSN whereas TKIP and WRAP is included to the standard to provide support for pre-RSN equipment.

As it can be inferred from above, the major difference between WPA and 802.11i is the implementation of CCMP instead of TKIP as the encryption protocol. CCMP uses the Advanced Encryption Standard (AES) which is a very secure and fast symmetric encryption algorithm. It is also used by the US government. AES encrypts fixed 128-bit blocks using a key size of 128, 192 or 256 bits. AES-CCMP uses 128-bit keys on 128-bit data blocks.

As its name implies, CCMP is the combination of Counter mode (CTR) AES and Cipher Block Chaining Message Authentication Code Protocol (CBC-MAC). While CBC-MAC provides authentication and integrity, confidentiality is achieved using CTR mode AES. CCMP requires the usage of a fresh temporal key for every session and a 48-bit unique nonce value, which is called packet number (PN), for each packet encrypted with a given temporal key. The idea behind CBC-MAC is the creation of message integrity code (MIC) using block ciphers in CBC mode as shown in Figure 16.

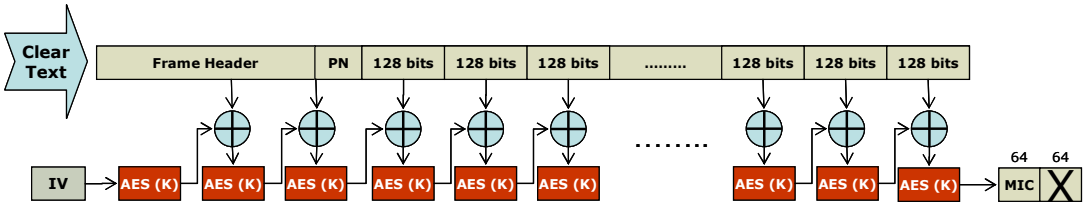


Figure 16. CBC-MAC

In counter mode AES, each 128-bit data block and the MIC is encrypted using AES algorithm which is fed with a random value (counter). Different counter values are used for each 128-bit block (Figure 17).

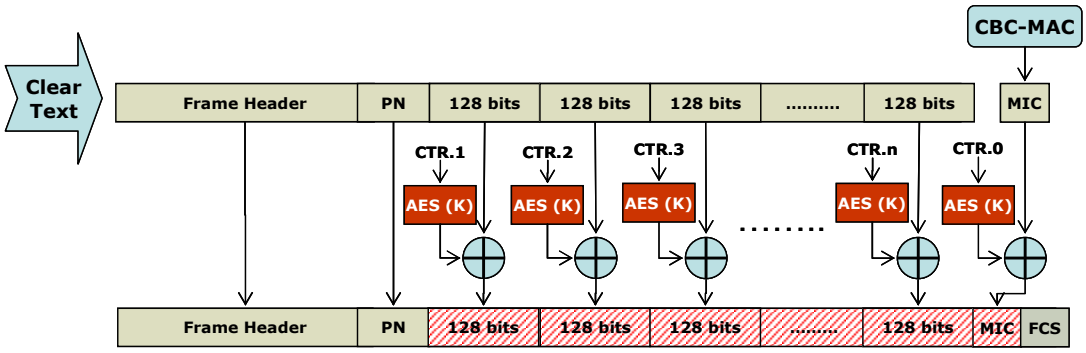


Figure 17. AES Counter Mode

802.11 MAC frame format, when CCMP encryption applied, is depicted in Figure 18.

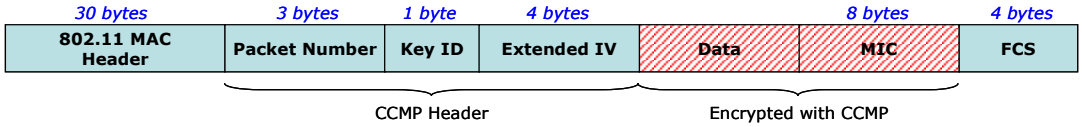


Figure 18. CCMP Encrypted 802.11 MAC Frame

IEEE 802.11i specifies an RSN information element (IE) that is used for the security parameters negotiation between communicating parties. It also helps to distinguish RSN and pre-RSN stations. While RSN capable stations include RSN IEs in various messages, pre-RSN stations do not use IEs. Figure 19 shows the RSN IE format. The size of the IE can be maximum 255 bytes.

Element ID	Length	Version	Group Cipher Suite	Pairwise Cipher Suite Count	Pairwise Cipher Suite List	Auth. & Key Mgmt. Suite Count	Auth. & Key Mgmt. Suite List	RSN Capabilities	PMK ID Count	PMK ID List
1	1	2	4	2	4m	2	4n	2	2	16s

m= Pairwise Cipher Suite Count n= Auth. & Key Mgmt. Suite Count s= PMK ID Count

Figure 19. RSN IE Format

RSNA establishment depends on the exchange of a number of messages which can be divided into six stages [12] to increase the comprehensibility (Figure 20).

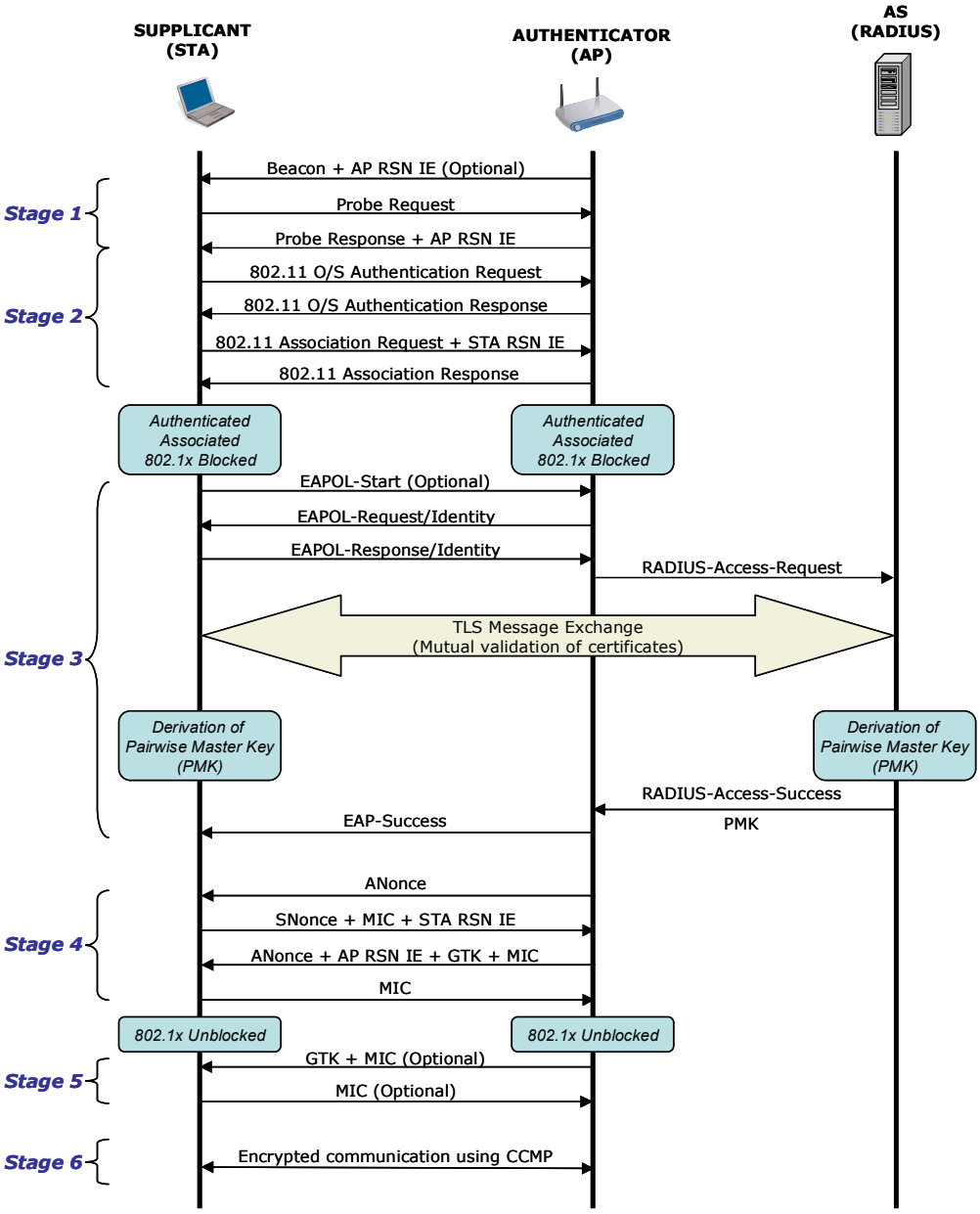


Figure 20. RSNA Establishment

• **Stage 1. Network and Security Capability Discovery:** This stage consists of Beacon, Probe Request, and Probe Response Frames. Authenticator announces its security capabilities by including RSN IE to Beacon or Probe Response Frames.

• **Stage 2. Authentication and Association:** This stage consists of 802.11 Authentication Request, 802.11 Authentication Response, 802.11 Association

Request, and 802.11 Association Response frames. Open system authentication is used here to provide backward compatibility. Controlled port on the authenticator is still closed and real authentication is done in the further steps using 802.1x protocol. Supplicant should announce its security capabilities to authenticator by including RSN IE to Association Request frame.

- **Stage 3. 802.1x Authentication:** In this stage authentication is done using 802.1x which is depicted in Figure 11.

- **Stage 4. 4-way Handshake:** This stage is a requirement for RSNA establishment. At the end of this stage authenticator and supplicant shares a fresh PTK (and maybe GTK) and controlled port is opened for data communication. 4-way Handshake is shown in Figure 13.

- **Stage 5. Group Key Handshake:** This stage is done to provide supplicants in the network with a GTK for broadcast/multicast traffic. Group Key Handshake is executed when the current GTK expires or a STA leaves the network.

- **Stage 6. Secure Data communication:** In this stage authenticator and supplicants communicate securely using PTKs or GTKs with the negotiated cipher suite which is CCMP for an RSN.

As discussed above 802.11i aims to provide a secure framework for WLANS which is called RSNs. RSNs are established through RSNAs between APs and STAs. 802.11i recommends RSN framework for maximum security. Furthermore RSN requires the usage of some specific protocols like CCMP for data encryption and integrity and 802.1x with one of the EAP types that provide mutual authentication for authentication and key management.

While providing effective authentication, key management, data confidentiality, and data integrity for WLAN communications, recent studies [12] show that 802.11i appears to be vulnerable to following DoS attacks even though RSNA is put into action:

- An adversary can disconnect a legitimate STA by forging and sending deauthentication and disassociation messages, which is called session hijacking.

- An adversary can prevent authentication by forging EAPOL-Start messages or spoof a STA by forging EAPOL-Success messages or disconnect a legitimate STA by forging EAPOL-Failure and EAPOL-Logoff messages.

- An adversary can repeatedly send Association Request messages to exhaust the EAP Identifier space which is only 8-bit long.

- An adversary can prevent 4-way handshake from being successful by modifying the RSN IE in the third message of the handshake and thus causing RSN IE confirmation fail, which is called RSN IE poisoning.

- An adversary can also perform 4-way handshake blocking attack by sending several first messages repeatedly and canceling all efforts done during authentication.

So far, 802.11i seems to be a promising solution for WLANs. Although individual protocols, like 802.1x, used in the standard are reported to have some weaknesses, it's important to understand that all the 802.11i pieces described above work together to form an overall security system. Taken individually and out of the context of the overall system, any single piece could be shown to have security weaknesses [14].

CHAPTER 3

OVERVIEW OF IEEE 802.16 STANDARD

IEEE 802.16 WMAN Standard, commercially named as WIMAX, is developed to provide wireless broadband services to mobile and stationary users. IEEE 802.16 is designed as an alternative to cabled access networks like Digital Subscriber Line (DSL) or Cable Broadband.

Beginning its studies in 1999, IEEE 802.16 working group published IEEE Standard 802.16 in 2001. 802.16 was for line of sight (LOS) applications utilizing 10-66 GHz spectrum. Published in 2002, 802.16a was an amendment to 802.16 addressing non-LOS applications utilizing 2-11 GHz. The working group completed the standard for fixed broadband wireless access (FBWA) and published 802.16-2004 (also known as 802.16d), which is a revision and replacement for 802.16 and 802.16a. The working group developed new enhancements that would provide mobile broadband wireless access (MBWA) with support to vehicular speeds up to 120 km/h and published 802.16e in December 2005. And finally, 802.16e and 802.16-2004 are combined in a single document, namely 802.16e-2005 [15], and published on 28 February 2006. General specifications of 802.16 standards are shown in Table 3.

Table 3. IEEE 802.16 Standards

Standard	**802-16**	**802.16a**	**802.16d**	**802.16e**
Range (km)	<8	<50	<50	<5
Bit Rate (Mbps)	<134	<75	<75	<15
Frequency (GHz)	10-66 Licensed	2-11 Licensed/Unlicensed	2-66 Licensed/Unlicensed	2-6 Licensed/Unlicensed
Environment	LOS	NLOS	NLOS	NLOS
Application	FBWA	FBWA	FBWA	FBWA/MBWA

IEEE 802.16 MAC layer consists of three sublayers: Service Specific Convergence Sublayer (MAC CS), MAC Sublayer Common Part (CPS), and Security Sublayer, whereas physical layer is composed of two sublayers: Transmission Convergence Sublayer (TCS) and Physical Medium Dependent (PMD) Sublayer (Figure 21).

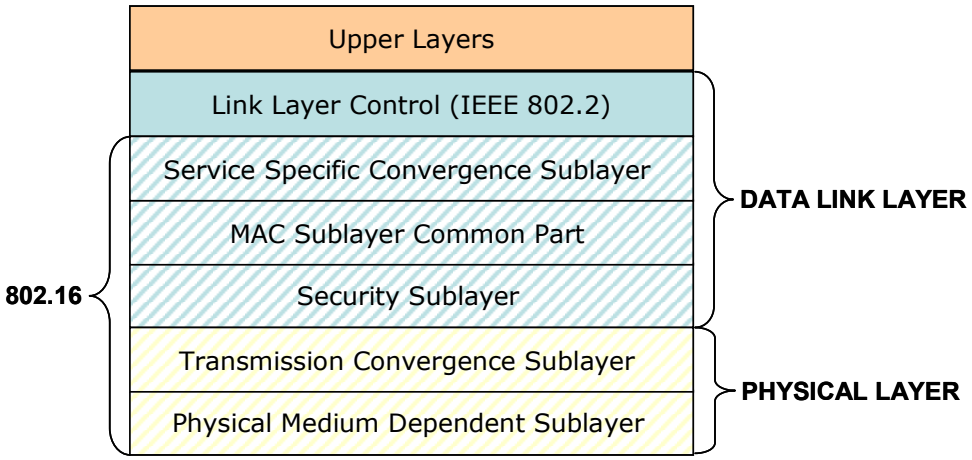


Figure 21. IEEE 802.16 Protocol Stack

MAC CS has two types: one is ATM convergence sublayer for ATM networks and the other is packet convergence sublayer for packet data services (Ethernet, PPP, IP etc.). The basic purpose of MAC CS is classifying upper-layer data as ATM cell or packet and passing it to MAC CPS. MAC CPS is the core of the 802.16 MAC layer. MAC CPS is responsible for key MAC functions like addressing, service definitions, service requests, and service access grants. Security sublayer is accountable for authentication, key management, encryption, and decryption. TCS performs the transformation of variable length MAC Protocol Data Units (PDU) into fixed length blocks. PMD sublayer is accountable for transmitting and receiving the data via wireless medium.

3.1 802.16 Network Architecture

IEEE 802.16 network architecture is similar to the architectural model of cellular networks. Each 802.16 coverage area or cell consists of one base station (BS) and one or more subscriber stations (SS). BS provides SSs with connectivity to the core network. SS is the equipment on the customer or end-user site, which is also known as customer premises equipment (CPE), providing end-users access to the broadband wireless network. A single 802.16 cell is depicted in Figure 22.

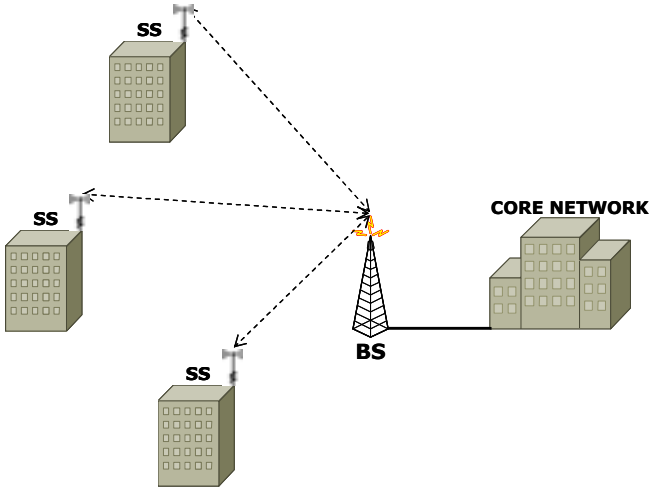


Figure 22. A Single 802.16 Cell

IEEE 802.16 supports both star (Figure 22) and mesh (Figure 23) topology. While SSs communicate only with BS in star topology, mesh topology gives the SSs the capability to communicate among each other.

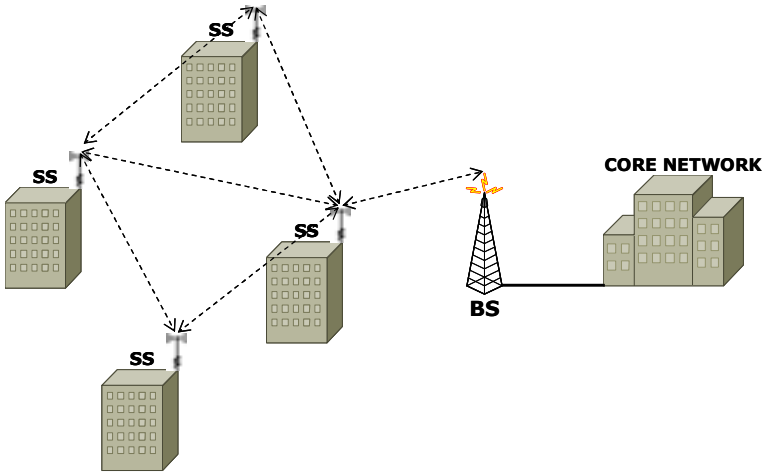


Figure 23. 802.16 Mesh Topology

802.16 makes it available to establish a backbone by using a number of base stations. These backbones might be connected to 802.11 or any other wired network via SSs. On the other hand subscribers with mobile devices such as laptops or personal digital assistants (PDA) can directly connect to a BS to access to the broadband wireless network.

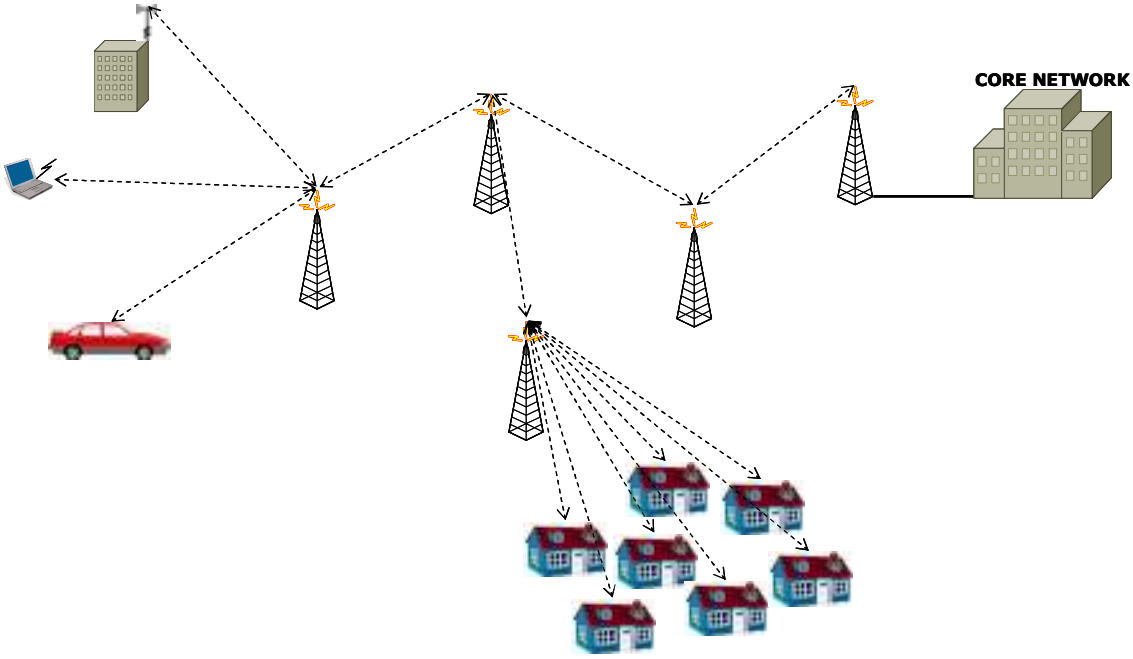


Figure 24. 802.16 Applications

3.2 802.16 Physical Layer

For the frequency bands in the 10-66 GHz range, 802.16 defines one air interface with a single-carrier modulation, which is called WirelessMAN-SC. For the frequency bands in the 2-11 GHz range, three air interfaces are defined: WirelessMAN-SCa, WirelessMAN-OFDM, and WirelessMAN OFDMA. Physical layer specifications of IEEE 802.16 are summarized in Table 4.

Table 4. 802.16 Physical Layer Specifications

AIR INTERFACE	FREQ.	LOS/NLOS	DUPLEXING	SUBCARRIERS	MODULATION
WirelessMAN-SC	10-66 GHz	LOS	TDD FDD	Single	QAM 16-QAM 64-QAM
WirelessMAN-SCa	2-11 GHz	NLOS		Single	
WirelessMAN-OFDM	2-11 GHz	NLOS		256	
WirelessMAN OFDMA	2-11 GHz	NLOS		2048	

WirelessMAN-SC is designed to operate in the 10-66 GHz frequency band for NLOS communications. WirelessMAN-SCa is also based on single-carrier technology and designed for NLOS operation in frequency bands below 11 GHz. WirelessMAN-OFDM uses OFDM with 256 subcarriers. WirelessMAN OFDMA uses OFDM with 2048 subcarriers and subcarriers can be organized into logical subchannels.

IEEE 802.16 supports two types of transmission duplexing: Time Division Duplexing (TDD) or Frequency Division Duplexing (FDD). In TDD, uplink (UL) and downlink (DL) shares the same frequency using different time slots, whereas in FDD, UL and DL can make transmissions simultaneously on different frequencies.

IEEE 802.16 uses dynamic adaptive modulation which means that it adjusts modulation depending on the Signal Noise Ratio (SNR). Three modulation schemes are available: Quadrature Phase-Shift Keying (QPSK) QPSK, 16-Quadrate Amplitude Modulation (16-QAM), or 64-QAM (Figure 25).

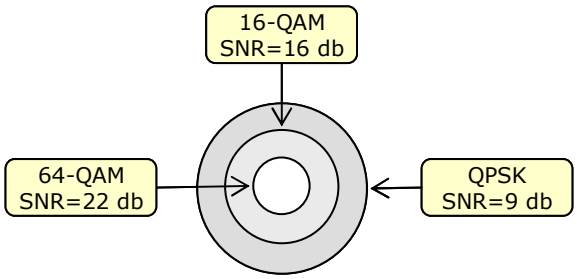


Figure 25. Dynamic Adaptive Modulation

3.3 802.16 MAC Layer

8021.6 MAC layer is designed for both point to multipoint and mesh connections. 802.16 uses a connection oriented method and supports quality of service (QoS). Unlike 802.11, 802.16 uses uplink and downlink maps to guarantee collision free communications. SS uses TDMA to share the uplink, while BS uses TDM. As it is mentioned above 802.16 MAC layer consists of three parts:

- MAC CS: Accepts, classifies, and processes higher layer PDUs and delivers them to the appropriate MAC service access point (SAP). There are two types of MAC CS specifications: ATM CS and packet CS. While ATM CS is an interface between different ATM services and MAC CPS SAP, packet CS constitutes interface between packet-based protocols (e.g. PPP, Ethernet) and MAC CPS SAP. ATM CS PDU format is shown in Figure 26.

ATM CS PDU Header				**ATM CS PDU Payload**
PTI (3 bits)	CLP (1 bit)	Reserved (4 bits)	VCI (16 bits)	ATM Cell Payload (48 bytes)

Figure 26. ATM CS PDU Format

• MAC CPS: Implements actual medium access functions such as; connection management, bandwidth distribution, request, and grant, uplink scheduling, and system access procedure. Each SS has a 48-bit MAC address as an equipment identifier. There are two types of connections: management and transport. And management connections may be of three types: Basic (short time-critical MAC and radio link control messages), Primary (longer, delay tolerant authentication and connection setup messages), and Secondary (standards-based management messages like DHCP, TFTP, and SNMP). A 16-bit connection identifier (CID) is used to reference connections for each direction. An SS can have several connections for different purposes. Transport connections are established when required. They are used for unicast or multicast user traffic.

• Security Sublayer: This layer will be handled in detail in the next section.

MAC PDU consists of three parts: fixed-length header, variable-length payload, and an optional CRC field. Headers can be of two types: generic and bandwidth request. While bandwidth request PDUs do not contain payload, others contain either management messages or MAC CS PDU in their payload field. MAC PDU format is depicted in Figure 27.

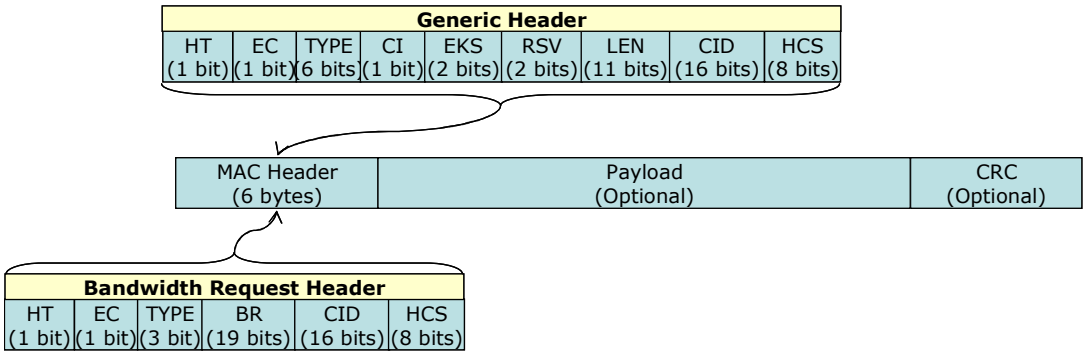


Figure 27. 802.16 MAC PDU Format

An SS must succeed the network entry procedure for initialization. This procedure is divided into following phases:

- SS scans for DL channel and establishes synchronization with BS.
- SS obtains DL and UL parameters.
- SS performs initial ranging to acquire correct timing and power adjustments and establishes primary management channel with BS.

- BS and SS negotiate on basic capabilities.
- BS and SS perform authorization and key exchange.
- BS requests for registration and acquires secondary management CID.
- SS invokes DHCP and gets necessary information required for IP connectivity using its secondary management connection.
- SS requests time of day from BS to have the current date and time.
- SS downloads operational parameters (configuration file) using TFTP on its secondary management connection.
- BS an SS setup connections.

3.4 802.16 Security

As it is stated above, 802.16 handles security issues by means of the security sublayer at the bottom of the MAC layer. 802.16 intends to provide authentication, key management, and confidentiality to the data link via this sublayer. Security sublayer consists of two component protocols:

- Encapsulation protocol: This protocol defines a set of cryptographic suites and the rules of applying these suites to the MAC PDU payload during authentication and encryption.
- Key management protocol: This protocol provides secure distribution of keying material. Default protocol used here is the Privacy Key Management (PKM) protocol.

Security state of a connection is maintained by security associations (SA). There are two types of SAs: SA for unicast connections and group SA (GSA) for multicast groups. SAs are identified by SAIDs and comprises of the following elements:

- 16-bit SAID,
- 128-bit key encryption key (KEK),
- 128 bit TEKs; TEK_0 and TEK_1,
- TEK lifetimes,
- 32-bit packet numbers (PN); PN_0 and PN_1,
- 32 bit receive sequence counters; $RxPN_0$ and $RxPn_1$.

And the contents of GSA are:

- Group key encryption key (GKEK),
- Group traffic encryption key (GTEK).

Every SS must establish at least one SA during initialization. Each connection, except primary and secondary management connections, must be mapped to SA.

3.4.1 Authentication and Key Management

Although PKMV1 was the key management protocol for 802.16, 802.16e supports PKMv2, which has more enhanced security features like a new key hierarchy, as well. PKMv2 supports both mutual and unilateral authentication. It uses either EAP or X.509 digital certificates together with RSA public key encryption algorithm for authentication.

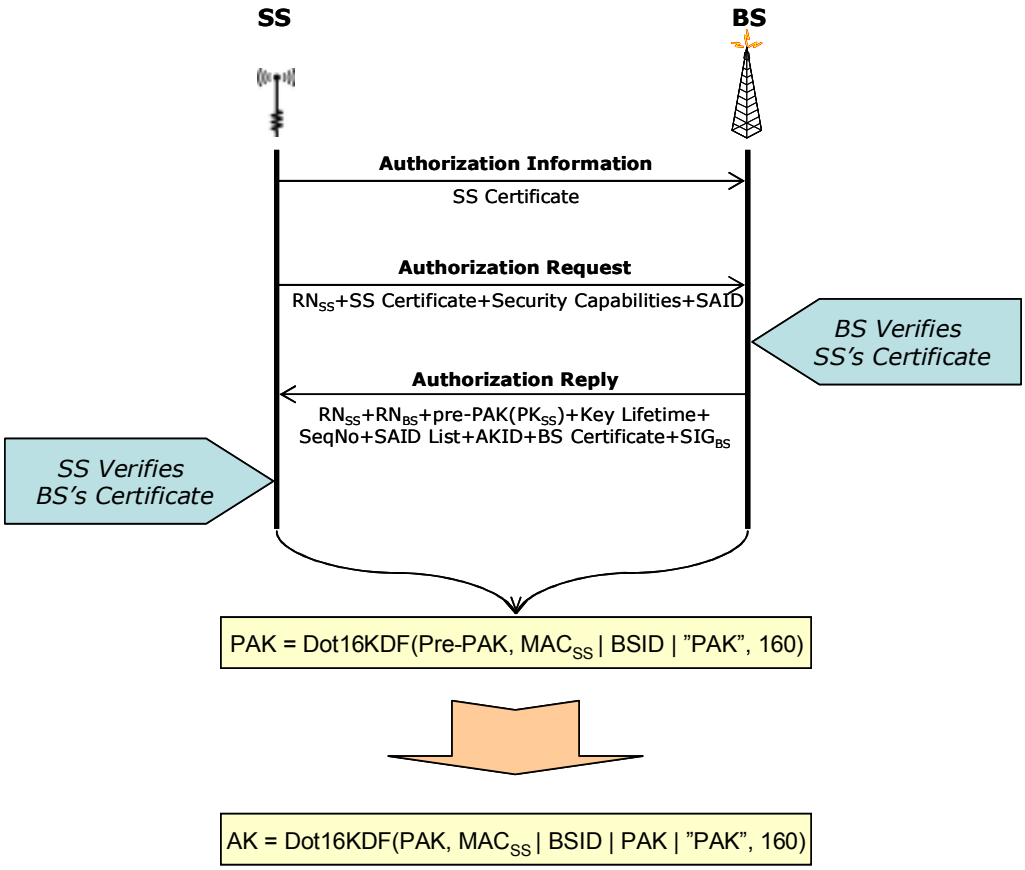


Figure 28. PKMv2 RSA Based Authorization

At the end of the authentication process 160-bit primary authorization key (PAK) (from RSA based authorization) or 160-bit PMK (from EAP based authorization) is established between BS and SS. A 160-bit shared secret key, namely authorization key (AK), is derived using PAK or PMK. AK is then used for the encryption of the subsequent PKM messages of 128-bit traffic encryption keys (TEK). All key derivations are done using Dot16KDF algorithm. RSA based authorization is depicted in Figure 28 and EAP based authorization is depicted in Figure 29.

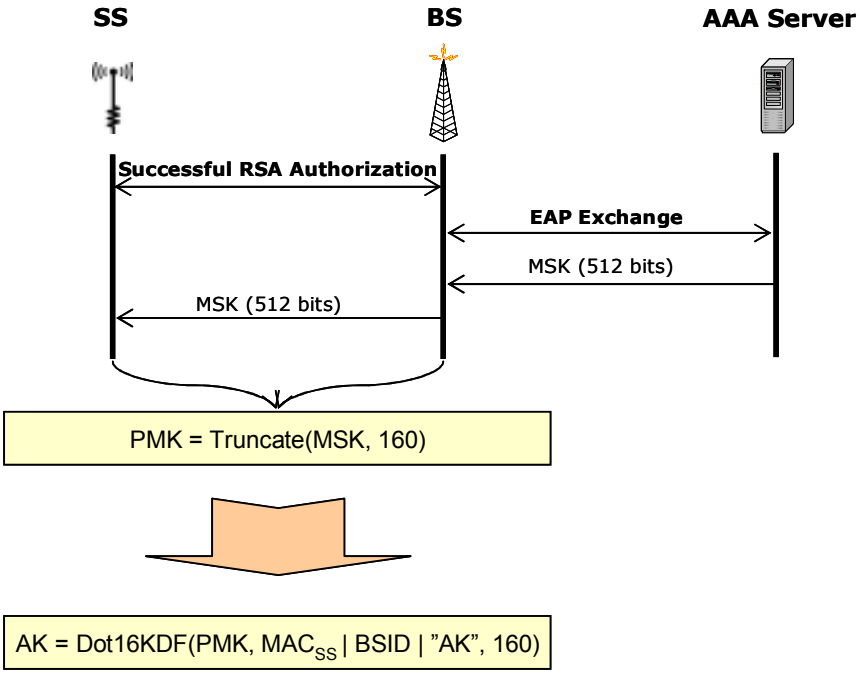


Figure 29. PKMv2 EAP Authorization

Additionally following keys are derived and used by 802.16:

- Key Encryption Key (KEK): Derived directly from AK and used to encrypt TEKs, GKEK, and all other keys sent from BS to SS in unicast message.
- Group Key Encryption Key (GKEK): Randomly generated by BS and used to encrypt GTEKs.
- Traffic Encryption Key (TEK): Randomly generated by BS and used for data encryption.
- Group Traffic Encryption Key (GTEK): Randomly generated by BS and used to encrypt multicast data packets.

- Message Authentication Keys (HMAC/CMAC): Derived from AK and used to sign management messages to validate the authenticity of these messages.

3.4.2 Data Encryption

Data encryption is applied on MAC PDU payload. A number of cryptographic methods can be used for encryption: DES in CBC mode, AES in CCM mode, AES in CTR mode, and AES in CBC mode. These methods use TEK and IV in the related SA to feed the encryption algorithm. Overview of 802.16 encryption process is depicted in Figure 30.

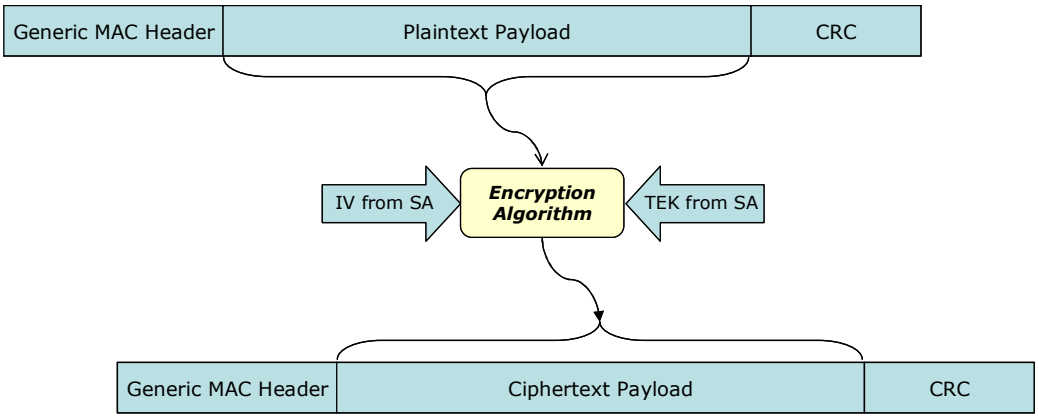


Figure 30. 802.16 Encryption Process

SS shall maintain two TEKs with overlapping lifetimes. Once the lifetime of the old TEK expires, SS shifts to the new TEK and sends a TEK request to BS. BS replies this request with a new TEK encrypted with the KEK as shown in Figure 31.

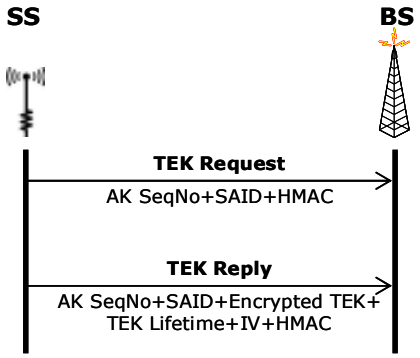


Figure 31. 802.16 Data Key Exchange

In 802.16, security sublayer is above physical layer, thus 802.16 networks are vulnerable to physical layer attacks like jamming and scrambling. Before 802.16e, the standard had security flaws in key management, authentication, and data encryption. But with the introduction of 802.16e, most of the vulnerabilities of the standard are resolved.

The most important enhancement done in 802.16e is the addition of PKMv2 to the standard. Authentication and key management problems arising from PKMv1 are solved in PKMv2. Mutual authentication requirement is fulfilled by giving BS a certificate and make it authenticate itself to SS. In addition to RSA, EAP, which extends the authentication to an AAA server, is added to the standard. There are a number of ways to be used for authentication such as RSA, RSA+EAP, EAP, and EAPinEAP. It is operator's choice to select one of the EAP types (i.e. EAP-TLS, EAP-TTLS, PEAP, and EAP-SIM). EAP can use different types of credentials such as X.509 digital certificate for EAP-TLS or Subscriber Identity Module for EAP-SIM. While addition of nonces to the authentication messages provides a protection against replay attacks, mutual authentication solves the man-in-the-middle-attack and rouge BS problems.

Weakness of the DES-CBC encryption used in the previous versions of the standard is solved by including AES to the standard. While it is still possible to use DES in CBC mode, 802.16e supports AES-CCM, AES-CTR, and AES-CBC. Correct use of AES-CCM addresses the most fundamental deficiency in the original data protection scheme-the lack of a data authenticity mechanism [16].

Although 802.16e introduces powerful solutions to the security weaknesses of previous versions, some of the security flaws appear not to be addressed. Critical threats are eavesdropping of management messages, BS or MS masquerading (if mutual authentication is not used), management message modification, and DoS attack [17]. It must be also kept in mind that 802.16e is a new standard and requires extensive further research to come to a complete and correct decision about its secureness.

CHAPTER 4

SECURE WIRELESS NETWORK ARCHITECTURE PROPOSAL

The architecture that will be proposed in this thesis will be for wireless networks in infrastructure mode. Ad hoc networks are out of the scope of this thesis. And also mobility will not be covered for 802.11 and 802.16 parts of the network. 802.11 will serve as wireless client's service access point, while 802.16 will be used as a backhaul for 802.11 hotspots. In other words, wireless clients or STAs will access to the DS of that organization by means of both WLAN and WMAN. A typical topology is provided in Figure 32.

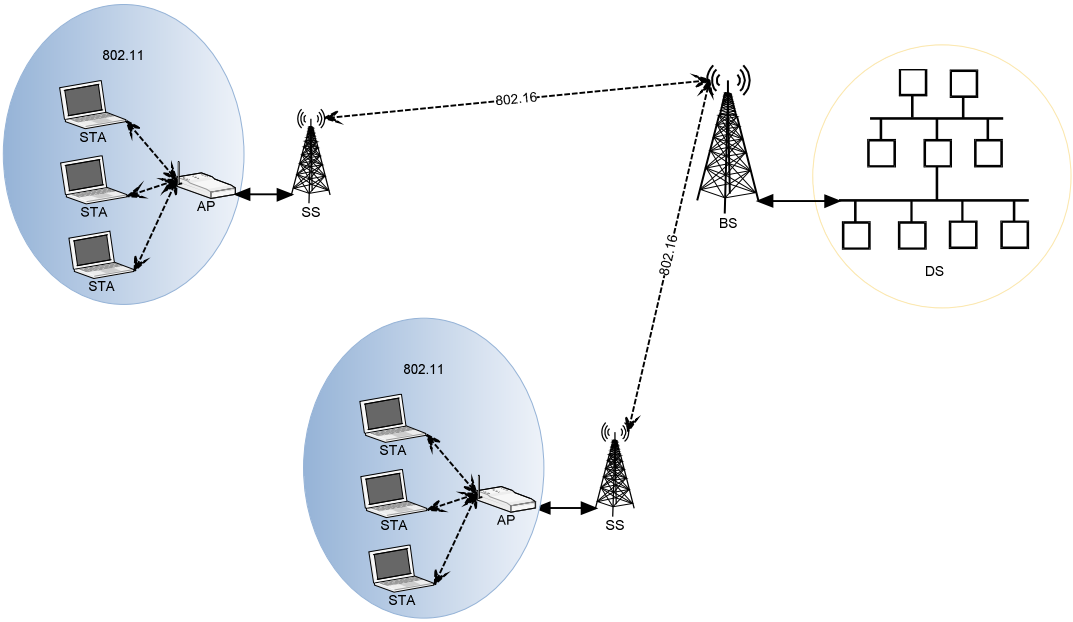


Figure 32. Typical Network Topology with 802.11 and 802.16

It can be inferred from previous chapters that wireless networks are extremely prone to security attacks. Therefore, when trying to establish a secure wireless network, all the available security technologies providing strongest measures should be observed closely and implemented in a swift manner.

Since 802.11 and 802.16 will be integrated to establish the wireless part of the network, it is important to contemplate security features of each together. In view of previous sections, both standards have similar security components like X.509 digital certificates, EAP, and AES. These features should thoroughly be investigated and redundancy should be prevented, giving attention to the level of the security provided, to increase performance and decrease complexity.

4.1 Rationale for a New Security Architecture

If RSN security framework is adopted for the WLAN part of the network, there will be two possible approaches as shown in Figure 33 and Figure 34: one is using a single authentication server behind 802.16 base station or separate authentication servers for each WLAN segment between the AP and the SS.

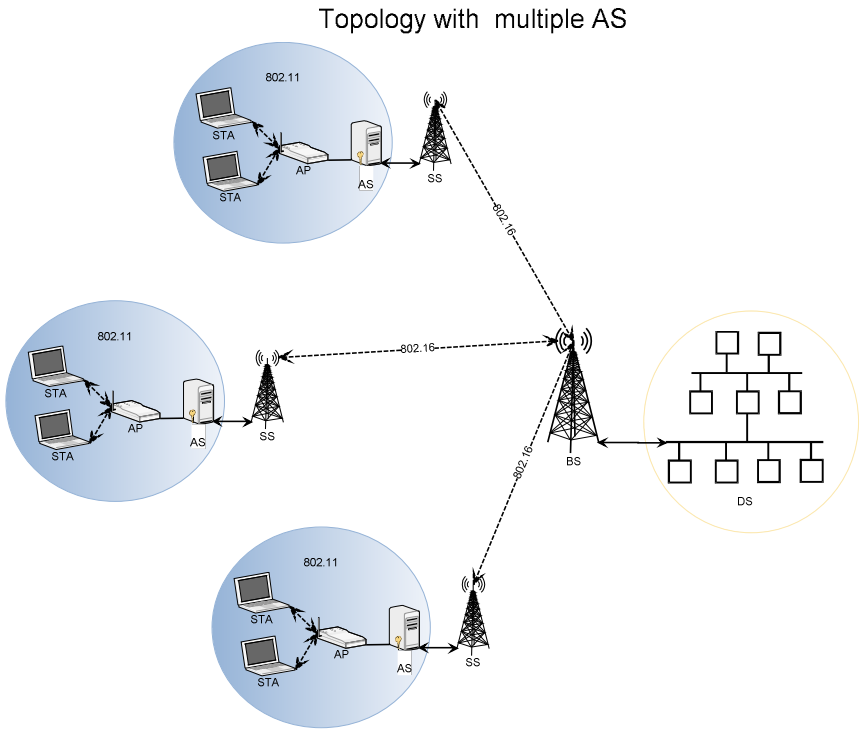


Figure 33. Network Topology Option with Multiple AS

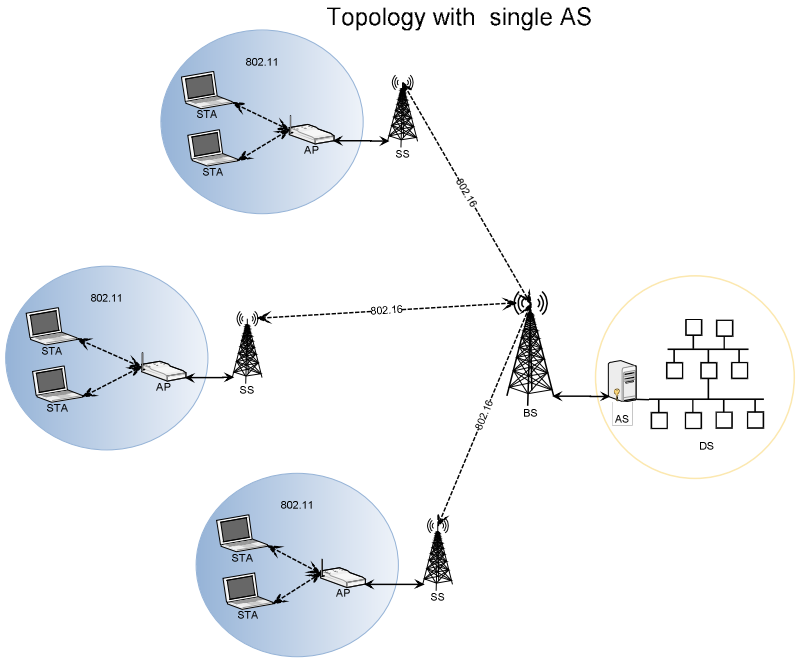


Figure 34. Network Topology Option with Single AS

Using multiple authentication servers will not only increase the equipment cost, but also complicate the manageability of the network. This situation will put a burden on network administrators by making them deal with several servers which can also increase the rate of management and configuration flaws.

On the other hand, using a single authentication server will put an extra load on the WMAN part of the network. Assuming that RADIUS is used as the authentication server, RADIUS messages will be sent to the RADIUS server encapsulated in UDP segments. Typical UDP segment for RADIUS communication is shown in Figure 35.

				RADIUS							
802.16 MAC	**LLC (SNAP)**	**IP**	**UDP**	**Code**	**ID**	**Legth**	**Authenticator**	**Attributes**			**CRC**
								Attribute	**Length**	**Value**	
6	8	20	8	1	1	2	16	1	1	0-253	4

Figure 35. UDP Segment Carrying RADIUS Data

As it is mentioned before, RSNs introduced by 802.11i make the usage of an EAP type providing mutual authentication compulsory. If we assume that EAP-TLS is used with RADIUS, message exchange between a wireless client and the authentication server will be as depicted in Figure 36.

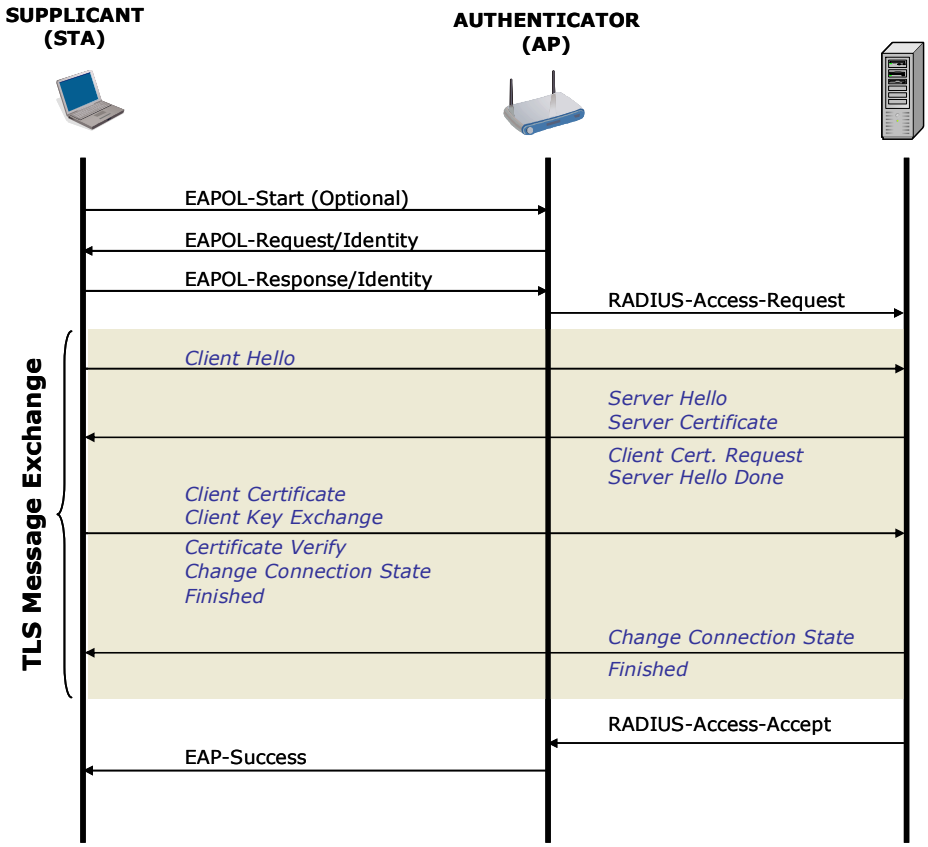


Figure 36. STA-AS Message Exchange with EAP-TLS

As it is shown in Chapter 5 (Table 11), the total load on WMAN part of the network due to RADIUS traffic is calculated as 3049 bytes. Following figure shows the graph of the authentication load on 802.16 portion of the network based on number of STAs.

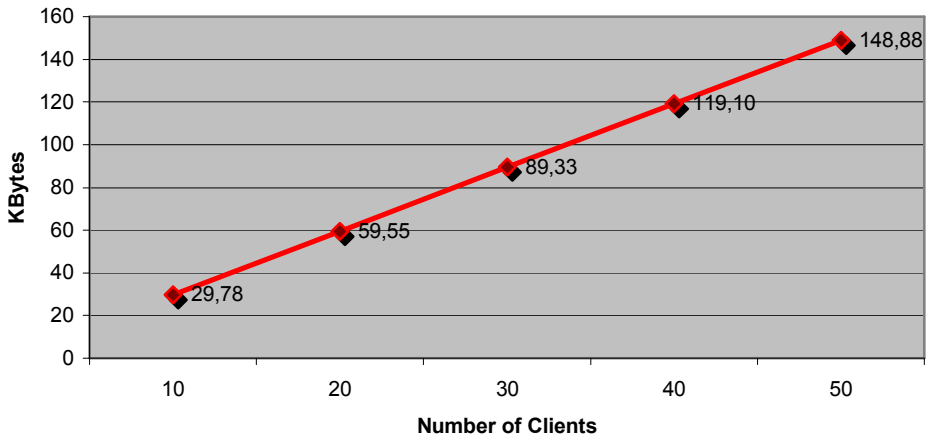


Figure 37. Authentication Load vs. Number of Clients on WMAN

Besides its additional load to the network, using a central AS will also increase the authentication time of the clients. In addition to the AP, UDP segments will be processed by both SS and BS. If we assume that SS is connected to the BS with 10 Mbps, BS is connected to the AS via 100 Mbps Ethernet, distance between SS and BS is 10 km., and distance between BS and AS is 100 m., additional authentication delay stemming from WMAN, neglecting the nodal processing delays, will be as follows:

$$Delay_{total} = Delay_{prop} + Delay_{trans}$$

$$Delay_{prop} = ((100\ m : 2x10^{8}\ m/sec) + (10.000\ m : 3x10^{8}\ m/sec))*6 = 201x10^{-6}\ sec$$

$$Delay_{trans} = (3049x8\ bit : 10^{6}\ bit/sec) + (3049x8\ bit : 10^{8}\ bit/sec) = 24635{,}92x10^{-6}\ sec$$

$$Delay_{total} = 201x10^{-6} + 12095{,}76x10^{-6} = 24836{,}92x10^{-6}\ sec = 24{,}84\ msec$$

Since 802.16 is connection oriented medium access delay is not included to the calculation. Consequently, RADIUS traffic on WMAN will add an additional 24,84 milliseconds to the total authentication time. It must be kept in mind that this value increases as the bit rates decrease and distance between devices increase.

4.2 New Security Architecture

In the security architecture that will be proposed here, mutual authentication between STA and AP and between SS and BS is provided by means of RSA based authentication. It requires the usage of X.509 digital certificates on STA, AP, SS, and BS, as well as a certificate authority (CA) server located behind BS. It is also required that their own and CA's digital certificates be installed on STA, AP, SS, and BS before being put into service. Digital certificates contain both public key and MAC address of that specific device. Renewal of the certificates will be handled by client devices and CA in the way as defined in 4.2.3. An overview of the new security architecture is depicted in Figure 38.

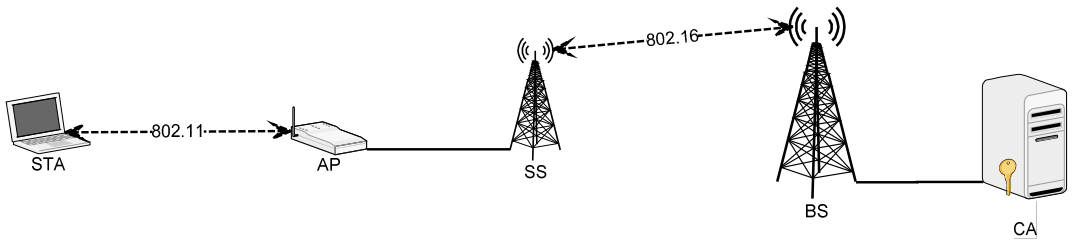


Figure 38. Overview of the New Security Architecture

4.2.1 WLAN Architecture

802.11i is used for the WLAN part of the network with some changes in the authentication scheme. In other words, a revised version of 802.1x will be used or it can be considered as an extension to the 802.1x protocol. AP and STA will authenticate each other using RSA protocol similar to 802.16e. RSA protocol uses X.509 digital certificates [18] and public key encryption algorithm [19] with SHA-1 hash algorithm. At the end of the authentication PMK is created using a cryptographically secure pseudo-random number generator (PRNG) by AP and sent to STA to be used for the derivation of PTK. And the rest of the security functions are same as that of 802.11i.

The authentication phase begins after 802.11's open system authentication and association phase. At this phase, controlled port is closed to the STA. STA and AP communicate using the uncontrolled port. Whenever authentication phase ends with success, AP opens the controlled port and STA communicates with the rest of the network using this port.

The communication between STA and AP is done via EAPOL frames as in 802.11i. The format of EAPOL frame is provided in Table 5.

Table 5. EAPOL Frame Format

FIELD	OCTET NUMBER
PAE Ethernet Type	1-2
Protocol Version	3
Packet Type	4
Packet Body Length	5-6
Packet Body	7-N

PAE Ethernet Type Entity field consists of Ethernet Type value assigned for use by the Port Access Entity (PAE). Protocol Version field identifies the version of the EAPOL protocol that is used. Packet Type field determines the type of the packet being transmitted and can take one of the following five values:

- EAP-Packet
- EAPOL-Start
- EAPOL-Logoff
- EAPOL-Key
- EAPOL-Encapsulated-ASF-Alert

Packet Body Length indicates the length of the Packet Body field in octets. And finally, Packet Body field contains a value if the type is EAP-Packet, EAPOL-Key, or EAPOL-Encapsulated-ASF-Alert.

In 802.1x, the authenticator PAE is responsible for relaying EAP frames between STA and AS. It relays only the EAPOL frames whose Packet Type fields have a value, explicitly all zeros, which correspond to EAP-packet. This means that any EAPOL frame with Packet Type value different from zero is not relayed to the AS and handled by the AP itself. Since no AS will be used in this proposal, a new Packet Type value, namely RSA-Packet, should be added to the standard to handle RSA-based authentication. When AP receives an EAPOL frame having this Packet Type value, it will not try to relay this frame to AS and will start the RSA based authentication procedure.

In RSA-based authentication, RSA packet has the same packet format of EAP packet shown in Table 6. The only difference is the ingredient of the data field.

Table 6. RSA Packet Format

FIELD NAME	OCTET NUMBER
Code	1
Identifier	2
Length	3-4
Data	5-N

Code field can take following values:

- Request
- Response
- Success
- Failure

Identifier field is for matching requests with responses. Length field indicates the length of code, identifier, length, and data fields in octets. And finally, data field consists of authentication related data and ingredients of it differ according to the type of the packet.

As in 802.1x, authentication starts with EAPOL-Start frame and STA can terminate the authenticated state by sending EAPOL-Logoff frame. Message flow during RSA authentication according to the proposed architecture is depicted in Figure 39.

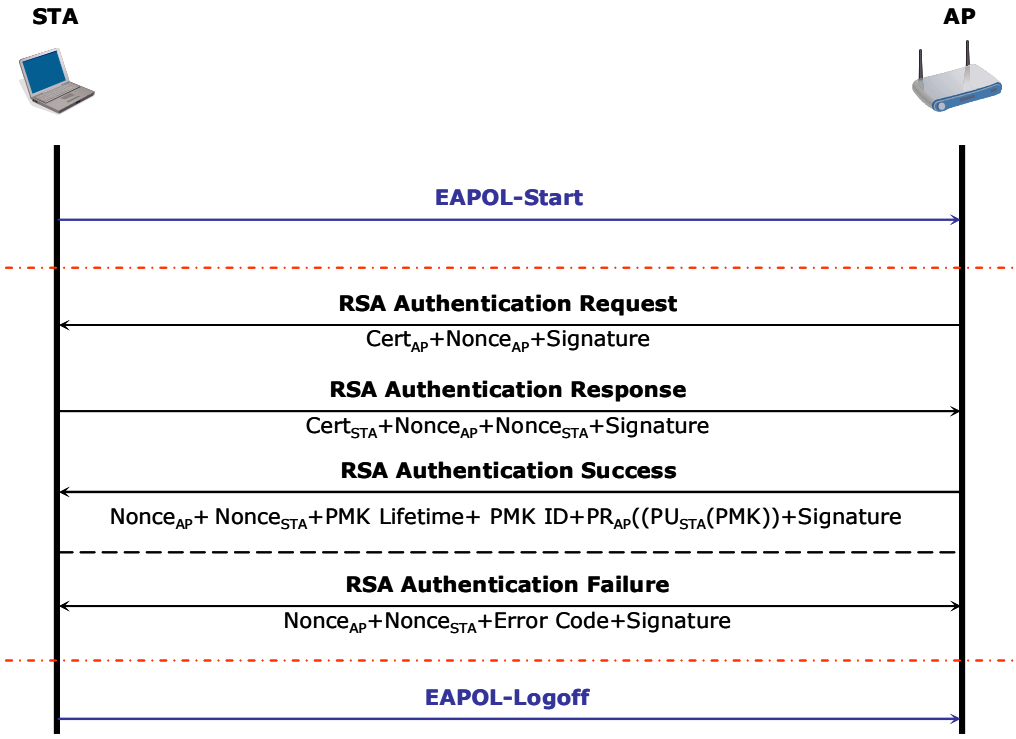


Figure 39. RSA Authentication

RSA Authentication Request Message:

This message is sent from AP to STA to start RSA authentication phase. It comprises of following data:

- $Cert_{AP}$: X.509 certificate of the AP
- $Nonce_{AP}$: 64-bit random value generated by AP
- Signature : RSA signature over all other data

RSA Authentication Response Message

This message is sent from STA to AP in response to the RSA authentication request message. This message is prepared and sent provided that AP's certificate is valid, namely signed by CA or not expired, and MAC address in the AP's certificate is the same as of the one on the source address field of the MAC frame. It comprises of following data:

- $Cert_{STA}$: X.509 certificate of the STA
- $Nonce_{STA}$: 64-bit random value generated by STA
- $Nonce_{AP}$: 64-bit random value sent by AP
- Signature : RSA signature over all other data

RSA Authentication Success Message

This message is sent from AP to STA in response to the RSA authentication response message. This message is prepared and sent provided that STA's certificate is valid, namely signed by CA or not expired, and MAC address in the STA's certificate is the same as of the one on the source address field of the MAC frame. It comprises of following data:

- $Nonce_{AP}$: 64-bit random value sent by AP
- $Nonce_{STA}$: 64-bit random value sent by STA
- PMK Lifetime : Lifetime of the PMK
- PMK ID : ID number of the PMK
- $PR_{AP}(PU_{STA}(PMK))$: PMK encrypted first with the public key of STA and than private key of AP
- Signature : RSA signature over all other data

RSA Authentication Failure Message

This message is sent by AP or STA in case the other party has an invalid certificate or the MAC address in the in its certificate is not the same as of the one on the source address field of the received MAC frame. It comprises of following data:

- $Nonce_{AP}$: 64-bit random value sent by AP
- $Nonce_{STA}$: 64-bit random value sent by STA
- Error Code : 1-byte code for reason of failure
- Signature : RSA signature over all other data

In order to prevent making major changes to 802.1x protocol, same Port Access Control Protocol (PACP) will be used with its defined state machines for STA and AP which are shown in APPENDIX A and APPENDIX B respectively. At the beginning of the communication both AP and STA are in the DISCONNECTED state. After the completion of 802.11 association phase STA and AP shift to CONNECTING state. After receiving the RSA-Request message STA shifts to AUTHENTICATING state and when the AP's certificate is validated successfully STA shifts to AUTHENTICATED state. Following the receipt of RSA-Response message AP shifts to AUTHENTICATING state and when the STA's certificate is validated successfully AP shifts to AUTHENTICATED state. In case of an RSA-Failure message sent either by STA or by AP, both parties shift to HELD state and authentication fails. If the STA wants to end the communication with the AP, it sends an EAPOL-Logoff message and both parties shift to DISCONNECTED state. STA and AP begin to implement Key Receive State Machine and Key Transmit State Machine respectively when they are in AUTHENTICATED state. During the execution of all these processes all the variables defined within the 802.1x standard are set accordingly.

After a successful authentication phase, each party possesses the PMK and generates PTK, which will be used in deriving session keys, using PMK, MAC_{AP}, MAC_{STA}, $Nonce_{AP}$, and $Nonce_{STA}$, by means of 4-way handshake. The rest of the architecture is just the same as the one in 802.11i. In order to provide maximum security AES-CCMP will be used for data encryption.

4.2.2 WMAN Architecture

Authentication in the WMAN portion of the network will have the similar structure that WLAN portion has. That is to say, authentication will be RSA-based. Since PKMv2 introduced by 802.16e already provides RSA-based authentication which is shown in Figure 28, existing structure will be used with some minor changes.

For RSA-based authentication 802.16e requires the BS and SS have factory installed certificates. However, in the architecture proposed here certificates of BS and SS, as well as the certificate of CA, must be installed manually before putting the devices into service. Management of the certificates will be handled in the way explained in 4.2.3.

As it is specified in 802.16e standard, at the end of the authentication phase a pre-PAK key is generated by BS and shared with SS. Pre-PAK is used for

derivation of PAK and PAK is used for derivation of AK. AK is then used for the derivation of KEK and HMAC keys. TEK, GKEK, and GTEK are randomly generated by BS and sent to SS encrypted with KEK.

For the encryption of the data, AES-CCM will be used for stronger protection.

4.2.3 Certificate Management

802.16e standard does not mandate or handle the renewal of the certificates of the devices. According to the standard, it appears that the factory installed certificates will be used during the lifetime of that device. In the proposed architecture, a new certificate management scheme will be defined and management of the certificates will be done dynamically after the initial manual installment. This scheme will not be only for WMAN part of the network, but it will also cover the WLAN segments.

The purpose of the certificate management procedure proposed in this thesis is to put forward a general initial outline to handle certificate renewal processes. It should be improved to handle other management issues like handling revocation lists etc.

The certificate renewal process requires that the current certificate of a device be valid. If the device possesses an invalid certificate for any reason, the renewal will result with failure. This situation may stem from being disconnected for a long period of time and trying to connect again after the certificate expires. This condition requires the manual installment of a valid certificate.

Expiry date of the certificate is checked regularly by the owner of the certificate and prior to the expiration date a request for a new certificate is sent to CA. To check the expiry date of CA's certificate is also clients' responsibility. If a client realizes that the CA's certificate is about to expire, it prepares a request and sends it to CA. New certificates will be valid only after the expiration dates of the old ones.

Since the devices, except the wireless clients, operate at layer 2 of the OSI model, certificate management messages will be handled by this layer. To achieve this, SNAP (Subnetwork Access Protocol) header, which is an extension to the LLC header, will be used for distinguishing Certificate Exchange Messages (CEM). Any 802.11 or 802.16 wireless device, in need of certificate renewal, will prepare a CEM, format of which is provided in Table 7. CEM will be encapsulated

with the LLC and MAC headers with the aforementioned SNAP header settings are done.

Table 7. Certificate Exchange Message Format

FIELD NAME	OCTET NUMBER
STA Address	1-6
AP Address	7-12
SS Address	13-18
Code	19
Identifier	20
Length	21-22
Type	23
Data	24-N

First 18 octets of the message are reserved for the MAC addresses of STA, AP, and SS. These addresses will be used for the correct forwarding of the CEM frames.

The code field is one octet and may have the following values:

- Request (0000 0000)
- Response (0000 0001)

The identifier field is two octets and used for matching response messages with request messages.

The length field is two octets and shows the size of the data field of the message in octets. Since the lengths of the other fields are fixed, they are not included.

The type field is one octet and may have the following values:

- Renew certificate with current CA certificate (0000 0000)
- Renew certificate with a new CA certificate (0000 0001)
- New certificate with current CA certificate (0000 0010)
- New certificate with a new CA certificate (0000 0011)
- Reject request (0000 0100)

The data field is in varying length and may have the following values:

- If type field has the value of 0000 0000 or 0000 0001, than the data field will contain PR_{Client} (New $Cert_{Client}$) which means new unsigned certificate of the requesting client encrypted with its current private key.
- If type field has the value of 0000 0010, than the data field will contain PR_{CA} (New $Cert_{Client}$) which means new signed certificate of the requesting client encrypted with CA's current private key.
- If type field has the value of 0000 0011, than the first octet of the data field will contain the length of the new client certificate in octets and the rest of the field will contain PR_{CUR_CA} (New $Cert_{Client}$, New $Cert_{CA}$) which means new signed certificate of the requesting client and new certificate of CA encrypted with CA's current private key.
- If type field has the value of 0000 0100, than data field will be empty.

Certificate management is primarily done by the clients. CA only accepts, evaluates, and processes the requests coming from the clients. CA decides whether the request owner is an authorized one by decrypting the data field of the request packet with the client's current public key. The connection between the CA and the client is assumed to be secure. If the type of the request packet equals to "0000 0000", than CA will sign the new $Cert_{CLIENT}$ with CA's current private key, encrypt it with CA's current private key, and send it in a response packet with type field equals to "0000 0010". If the type of the request packet equals to "0000 0001", than CA will sign the new $Cert_{CLIENT}$ with its new private key, encrypt both $Cert_{CA}$ and $Cert_{CLIENT}$ with its current private key, and send it in a response packet with type field equals to "0000 0011". If CA receives an invalid request, it will prepare and send a response packet with type equals to "0000 0100", which will stand for reject. Certificate management procedure followed by the wireless devices is depicted in APPENDIX C and scenarios for the implementation of the certificate management process are provided in APPENDIX D.

Handling of the address fields by STA, AP, SS, and BS primarily rely on the code field of the CEM. If the code field is REQUEST; STA, AP, and SS copies their MAC addresses to the corresponding fields regardless of other address fields. In case of RESPONSE;

- AP checks the STA Address field. If it is empty it means that final destination of the message is AP itself, otherwise it forwards the message to the relevant STA.
- SS checks the AP address field. If it is empty it means that final destination of the message is SS itself, otherwise it forwards the message to the relevant AP.
- BS checks the SS Address field. If it is empty it means that final destination of the message is BS itself, otherwise it forwards the message to the relevant SS.

CHAPTER 4

SECURITY AND PERFORMANCE ANALYSIS

Analysis of the proposed architecture will be implemented from two aspects: performance and security. Performance analysis will be based on theoretical comparisons between current and proposed architectures.

WLAN and WMAN portions of the proposed architecture will be analyzed separately, assuming that the link between WLAN and WMAN, namely AP and SS, is secure. The analysis will be done according to the following wireless security requirements:

- Confidentiality
- Authentication
- Integrity
- Availability

Besides the wireless security requirements mentioned above, proposed architecture will be assessed against most common wireless threats:

- Passive Eavesdropping
- Message Injection
- Message Deletion and Interception
- Masquerading and Malicious AP
- Session Hijacking
- Man-in-the-Middle
- Denial of Service

5.1 Security Analysis

Security analysis will be done for WLAN and WMAN parts of the network separately.

5.1.1 WLAN Security Analysis

- **Confidentiality**: Confidentiality of data is provided by AES-CCMP encryption protocol. It's much more secure than WEP by the usage of 128-bit-key instead of 40-bit key, 48-bit IV instead of 24-bit IV, per-packet key instead of network-wide single key, and block cipher instead of stream cipher.

  Considering 4-bit WEP keys can be cracked in less than 50 hours using brute force attack [7], to crack a 128-bit key will take more than 1024 years which will make brute force attack infeasible.

  Repetition of IV values is also an important security flaw in WEP as mentioned previously. If we assume that an access point uses the 50 % of the bandwidth for sending packets and the rest is used by clients, for a WLAN with 11 Mbps rate, the bandwidth used by the AP will be 5.5 Mbps. If the AP continuously sends 1500-byte packets at this rate, IV space with 2^{24} values will be consumed approximately in 10 hours as calculated below:

  $$5{,}5 \times 10^6 / 8 = 687500 \text{ bytes/sec}$$

  $$687500 / 1500 = 458 \text{ packets/sec}$$

  $$2^{24} / 458 = 36631{,}48 \text{ sec} = 10{,}2 \text{ hours}$$

  However, when the IV length is increased to 48 bits for the above scenario, the time needed to consume the IV space will increase to about 19488 years as calculated below:

  $$2^{48} / 458 = 614574184957{,}76 \text{ sec} = 19488 \text{ years}$$

  It can be inferred from above that the encryption scheme used in WLAN part of the network provides sufficient confidentiality.

- **Authentication**: Proposed authentication mechanism requires the usage of X.509 digital certificates. Both AP and STA should possess a certificate.

They authenticate each other by means of public/private key encryption thus providing mutual authentication which is a requirement of 802.11i RSN.

- **Integrity**: Integrity of the messages during authentication phase is achieved by signing the data with the sender's private key. On receipt of the message, the receiver calculates the hash of the data and compares it with the signature after decrypting it with sender's public key. By this way the receiver understands whether the data is changed or not.

  Providing the integrity of the other packets is achieved by AES-CCMP. A 64-bit MIC is created for each packet using block ciphers in CBC mode. A 128-bit integrity key is used for the creation of the MIC.

- **Availability**: Availability is the most vulnerable face of wireless networks. Jamming and scrambling at physical layer constitutes a significant threat. Wireless networks are also vulnerable to DoS attacks as described in Chapter 2. Although the characteristics of the medium used by wireless networks ease the job of an adversary to launch a DoS attack, there are some techniques developed to detect and prevent these attacks as described in [43].

5.1.2 WLAN Threat Analysis

- **Passive Eavesdropping**: This threat can not be avoided due to the characteristic of wireless networks. However, strong encryption mechanism, AES-CCMP, makes it useless for the adversary.

- **Message Injection**: This threat is also inevitable for wireless networks; nevertheless since the adversary does not know the encryption keys used for the traffic, malicious packets will be dropped by the authorized receivers.

- **Message Deletion and Interception**: Although this threat is a hard to implement one, it is not impossible. This threat will only decrease the availability of the network leaving the other wireless security requirements unaffected.

- **Masquerading and Malicious AP**: Authentication mechanism prevents any unauthorized node from masquerading. At the mean time, the mutual

authentication scheme avoids malicious APs. This threat becomes critical, if an adversary possesses the valid certificate of any node.

- **Session Hijacking**: Although it is possible for an adversary to disconnect a wireless client, it is impossible to initiate a new session with already used authentication messages due to usage of nonce values. Confidentiality and integrity mechanisms also make it impossible for an adversary to read encrypted packets and send valid packets even he/she manages to start a new session.

- **Man-in-the-Middle**: To accomplish a man-in-the-middle attack the adversary must disconnect the STA first. After that it must masquerade as the AP to establish a session with the target STA. Because of the existence of a mutual authentication mechanism, this attack is not possible unless the adversary possesses the credentials of the AP.

- **Denial of Service**: WLAN is open to DoS attacks as described in 2.4.3. The main reason of such vulnerability is that management and control frames are not protected. Although DoS is a threat against the availability of the network, the security of the exchanged information remains protected.

5.1.3 WMAN Security Analysis

- **Confidentiality:** Since 802.16e introduced AEC-CCM, which is much more secure than previously used DES-CBC encryption mode, WMAN part of the network can be said to meet the confidentiality requirement. To have an idea about the security provided by AES can be understood by comparing it with DES. If it takes only one second to crack the 56-bit DES key, then it will take 149 trillion years to crack the 128-bit AES key [20].

- **Authentication:** Although mutual authentication was not possible before, 802.16e fixed this problem. It allows both RSA-based and EAP-based authentication. Both SS and BS have to possess valid certificates and thus mutually authenticate each other, which provide a sufficient level of authenticity.

- **Integrity:** Integrity of the data is provided by AES-CCM. A message authentication code is created by applying CBC-MAC algorithm to the message which is then encrypted using AES in counter mode.

- **Availability:** As in 802.11, availability is a serious problem of 802.16 due to the physical characteristics of wireless communications. Jamming and scrambling are possible physical layer attack types. MAC layer DoS attacks can easily be executed to decrease the availability.

5.1.4 WMAN Threat Analysis

- **Passive Eavesdropping**: This threat is possible for management frames sent in clear text form. An adversary can also eavesdrop other traffic, but since they are encrypted it is not possible for an adversary to understand the contents of the message.

- **Message Injection**: An adversary can easily inject messages to the network. However, unauthorized messages will be dropped by the nodes. This threat will result only with a decrease in availability.

- **Message Deletion and Interception**: This threat is also possible, in spite of its hardness. It has no other effect apart from decreasing availability as in message injection.

- **Masquerading and Malicious AP**: This threat is not possible due to the mutual authentication mechanism added to the 802.16 standard by 802.16e amendment.

- **Session Hijacking**: Session hijacking is also not possible to occur due to the provided authentication and integrity mechanisms.

- **Man-in-the-Middle**: This threat is possible for unprotected management messages. Modification of management messages will affect the operation of the communications. Man-in-the-middle attack is not possible for other traffic due to the mutual authentication mechanism.

- **Denial of Service**: An adversary can execute a MAC layer DoS attack by sending numerous authentication messages. Jamming or scrambling done at physical layer also constitutes a serious threat, which can hamper all communications.

5.2 Performance analysis

Performance analysis will be done for certificate management of the network in general and for authentication at the WLAN part of the network.

5.2.1 Analysis of Certificate Management

The main differences pointed out with the proposed architecture are authentication scheme of WLAN segment of the network and certificate management procedure.

Certificate renewal process is achieved by a two way communication; wireless device sends a certificate request message to the CA server and CA server replies with a response message. All this communication is done at Layer 2 of the OSI model as described in 4.2.3.

Assuming that the typical size of a certificate is 1Kbyte, the length of the CEM will be about 1047 bytes and total size of 802.11 and 802.16 frames will be 1113 and 1065 bytes respectively as depicted in Figure 40. 802.16 physical layer PDU consists of multiple DL and UL burst which means that multiple incoming and outgoing MAC frames are carried in a single physical layer PDU. Moreover, 802.16 has a flexible physical layer which makes it impossible to calculate fixed physical layer overhead for a single MAC frame. Because of this reason 802.16 physical layer overhead is not included in the figure below.

802.11

PHY	MAC	LLC	Data (CEM)	CRC
24	30	8	1047	4

802.16

MAC	LLC	Data (CEM)	CRC
6	8	1047	4

Figure 40. Certificate Management Messages

If we assume that the STA is connected to the AP with 11 Mbps and distance between AP and STA is 100 m., certificate renewal process of a STA will keep the WLAN part of the network busy for about 1.82 msec as calculated below. (RTS=44 byte, CTS=38 byte, ACK=38 byte, Data=1113 byte, DIFS=50 μsec, PIFS=30 μsec, SIFS=10 μsec)

$$Time_{WLAN} = Time_{request} + Time_{Response}$$

$$\begin{aligned} Time_{request} &= DIFS+RTS+d_{prop}+SIFS+CTS+d_{prop}+SIFS+Data+d_{prop}+SIFS+ACK+d_{prop} \\ &= DIFS + 3(SIFS) + 4(d_{prop}) + RTS + CT\ S + Data + ACK \\ &= 50\ x10^{-6} + 3(10x10^{-6}) + 4(100/(3x10^{8})) + (44x8)/(11x10^{6}) \\ &\quad + (38x8)/(11x10^{6}) + (1113x8)/(11x10^{6}) + (38x8)/(11x10^{6})\ sec \\ &= 50 + 30 + 1{,}33 + 32 + 27{,}6 + 809{,}45 + 27{,}6\ \mu sec \\ &= 977{,}98\ \mu sec \end{aligned}$$

$Time_{Response}$ = PIFS + Data + d_{prop}
= $30x10^{-6}$ + $1113x8/(11x10^{6})$ + $100/(3x10^{8})$ sec
= 30 + 809,45 + 0,33 µsec
= 839,78 µsec

$Time_{WLAN}$ = 977,98 + 839,78 µsec
= 1817,76 µsec
= 1,82 msec

On the other hand, if we assume that SS is connected to the BS with 30 Mbps and distance between SS and BS is 10 km. certificate renewal process of a STA will keep the WMAN part of the network busy for 1,78 msec. Since 802.16 is connection oriented, medium access delay is not included to the calculations below.

$Time_{WMAN}$ = $Time_{request}$ + $Time_{Response}$

$Time_{request}$ = $Time_{Response}$ = d_{trans} + d_{prop}
= $(1065x8/10x10^{6})$ + $(10000/3x10^{8})$ sec
= 33,33 + 852 µsec
= 885,33 µsec

$Time_{WMAN}$ = 1770,66 µsec
= 1.78 msec

Although certificate management seems to be an additional load to the network and certificates are to be renewed in a periodic manner, periods between each cycle can be days even weeks. Low frequency of this process makes the extra load on the network quite negligible.

5.2.2 Analysis of Authentication Scheme

Following assumptions are made for the calculation of the size of the authentication traffic:

- Length of an X.509 certificate is 1024 bytes.
- Identities (e.g. user name, password) are 16 bytes.
- Signatures of the RSA authentication messages are 160 bytes.
- Cipher Suite in "Client Hello" message is 20 bytes.
- Certificate Types and Certificate Authorities in "Certificate Request" message are 20 bytes each.

Proposed authentication scheme with a central CA server, requires only 4 message exchanges at WLAN (Table 8) and WMAN (Table 9) segments of the network for authentication of a STA.

Table 8. Authentication Message Flow on WLAN without AS

MESSAGES	PHY	MAC	LLC	EAPOL	RSA	CRC	TOTAL
EAPOL-Start	24	30	8	6	0	4	72
EAPOL/RSA Auth. Request	24	30	8	6	1056	4	1128
EAPOL/RSA Auth. Response	24	30	8	6	1064	4	1136
EAPOL/RSA Auth. Success	24	30	8	6	74	4	146
TOTAL (bytes)							**2482**

Table 9. Authentication Message Flow on WMAN without AS

MESSAGES	MAC	LLC	EAPOL	RSA	CRC	TOTAL
EAPOL-Start	6	8	6	0	4	24
EAPOL/RSA Auth. Request	6	8	6	1056	4	1080
EAPOL/RSA Auth. Response	6	8	6	1064	4	1088
EAPOL/RSA Auth. Success	6	8	6	74	4	98
TOTAL (bytes)						**2290**

However, in central AS architecture, eight message exchanges occur at the WLAN segment (Table 10) and six message exchanges occur at the WMAN segment (Table 11). In multiple AS architecture, again eight message exchanges occur at the WLAN segment while no message exchange occurs at the WMAN segment.

Table 10. Authentication Message Flow on WLAN with AS

MESSAGES	PHY	MAC	LLC	EAPOL	EAP	TLS	CRC	TOTAL
EAPOL-Start	24	30	8	6	0	0	4	72
EAPOL/Request Identity	24	30	8	6	21	0	4	93
EAPOL/Response Identity	24	30	8	6	21	0	4	93
EAPOL/Client Hello	24	30	8	6	5	94	4	171
EAPOL/Server Hello	24	30	8	6	5	1149	4	1226
EAPOL/Server Certificate								
EAPOL/Client Certificate Request								
EAPOL/Server Hello Done								
EAPOL/Client Certificate	24	30	8	6	5	1328	4	1405
EAPOL/Client Key Exchange								
EAPOL/Certificate Verify								
EAPOL/Change Connection State								
EAPOL/Finished								
EAPOL/Change Connection State	24	30	8	6	5	34	4	111
EAPOL/Finished								
EAPOL/Success	24	30	8	6	5	0	4	77
TOTAL (bytes)								**3248**

Table 11. Authentication Message Flow on WMAN with central AS

MESSAGES	MAC	LLC	IP	UDP	RADIUS	EAP	TLS	CRC	TOTAL
RADIUS/Access Request	6	8	20	8	38	0	0	4	84
RADIUS/Client Hello	6	8	20	8	22	5	94	4	167
RADIUS/Server Hello	6	8	20	8	22	5	1149	4	1222
RADIUS/Server Certificate									
RADIUS/Client Certificate Request									
RADIUS/Server Hello Done									
RADIUS/Client Certificate	6	8	20	8	22	5	1328	4	1401
RADIUS/Client Key Exchange									
RADIUS/Certificate Verify									
RADIUS/Change Connection State									
RADIUS/Finished									
RADIUS/Change Connection State	6	8	20	8	22	5	34	4	107
RADIUS/Finished									
RADIUS/Access Accept	6	8	20	8	22	0	0	4	68
TOTAL (bytes)									**3049**

Authentication load on WLAN part of the network is 3248 bytes with AS and 2482 bytes without AS as shown in Figure 41.

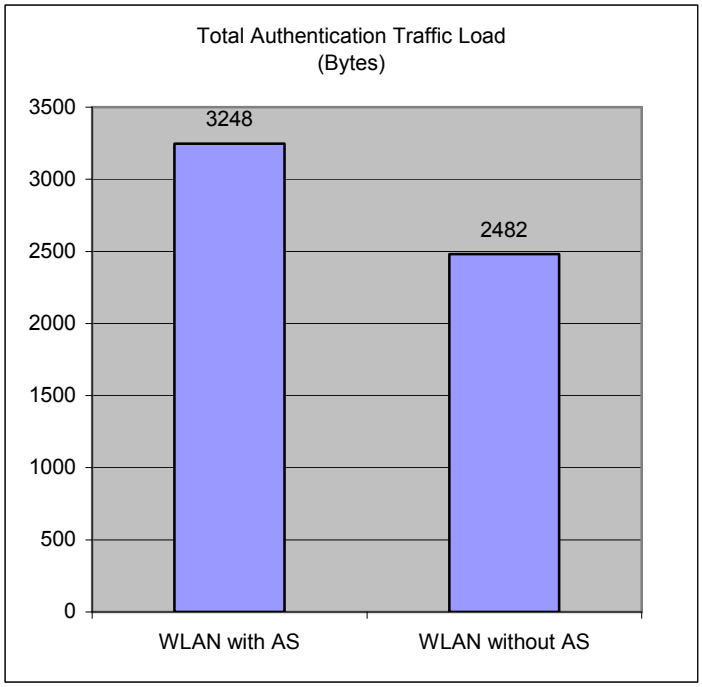


Figure 41. Authentication Load on WLAN

On the other hand, authentication load on WMAN part of the network is 3049 bytes with AS and 2290 bytes without AS as shown in Figure 42.

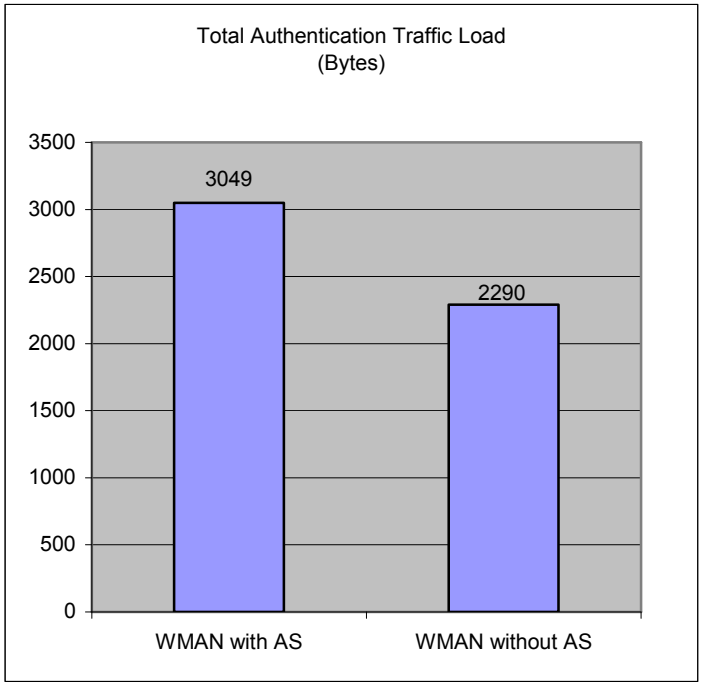


Figure 42. Authentication Load on WMAN

As it can be inferred from the graphs, the new authentication scheme decreases the authentication traffic on both WLAN and WMAN. The only exception is the increase in the WMAN traffic in the multiple AS versus central CA scenario. However, decreasing the traffic on WLAN, decreasing the cost, and decreasing the management overhead make the new authentication scheme still more favorable.

While conventional authentication scheme requires eight message exchanges, proposed architecture requires only four. This will lead to an additional decrease in the authentication traffic on the WLAN part of the network with the proposed scheme stemming from the MAC access procedure of the 802.11. RTS, CTS, ACK frames and interframe spaces defined by 802.11, will put additional load and latency on the network.

5.2.3 Modification Requirements

We should also take the modifications that should be done to the wireless network devices and effects of these modifications to performance of these devices into consideration. Following modifications are required for the implementation of the proposed architecture:

- **STA:** Software modification for certificate management procedures.
- **AP:** Software modification for the new 802.1x implementation, hardware modification comprising of integrating a security processor that will handle RSA operations, manual certificate installation capability, and software modification for certificate management procedures.
- **SS:** Manual certificate installation capability, software modification for certificate management procedures.
- **BS:** Manual certificate installation capability, software modification for certificate management procedures.

As it can be inferred from above, AP requires more comprehensive modifications than the other devices which attract the attention mainly on AP. While the proposed authentication scheme gets rid of the usage of an AS, it does not require the AP to do the entire job the AS does. It authenticates a client by verifying that the certificate is valid and really signed by the authorized CA and authentication request message is signed by the private key of the client. To achieve the necessary modifications a software upgrade will be enough for the 802.1x part of the implementation, but to make RSA encryption/decryption operations we need a cryptographic processor supporting RSA should be installed.

Proposed authentication algorithm requires the AP to perform RSA based operations which stands for additional process load to the AP. However, latest developments in security processor technologies free the APs from this burden. High performance processors doing almost 7.000 1024-bit RSA operations per second (e.g. Cavium's Nitrox Lite Security Processor) are in the market now. Since the number of clients per AP is limited (maximum 25-30 clients per AP) due to the bandwidth considerations, with a separate security processor the drop in AP's performance will be marginal. RSA authentication scheme used in the proposed architecture requires the AP do following five RSA operations per client: one verification, one signature, one key generation, one private, and one public key encryption as shown in Figure 39. If we assume that we use an average processor with 3.000 RSA operations/second performance, the processing time needed to make the RSA operations needed for the authentication of a single client will take about 1.7 milliseconds. Considering that

authentication is done only at the beginning of the communication, it is obvious that RSA based authentication will not put a conspicuous burden on an AP with a security processor installed.

CHAPTER 6

CONCLUSIONS

This chapter summarizes the proposal, pros and cons, and future work suggestions.

6.1 Synopsis of the Proposal

The proposed security architecture is depicted in Figure 43 and requires some minor changes to the aforementioned standards, 802.11i and 802.16e, to provide a more manageable and efficient authentication mechanism.

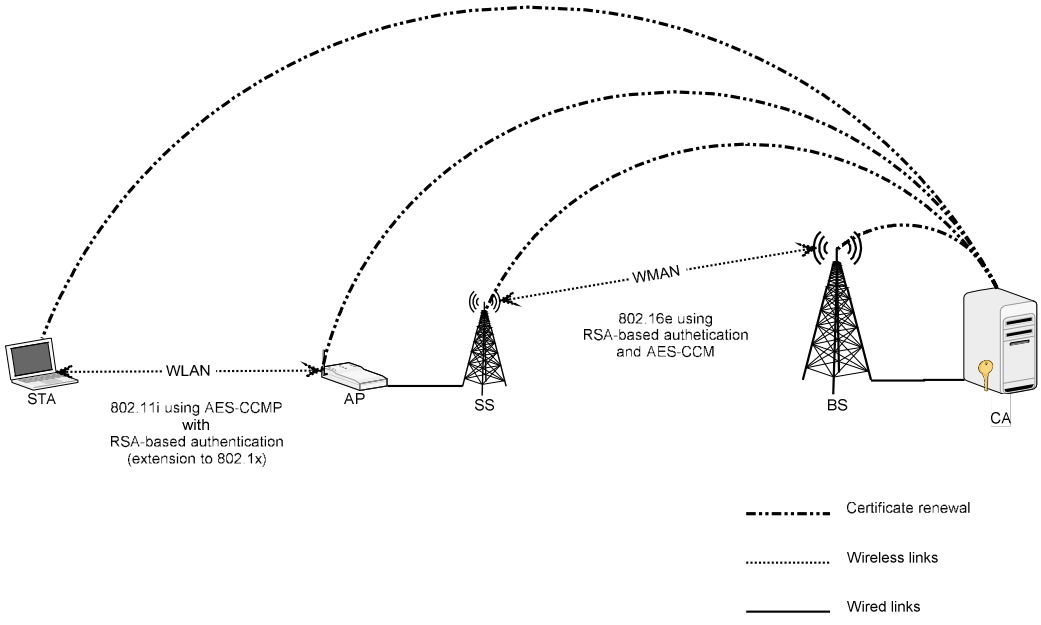


Figure 43. Proposed Security Architecture

Instead of using multiple authentication servers for each WLAN segment, which will complicate the manageability and increase the cost of the network, or single authentication server for the whole network, which will increase both the overhead on the WMAN segment and time required for authentication, this architecture requires a single central CA server. The link between AP and SS and between BS and CA is assumed to be secure.

The change required for WLAN comprises the addition of RSA-based authentication capability by means of a security processor, installing digital certificates to APs, and running an algorithm to keep the certificates up-to-date. 802.1x is not excluded not to disrupt the integrity of the standard and proposals are made as an extension to the current standard.

On the other hand, the changes required for 802.16 part of the network comprises the capability of installing digital certificates to SSs and BS and running an algorithm to keep the certificates up-to-date. Since 802.16e has the capability of RSA-based mutual authentication, there is no need to make any changes to the authentication mechanism provided by the current standard.

6.2 Pros and Cons

802.11 and 802.16 networks used to have numerous security flaws until the introduction of new security amendments; 802.11i and 802.16e. These latest amendments are developed in a fashion to overcome the vulnerabilities of WEP. The analysis' that have been done so far about the security features of these standards show that, if applied correctly, IEEE meets the wireless security requirements except availability. Both 802.11i and 802.16e provide a strong mutual authentication and AES based data privacy and integrity mechanisms to thwart known threats while leaving the availability problem almost unsolved. Of course the real reason lying under this is the complication of preventing such attacks, which stems from the physical characteristics of wireless communications, threatening the availability of the network. However, this drawback can be regarded to be negligible considering that the main purpose of the addressed networks will be mainly to prevent any adversary from ciphering out or changing the information carried across the network.

Proposed architecture decreases the overhead born of authentication scheme which is put forward by 802.11. It decreases authentication traffic both on WLAN and WMAN parts of the network. It also suggests the usage of a certificate

renewal mechanism which will keep the certificates fresh to give less opportunity to an adversary to collect enough data to crack the keys and provides central control and management of the certificates for the entire network by means of the CA server. Another advantage is that getting rid of multiple ASs decreases the cost and increases the manageability of the network and thus decreases the possibility of management and security flaws.

On the other hand, a new overhead occurs due to certificate management procedure. However this overhead is insignificant because of the low frequency of certificate renewal process. Manual installation of the certificates to STA, AP, SS, and BS is also another workload to the administrators but it should be kept in mind that this process will be done only at the initial deployment of these devices. The main disadvantage may be the integration of a RSA capable security processor to the APs, which means a hardware modification. This will make it harder to use COTS devices and thus hinder interoperability.

6.3 Future Work

A potential research on this topic may be the simulation of the proposed architecture that will give more precise performance measurement results and the reaction of the new architecture in heavy traffic conditions.

Another possible future work may be the implementation of the WLAN part of the network to test the new authentication and certificate management mechanisms. This can be achieved by modifying available open source software or developing a new software that can be used to customize the AP and the STA.

And finally another potential future work may be to put forward a more secure architecture that will provide the governments with the capability to exchange classified information over wireless networks. A starting point of this research may be the examination of current practices. For example, U.S. Army is capable of exchanging secret level classified information through 802.11 and 802.16 wireless networks using network devices, namely SecNet11 and SecNet54, running proprietary encryption algorithms.

BIBLIOGRAPHY

[1] Wong, S. (2003). The evolution of wireless security in 802.11 networks: WEP, WPA, and 802.11 standards. *SAN Institute.*

[2] Walker J.R. (2000). Unsafe at any key size; An analysis of the WEP encapsulation. *IEEE Document 802.11-00/362*.

[3] Borisov N., Goldberg I. & Wagner D. (2001). Intercepting mobile communications: The insecurity of 802.11. *Seventh Annual International Conference on Mobile Computing and Networking*.

[4] Arbough W.A., Shankar N. & Justin Wan Y.C. (2002). Your 802.11 wireless network has no clothes. *IEEE Wireless communications, 11/6, 677-686.*

[5] Fluhrer S., Shamir A. & Martin I. (2001). Weakness in the key scheduling algorithm of RC4. *Selected Areas in Cryptography, Canada*.

[6] Arbough W.A. (2001) An inductive chosen plaintext attack against WEP and WEP2. *IEEE Document 802.11-01/230*.

[7] Brown B. (2003). The security difference between b and i. *IEEE Potential, 22/4, 23-27*.

[8] Wi-fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks. (2003). *Wi-Fi Alliance*.

[9] IEEE 802.1x-2004: IEEE standard for local and metropolitan area networks: port-based network access control. (2004).

[10] RFC 3748: Extensible Authentication Protocol. (2004). *IETF.*

[11] IEEE Std 802.11i-2004: IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements. (2004).

[12] Changhua H. & Mitchell J.C. (2005). Security Analysis and Improvements for IEEE 802.11i. *In Proceedings of the 12th Annual Network and Distributed System Security Symposium, San Diego, CA, USA*.

[13] Moskowitz R. (2003). Weakness in Passphrase Choice in WPA Interface. *Retreived January 3, 2007, from http://wifinetnews.com/archives/002452.html*.

[14] Eaton D., (2004). Diving into the 802.11i Spec: A Tutorial. *Retreived January 8, 2007, from http://www.commsdesign.com/printableArticle/?articleID =16506047.*

[15] IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor 1-2005: IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems—Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum. (2005).

[16] Johnston D. & Walker J. (2004). Overview of IEEE 802.16 Security. *IEEE Security and Privacy, 2/3, 40-48*.

[17] Barbeau M. (2005). WiMax/802.16 Threat Analysis. *Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks.*

[18] RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. (2002). *IETF*.

[19] RFC 3447: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. (2003). *IETF*.

[20] National Institute of Standards and Technology (NIST), *Retreived March 12, 2007, from http://www.nist.gov/public_affairs/releases/aesq&a.htm.*

[21] Eklund C., Marks R., Stanwood K. (2002). IEEE Standard 802.16: A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access. *IEEE Tutorial C802.16-02/05.*

[22] Abichar Z., Peng Y., Chang J. (2006). WIMAX: The Emergence of Wireless Broadband. *IEEE IT Professional Magazine, 8/4, 44-48.*

[23] Ma L., Jia D. (2005). The Competition and Cooperation of WiMAX, WLAN and 3G. *IEEE 2nd International Conference on Mobile Technology, Applications and Systems.*

[24] Xu S., Matthews M., Huang C. (2006). Security issues in privacy and key management protocols of IEEE 802.16. *Proceedings of the 44th Annual ACM Southeast Regional Conference.*

[25] Burbank J., Kasch W. (2005). IEEE 802.16 broadband wireless technology and its application to the military problem space. *IEEE Military Communications Conference.*

[26] Chen J., Jiang M., Liu Y. (2005). Wireless LAN Security and IEEE 802.11i. *IEEE Wireless Communications, 12/1, 27-36.*

[27] Gurkas G., Zaim H., Aydın M. (2006). Security Mechanisms and Their Performance Impacts on Wireless Local Area Networks. *International Symposium on Computer Networks.*

[28] Hole K., Dyrnes E., Thorsheim P. (2005). Securing Wi-Fi networks. *IEEE Computer Magazine, 38/7, 28-34.*

[29] Wi-Fi Alliance (2003). Wi-Fi Protected Access: Strong, Standards-Based, Interoperable Security for Today's Wi-Fi Networks.

[30] Wi-Fi Alliance (2003). Securing Wi-Fi Wireless Networks with Today's Technologies.

[31] Williams J. (2002). Providing for Wireless LAN Security, Part 2. *IEEE IT Professional Magazine, 4/6, 38-39.*

[32] Chen J., Wang Y. (2005). Extensible authentication protocol (EAP) and IEEE 802.1x: tutorial and empirical experience. *IEEE Communications Magazine, 43/12, 26-32.*

[33] Potter B., McGraw G. (2003). Wireless Security's Future. *IEEE Security & Privacy Magazine, 1/4, 68-72.*

[34] Feil H. (2003). 802.11 Wireless Network Policy Recommendation for Usage within Unclassified Government Networks. *In Proceedings of IEEE Military Communications Conference.*

[35] Wei N, Zhou J., Xin Y., Li L. (2006). A Security Architecture for IEEE 802.11 Wireless Networks in Large-Scale Multinational Corporations. *In Proceedings of IEEE 6th International Conference on ITS Telecommunications Proceedings.*

[36] Sorman M., Kovac T., Maurovic D. (2004). Implementing improved WLAN Security. *In Proceedings of IEEE 46th International Symposium Electronics in Marine.*

[37] Altunbasak H., Owen H. (2004). Alternative Pair-wise Key Exchange Protocols for Robust Security Networks (IEEE 802.11i) in Wireless LANs. *In Proceedings of IEEE Southeast Conference Proceedings.*

[38] RFC 4346: The Transport Layer Security (TLS) Protocol Version 1.1 (2006). *IETF.*

[39] RFC 2865: Remote Authentication Dial In User Service (2000). *IETF.*

[40] Hong S., Lee J. (2006). Supporting Secure Authentication and Privacy in Wireless Computing. *In Proceedings of IEEE International Conference on Hybrid Information Technology.*

[41] Ding P., Holliday J., Celik A. (2004). Improving the Security of Wireless LANs by Managing 802.1x Disassociation. *In Proceedings of IEEE First Consumer Communications and Networking Conference.*

[42] Pelechrinis K., Iliofotou M. (2006). Denial of Service Attacks in Wireless Networks: The case of Jammers. *UC Riverside Department of Computer Science and Engineering.*

APPENDICES

APPENDIX A: PAE STATE MACHINE IN STA

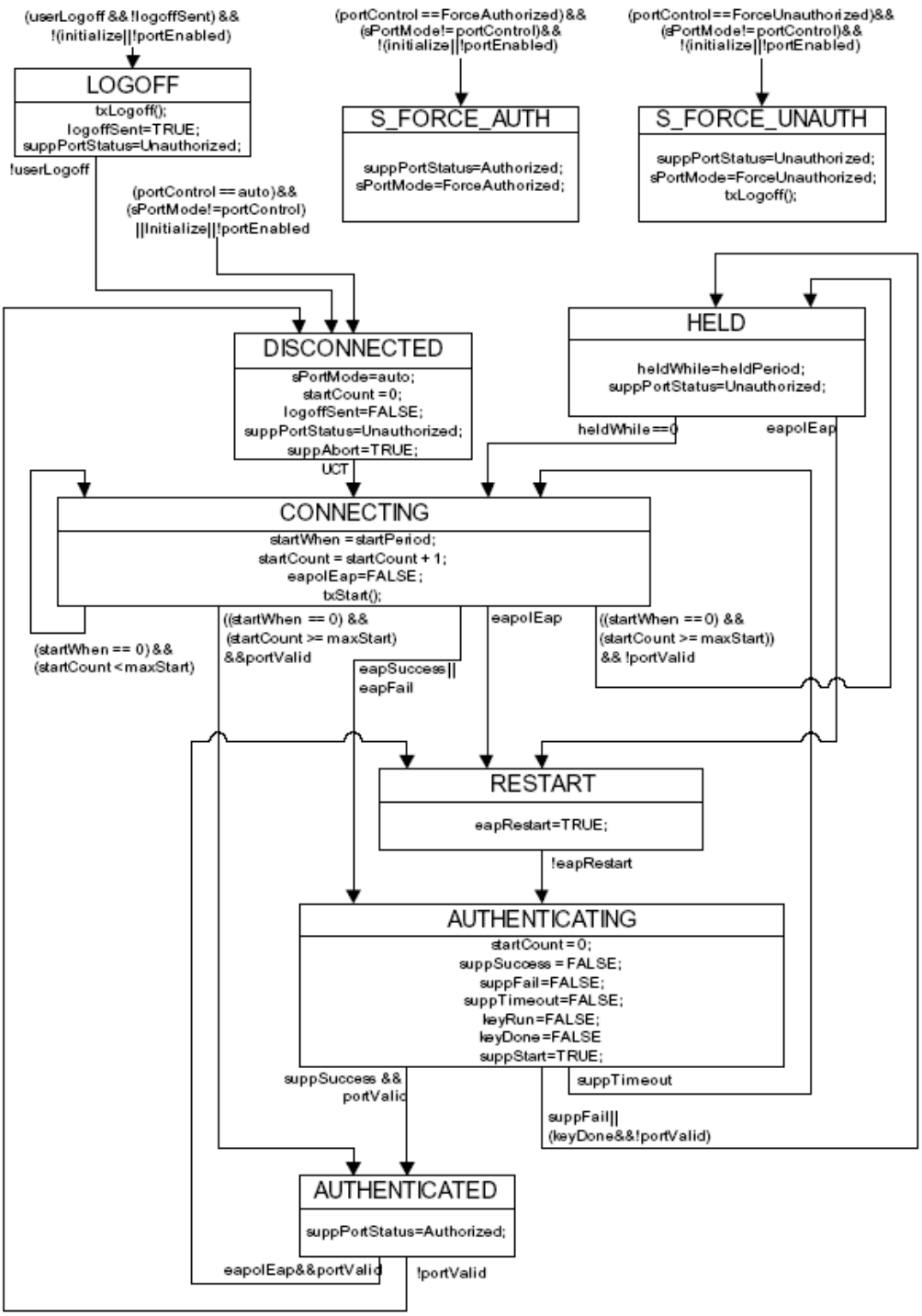


Figure 44. PAE State Machine in STA

APPENDIX B: PAE STATE MACHINE IN AP

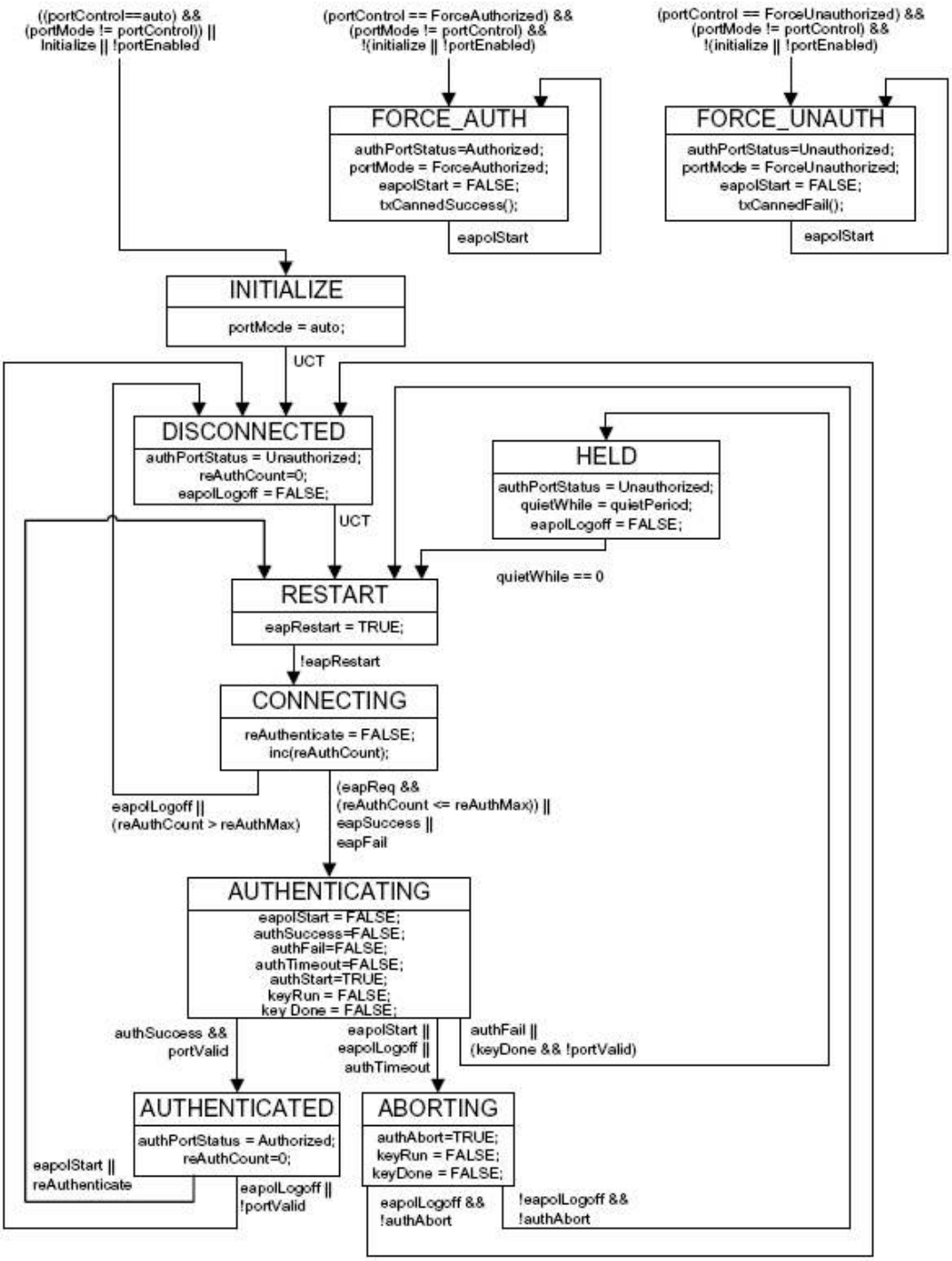
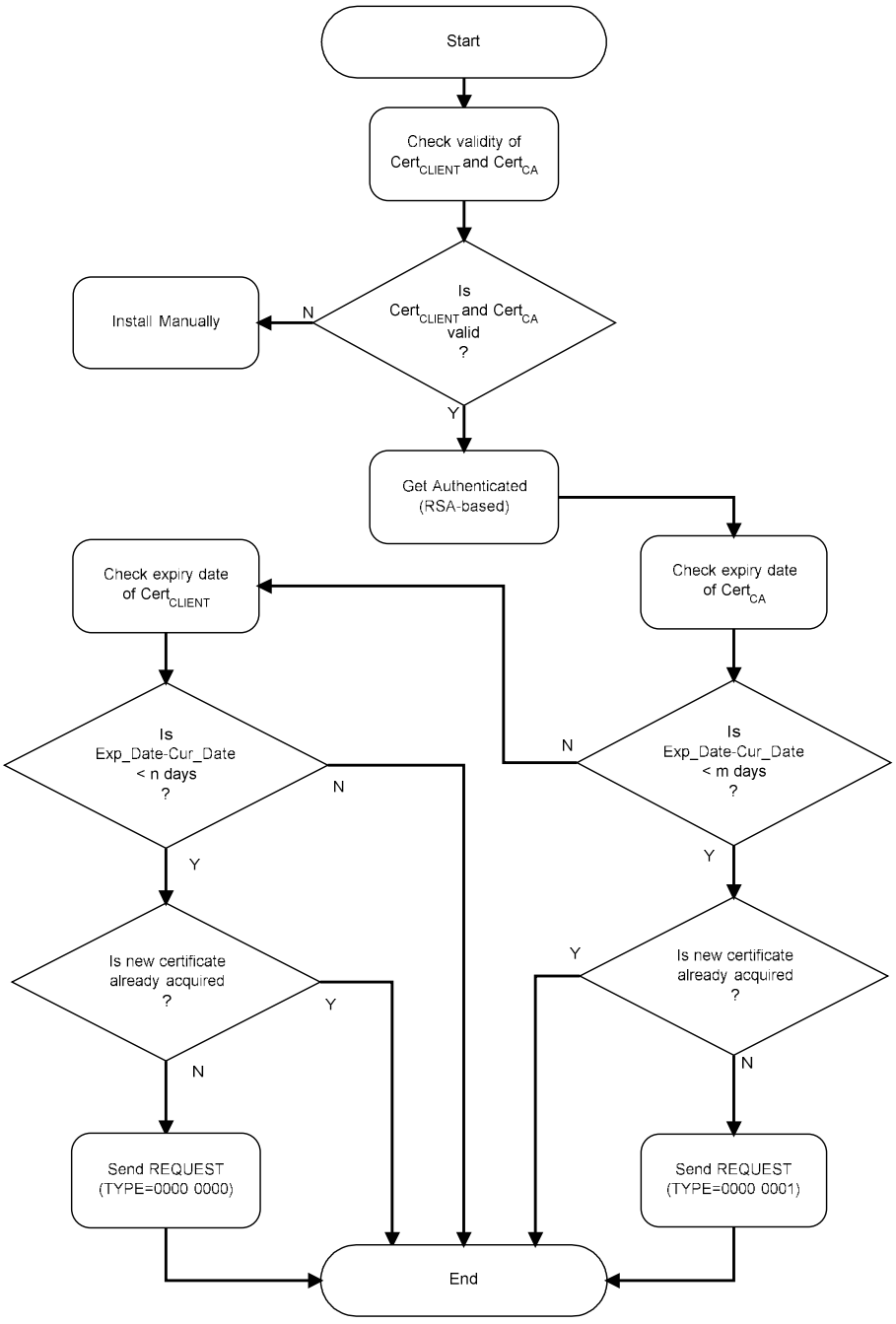


Figure 45. PAE State Machine in AP

APPENDIX C: CERTIFICATE MANAGEMENT PROCESS FLOW DIAGRAM



Note: m and n are defined by network administrator.

Figure 46. Certificate Management Process Flow Diagram

APPENDIX D: CERTIFICATE MANAGEMENT SCENARIOS

Table 12. Scenario 1 – Certificate renewal of STA

STA	Prepare CEM (STA Address=MAC Address, Code=REQUEST)
	Encapsulate with LLC/SNAP and 802.11 MAC headers
	Send to AP
AP	Decapsulate
	Check SNAP header
	If Code=REQUEST then configure CEM (AP Address=MAC Address)
	Encapsulate with LLC/SNAP and 802.3 MAC headers
	Send to SS
SS	Decapsulate
	Check SNAP header
	If Code=REQUEST then configure CEM (SS Address=MAC Address)
	Encapsulate with LLC/SNAP and 802.16 MAC headers
	Send to BS
BS	Decapsulate
	Check SNAP header
	Encapsulate with LLC/SNAP and 802.3 MAC headers (Dest. MAC Address=CA MAC Address)
	Send to CA
CA	Decapsulate
	Find the public key of STA using STA Address on CEM
	Decrypt data field
	Sign and record new certificate
	Prepare CEM (Code=RESPONSE, set address fields according to the incoming CEM)
	Send to BS
BS	Decapsulate
	Check SNAP header
	If Code=RESPONSE then encapsulate with LLC/SNAP and 802.16 MAC headers
	Send to SS (using SS Address on CEM)
SS	Decapsulate
	Check SNAP header
	If Code=RESPONSE then encapsulate with LLC/SNAP and 802.3 MAC headers
	Send to AP (using AP Address on CEM)
AP	Decapsulate
	Check SNAP header
	If Code=RESPONSE then encapsulate with LLC/SNAP and 802.11 MAC headers
	Send to STA (using STA Address on CEM)
ST	Decapsulate
	Check SNAP header and record the new certificate

Table 13. Scenario 2 – Certificate renewal of AP

AP	Prepare CEM (AP Address=MAC Address, Code=REQUEST)
	Encapsulate with LLC/SNAP and 802.3 MAC header
	Send to SS
SS	Decapsulate
	Check SNAP header
	If Code=REQUEST then configure CEM (SS Address=MAC Address)
	Encapsulate with LLC/SNAP and 802.16 MAC headers
	Send to BS
BS	Decapsulate
	Check SNAP header
	Encapsulate with LLC/SNAP and 802.3 MAC headers (Dest. MAC Address=CA MAC Address)
	Send to CA
CA	Decapsulate
	Find the public key of AP using AP Address on CEM
	Decrypt data field
	Sign and record new certificate
	Prepare CEM (Code=RESPONSE, set address fields according to the incoming CEM)
	Send to BS
BS	Decapsulate
	Check SNAP header
	If Code=RESPONSE then encapsulate with LLC/SNAP and 802.16 MAC headers
	Send to SS (using SS Address on CEM)
SS	Decapsulate
	Check SNAP header
	If Code=RESPONSE then encapsulate with LLC/SNAP and 802.3 MAC headers
	Send to AP (using AP Address on CEM)
AP	Decapsulate
	Check SNAP header
	Record the new certificate

Table 14. Scenario 3 – Certificate renewal of BS

BS	Prepare CEM (Code=REQUEST)
	Encapsulate with LLC/SNAP and 802.3 MAC headers (Dest.MAC Add. =CA MAC Address)
	Send to CA
CA	Decapsulate
	Find the public key of BS using Source Address on MAC header
	Decrypt data field
	Sign and record new certificate
	Prepare CEM (Code=RESPONSE, set address fields according to the incoming CEM)
	Send to BS
BS	Decapsulate
	Check SNAP header
	Record the new certificate

Table 15. Scenario 4 – Certificate renewal of SS

SS	Prepare CEM (SS Address=MAC Address)
	Encapsulate with LLC/SNAP and 802.16 MAC headers
	Send to BS
BS	Decapsulate
	Check SNAP header
	Encapsulate with LLC/SNAP and 802.3 MAC headers (Dest. MAC Address=CA MAC Address)
	Send to CA
CA	Decapsulate
	Find the public key of SS using SS Address on CEM
	Decrypt data field
	Sign and record new certificate
	Prepare CEM (Code=RESPONSE, set address fields according to the incoming CEM)
	Send to BS
BS	Decapsulate
	Check SNAP header
	Encapsulate with LLC/SNAP and 802.16 MAC headers
	Send to SS (using SS Address on CEM)
SS	Decapsulate
	Check SNAP header
	Record the new certificate