Access control and availability aspects using wireless solutions based on IEEE 802.11 technologies, providing access to classified networks

by

Tor Kristian Borgi

Thesis in partial fulfilment of the degree of
Master in Technology in
Information and Communication Technology

Agder University College
Faculty of Engineering and Science

Grimstad, Norway

May 2007

Abstract

Wireless networking is among the fastest growing trends in technology. For military objectives wireless networks are effective and flexible ways of communicating, and important elements in operating quick, accurate and independent. Over the last year's commercial technology, based on the wireless IEEE 802.11 standard has grown to be low-cost products offering cheap and easy ways to establish rapid communication services. For all that, lacking elements of security, increased availability, weak mechanisms and capabilities in order to protect and safeguard private wireless networking, concerns costumers which require high assurance communication facilities. To comply with physical security, high-end wireless security requirements and protection mechanisms are required to fully ensure the wireless environment and control the enterprise. Wireless networks has not been considered secure enough to be implemented as part of high assurance communication systems which have access to classified information networks. This thesis considers security aspects of wireless networking related to access control and availability, which means that a wide range of security issues will be discussed. Based on availability, the thesis will focus on requirements and mechanisms related to authentication, confidentiality, integrity and authenticity.

The thesis has indicated through two problem scenarios that high-end requirements signifies complexity and that security mechanisms must be implemented through adoption and adjustment of the available security protocols IEEE 802.1X and IEEE 802.11i. Still, the thesis has shown that security protocols such as IEEE 802.1X and 802.11i does not solve all security problems. Additional wireless protection systems are required to supervise and control state security in order to protect the wireless network environment. In addition, network-layer security is required to oblige end-to-end security control. The conclusion brings security in wireless network into comprehensive challenges that require fully control to analyze data and operations to consolidate the wireless environment.

Considering wireless protection systems which operate as integrated parts of high assurance wireless system, the thesis has investigated mechanisms and ways to actively protect the wireless network environment. The thesis has shown that wireless monitor and honeypot networks introduce potential solutions to meet availability aspects in turns of automatic detection, protection and prevention.

Preface

This thesis fulfills the master degree in Information and Communication Technology at Agder University College, faculty of engineering and science and concludes a two year master science program.

This master project has been initiated by FLO/IKT, developed and performed by Tor Kristian Borgi. I would like to thank supervisor Magne Arild Haglund HIA and Eli Winjum FFI for excellent guidance and feedback during the project period. I also would like to thank Knut Aksel Sæthre FLO/IKT for helping me out with thesis principals and the application area.

Author:

Tor Kristian Borgi

Supervisors:

Magne Arild Haglund, HIA
Eli Winjum, FFI

Tasks and principals:

Knut Aksel Sæthre, FLO/IKT

Grimstad, May 2007

Tor Kristian Borgi

Table of contents

List of figures

List of tables

Abbreviation

AAA	Authentication, Authorization and Accounting
AAAK	Authentication, Authorization and Accounting Key
AAD	Additional Authentication Data
ACL	Access Control List
AES	Advanced Encryption Standard
AKM	Authentication and Key Management
AP	Access Point
ARS	Active Response System
AVP	Attribute-value pairs
ACK	Acknowledgement
AS	Authentication Server
BSS	Basic Service Set
BSSID	Basic Service Set Identification
CA	Certification Authority
CBC	Cipher Block Chaining
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCM	Counter Mode with Cipher Block Chaining MAC
CCMP	Counter mode and cipher block chaining message authentication code protocol
CHAP	Challenge handshake authentication protocol
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier sense multiple access with collision avoidance
CTS	Clear to send
DAIR	Dense Array Inexpensive Radios
DS	Distribution system
EAP	Extensible Authentication Protocol
EAP-FAST	Extensible Authentication Protocol - Flexible Authentication via Secure Tunnel
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol - Tunneled Transport Layer Security
EAPOL	Extensible Authentication Protocol - Over LAN
EAPOL-KCK	Extensible Authentication Protocol – Over LAN Key Confirmation Key
EAPOL-KEK	Extensible Authentication Protocol– Over LAN Key Encryption Key

EMSK	Extended Master Session Key
ESP	Encapsulating security payload
ESS	Extended Service Set
ETSI	European Telecommunication Standard Institute
FCS	Frame Check sequence
FIPS	Federal information processing standards
FLO/IKT	Forsvarets Logistikkorganisasjon Informasjon og Kommunikasjons Tjenester
GMK	Group Master Key
GTC	Generic Token Card
GTK	Group Temporal Key
HMAC	Hash Message Authentication Code
HMS	Hardware security module
IBSS	Independent Basic Service Set
IDS	Intrusion detection system
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange protocol
IP	Internet Protocol
IPsec	Internet Protocol security
IV	Initialization Vector
KGD	Key Generation and Distribution
LAN	Local Area Network
LLC	Logical link controller
MAC	Medium Access Control
Mbps	Megabit per second
MDS	Monitor Defence System
MFP	Management Frame Protection
MIC	Message Integrity Code
MS-CHAP	Microsoft Challenge-Handshake Authentication Protocol
MSK	Master Session Key
MTU	Maximum Transmission Unit
NIC	Network Interface card
NIST	The National Institute Of Standards and Technology

NSM	Norwegian National Security Authority
OSI Model	Open System Interconnection Basic Reference Model
OTP	One-time Password
PAC	Protect Access Credential (Cisco system)
PEAP	Protected Extensible Authentication Protocol
PHY	Physical Layer (OSI-model)
PLCP	Physical Layer Convergence Procedure
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMK	Pairwise Master Key
PN	Packet Number
PRF	Pseudo-Random Function
PSK	Pre Shared Key
PTK	Pairwise Transient Key
RADIUS	Remote Authentication Dial In User Services
RF	Radio Frequency
RSN	Robust Security Network
RSNA	Robust Security Network Association
RSNIE	Robust Security Network Information Element
RSSI	Received Signal Strength Indication
RTS	Ready to send
SSID	Services Set Identifier
SSL	Secure Socket Layer
STA	Station, wireless endpoint device
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
USB	Universial Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Networking
WEP	Wired Equivalent Privacy
WIDPS	Wireless Intrusion Detection and Protection System
Wi-Fi	Wireless Fidelity, also known as WLAN

WLAN	Wireless Local Area Networks, based on IEEE 802.11 technology
WNC	Wireless Network Card
WPA	Wi-Fi Protected Access

Thesis definition

The Norwegian Defence owns and manages its own information and communication network based on known IP technology. The infrastructure today is based on wired communication using both copper and fiber optic cables. As an extension of this environment, FLO/IKT would like to add wireless solutions. However, it is very important that such wireless networks do not leak any information or data that can be used to compromise the information system. To prevent this FLO/IKT would like to insert mechanisms and implement solutions for prevention and protection. This thesis will consider security aspects of wireless IEEE 802.11 environments, and discuss secure architectures based on available components and technology. Earlier studies of wireless networks have concluded that wireless technology is not mature enough and should be precluded from use in terms of critical infrastructure, or in environments where availability is a primary requirement. Due to the fact that research has improved security in wireless systems, the main research questions in this thesis will be;

1. *Is it possible with today's knowledge and technology to design and implement a wireless system platform based on IEEE 802.11 technologies, which can be recommended for use in a military environment with access to classified information?*

2. *Due do the facts that wireless networks being an open medium available for an outsider and based on the surrounding threats, is it possible with today's technology to insert mechanisms and components that are capable of controlling the wireless network activity?*

The thesis will investigate security aspects connected to access control technology, confidentiality and availability and suggest ways to protect the wireless environment against malicious activity and attacks. The thesis work will be focused on different described security scenarios which will be related to operational activity. If conclusions or part of the conclusions means any change or add in the today's WLAN/LAN architecture, the changes must be adapted regarding the over all security requirements. All changes in security architecture and mechanisms related to information and communication services must be evaluated and approved by the Norwegian National Security Authority (NSM).

Author: Tor Kristian Borgi and Magne Arild Haglund

1.1 Problem introduction and background

Security in wireless networks is a well defined problem area. Because of the availability and the lack of control over which subjects receiving signals from the network, a challenge in developing secure solutions based on wireless technology will arise. The problem area has a range of security challenges associated and many of them differ in technology classifications. Basically there are two parts of the WLAN security conundrum. One concerns wireless availability, which involves access control and confidentiality requirements using authentication, encryption and integrity. The second concerns monitoring and attacks affecting the infrastructure, which requires detection and protection mechanisms to prevent the systems from being compromised. Attackers using wireless clients and rogue access points to gain access to wireless systems are a threat as well as internal factors that will degrade the wireless network performance. FLO/IKT is responsible for delivering information and communication services for the Norwegian Defence. As a consequence of this, security features are important and needs to be thoroughly considered. FLO/IKT would like to offer flexible and effective communication services to meet the demanding and requirements from operational activities. Providing new services involves security considerations and it is important that such solutions do not signify weaknesses which are capable of disrupting or compromising the system.

The use of wireless networks based on the IEEE 802.11 standard [8] has increased dramatically over the last years. Producers and the commercial market offer laptops, mobiles and other computer widgets with automatic built-in wireless IEEE 802.11 technology. This has influenced users and communities which have discovered the big advantages of going wireless. Wireless networks will probably continue to grow and many people will rely on its services. Interacting wirelessly is undoubtedly effective, flexible and inexpensive ways of communicating. For military objectives efficient communication is an important element in operating quick and accurate. In difference, wireless networks being an open medium with no precise bounds make it difficult to apply physical security. Compared to wired networks, privacy can not be compromised unless someone uses special equipment to intercept data. To implement wireless solutions in terms of providing access to classified networks, security elements need to be closely evaluated. Wireless access involves employing approved methods for access control, confidentiality and integrity which are well documented and authorized for use in a military context.

1.2 Concepts and definitions

Concepts	Definitions [20,11]
Classified networks	*The Norwegian classifications grouping consist of four levels of sensitivity; BEGRENSET, KONFIDENSIELT, HEMMELIG and STRENGT-HEMMELIG.*
BEGRENSET	*The lowest of four Norwegian classification levels.*
Controlled area	*An area where the user organisation applies legal measures to control access*
Authentication	*Establishing the genuineness or correctness of an entity or of some information*
Authorisation	*The permission to access and perform operations on some information.*
Authenticity	*The correctness of an entity or some information*
Association	*A relationship between objects which allows objects to perform an action on its behalf. [11]*
Encryption and cryptographic mechanisms	*A function, algorithm or protocol designed to provide or support provision of confidentiality, integrity or authenticity*
Integrity	*The property that some information has not been subjected to unauthorized change*
Intrusion Detection System (IDS)	*Intrusion detection is the process of monitoring data traffic in a computer system or network and analysis the data for intrusion attempting to compromise confidentiality, integrity or availability [72].*
Smartcard	*A smartcard is defined as any pocket sized card with embedded electronic integrated circuits containing memory storage components, security logics and perhaps a*

	microprocessor component.
Institute for Electrical and Electronic Engineers (IEEE)	*The IEEE is non-profit professional organization founded by engineers in 1884 for the purpose of consolidating ideas dealing with electro technology. The IEEE plays a significant role in publishing technical networks and network standard developments. For example IEEE 802.3 (Ethernet), IEEE 802.5 (token ring)) and the IEEE 802.11 (WLAN) standard. [48]*
National institute of standards and technology (NIST)	*NIST is a none-regular agency of the United States Department of commerce's Technology administration. The mission is to advance measurements science, standards and technology to improve quality and enhance security.*
Federal information processing standard (FIPS)	*FIPS are publicly announced standards developed by United states federal government for use by all none-military governments' agencies and government contractors.*
Public Key Infrastructure (PKI)	*Traditional PKI is based on certificates containing asymmetric crypto using private and public encryption keys.*
Hardware Security Module (HSM)	*HSM is usually referred to as a external plug-in-card or devices which can be used to securely generate and protect crypto graphical secrets for example certificates and private keys used for authentication.*

Table 1: Master thesis concepts and definitions

1.3 Security requirements

To address military network security requirements [20], solutions must be adapted according to the level of confidentiality and sensitivity. The “BEGRENSET” level of confidentiality, which is relevant for this master thesis, is defined as the following:

> ***BEGRENSET*** *shall be used if it could to any extent entail adverse consequences for the security of Norway or its allies, its relationship with foreign powers or other vital national security interests if the information were to become known to unauthorized persons. [20]*

Basic security requirements are expressed and defined for level BEGRENSET and below (unclassified). The definition of basic security is based and founded on the level of confidentiality and is described as follows:

> ***Basic security:*** *When a breach of the service results in loss of integrity or authentication of systems or information, causing damage equivalent to compromise of unclassified information or information classified BEGRENSET. [20]*

As described in [20], the basic security level may apply to situations where loss of integrity or authentication of systems or information causes only disturbance on mission or system effectiveness. This thesis deals with communication systems connected to classified networks approved for BEGRENSET and signifies that system requirements are related to elements of “Basic security”. The level of “Basic security” contains requirements according to the employment of approved cryptographic mechanisms, integrity and authenticity, which will not be evaluated in this document. Such approvals and accreditation must be conducted by the Norwegian National Security Authority (NSM). Suggestions in this master thesis will be based on official documents, research and general security methodology. Another concern related to wireless network is the adoption of physical security, which involves physical control to network resources, such as infrastructures, system-components and devices. Physical security can not be applied to radio waves and therefore security needs to be ensured using approved cryptographic techniques. This thesis will consider architectures, methods and protocols which can be used to improve and increase the overall security and trust in wireless environments base on 802.11 technologies.

1.4 Problem area

Working with security in wireless local area networks is a comprehensive field. In order to evaluate and analyze security aspects connected to classified network, all paramount security conundrums needs to be considered. On top of the hierarchy there are basically four central research objectives and requirements relevant for this master thesis [10, 11]:

- *Access control* – Includes restrictions to individuals or devices to access network resources. This involves system authentication, message authenticity and authorization mechanisms.
- *Confidentiality* – Ensuring that information can only be read by those authorized to have access. This involves using cryptographic mechanisms to protect information being transmitted.
- *Integrity* – Detection and protection of unauthorized changes to data during communication. This involves using cryptographic hash mechanisms to detect unauthorized modifications.
- *Availability* – Ensuring that authorized individuals and devices can access resources when needed, as well as prevent access from unauthorized devices.

To build security in wireless networks it is required to design a secure framework that consists of approved mechanisms for access control, confidentiality and integrity. These are typical security classifications which are important in any communication network, but in a wireless context such mechanisms are essential. Availability concerns two important security related aspects. The first aspect is connected to availability for those authorized to use the network and assurance that services are accessible. The other aspect is related to the fact that radio equipment, radio waves and radio signals are available to others in the area, including neighbours and possible intruders. This requires severe quality to cryptographic technology protecting the wireless information flow. In other words, security in wireless networks needs to be addressed to all four research objectives; access control, confidentiality, integrity and availability.

Another important objective is that wireless security solutions must be applied according to the specific employment and the surrounding threats. There is no fully answer to how security should be constructed and deployed in a wireless environment, but there exist several different protocols, methods and mechanisms that may be implemented in order to form an accommodation for a best practice security solution. One of the biggest challenges is to shape a consistent and effective solution which transparently takes care of security issues in a controllable context and protects the environment against particular threats and vulnerabilities.

1.4.1 Security problem scenarios

The goal of this thesis is to investigate security related mechanisms and systems which can be used to improve security in wireless networks. Wireless networks based on IEEE 802.11 technologies may range many types of applications, and the employment may have different purposes. The thesis will discuss and suggest security related improvements related to two problem scenarios. These scenarios are both connected to a deployment of networks based on the wireless standard; IEEE 802.11. In general, these types of network are easy to use, most of them inexpensive, and highly flexible for interconnection and communication. If we are able to add high level of security which can ensure reliable services, wireless network systems may become attractive solutions for building secure, flexible and transparent network communication facilities. Below I will introduce both security problems, which I will handle and evaluate in my master thesis. Both security cases are connected to operational contexts and are based on using commercial products in terms of providing access to classified systems. Each scenario will be described generally, which means that the existing overall system solution will not be explained in details regarding security restrictions. I will also refer to chapter 6 for further information and details.

1.4.1.1 Case one

Case number one is related to wireless links between two access points (nodes), “one-to-one”, whereas one of the nodes is connected to a mobile unit environment communicating with its home network environment. In this case confidentiality and integrity are insured using virtual private network (VPN) technology based on IP security encapsulating security payload (IPsec ESP) as an end-to-end security solution. The mobile unit environment is then able to communicate with its home environment systems, classified and approved for “BEGRENSET”. The security issues in this case are connected to access control and availability aspects to the wireless IEEE 802.11 network and its devices. The wireless network components need to be secured and protected against intruders and malicious activity. Both access points are physically secured, but are located in public areas. This means that since we are using commercial products operating within a commercial frequency area, the radio signals are public available. This requires severe security mechanisms which are able to confine access to the wireless system as well as protecting the access points (AP's). This problem scenario involves threats ranging from high professional attackers to regular people who just happen to be in the area. The wireless systems should be configured in a way that network facilities are logical concealed. If this is possible it will prevent most devices from requesting services from the AP. Another important issue is connected to control within the radio channel range, which indicates the ability to detect wireless unauthorized devices experimenting to associate with the high assurance wireless network. Figure 1 shows an overview of this problem scenario.

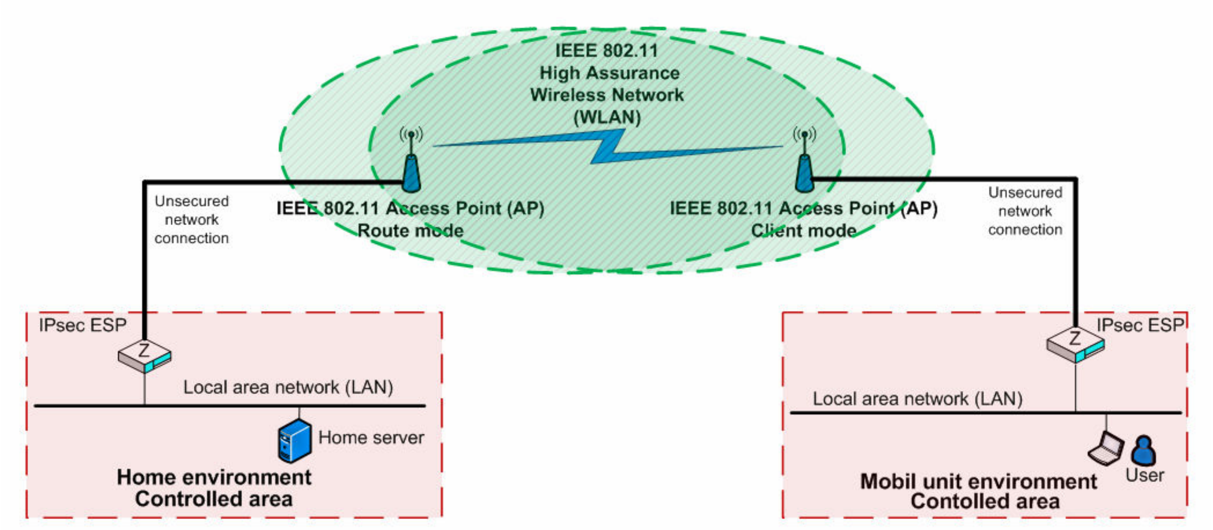


Figure 1: Case one, problem scenario descriptions.

Case number one describes a scenario where it is required to add mechanisms and systems that are capable of controlling access to the wireless environment, including the ability of detect local intruders fumbling with the wireless network. It is also important to look at protection mechanisms which are able to avoid unauthorized devices from trying to attack or associate with the wireless system.

1.4.1.2 Case two

Problem scenario number two has a different security operational setting and involves wireless clients communicating with a wireless access point within controlled area. This scenario differs from the previous case because confidentiality, authenticity and integrity must be added on to the wireless client device. In other words, this case involves security aspects connected to a deployment of a wireless system in a "one-to-many" operational setting. Based on this, case two consists of a whole different range of security challenges to be considered. Basically, the VPN-IPsec ESP solution only provides secure interconnection between the mobile environment and the home environment. In addition we need to add security mechanisms to protect wireless communication, the clients, and the access point. The communication needs to be secured using commercial security protocols and techniques. This signifies that such a configuration must be closely evaluated. The thesis goal in this case is to suggest ways to secure a wireless environment based on high-end security requirements, forming the best practice security architecture. This includes proposing ways to secure the communication between clients (STA's) and the AP as well as the ability to control the wireless environment and wireless infrastructure. Figure 2 shows an overview of this problem scenario context.

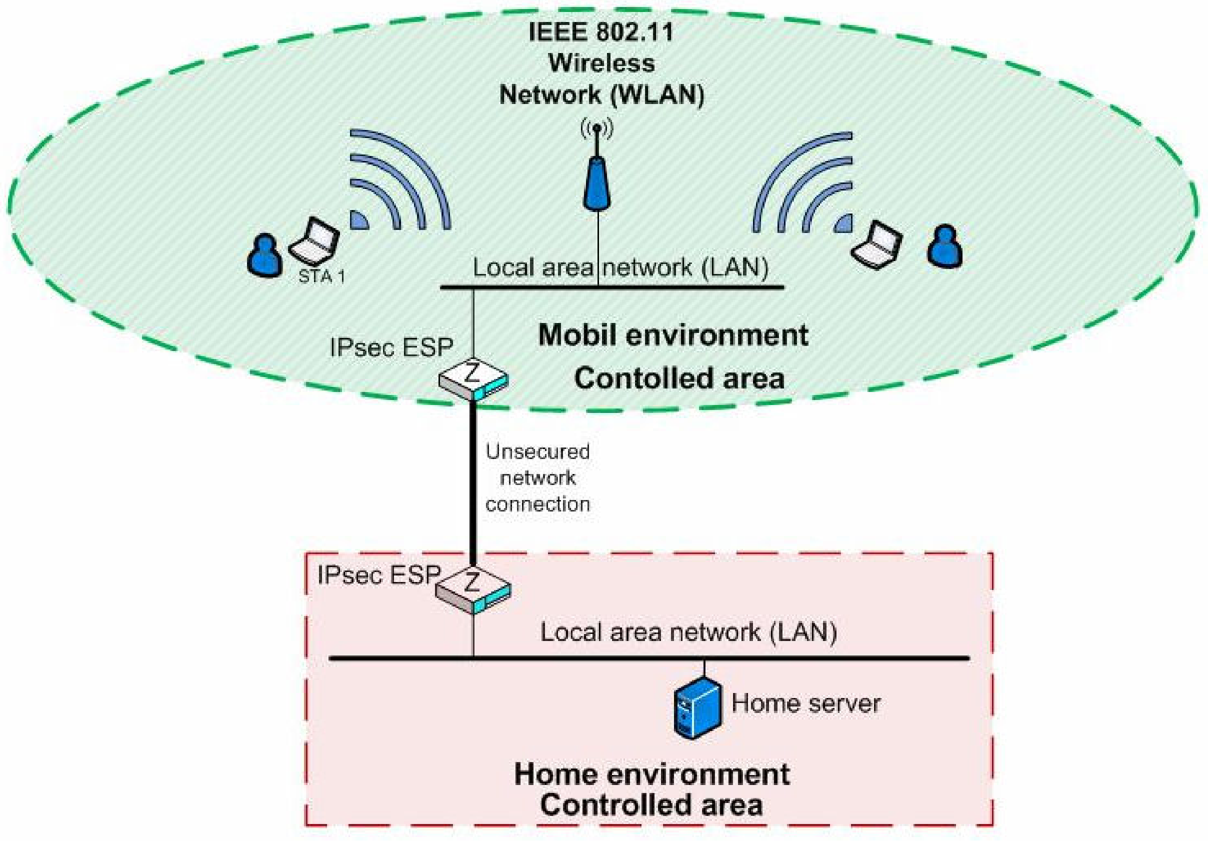


Figure 2: Case two, problem scenario description.

To make a secure solution we need to address threats, vulnerabilities and add high-end requirements considering infrastructure based wireless networks. The main focus will be access control and availability aspects, which involves implementing authentication and confidentiality mechanisms as well as systems for wireless control with detection and protection capabilities.

1.4.2 Particular sub problems

1. How to design a secure solution for wireless access control?
    a. A fundamental issue designing secure wireless solutions is to make sure that only authorized users may access the wireless network. This sub problem involves studying centralized access control systems and authentication methods based on the IEEE 802.1X protocol used in wireless networks. The preferred access control solution should be described through claims based on a well known security foundation. This sub problem involves choosing set of mechanisms, protocols to discuss appropriate architectural requirements.

2. How to provide confidentiality, integrity and authenticity?
    a. The only approved solution for transmitting military classified data over unsecured networks is using military encryption-devices, developed and approved by the National Security Authority. The solution is based on network-layer security mechanisms and is not adapted for use in wireless networks. To ensure confidentiality, integrity and authenticity in wireless networks it is required to investigate link-layer (OSI-layer-2) security aspects to consider commercial technology that offers over-the-air cryptographic mechanisms and protection functionality. It is required to discuss the wireless security standard IEEE 802.11i, addressing WPA2 security features, to investigate and discuss potential solutions.

3. How to secure the wireless infrastructure against local threats and availability aspects?
    a. Because of availability, wireless technology used in high assurance networks, represents a wide range of threats and vulnerabilities to be considered. To establish secure wireless solutions it is required to discuss the circumstances of availability related to wireless IEEE 802.11 networking involving high degree of availability to equipment, radio signals and security technology. Based on the lacking possibilities to provide physical security in wireless network, it is required to investigate security mechanisms capable to control the wireless environment. This sub problem involves studying mechanisms for control, detection and protection of wireless high assurance environments to prevent the wireless system from being compromised.

1.5 Methods and thesis work

This thesis work will be based on descriptive and explanatory research, founded on theoretical approaches to implement high assurance wireless networks. The thesis has defined two problem scenarios which will be discussed and solved through a study based on prior research, approved documents and general security methodology. The thesis work will focus on architectural challenges combined with problem issues including principals, methods, protocols, mechanisms and features which involve defining high-end security requirements to enable high assurance wireless network communication.

1.6 Delimitations and presumptions

Security in wireless networks is a comprehensive topic and it is an extensive process to consider all security aspects of wireless networking. The thesis will handle security aspects connected to access control and availability, which involves authentication, confidentiality, integrity and authenticity. Due to the time limit, the thesis will not be able to deliver a finished product on how to secure a wireless network infrastructure. Based on two problem scenarios, the goal of this thesis will be to study and discuss important security aspects and challenges and propose security requirements recommended for high assurance wireless network. The scope will be confined by the network layer (OSI-layer-3) of the Open System Interconnection Basic Reference model (OSI-model), but the main focus will be the physical-layer (OSI-layer-1) and the link-layer (OSI-layer-2). The specification of this master thesis document will be based on the IEEE 802.11 standard and the thesis will basically focus on IEEE 802.11X and the IEEE 802.11i settlement, known as WPA 2.0, on how to establish secure wireless communication channels. Older security protocols already known as insecure, such as WEP, will not be considered in this thesis. In addition the thesis will study wireless monitoring and intrusion detection and protection systems for wireless networks. Wireless protection mechanisms are highly challenging fields, and official research paper and documents are lacking on this area. Thus, the thesis work will be based on ideas, some prior approved documents and proposals according to implement mechanisms for automatic protection of high assurance wireless environments.

1.7 Requirements

Basic knowledge of radio technology anatomy and wireless IEEE 802.11 networks is required. Basic understanding of the OSI-model is an advantage, and knowledge to information security is presumed.

1.8 Motivation and thesis outcome

Wireless communication offers organisations and users many benefits compared to wired infrastructures and wireless networking is among the fastest growing trends in technology. In difference, security contribution is a rather slow process, which sometimes tends to be neglected by product developers and vendors offering commercial communication products. Higher data-rates, flexibility, transparency, low cost, and other features make it easier for the publicity to use and employ wireless networks. Security is very often not a concern before someone, or something exploits and utilizes weak points in communication in order to collect information, steal facts or particulars based on, for example financial motives. Security must be a closely integrated process of product development, and upcoming products should be strictly evaluated before they can be implemented into high assurance networks. Even though, security in wireless IEEE 802.11 networks is a popular research area and over the last years a lot of security related work has been composed. The challenge is that no standard approved model has been created according to recommend wireless solutions for use in high assurance environments with access to, for example classified information networks. Previous papers and research have concluded fatal weaknesses to wireless networks, which signify that such networks should not be connected to systems requiring high level of security. Vendors and researchers have contributed in developing security protocols, mechanisms, functionality and systems to increase security for wireless network establishments. This development is interesting approaches when it comes to designing secure wireless environments and constructing wireless solutions for military purposes. The outcome of this thesis will be important work and contribution according to visualize requirements and challenges in terms of using wireless communication systems for enclosed computer networks and high assurance prospectives.

1.9 Project outline

This master thesis provides the following project outline:

- Chapter 2: Introduces the basics of wireless LAN technology based on the IEEE 802.11 standard and presents wireless LAN threat aspects, security protocols and protection technology.

- Chapter 3: Discusses access control and security requirements based on IEEE 802.1X standard.

- Chapter 4: Discusses confidentiality, integrity and authenticity mechanisms based on the IEEE 802.11i standard framework.

- Chapter 5: Discusses availability aspects and investigates ways to monitor, control, supervise and protect the wireless LAN environment.

- Chapter 6: Proposes requirements and architectural ways to implement high assurance security networks in context of two relevant WLAN security scenarios (case one and case two).

- Chapter 7: Conclusion and further work

2 Preliminaries and literature studies

This chapter presents basic introduction to the IEEE 802.11 standard network protocol, describing general operations and functionality related to wireless infrastructure networking. Additional the chapter introduces known threats and vulnerabilities concerning IEEE 802.11 networks, and provides a brief overview of WLAN security aspects including specification, security standards, and security functionalities. Security issues related to access control, confidentiality and availability will be introduced together with protocol specifications, mechanisms and security improvements composed over the last years. The introduction will basically restrict to OSI-layer one and OSI-layer two securities, but at the end of this chapter OSI-layer three security mechanism adapted for wireless networks will be mentioned.

2.1 The wireless architectural model

The IEEE 802.11 standard defines a topological infrastructure which offers wireless communication services approximately comparable to the IEEE 802.3 Ethernet standard. Ethernet is based on permanent cable infrastructure which limits the ability to provide mobile and seamless connectivity services. To create a wireless network, basic wireless network components interact and establish wireless services through known concepts of radio communication. Consequently these wireless systems build their own architectural model providing mobile and flexible local area network services. The infrastructure model consists of wireless clients and access points providing connectivity within the radio coverage area. Below some basic definitions from [15, 9] introducing the concept of wireless infrastructure networking are presented.

- **Infrastructure Mod**e – A wireless configuration where an access point transfers data from different STAs to a wired distribution system.
- **Access Point (AP)** – An AP is wireless logical unit which connects different STAs with a wired network infrastructure (Distribution system).
- **Stations (STA)** – A wireless endpoint device such as laptop, mobile phone, PDA.
- **Basic service set (BSS)** – BSS is the basic building block of a WLAN. The BSS consists of on AP surrounded with one or more STAs configured in infrastructure mode.
- **Distribution system (DS)** – DS is an infrastructure, typical wired LANs, that

interconnects different BSSs

- **Extended service set (ESS)** – ESS is a WLAN consisting of more than one BSS connected to distribution system (DS).

A representative IEEE 802.11 network infrastructure consists of one or more access points (AP) offering wireless communication within the radio coverage area. To connect to an AP you will need a wireless network card (WNC) designed for the IEEE 802.11 communication standard. The AP is usually connected to a distribution system (DS) which offers access to local information systems, application-services and links to other networks. An overview of a typical wireless LAN system is shown in figure 3.

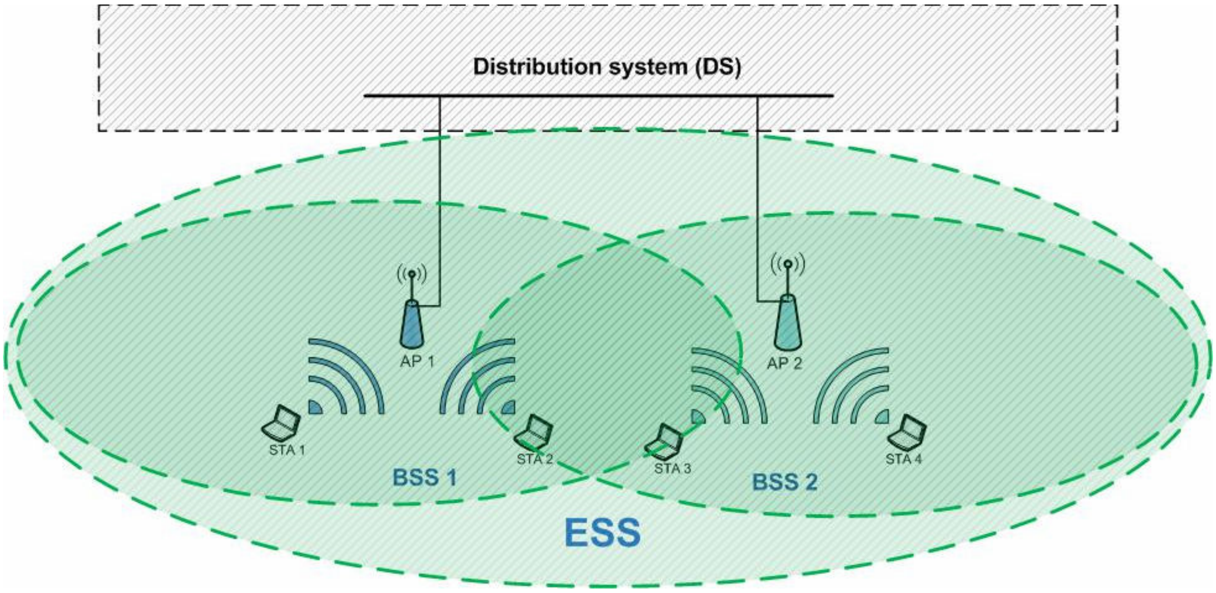


Figure 3: Wireless IEEE 802.11 topology in infrastructure mode

2.2 *Physical characteristics*

In June 1997 [48], the IEEE organization finalized the initial standard of wireless IEEE 802.11 networks. The IEEE 802.11 topology, as shown in figure 3, consists of interacting components providing wireless LAN's (WLAN) services that enable mobile and transparent communication facilities for higher protocol layers [39]. The standard specifies two different radio frequency ranges, the 802.11a standard using the 5 GHz frequency band and 802.11b standard using the 2.4 GHz ISM band. These specifications are based on physical characteristics which contain functionality and properties to provide radio network communication services. In table 2 and an overview of physical characteristics of WLAN systems are shown.

Characteristics of WLAN	Description
Physical layer	*Direct Sequence Spread Spectrum **(DSSS)**, Frequency Hopping Spread Spectrum **(FHSS)**, Orthogonal Frequency Division Multiplexing **(OFDM)**, IR*
Random Access Control	*Carrier Sence Multiple Access with Collision Aviodance **(CSMA/CA)***
Modulation schemes	***OFDM Binary phase shift keying (BPSK)** – 1 to 2Mbps.* ***OFDM Quadrature phase shift keying (QPSK)** – 5,5 to11Mbps.* ***OFDM 64- Quadrature phase shift keying (64-QPSK)** – up to 54 Mbps.* ***OFDM-MIMO 256 Quadrture phase shift keying (256-QPSK)** – up to 300Mbps.*
Standard WLAN models	*802.11a, 802.11h, 802.11b, 802.11g, 802.11n*
Coding techniques	*11bit- barker code sequence* *8 bit - Complementary Code Keying (CCK)*
Frequency band	***802.11 b, g and n**:* *2.400 – 2.4835 Ghz (ISM band) and* ***802.11 a, h and n:*** *5,150 - 5350 Ghz and* *5,725 – 5,825 Ghz*
Channels	*802.11b and g - **11 channels** (3 none overlapping channels)* *802.11a and h – **8 channels** (none overlapping)*
Data rates	*1 Mbps, 2Mbps 11Mbps (11b), 54 Mb (11a og 11g), 300Mbps (11n)*
Defined protocol layers	***Physical layer** (PHY), **Medium Access Control** (MAC) and **Logical Link Control** (LLC)*
Operation range	*50-100 meters*
Security standards	*802.1X , 802.11i, 802.11w*

Table 2: Characteristics of WLANs

2.3 IEEE 802.11 protocol

The following section provides a small introduction to the wireless communication based on the IEEE 802 11 standard. To be able to discuss security within wireless networks we need to address the main functionality and characteristics of the basic protocol. The IEEE 802.11 protocol describes the two lowest layers of the OSI-model [39, 48]. As shown in figure 4 these two layers provide requisite functionality to enable wireless communication facilities. The physical layer defines electrical and mechanical characteristics providing encoding schemes and modulation mechanisms enabling transmissions of bits through a wireless communication channel. The data link layer provides medium access control (MAC) and logical link control (LLC) enabling multiple appliances to share a transmission medium via carrier sense multiple access (CSMA) techniques [48]. Basically, these two layers provide the physical framework for sending data packets between two network entities, for example between wireless stations (STAs) and access points (APs). Usually entity communication is protected by cables which offer enclosed physical connections between two network components. The unique about IEEE 802.11 networks is that OSI-layer 1 and OSI-layer 2 information are available for anyone within radio range. This availability aspect is of concern regarding security considerations, and for high assurance networks which implements wireless communication services.

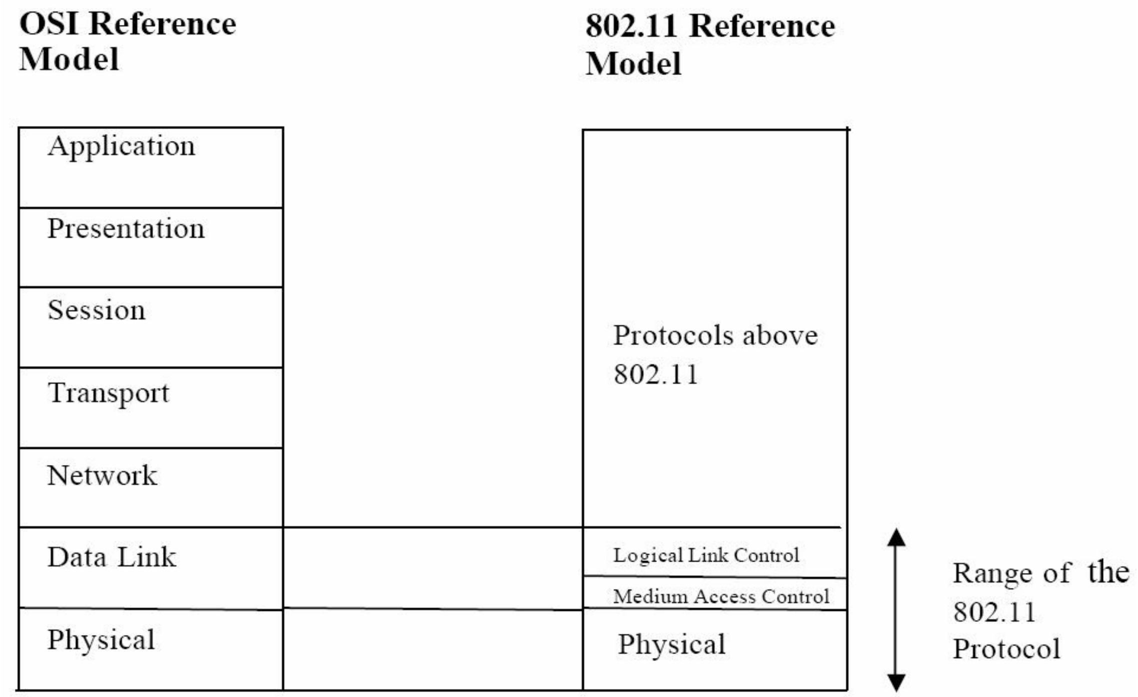


Figure 4: Corresponding of the IEEE 802.11 layers to the layers of the OSI Model [43]

The IEEE 802.11 networks address the OSI data-link layer (MAC/LCC) and the physical layer (OSI-PHY). As you can se from figure 5, the physical layer defines the different wireless standards related to 802.11 networks. The Data-link MAC layer provides interoperability between the physical layer and upper layers using a medium control mechanism called CSMA/CA. Since all users share the same media and radio frequencies, CSMA/CA sense the medium before sending data and uses a random back off timer if the medium is busy. In addition, the MAC layer defines functionality for medium reservation using ready-to-send/clear-to-send (RTS/CTS) polling coordination. These mechanisms together avoid clients and data-packets from interference and collisions.

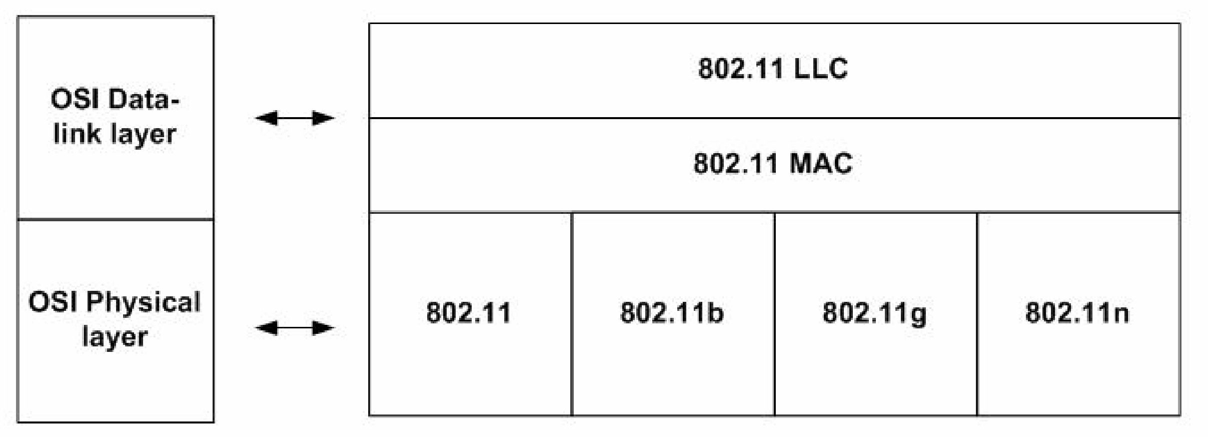


Figure 5: Lower OSI layers corresponding the IEEE 802.11 structure.

The Logical Link control (LLC) [48] is the highest layer of the data link protocol and provides functionality to exchange data between end users across the wireless LAN. The LLC tasks are connected to addressing and data link control mechanisms indicating that the LLC layer is responsible for transmitting error-free layer 2 packets from one destination to another. To provide this functionality the LLC appends a control header and creates an LLC protocol data unit (PDU), which adds control information at the beginning and at the end of the MAC frame packet. This control information is needed for quality assurance and operation of the MAC protocol.

The data link layer (LLC/MAC) communicates with each other using simple service primitives [48]. These primitives define the protocol functionality in general.

- **Request** – request services from other layers
- **Confirm** – conveys the result of previous services
- **Indication** – indicate for other layers that a significant event has occurred
- **Response** – completes a procedure indicated by a indication primitive

These data link primitives can handle connection oriented services and acknowledged/unacknowledged connectionless services which depends on the LLC implementation. In the next section we will take a look at the data-link layer communication format, the MAC frame structure.

2.3.1 IEEE 802.11 frame structure

The IEEE 802.11 standard specifies the MAC frame format [5, 48], consisting of a MAC header, a Frame Body and Frame Check Sequence (FCS). This format is shown in figure 6.

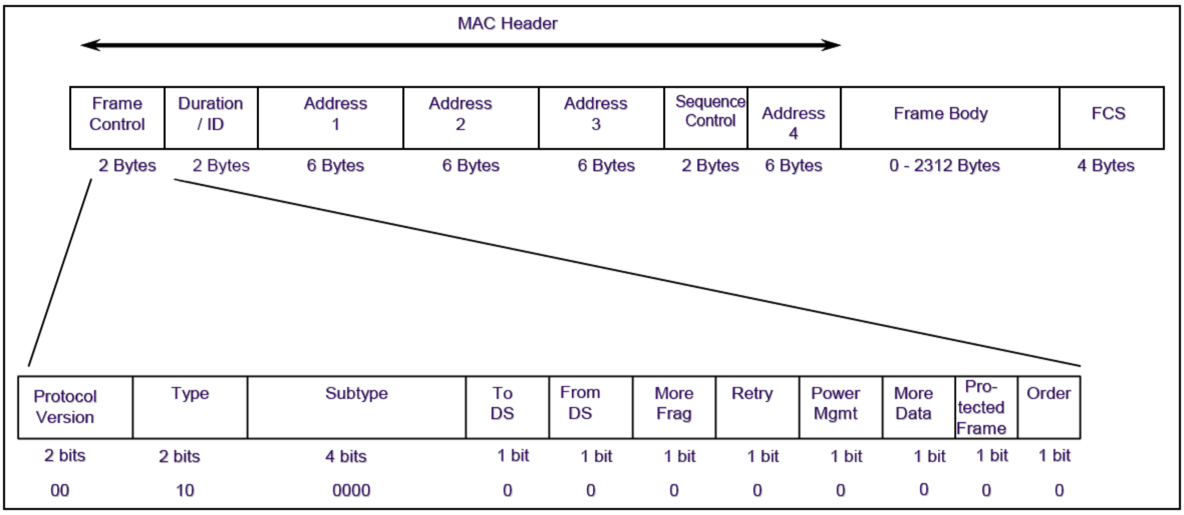


Figure 6: The overall MAC frame format [9].

The frame body contains MAC frame payloads, which depending on the frame type includes application data from higher layers of the OSI-model. The FCS field contains a 32-bit cyclic redundancy check (CRC) which calculates the entire MAC frame to verify transmission errors. The MAC header is quite interesting in wireless contexts, because this header will be visible for anyone monitoring the wireless network. The MAC header consist of 4 address fields, 1 frame control field, 1 sequence control field and a ID/duration field. The address field 2, 3 and 4, the sequence control field and the frame body are not found in every frame [5], indicating that these fields are optional and based on the message intention. The frame control field, showed in figure 6, carries information necessary for the STA's and the AP to read, understand and handle the MAC frame. This frame information contains basic frame control data including frame type and subtype, if the frame originates from a DS or from the wireless network and if the frame is encrypted. The duration/ID field [5] includes a duration value and identifies the duration of the next frame sent from a STA or AP. Other STAs on the network monitor this information, to hold off transmissions and prevent collisions. The address field contains different types of addresses depending on the frame being sent. There are basically five types of addresses being transmitted, source address, destination address, transmitting station address, receiving station address and the basic service set identification (BSSID). These addresses are based on 48-bit IEEE 802 Link Layer Address [5], also referred to as MAC-address. The BSSID defines the MAC-address of the AP and for infrastructure networks this address is used to connect STAs to the corresponding AP. The frame body has a variable length and the payload carries information according to the specific frame. This field may contain a PDU (LLC), as described in section 2.3, providing application data. The sequence control field is used to control the number of PDU's (LLC) being transmitted, by incrementing a sequence number field for each successive transmission.

2.3.2 IEEE 802.11 frame types

Regarding different types of MAC-frame data, the frame structure shown in figure 6 is passed to the physical layer for transmission. The physical layer appends a new header at the front of every transmission frame. The MAC-frame carries information that pertains to the specific frame and the functionality of the data packet. Based on this the IEEE 802.11 specification divides MAC-frames into three categories being transmitted between STAs and AP in an IEEE 802.11 network [9, 48]:

- **Data frames.** The data frame carries the payload from upper layers of the OSI-model. This payload is encapsulated and forwarded in PDU packets determined by the LLC layer. The data frames allow upper layer application to deliver data packets between STA's and AP.

- **Management frames.** Management frames are responsible for carrying management information. The purpose of management frames is to establish initial communication between STAs and AP. Management frames provides the ability to handle MAC layer services such as authentication, association, beacons and probe-request and other required messages handlings between STAs and AP.

- **Control frames.** After an authentication and association process, the control frames are used to control the exchange and the flow of data frames. Examples of control frames are request to send (RTS), clear to send (CTS), acknowledgement (ACK), power save Poll (PS Poll) etc.

These three types of MAC-frames are all required to provide wireless communication facilities. Regarding security in wireless networks, security protocols such as IEEE 802.11i has been introduced to protect the Data-frames. This protocol will be closer described in section 2.5. Unfortunately no available protocol standard has been focusing on protecting the Management-frames and the Control-frames, but a new upcoming security standard, 802.11w is working on this security issue.

2.3.3 The 802.11 state machine and the association process

The IEEE 802.11 standard defines different types of MAC-frames providing services for the LLC to exchange PDUs datagram's between two entities on the network. These services, implemented by the MAC layer, can be divided into two system categories [48]:

- **Station services**. Includes distribution of PDUs to STA, involving services like authentication, deauthentication, authorization and privacy.

- **Distribution System Services**. These services include association, disassociation, distribution and reassociation.

These services are required to provide necessary functionality between stations (STAs) and access points (AP) in order to send and receive data packets. This is also where security issues raises, because availability aspects require adequate levels of security to be implemented to ensure STA and network privacy. As described in figure 7, IEEE 802.11 state machine has three existing states between source and destination. The first state occurs when a STA activates the wireless network card (WNC) and appears unauthenticated and unassociated with the AP. The STA will then transmit an authentication request to the AP, and the AP will respond with an authentication challenge. If the STA is able to figure out the correct challenge-response, the STA will move into state 2. This state indicates that the STA has passed authentication successfully. In state 3 the STA tries to associate with the AP. The association process maps the STA to the distribution system (DS) in order to establish a connection and obtain network connectivity. Often the DS requires a second authentication process to access local DS network services. Figure 7 shows an overview of the general association process of STA's requesting services from the AP and until the association is granted and network access is obtained.

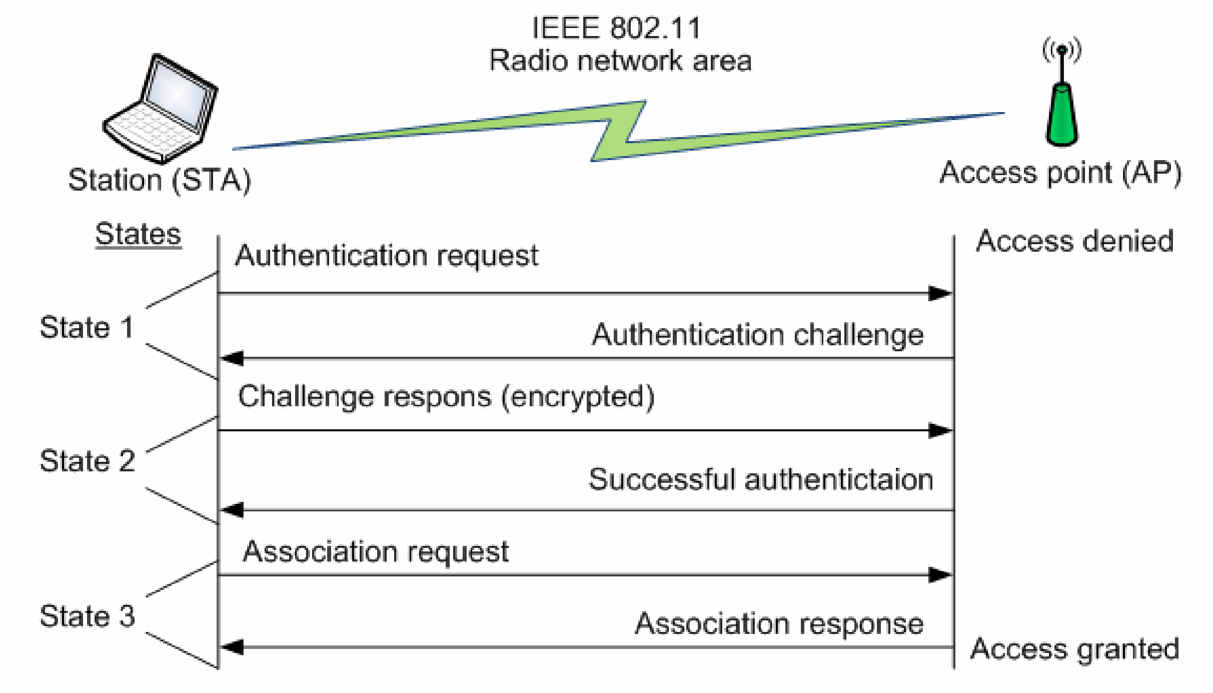
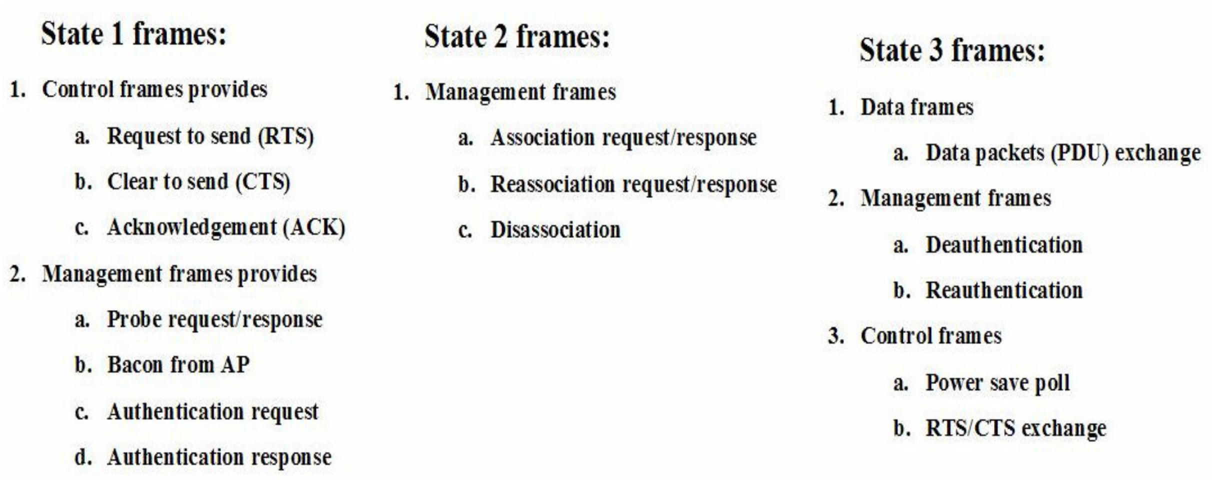


Figure 7: Basic WLAN association

For the authentication and association process the STA and AP uses control frames and management frames. Referred to [48], the transition process shown in figure 7 can be reviewed in figure 8 as the following combination frame-state:



State 1 frames:

1. Control frames provides
   a. Request to send (RTS)
   b. Clear to send (CTS)
   c. Acknowledgement (ACK)
2. Management frames provides
   a. Probe request/response
   b. Bacon from AP
   c. Authentication request
   d. Authentication response

State 2 frames:

1. Management frames
   a. Association request/response
   b. Reassociation request/response
   c. Disassociation

State 3 frames:

1. Data frames
   a. Data packets (PDU) exchange
2. Management frames
   a. Deauthentication
   b. Reauthentication
3. Control frames
   a. Power save poll
   b. RTS/CTS exchange

Figure 8: The association process and frame types

Because of the radio frequency availability, the association process must be securely protected. In other words, security mechanisms must to be implemented in order prevent unauthorized devices from accessing and compromising the wireless system. Before we look into security protocols and improvements, I would like to introduce an overview of threats and vulnerabilities considering IEEE 802.11 infrastructure networks. These threats are the basis for what security mechanisms and functionalities which are required to fully secure a wireless network environment. The next section introduces WLAN threats and security challenges.

2.4 *WLAN threats and security challenges*

Referred to [20] there are different threat levels depending on the application area, the system operation and the attached employment. The threat picture connected to a WLAN deployment needs to be considered as a consequence of a threat evaluation and an estimated vulnerability analysis. Such an evaluation is out of the scope of this thesis, but in a security manner it is important that the different threats can be addressed through implementation of security mechanisms and functionality.

2.4.1 Threat levels and definitions

To analyze security in wireless networks we need to define the threats, vulnerabilities and potential attacks. Because of the local availability aspects, there are lots of uncertain security issues and riskiness concerning employments of wireless IEEE 802.11 networks; especially for networks providing access to classified information. According to [20] there are three threat levels defined; low threat, medium threat and high threat. Because of the radio access availability aspects, and accordingly that a wireless 802.11 network is available outside controlled area as well inside controlled area, there exist a certain high threat appreciation connected to WLAN deployments. This signifies that wireless LAN systems should be capable of handling availability aspects and address security issues before it may be implemented into real-time classified systems.

2.4.2 Wireless threat aspects

Entities operating within in a wireless network are basically concerned with the same threats as any other devices connected to local area networks (LAN's). In addition, wireless network communication is physically available and therefore introduces several security challenges and vulnerabilities. The following section presents the most relevant threats and vulnerability aspects related to wireless networks.

2.4.2.1 Eavesdropping

Eavesdropping is when someone secretly listens to some others conversation [26]. Because of radio waves availability, an attacker can passively monitor wireless network communication without being detected. Confidentiality mechanisms are required to prevent against eavesdropping threats.

2.4.2.2 Monitoring and traffic analysis

Attackers passively or actively monitor wireless transmission to identify patterns, architectures, participators, and network/security configurations in order to map a network overview. This information can be used to find the weakest point in defense and to adjust potential attacking techniques.

2.4.2.3 Brute force attack

Because of eavesdropping and radio access availability aspects, attackers can use brute force methods to compromise data-encryption, to recover cryptographic keys and to formulate plaintext data. This demonstrates that encryption technology used in wireless networks must be well founded and approved mechanisms which are well protected against brute forces mechanisms.

2.4.2.4 Man-in-the-Middle attack

In a Man-in-the-Middle attack the attacker actively intercepts the communication path between two legitimate parties, to obtain credentials and data. The goal is to use cryptographic keying materials, passwords or other authentication credentials that it receives, to gain access to the wireless network. IEEE 802.11 networks are particularly vulnerable to Man-in-the-Middle attacks because of the radio communication availability, and such attacks can be achieved through bogus [9] or rough access points, which intends to act as authorized devices.

2.4.2.5 Message modification and replay attacks

Because of availability aspects it is possible for attackers to modify legitimate messages sent over wireless network, for example in direction of a Man-in-the-Middle attack. Messages can be modified by deleting, adding or changing the packet content. In IEEE 802.11 networks this is a relevant problem for messages sent over the air in plaintext and without any integrity protection (MIC). Authenticity and integrity protection methods can prevent against modification by detecting the origin of and changes to packet content. Replays intends to record series of frames and packets, for example authentication messages, to replay them to gain access to the network. Such attacks can be avoided using packet counters, signatures and counter integrity protection (MIC).

2.4.2.6 Spoofing and masquerading attacks

Spoofing and masquerading is related to attackers that try to impersonate authorized devices, for example to fake the origin of packets in order to achieve various advantages. Another example is attackers that modify (fake) the MAC address [28], which is currently a WLAN security problem. A MAC-changing tool such as SimpleMAC [79] is free software which can be used to spoof MAC addresses. Spoofing and masquerading are often used in combination with other attacks like Man-in-the-Middle and Session hijacking.

2.4.2.7 Session hijacking attack

This type of attack intents to take control over legitimate sessions by using authorized devices to gain access to the wireless networks. In a typical Session Hijacking attack the attacker receives the challenge response from a legitimate AP, which is forwarded to a legitimate STA. The legitimate STA encrypt and respond to the challenge, and the attacker uses the STA-response to authenticate. The legitimate STA receives a log off message from the attacker to prevent suspiciousness. To prevent this irreversible authenticity methods are required to avoid accomplishment of session hijacking attacks.

2.4.2.8 Rogue access points, rough clients and phishing attacks

Rogue access points (AP) and rogue clients (STA's) are unauthorized devices which infiltrate the wireless network area attempting to connect and associate with the authorized system. Rogue devices are typical low cost and SOHO products [27] which are brought in by employees or visitors. STA's may automatically try to connect to a rough access point if it accidental uses the same SSID. For attackers rogue access points and rough clients can detect authentication credentials, cryptographic key materials and request/responses in order to compromise the wireless system. Rogue AP and STA's are also described as *phishing* attacks [74] where the intention is to impersonate legitimate devices and lure clients to connect to it. Wireless control, detection and active protection mechanisms are required to prevent rough devices from infiltrating the wireless network area.

2.4.2.9 Denial of Service (DOS) and flooding attacks

Attackers may try to prohibit devices and wireless components to degrade network performance. Such attacks are meant to disrupt wireless networking by sending more requests than the network devices can handle [25]. These types of attacks can cause network downtime and loss of productivity. For wireless LAN such attack often assails the basic IEEE 802.11 protocol to exploit flaws and to overload network devices. Dos attacks can be directed towards STA's as well as access points (AP) and in a wireless context it can be difficult to find the inducing source. Flooding [9] is similar to DOS attacks and involves sending large numbers of messages to an access point to avoid other STA's to access the wireless channel. This is a difficult security area which requires well founded security protocols to be established. In addition data flow control is required to detect abnormalities and to protect network devices.

2.4.2.10 RF Jamming attacks

RF jamming [9] involves using electromagnetic energy to interfere within the WLAN frequency area. Jamming intends to interrupt WLAN services and disturb communication. Jamming and radio disturbance may origin from deliberating or unconscious sources for example; neighbor WiFi networks, microwaves, wireless jamming products [65, 67] or other interfering radio systems. Jamming attacks are very difficult to handle and all type of radio networks are vulnerable to frequency disturbances. Wireless radio frequency (RF) control mechanisms and location services can potentially be used to locate jamming devices from where they can be physically removed.

Based on these attacks and vulnerabilities security protocols and mechanisms are required to meet the threats in order to establish reliable and secure wireless communication services. In the next section I will introduce WLAN security aspects and mechanisms related to access control, confidentiality and availability and take a closer look at protocol improvements that have been done to safeguard wireless networking.

2.5 *Overview of IEEE 802.11 WLAN security*

Security in wireless LAN's (WLAN's) have been discussed widely since the introduction of the IEEE 802.11 standard (Wi-Fi) in 1997 [8]. To improve security in wireless LANs, protocols like IEEE 802.1X and IEEE 802.11i has been proposed to provide access control and confidentiality respectively. In addition, availability aspects concerning WLAN networks have introduced several security challenges which for high assurance networks must be addressed. This section provides a brief historical overview of fundamental security protocols and mechanisms which intend to meet the threats and vulnerabilities as introduced in section 2.4. Access control introduces IEEE 802.1X, confidentiality introduces IEEE 802.11i, and availability introduces control, detection and protection facilities.

2.5.1 Access Control

The goal of access control [5] is to ensure that sensitive data can be accessed only by authorized users. The basic IEEE 802.11 specification defines two ways to identify wireless devices attempting to access WLANs resources; Open system authentication and Shared key authentication. IEEE 802.11 standard requires that the open system authentication is supported, while the shared key authentication is optional. The open system authentication mechanism identifies the following information:

- **Service Set Identifier (SSID) for the Access point**
  SSID is the specified identification name assigned to the WLAN. This name is broadcasted in over the air in clear text, and is used to distinguish different WLAN's.

- **Media Access Control (MAC) Address for the devices**
  MAC address [11] is a unique value associated with the network adapter. This value consists of 48 bits and is also known as the physical address assigned any network interface.

Open system authentication is basically a null authentication mechanism, and does not authenticate any device that connects to the AP. Therefore STAs have to trust communication based on the SSID. This can be misused easily and is no assurances for any identities. Shared key authentication is based on a secret cryptographic key, known as Wired Equivalent Privacy (WEP), which is considered as an extremely weak and flawed confidentiality mechanism [9].

A secret WEP key is shared between AP and STA on order to access the wireless network. Shared key authentication uses a simple challenge-response message to determine and authorize the STA. Each STA has to know the WEP key to be able to answer the challenge and thereby access the network. Shared key authentication is not a secure authentication because the AP can not decide if the STA is legitimate or not. Thereby, standard access control solutions for IEEE 802.11 networks are extremely vulnerable for exploitations. In other words, external access control mechanisms are needed to assure a secure authentication and association process.

In general there are three aspects of an authentication process [3]; access to the basestation, access to the wireless network and access to the local area network (LAN). Figure 9 show these challenges concerning secure wireless access control and access to wired LAN resources.

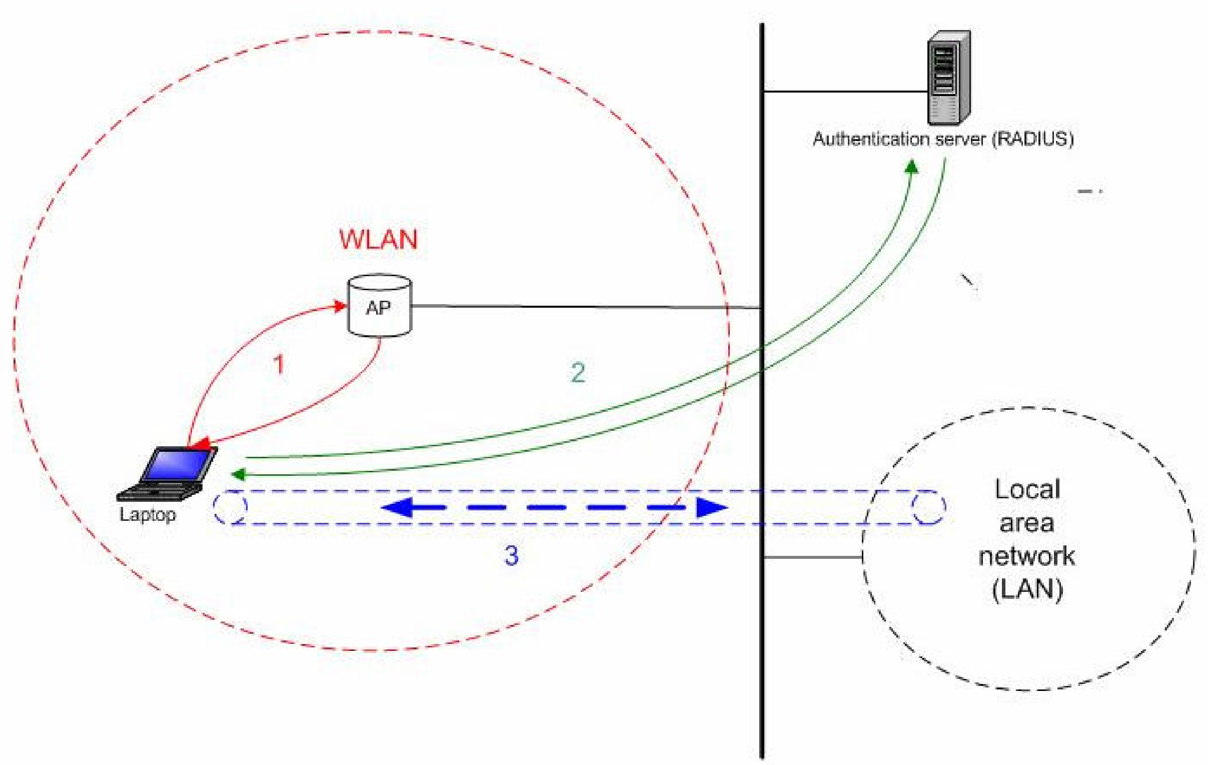


Figure 9: Wireless client authentication before it gains access to other LAN resources.

In order to ensure secure authentication the 802.11X standard has been purposed, offering port-based network access control. A port in this context is a single point off attachment in reaching the LAN infrastructure. As we can see from figure 9, a STA (laptop) requests WLAN access by probing the AP. The AP will ask for some STA identification, which the

STA has to return to the AP. The AP, which in this case acts as the authenticator, unpacks the message and forwards it to an authentication server (RADIUS). As session number 2 in figure 9 shows, the authentication server will decide if the STA is authorized to access and associate with the wireless network. During the authentication process only the authentication protocol is enabled for access, all other ports are closed. This means that after authorization a certain communication port will open up and allow the STA to establish a secure connection to distribution system (LAN area).

The authentication process as shown figure 9 may include use of various types of protocols. Different set of rules and algorithms can be established depending on the environment, the configuration and the level of security. To build a secure system it is important to analyze the user range, the protocols and the environment. Based on such evaluation and in relation to the requirements, the goal is to establish an appropriate solution. However, improper authentication can undermine all security measures. The IEEE 802.11X [9] standard is a general purpose and an extensible framework to authenticate user as well as distributions of cryptographic keys. Mainly there are two types of authentication schemes; *Pre-shared-key (PSK)* which is based on a shared secret, or using the *Extensible authentication protocol (EAP),* which makes it possible to authenticate user based on something you know (username/password etc.) or something you have (smartcard, certificate etc.). Using an EAP solution requires the authentication process to be closely evaluated, and there exists some EAP protocols that are considered insecure [9]. On the other hand EAP may be an effective way to authenticate users, especially for larger networks. Using a PSK authentication scheme requires more administration because each STA in the system needs to be continually aware of the shared secret. It is also possible to combine EAP and PSK in terms of enhanced security configurations. One main concernment is the question to allow some authentication messages to be sent in clear text or not. A PSK scheme could prevent this by providing a temporal encryption start key. Chapter 3 will discuss and analyze IEEE 802.1X standard and combinations of EAP protocol mechanisms to find potential access control mechanisms to be used for high assurance wireless networks.

2.5.2 Confidentiality and integrity

Confidentiality [13] involves how to ensure that transmitted data can be received and understood only by the intended and the authorized audience, whereas integrity [10] intends to prohibit unauthorized writing. Confidentiality is often associated with encryption technologies by hiding information using cryptographic keys with cryptographic algorithms. Integrity is often familiar with cryptographic hash functions, which intents to produce an irreversible cryptographic checksum [10] to verify changes to transferred data. As mentioned in section 2.5.1 the IEEE 802.11 standard defines the WEP protocol to ensure user confidentiality and integrity for over-the-air data transmission. The WEP protocol uses a RC4 stream cipher algorithm [10], which is remarkably simple. Basically the RC4 algorithm consists of a look up table containing permutations of a 256 byte value. An initialization vector (IV) of 24 bit is used to initialize the cryptographic stream key. Based on the IV, which unfortunately is sent over the air in clear text, enables the basic starting point of the data encryption phase. This encryption scheme is vulnerable because an eavesdropper, by the advance of the initialization vector, can monitor the network and analyze a relative small amount of data to recover the key. To ensure integrity to messages transmitted, the IEEE 802.11 standard suggests the use of a 32 bit cyclic redundancy check (CRC-32). CRC-32 [14] is a binary check sum which consists of a data calculation before and after transmission. Basically CRC is particular good at detecting common errors caused by noise added during transmission. As an integrity check CRC-32 is a pore solution because attackers that monitor the wireless network can easily change both the message and the CRC-32 checksum to order to change data without being detected. In other words the standard IEEE 802.11 protocol does not include any secure confidentiality solutions for over-the-air transmission. To improve this we need to add new cryptographic algorithms and integrity mechanisms that are capable of securing the amount of data being transported.

2.5.2.1 Robust Security Networks (RSN)

The IEEE 802.11i [3, 9] standard introduces a new baseline for confidentiality and integrity in wireless networks. The IEEE 802.11i standard was ratified in June 2004 introducing new mechanisms to fix all WEP weaknesses, and propose a security configuration which appeals to Robust Security Networks (RSN) [9] configurations. The IEEE 802.11i standard defines three basic elements to enhance security in wireless networks.

- Temporary Key Integrity protocol (TKIP)
- Counter Mode with the CBC-MAC protocol (CCMP)
- 802.11X port based network access control configuration

TKIP is basically an improvement of the WEP protocol and the RC4 algorithm. The intention is to increase confidentiality and integrity without requiring new hardware replacement. Among other things TKIP introduces a pr frame encryption key change and a new message integrity code (MIC) which is fundamental security improvements. On the other hand TKIP protocol has revealed some weak points [9] that under some conditions may be easily exploited by an attacker, as shown in the following video [50].

The Counter Mode with Cipher Block Chaining Message Authentication Code protocol (CCMP) is a new confidentiality and integrity framework which requires new hardware both for access points (AP) and for stations (STA's). The CCMP protocol introduces a "generic authenticated encryption block chipper mode“ [9] of the Advanced Encryption Standard (AES) that combines two well known and founded cryptographic techniques to provide robust confidentiality, integrity and authenticity. The Counter mode (CRT) is used for integrity and the CBC-MAC protocol are used both for integrity and message authentication (Authenticity). The CCMP protocol is considered to be the most secure low layered protocol solution for use in WLAN.

The IEEE 802.11i uses 802.11X (EAP protocol) to provide mutual authentication between STA's and the WLAN infrastructure. The IEEE 802.11i introduces some techniques from the internet protocol security (IPSec) standard (see section 2.6) and generates cryptographic checksums based on a hash message authentication code (HMAC) [9]. Figure 10 shows an overview of basic IEEE 802.11 security and 802.11i (RSN) security.

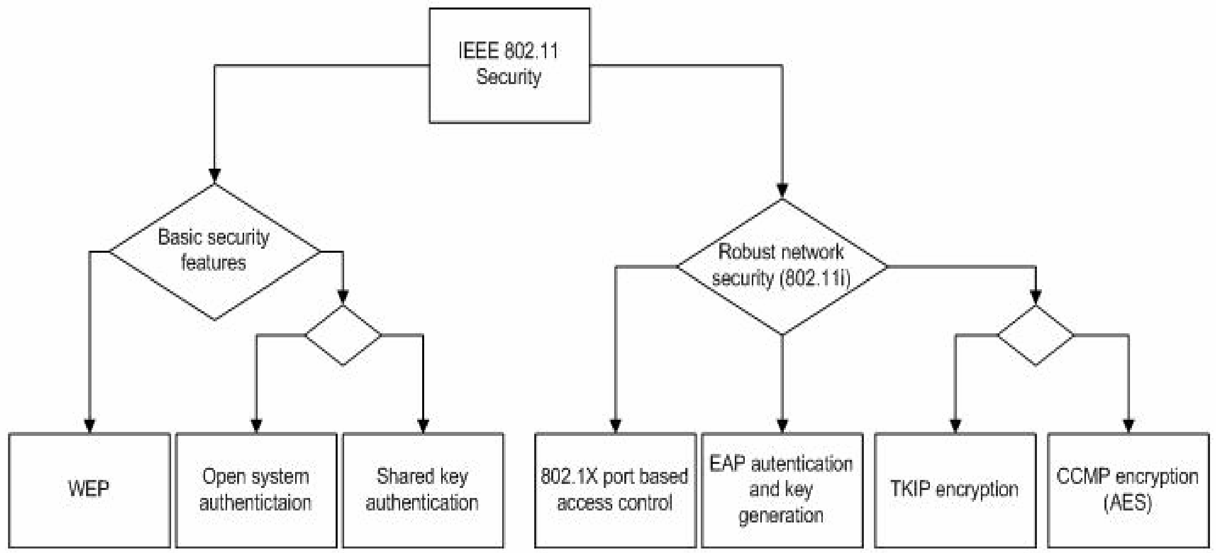

IEEE 802.11 Security
Basic security features
Robust network security (802.11i)
WEP
Open system authentictaion
Shared key authentication
802.1X port based access control
EAP autentication and key generation
TKIP encryption
CCMP encryption (AES)

Figure 10: Overview of 802.11 security protocol configurations

As mentioned, the IEEE 802.11i standard introduces the concept of Robust Security Network (RSN) [9], which is also referred to as the WPA2 standard. The RSN allows a creation of Robust Security Network Association (RSNA) which is a security relationship established trough a 4-way handshake process. This 4-way handshake protocol requires the entities to possess a Pairwise Master Key (PMK), and is responsible to confirm ciphers suits and temporal key distributions. The 4-Way handshake will be closely described in chapter 4. The RSNA [9] enables the following features of robust WLAN security:

- Enhanced user authentication mechanisms
- Cryptographic key management
- Data confidentiality
- Data authenticity and integrity
- Replay protection

To achieve robust security the 802.11i standard introduces numbers of cryptographic algorithms and techniques. These algorithms can be categorized to solve different security problems to ensure confidentiality and integrity in wireless networks.

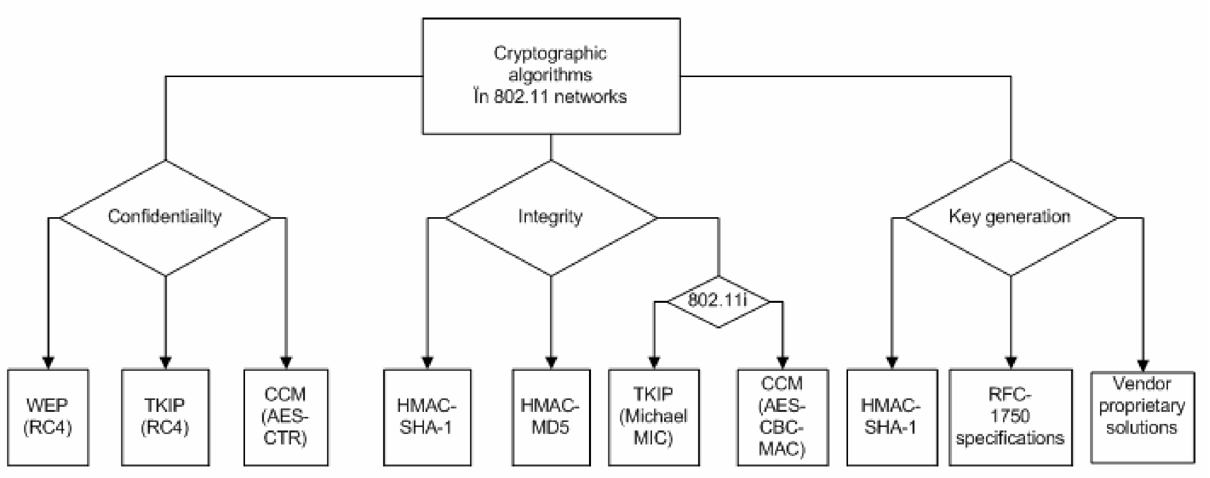


Figure 11: Cryptograpic algorithms used in IEEE 802.11 networks

Figure 11 shows some of the amendment referred to IEEE 802.11i cryptographic algorithms. The keyed-hash message authentication code (HMAC) [52] is widely used to provide integrity and confidentiality solutions. HMAC is a cryptographic hash function which calculates a message authentication code in combination with a secret key. In other words, HMAC can be used to both verify data integrity and to ensure message authenticity. To calculate a HMAC the SHA-1 algorithm [52] can be used. The Secure Hash algorithm (SHA) is a public announced and FIPS approved algorithm which with a high degree of probability produces a unique value of given data input. Referred to [53] the SHA-1 algorithm has not been broken or compromised. The HMAC-MD5 algorithm is a hash function which is very similar to the SHA-1. The major practical difference is that MD5 [10] produces a 128-bit output, whereas SHA-1 produces a 180-bit output. According to [10, 53] MD5 is not longer considered secure because collisions have been found, which indicates that the algorithm is possible to break. Referred to figure 11, not all available and used cryptographic algorithms are shown. For example other key generation algorithms using the EAP protocol may be implemented for particular solutions. Referred to RFC-1750 [51], which discusses the generation of randomness related to key establishment, key generation techniques are extremely important elements in building confidentiality and integrity solutions, especially for wireless networks. In chapter 4 I will discuss confidentiality, integrity and key generation mechanisms more in detail.

The IEEE 802.11i standard suggest to combine CCMP, using AES-CRT and AES CBC_MAC together with the 802.11X protocol to increase robustness and security in wireless networks. RSN and 802.11i are interesting and promising approaches to build secure wireless solutions. In chapter 4 I will continue the discussion security improvements of the RSN and the IEEE 802.11i standards, focusing on the CCMP encryption and integrity mechanisms.

2.5.2.2 Cryptographic key hierarchies, generation and key management

Cryptographic keys are used to provide confidentiality, integrity and authenticity. This means that cryptographic keys are used in both the authentication process (IEEE 802.1X) and in the confidentiality process (IEEE 802.11i). Consequently a hierarchy of cryptographic keys arises and a subsequent process to handle and control the keys is required. This process is called key management [9] which is responsible for handling the keys and related materials during the key component lifetime including generating, distributing, storing and destroying. Since cryptography is a security foundation, it is essential to keep the keys concealed from outsiders. Therefore keys needs to be protected and ensured to prevent the security configuration form being compromised. The IEEE 802.11i standard introduces two types of hierarchies to handle and safeguard the key management system. The first key hierarchy is the Pairwise Key Hierarchy as shown in figure 12, which organizes a key structure indenting to protect unicast data traffic. The second key hierarchy is the Group Key Hierarchy which is used to protect multicast and broadcast data exchange. As we can se from figure 12, there are two fundamental keys on top of the hierarchy, a pre-shared key (PSK) and an Authentication, Authorization and Accounting key (AAAK), also referred to as the *root keys* [9]. PSK is a static key which must be in place at the STA before a connection to the AP can be established. The PSK can be manually distributed through USB devices or smartcards, or generated and installed using public key cryptographic [63] approaches. The AAA key, also known as the Master Session Key (MSK), is used to authenticate and authorize the STA and the AP in order to establish an RSNA connection. A centralized RADIUS server is used to perform the approvals. The AAA key is a session key delivered through the EAP protocol, and the key changes each time the STA has to reauthenticate. The AAA key is generated and installed using the EAP mechanisms, which will be closer described and discussed in chapter 3.

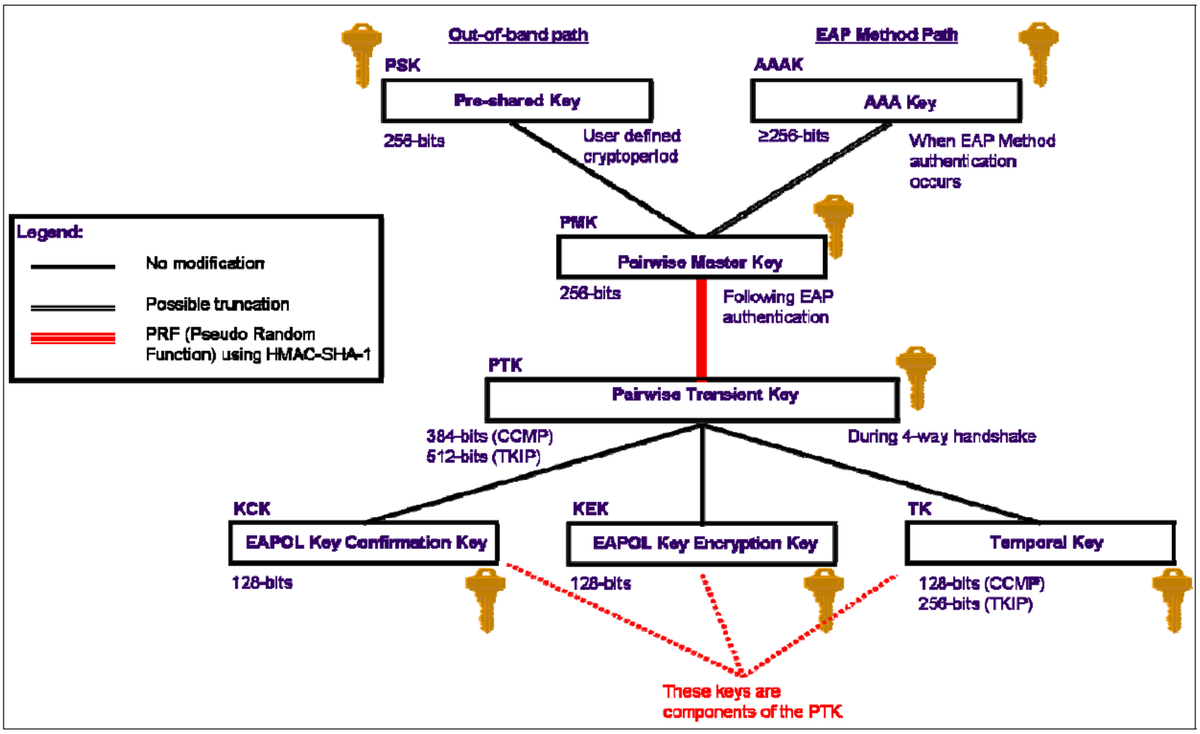


Figure 12: IEEE 802.11i pairwies key hierarchy[[9]

The PSK and the AAAK, are both required to provide additional keys in order ensure several of the confidentiality and integrity protections processes. As we can see from figure 12, the PSK and AAAK inputs and formulates the Pairwise Master Key (PMK) which is generally a key-generation key used for the derivation of the Pairwise Transient Key (PTK). A pseudo random function (PRF) using the HMAC-SHA-1 is used to generated PTK. The PTK inputs are based on the PMK, the STA identity (MAC address), and a random nonce which suppose to prevent outsiders from calculating the key. The PTK is composed with three different important keys. The EAP over LAN Key Confirmation Key (EAPOL-KCK) are used to provide confidentiality and integrity to the IEEE 802.11 control frames which is used to establish and setup IEEE 802.11i connections. The EAPOL Key encryption Key (EAPOL-KEK) is used to protect cryptographic keys and other RSNA materials. The Temopral Key (TK) is used to protect particular data transmission and user traffic. Table 3, shows a summary of cryptographic keys that will be closer discussed in chapter 3 and 4.

Key name	Description	Purpose	Bit-size	Key-type
AAAK (MSK)	Authentication, Authorization and Accounting key, the Master Session Key	Used for the 802.1X authentication and authorization. Derives the PMK.	≥256	Root key and key generation
PSK	Pre-shared Key	Key is required to establish AP connection. Used to derive the PMK:	256	Root key and key generation
PMK	Pairwise Master Key	Master key generated from PSK and AAAK. Used with other inputs to derive the PTK	265	Key generation key
GMK	Group Master Key	Same as PMK, used in multicast and broadcast network transmissions	128	Key generation key
PTK	Pairwise Transient Key	Generated from PMK and comprises the EAPOL-KCK and EAPOL-KEK and TK	512 (TKIP) 384 CCMP)	Composite key

TK	Temporal Key	Used with the CCMP or the TKIP algorithm provide confidentiality and integrity protection	256 (TKIP) 128 (CCMP)	Traffic key
GTK	Group Temporal Key	Generated from GMK. Same as TK but used in multicast/broadcast networks.	256 (TKIP) 128 (CCMP)	Traffic key
MIC key	Message Integrity Code Key	Used by TKIP to provide message integrity protection using a Michael MIC	64	Message integrity key
EAPOL-KCK	EAPOL Key Confimation Key	Used to provide integrity protection for control frames data distributed during the 4-Way Handshake	128	Message integrity key
EAPOL-KEK	EAPOL Key Encrytion Key	Used to ensure confidentiality for other key material distributed	128	Encryption/traffic key

Table 3: IEEE 802.11i keys [9] used for confidentiality, integrity and authenticity

2.5.3 Availability

Access control, confidentiality and integrity are all very important aspects in developing secure wireless communication systems. On the other hand such mechanisms and implementations are not enough to safeguard and control a wireless LAN environment. Availability has two major concerns, one which includes the fact that system equipment, protocols and technology are available to outsiders and possible attackers; another concern is the network and the signals which are available for authorized users as well as unauthorized user. Because of the availability aspects there are several obvious threats and vulnerabilities to a WLAN infrastructure. Some of these wireless threats, as described in section 2.4, can be met through secure access control solutions and cryptographic technology, as introduced in section 2.5.1 and 2.5.2. If we look at the different threats from section 2.5 we may conclude that not all the vulnerabilities and threats can be addressed. Examples are denial of service (DOS) and flooding attacks, which potentially can turn down AP's or STA's in order to degrade network performance. Other typical threats which can not be handled are the presence of rogue devices that infiltrates the network area, and jamming which interferes with WLAN frequencies. To meet these vulnerabilities we need to implement a set of security tools that can observe and supervise the wireless environment and report if some undesirable situations occur. At the same time the observation system must be able to respond to sudden occurrences, attacks and threats that emerge. In other words, it is required to add "environmental control" and mechanisms that are capable to monitor, control, detect and protect the wireless environment against intruders and suspicious behavior.

2.5.3.1 Wireless environmental control using wireless sensor devices

Wireless environmental control involves the ability to observe and guard the wireless network to increase trust and to give administrators the opportunity to reveal irregularities. A wireless monitor system which implements passive and active sensor devices may potentially supervise and protect the wireless network. The sensor target is to capture PHY/MAC frames and transmit them to a detection system. Figure 13 shows an overview of a monitoring system architecture implemented using wireless sensor devices (monitor Access Points).

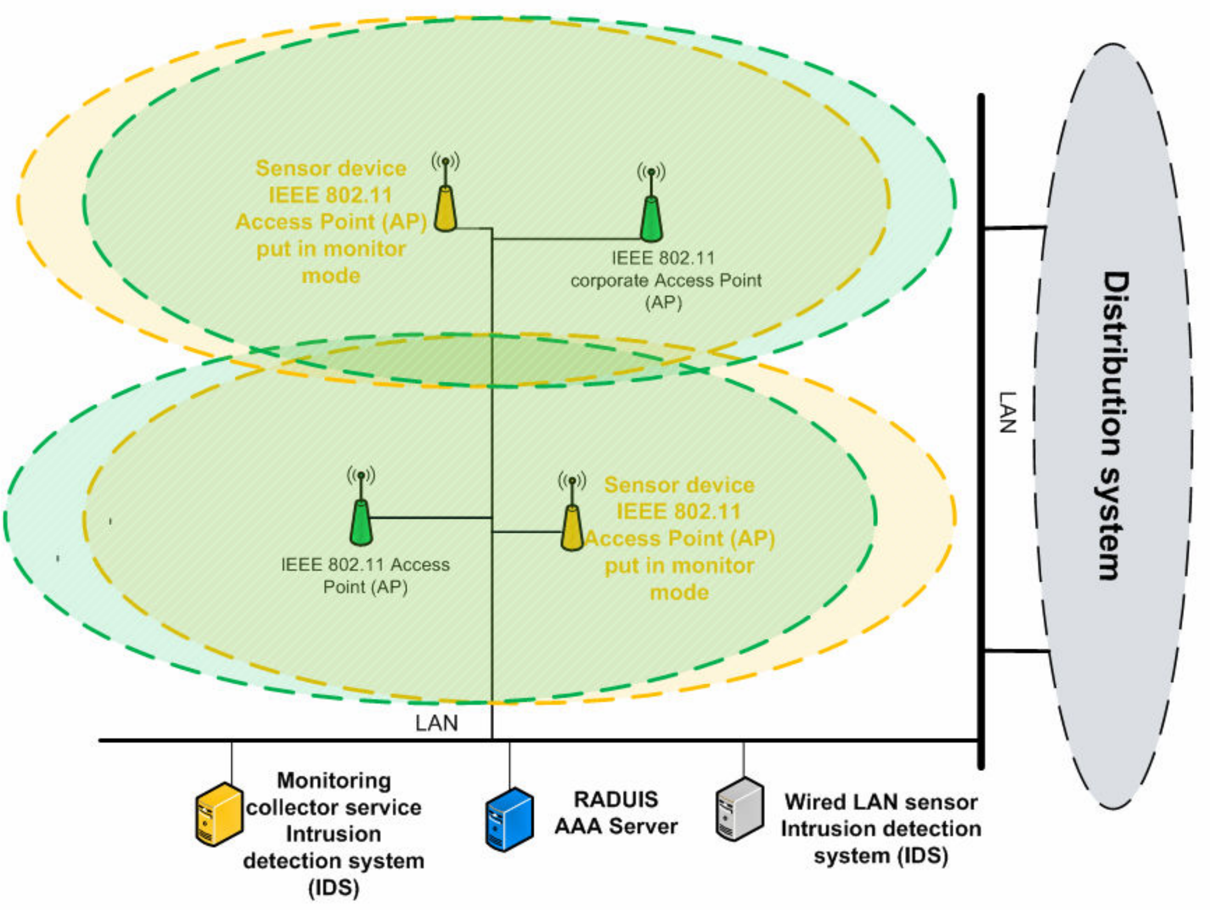


Figure 13: WLAN monitoring system principal architecture

Based on a wireless monitoring system, intrusion detection technology [72] can be implemented to detect unwanted wireless activity. Such activity can be unauthorized devices that intend to connect and access the network, emerging rogue devices (AP/STA), denial of service attacks, flooding attacks or simply disturbance/interruptions that affect the wireless network performance. Research [73, 74, 75] has concluded that wireless sensor based systems have many potential goals that could increase security for enterprise wireless solutions, especially for high assurance wireless environments. Wireless monitoring and capability aspects will be presented and discussed in chapter 5. As introduced in [75], a wireless monitor system can be used for active protection of the wireless network. This is a complicated problem scenario because physical aspects of the IEEE 802.11 protocol make it relatively easy to destroy wireless connectivity. In chapter 5 the thesis will look into and discuss protection mechanisms and models which have potential options to meet some of these vulnerabilities.

2.5.4 Summary of WLAN security challenges

As introduced in section 2.5.1, 2.5.2 and 2.5.3, fairly complicated security protocols has been adapted to meet security threats in order to apply high-end security requirements for wireless networks. To summarize the security prospectives, figure 14 shows an overview of security challenges associated with WLAN's. This scenario encircles the implementation of a wireless network, based on the IEEE 802.11 technology, which provides access to a high assurance classified information network.

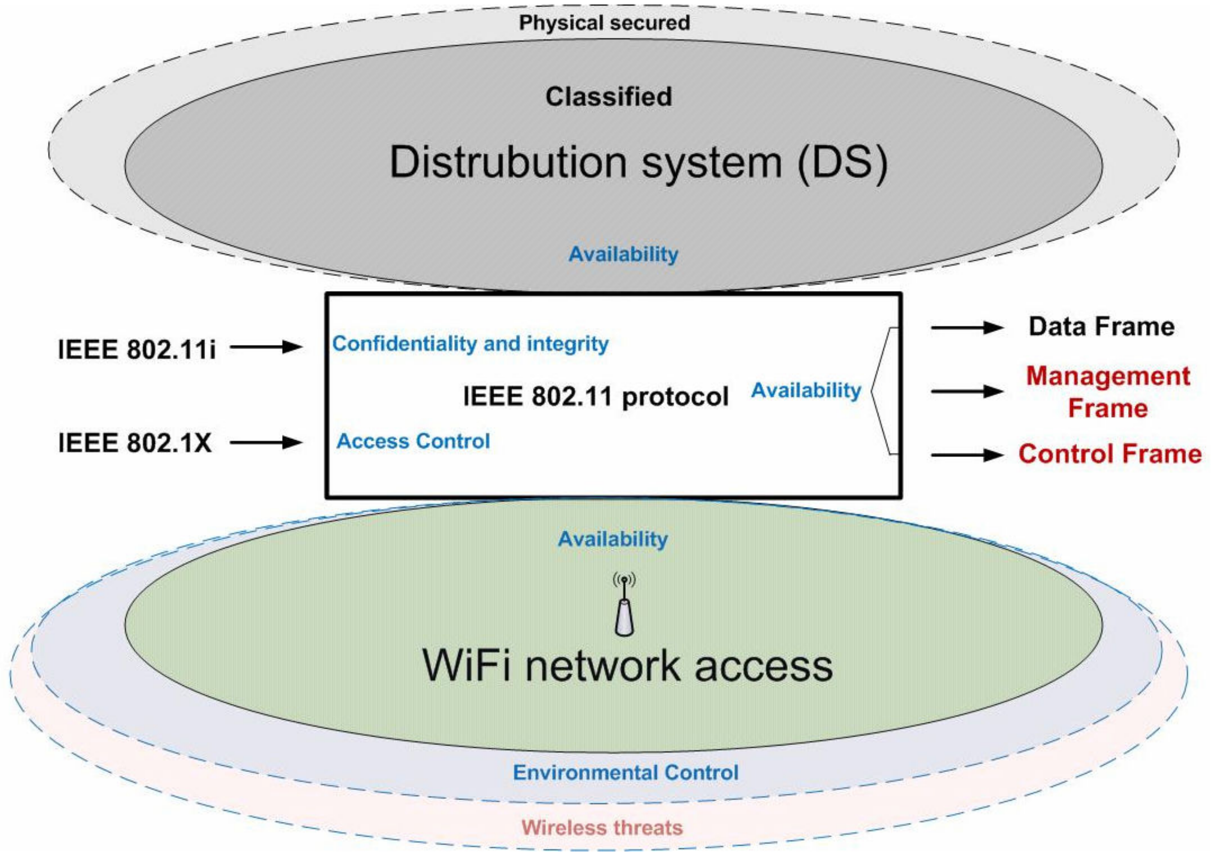


Figure 14: The IEEE 802.11 protocol and security challenges

As shown in figure 14, the IEEE 802.11 protocol system operates as a link-layer forwarder which exchanges OSI-link layer packets between the WiFi network and the DS. To safeguard the wireless link we must implement security protocols, such as IEEE 802.1X and IEEE 802.11i, which inserts access control mechanisms and confidentiality/integrity technology. Management and control frames are marked in red because these frames are not protected by the IEEE 802.11i security settlement. Because of the wireless availability aspects there are challenges connected to the WiFi radio access availability, which means that the WLAN network must be controlled and protected against a wide range of wireless threats. As shown in figure 14, mechanisms for "environmental control" are required to oblige and cover the different wireless threats and vulnerabilities which can not be achieved by implementing 802.1X and 802.11i mechanisms.

2.6 *VPN/IPsec for network-layer security*

VPN/IPSec is not a part of the 802.11 protocol but can be used to provide confidentiality and integrity to wireless data transmissions. VPN and IPsec are methods and mechanisms that can add network layer (OSI-layer 3) securities to the data transfer. VPN and IPsec are well founded and established mechanism that can be used in wireless networks as well as wired LAN environments. The main advantage is that layer 3 provides end-to-end security between sender and recipient. As case 1 in section 1.4.1.1 describes, IPsec ESP can be used to provide confidentiality and integrity, transparently independent of transmission media. In the following section we will shortly describe the main functionality of using VPN/IPsec solutions in WiFi networks.

2.6.1 IPsec in wireless networks

IPsec is an open standard framework [10, 61] which operates on the network layer (layer 3). In IEEE 802.11 networks, IPsec can be used to provide confidentiality, authenticity and integrity to data packets transferred over the wireless network. The major advantage of the IPsec protocol is that it’s transparent to applications and devices as well as access points (AP), stations (STA’s) and the wireless environment. This means that an IPsec solution can provide IP end-to-end security on the network layer compared to CCMP which only can handle the wireless environment and provide security between two entities on the data link (OSI layer 2) level.

2.6.1.1 IPsec ESP

IPsec ESP is one of several IPsec security protocols protecting IP network communication services. The encapsulating security payload (ESP) is a security protocol which combined with IPsec can provide confidentiality, authenticity and integrity to the IP packet. ESP can operate in two different modes; transport mode or tunnel mode. In transport mode the ESP header is placed between the IP header and the data-field and provides confidentiality to the transported data only. In tunnel mode, ESP encrypts the entire IP packet and creates a new IP header for each new packet, signifying that the original header is no longer visible for outsiders. This is particular valuable if tunnel mode is used between to firewalls, because outsiders monitoring the network can not see which hosts are communicating. A disadvantage of the ESP tunnel mode solution is increased overhead for additional IP headers, which in a wireless context will degrade throughput performance.

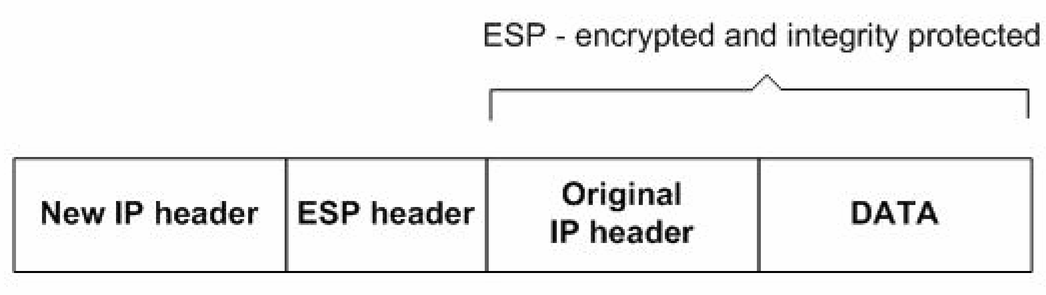


Figure 15: IPsec ESP tunnel mode

The ESP encryption process offers symmetric block cipher encryption [62] base on the Advanced Encryption Standard (AES). ESP uses AES-CBC and AES-CTR algorithms, which are similar to the CCMP protocol, or alternatively Triple DES (3DES) encryption.

2.6.2 Virtual Private Network (VPN)

VPN [62] is a virtual network integrated on top of an existing network providing secure communication channels for IP packets transmitted over unsecured networks.

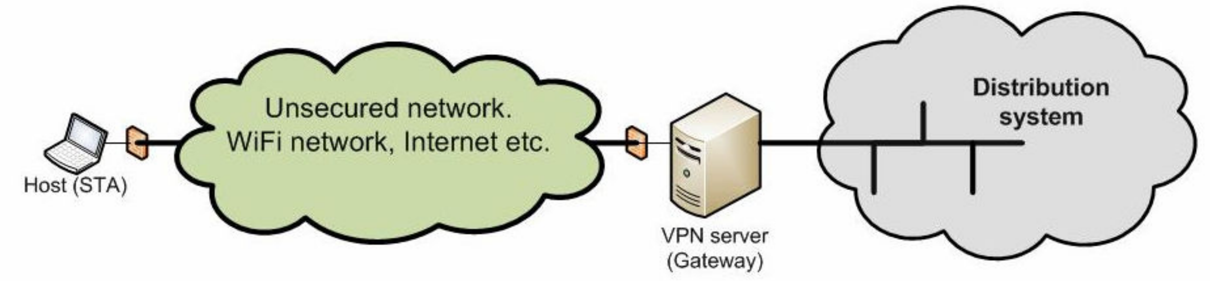


Figure 16: VPN host-gateway configuration

VPN renders three types of architectures; a host-to-gateway architecture as shown in figure 16, a gateway-to-gateway architecture and a host-to-host architecture. A host-to-gateway solution is especially adapted for use in wireless IEEE 802.11 networks, where stations (STA) authenticates and operates towards a VPN gateway server. Implementing IPsec with VPN involves using both symmetric and asymmetric cryptography. Asymmetric crypto, also known as public key crypto [63], is used to authenticate both parties (host and VPN-gateway), and symmetric crypto is used to ensure confidentiality and integrity for transported data packets.

3 Access control based on IEEE 802.1X

This chapter will focus on access control and authentication mechanism to intending to provide secure access to a high assurance wireless network. The wireless network is based on the IEEE 802.11 standard protocol and by employing the concept of Robust Network Security (RSN), I will investigate the standardized port-based protocol IEEE 802.1X together with the extensible authentication protocol (EAP). Furthermore I will introduce and discuss access control mechanisms, security issues and architectural requirements according to implement a best practice access control configuration. RSN networks do not specify or predefine wireless security configurations and leaves implementation issues to supplier and customers to find appropriate solutions based on stated requirements. This chapter will mainly cover two important aspects of access control which considers the discovery phase and the authentication phase [9, 23, 41, 42], where the objective is to security map authorized STA's to access the wireless network. Chapter 4 will cover the key management phase, the data protection phase and the termination phase.

3.1 Access control operations

First of all I will start this chapter by introducing the general frame exchange model represented by Robust Security Networks (RSN) described in [9]. RSN operations occur in five different phases, where some of the phases are familiar with the general standard IEEE 802.11 association process described in section 2.3.3. The goal of the five phases is to securely map and interconnect authorized STAs to the WLAN network and furthermore associated the STA's with the distribution system and computer networks connected to the wired LAN environment. Figure 17 shows the five operational phases. The network association process is basically split into two parts, where the first part is a network association phase with the wireless IEEE 802.11 network, providing access to the local wired LAN infrastructure. The second part is STA association process with the local distribution systems, which requires the STA to authenticate and associate with high assurance classified application services and data systems. That phase is out of the scope of this thesis and will not be covered in this document. The following chapter will present the discovery phase and the authentication phase.

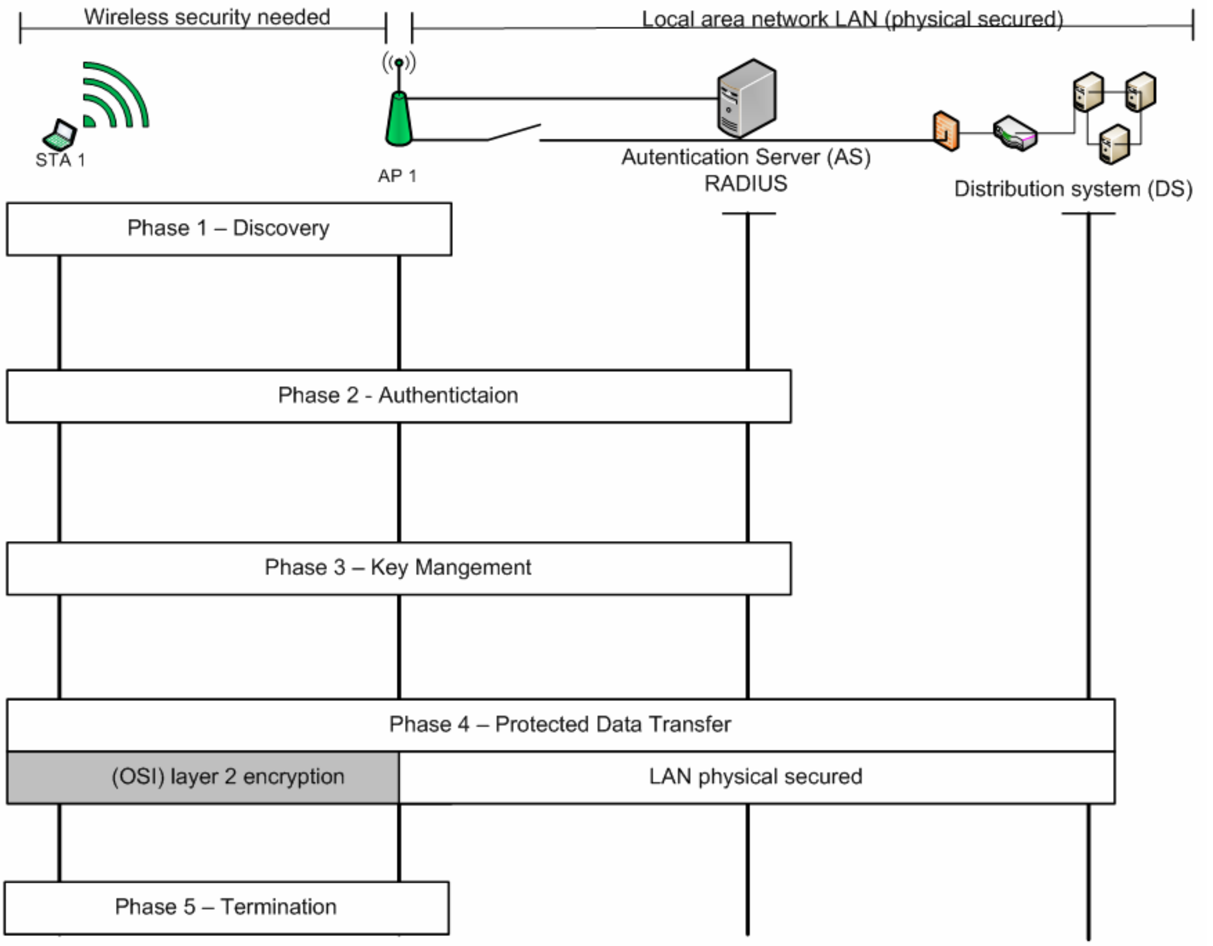


Figure 17: The RSN association process

- **Phase 1: Discovery.** The access point (AP) and STA's use beacons signals and probe request to announce their existence and to communicate the security policy.
- **Phase 2: Authentication.** The authentication process requires that both STA and the authentication server (AS) prove their identities to each other. The AP blocks all STA traffic except from authentication transactions. The AP does not participate in the authentication process except from forwarding authentication messages between STA's and the AS.
- **Phase 3: Key Management.** AP and STAs performs operations which generate, distribute and handle cryptographic keys, as described in chapter 2. The key exchange frames are exchanged between STA and the corresponding AP only, and uses the EAP protocol for protection. This phase will be handled in chapter 4.
- **Phase 4: Protected Data Transfer.** To protect the data frames being exchanged between STA and AP, cryptographic algorithms provides secure wireless data transfer. An important signification is that security is only insured for wireless traffic and not

end-to-end. This phase will be described and handled in chapter 4.

- **Phase 5: Connection termination.** This phase occurs when the wireless connection is terminated. This involves that the termination process should restore to the initial state. This phase will be described in chapter 4.

3.1.1 The discovery phase

The first stage of the discovery phase is when the STA discovers the wireless network and initiates contact with access point (AP). To locate the AP, the STA listens to beacon frames which are periodically is broadcasted by the AP to communicate its network identity. The Beacon frame contains a timestamp, a beacon interval, supported data rates, and a service set identifier (SSID). To distinguish different AP's within the same radio coverage area, the STA conducts to the SSID configuration. This indicates that the first initial conversation-request performed by STA's, depends on the reliability and the trust of the beacon SSID broadcast message. In other words, a STA will automatically try to associate with a wireless network operating on an approved SSID identity.

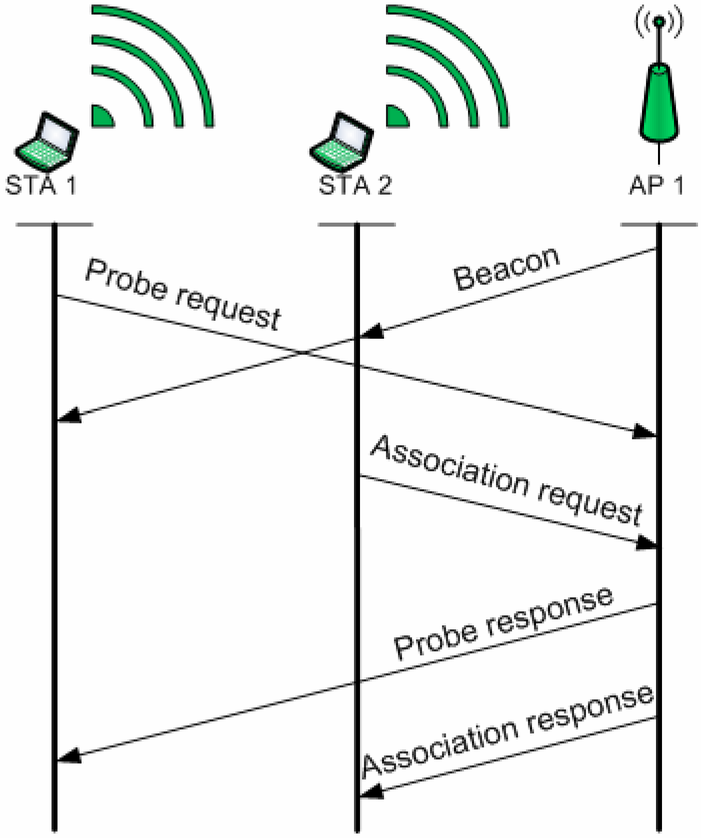
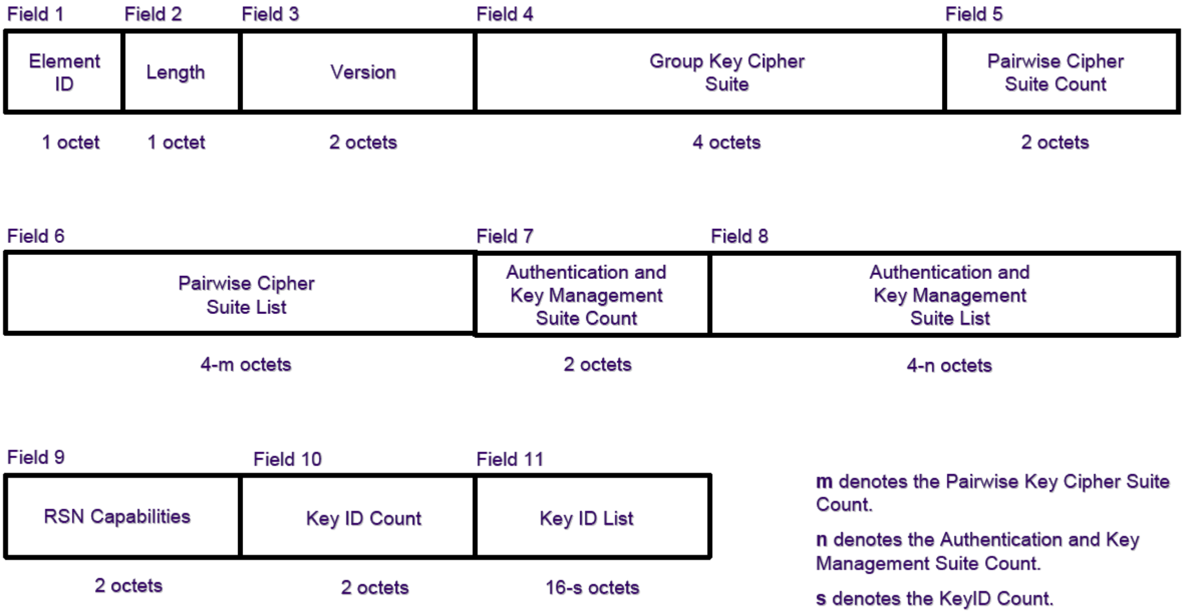


Figure 18: The discovery phase

During the discovery phase the STA and the AP exchange and negotiate physical-layer (OSI-layer one) technical prospects to be able to establish a reliable communication channel. This is prospects related to radio communication parameters, modulation schemes, coding, channel settings etc. To be able to establish a secure connection between the STA and the AP, it is necessary to negotiate security configuration data, informing each party what type of security setup that should be established. This security exchange implies informing the AP and the STA about available security capabilities and supported security functionalities, such as authentication methods, confidentiality protocols, key management and integrity protocols. As described in [9], the security capability broadcast message includes a RSN information element, which is part of the AP's beacon broadcast and the STA's probe request frame.



m denotes the Pairwise Key Cipher Suite Count.

n denotes the Authentication and Key Management Suite Count.

s denotes the KeyID Count.

Figure 19: RSN information element (RSNIE) [9]

As shown in figure 19, the Robust Security Network Information Element (RSNIE) fields conveys and informs STA's about required security settings, which includes required key cipher suites, authentication and key management suites and other security capabilities. The STA will have to meet the security claims to be able to authenticate with the AP and wireless network. In figure 20, the discovery frame sequence is shown, demonstrating the AP and STA association process before authentication. This phase is vulnerable because neither the STA nor the AP is able to confirm the other parts identity. This signifies that message between AP and STA are based on simple trust. The STA requests to connect to the preferred SSID network and the AP which match the SSID probe request will respond. Furthermore, the STA and AP will go through a null authentication process (open system authentication described in section 2.5.1) as shown in figure 20. This authentication process simply maps the two wireless entities according to the 802.11 state machine described in section 2.3.3, to maintain backward compatibility to the with IEEE 802.11 hardware [9]. The STA will then try to associate with the AP and wireless network by satisfying the claims and the selected security mechanisms and parameters. If the STA can not meet the security claims requested, the AP will automatically refuse the association request and block the STA communication based on the MAC address. The STA will also block the AP, in case of a rough access point, or if the AP do not meet the STA security requirements.

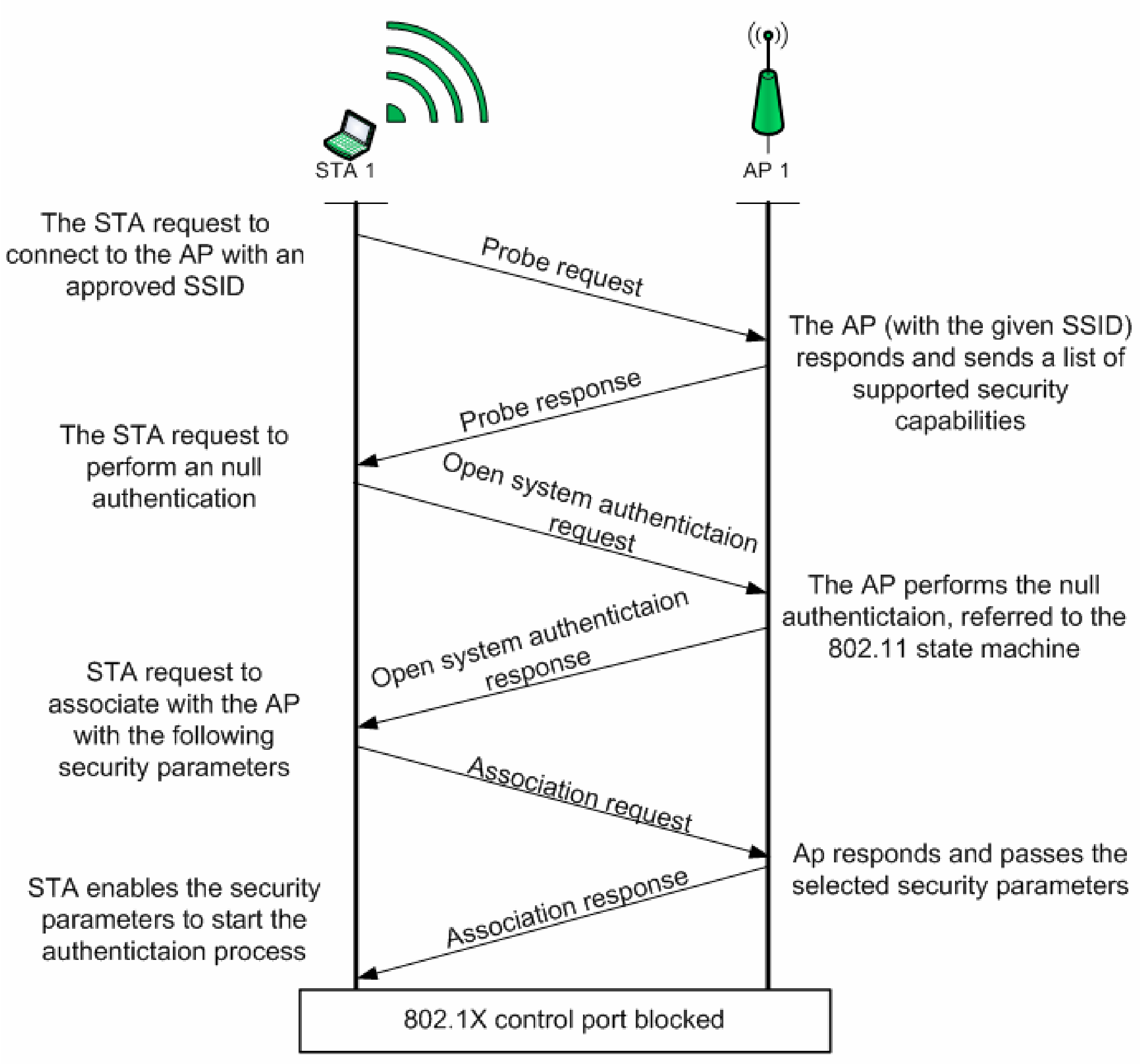

STA 1
AP 1
The STA request to connect to the AP with an approved SSID
Probe request
The AP (with the given SSID) responds and sends a list of supported security capabilities
Probe response
The STA request to perform an null authentication
Open system authentictaion request
The AP performs the null authentictaion, referred to the 802.11 state machine
Open system authentictaion response
STA request to associate with the AP with the following security parameters
Association request
Ap responds and passes the selected security parameters
Association response
STA enables the security parameters to start the authentictaion process
802.1X control port blocked

Figure 20: The discovery frame sequence process before 802.1X authentication

We may already conclude that the security configuration policy enabled within the wireless environment is available for anyone monitoring the network. Based on the IEEE 802.11 standard it is not possible to hide security configuration, and any outsiders within the wireless covering area can passively monitor AP beacon frames to map the security policy and parameters. It is possible, as shown in figure 18, to turn of AP beacon broadcasting, but the probe-request and probe-response exchange advertises the same security information for entities monitoring the network. A wireless network configured for RSN, IEEE 802.1X for authentication and AES-CCMP for unicast and broadcast traffic, will automatically refuse to communicate with STA's or AP that cannot meet the security configuration policy. Even though this is not a particular increasing security factor which certainly demonstrates that security algorithms, cryptographic mechanisms and key-management is the key to establish a safe and secure wireless network. Although, every STA and AP within a RSN network has to accomplish an authentication process before they can associate with wireless network. As figure 20 indicates, the 802.1X control port is closed until the STA can meet the security requirements. Based on the STA security conditions the AP will open up the 802.1X uncontrolled port, permitting the STA to start the authentication phase.

3.1.2 The authentication phase

After succeeding the discovery phase the STA and the AP enters the authentication phase. According to an RSN configuration, the AP does not participate during the authentication process, but only forwards frames and is responsible to open a communication port to allow the STA to exchange authentication frames with an authentication server (AS). The AS and STA has to prove their identity before the AP will allow other traffic and access to WLAN/LAN resources.

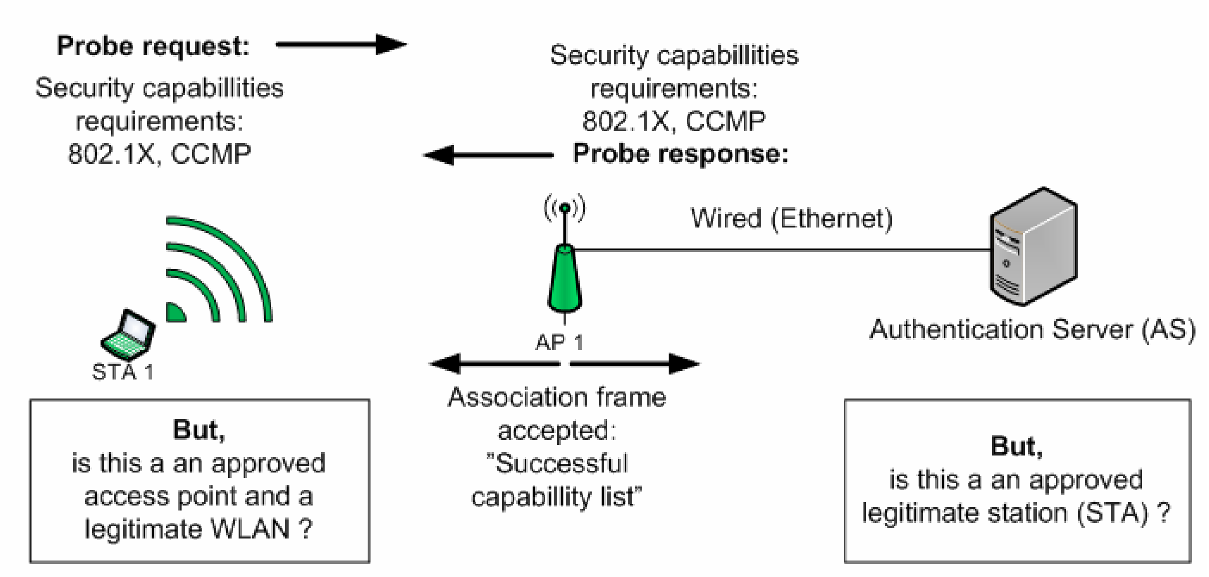

Probe request:
Security capabillities requirements: 802.1X, CCMP
Security capabillities requirements: 802.1X, CCMP
Probe response:
Wired (Ethernet)
STA 1
AP 1
Authentication Server (AS)
Association frame accepted: "Successful capabillity list"
But, is this a an approved access point and a legitimate WLAN ?
But, is this a an approved legitimate station (STA) ?

Figure 21 : Authentication phase

The authentication phase is a security critical process which supposes to prevent unauthorized STA's and AP's from accessing the wireless network. During the discovery phase the STA and the AP can not resolve if the other part is legitimate or not. Therefore the authentication process is extremely important, and improper authentication mechanisms may undermine the overall security.

3.1.2.1 IEEE 802.1X framework and concepts

As mentioned in section 2.4.1, the IEEE 802.11 standard uses the IEEE 802.1X frame work to provide secure network access control. As described in [54, 9], he IEEE 802.1X standard is an extensible frame work, which uses port-based network access control mechanisms to carry through the authentication and authorization process of wireless network devices. The IEEE 802.1X allow a STA to communicate via an authenticator (AP) trough a single point-to-point connection, preventing access to all other logical ports except those used for authentication services. As shown in figure 22, the authentication server is usually placed in the wired LAN environment, and communicates with the STA through a single AP authentication port (Uncontrolled Port).

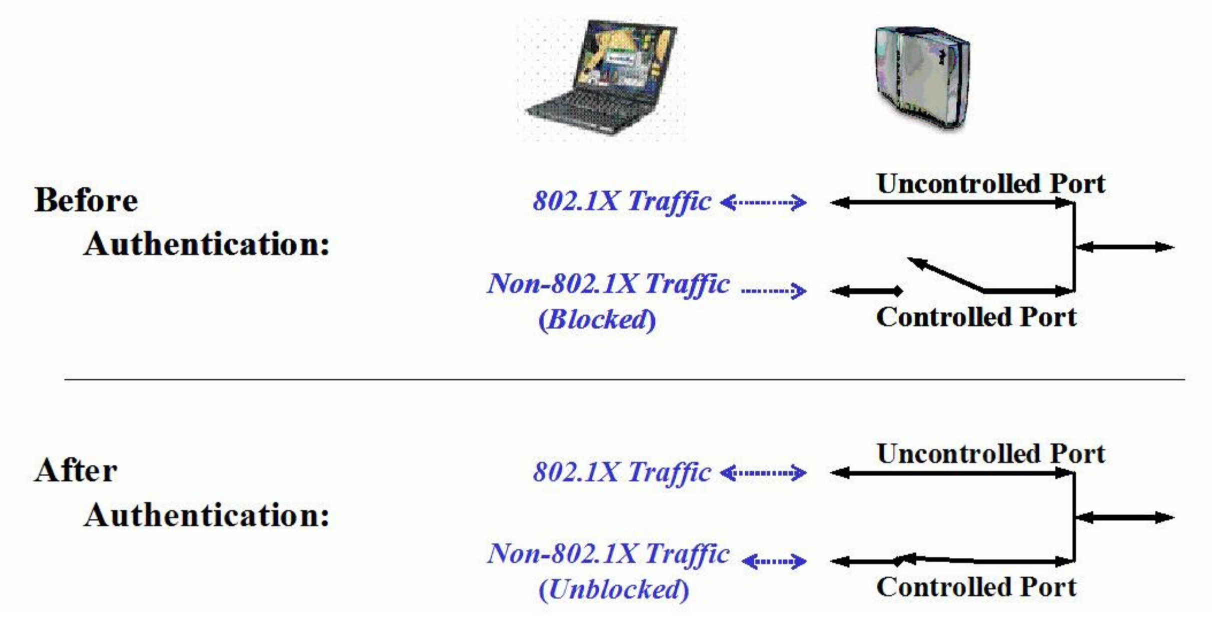


Figure 22: IEEE 802.1X port based access control modell, used in 802.11 networks [55]

The uncontrolled port as shown in figure 22, allows IEEE 802.1X traffic to be exchanged, and of the result from the mutual authentication process, the STA and AS set their controlled port to either authorized or unauthorized state. As explained in [54], the IEEE 802.1X standard provides an own protocol to exchanging authentication credentials. Depending on the outcome of this protocol, and the control state of both STA and AS, and the authenticator

(AP) determines to open the controlled port. On the other side the 802.1X protocol does not specify any authentication mechanisms or authentication decision method. This is left to vendors and system suppliers to implement secure methods which exchanges authentication data. Based on this approach, the Extensible Authentication Protocol (EAP) has been developed as general authentication exchange framework. Incorporated with the EAP protocol several authentication methods are supported. Based on the 802.1X frame work, EAP authentication traffic are allowed to pass through the uncontrolled authenticator port, whereas non EAP traffic are blocked or passed according the 802.1X authentication state. Based on the adopted EAP method, the EAP protocol is designed to securely exchange identity credentials, authentication materials and cryptographic keys. Figure 23 shows the relation ship between the link layer protocol, the 802.1X frame work and the EAP methods layer.

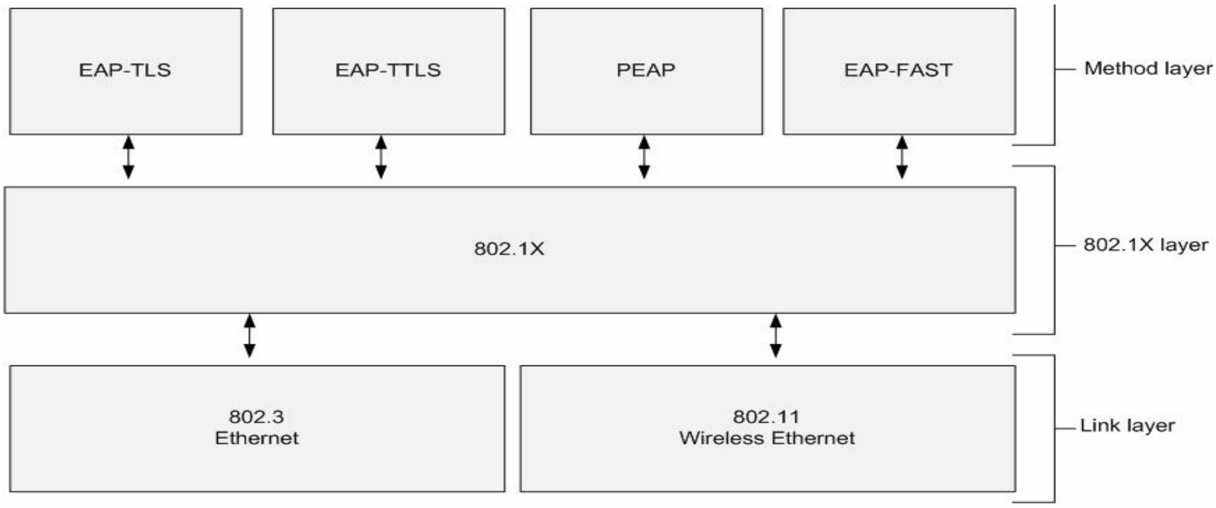


Figure 23: The 802.1X layer relationship

EAP messages which are exchanged between an STA and an AS, must to be securely transmitted and strictly controlled. The authentication server (RADIUS) uses a specified RADIUS protocol to encapsulate EAP messages, and to safely transmit authentication credentials over the LAN interface. For wireless transmission, the EAP messages uses the EAP over lan (EAPOL) protocol, as introduced in section 2.5.2.2, which are used to securely transmit authentication data between an authenticator (AP) and STA. EAP messages, EAPOL frames and RADIUS frames are shown in figure 24.

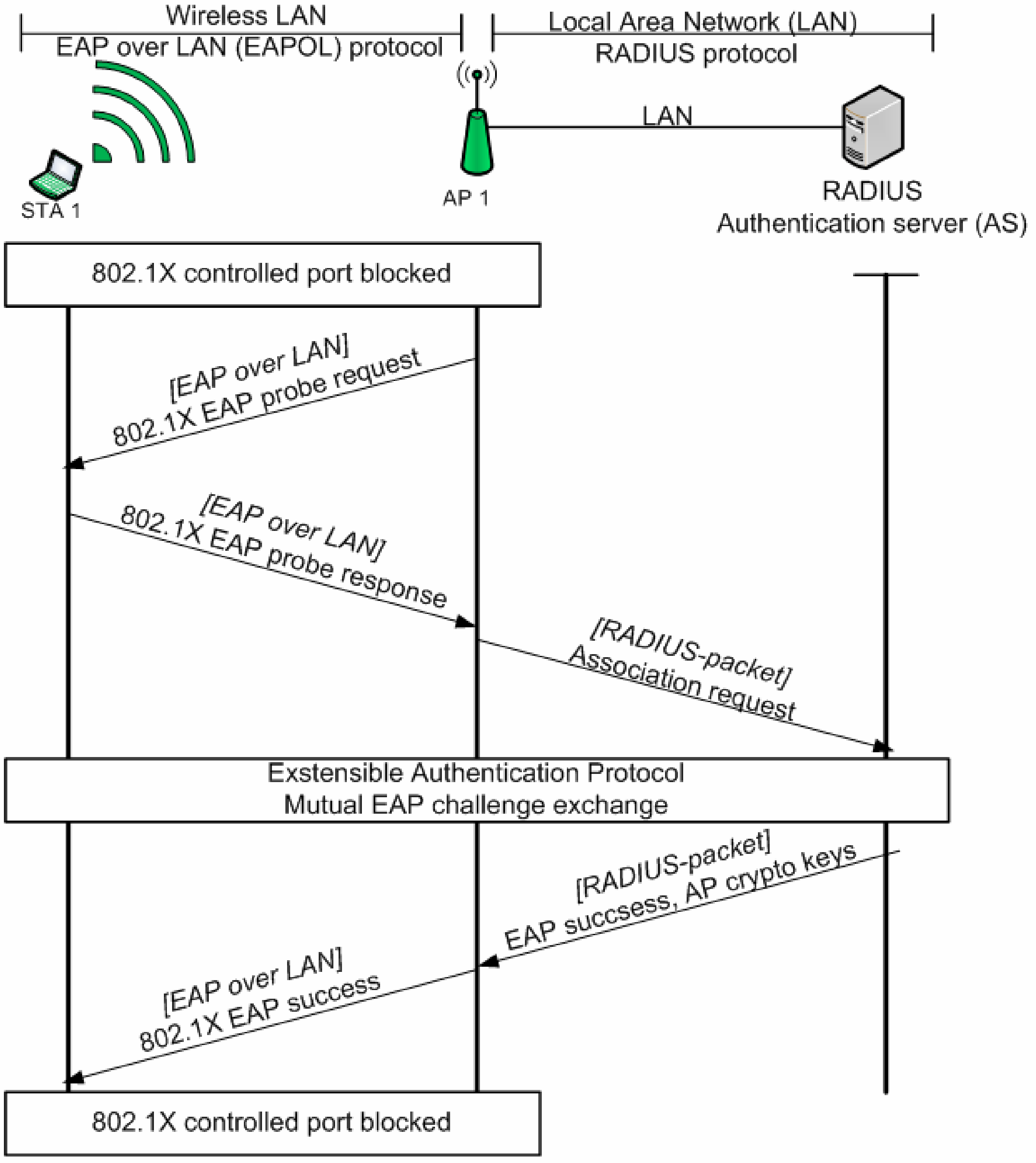

Wireless LAN
EAP over LAN (EAPOL) protocol
Local Area Network (LAN)
RADIUS protocol
LAN
STA 1
AP 1
RADIUS
Authentication server (AS)
802.1X controlled port blocked
[EAP over LAN]
802.1X EAP probe request
[EAP over LAN]
802.1X EAP probe response
[RADIUS-packet]
Association request
Exstensible Authentication Protocol
Mutual EAP challenge exchange
[RADIUS-packet]
EAP succsess, AP crypto keys
[EAP over LAN]
802.1X EAP success
802.1X controlled port blocked

Figure 24: Operations during the authentictaion phase

Figure 24 is a continuation of the discovery frame sequences shown in figure 21. The authenticator (AP) starts the EAP process initiating an EAP identity request frame. The STA will respond with its identity using a EAP probe response, which the authenticator passes on to uncontrolled port as a RADIUS-packet posting the authentication, authorization and accounting (AAA) RADIUS server. The RADIUS server and the STA start the authentication-challenge process where the RADIUS server initiates with a RADIUS-access-challenge packet and the STA formulates an EAP-challenge response. The authenticator (AP) is responsible for converting messages between EAP-frames and RADIUS-frames. If the STA correctly replies to the challenge, the RADIUS server will inform the AP to let the STA access the wireless network. Although, the RADIUS server does not set the controlled port to an authorize state until the AP and STA have received and installed temporal encryption keys. This means that no network traffic will be entering the DS, before STA's and AP has installed required cryptographic keys. The temporal key exchange process occurs via a 4-way handshake protocol, which will be closer described in chapter 4. The cryptographic key result from the 4-way handshake is referred to as the AAA root-key, or the master session key (MSK), which is used to generate other cryptographic keys, for example to secure the wireless communication channel. The cryptographic key is crucial to network security, and compromising it could devastate the overall WLAN security system. Referred to figure 22, the last frame is an EAP-success message delivered to the STA that enables the STA initiates the 4-way handshake process. In the next section I will take a closer look at the EAP protocol, EAP methods and EAP requirements according to safely exchange authentication credentials and key materials.

3.2 Extensible Authentication Protocol (EAP)

To safeguard access control to wireless IEEE 802.11 network a recommended solution has been purposed using the 802.1X port based authentication together with the extensible authentication protocol (EAP). EAP was first defined in the IETF RFC 2284 [41] released in mars 1998. In June 2004 a second release, RFC 3748 [42], and new and extended version the EAP protocol was revised, which considering security, included a new EAP frame work and improved interaction with other protocols. EAP supports a wide range of authentication methods, called *EAP methods* [42]. These methods enables authentication based on password, certificates, smart cards, tokens or combination of different authentications techniques. EAP can also be use to pass trough authenticity, which enables an AP to forward authentication messages to and from a backend centralized authentication system. As mentioned in section 3.1.2.1, the most common protocol to transport EAP authenticity and key distribution credentials over LAN is called the RADIUS protocol. A RADIUS solution carries RADIUS packets containing EAP conversation in order to accomplish secure system authentication. In the next section we will take a look at the different EAP methods and investigate the combination of EAP methods and wireless systems requirements for secure access control.

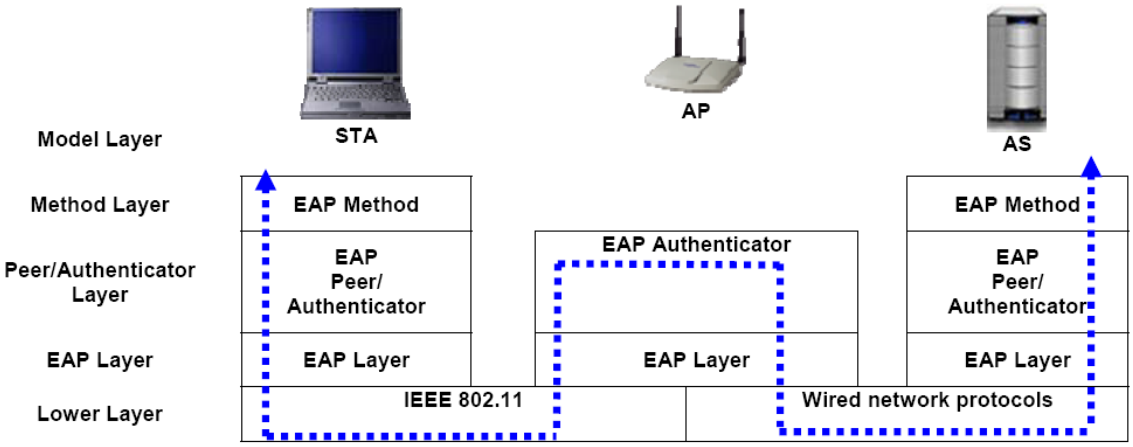


Figure 25: EAP traffic flow [9]

3.2.1 EAP methods

EAP provides a flexible link layer security framework, and can run over any link layer protocols, for example other 802.X networks like Ethernet. EAP methods perform authentication transactions and generate key materials, which is used to protect the communication channel. The EAP methods supports many different authentication types, and based on [9] there exist about 40 different EAP methods developed for different purposes. In this thesis we will only describe some the most relevant and widely supported. One important factor is mutual authentication which means that both the STA and the authentication server must authenticate each other. This does not necessarily signify symmetric authentication, because AP and the client may use different authenticity metods. For example it is possible to use a certificate based solution to authenticate the Authentication Server (AS), while the STA authenticates using a smartcard, passwords or biometrics. To protect EAP traffic against certain attacks, the EAP conversation allows only one EAP method at the time. To support multiple EAP sessions an EAP multiplexer/EAP server needs to be implemented. This enables multiple of user to authenticate simultaneously, and support functionally to use and distinguish several types of EAP conversations. I will not consider security aspects connected to multiple EAP conversations in this thesis. Another important EAP issue is EAP tunneling techniques which means that several EAP methods dependant on another can be tunneled into to same EAP conversation.

3.2.2 EAP requirements

RFC 4017 [44] and RFC 3748 [42] describes security claims and requirements related to EAP method development and guides developers in designing new EAP methods for use in WLANs. The RFC's also describe different EAP methods which provide different levels of security. To evaluate, compare and to help people to understand the level of security each EAP method provides, a security claim list has been composed. This claims list, which can be shown in table 4, is based on some important EAP declarations [42]:

1. **Mechanisms.** This is a statement of authentication technology, for example how authentication is performed; certificates, passwords, tokens, smartcard etc.
2. **Security claims.** This is the statements of the claimed security properties of the EAP method. These claims are shown in table 4.
3. **Key strength.** EAP methods that derive keys, the effective key length must be estimated. This means that potential users should be able to determine the strength of the key produced and if this is enough for the indented application. The effective key strength depends on the method that is used to derive the keys and therefore users need to aware of the quality. For example if a key is derived from a shared secret, for example a password, the effective key length can be limited by the strength of the password.
4. **Description of the key hierarchy.** EAP methods that derive keys must explain and describe their relation to the Master Sessions Key (MSKs), the Extended Master Session Keys (EMSKs) or refer to the original key hierarchy reference.
5. **Indication of vulnerabilities.** Each EAP method must indicate which security claims that is not made according to table 4.

Different EAP methods provide different types security features, and for high assurance wireless networks, administrators needs to evaluate security conditions and requirements before they may implement an appropriate EAP method. On the next page, the EAP claim list is presented concerning WLAN security implementation of different EAP metods.

3.2.2.1 EAP claim list [44, 42]

Security claim	Requirement	Descriptions
Protected cipher suite negotiation	Mandatory	*This refers to the ability of an EAP method to negotiate the cipher-suite used to protect the EAP conversation, as well as to integrity protect the negotiation. It does not refer to the ability to negotiate the cipher-suite used to protect data.*
Mutual authentication	Mandatory	*This refers to an EAP method in which, within an interlocked exchange, the authenticator authenticates the STA and the STA authenticates the authenticator. Two in dependent one-way methods, running in opposite directions do not provide mutual authentication as defined here.*
Man-in-the-middle attack resistance, including integrity, replay and session protection	Mandatory	*This refers to prevent attackers from using a WLAN device to proxy communication between and STAs and an AP in a unauthorized manner.*
Confidentiality	Recommended	*This refers to encryption of EAP messages, including EAP Requests and Responses, and success and failure result indications. A method making this claim MUST support identity protection*
Key derivation	Mandatory	*This refers to the ability of the EAP method to derive exportable keying material, such as the Master Session Key (MSK), and Extended Master Session Key (EMSK). The MSK is used only for further key derivation, not directly for protection of the EAP conversation or subsequent data. Use of the EMSK is reserved.*
Key strength	Mandatory	*If the effective key strength is N bits, the best currently known methods to recover the key (with non-negligible probability)*

		require, on average, an effort comparable to 2^(N-1) operations of a typical block cipher.
Dictionary attack resistance	Mandatory	*Where password authentication is used, passwords are commonly selected from a small set (as compared to a set of N-bit keys), which raises a concern about dictionary attacks. A method may be said to provide protection against dictionary attacks if, when it uses a password as a secret, the method does not allow an offline attack that has a work factor based on the number of passwords in an attacker's dictionary.*
Fast reconnect	Optional	*The ability, in the case where a security association has been previously established, to create a new or refreshed security association more efficiently or in a smaller number of round-trips.*
Cryptographic binding	Mandatory	*The demonstration of the EAP peer to the EAP server that a single entity has acted as the EAP peer for all methods executed within a tunnel method. Binding MAY also imply that the EAP server demonstrates to the peer that a single entity has acted as the EAP server for all methods executed within a tunnel method. If executed correctly, binding serves to mitigate man-in-the-middle vulnerabilities.*
Fragmentation	Recommended	*This refers to whether an EAP method supports fragmentation and reassembly. EAP methods should support fragmentation and reassembly if EAP packets can exceed the minimum MTU of 1020 bytes.*
Channel binding	Optional	*The communication within an EAP method of integrity-protected channel properties such as endpoint identifiers which can be*

		compared to values communicated via out of band mechanisms (such as via a AAA or lower layer protocol).

Table 4: EAP methods claim list for use in WLAN from [44, 42]

3.2.3 EAP methods based on RFC 3748

The first EAP methods were introduced and defined in RFC 3748 [42]. This document [42] describes three basic EAP models, which are all important security feature and authenticity techniques. The main problem with these is that none of them can meet any of the security claims described above. These methods need to be combined with other methods, for example tunneling and encryption techniques to be able to meet the security requirements.

- **EAP MD5-challenge**

  The MD5-challenge [9] method is based on the challenge handshake authentication protocol (CHAP). The primary advantage of this method is that password or other types of authenticity is never transmitted in clear text. The authentication server (AS) transmits the challenge-text to the client. The client inputs this challenge-text along with a password into the MD5 algorithm and creates a hash value. This value is sent back to the AS, which will perform the same operation and compare the two values. Unfortunately, this type of challenge response method is vulnerable to offline dictionary attacks and man-in-the middle attacks. Attackers can place them self in between AP and clients (STA's), called man-in-the-middle, in order to capture the challenge/response messages. Based on the challenge/response information, an offline dictionary attack can be preformed by using the MD5 algorithm to find the correct inputs. To prevent this sort of attack, the protocol needs to be carefully designed, including sufficient entropy in the challenge, appropriate key length and a strong hash function. One possibility is to let the MD5 algorithm to be tunneled within a method that encrypts the entire challenges response method. This means that all challenge/ response messages will be encrypted and thereby mitigate the risk of man-in-the-middle attacks.

- **EAP OTP (One time password)**

  The One-time-password (OTP) method suggests to use identical OPT generators at the client and at the authentication server (AS). These OTP generators use an algorithm to produce a unique series of passwords. The algorithm procedure is based on using rounds of secure hash functions combined with random inputs which generates series of unique words. The OTP generator may be implemented in hardware or in software, but is vulnerable as a stand alone authentication method. As the MD5 challenge, OTP needs to be combined with tunneling techniques to mitigate the risk of being attacked.

- **EAP GTC (Generic token card)**

  The generic token card is based on a hardware solution, which requires the user to input values. An EAP challenge request is send from the AS to the client, where the STA returns a token, based on inputted authentication credentials.

The EAP methods described above has numbers of shortcomings and the most important security issue is that these methods do not offer key generation and key material protections. Cryptographic keys need to be applied in order to protect traffic between STAs and the AP. In other words EAP methods must include other methods than those defined in [42], to safeguard authentication and EAP protection. To achieve high level of security EAP methods should be based on well known and analyzed key-establishment and key generation techniques. The first well established security protocol to be recommended [9] is the Internet Key Exchange protocol (IKE) which is commonly used with the Internet Protocol Security (IPSec) to provide Virtual Private Networking (VPN). The second recommendation [9] is the Transport Layer Security (TLS) which is based on the Secure Sockets Layer (SSL) known from secure web site communication. Both IKE and TLS use certificates based on Public Key Infrastructure (PKI) [63] to ensure authentication and the transfer of key materials. The IKE and the TLS protocol are both founded methods and potential algorithm for use in wireless environments. However, TLS has been designed to provide mutual authentication between a authentication server and a STA. Based on this, TLS has emerged as the most dominant protocol for building access control solutions using EAP methods. TLS uses either a public key certificate or pre-shared key (PSK) for authentication, and additional EAP methods are tunneled within a TLS session. If mutual authentication is required then only the authentication server needs to possess a certificate. On the other hand a copy of this certificate needs to be distributed among the STA's in order to verify the authentications server. Below I will discuss some well-known EAP methods that have been developed.

3.2.3.1 EAP-TLS

EAP-TLS was published in October 1999 [9] and is considered as one of the most secure EAP methods. The EAP-TLS method, which is defined in RFC 2716 [46], is today widely supported with varies of products and systems. To be able to obtain mutual authentication each STA needs to host its own unique PKI certificate [63], which indicates that organizations using EAP-TLS must maintain a public key infrastructure. The certificates may be installed on hard disks or in firmware, but as described in [9], the certificates are recommended to be stored on a smartcard or physical devices which can be removed from the STAs. A certificate which is combined with a physical device also requires users to identify them. This can be done by using personal pin-codes, passwords or by using biometric verification. Otherwise, the physical device may be easily misused. Implementing PKI certificates [10] also involves a certificate policy, practice statements, certificate authorities (CAs), and maintaining a certificate revocation list (CRLs) to verify access to the network. It is out of the scope of this thesis to discuss PKI in detail, but traditional PKI implementations require considerable investments in building infrastructures and resources supplies.

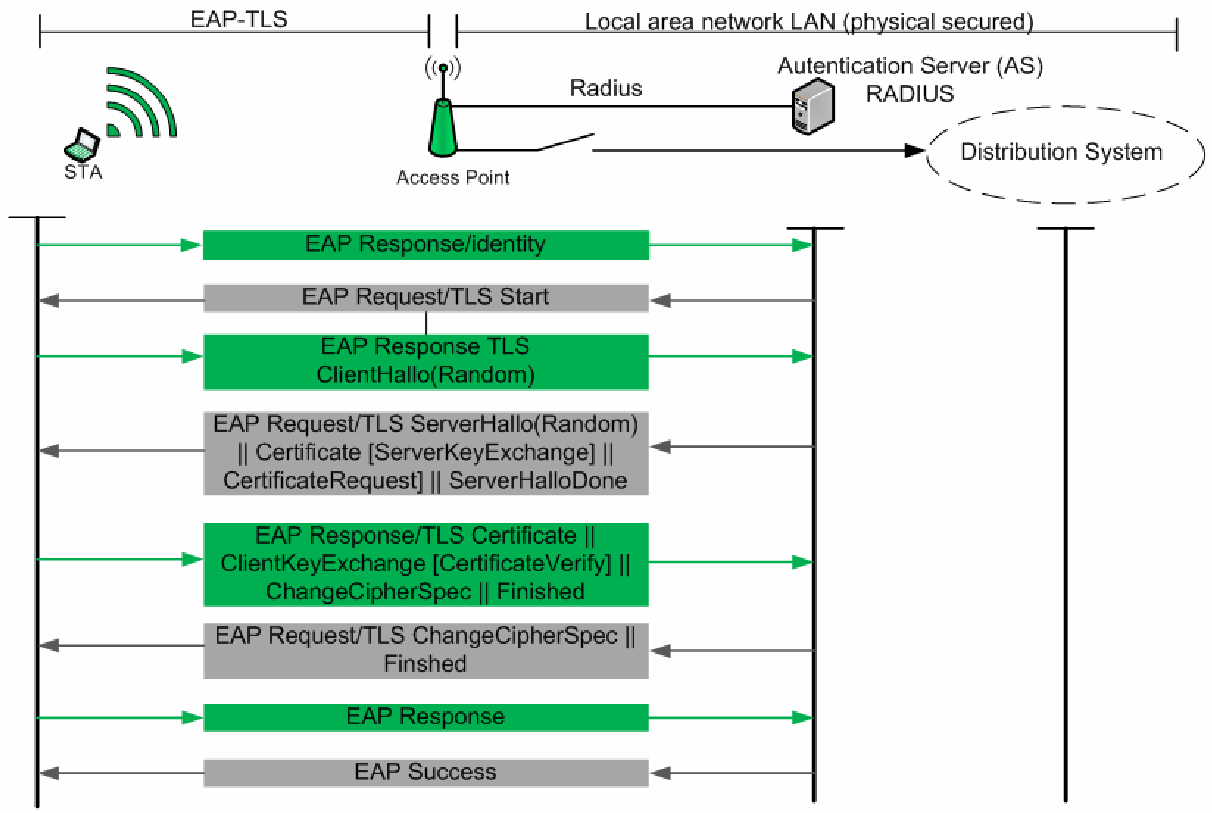

EAP-TLS
Local area network LAN (physical secured)
Autentication Server (AS)
RADIUS
Radius
STA
Access Point
Distribution System
EAP Response/identity
EAP Request/TLS Start
EAP Response TLS ClientHallo(Random)
EAP Request/TLS ServerHallo(Random) || Certificate [ServerKeyExchange] || CertificateRequest] || ServerHalloDone
EAP Response/TLS Certificate || ClientKeyExchange [CertificateVerify] || ChangeCipherSpec || Finished
EAP Request/TLS ChangeCipherSpec || Finshed
EAP Response
EAP Success

Figure 26: EAP-TLS conversation between STA and the RADIUS server

TLS is based on the secure socket layer (SSLv3.0) protocol and was basically created as a transport-layer (OSI-layer-4) protocol to provide confidentiality, integrity and authenticity between two communicating applications. The EAP-TLS protocol implements TLS on the link-layer (OSI-layer-2) level in order to ensure communication between two entities as shown in figure 26. During the authentication phase the access point (AP) acts as a forwarder between the STA and the authentication server (AS RADIUS). As shown in figure 26, the conversation starts with STA sending EAP Response/identity messages to the AP. The AP forwards this message to the RADIUS server. The RADIUS server must respond with an EAP TLS-start message, which is a request-packet to start a TLS session with corresponding STA. The STA responds with a ClientHallo message which contains a client TLS version number, sessionID, random number and set of supported client ciphersuites. According to figure 26, the RADIUS server responds with a new EAP-Request packet containing its TLS-certificate, a STA certificate request, a serverKeyExchange, a change cipher specification and serverHallo message. The STA responds with an EAP Response packet and includes its STA certificate, change cipher specifications, certificate verification and clientKeyExchange message. The clientKeyExchange message is used to complete the exchange of a master secret between the STA and the RADIUS server, and this message is encrypted using the AS public key. As mentioned in section 2.5.2.2, this secret is referred to as the Master Session Key (MSK) or the AAAKey (AAAK). The EAP-TLS conversation ends up with the STA signing an EAP-Respons message, whereas the RADIUS returns and EAP-Success packet including digital signature if requested.

3.2.3.2 EAP-TTLS

The purpose of the EAP-TTLS method is to extend the EAP- TLS to allow one-way TLS authentication to additional provide mutual authentication. The authentication server (AS) is authenticated to the STA using a TLS handshake, which is a one-way authentication process creating an encrypted tunnel between the AS and the STA. This tunnel is then used to perform a second authentication, where the STA authenticates the AS. The last transaction is called *inner application* [9] and consists of series of attribute-value pairs (AVP). The AVP is compatible with the RADIUS message format and specifies the standard protocol and supported algorithms. The inner application can also be another EAP method, and is then referred to as the *inner EAP method* [9]. EAP-TTLS operates similar to accessing secure web pages, where the STA first validates the authentication server, establishes an encrypted session with the server and then transfer user credentials though an encrypted TLS tunnel. One big advantage using EAP-TTLS is that the inner application may support many types of authentication techniques using them as the inner authentication method. This signifies that EAP-TTLS does not require certificates or a public key infrastructure (PKI) to be installed on every STA client. On the other hand this might be a weak point in defense because the over all authentication security will be based on the strength of the authentication method. If this method is based on user passwords, the strength of the password will affect the overall security level. However, EAP-TTLS reduces the administrative complexity since only authentication server's needs to obtain certificates. On the other hand, each client needs to verify the AP certificate and therefore the root certificate needs to be securely transferred to the client. This opens up for man-in-the-middle attacks and since public key crypto is not represented, man-in-the-middle attacks become the shortcomings of using EAP-TTLS methods.

3.2.3.3 Protected EAP (PEAP)

Protected EAP (PEAP) is a co-operation between Microsoft, Cisco systems and Extundo. PEAP is vary similar with the EAP-TTLS based method, and uses certificates only to provide AS authenticity to the STAs and thereby establish a secure connection for a communication channel to protect further transactions. As a mandatory security requirement, PEAP requires the root certificate to be distributed among the STAs, for secure verification. The main difference between EAP-TTLS and PEAP is that PEAP uses another chosen EAP method instead of AVPs. This indicates that the authentication method used in PEAP, called the *inner EAP method*, can be any developed and preferred EAP method. PEAP is a well supported protocol in Microsoft and Cisco system products, but lacks compatibility with other vendors. Unfortunately, Windows XP systems only supports EAP methods like MS-CHAP and MS-CHAPv2, which based on [9] is considered as insecure, and in addition limited for authentication with Microsoft domains or active directory. Another important issue is that neither EAP-TTLS nor PEAP have been approve as IETF standards, which signifies that implementation using PEAP or EAP-TTLS should be closely evaluated before use.

3.2.3.4 EAP-FAST

The last EAP method that I would like to mention is EAP-FAST developed by Cisco systems. EAP-FAST uses Protect Access Credential (PAC) to establish an encrypted tunnel for secure communication. This establishment is either based on a pre-shared key or public key encryption. After a tunnel establishment, an inner EAP method can be used for further authentication. Because of PAC, EAP-FAST does not require certificates on AS or STAs. Instead Cisco has included a mechanism that refreshes the PACs after each successful authentication. Since EAP-FAST does not require a TLS handshake process it provides computing advantages which indicates that EAP-FAST is adapted for small devices with less computing power. The problem with EAP-FAST is that establishing a PAC is not more secure or easier than using certificates, and often the inner EAP authentication involves digital certificates anyway. Therefore EAP-FAST is basically very similar to EAP-TTLS and PEAP. Another issue is that Cisco systems is the only vendor supporting the EAP_FAST method, and the method has not been official approved as an IETF standard.

3.2.4 EAP methods evaluation

The RSN frame work recommends the IEEE 802.1X standard combined with EAP to ensure secure authentication, but implementation details and subsequent claims are left to vendors and organizations to implement. Therefore EAP solutions have to be adapted to the preferred security configuration. Table 5 displays a review of the different EAP methods and shows each method compared to the claim list defined in section 3.2.3.1. As you can se from table 5, none of the RFC 3748 methods can meet any of the security requirements, but these methods can still be used as and tunneled inner EAP applications. The TLS-based methods differ from requiring PKI support to requiring certificates distributed among STAs and APs. This means that the preferred EAP method model will depend on the particular network configuration and the security requirements. Based on [9] the EAP-TTLS and the PEAP are emerging as the industry preferred methods for WLANs. The EAP-FAST is still a Cisco system variant, which is still a proprietary solution not widely supported.

Security Claims	EAP methods				
	RFC 3748 Methods MD5/OTP/GTC	TLS based Methods			
		EAP-TLS	EAP-TTLS	PEAP	EAP-FAST
Key derivation	No	Yes	Yes	Yes	Yes
Key Strength	No	Yes	Yes	Variable	Yes
Mutual authentication	No	Yes	Depends	Depends	Yes
Shared state equivalence	No	Yes	Yes	Yes	Yes
Dictionary attack resistant protection	No	Yes	Yes	Yes	Yes
Man-in-the-middle attack	No	Yes	Depends	Depends	Yes
Protected ciphersuite negotiation	No	Yes	Yes	Yes	Yes
Fragmentation	No	Yes	Yes	Yes	Yes
Confidentiality	No	Yes	Yes	Yes	Yes
Channel binding	No	?	Optional	Yes	No
Fast reconnect	No	?	Yes	Yes	Yes
STA certificate	None	Required	Optional	None	None
AS certificate	None	Required	Required	Required	Optional
Tunnel authentication protocols	None	None	AVP	EAP	EAP

Table 5: EAP methods and the security claim list. Based on information from [9, 42, 44]

3.3 Access control conclusion

The IEEE 802.1X standard combined with the EAP protocol is a sufficient starting point for designing secure access control architectures for high assurance wireless environments. The EAP frameworks are divers but needs to be implemented and adapted with the organization security requirements. Referred to [59], it can be demonstrated that EAP-methods tunnelled within another protocol, such as EAP-TTLS and EAP-PEAP, can be vulnerable to Man-the-Middle attacks. Regardless, such attacks are possible only if the authentication process is weak and allow a one-way association, for example that the STA authenticate the AP and not visa versa. In other words strong mutual authentication is a certain security requirement irrespective of what EAP method to implement. As mentioned in [59] other premises for a successful Man-in-the middle attack is the possibility for an attacker to obtain the session key (TK) and to compromise the Pairwise Master Key (PMK). The PMK is fundamental to security and must be strongly protected (referred to section 2.5.2.2 figure 12). For high assurance wireless networks, the recommendation [9] is to implement a hardware security module (HSM), for example a smartcard solution, integrated with PKI certificates, using EAP-TLS for authentication and cipher exchange. As shown in table 5 only EAP-TLS and EAP-TTLS can be used in environments requiring certificates distributed among all authorized entities. To conquer the access control challenges in wireless networks, the overall security design must be based known security principals. From the discussion above, we can conclude that a secure access control solutions should preferably be implemented to follow strong security requirements. In the following section I will describe some important architectural issues and security characteristics which should be adapted for access control concerning high assurance wireless IEEE 802.11 implementations.

3.3.1 Wireless access control requirements

- ***Two-factor based authentication model at minimum.***

Access control is a very important part of high assurance wireless security systems. The access control solution determines an authentication model with mechanisms to keep unauthorized devices blocked from the wireless network. Based on this, the authentication model should be founded on minimum two factors of cryptographic authentication mechanisms. This means that the authentication model should combine mechanisms for “something you have”, “something you know” or “something you are” [10]. Two-factor authentication principals will prevent that a single compromised password or a compromised STA will be able to undermine the entire security system.

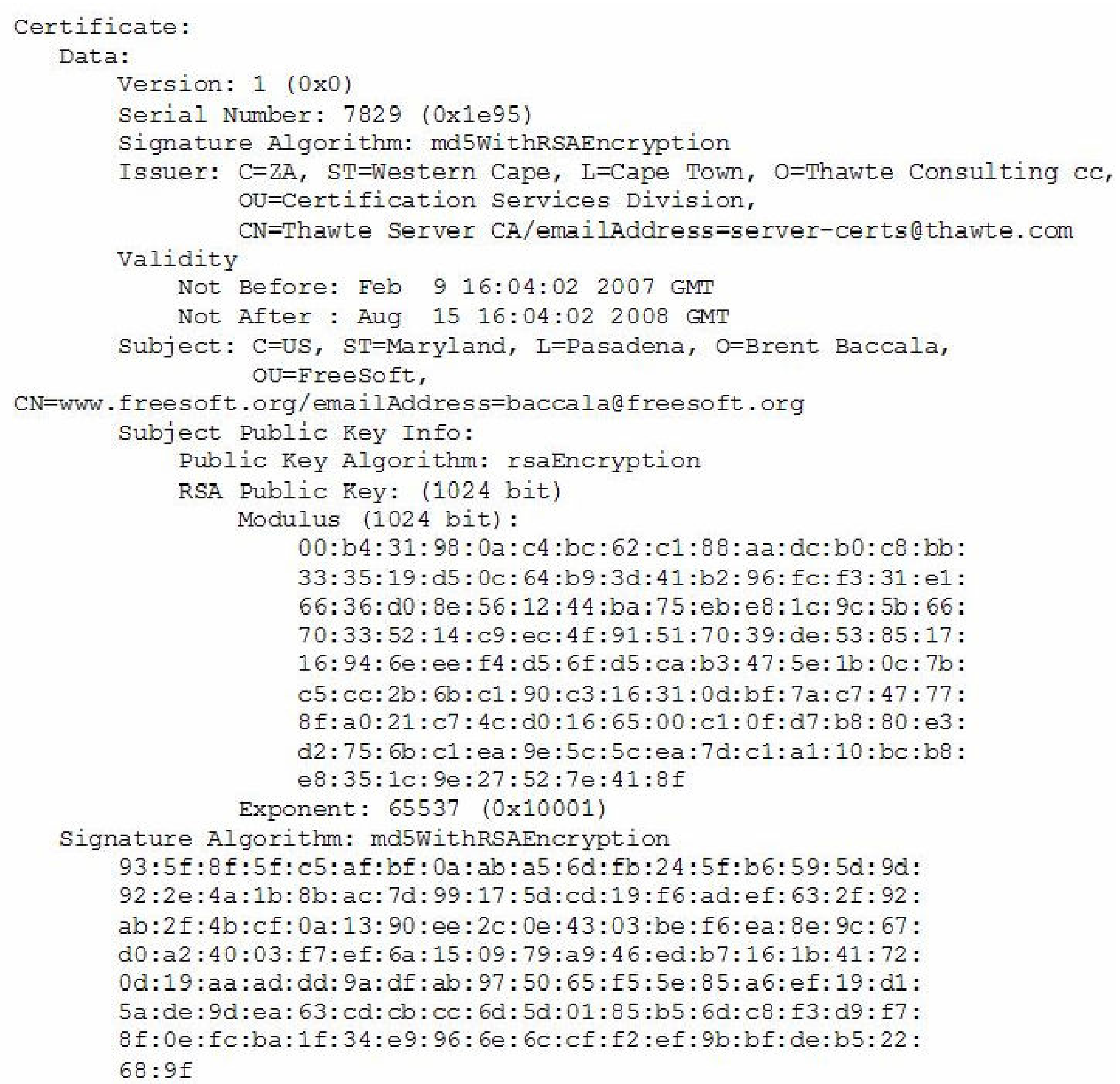
Hardware security module (HSM)

To implement a two-factor authentication model, the access control solutions should be based on separated security modules combined with several various authenticity components. A hardware security module (HSM), for example a smartcard, can be used as a physical security device, where authentication components such as digital certificates can be stored inside as a cryptographic token. A smartcard can provide authentication based on a combination of hardware, software, digital certificate, cryptographic key, password, pin-code or biometrics verification methods. The smartcard hardware-chip can be used to store, generate and handle security critical objects used for system device authenticity and confidentiality. One advantage of using a smartcard solution is that security critical components can be easily removed from the STA to prevent misuse and to separate security mechanisms from other STA hardware/software. An alternative solution to smartcards is the generic token card (GTC) as described in section 3.2.3. The combination of HSM, digital certificate and user ID password results in a three-factor authentication model. To compromise and hack into a wireless three-factor based authentication model, attackers need to obtain a certain HSM, steal or compromise the associated password as well as exploiting a stored and valid digital certificate. This is a much more complicated scenario compared to just compromising a single username and password.

Figure 27: "eToken PRO " Portable USB token smartcard with PKI support

Public Key Infrastructure (PKI) certificates

Public Key Infrastructure (PKI) is basically a management system which provides and administrates public key certificates and asymmetric cryptographic keys [6]. A software PKI-certificate is related to "something you have", can be used to provide authenticity, integrity and confidentiality. Table 6 summarizes additional PKI features. Traditional PKI is known as asynchronous cryptography which means that a public key is used for encryption whereas a private key is used for decryption. Only the owner knows the private key, whereas the public key is known for everyone. This also indicates that the private key can be used to provide unique digitally signatures, which can be used to sign messages and transactions in order to ensure authenticity. PKI has several advantages compared to symmetric crypto (AES etc.), and obviously public key crypto does not require an established key in advance. This means that PKI is well suitable for wireless networks when it comes to establish secure communication channels. A drawback is that PKI adds substantial transaction overhead and depending on the PKI implementation, could result in slower and less effective link-layer operations.



```
Certificate:
   Data:
       Version: 1 (0x0)
       Serial Number: 7829 (0x1e95)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Validity
           Not Before: Feb  9 16:04:02 2007 GMT
           Not After : Aug  15 16:04:02 2008 GMT
       Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
                OU=FreeSoft,
CN=www.freesoft.org/emailAddress=baccala@freesoft.org
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
                   33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
                   66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
                   70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
                   16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
                   c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
                   8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
                   d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                   e8:35:1c:9e:27:52:7e:41:8f
               Exponent: 65537 (0x10001)
   Signature Algorithm: md5WithRSAEncryption
       93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
       92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
       ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
       d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
       0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
       5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
       8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:
       68:9f
```

Figure 28: Example of a PKI certificate X 509 [11]

PKI protections	Description
Authenticates identity	Digital certificates issued as part of your PKI allow individual users organizations to confidentiality validate the identity of each party in an transaction
Verifies integrity	A digital certificate ensures that the message or document which the certificate signs has not been changed or corrupted when transmitted
Ensures privacy	Digital certificates product protects information from interception during transmission
Authorizes access	PKI digital certificates replace easily guessed and frequently lost user ID's as vulnerable authentication mechanisms.
Authorizes transactions	With PKI solutions your enterprise can control access privileges for specified transactions
Supports nonrepudiation	Digital certificate validate their users identities making it nearly impossible to later repudiate a digitally signed transaction

Table 6: PKI features for access control and protection [6]

- ***Digital certificate issues***

Deploying certificates solutions for STA's, AP and AS represents potensial vulnerabilities and threats. A public key certificate (PKI) is only valid if it's signed by a trusted 3rd party certified authority (CA), which signifies that STA's basically will trust an AS with any valid CA-certificate. As long as the AP has a correct SSID and a CA corresponding certificate, the STA will try to associate with the AP. This is vulnerable because an attacker can easily fake SSID and obtain valid certificates from certified authorities (CA), which furthermore can be used to set up a rough access point to capture STA's authenticity credentials. As proposed in [46, 9] this can be prevented by demanding a specific RADIUS server to require the STA to authenticate based on a valid and adapted "server-name" certificate. This is basically because it is much more difficult for attackers to imitate private certificate than a general CA certificate. The STA and AS should be adapted to verify several local certificate credentials, for example verify the certificate origin, the specific name, the correct IP sub-domain etc.

Personal identification

Personal user secrets such as passwords or pin-codes, are related to “something you know”, and are ordinary identification methods used in many of today’s information systems. On the other side, such identification is vulnerable if access control mechanism depends on simple usernames and passwords exclusively. Personal user secrets are important authenticity elements which in combination with digital certificates provide reasonable security and trust. An alternative solution for personal identification is biometric systems based on for example fingerprints. A biometric system is even more complicated and introduces challenges according to robustness and error rates [10].

EAP- methods

Referred to 3.2.3.1, EAP-TLS is designed to be implemented in PKI environments where certificate are stored on STA’s and AS. In addition EAP-TLS is well supported and native to recent windows version. Based on [9], a smartcard PKI solution based on EAP-TLS generally offers the greatest security. Another interesting EAP approach is a combination of PEAP and EAP-TLS called PEAP-EAP-TLS as described in [68].

AP communication to authentication server (AS) and distribution systems (DS)

The IEEE 802.11i approach is only adapted for securing the wireless radio link between STA’s and AP. The wired communication link between the AP and the AS, and AP and distribution system (DS) is not a part of the RSN 802.11i specifications. This is vulnerable to physical availability and signifies that the access point LAN side is postponed to be compromised in terms of unauthorized monitoring. To prevent this, the communication between the AP and AS, which basically consists of RADIUS messages, should be secured and encapsulated using VPN IPsec techniques (network layer security) as introduced in section 2.6. Other suitable protection mechanisms is to use is key wrapping tools like the AES key-wrapping algorithm, which will be described in chapter 4, to protect key materials which is transmitted between the authentication server (AS) and the AP. The communication link between AP and DS should also be protected, because default IP traffic will be transmitted in clear text. The LAN between the AP and DS must be physical secured and VPN IPsec techniques can be used protect data. Another approach to protect AP to DS communication is to establish VPN IPsec tunnels directly from the STA's to a VPN server located within the DS area. This is regardless a little more complicated scenario, which I will closer describe in chapter 6.

- **STA identification signature**

To prevent DOS and flooding attacks on the RADIUS authentication server, the AP should challenge the STA before sending the authentication request to the RADIUS server. Using public key infrastructure this can be done by requiring the STA to transmit a signed message to the AP. The AP verifies the message using the public key, if approved the AP forwards the authentication request. This will prevent unauthorized devices from challenging the AS server independently. The identification signature could for example be based a signed password and nonce, attached to the physical address.

Example: ([“password” + “MAC-address” + nonce]$_{\textbf{SHA-1}}$) **Signed with STA private key**

- ***Mutual authentication for both STA and AP/AS***

A mutual authentication process is imperative. As discussed above both STA and AP (on behalf of the AS) must be authenticated. Based on a PKI infrastructure each participating device must obtain a valid PKI certificate. The public key certificate must be verified by the STA and the AS in order to accomplish the authentication process.

- ***STA high assurance WLAN configuration.***

Each STA's must be forced to use a certain particular high assurance WLAN only. STA's which are authorized to use a specific high assurance wireless network should not be able use other unclassified and insecure WLAN systems. This is because STA's could leak information if a multiple of different WLAN connections are allowed. This can be accomplished through STA firewall rules, enforced certificate policy and a locked SSID.

- ***Vulnerabilities to the MAC protocol***

Based on [77], RSN networks are vulnerable due to series of flaws in the 802.11 protocol. However, these flaws can be prevented by adding security synchronization functionality and authenticity to EAP messages and management frames. WLAN systems which are implemented with Public Key Infrastructures (PKI), can use private keys to sign link-layer messages to ensure transaction authenticity. On the other side such a solution would create substantial overhead and probably degrade the WLAN network performance. Since only a minority of WLAN networks uses PKI, the IEEE 802.11w Task Group (TG) [2] is currently working on authenticity improvements as general approach to improve the IEEE 802.11 protocol.

- ***Fallback authentication strategy***

If authorized STA's and users fail to authenticate to the WLAN system, a policy should be established to handle such situations. Typical reasons could by expired certificate, forgotten passwords, smartcard trouble or other STA problems. A fallback method should establish routines according to log occurrence and handle the reconditioning process. For example EAP-TLS alert message can be collected to investigate failures to the authentication processes.

- ***Location based access control***

As described and proposed in [82], location data can be used to provide access control in wireless environments. The goal of location based access control is to define and determine a maximum allowed distance between the AP and STA. If the STA moves to far away from the legitimate access point (AP), the system can refuse further network negotiation. Location measurement mechanisms must be implemented in order to locate and position devices. Location based access control would potentiality prevent intruders from using high quality antennas to access the wireless network far away from wireless area. The challenge with location control is to implement an accurate location measurement system which can be used to locate STA's and AP's. For example, calculations based on the received-signal-strength (RSS) can be used to provide location data. Location control and location measurement will be closer described in chapter 5.

4 Confidentiality and integrity based on IEEE 802.11i

This chapter will focus on the key management phase (key establishment), the data protection phase and the termination phase which was introduced inn chapter 3, figure 17. The key management phase is responsible for handling and generating cryptographic keys and cryptographic key materials which are used by cryptographic algorithms to protect the wireless data transmission in terms of confidentiality, integrity and authenticity (origin authentication). In the following chapter I will investigate and discuss the IEEE 802.11i RSN settlement related to AES CCMP combined with the 4-way handshake protocol to provide robust and secure data transmission.

4.1 RSN confidentiality, authenticity and integrity protocols

Basically the IEEE 802.11i standard settlement provides two types of confidentiality protocols; the Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Standard (AES). The AES algorithm is based on the Counter Mode with Cipher Block Chaining Message Authentication protocol (CCMP) which is identical to the algorithm used in VPN IPses ESP [63] networks. Because TKIP is using the RC4 algorithm which has known weaknesses, TKIP is not suitable for high assurance environments [2, 9]. Based on this, TKIP will not be discussed in this thesis as a relevant layer two confidentiality protocol. For environments requiring high level of security, AES CCMP is considered as a much better solution, and this section will take a closer look at how CCMP solves the confidentiality, authenticity and integrity problems in wireless 802.11 networks. For IEEE 802.11i RSN configurations in wireless networks, CCMP is the only approved cryptographic model. In the next section I will take a closer look at the CCMP functionality including encryption and decryption methods.

4.1.1 CCMP

Counter Mode with Cipher Block Chaining MAC Protocol (CCMP) [9, 23, 56] is a confidentiality protocol defined by the IEEE 802.11i standard [23]. CCMP is based on CCM which is a generic authenticated encryption block cipher modus based on the advanced encryption standard (AES) [57]. The distinct difference to the other wireless confidentiality protocols, such as WEP and TKIP, is that CCMP requires new hardware replacement in both Access Points (AP's) and Stations (STA's). The intention is to develop a confidentiality protocol based on a secure long-term solution based on proven concepts and high security definitions. CCMP is therefore a mandatory component in creating wireless RSN networks. To provide robust network security, CCMP consists of two well known and proven cryptographic techniques. The first technique is counter (CRT) mode which is used for confidentiality and the cipher block chaining MAC (CBC-MAC) mode, which is used authenticity and integrity protection. The combinations of these two techniques forms block ciphers [10] with a 128-bits block size. To minimize complexity, CCM used in IEEE 802.11 networks, operates with a single 128-bit session key (TK) which is used to protect the duplex data channel (send and receive). The key size has a range of 2^{128} possible values and is renewed for every new log on session. Additional, the key is used to constructs a 48-bit packet number (PN) nonce to protect against replay attacks. Because of the random nonce value, the CCM can be used for both confidentiality and integrity without compromising each other.

4.1.1.1 CCM encryption process

The CCM provides integrity for the data payload (link layer PDU datagram's as described in section 2.3.1) and integrity protection for parts of the 802.11 MAC-header. For this purpose a single cryptographic key is used to maximize the performance. As mentioned in section 2.5.2, the WEP and TKIP cryptographic model is based on the RC4 algorithm which uses stream cipher [10] encryption methodology. Stream ciphers are optimized to be simple and efficient especially for radio communication networks, but due to security algorithm vulnerabilities there have been little effort in developing new stream ciphers. On the other side, block ciphers are announced as the future algorithm for the combination of secure and efficient cryptographic designs. Based on this, one important issues when designing the CCM block cipher algorithm, is to enable fast comparisons, high security and to a minimal cost of operations. The CCM encapsulation process is shown in figure 29.

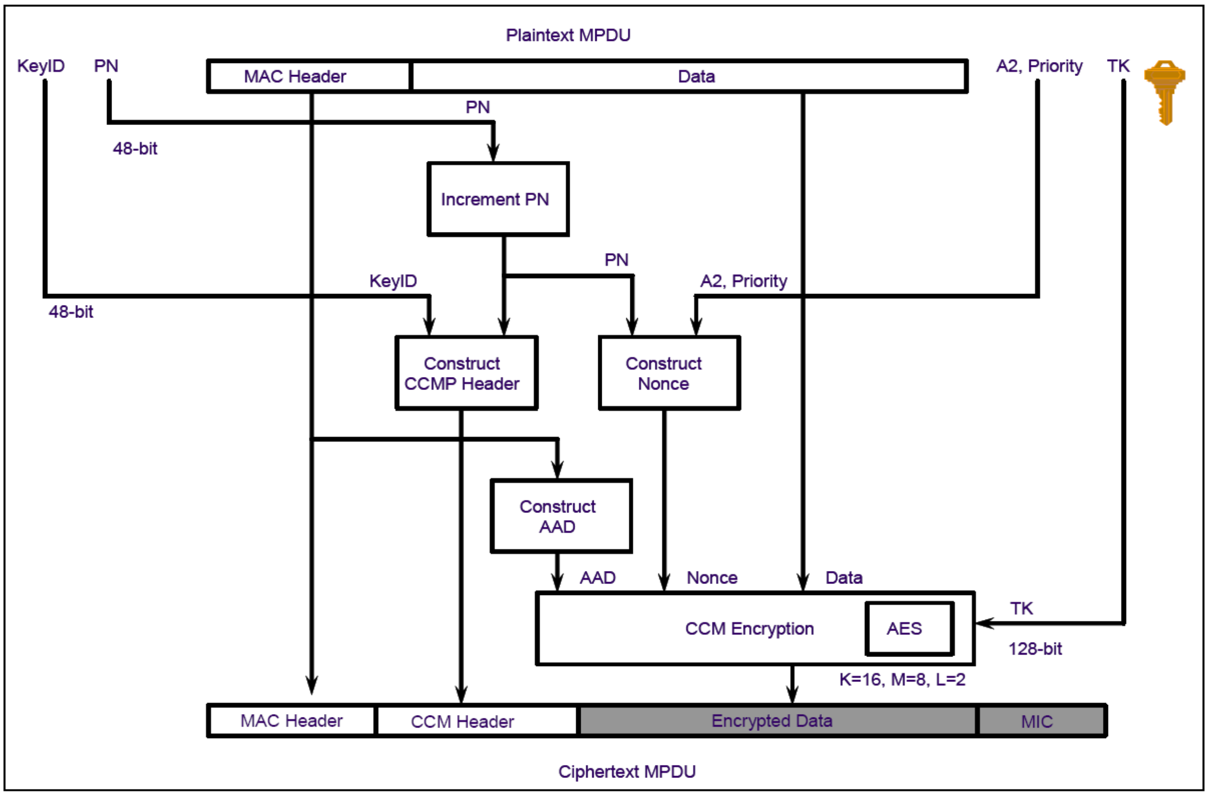


Figure 29: CCM encapsulation prosedure [9]

The CCM encryption process, which is referred to as the CCMP encapsulation procedure in figure 29, is the process of generating a cryptographic payload from the plain text data. As introduced in chapter 2, the plain text data includes layer two data (PDU datagram's) and a MAC header. The plaintext data and parts of the MAC-header are combined with the CCM encryption algorithm to derive a cipher-text MPDU datagram. The CCM algorithm has the following input values [9]:

- Frame body data (variable plain text) and MAC-header
- Temporal cryptographic Key (TK) 128-bit (Session Key)
- Packet number (PK) and a nonce (48-bit)
- Additional Authentication Data (AAD)

From figure 29 we observe that the 48-bits packet number (PN) is incremented, and in combination with the transmitter address (A2), constructs a unique nonce value. The incremented packet number and the KeyID, which is a temporal key identification, are used to generate the CCM header. The additional authentication data (ADD) is a 22 byte or 28 byte parameter which comprises several fields, like the MAC-address fields and the quality of service field, to provide integrity and authenticity to the data packet. The ADD, the nonce value, the 128-bit temporal key (TK) and the plain text data creates a fixed encrypted CCM data output. A message integrity code (MIC) is added at the end of the MPDU for frame integrity protection. As shown in figure 29 the final encrypted datagram contains four fields; a MAC field, a CCM field, an encrypted data field and a MIC field.

4.1.1.2 CCM decryption process

The decapsulation process, which is used to recover the encrypted datagram, is shown in figure 30. This process is very similar to encapsulation procedure, except from the deriving sequence, and that you need to possess necessary key materials to be able to accomplish the decryption proceedings. To be precise, the recipient needs the correct temporal session key (TK) and the nonce value to able to recover the MPDU datagram into plain text data.

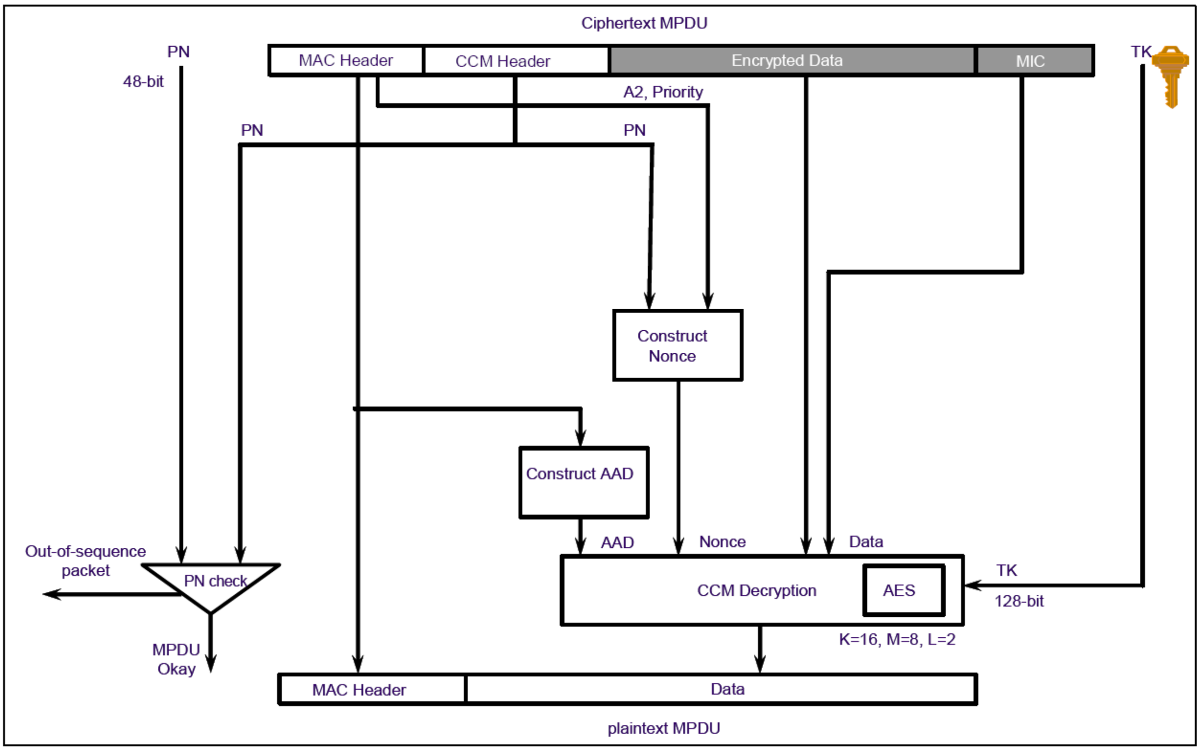


Figure 30: CCM decapsulation prosedure [9]

The first thing that occurs when the MPDU datagram is received by the STA or the AP is to analyze the MAC and the CCM header to reconstruct the ADD and the nonce value. The nonce value is formed based on the received packet number (PN), the transmitter address A2 and the priority fields. The purpose of PN value is to protect against relay attacks, and if the received PN value is not a greater than the session PN or part of the maintained session PN the frame will be discarded automatically. Furthermore, as shown in figure 25, the CCM algorithm uses the additional authentication data (ADD), the nonce value, the en encrypted frame, the MIC and the temporal key to recover the plain text data. The MIC is used for an integrity check and if the MIC fails, the CCM will not continue the decryption process and the frame will be discarded.

4.2 CCMP, key establishment and management

To establish a secure CCMP communication link in terms of a Robust Security Network Association (RSNA), the STA and the Access point must exchange secrets which are necessary to derive keys from the pair-ways master key (PMK). To do this the wireless high assurance system must organize its keys hierarchy through key management and key handling processes. The Internet Engineering Task Force (IETF) defines key management [3] as "the process of handling and controlling cryptographic keys and related material (such as initialization values) during their life cycle within a cryptographic system, including ordering, generating, distributing, storing, loading, escrowing, archiving, auditing, and destroying the material." In other words, key-generation, key-distribution, key-handling, key-storing and key-destruction are important key factors in wireless high assurance networks. If the key generation, distribution or storing process renders the possibility to compromise cryptographic keys it would devastate the overall wireless security system. Based on this key management should conduct the following requirements [9]:

- Keys needs to be randomly generated to reduce the probability that they can be determined
- The key in use needs to frequently changed to reduce the possibility of successful cryptoanalysis
- The keys need to be protected while in storage
- The keys need to protected during transmission
- The keys need to be completely erased after use, without leaving any tracks.

As described in section 2.5.2.2, the IEEE 802.11i standard defines the Pairwise Key Hierarchy (PMK) for unicast communication, and Group Key Hierarchy (GMK) for multicast/broadcast communication protection. Both hierarchies rely on a root-key which is either pre-shared (PSK) or distributed (AAAK). The root-key is formulated and associated as a key-generation-key used to derivate Pairwise Transient Keys (PTK).

4.2.1 The 4 way-handshake

After a successful authentication process as described in chapter 3, the AP and the STA has to agree on what encryption key to use. Referred to chapter 3 figure 15 the subsequent phase 3, the key management phase, is vital to establish a secure AES CCMP encrypted communication channel. To be able to securely exchange essential key materials, both AP and STA has to perform series of functions resulting in a secure handshake procedure positioning cryptographic keys in both entities. Referred to [9] this procedure is called the key generation and distribution (KGD) phase. In RSN 802.11 networks the KGD phase also provides the finale step in authentication and makes sure that both AP and STA has correct keys to establish a secure wireless communication channel. One of the objectives behind the KGD phase is to confirm several important derivation issues. For example the KGD phase confirms that there exist a PMK, that secure association keys are new and that the cipher suite selection is correct. I addition, the KGD derives and synchronizes the installation process of temporal traffic encryption keys for AP and STA's and distribute group keys for multicast/broadcast traffic protection. To perform the KGD there exist two different procedures, the 4-way Handshake and the group Handshake. Both these handshakes provide the ability to securely exchange key materials, but the group-handshake is only used when STA participates in multicast or broadcast traffic. Both handshakes procedures provide the following fundamental security features [9]:

- Message integrity check to prevent message tampering and source validation
- Message encryption to protect against eavesdropping and message disclosure

To provide both confidentiality and integrity for the handshake process there currently exists to supported algorithms; The RC4 encryption with HMAC-MD5 or the AES key Wrap with HMAC_SHA-1-128. Base on the RC4 vulnerabilities, the RSN 802.11 configurations recommends the AES Key Wrap algorithm [58]. The AES Key Wrap algorithm is specially designed to encrypt cryptographic keys. The algorithm use AES codebook mode along with EAPOL-KCK (section 2.5.2.2) derived from the PTK and forms key-blocks of 64 bits to be encrypted ("wrapped"). The 4-way handshake is shown in figure 31, and shows a frame exchange procedure where STA and AP perform several computations and generations resulting in cryptographic keys and a secondary mutual authentication process.

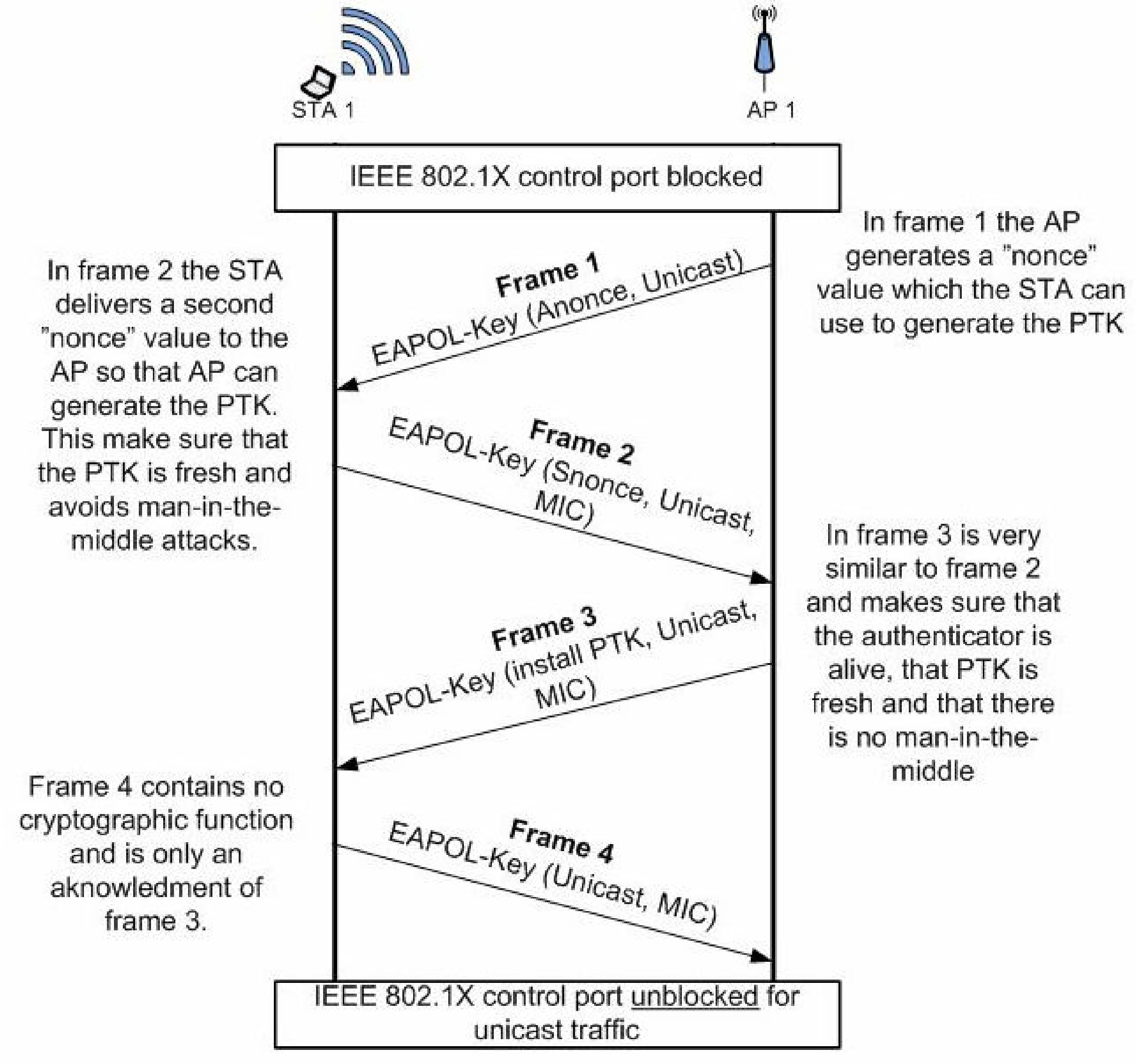

STA 1
AP 1
IEEE 802.1X control port blocked
Frame 1
EAPOL-Key (Anonce, Unicast)
In frame 1 the AP generates a "nonce" value which the STA can use to generate the PTK
Frame 2
EAPOL-Key (Snonce, Unicast, MIC)
In frame 2 the STA delivers a second "nonce" value to the AP so that AP can generate the PTK. This make sure that the PTK is fresh and avoids man-in-the-middle attacks.
Frame 3
EAPOL-Key (install PTK, Unicast, MIC)
In frame 3 is very similar to frame 2 and makes sure that the authenticator is alive, that PTK is fresh and that there is no man-in-the-middle
Frame 4
EAPOL-Key (Unicast, MIC)
Frame 4 contains no cryptographic function and is only an aknowledment of frame 3.
IEEE 802.1X control port unblocked for unicast traffic

Figure 31: 4-Way Handshake procedure

After a successful 4-way handshake, the IEEE 802.11 controlled port is open and allows the STA to send and receive data from the wireless network. As described in figure 26, frame 2, 3 and 4 are protected with a MIC which is computed over the entire EAPOL-frame, and protects messages against modifications. Although frame 1 is not MIC integrity protected because the STA needs the AP nonce value to be able to derive the EAPOL-KCK (se section 2.5.2.2) which is used to compute the MIC for EAPOL key packets. Modifications to frame 1 are still possible to detect using other checking mechanisms [9]. As mention in section 2.5.2.2 the STA during the 4-way handshake also drives the EAPOL-KEK which is used to ensure confidentiality to EAPOL-Key packets and the temporal key (TK) which is used to encrypt wireless data traffic.

4.2.2 Secure connection termination

As shown in chapter 3 figure 17, the last phase in the RSNA process is the termination phase. In this phase the STA and the AP terminates the connections, deletes the association and restore the connection to the initialized state. This termination phase is important because all association tracks, encryption keys and temporal keys must be deleted. In addition the IEEE 802.11 controlled port is locked immediately after disassociation.

4.3 Confidentiality, authenticity and integrity conclusion

The CCMP confidentiality protocol is a well founded and approved security protocol which according to [9] can be recommended as a standard encryption algorithm for high assurance wireless networks. As long as the input values are kept secret and randomized, crypto analysing processes and brute force attacks are considered extremely difficult. Based on this, security relies on the capability to safely exchange key derivation materials. The IEEE 802.11i RSN networks introduce the 4-way handshake protocol for this purpose. As described in section 4.2.1 the handshake protocol can be used to authenticate as well as to exchange key credentials. Even if the PMK is generated from a pre-shared key (PSK) or from the EAP handshake process described in chapter 3, the 4-way handshake protocol must execute in order to confirm fresh crypto keys, cipher suites and to verify the STA authenticity. Additionally the authenticator (AP) and the STA can use the 4-Way handshake protocol to refresh the PTK key periodically. This indicates that based on the AP and STA configuration, the CCMP session key (TK) can be refreshed several times during a session using the 4 way-handshake protocols, but for one instance of the protocol, only one fresh PTK value is valid. In case of packet loss or delay, which is general in wireless networks, the 4-way handshake protocol must be able to handle multiple protocol instances in parallel. For example if frame-two (shown in figure 31) is lost, the instance of frame-one will be discarded by the STA. Therefore the STA has to allow any instance of frame-one and accordingly, referred to [60], the 4-Way Handshake protocol is vulnerable to frame-one flooding attacks. This means that attackers can initialize new instances of the handshake protocol to block valid frame-one messages. As described in [60] and [64] the handshake problem can be solved by adding a different MIC code to the frame-one message. Since the problem with the frame-one is that the STA does not have the nonce value, the PMK combined with a sequence counter can be used to assure message-one authenticity and integrity. If the WLAN access control system is based on PKI certificates, another approach to solve this problem is using the private key to sign frame-one messages. As a general approximation PKI can be used to sign any frames within the 802.11 protocol but such an implementation would be extensive and probably affect network performance. Another problem, as shown in section 2.5.4 figure 14, is that IEEE 802.11i does not protect management frames and control frame. This is vulnerable, and the IEEE 802.11w project is working on these problem issues. If the high assurance WLAN solution implements PKI, private keys can be used to provide authenticity and thereby avoid several attacks, such as DOS and flooding attacks, related to management and control frames.

Security Protocol	Security functionality
IEEE 802.1X	Defines a layer two framework for access control based on the Extensible Authentication Protocol (EAP) where EAP messages are used to exchange authentication data, execute authentication sequences and derivate cryptographic keys. The framework introduces an Authentication Server (AS), such as a RADIUS server, and uses port based access control (controlled/uncontrolled port) to restrict access to the distribution systems (DS). The EAP Transport Layer Security (EAP-TLS) protocol is a well supported and quality assured protocol, which is particularly adapted for WLAN public key infrastructures (PKI).
IEEE 802.11i	IEEE 802.11i is a layer two specific security protocol, where IEEE 802.1X provides the authentication framework within an IEEE 802.11i settlement. IEEE 802.11i, also known as the WPA2 standard, introduces specifications on encryption, authenticity, integrity and approaches to key management. IEEE 802.11i defines the 4-way handshake which is used to establish, confirm and authenticate key materials. I addition AES-CCMP is implemented to protect transmission of wireless data traffic. IEEE 802.1X based authentication and IEEE 802.11i AES-CCMP, establishes Robust Security Networks (RSN's).

Table 7: Summary and overview of IEEE 802.1X and IEEE 802.11i

4.3.1 Further work

We may conclude that security protocols such as IEEE 802.1X combined with IEEE 802.11i is a good starting point for building secure wireless solutions. In addition, if access control and authentication mechanisms are based on PKI implementations, it is possible to manage a wide range of threats concerning wireless networks. But, even if we implement such solution we do not have any control over which device that operates within the wireless area or receiving signals from the network. As a compromise to physical security, we need to implement functionality to observer, control and guard the wireless channels and the network to supervise availability. This brings along the problem that IEEE 802.1X and IEEE 802.11i does not have the ability to protect the wireless network and prevent devices against attackers and intruders which tries to infiltrate the wireless environment. We need mechanisms which are capable to detect unauthorized devices that try to associate with network and device which initiates attack against the WLAN infrastructure. I addition we need mechanisms which are capable to automatically handle the threats, protect the environment and locate devices which operates denunciatory. In the next section I will introduce a system that potentially may meet availability aspects by inserting mechanisms for monitoring, control, detection and protection of high assurance wireless environments.

5 Availability – control, detection and protection

In order to safeguard the wireless network it is required to add security mechanisms to protect the wireless environment against threats and malicious activities. Intrusion detection system (IDS) [72] for wired LAN networks have been known for many years and introduces sets of security tools with capabilities to supervise and protect computer networks. The idea behind IDS systems can be transferred into wireless networks in order to observe, control and detect unwanted and spurious wireless traffic. To implement a wireless detection system, wireless sensor devices must be distributed to monitor data channels and frames in order to analyze traffic, detect abnormalities and protect the wireless network environment. Over the last years vendors and research companies [16, 27, 32, 33, 34] have been working on developing solutions for wireless detection and protection systems based on using IEEE 802.11 access points put in monitor mode, set to observe the wireless network. Some solutions have monitor functionality implemented into corporate access points (AP's), others suggest external and independent distributed monitors (sensor AP's) for wireless system monitoring and supervision. In the following chapter the thesis will investigate wireless intrusion detection and protection mechanisms and discuss how wireless monitor devices (access points put in monitor mode) can be used for perimeter control and to identify wireless threats and vulnerabilities. In terms of protecting the wireless environment and its legitimate devices, the thesis will discuss and propose ways to design a monitor defence system including capabilities to respond to active attacks. Since no architecture for wireless protection systems has been provided, the monitor system architecture presented in this thesis will be based on ideas concerning the following papers [73, 74, 75], which renders the possibility to develop a Monitor Defence System (MDS) as a principle design.

5.1 Availability aspects

To address availability aspect of wireless networks, access control, confidentiality, integrity and authenticity are important security prospects in order to oblige WLAN threats and vulnerabilities. Even though, to comply with physical security and to handle availability challenges, research [73, 74, 75] has introduced ideas of using wireless sensor devices to observe the wireless network environment in order to control the enterprise, its operations and the security settlement. To do this, passive WLAN monitors must be distributed to "watch the waves", giving administrators the ability to foresee and detect security breaches and threat occurrence. This requires a trusted 3rd party security system to be implemented capable to address WiFi availability aspects which can not be handled by implementing protocols such as IEEE 802.1X and IEEE 802.11i. Wireless monitor systems with intrusion-detection-and-protection capabilities are still in the early evolution process, but the fundamental idea behind such implementations has security promising opportunities. This section will describe and discuss wireless monitor system used for intrusion detection in wireless environments and how wireless active protection system can be used to guard the wireless network.

5.1.1 Observing the wireless network and the environment

Observing the wireless network can be performed by corporate access points (AP's) or using external wireless access points (AP's) put in monitor mode (sensor devices). As mentioned in [74], a single AP can not effectively monitor the WLAN network environment without adversely impacting associated clients and degrade network performance. The main task of traditional AP's is to operate as a link-layer-forwarder (wireless link-layer bridge) and exchange data packets between the wireless network and the corporate wired network (DS). If the AP is configured to monitor the WiFi channels for intrusion detection, it will potentially degrade network performance. Passive sensor devices (monitor AP's) that are dedicated as observation posts and set to report what it can "hear", will not interfere with operational wireless system. On the other side, using wireless sensors in encrypted wireless environments signifies that only the physical-layer (OSI-layer-1) and link-layer (OSI-layer 2) headers can be supervised. As shown in figure 32, the access point can also operate as an active protection device (red). Active protection devices will be closer described later in this chapter in section 5.2.

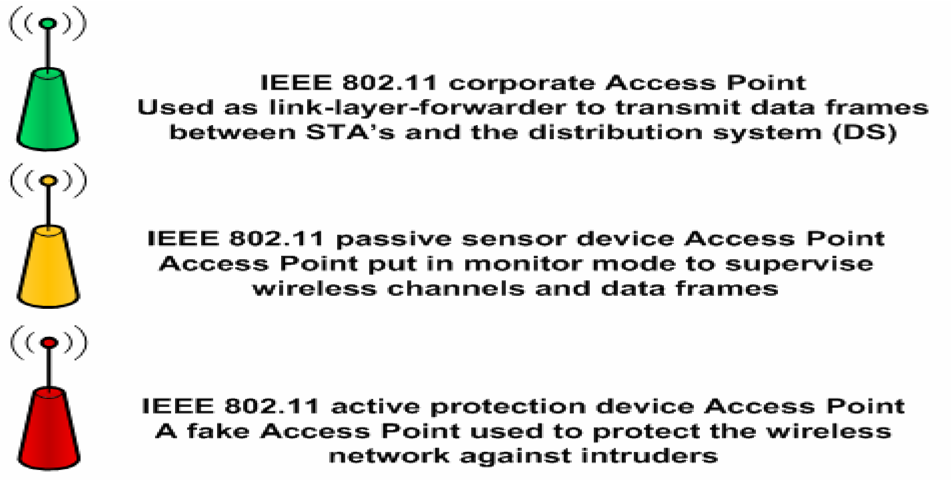

IEEE 802.11 corporate Access Point
Used as link-layer-forwarder to transmit data frames between STA's and the distribution system (DS)
IEEE 802.11 passive sensor device Access Point
Access Point put in monitor mode to supervise wireless channels and data frames
IEEE 802.11 active protection device Access Point
A fake Access Point used to protect the wireless network against intruders

Figure 32: Shows three access points used in different scenarios

5.1.1.1 Types of wireless sensor and detection systems

As a general approach, there are four potential ways to observe the wireless network. The first two ways are either using the existing wireless infrastructure (corporate AP's) or using independent wireless distributed sensor devices (monitor AP's) to observe data traffic. The third way to observe wireless communication aspects is host based sensor systems implemented into STA's and a fourth possibility is to use wired sensor systems implemented on the LAN side. Often a combination of such sensors is required to fully analyse the network communication spectrum. The wireless sensor system scenario is shown in figure 33. Because different sensors have various capabilities, a wireless monitor solution should be deployed as a welled combination of wireless distributed sensors, host-sensors and wired LAN sensors which together provide data collection and abnormal detection functionality. This thesis will mainly focus on wireless distributed sensor devices and capabilities.

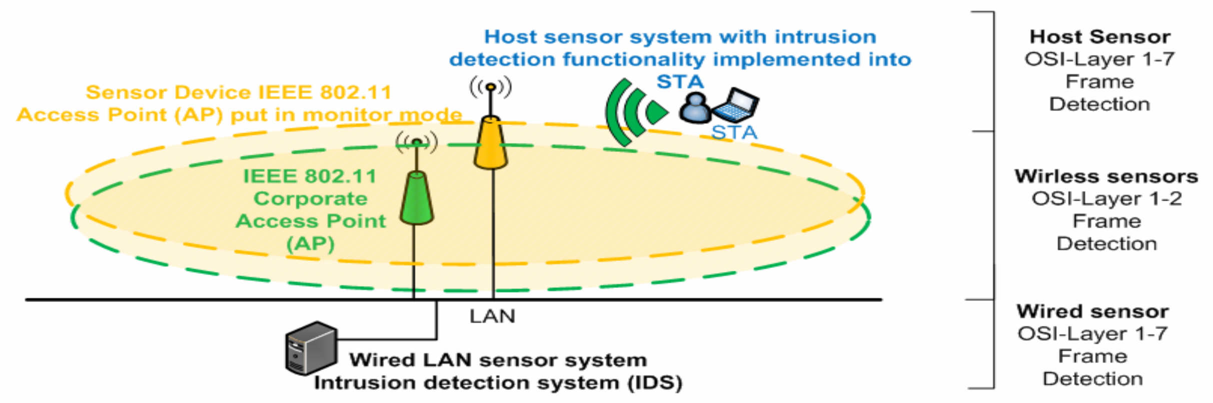

Host sensor system with intrusion detection functionality implemented into STA
Sensor Device IEEE 802.11 Access Point (AP) put in monitor mode
STA
IEEE 802.11 Corporate Access Point (AP)
LAN
Wired LAN sensor system Intrusion detection system (IDS)
Host Sensor
OSI-Layer 1-7
Frame
Detection
Wirless sensors
OSI-Layer 1-2
Frame
Detection
Wired sensor
OSI-Layer 1-7
Frame
Detection

Figure 33: Types of sensors in wireless network

1. Wireless sensors using corporate access points (AP's)

A wireless sensor system may be implemented into AP's using the existing wireless infrastructure network to collect data. Besides forwarding link-layer network traffic, the AP has to scan channels and report events to a detection server. The advantage of using the AP to monitor the wireless network is to possibility to supervise clear text frames including data and headers. The drawback is that the AP will operate less effective and for a WLAN system which handles a large number of users, it will potentially affect and degrade the wireless network performance. The thesis will not consider AP as a topical sensor device.

2. *Distributed wireless sensors devices*

Distributed wireless sensors are based external IEEE 802.11 access points, which are put into monitoring mode to observe the wireless network traffic. These devices act as sensor probes collecting frames and forwarding them to a detection system which examines the frames and the headers. This requires the sensors to be distributed within wireless network area to cover the scope and the channel accessibility. A drawback is that distributed wireless sensors cannot analyse encrypted frames and thereby not capable to examine data from higher layers. On the other side, wireless sensors can observe the physical-layer and link-layer headers which render the possibility to detect a wide range of wireless threats and vulnerabilities. This is because the wireless association process basically consists of OSI-layer 1 and OSI-layer 2 communication prospectives, shown in figure 34. In section 5.1.3 and 5.1.4 wireless sensor capabilities, advantages and disadvantages will be discussed.

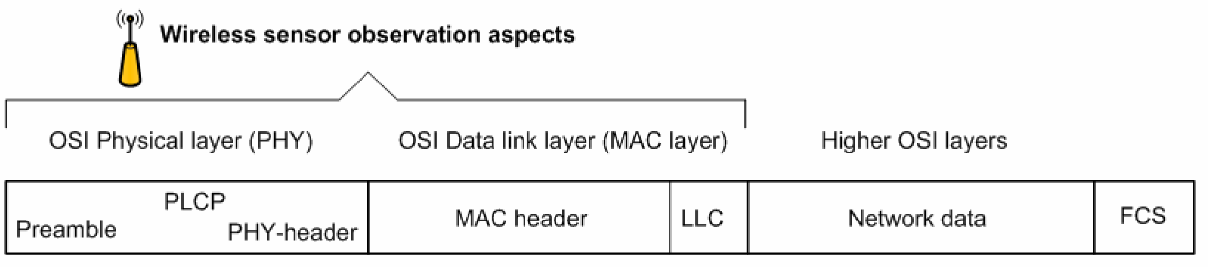


Figure 34: Wireless sensor observation aspects

3. *Wired LAN sensors*

A wired LAN sensor, which is used by traditional intrusion detection systems (IDS), is typically implemented on the LAN side behind the access point (AP) and plays an important part of a wireless monitoring solution. A wired LAN sensor system is shown in figure 35. The wired-sensors referred to as “Land-Monitors” in [74], can be used to analyse clear text LAN packets as well as clear text frames and can examine data from the higher OSI-model layers. The wired sensor can observe LAN traffic and collect data frames floating between the AP and the distribution system (DS) as well as between the AP and the authentication server (AS).

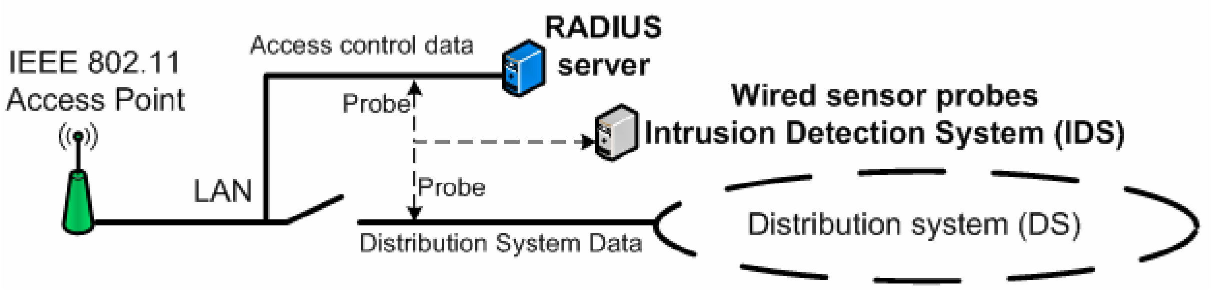


Figure 35: Wired LAN sensors Intrusion Detection System (IDS)

4. *Host sensors implemented into STA's*

Host sensor system, known as host based intrusion detection systems (IDS), is implemented into each authorized STA's which uses the high assurance wireless network. A host based IDS is capable to detect several potential vulnerabilities directed towards STA's both covering OSI-layer one and two, as well as higher OSI-layers. The host-sensor IDS system can block the STA wireless access if severe threat occurs, and report threat events to the wireless monitor system. The advantage is that a host IDS can examine clear text data, but the drawback is that with heavy load of data the IDS will potentially degrade STA communication performance. Due to the time limit, this thesis will not be able to focus on STA sensor IDS system.

5.1.2 A wireless distributed monitor architecture

A wireless monitor system typically consists of several components which interconnects and solves different tasks in order to supervise and control the wireless environment. Figure 36 show a principle design model how of wireless monitor system architecture could look like.

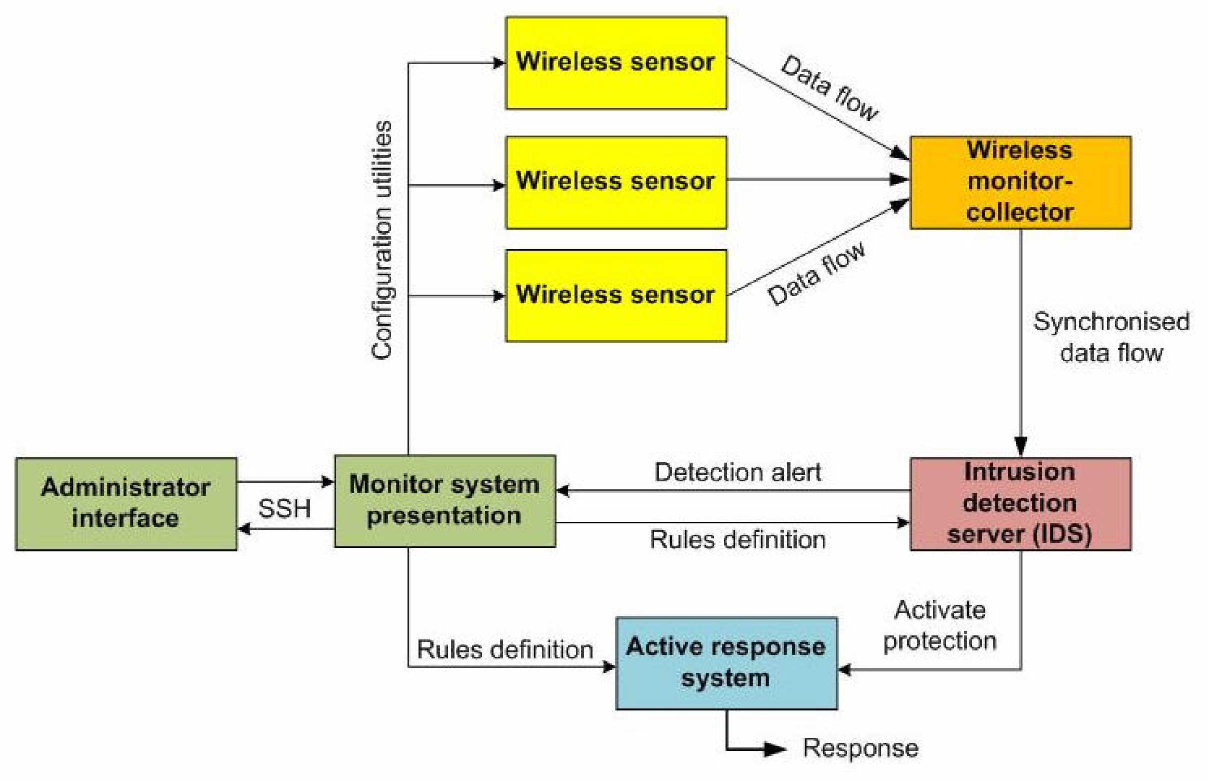


Figure 36: Principle architecture of a wireless monitoring system

As figure 36 shows, the wireless sensor devices (yellow) perform monitoring as stand alone hardware sensors distributed within the wireless environment. These devices report RF-channel data frames to a wireless monitor-collector. The monitor collector is responsible to organize the wireless data channels and synchronize the data to be delivered to the intrusion detection system (IDS). The intrusion detection system analysis and examines the data stream based on rules defined by the administrator system. The sensor-devices operates passively, which means that they can not be wirelessly detected, connected to or associated with using other wireless LAN equipment. The wireless sensor listens to IEEE 802.11 traffic frames, by scanning available channels within the wireless network area. As shown in table 2 chapter 2, the ISM band (2.4 Ghz) consists of 11 channels, and to cover channel range, the sensor-devices must listen to different channels in time. This signifies that incoming frames on particular channels may be lost. To prevent this, more sensor devices must be distributed to cover the different channels more effectively. The active response system is meant to act and respond to different threats and attacks detected by the IDS system. The active respond systems system will be closer described section 5.2. A wireless monitor system and components are shown in figure 37.

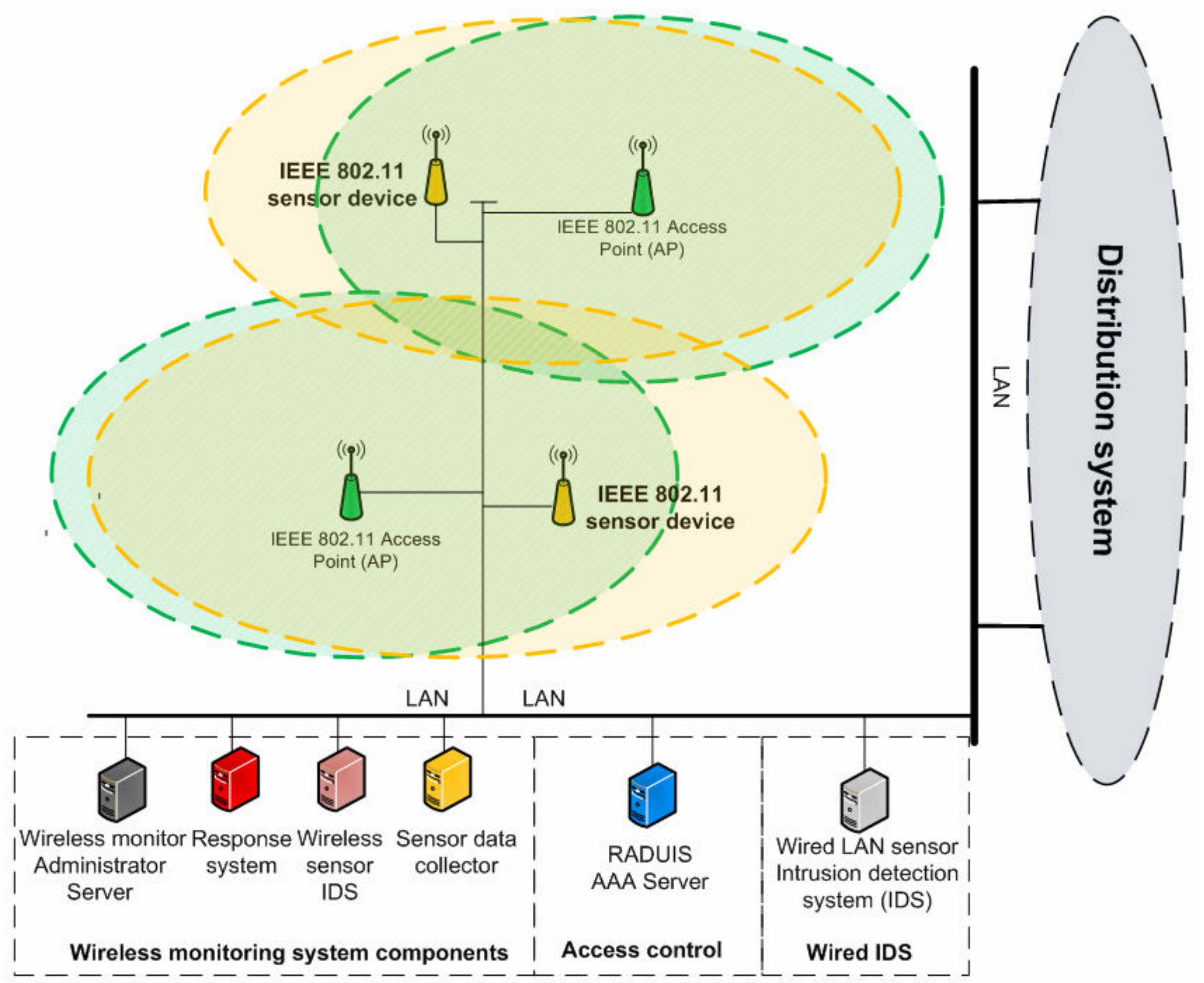


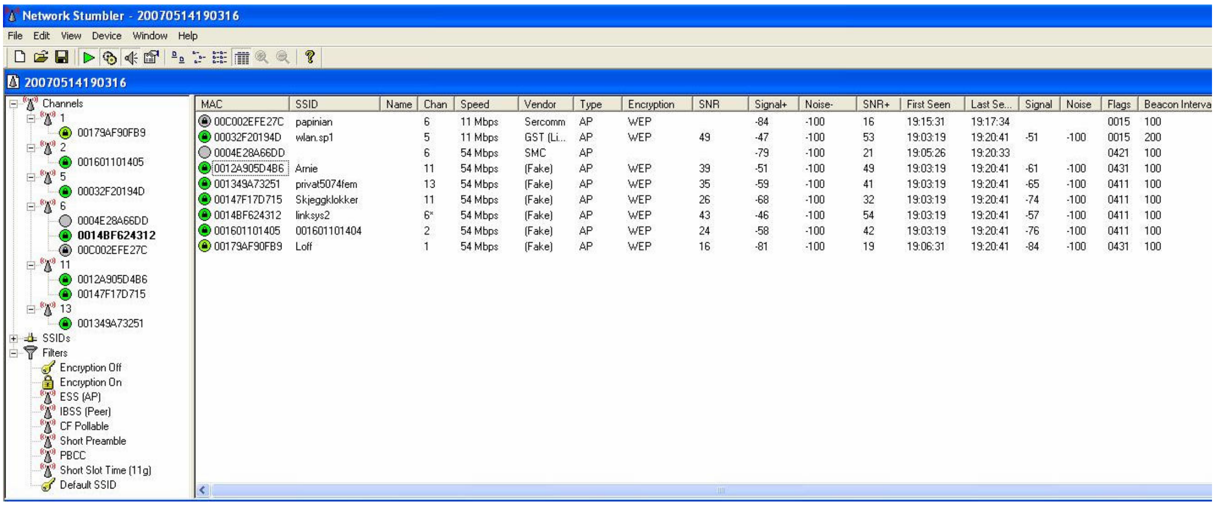
Figure 37: Wireless monitor system implementation

5.1.3 Wireless monitor system advantages and capabilities

As earlier discussion indicates, wireless monitoring system has many potential options that can be used to address several security challenges related to wireless network. The capability list is entirely interesting and research is still progressing to meet new types of threats and vulnerabilities. In following section I will present some of the main security tasks and principle application areas which such systems are capable to address.

- ***Detection of SSID, channels and security configuration***

Even if an AP broadcasts SSID or not, STA and AP beacons signals can be easily identified by monitoring the wireless network environment. Based on this, mechanisms can be used to filter out different networks and their security configuration and requirements. Network Stumbler (NetStumbler) [76] is an example of a free software tool that monitors and captures information about nearby WLAN networks. Monitoring channels, SSID's and security parameters can be used for protection objectives as well as for potential intruders that seeks wireless network information. Figure 38 shows how NetStumbler easily captures information on different access points related to SSID, channels, MAC addresses, security configurations, signal level, noise level, data rates, protocols etc.



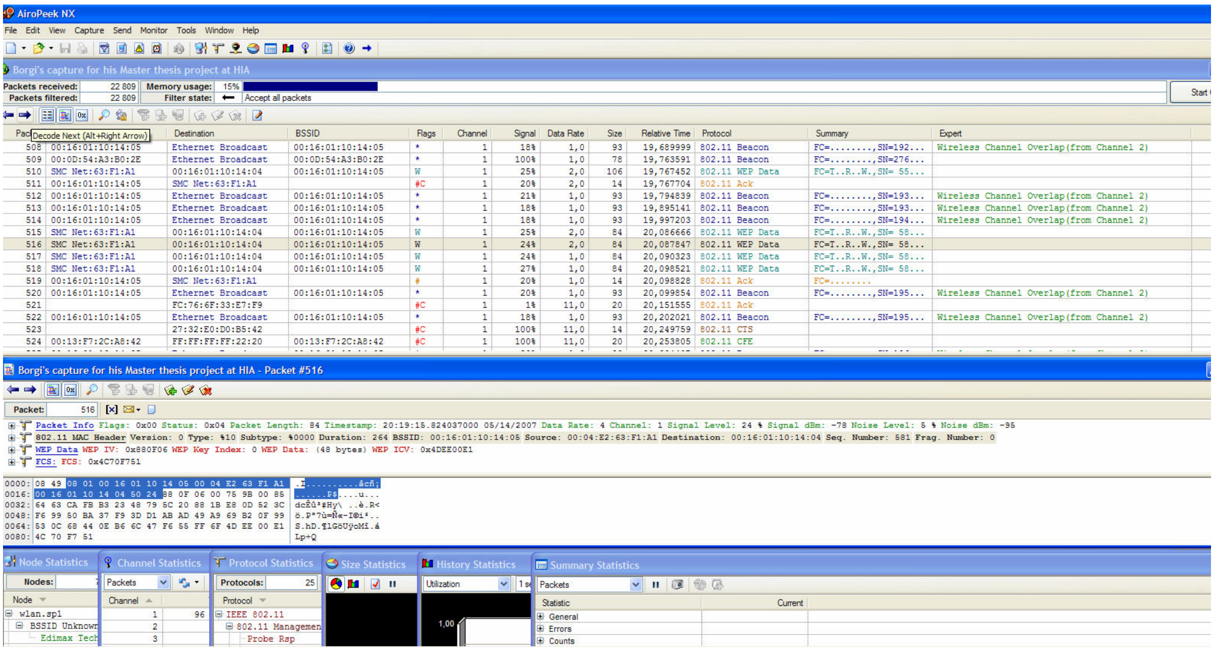
Channels
1
00179AF90FB9
2
001601101405
5
00032F20194D
6
0004E28A66DD
0014BF624312
00C002EFE27C
11
0012A905D4B6
00147F17D715
13
001349A73251
SSIDs
Filters
Encryption Off
Encryption On
ESS (AP)
IBSS (Peer)
CF Pollable
Short Preamble
PBCC
Short Slot Time (11g)
Default SSID

MAC	SSID	Name	Chan	Speed	Vendor	Type	Encryption	SNR	Signal+	Noise-	SNR+	First Seen	Last Se...	Signal	Noise	Flags	Beacon Interva
00C002EFE27C	papinian		6	11 Mbps	Sercomm	AP	WEP		-84	-100	16	19:15:31	19:17:34			0015	100
00032F20194D	wlan.sp1		5	11 Mbps	GST (Li...	AP	WEP	49	-47	-100	53	19:03:19	19:20:41	-51	-100	0015	200
0004E28A66DD			6	54 Mbps	SMC	AP			-79	-100	21	19:05:26	19:20:33			0421	100
0012A905D4B6	Arnie		11	54 Mbps	(Fake)	AP	WEP	39	-51	-100	49	19:03:19	19:20:41	-61	-100	0431	100
001349A73251	privat5074fem		13	54 Mbps	(Fake)	AP	WEP	35	-59	-100	41	19:03:19	19:20:41	-65	-100	0411	100
00147F17D715	Skjeggklokker		11	54 Mbps	(Fake)	AP	WEP	26	-68	-100	32	19:03:19	19:20:41	-74	-100	0411	100
0014BF624312	linksys2		6*	54 Mbps	(Fake)	AP	WEP	43	-46	-100	54	19:03:19	19:20:41	-57	-100	0411	100
001601101405	001601101404		2	54 Mbps	(Fake)	AP	WEP	24	-58	-100	42	19:03:19	19:20:41	-76	-100	0411	100
00179AF90FB9	Loff		1	54 Mbps	(Fake)	AP	WEP	16	-81	-100	19	19:06:31	19:20:41	-84	-100	0431	100

Figure 38: NetStumbler overview

- ***Physical layer and data link layer frame analysis***

As indicated in figure 38, the physical layer frame header can be used to examine signal strength, noise levels and data rates in order to detect disturbances/interference and areas of poor wireless coverage. This is an important tool in planning a WLAN settlement and to find appropriate locations for AP's. The data link layer, including the MAC frame as described in section 2.3.1, can be used to verify information, such as valid MAC addresses (physical addresses), frame types (data, control or management frame), protocol types, different types of nodes, encrypted networks etc. Another example is that monitoring system can observe the RSNI field, as show in figure 19 in chapter 3.1, which makes it possible to outline number of unauthorized devices which do not meet the security requirements. Figure 39 shows an example of a wireless network-analyser tool called AiroPeek[85], which shows how OSI-layer one and OSI-layer two information aspects can be easily observed through monitoring.


AiroPeek NX
File Edit View Capture Send Monitor Tools Window Help
Borgi's capture for his Master thesis project at HIA
Start

Packets received:	22 809	Memory usage:	15%
Packets filtered:	22 809	Filter state:	Accept all packets

Decode Next (Alt+Right Arrow)

Pac		Destination	BSSID	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol	Summary	Expert
508	00:16:01:10:14:05	Ethernet Broadcast	00:16:01:10:14:05	*	1	18%	1,0	93	19,689999	802.11 Beacon	FC=........,SN=192...	Wireless Channel Overlap(from Channel 2)
509	00:0D:54:A3:B0:2E	Ethernet Broadcast	00:0D:54:A3:B0:2E	*	1	100%	1,0	78	19,763591	802.11 Beacon	FC=........,SN=276...	
510	SMC Net:63:F1:A1	00:16:01:10:14:04	00:16:01:10:14:05	W	1	25%	2,0	106	19,767452	802.11 WEP Data	FC=T..R..W.,SN= 55...	
511	00:16:01:10:14:05	SMC Net:63:F1:A1		#C	1	20%	2,0	14	19,767704	802.11 Ack		
512	00:16:01:10:14:05	Ethernet Broadcast	00:16:01:10:14:05	*	1	21%	1,0	93	19,794839	802.11 Beacon	FC=........,SN=193...	Wireless Channel Overlap(from Channel 2)
513	00:16:01:10:14:05	Ethernet Broadcast	00:16:01:10:14:05	*	1	18%	1,0	93	19,895141	802.11 Beacon	FC=........,SN=193...	Wireless Channel Overlap(from Channel 2)
514	00:16:01:10:14:05	Ethernet Broadcast	00:16:01:10:14:05	*	1	18%	1,0	93	19,997203	802.11 Beacon	FC=........,SN=194...	Wireless Channel Overlap(from Channel 2)
515	SMC Net:63:F1:A1	00:16:01:10:14:04	00:16:01:10:14:05	W	1	25%	2,0	84	20,086666	802.11 WEP Data	FC=T..R..W.,SN= 58...	
516	SMC Net:63:F1:A1	00:16:01:10:14:04	00:16:01:10:14:05	W	1	24%	2,0	84	20,087847	802.11 WEP Data	FC=T..R..W.,SN= 58...	
517	SMC Net:63:F1:A1	00:16:01:10:14:04	00:16:01:10:14:05	W	1	24%	1,0	84	20,090323	802.11 WEP Data	FC=T..R..W.,SN= 58...	
518	SMC Net:63:F1:A1	00:16:01:10:14:04	00:16:01:10:14:05	W	1	27%	1,0	84	20,098521	802.11 WEP Data	FC=T..R..W.,SN= 58...	
519	00:16:01:10:14:05	SMC Net:63:F1:A1		#	1	20%	1,0	14	20,098828	802.11 Ack	FC=........	
520	00:16:01:10:14:05	Ethernet Broadcast	00:16:01:10:14:05	*	1	20%	1,0	93	20,099854	802.11 Beacon	FC=........,SN=195...	Wireless Channel Overlap(from Channel 2)
521		FC:76:6F:33:E7:F9		#C	1	1%	11,0	20	20,151555	802.11 Ack		
522	00:16:01:10:14:05	Ethernet Broadcast	00:16:01:10:14:05	*	1	18%	1,0	93	20,202021	802.11 Beacon	FC=........,SN=195...	Wireless Channel Overlap(from Channel 2)
523		27:32:E0:D0:B5:42		#C	1	100%	11,0	14	20,249759	802.11 CTS		
524	00:13:F7:2C:A8:42	FF:FF:FF:FF:22:20	00:13:F7:2C:A8:42	#C	1	100%	11,0	20	20,253805	802.11 CFE		

Borgi's capture for his Master thesis project at HIA - Packet #516

Packet: 516

```
Packet Info Flags: 0x00 Status: 0x04 Packet Length: 84 Timestamp: 20:19:15.824037000 05/14/2007 Data Rate: 4 Channel: 1 Signal Level: 24 % Signal dBm: -78 Noise Level: 5 % Noise dBm: -95
802.11 MAC Header Version: 0 Type: %10 Subtype: %0000 Duration: 264 BSSID: 00:16:01:10:14:05 Source: 00:04:E2:63:F1:A1 Destination: 00:16:01:10:14:04 Seq. Number: 581 Frag. Number: 0
WEP Data WEP IV: 0x880F06 WEP Key Index: 0 WEP Data: (48 bytes) WEP ICV: 0x4DEE00E1
FCS: FCS: 0x4C70F751
```

```
0000: 08 49 08 01 00 16 01 10 14 05 00 04 E2 63 F1 A1  .I..........âcñ¡
0016: 00 16 01 10 14 04 50 24 88 0F 06 00 75 9B 00 85  ......P$....u...
0032: 64 63 CA FB B3 23 48 79 5C 20 88 1B E8 0D 52 3C  dcÊû³#Hy\ ..è.R<
0048: F6 99 50 BA 37 F9 3D D1 AB AD 49 A9 69 B2 0F 99  ö.Pº7ù=Ñ«-I©i²..
0064: 53 0C 68 44 0E B6 6C 47 F6 55 FF 6F 4D EE 00 E1  S.hD.¶lGöUÿoMî.á
0080: 4C 70 F7 51                                      Lp÷Q
```

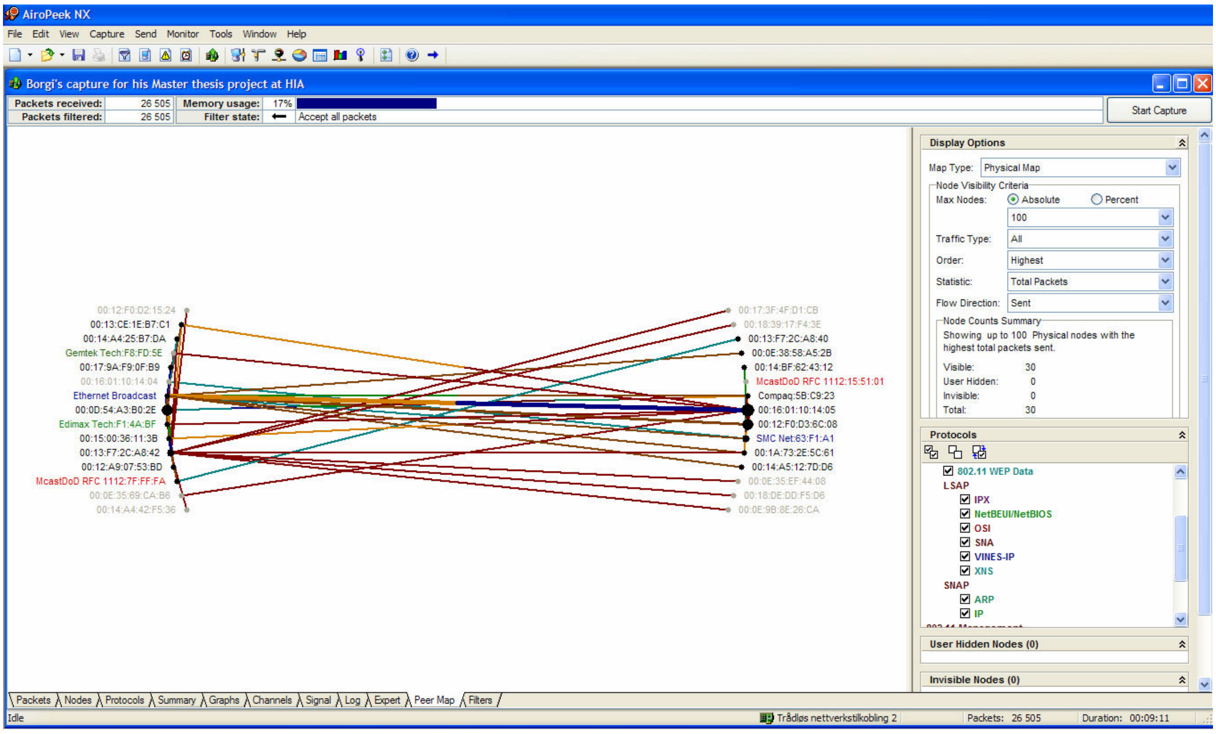
Figure 39: AiroPeek NX, a wireless LAN network analyser tool from Wildpackets.

Identifying STA/AP request/responses exchange

As shown in figure 39, a wireless monitoring system can be used to examine the messages flow between STA's and AP's in order to detect abnormal behaviour. This is a valuable property especially to supervise identification, authentication and association processes as discussed in chapter 3 and 4. For example the monitor system can detect increased numbers of disassociation messages which could indicate a flooding attack. The wireless monitor system has to interact with the access control server (RADIUS) to effectively verify and detect undesirable changes to the message flow. The RADIUS server possesses information on public keys used in the wireless network, and the public key can be used by the monitor system to verify different STA's authenticity. This signifies that the wireless monitor systems must be interconnected and integrated with the high assurance wireless system to be able to make the most out of its potential.

Mapping devices which operates within the wireless environment

As shown in figure 40, AiroPeek which is a wireless LAN analyzer tool, indicates that a monitoring system can be used to map devices which operate and communicate within the nearby wireless environment. Such a map can be used by a monitor system to detect wireless devices, which based on the physical address (MAC-address), do not belong to the corporate high assurance wireless network. The monitor system can use such information to follow unauthorized devices activity and detect the devices that experiments with high assurance network. Notice that such analyzer is dependant on that device acquires information and probes the air for available access points. It can not detect passive devices which operate within the wireless network area.



Packets received: 26 505 Memory usage: 17%
Packets filtered: 26 505 Filter state: ⟵ Accept all packets

Display Options

Map Type: Physical Map

Node Visibility Criteria

Max Nodes: ● Absolute ○ Percent

100

Traffic Type: All

Order: Highest

Statistic: Total Packets

Flow Direction: Sent

Node Counts Summary

Showing up to 100 Physical nodes with the highest total packets sent.

Visible:	30
User Hidden:	0
Invisible:	0
Total:	30

Protocols

- ☑ 802.11 WEP Data
- LSAP
  - ☑ IPX
  - ☑ NetBEUI/NetBIOS
  - ☑ OSI
  - ☑ SNA
  - ☑ VINES-IP
  - ☑ XNS
- SNAP
  - ☑ ARP
  - ☑ IP

User Hidden Nodes (0)

Invisible Nodes (0)

Idle Trådløs nettverkstilkobling 2 Packets: 26 505 Duration: 00:09:11

Figure 40: AiroPeek shows communication mapping based on the wireless observed MAC-addresses

Wireless rogue device detection

Typical threats to WLAN's systems are unauthorized devices such as rogue clients or access point's that acquires access to wireless network credentials or resources. A rogue AP device can be physically placed inside your network area (controlled area) either connected or not connected to the local infrastructure (LAN). These rough devices can be brought in by employees, visitors or attackers that gains physical access to the network area. Alternatively, rogue AP's can be placed as neighbouring network outside the network area but still reachable for STA's and AP's within the controlled area. If a legitimate STA connects to a rogue AP, or a rogue AP manages to associate with the local distribution system (LAN), it can potentially reveal all WLAN security. Distributed monitor systems can be used to detect new devices that occur within WLAN range. As described in [74] this can be done implementing filters that summarizes the SSID (AP network name) and the belonging MAC addresses (physical address), and at regular intervals transmit this information to a detection server. This functionality might be vulnerable because attackers can use phishing techniques to fake both SSID and the MAC address. The rogue devices detection mechanisms should include a counter that systematize the number of AP's and verifies broadcast messages to verify public keying signatures. This signifies that the monitoring system must know the public keys deployed in the wireless network and, as all ready mentioned, cooperate with the access control server (RADIUS). In addition the wireless monitor systems must confirm if rogue AP's are physical connected to corporate LAN or not. This can be accomplished by checking if the rogue device is reachable from the LAN side. Based on this verification the detection server can decide what action to perform to prevent to rogue devices to obtain network critical information.

- ***Location providers***

A distributed sensor system can be used to locate devices (STA's) operating within the WLAN network area by measuring the received signal strength from wireless devices. For accurate location estimation, multiple sensors should work together and exchange measurement data. The wireless sensor system can be used to collect data that can be used draw maps and position STA's and AP's current location. Location services can be used for defence control, access control and for attacking objectives. The thesis will discuss location services in section 5.2.4.

- ***Detection of Denial Of Service (DOS) attack***s

Several flaws in the IEEE 802.11 network architecture [78, 77] can be used to perform variety of DOS attacks to wireless networks. Attackers exploiting flaws in 802.11 protocols may potentially disable the wireless link and disrupt communication. For example primitive radio equipment can be used to broadcast noise which interferes with the WLAN 2,4 GHz frequencies area, or invalid frame can be broadcasted to AP's and STA's in order to interrupt the wireless communication. A described in [77], large number of association/disassociation request or EAP-authentication failure messages can be transmitted in order to turn down AP's and STA's. Apparently, the detection system may easily detect such abnormal behaviour, and the AP can automatically block the attacker MAC address to prevent further actions. On the other side an attacker may use random MAC address spoofing to perform the attack, which complicates the protection process. To handle such scenarios active respond mechanisms are required to either lure the attacking devices to a "wireless honeypot network" or as described in [78] transmit malformed frames directed specifically at the intruder to crash the attacker system. Using the monitor system to locate the attacking devices makes it possible physically to find and remove the enemy device. Active responds systems are closer described in section 5.2.

- ***Supervise flaws of the MAC protocol***

Because of the flaws in the IEEE 802.11 MAC protocol described in [77], a wireless monitoring system renders the possibility to observer the MAC protocol and report if changed behaviour occurs. Referred to [73], this is crucial for effective diagnostic of wireless LAN's. The monitor system can observe frames and detect changes based on known flaws of the 802.11 protocol, for example disassociation frames or unsecured management and control frames.

5.1.4 Wireless monitor systems drawbacks and infirmities

The following will describe some challenges and weaknesses considering a wireless monitoring systems deployment.

- ***Monitoring in wireless encrypted data network***

A wireless monitoring system which is implemented as part of an encrypted OSI-layer 2 RSN environment lacks the ability to examine data frames. This means that the intrusion detection server, as shown in figure 36 and 37, can not examine other information aspects than physical layer headers and the link layer headers. To be able to examine higher layers of the OSI model, a wired LAN IDS system [72] must be implemented on the LAN network to capture and analyse clear text data frames. A wired LAN IDS system, as showed in figure 35, can control data in order to supervise and detect suspicious network traffic coming from the higher OSI-layers.

- ***High costs and heavy implementations***

A wireless monitoring system may constitute a complicated implementation, involving a large number of sensors, over-complex system architecture and high costs. The DAIR [74] project introduces ides of using wireless USB devices based on IEEE 802.11 technology to be distributed among stationary machines and laptops using the enterprise network infrastructure to probe the wireless network. This is an interesting approach to large enterprise wireless solutions which requires wireless detection and protection systems. For example it possible to equip each authorized STA with two wireless network cards, where one of the cards is used to operate towards the corporate WLAN network, whereas the other network card is used the monitor wireless activity.

- ***Limited capacity of each sensor and capturing capability***

Each sensor devices used in a wireless monitoring system may either scan a subset of the available channels or constantly monitor a predefined channel. If a sensor is set to scan channels it is possible to miss important frames and network message when hopping to other channels. If the sensor stays on dedicated channel it will capture all particular channel information, but it will miss information on other frequency-channels. To solve this more sensors must be distributed and interconnected to effectively cover a more appropriate channels subset. This is also a question of complexity, probability and the consequences of loosing some frames. Based on [77], a single wireless sensor and its capturing capability are limited in terms of measurement loss (packets loss) and the hearing (receiving) range. Additionally the sensor can only collect data from one channel at the time, and the receiving capability is depending on sensor hardware, antenna propagation and the signal strength.

- ***False positives detections***

The system relays on the intrusion detection server to analyse data in order to detect suspicious activity. This might result in false alarms when legitimate devices fail to authenticated to the WLAN system. IDS rules and statistics must be implemented in order to separate normal activity from abnormal behaviour and to segregate intruders from authorized devices. This means that a wireless monitor system must learn and tune its detection capabilities. For example, the monitor system could make statistics on particular flawed frames, such as deauthentication frames, and observer and estimate changes compared to normal activity. This would make it possible to detect potential flooding attacks and DOS attacks which utilize weaknesses of the IEEE 802.11 MAC protocol [77].

- ***Eavesdropping and passive attacks***

Eavesdropping as explained in section 2.4.2.1, are based on attackers and outsiders that passively listens to the wireless data traffic, and secondly uses code breaking techniques to compromise data packets. As concluded in [74] such attacks are extremely difficult to handle, if not impossible to detect by a monitoring system and therefore the wireless security system must relay on the implemented confidentiality mechanisms. On the other side [78] suggest to meet such threats by inserting a legitimate “Fake-AP” network and a “wireless honeypot” which indents to confuse and lure eavesdroppers/attackers to listen to and potentially associate with a fake wireless system. Wireless honeypot system is a fundamental idea according to insert protection functionality in wireless networks, and the thesis will investigate this idea in section 5.2.

- ***Data collection scalability***

In an enterprise high security wireless network environment, a large amount of monitoring data will be collected, which means that the monitoring system must handle heavy loads of information. A centralized detection server solution may be become a bottleneck. To increase scalability aspects the wireless sensor device can be composed with intelligence, which in distributed manner can solve detection and protection task more efficiently.

5.2 Monitor system and active responses

An ideal intrusion detection system (IDS) should actively respond to threats. Wireless monitor system which uses passive components (passive sensor AP's), creates challenges according to perform active protection to prevent none-legitimate devices and intruders from fumbling with the corporate WLAN system. A wireless monitor protection system requires active devises which based on threat-occurrences may correspond and communicate with potential intruders in order to defend the wireless network. As discussed section 5.1.3, unauthorized devices which attempts to connect to corporate WLAN can be easily detected by the monitoring system. To respond to such incidents active sensor devices (AP's), which in this section will be referred to as "Fake AP response devices", must be implemented by the monitor system to be able to warn intruders and inspect the potential threat.

5.2.1 A monitor protection system and architectural issues

Working on active protection functionality in a wireless environment is difficult and very challenging area. Monitoring system can easily detect a wide range of attacks against a wireless infrastructure, but how can we implement mechanisms which can automatically handle threats and attacks? As shown in figure 41, the wireless monitor system has been expanded with an Active Response System (ARS) marked in red. The ARS consists of several IEEE 802.11 "Fake access points" acting as response devices connected to a response system which prepares a "Fake AP honeypot network" (red). Referred to figure 37, the Active Response System (ARS) is part of a wireless monitor system solution, where active devices are used cover protection aspects which the passive devices can not handle. The purpose of using active devices is the opportunity to correspond with potential intruders and to collected information about impending devices. Active devices, which is basically a normally access point, have the ability to actively respond to threats. As shown in figure 41, the "Fake AP" honeypot network is interconnected with the active device and establishes a "Fake AP" environment which from an attacker point of view tends to look like the corporate high assurance WLAN network. The active respond system is responsible to coordinate the active protection process which involves interconnection and cooperation with the passive monitor system and the corporate WLAN environment. As shown in figure 41, a location server has been added as physical component responsible for location services. Location services [81, 82, 83] can be achieved by using several passive and active IEEE 802.11 devices to measures signal strength and propagation to map and determine location control and distance to wireless devices which operates within the wireless environment. Location services will be closer described in section 5.2.4.

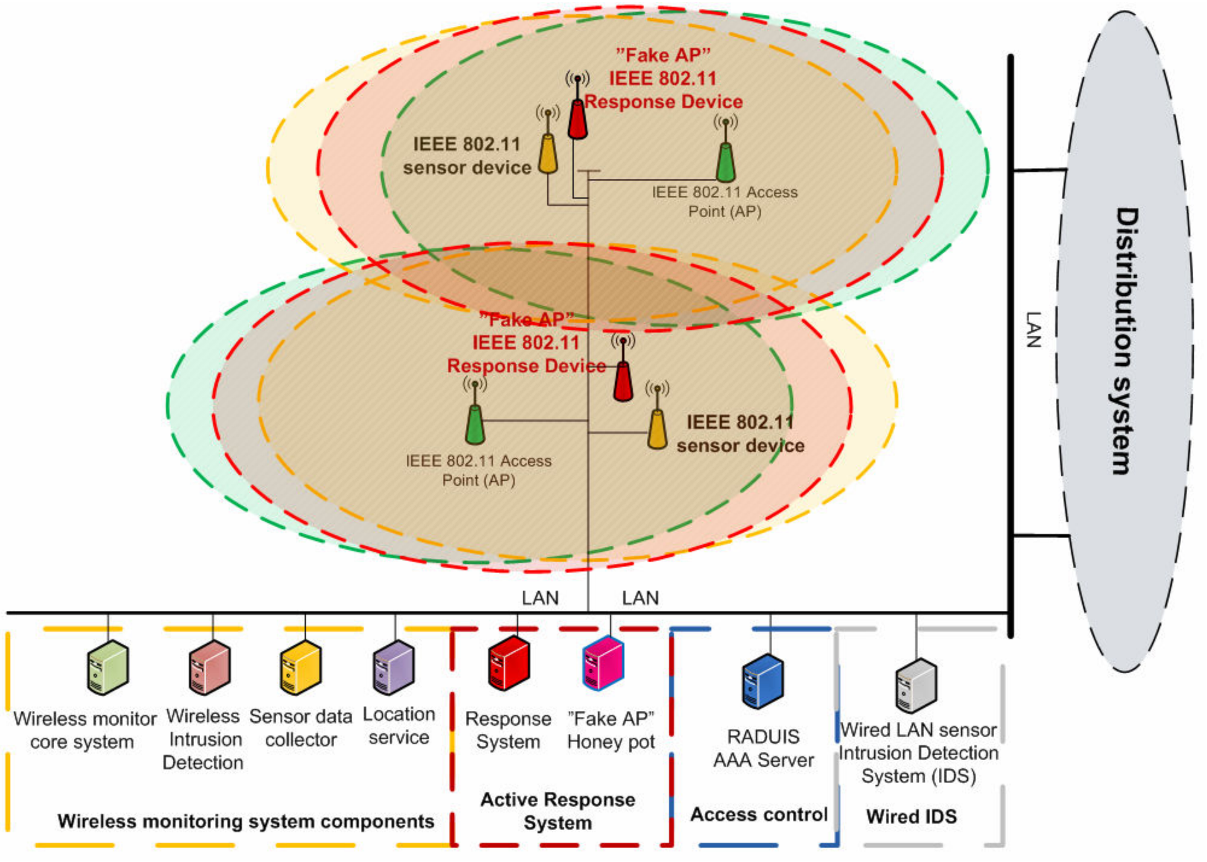


Figure 41: A wireless monitor and protection system principle design

As general approach, the wireless monitor protection system is capable to oblige several threats to WLAN's, and in the next section I will take a closer look at honeypot system, and how active devices are capable to protect the network. The following section 5.2.2 to 5.2.5 will discuss four important opportunities and challenges by implementing an active protection system. These challenges are; WLAN honeypot network (Fake AP), correspondence with none-legitimate devices, location service and active responses to threats.

5.2.2 Fake AP and WLAN honeypot network

To protect the WLAN environment and to confuse potential intruders the Active Response System (ARS) introduces decoys. A honeypot system [75, 80] is a fake computer system which is set up to trap attackers. In a wireless context fake access-point-networks can be established to lure attackers to connect to a falsified wireless network. The idea behind such network is to obtain information on potential intruders as well as to prevent none-legitimate devices from accessing and attacking the corporate WLAN network. The “Fake AP” honeypot system must perfectly simulate the corporate AP including configuration and security settings. To achieve this, the corporate AP must cooperate with the fake honeypot AP. In addition the active response system must cooperate with the RADIUS server. Only the RAIDUS server and the active response system know which access point is corporate and which is fake. This scenario is shown in figure 42.

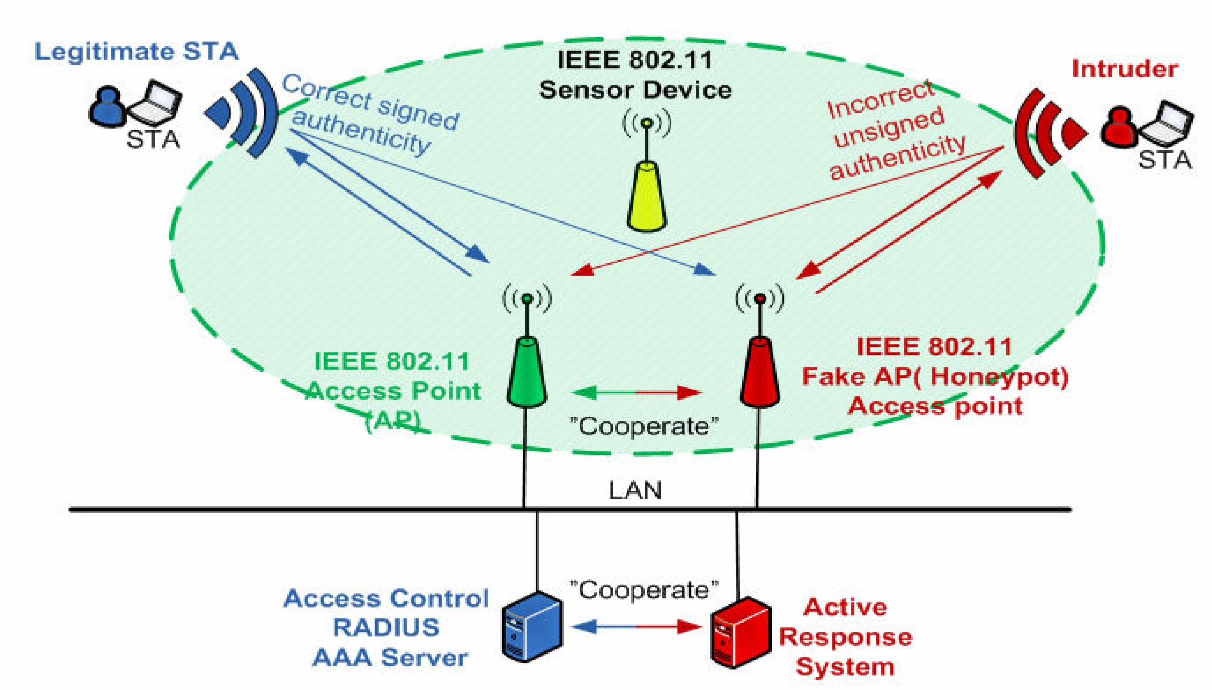


Figure 42: Wireless honeypot must cooperate with the legitimate WLAN.

The fake AP, which is controlled by the active response system (ARS), provides access to a honeypot wireless solution. The active response system (ARS) can then be used to capture information on the intruder device (STA) such as to check software, operation system, configurations and protocol types, security settings, port scanning, firewall etc. This data can be used to profile potential intruders and warn non-legitimate devices which experiments with the wireless network. The scenario has many potential challenges according to how such system, as shown in figure 42, should “corporate” to separate legitimate STA’s from intruder devices. If the wireless network is based on PKI, the corporate AP could use authenticity through correct signed requests (private key signature) and message verification to determined if the device is legitimate or not. If the device, as the intruder shown in figure 42, has an incorrect authenticity, the corporate AP could request the fake AP to connect with the devices. This is also shown in figure 43. The request can be forwarded by the RADIUS server to the active response system to initiate a connection with potential intruder device. The intruder devices will then associate with the fake AP honeypot system. The honeypot system may inform and warn the intruder devices about that it is trying to associate with wireless network which it is not authorized to use. A potential problem with this scenario may arise due to transmission bit-errors and interference, which may result in that legitimate devices associating with the network ends up in the fake AP honeypot solution. The WLAN honeypot solutions is still only a theoretically approach to how an active response system can be used to implemented automatic protection in high assurance WLAN systems. The idea needs to be closer evolved before it can be implemented, tested and verified as a protection solution for high assurance wireless networks.

5.2.3 Correspondence with none-legitimate devices

Another important challenge is how the fake AP honeypot solution will correspond with none-legitimate devices and how such systems would perfectly separate authorized STA's from unauthorized devices. "Wardriving" software [75], such as NetStumbler [76] and other wireless network tools can be used to acquire information about neighbourhood wireless network. These network tools request information, such as SSID, protocol types, configuration and security settings from nearby available Access Points (AP's) as shown in figure 38. Such network tools leave behind their connected hardware address (MAC address) and a monitor system will automatically detect addresses as a none-legitimate device. As described in [75], the monitor system can use the active devices, such as the fake AP honeypot, to fingerprint possible intruders to determined information such as software configuration, protocols configuration and operation system. This information can be used to profile the intruder for known vulnerabilities.

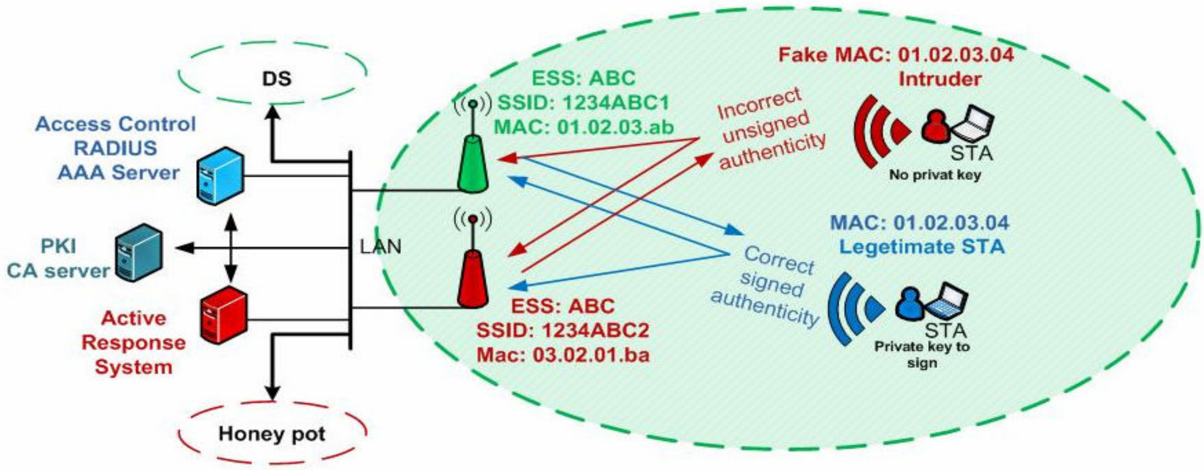


Figure 43: Intruder (fake MAC-address) ends up in the honey pot because of lacking authenticity.

If the intruder launches an attack against the WLAN network, the monitor system can defend the network more efficiently by exploiting the vulnerabilities and lure the attacker based on its own weaknesses. As shown in figure 43, the intruder uses a fake MAC address [79], the same address as the legitimate STA (blue). This creates problems for the monitoring system to separate unauthorized devices from authorized. The separation method should be based on authenticity verification in terms of a PKI implementation, as shown in figure 43. Based on the private-key signature verification the RADIUS server and the active response system coordinate which access point to reply. If the corporate access point (green) detects an unsigned authenticity request, it simply forwards this message to the RADIUS server which requests the fake AP (red) to associate with the potential intruder device.

5.2.4 Location services and location capability

Location services are important security features for high assurance WLAN's. As described and mentioned in [81, 82, 83, 84], location services can be implemented using information aspects considering the basic 802.11 protocol, such as collecting received-signal-strength-indication (RSSI) information and observing signal propagation delay [81, 83]. The RSSI field (1 byte) is defined by the 802.11 standard and consists of a numeric integer value with 256 different signal levels, ranging from 0-255. The STA RSSI value varies according to the distance between the STA and AP and the noise level. By comparing RSSI values received by several passive devices it is possible to determine the distance and the location of corresponding STA's. As mentioned in section 5.1.3, wireless location services and the ability to physically map devices, both legitimate and none-legitimate operating within the WLAN environment, are important security features. To do this the monitor system must include components which has location service functionality and is responsible for location control. The location server, which receives RF location data, is shown in figure 44. According to [81] location system which operates within a WLAN scenario must measure the signal strength and propagation delay from several sensor devices to parameterize a model of the WLAN environment. Active devices can be used to actively correspond, communicate and measure the round-trip latency [82], by exchanging messages. The location scenario is shown in figure 44.

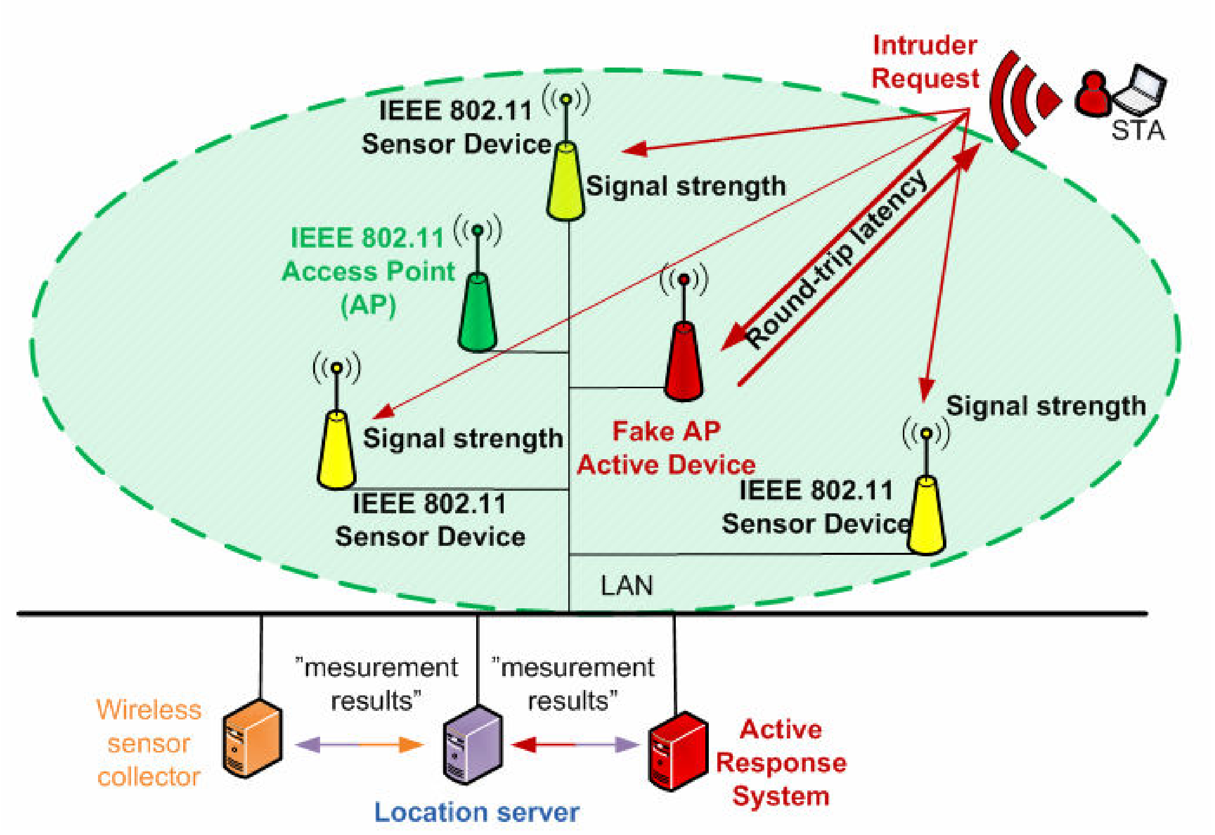


Figure 44: Location services

As shown in figure 44, both passive sensor devices (yellow) and the active fake-AP device (red) are used to determine the exact intruder devices location. The passive sensors devices measures the received signal strength level based on RSSI information, while the fake-AP initiates contact with devices and transmits random bit-patterns to determined the packet-transmission-time [83]. This measurement process is quit complex and as described in [83] the timing issue and device processing time makes it difficult to carry out accuracy. According to [84] calculations based on RSSI information field provides fairly accurate location assessment. An alternative solution is to implement location services by using global positioning systems (GPS) in order to localize wireless devices. As shown in figure 44 the location server must communicate and interconnect with the passive devices as well as the active devices. For additional security features the location server can be used to provide location based access control, as discussed in section 3.1.3. The RADIUS server can interconnect with the location server to provide WLAN location based access control [82]. This requires the location data to be implemented as part of the authentication requirement, and the LBAC protocol [82] describes how this could be accomplished.

5.2.5 Active responses

Basically there are several ways to actively respond to attackers which infiltrate the wireless network. Typical active invasions, such as flooding and DOS attacks, can ruin wireless communication services completely. A certain way to protect the WLAN system from these threats is to let AP's and STA's automatically block the intruder based on the MAC address. On the other side, the MAC address is easy to spoof and attackers may change to a valid hardware address using eavesdropping and MAC-changing [79] tools. Alternatively the AP or STA being attacked could automatically disable the wireless connection to prevent the system from being compromised. On the other hand such response will automatically degrade the network performance which is probably the attacking objective in the first place. Other ways to defend the network is to perform counterattacks using the same weapons such as STA flooding or DOS attacks to turn down the attacking device. Alternatively, as explained in [75], the monitoring system could use the intruder profile to exploit weaknesses and to direct malformed frames at the attacker device to crash the attacking computer system. According to [75] this is not recommended as primary protection mechanism. A fourth way to handle active attacks is mechanisms to lure the attacker to associate with the "Fake AP honey pot" system as described in section 5.2.2 and 5.2.3. This will prevent the corporate WLAN network from being affected. The "Fake AP" honeypot system could alert administrator as well as worn the intruder, and use the monitor system to locate the device so that administrators can remove it physically. The active response system can potentially operate as followings:

1. The passive monitor system observes the available channels, frames and the wireless traffic. If a threat is detected, the detection system will alarm the administrator system.
2. If the "intruder", as an unauthorized device (unsigned authenticity), experiments to associate with cooperate WLAN network, the corporate AP will block the intruder MAC address, and the wireless monitor system will automatically alert administrator and contact the active response system to transfer the "intruder" into the AP honeypot system. The AP honeypot system can warn the intruder and implore it to disconnect from the wireless network.
3. If the "intruder" as an unauthorized device, performs flooding, DOS or other active attacks against the WLAN system, the monitor system should automatically

transfer the intruder to attack the “Fake AP” honeypot system. This will potentially prevent the cooperate network from being affected. The monitor system should locate the device from where it can be physically removed.

4. If the intruder cannot be transferred to AP honeypot and continues to perform flooding or DOS attacks on a corporate WLAN AP, the monitor system may use its active devices (fake AP) to initiate counterattacks on the attacking device. The active response system will adjust the attack based on the intruder profile.
5. The last way to defend the network is to disable the wireless connection to the AP or the STA being affected and alert administrator. Furthermore, use the monitor system to locate the device from where it can be physically removed.

5.3 A Monitor Defences System (MDS)

As discussed above, a wireless monitor system made up with active response capabilities may increase security and in terms of protecting the wireless high assurance network. Still the system is complex and the idea must be composed and compiled for testing scenarios. In addition, as shown in the previous section, the MDS must interconnect with the corporate WLAN network to operate effectively and to be able to accurately separate legitimate and none-legitimate devices. Irrespective, a monitor defence system is a very good starting point for facing availability aspects concerning IEEE 802.11 environments. The monitor defence system architectural issues are shows in figure 45. The monitor system has been extended with active devices operating as "Fake AP's" connected to a wireless honeypot solution. The active response system must interact with the RADIUS access control server to be able to automatically respond to devices which fail to authenticate. A location server has been inserted to provide location services. The location server receives location data from the passive devices as well as the active devices to determine legitimate and none-legitimate STA and AP positions.

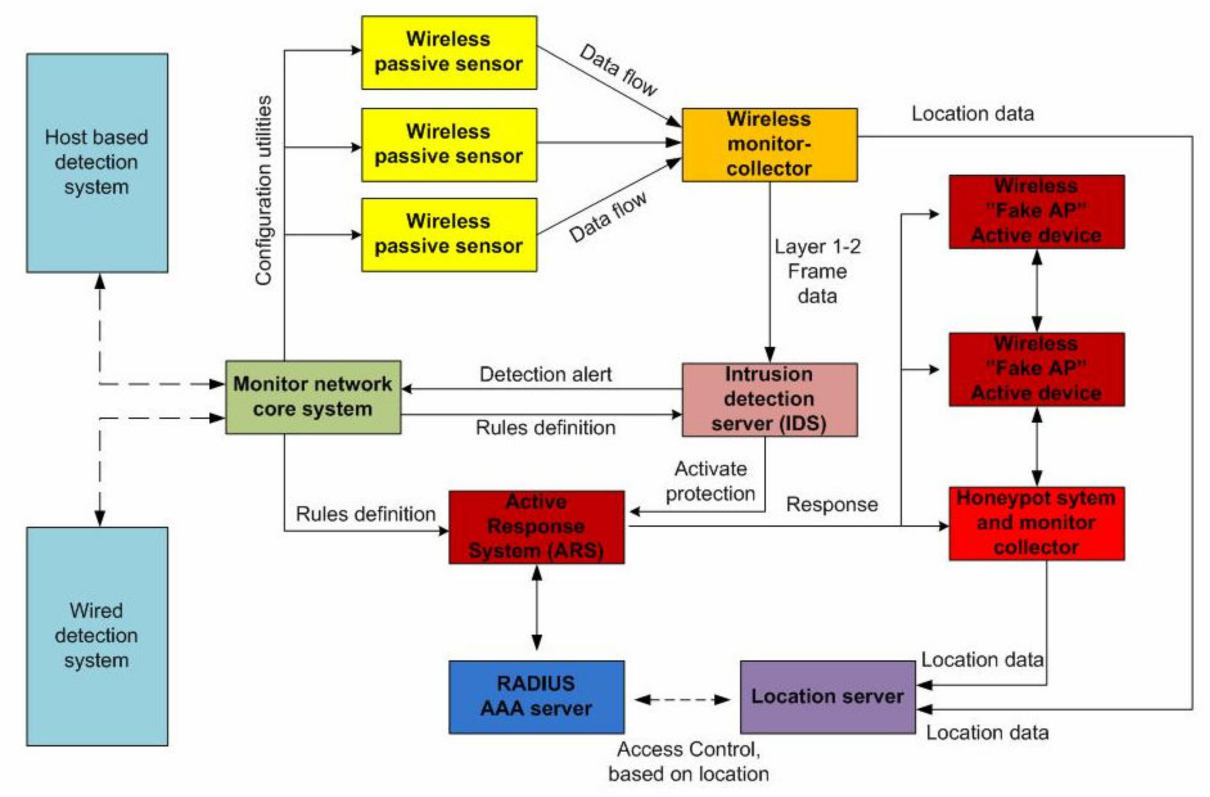


Figure 45: Monitor Defence System as a principal design

The monitor defence system can be connected to a host based detection system and wired LAN based detection system. These systems are shown in figure 45 as potential expansion to interconnect with the monitor core system. In addition, the Monitor Defence System must have a collaborative design, merging with the corporate WLAN solution. The monitor defence system interacting with the corporate WLAN network is shown in figure 46.

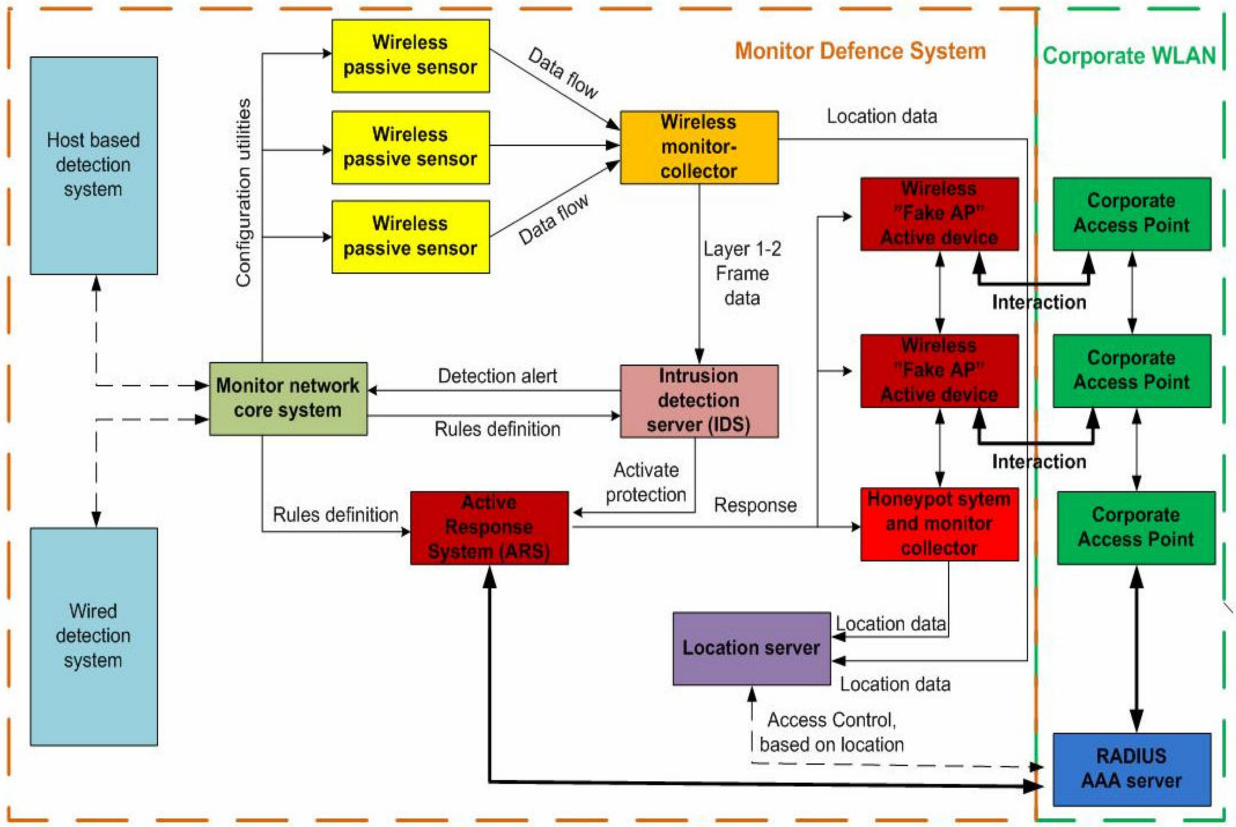


Figure 46: A Monitor Defence System interconnecting with the corporate WLAN network

5.4 *Monitor systems used by attackers*

It is important to realize and confirm that wireless monitor systems can also be used by attackers to observe and obtain wireless network information. Achievable information aspects are identical to what traffic the wireless monitor sensor devices may capture. The advantage of a monitor defence system (MDF) is that interconnecting it with the corporate high assurance WLAN system, such as the RADIUS server, the location server and the corporate access points, adds benefits related verify information aspects connected to authenticity, confidentiality, integrity etc. An attacker monitor system (eavesdropper) does not know anything about keys or secrets and therefore lacks the ability to look into WLAN interoperability aspects. In addition if an attacker monitor system uses active devices, this will be quickly revealed by the monitor defence system. On the other side, attacker's active devices can be used to probe types of response mechanisms which the monitor system has implemented. For example the attacker can find out if the wireless network has a honeypot solution. But, by requesting services from the high assurance wireless network, attackers can not avoid being detected. Regardless, the monitor defence system has potential advantages beyond attackers which make it more difficult for attackers to infiltrate the high assurance network without being detected.

5.5 Wireless monitor system conclusion

We can conclude that monitoring systems based on wireless IEEE 802.11 sensors devices are fundamental and crucial tools to build secure wireless communication services. Wireless availability aspects demand the ability to control operations, supervise the wireless environment and protect wireless components. A system that analyses the physical layer, the link-layer frames and also network layer packets has the ability to meet a wide range of threats concerning wireless LAN environments. The capability to handle intrusion and attacks depends on the ability to observer and detect abnormal behaviour and unwanted traffic. To respond the wireless threats, active components are required to correspond with potential intruders and to avoid prospective occurrence. Potential intruders and unauthorized devices which actively attempt to access the corporate WLAN can be automatically transferred to a honeypot AP system, which furthermore potentially could warn the intruder and prevent the devices from affecting the high assurance corporate WLAN. A wireless honeypot solution implemented for protection objectives in high assurance network, is preliminary theoretically approaches to how active response mechanisms could be implemented in a wireless context. Many challenges still remain according to interconnect and link up such solutions as a part of the corporate wireless network. It is way too early to recommend active protection mechanisms for implementation in high assurance wireless network, but the fundamental idea is promising and could potentially meet availability aspects and increase prevention for high assurance wireless networks.

6 WiFi security scenarios

6.1 Case 1: Wireless links in public environments, using IEEE 802.11 technology providing access to classified information networks.

6.1.1 Problem description

This first problem scenario is related to wireless IEEE 802.11 access points used as link-layer forwarders providing mobile radio access to communicate with a home environment. FLO/IKT offers wireless communication based on IEEE 802.11 technology in areas where mobile units drop in, for example military boats/ships ashore. Instead of using satellite communication services or cables, wireless networks can be used to provide flexible communication services using IEEE 802.11 technology. When a mobile unit comes within the range of a military WLAN transceiver, the mobile unit automatically interconnects with the wireless access point (AP), as shown in figure 47.

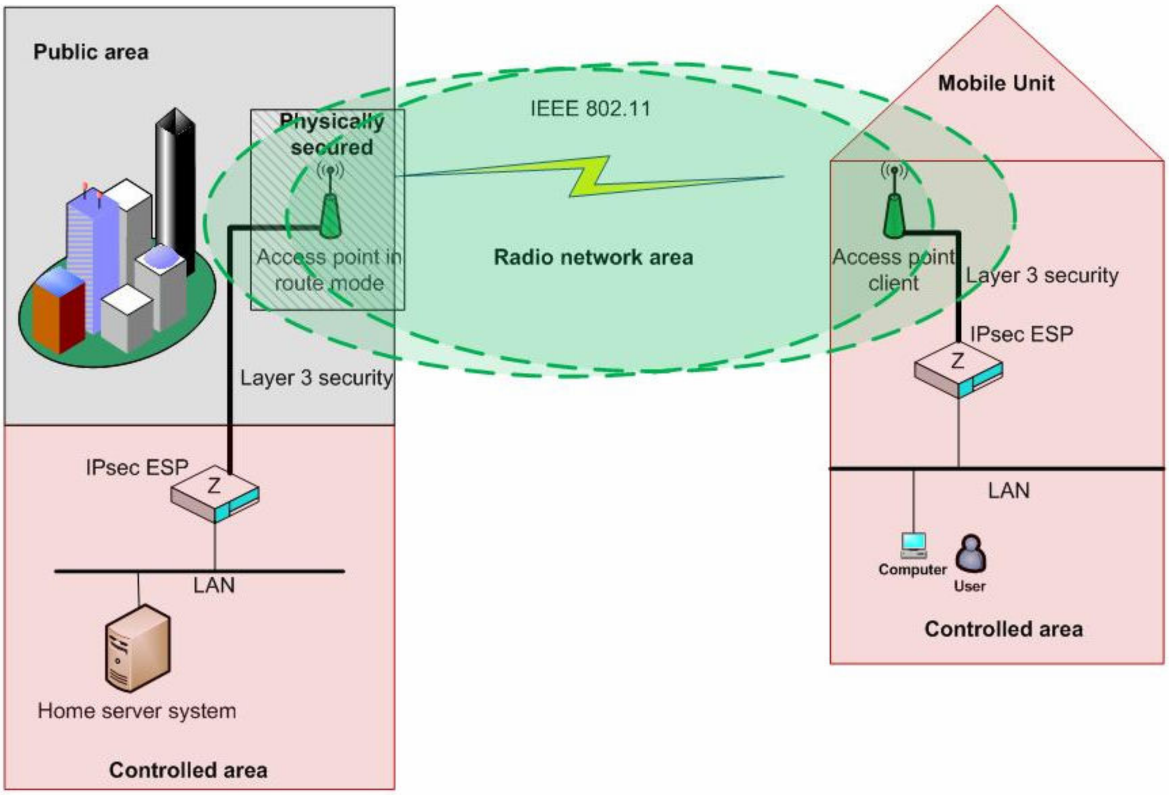


Figure 47: Case 1

Security is ensured using an IPsec ESP solution to provide data confidentiality and integrity to the network layer (OSI-layer 3) and protect higher OSI-layers. The scenario considers a one-to-one communication prospective. The problem with employing WLAN technology is security aspects concerning the wireless radio transmission availability and access control. Wireless access points (AP's), which are physically secured and placed in public areas, are still available for anyone with equipment adapted for the IEEE 802.11 technology. To protect AP's and the radio signal availability, mechanisms and security functionality must be implemented. Based on chapter 2, 3 4 and 5, this chapter will suggest ways to improve security related to the case 1 scenario, by proposing requirements and mechanisms to be implemented in order to ensure control access, supervise the environment and protect the wireless network.

6.1.2 Threats

Confidentiality and integrity are ensured using IPsec/ESP as an end-to-end IP security solution. Threats and vulnerabilities are concerned with access control and wireless availability aspects using the IEEE 802.11 technology. This scenario is shown in figure 48. The radio network requires OSI-layer 2 security and control mechanisms to secure to the wireless link between the access points (AP client and AP in route mode).

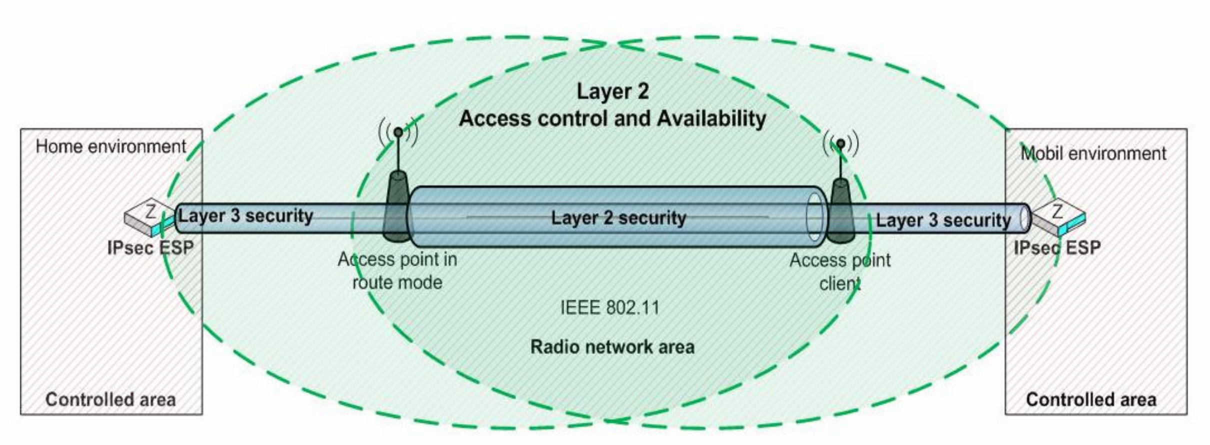


Figure 48: Case 1 security aspects and threats concerning physical-layer and link-layer

6.1.3 Solution requirements

Based on the discussion from chapter 2, 3, 4 and 5 the following requirements should be established to provide high assurance wireless interconnections:

- Hardware security modules (HSM)
- Public Key Infrastructure (PKI) and digital certificates
- Centralized RADIUS server for access control and certificate verification
- Three factor based authentication mechanisms (HSM, PKI-certificate, ID-password)
- IEEE 802.1X mutual authentication using EAP-TLS
- IEEE 802.11i RSN layer 2 confidentiality/integrity mechanisms, including AES-CCMP and the 4-way handshake protocol
- VPN architecture providing IPsec ESP connections for network layer (OSI-layer 3) security
- Wireless monitor systems for supervision, detection and prevention
- Wired based intrusion detection system (IDS)
- Detection and respond policy enabled

Security mechanisms used in high assurance wireless network should be based on requirements well founded in security methodology. Mechanisms and principles should be a composition of methods which in combination provides the ability to meet the threats and the surrounded vulnerabilities. The access control solutions should be based on “something you know” and “something you have” at minimum, which signifies that the implementation should have a logical separated software/hardware security solution in combination with numbers of secrets. For example, a physical devices such as a hardware security module (HSM), makes it possible to add security features as a separated concept, flexible and independent from various types of wireless network components. A hardware security module (HSM) in combination with PKI digital certificates provides a flexible and strong basis for authentication and validation. Implementing a centralized RADIUS server solution in combination with EAP-TLS, access control prospectives should be well assured and well protected. Due to wireless availability aspects, it is recommended to use AES-CCMP (OSI layer 2 encryption) to protect network layer (layer 3) information. A wireless monitor system is required to supervise and control the wireless environment. The monitor system can be used to detect security breaches and threats, and report the security condition. Based on this a respond policy should be established to protect the network if a threat or an attack is detected. A wired intrusion detection system is capable to analyze data which the wireless monitor system can not validate. The overall architecture is shown in the next section.

6.1.4 Architectural discussion

The security architecture is based on using a public key infrastructure to implement high assurance access control, adapted with Robust Security Network configuration (RSN) based on IEEE 802.11i and IEEE 802.11X principals. To separate security, a Hardware Security Module (HSM) has been integrated to handle security processing, key handling and storage. The architectural scenario is shown in figure 49.

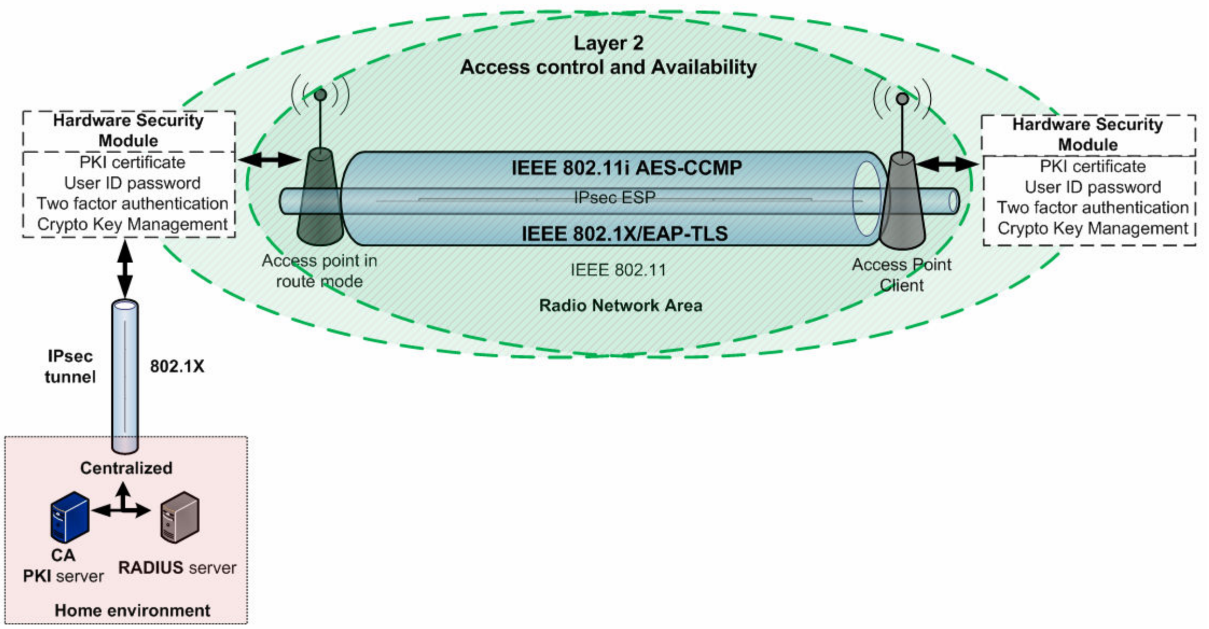


Figure 49: A PKI based HMS architecture using IEEE 802.1X and IEEE 802.11i

As discussed in chapter 3, implementing PKI with 802.1X leads to that EAP-TLS is the best choice as a well adapted protocol for PKI services, and well supported for handling secure transmission of authentication credentials and key establishment data. The HSM device with a valid PKI certificate, plus a user identification password is required to authenticate with RADIUS server and to establish a wireless connection. This signifies that three-factor based authentication is recommended for accessing the wireless network. Since the number of wireless links towards the route-mode access-point is considered to be few, a centralized RADIUS server solution would be a flexible and scalable solution, but as discussed in chapter 3 and 4, the AP should be able to verify signed EAPOL request, to effectively refuse clients which do not have a valid PKI certificate. Private keys can be used to sign layer two messages to ensure authenticity. For example unauthenticated association requests could be effectively refused by the access points. As shown in figure 50, this requires that both access points and the RADIUS server possess PKI certificates. This will prevent unauthorized device from experimenting with the RADIUS server and thereby decrease the flow of unauthorized RADIUS authentication messages on the LAN side. Due to eavesdropping and passive monitoring, layer 2 encryption using AES-CCMP limits the availability and protects network layer information aspects. To transmit data between the access point and the home environment, VPN IPsec tunnels are used to protect the communication. The scenario is shown in figure 50.

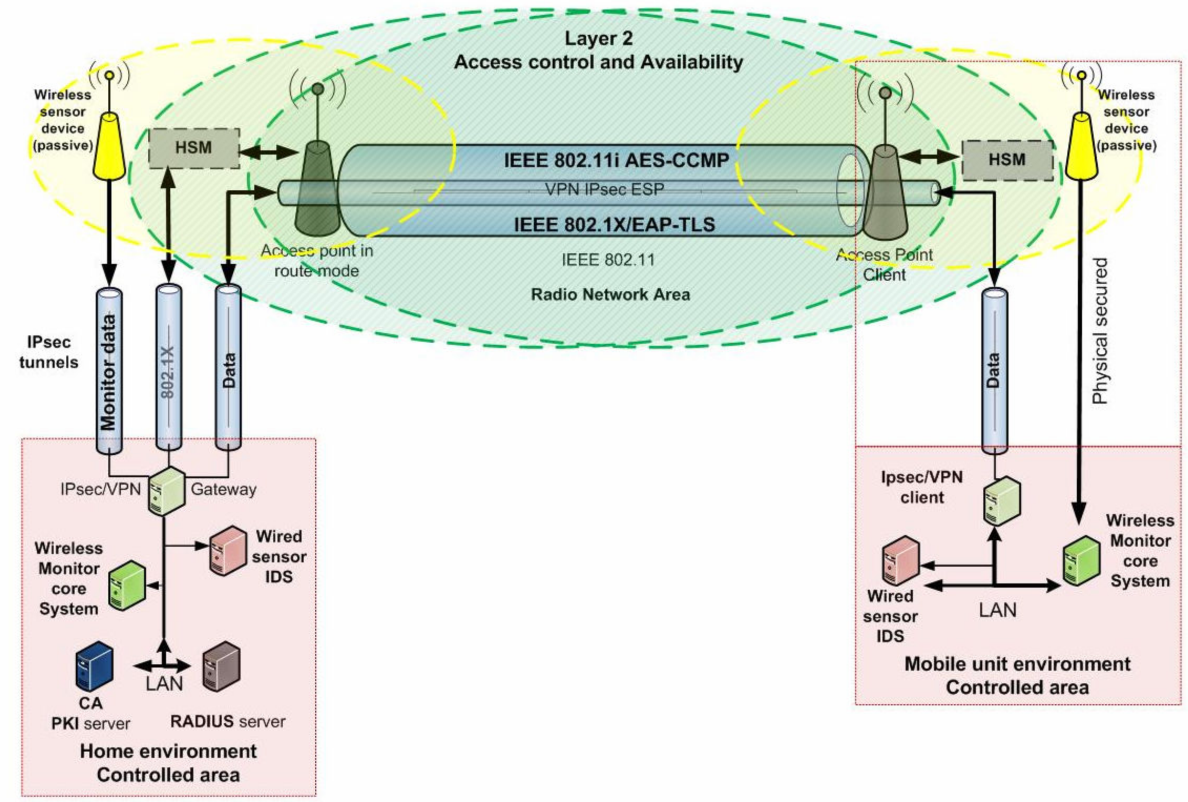


Figure 50: Best practice security architecture

IPsec tunnels are used to protect authentication and key distribution traffic transmitted between the HSM and the RADIUS server on the wired network. The same security solution is used to transmit monitor data between the wireless sensor and the monitor core system. The monitor system is responsible for AP perimeter control which involves supervising the wireless channels surrounded with the corporate access point (AP). A response policy should be established if threats or intrusions are detected. A typical policy can be to terminate the wireless AP connection and use satellite transmission if severe event or attacks threatening the wireless network. An alternative solution is to implement an active response system and honeypot network as discussed in chapter 5, but such solution will increase the overall complexity considerably. Because the AP operates in public environments, the monitor system will become an essential tool for wireless prevention. In addition a wired LAN sensor IDS system should be implemented to analyse plaint text data and to handle frames which the monitor system can not validate. A shown in figure 50 the IDS systems must be implemented at the mobile unit and within the home environment.

Advantages:

- Strong security requirements enabled
- Hardware security module provides an external security element which result in high flexibility and AP independency
- Dual encryption (VPN Psec/ESP and CCMP)
- Scalability due to a centralized PKI deployment for secure authentication and key establishment
- PKI can be used to sign frames floating between STA and AP, which would increases security when it comes to message authenticity, secure access control and prevent particular DOS and flooding attacks.
- A monitor systems could be used to control and supervise access point availability by scanning Wi-Fi channels and report this information to a detection server

Potential improvements and disadvantages:

- Data throughput and performance
- High complexity
- Wireless monitor core system interaction must be closer evolved
- HSM support in AP’s
- Authenticity to management frames and control frames (802.11w)
- Using PKI to sign OSI-layer 2 messages requires solution development

6.2 Case 2: Establishing wireless environments based on IEEE 802.11 technology providing accesses to classified information networks.

6.2.1 Problem description

This problem scenario is related to establishing deployable military wireless environments based on IEEE 802.11 networks, providing access to classified information systems. The wireless operation concept is considered as a one-to-many relation. The scenario differs from the previous case because confidentiality, authenticity and integrity must be added on to the wireless clients. Each STA device that operates within the wireless network must be authorized to be able to establish connection with the AP. The case concept requires access control, confidentiality, authenticity and integrity mechanisms as well as availability protection. In this section design issues and requirements related to architectural security solutions will be presented. The architecture is based on discussions and conclusions from chapter 2, 3, 4 and 5, and the thesis proposes a basis fundament for implementing high assurance WLAN networks. Figure 51 shows WLAN prospectives related to the case two scenario.

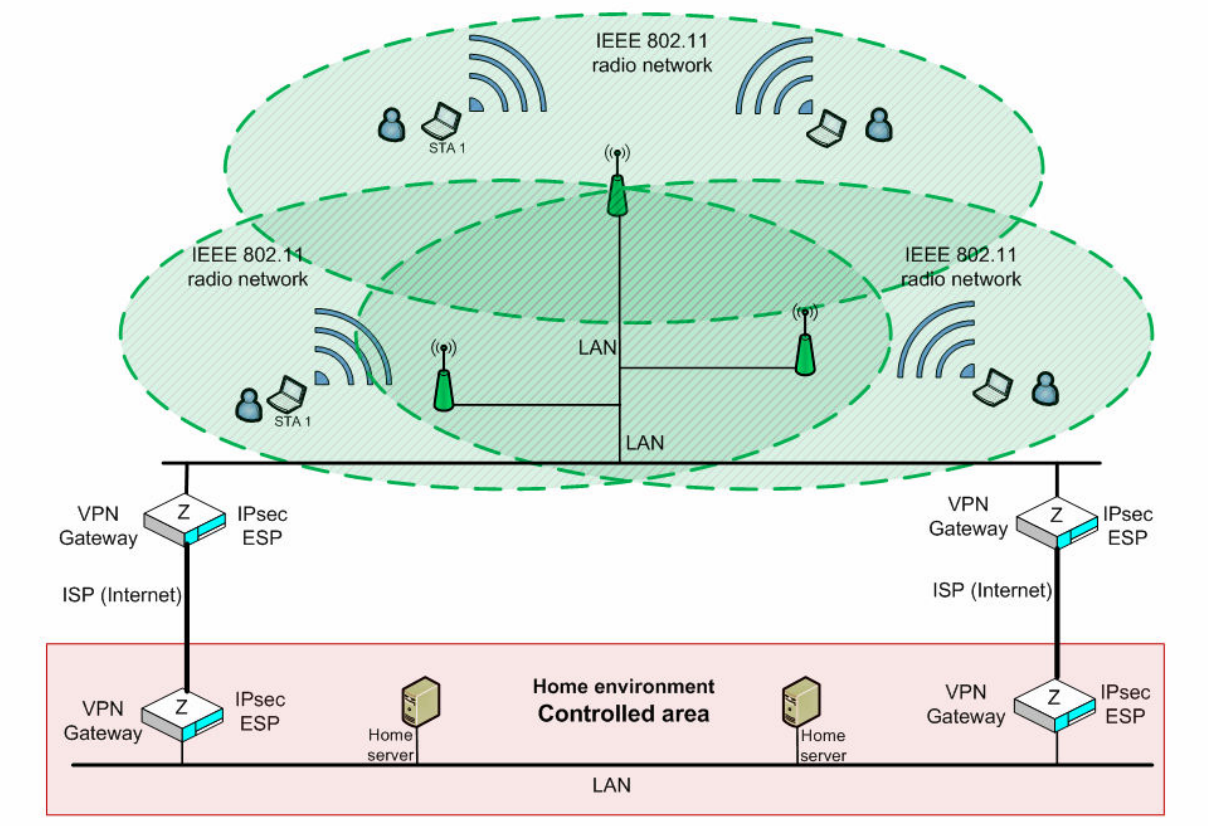


Figure 51: Case 2

6.2.2 Threats

Case two threat aspects are concerning access control, confidentiality and availability, which means that approved security functionality must be added to the wireless clients (STA's). Threats are surrounded with the 802.11 protocol establishing secure connections to a distribution system with access to classified information. The scenario is shown in figure 52.

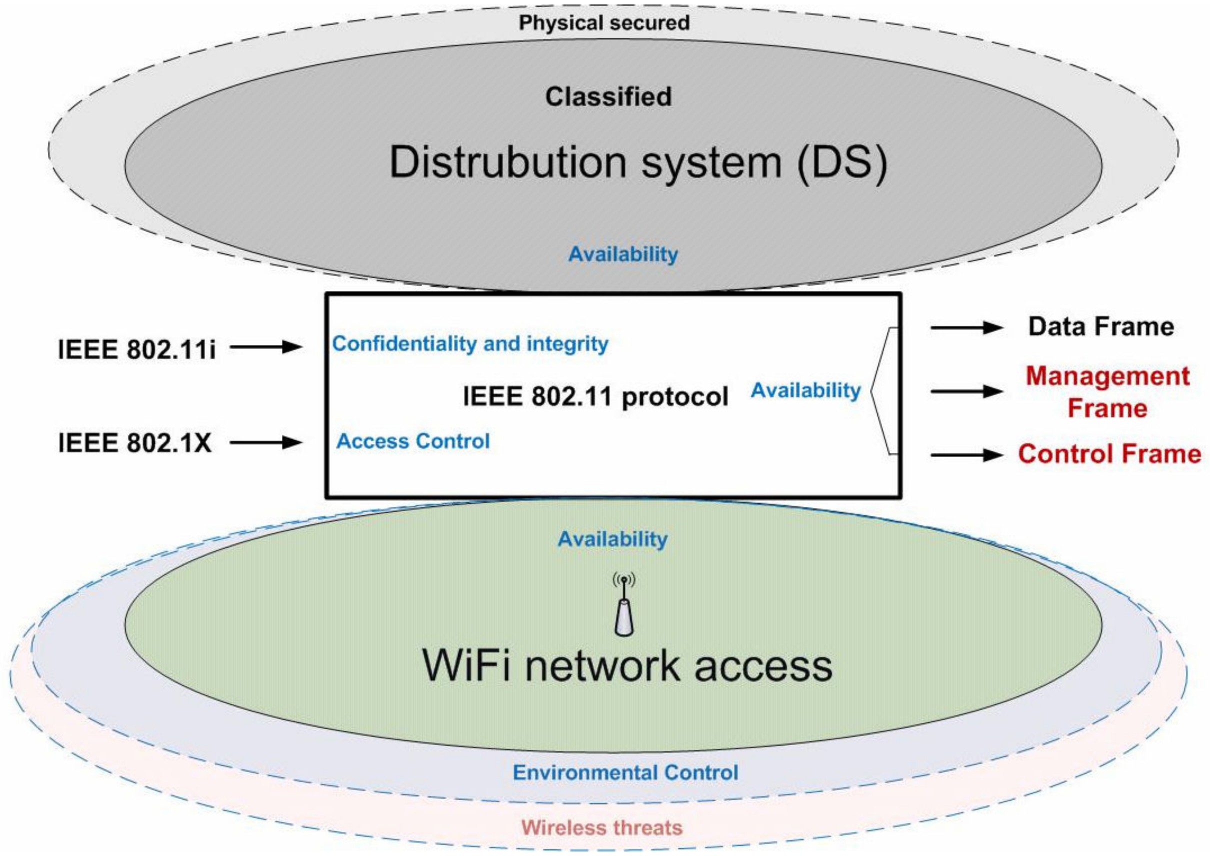


Figure 52: Threats concerning high assurance WLAN environments to access classified DS

6.2.3 Solutions requirements

Based on the discussion from chapter 2, 3, 4 and 5 the following requirements should be established to provide high assurance wireless interconnections:

- Hardware security module (HSM)
- Public Key Infrastructure (PKI) and digital certificates
- RADIUS server for access control
- Three-factor based authentication mechanisms (HSM, PKI-certificate, id-password)
- IEEE 802.1X mutual authentication using EAP TLS
- IEEE 802.11i RSN layer 2 confidentiality/integrity mechanisms, including AES-

CCMP and the 4-way handshake protocol

- VPN architecture providing IPsec ESP end-to-end connections for network layer (OSI-layer 3) security
- Location system for access control, wireless mapping and location overview
- Monitor sensor system for perimeter control and supervision
- Wired LAN based intrusion detection system (IDS)
- Protection and wireless honeypot system for automatic responses and prevention.
- Detection and respond policy enabled.

6.2.4 Architectural discussion

The security architecture showed in figure 53 describes the authentication process from AP discovery to an AES-CCMP encrypted link (OSI-layer-2) is up and running. The architecture consists of digital certificates (PKI) implemented into STA's, Access Points (AP's) and the RADIUS server, whereas IEEE 802.1X combined with mutual EAP-TLS mechanisms is used to establish secure and encrypted wireless link-layer (OSI-layer-2) connections. The frame work is basically similar to the access control approach discuss end described from chapter 3 and 4.

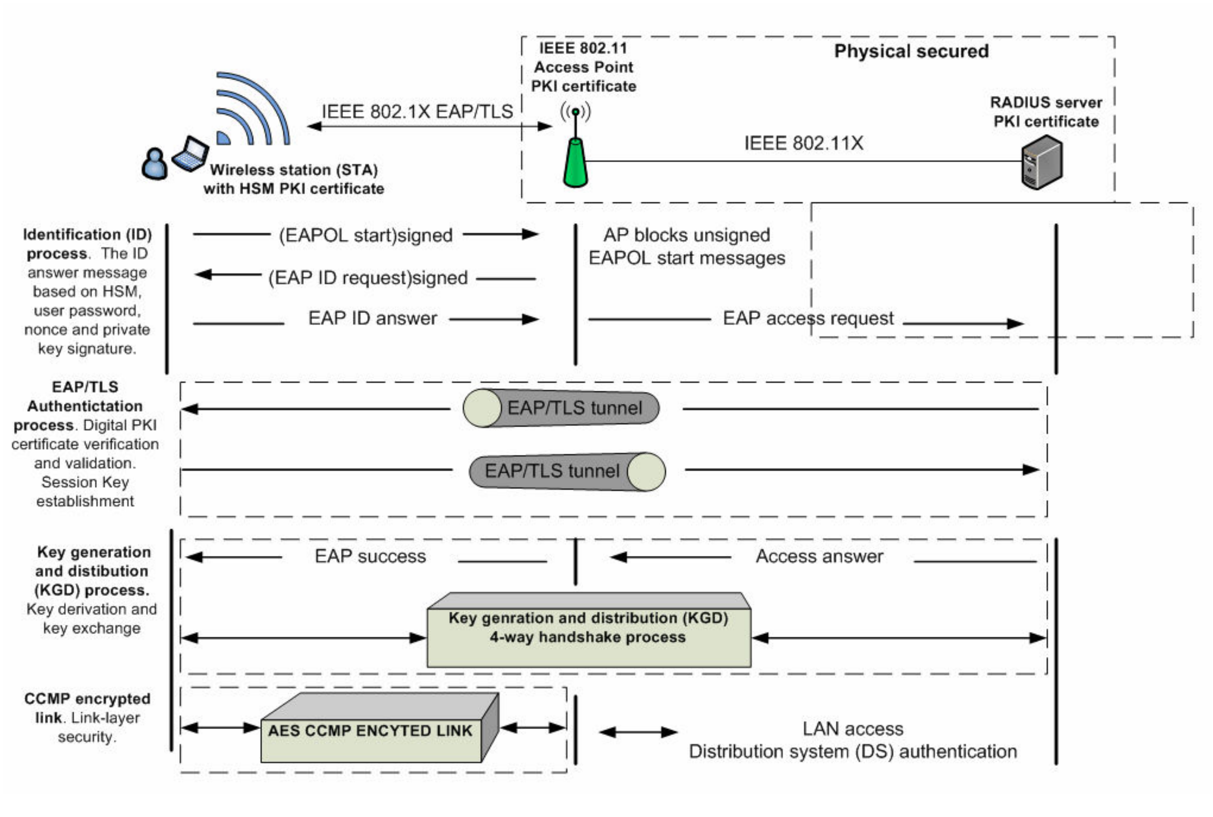

IEEE 802.11
Access Point
PKI certificate
Physical secured
RADIUS server
PKI certificate
IEEE 802.1X EAP/TLS
IEEE 802.11X
Wireless station (STA)
with HSM PKI certificate
Identification (ID) process. The ID answer message based on HSM, user password, nonce and private key signature.
(EAPOL start)signed
(EAP ID request)signed
EAP ID answer
AP blocks unsigned
EAPOL start messages
EAP access request
EAP/TLS Authentictation process. Digital PKI certificate verification and validation. Session Key establishment
EAP/TLS tunnel
EAP/TLS tunnel
Key generation and distibution (KGD) process. Key derivation and key exchange
EAP success
Access answer
Key genration and distribution (KGD)
4-way handshake process
CCMP encrypted link. Link-layer security.
AES CCMP ENCYTED LINK
LAN access
Distribution system (DS) authentication

Figure 53: IEEE 802.1X EAP/TLS combined with PKI certificates

Since the architecture implements PKI, private keys can be use sign messages. Ideally, every frame transported between the STA and AP should include signatures to ensure authenticity, but that would potentially degrade network performance. As long as the AES-CCMP encrypted link is up and running, authenticity to data frames are ensured by the IEEE 802.11i settlement. To improve authenticity, the thesis suggests adding signatures to the first two EAP messages shown in figure 53; EAPOL-start and EAP-ID request. This can be done by using implemented PKI features to sign these messages using the private key. Such solution will efficiently prevent STA's from connecting a rogue access point as well as the corporate AP to block falsified STA certificates. Additionally, this will prevent the AP from EAPOL flooding attacks, and it makes it possible for the AP to automatically block STA's which do not have a valid signature. As shown in figure 53 this requires the AP to known the public keys. Another problem issue is management frames and control frames which is not covered by the RSN 802.11i settlement. It is not necessary to encrypt these frames but it is important for the AP and STA can verify the transmitter. One approach is to use PKI features to add authenticity to management frames and control frames. This would potentially prevent flooding and DOS attacks against management and control frames, but it would probably slow down network performance. Such a scenario must be tested and confirmed for it can be recommended. As discussed in chapter 5, the monitor defence system can monitor EAPOL messages and interconnect with RADIUS server in order determined if a device should connect to the wireless honeypot network or to the corporate wireless network. Such solution requires the monitor system to know the public keys. Figure 54 shows a recommended wireless IEEE 802.11 architecture, which enables and implements OSI-layer 2 access control, location control, wireless detection, and protection functionality. As discussed in chapter 5, the solution is based on implementing a wireless monitor defence system (MDS) which consists of passive and active sensor devices. As concluded in chapter 5 the monitor defence system is only a theoretically approach, and a market research study is required to find status on available monitor defence systems capabilities.

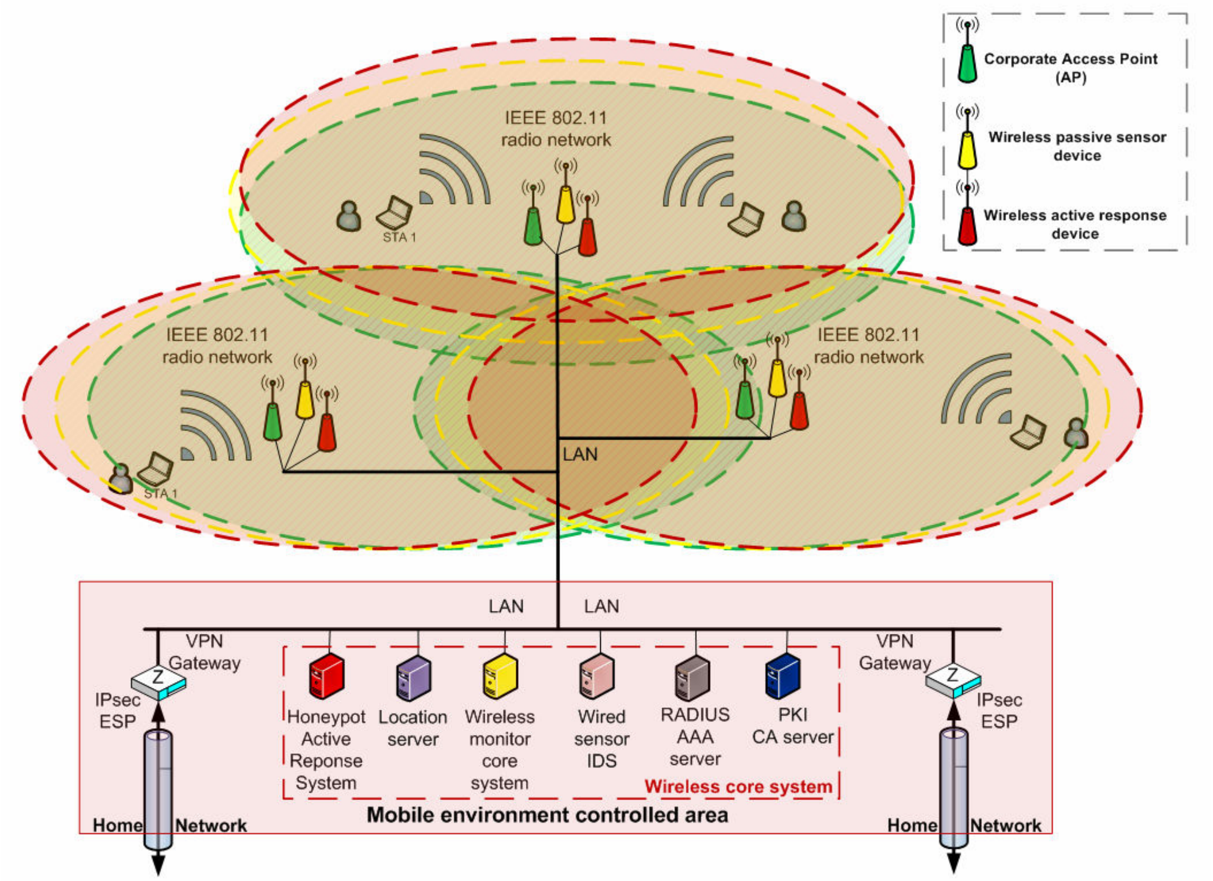

Corporate Access Point (AP)
Wireless passive sensor device
Wireless active response device
IEEE 802.11 radio network
IEEE 802.11 radio network
IEEE 802.11 radio network
STA 1
STA 1
LAN
LAN
LAN
VPN Gateway
VPN Gateway
IPsec ESP
IPsec ESP
Honeypot Active Reponse System
Location server
Wireless monitor core system
Wired sensor IDS
RADIUS AAA server
PKI CA server
Wireless core system
Mobile environment controlled area
Home Network
Home Network

Figure 54: Wireless IEEE 802.11 environment with a monitor defence architecture

Case two considers the number of wireless links towards the access-point to be many, which means that the wireless core system, compared to case one, has been extended as shown in figure 54. A passive wireless monitor system is still represented, but in addition, an active response system and a honeypot solution have been added. As discussed in chapter 5, an active response system is required to automatically respond to threats. The location server is recommended to be used for access control and for the monitor system to locate devices. This will make it possible to control the wireless access range. The passive devices and the monitor system task accomplish parameter control and wireless network supervision. In addition the monitor core system uses the active response devices to protect and prevent the wireless environment from threats, as described in section 5.2.

To establish a secure wireless interconnection with the controlled area, link-layer security can not provide end-to-end security. VPN technology in terms of a VPN concentrator (gateway) can be sued to establish secure network layer (OSI-layer-3) connection from STA’s and in to the controlled network area. This scenario is shown in figure 55.

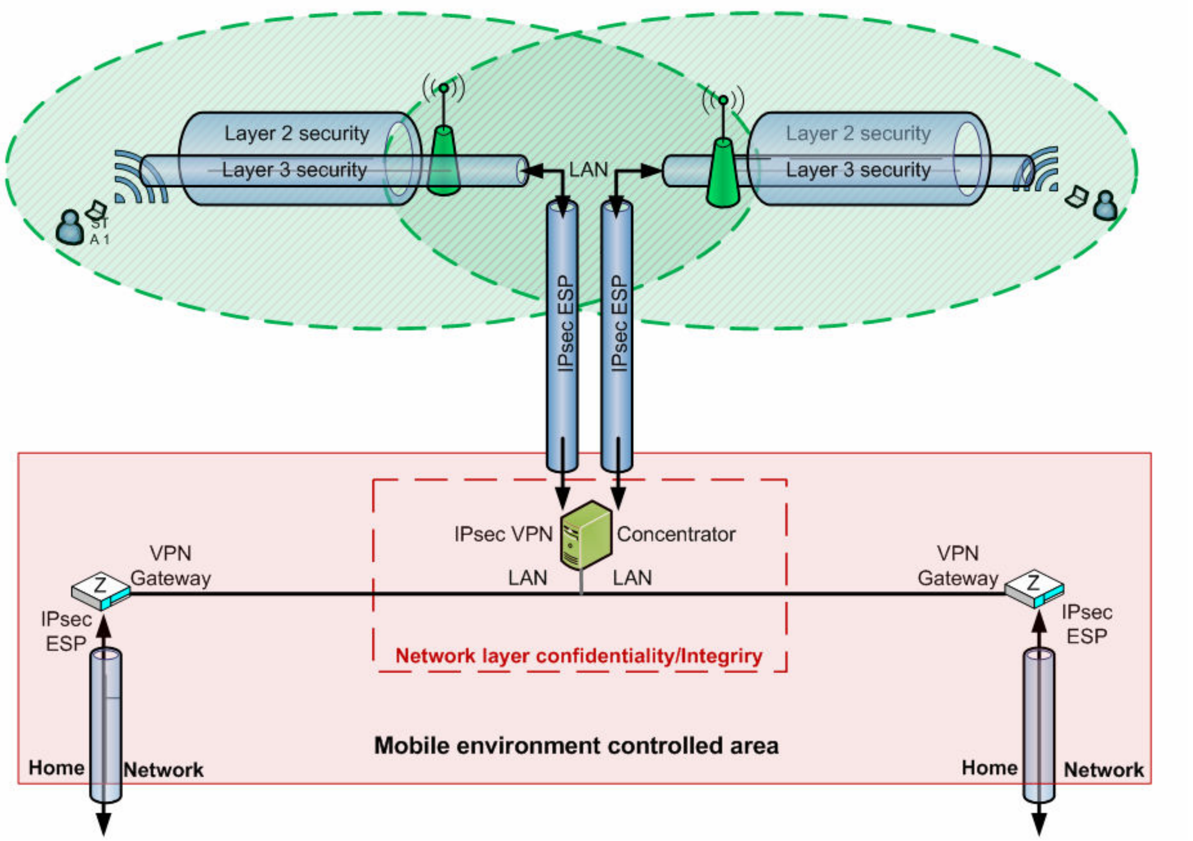


Figure 55: Network layer security with VPN concentrator placed within the mobile environment

The network layer, as described in section 2.6 provides the ability to secure data transmission transparently, and ensure security for end-to-end prospectives and requirements. The solution in figure 55 is based on IPsec ESP tunnels directed from the STA and in to the mobile environment controlled area. A secondary IPSec ESP solution must be established to transmit data from the mobile environment to the home environment distribution system. It is important to confirm that network-layer security such as VPN IPSec technology only provides extended security features to data being transmitted between the STA and the distribution system (DS). VPN IPsec is transparent to wireless network security technology and does not increase wireless security aspects.

One alternative solution to figure 55, is to let the STA establish an IPsec ESP connection directly from the client (STA) to the home network controlled area (distribution system). This scenario is shown in figure 56.

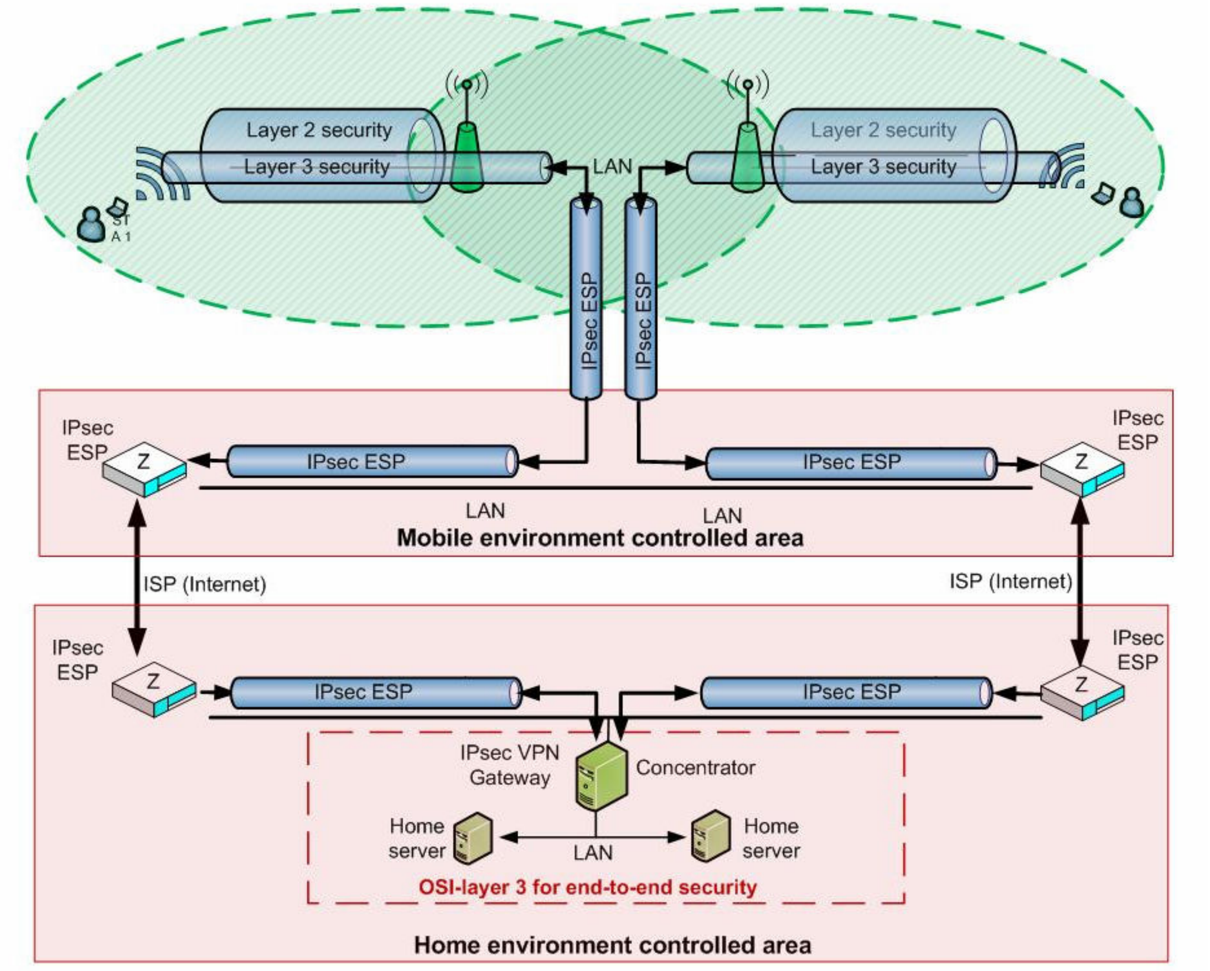


Figure 56: Network layer and end-to-end security between STA and home environment VPN concentrator

As shown in figure 56, IPSec ESP security is tunneled from the STA and let the STA establish secure network layer connection from its device into the home environment VPN gateway (VPN concentrator). This solution represents high level of transparency as well as a high level of security. The problem is that the mobile environment system does not have the possibility to examine and verify data before it is transmitted to the home network area. Basically this signifies that the wired sensor IDS system, shown in figure 54, must be implemented at the home environment.

Advantages:

- Strong security requirements enabled
- Hardware security module provides an external security element which result in high flexibility and STA/AP independency
- Dual encryption (VPN IPsec/ESP and CCMP)
- PKI and digital certificates for secure access control including authentication and key establishment.
- PKI can be used to sign frames transmitted between STA and AP, which would increases security related to authenticity and message origin (transmitter verification)
- PKI signature could prevent several threats related to DOS, flooding attacks and particular rogue access points
- A wireless monitor system which implements passive devices is used to control and supervise availability by scanning Wi-Fi channels and report channel data to a intrusion detection system
- Location services which makes it possible to physically map and position wireless devices within the wireless network area
- Location based access control would prevent devices to operate to far away from the corporate wireless network area.
- Wirelesses monitor system which implements active devices to protect the wireless network environment.
- Monitor defence system which inserts protection functionality by implementing a wireless honeypot network to trap attackers.
- VPN IPsec technology to provide end-to-end security control

Potential improvements:

- STA firewalls and IDS systems have not been discussed in this thesis but is an important part of STA security aspects, especially for protection of higher OSI-model layers.
- AP and STA configuration aspects have not been discussed widely but referred to the thesis appendix, some important wireless configuration utilities are considered.
- Combining IPSec ESP and AES-CCMP will potentially degrade network performance and data throughput. The scenario should be tested and verified as composite solution.
- The IEEE 802.11w standard introduces improved security aspects related to safeguard management and control frames. An approved version of 802.11w is extended to be announced in 2008. The thesis appendix introduced the 802.11w security improvements.

7 Conclusion

7.1 Access control and availability aspects

This thesis has discussed access control and availability aspects concerning wireless technology based on the IEEE 802.11 protocol. Based on this, the thesis has presented and proposed important requirements and claims which compose architectural ways to achieve high-end security in wireless networks. By employing principles based on Robust Security Network (RSN) using IEEE 802.1X for access control and IEEE 802.11i for confidentiality, integrity and authenticity, wireless communication aspects are fairly secured. Due to the lack of authenticity, especially for handling management frames and EAP start messages, wireless networks are still vulnerable to various attacks. To meet such vulnerabilities, authenticity should be implemented into every frame transmitted between the wireless station (STA) and the access point (AP). Implementing WLAN solution based on public key infrastructures (PKI) would straighten these problems because PKI features can be used to sign link-layer messages and verify transmitters (message origin).

7.1.1 Access control requirements

The thesis has focused on important access control requirements which a high assurance wireless network should be founded on. The most important issue is connected to implementing a hardware security module (HSM) combined with digital PKI certificates to provide three-factor authentication. Access control is ensured using IEEE 802.1X with EAP-TLS and IEEE 802.11i to provide robust security networks associations (RSNA's) including mutual authentications, key establishment through the 4-way handshake procedure and establishment of an AES-CCMP link-layer encrypted data-channel providing confidentiality, integrity and authenticity.

7.1.2 Network layer advantages and requirements

Network layer security introduces additional security features in terms of end-to-end security control in wireless networks. The thesis recommends VPN and IPSec ESP tunnelling techniques to be used to securely transmit data between wireless end-devices and the controlled area.

7.1.3 Control, detection and protection requirements

In chapter 5 the thesis has introduced wireless monitor systems which are responsible for perimeter control and capable to detect abnormalities and handle threats from intruder devices in order to protect and supervise the wireless network environment. A monitor defence system (MDS) introduces complex architectures and subsequent high costs, but may potentially control availability and overcome a wide range of threats concerning IEEE 802.11 networks. An optimized monitor defence system must interconnect with the corporate AP network to be able to verify security conditions and effectively detect security breaches. The monitor system introduces passive and active devices to be able protect the wireless network. The passive devices act as sensors to monitor wireless channels and frames, whereas the active devices introduce decoys to lure potential attackers by implementing wireless honeypot networks. In addition wireless location control has been recommended as important security features to map and position wireless devices. The wireless monitor defence system is only a theoretically approach on how to insert security mechanisms for active protection functionality and requires further investment in terms of prototyping and development for testing scenarios. Passive and active monitoring systems may also be used by attackers (eavesdroppers) to obtain wireless network information. Attackers and intruders can use passive monitor systems to obtain physical-layer and link-layer header information aspects. Passive monitoring is difficult to handle and requires the wireless high assurance system to trust implemented confidentiality mechanisms. By implementing a monitor defence system, the corporate high assurance WLAN environment implements facilities to detect active devices within the wireless network area, and thereby the ability to control the wireless network environment.

7.1.4 Security scenarios requirements

Based on a study focussing on access control and availability aspects, the thesis has discussed and recommended security architectures for two WLAN problem scenarios. The proposed solution includes several important security features which a high assurance wireless network should be founded on. It can be concluded that security mechanisms must be implemented through adjustments of the two available security protocols IEEE 802.1X and IEEE 802.11i, in combination with wireless monitor systems adding control, detection and protection facilities. As described and shown in chapter 6, security mechanisms implemented for high assurance wireless networks signifies heavy implementations, high complexity and subsequent high costs. Further investment and research would potentially develop more integrated high assurance functionality to simplify circumstances and the environmental complexity.

7.2 *Further work*

This thesis work has been based on descriptive and explanatory research and is founded on a theoretically approach to an implementation of a high assurance wireless solution focusing on access control and availability aspects. Work still remains, and the following is recommended for further studies:

- CCMP combined with IPsec – compatibility and efficiency
- WLAN security performance and scalability aspects
- Market research for monitor systems and implementation capabilities
- RSN high assurance WLAN prototype system built as a laboratory environment
- Implementation of STA firewalls and intrusion detection system (IDS)
- Appropriate HSM solution for high assurance WLAN environments
- Implementation issues considering WLAN honeypot’s and fake access points.
- Communication and cooperation aspects considering interconnected high assurance WLAN networks and wireless defence systems
- Wireless defence system prototyping

8 References

1. Airdefense, “Anywhere, Anytime Wireless Protection”. Discussion wireless protection systems and papers concerning WLAN security issues”.
   Available at: http://www.airdefense.net

2. Jessie Walker, Chair: “Status of the project IEEE 802.11 Task Group”. Enhancement to the IEEE 802.11 medium access control layer, available at:
   http://grouper.ieee.org/groups/802/11/Reports/tgw_update.htm

3. IETF, “Internet security glossary”, May 2000.
   Available at: http://www.ietf.org/rfc/rfc2828.txt

4. Steven K. Brawn, “802.1x secure wireless computer connectivity”. October 2004 Available at: http://delivery.acm.org/

5. Benny Bing, “Wireless local Area Networks”. 2002, ISBN 0-471-22474-X

6. Cisco Systems white paper. “Extensible Authentication Protocol Transport Layer Security Deployment Guide for Wireless LAN networks” From 2002.

7. Auscert, “Australian computer Emergency response team”, “Denial of service vulnerabilities for wireless devices, 2004.
   http://www.auscert.org.au/render.html?it=4091

8 ANSI/IEEE Std. 802.11, 1999 Edition (R2003), Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Computer Society

9. National institute of Standards and technology, Sheila Frankel, Bernard Eydt Les Owens, Karen Kent, “Guide to IEEE 802.11i: Establishing robust security networks” June 2006.

10. Mark Stamp, “Information security: Principals and Practice”, 2006, ISBN-13 978-0-471-73848-0

11. Wikipedia, A free web based encyclopedia with written collaboratively by volunteers.
    Available at: http://www.wikipedia.org

12. Wikipedia, The Free Encyclopedia “MAC addresses” http://en.wikipedia.org/wiki/MAC_address

13. Wikipedia, The Free Encyclopedia “Confidentiality” http://en.wikipedia.org/wiki/Confidentiality

14. Wikipedia, The Free Encyclopedia “CRC check” http://en.wikipedia.org/wiki/Cyclic_redundancy_check

15. IEEE Approved draft by IEEE-SA, 18 March 1999, “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

16. Network Chemistry, Company providing technology industry standards for “securing the mobile enterprise”. Home site available at http://www.networkchemistry.com/

17. National institute for standard and technology (NIST), Advanced Network Technology Division; “Trustworthy Networking”, http://w3.antd.nist.gov/

18. George Ou, ”LAN Architect” ,Wireless LANs, Available at: http: //www.lanarchitect.net

19. Cisco Wireless LAN security solution, papers and guides, available at: http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/networking_solutions_package.html

20. Norwegian National Security Authority (NSM), “NSM cryptographic requirements”. Updated version: 12.01.2006. Available at: www.nsm.stat.no

21. Wi-Fi Alliance organization, Wi-Fi certified products. Home site: http://www.wi-fi.org

22. Federal Information Processing Standard Publication (FIPS), Secretary of commerce approved standards. Home site: http://www.itl.nist.gov/fipspubs/

23. IEEE 802.11i Approved by IEEE-SA, 18 March 1999, “Amendment 6: Medium access control MAC Security enhancements“ , 2004: IEEE computer

24 Wikipedia, The Free Encyclopedia. “The 4-way hand shake based on the IEEE

802.11i". Available at: http://en.wikipedia.org/wiki/802.11i

25. Wikipedia, The Free Encyclopedia. "Denial of service attacks". http://en.wikipedia.org/wiki/Denial_of_service on Cisco leap protocol

26. Eavesdropping, The Free Encyclopedia. "Eavesdropping". Available at: http://en.wikipedia.org/wiki/Eavesdropping

27. Airtight Networks, Company providing services to monitor and secure a wireless LAN environment. Article, "Best practice for securing your enterprise wireless network". 2005 Available at: www.AirTight.org

28. Joshua Write, "Detecting wireless LAN MAC address Spoofing", 2003 http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf

29. Jamil Farshchi, "Wireless Intrusion Detection Systems" 2003. http://www.securityfocus.com

30. Joshua Write, "Layer 2 Analysis of WLAN Discovery application for intrusion detection", 2002. Available at www.rootsecure.net

31. Frank, Bulk, Network Computing, security article. "Distributed security monitors", 23 June 2005. Available at: http://www.networkcomputing.com/

32. Cisco systems, "Integrated wireless IDS capabilities" Home site: http://newsroom.cisco.com/dlls/2004/prod_111004c.html

33. Airmagnet, company specialized in WiFi enterprise analyzer tools and equipment. Article: "Smart edge sensors" Home site available at : http://www.airmagnet.com/products/enterprise.htm

34. AirDefense, Company that develops wireless intrusion prevention systems that monitors the wireless enterprise network. Article: "Accurate Wireless Intrusion Detection & Monitoring"
Home site: http://www.airdefense.net/products/enterprise.php

35. Wikipedia, The Free Encyclopedia "Host based intrusion detection system". Available at: http://wikipedia.com

36. Wikipedia, The Free Encyclopedia “Intrusion detection system”
Available at: http://wikipedia.com

37. Wikipedia, The Free Encyclopedia “Anomali based intrusion detection system”, Available at: http://en.wikipedia.org/wiki/Anomaly-based_intrusion_detection_system

38. Norwegian National Security Authority (NSM), “Temahefte”, “Sårbarheter og trusseler mot informasjonsystemer” 2006.

39. Open interconnection basic reference model (OSI modell), from Wikipedia.
Available at: http://en.wikipedia.org/wiki/OSI_model

40. Cisco systems “Cisco SAFE wireless LAN security in Depth.” 2003.
Available at: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm

41. L. Blunk, J. Vollbrecht, Internet working group,RFC 2284, “PPP Extensible authentication protocol” , 1998, At: http://www.ietf.org/rfc/rfc2284.txt

42. B. Adoba, L. Blunk, J. Vollbrecht, Internet working group, RFC 3748, “ Extensible authentication protocol”, 2004. At: http://www.ietf.org/rfc/rfc3748.txt

43. Eduardo B.Fernandez, Imad Jawhar, M. Larrondo-Petrie and VanHilst, ”An overview of the security of wireless networks”, November 19, 2004.

44. D. Stanley, J. Walker, Internet working group, RFC 4017, “ EAP methods Requirements for Wireless Lan’s” 2005. At: http://www.ietf.org/rfc/rfc4017.txt

45. B. Adoba, P. Calhoun, ”RADIUS (Remote Authentication Dial In User Services) Support for EAP.” , 2003. At: http://www.ietf.org/rfc/rfc3579.txt

46. B. Adoba, D.Simon ”PPP EAP TLS Authentication Protocol” , October 1999.
http://www.ietf.org/rfc/rfc2716.txt

47. Cisco systems ” A comprehensive Review of 802.11 wireless lan security and the Cisco wireless security suit” , White paper 2002.

48. Jim Geier, ”Wireless LANs”, second edition 2002, ISBN 0-672-32058-4

49. Neeli Prasad and Anand Prasad, “WLAN Systems and wireless IP for Next generation communication” 2001, ISBN 1-58053-290-X

50. Christophe Devine, “Aircrack - cracking WPA with WHAX”, juni 2005. Last available at: http://sid.rstack.org/videos/aircrack/whax-aircrack-wpa.html

51 D. Eastlake, S. Crocker, cybercash, J. Schiller, ”Random recommendation for security” , 1994. At: http://www.ietf.org/rfc/rfc1750.txt

52 Wikipedia, The Free Encyclopedia “HMAC”, last updated http://en.wikipedia.org/wiki/HMAC-SHA1

53 NIST, “NIST last comments on recent cryptanalytic attacks on secure hash functions” year 2004, Available at: http://csrc.nist.gov/hash_standards_comments.pdf

54 IEEE computer Society, “802.1X port based network access control” 13 December 2004. Available at: http://standards.ieee.org/getieee802/download/802.1X-2004.pdf

55 Jesse Walker, Intel cooperation, “802.11i overview”, 2 September 2005. Available at: www.drizzle.com/~aboba/IEEE/11-05-0123-01-0jtc-802-11i-overview.ppt

56 D. Whiting, R. Housley, N. Ferguson, Macfergus. Internet working group,RFC 3610. “Counter with CBC-MAC”. Request for comments - September 2003 Available at: http://www.ietf.org/rfc/rfc3610.txt

57 S. Frankel, R. Glenn, S. Kelly. “AES-CBC algorithm and its use with IPsec”, September 2003.Available at: Standard http://www.ietf.org/rfc/rfc3602.txt

58 J. Schaad, and R. Housely. RSA laboratories, September 2004 “ AES Key Wrap algorithm. Available at: http://www.ietf.org/rfc/rfc3394.txt

59 N. Asokan, Valtteri Niemi, Kaisa Nyberg, Nokia Research center. “Man-in-the-Middle in Tunnelled Authentication Protocols”, November 2002. Last available at: http://eprint.iacr.org/2002/163.pdf

60 ChanghHua He, John C. Mitchell. Stanford University. “1 Message Attack on the 4-

Way Handshake" May 2004.

61 S. Kent, R. Atkinson.. "Security architecture for the internet protocol" November 1998 Available at: http://www.ietf.org/rfc/rfc2401.txt

62 National institute of standards and technology (NIST). "Guide to IPsec VPNs" December 2005. Available at: http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf

63 Wikipedia, The Free Encyclopedia. "Public key crypto"
Available at: http://en.wikipedia.org/wiki/Public_key

64 Changhua He, John C Mitchell. "Analysis of the 802.11i 4-Way Handshake", October 2004. Available at the ACM digital library: http://portal.acm.org/dl.cfm

65 2.4Ghz WiFi and wireless jammer. Last updated and available, 10 mach 2007 at: http://www.globalgadgetuk.com/wireless.htm

66 F.Bersani, H. Tschofenig. "The EAP-PSK protocol". Introduces and new and interesting EAP method. January 2007.
Available at http://www.ietf.org/rfc/rfc4764.txt

67 Wave bubble. "A design for a self tuning portable RF Jammer". 8 mars 2007.
Available at: http://www.ladyada.net/make/wavebubble/index.html

68 Microsoft TechNet. "PEAP" 21 January 2005. Last updated:
http://technet2.microsoft.com/WindowsServer/en/library/3e94a25d-8922-4935-b248-540aa6b8c5101033.mspx?mfr=true

69 National Security Agency (NSA), United States of America, Ft. George G. Meade , MD. System and network attack centre, "Recommended 802.11 Wireless Network Local Area Network Architecture" 23 September 2005. Available at: www.nsa.gov

70 KARMA, "Wireless client security assessment tool". Available at:
http://www.theta44.org/karma/

71 Networkworld, Joshua Wright, Article: "Issues with SSID cloaking" 5 mars 2007.
Available at: http://www.networkworld.com/columnists/2007/030507-wireless-

security.html

72 Rebecca Bace, Peter Mell, National Institute of Standards and Technology (NIST). "Intrusion detection systems", compose in 2000.

73 Jhiwang Yeo, Moustafa Youssef, Ashok Agrawala. "A framework for wireless LAN monitoring and its applications" 1 October 2004. Available at: http://delivery.acm.org/

74 Bahl, Chandra, Padhye, Ravindranath, Singh, Wolman, Zill, Microsoft research. "Enhancing the security of cooperate WiFi networks using DAIR" 22 June 2006. Available at: http://delivery.acm.org/

75 Yu-Xi Lim, Tim Schmoyer. "Wireless Intrusion Detection and Responses" 2003. Available at: Available at: http://delivery.acm.org/

76 Clincy Victor, Sitaram Ajay Krithi. "Evaluation and of a free software (FS) tool for wireless network monitoring and security" composed in 2005. Available at: http://delivery.acm.org/

77 Arunesh Mishra, William A Arbaugh, Maryland . Document: "An initial security analyses of the 802.1X standard" 6 Feb 2002. Available at: http://delivery.acm.org/

78 John Bellardo and Stefan Savage. "Denial-of-service-attacks: Real vulnerabilities and particle solutions" , 2003. Available at: http://delivery.acm.org/

79 SimpleMAC. A network tool that changes the MAC address connected to the computer network card. Available at: http://dukelupus.pri.ee/simplemac.php

80 Wikipedia. The Free Encyclopedia. Search for " Honeypot". Available at http://en.wikipedia.org/wiki/Honeypot_%28computing%29

81 Thomas Mundt. "Two methods of authenticated positioning". 2 October 2006. Available at: http://delivery.acm.org/

82 YounSun Cho, Lichun Bao, Michael Goodrich. "Secure access control for location-based applications in WLAN systems". Available at: http://delivery.acm.org/

83 Naveen Sastry, Umesh Shankar, David Wagner. "Secure Verification of Location

Claims". Available at: http://delivery.acm.org/

84 Cisco Systems. "Cisco wireless Location Appliances". Available at: http://www.cisco.com/en/US/products/ps6386/products_data_sheet0900aecd80293728.html

85 AiroPeek Wildpackets. A wireless LAN network analyzer tool. "RF spectrum analyzer for Wi-Fi networks" 2007. Available at: http://www.wildpackets.com/

9 Appendix

9.1 *WPA 2.0*

The WPA 2.0 standard was released in September 2004, and introduces the complete ratified version of the IEEE 802.11i standard. According to [9], products that holds a WPA 2.0 certification compiles with the IEEE 802.11 standard as amended by IEEE 802.11i which means that such products can be recommended for use in Robust Security Networks (RSN). WPA 2.0 enterprise certified and FIPS validated products builds on a quality assurance related to high assurance wireless communication services. The WAP 2.0 certification validates interoperability with selected EAP methods, and is approved according to compatibility with operational requirements. The problem with WPA 2.0 is that there currently exist no WPA 2.0 certified products providing AS functionality [9]. This means that implementing RADIUS (AAA) servers may cause interoperability problems with WPA 2.0 certified products. This signifies that commercial WPA 2.0 products used to provide RSN solutions must be tested and closely evaluated before implementation.

9.2 *WLAN security configuration aspects*

In this section we will identify some important security aspects and configuration utilities which should be considered in order to implement wireless solutions for high assurance networks.

9.2.1 Configuration security aspects

In this section I will shortly discuss some vulnerabilities and security aspects following the aim for a best practice security configuration.

- ***SSID broadcasting and configuration***

The Service Set Identifier (SSID) is the name that identifies and distinguishes different WLAN's. The SSID must be changed from the default value to an appropriate name. Because this name identifies the WLAN, it should be hard to guess for outsiders and must not provide any information about the organization. SSID cloaking techniques, as described and recommended in [69], proposes to hide the SSID information by replacing a null value in to the SSID field in broadcast and probe request messages, as well disabling AP's SSID broadcasting. The intention is to reduce availability and to make it difficult to discover the wireless network. Thus, cloak-configuration can be vulnerable to attacks using attack tools such as KARMA [70] which identifies probe request messages in order to set up rogue access points. As described in [71], KARMA can detect a disclosed SSID from a STA probe request to impersonate the AP and to fool the STA to connect to a none-legitimate rogue access point. We can conclude that hiding the SSID in an 802.11 network is extremely difficult, but by making complicated SSID names, changing them at regular intervals, and turning off SSID broadcast will prevent the wireless network from easy discovery.

- ***WLAN firewalls, personal firewalls and anti-virus software for all STA's***

A firewall solution can be used to enforce a certain security policy by creating rules and allow authorized protocols and services to traverse. Such a solution can be used protect the interface between the WLAN and the distribution system, as well as between AP and STA's. Firewalls and antivirus software must be required for all STA's, and a firewall solution can be locally adapted to enforce strong security requirements. According to [9], a STA-firewall solution can prevent direct attacks on STA's before the 4 way-handshake has successfully completed.

- ***WLAN and secure system management***

IEEE 802.11i does not specify any requirements according to safeguard management system and administration of wireless networks. Based on this and because of wireless availability aspects, high assurance WLAN system should deactivate the possibility to manage the WLAN system over the wireless interface. A physical connection adapted with a suitable security protocol (SNMPv3, SSL/TLS, SSH or IPSec) can be used for administrative purposes. To extend management security, as described in [9], a dedicated Virtual LAN (VLAN) channel can be established to segregate management traffic. This will prevent none-administrators from accessing management resources.

9.3 IEEE 802.11w, work in progress

According to [77] management frames are not authenticated. This is very vulnerable because attacker can use such use such frames to perform DOS attacks. The 802.11w standard aims to provide management frame protection (MFP) by appending authenticity to each management frame sent between STA and AP. The authenticity is implemented using a signed AES HMAC code (AES hash messages authentication code (HMAC)). As a result the AP will not accept management's frame which do not have a valid authentication code, and thereby potentially block flooding and DOS attacks. The IEEE 802.11 standard is expected to be announced in 2008.