AEROMACS - Security Analysis

Document information	
Project Title	Airport Surface Datalink
Project Number	15.02.07
Project Manager	INDRA
Deliverable Name	AEROMACS - Security Analysis
Deliverable ID	D08.2
Edition	00.01.00
Template Version	03.00.00
Task contributors	
AENA, AIRBUS, DSNA (TASK LEADER), EUROCONTROL, INDRA, SELEX ES, THALES	

Abstract

This deliverable has been developed by SESAR Project 15.2.7 "Airport Surface Data Link within WA8 "Safety and Security Analysis" that aims at performing an extensive analysis to identify the impact on security and safety issues of the new IEEE 802e/aero datalink.

This document consist of part 2 of the deliverable, and WiMAX security is addressed to derive guidance at standardisation, implementation and deployment phases of the AeroMACS system.

Authoring (D08-Part2)

Prepared By - *Authors of the document.*		
Name & Company	Position & Title	Date
[redacted]/ ENAC for DSNA	[redacted]	17/02/2014
[redacted]/ ENAC for DSNA	[redacted]	17/02/2014
[redacted] INDRA	[redacted]	17/02/2014
[redacted] THALES	[redacted]	17/02/2014

Document History (D08-Part2)

Edition	Date	Status	Author	Justification
00.00.01	15/02/2011	Draft	ENAC	Draft deliverable describing the Security analysis methodology
00.00.02	08/03/2011	Draft	ENAC	Draft addressing partners comments
00.00.03	11/04/2011	Draft	INDRA	Draft contribution on section 3
00.00.04	08/07/2011	Draft	THALES	Draft contribution on section 4
00.00.05	17/08/2011	Draft	ENAC	Draft simulations results regarding risk propagation
00.00.06	22/05/2012	Draft	ENAC	Final simulations results incorporating suggested additional simulation scenarios
00.00.07	12/11/2012	Draft	ENAC	Draft deliverable including simulations results on risk propagation
00.00.08	13/05/2013	Draft	ENAC	Draft deliverable including analysis of Wimax system and end-to-end security vulnerabilities
00.00.09	15/11/2013	Draft	ENAC	Draft deliverable addressing partners comments, WG82 comments, including annex on comparison between Radius and Diameter, CVSS datagram description, algorithm diagram. Draft disseminated to ICAO.
00.00.10	26/03/2014	Draft	ENAC	Final version for handover addressing ICAO comments
00.01.00	27/03/2014	Final	INDRA	Version for handover

Intellectual Property Rights (foreground)

This deliverable consists of SJU foreground.

Table of Contents

List of tables

List of figures

Executive summary

In this deliverable, WiMAX security is addressed to derive guidance at standardisation, implementation and deployment phases of the AeroMACS system.

First, WiMAX security features are analysed considering WiMAX security framework integrated into the MAC layer (i.e. Privacy sublayer) and the WiMAX interworking security, meaning the security mechanisms used in addition to the built-in WiMAX MAC security. Guidances are provided to mitigate WiMAX intrinsic vulnerabilities to be considered during AeroMACS standardization activities.

Then, a quantitative risk assessment methodology for network security based on risk propagation is described and applied to the AeroMACS deployment scenarios. The proposed methodology estimates the network risk level quantitatively based on several criteria such as the complexity of the conducted attack, or its impact within the network. Vulnerability statistics on WiMAX systems issued from the NVD public database are used within the methodology throughout the CVSS impact scores. The AeroMACS security is analyzed using the risk assessment methodology, the experimental results highlighted several weaknesses of the AeroMACS system in an isolated network topology (i.e. without additional security features), meaning that the system needs more considerations from a security point of view. Following several guidance's drawn after the preliminary results, the AeroMACS network topology has been improved step by step in order to reduce the network security risk. Guidance arising from this risk assessment on AeroMACS should be considered by manufacturers and network operators in order to reduce the network security risk.

1 INTRODUCTION

AeroMACS is a new aviation-dedicated transmission technology based on the WiMAX IEEE 802.16e standard. The aim is to support safety and regularity of flight communications with mobile (aircraft and airport vehicles) at the airport surface. The AeroMACS technology allows MSs (Mobile Stations) such as aircraft or surface vehicles to communicate with airline operators and airport staff at three different surface zones: RAMP (where the aircraft is at the gate before departure), GROUND (the aircraft is taxing to the runway), and TOWER (until the aircraft takes-off).

Note: In some countries, AeroMACS can be used for communication with fixed subscribers for ATC and Airport operations.

Using a WiMAX-based technology standard is profitable for the aviation industry for many reasons. First, the standardization and deployment processes are fast and cost-effective at the opposite of a newly developed standard for the sake of airport communications. Moreover, the scientific community has been working on IEEE 802.16 standards since many years. Highly qualified certification agencies such as the WiMAX Forum are continuously looking after interoperability and technical issues related to the standard. The AeroMACS standard is currently a hot topic in datalink communications and many tests are already running their way for a future deployment. For instance, an AeroMACS profile was recently developed jointly by the RTCA SC-223 and EUROCAE WG-82 and intended to provide performance requirements for the system implementation.

In this document, the WiMAX technology and its security features are presented and a security analysis is provided on AeroMACS deployment scenarios. The goal is to introduce some basic networking concepts and discuss the security issues that may be faced when the technology will be deployed as an Aeronautical system. The security features defined in the WiMAX standard are explained, then a network security risk assessment is conducted.

Risk assessment is generally considered as the core of the computational framework in a risk management process for a network information system. Usually, it is conducted based on threat likelihood and impact, which are respectively the probability of occurrence of a threat and potential damages resulting from it on the system. A threat is the possibility for an intruder to violate the privacy of a system. This process is mandatory and crucial for the protection of interconnected systems that provide various services to their clients or users. As the involved factors (likelihood, impact) can be modeled in many ways, numerous risk assessment techniques have already been proposed. Mostly, these risk assessment methods are based on subjective factors such as qualitative expert investigation. In addition, these methods could be not perfectly adapted to complex network infrastructure for which it is not easy to deduce exactly the total risk of the infrastructure, even if we can evaluate this risk node by node. In fact, apart from individual vulnerabilities, the interconnected nodes can seriously compromise global network security. Indeed, many endogenous and exogenous factors have to be analyzed in order to determine as accurately as possible the risk level for the whole network. On the one hand, the global network risk can be very low even if the risk to a single node is very high (this node is isolated from the rest of the network and does not communicate with many other nodes). On the other hand, the security of the whole network can be heavily compromised by nodes, which have strong interconnections, and data flow exchanges with the rest of the network even if those nodes have individually a low network risk.

Considering all these factors, a new approach is proposed in this document for AeroMACS network security assessment that measures quantitatively the network risk level based on critical aspects such as the impact of a successful attack on a node and the risk propagation of that attack within the network.

Note: the guidance's derived from the present analysis should also be considered as preliminary inputs by SESAR Project 15.2.4 to analyze security from an end-to-end perspective considering all the access networks foreseen in the Future Communication Infrastructure.

1.1 DOCUMENT STRUCTURE

This report is structured as follow:

- The first part of the deliverable discussed the security issues related to the WiMAX protocol from two points of view: the first one takes into considerations the security weaknesses of the protocol itself, at the MAC layer where the security framework has been defined. The second point of view refers to the interworking security issues that could be faced when the AeroMACS is connected to other COTS nodes such as DHCP or AAA servers.
- The second part of the deliverable addresses these security issues from a third point of view, namely risk assessment of vulnerabilities inherited from those security flaws and implementation issues.

Both parts should provide guidances to secure AeroMACS infrastructure to be considered during system standardization and implementation phases.

In addition, some specific AeroMACS issues are addressed in ANNEX and are relevant for implementation and standardization:

- Annex C: Comparison between Radius and Diameter AAA protocols: according to WiMAX Forum, both protocols can be used to secure WiMAX. A choice is required to ensure interoperability.
- Annex D: this annex refers to a working paper submitted to ICAO by SESAR P15.2.7 to discuss the different EAP methods foreseen in WiMAX AAA framework: EAP TLS, EAP TTLS and EAP AKA. To ensure interoperability, one must be selected. In addition, are provided some preliminary information regarding a potential solution to provide authentication and authorization capabilities at service levels (ATC, AOC, Airport operations) based on AAA architecture.

1.2 INTENDED READERSHIP

This document is the final deliverable of the security task related to the SESAR 15.2.7 WP. The intended readership includes (but is not limited to) people involved in:

- Security task related to SESAR or new aeronautical data link technologies (*e.g.* ICAO ACP members);
- AeroMACS standardization such as RTCA SC-223 and EUROCAE WG-82 members;
- Manufacturers of AeroMACS system,
- ASN and CSN operators,
- Risk assessment in network security.

1.3 ACRONYMS AND TERMINOLOGY

Term	Definition
AAA	Authentication Authorization Accounting
ACD	Aircraft Control Domain
ACK	Acknowledgment

Term	Definition
ACP	Aeronautical Communication Panel
AEROMACS	Aeronautical Mobile Airport Communication System
AES	Advanced Encryption Standard
AISD	Airline Information Service Domain
AK	Authentication Key
ALE	Annual Loss Expectancy
AOC	Airline Operational Communications
AOPCL	Airport Operation Centers Clearance
APC	Airline Passenger Communications
APT	Airport
ARINC	Aeronautical Radio Corporation
ARR	Arrival
ASN	Access Service Network
ATC	Air Traffic Communications
ATM	Air Traffic Management
ATS	Air Traffic Services
AUTH-INVALID	Authentication Invalid
BS	Base Station
BSID	Base Station Identifier
CC	Common Criteria
CCTA	Central Computer and Telecommunications Agency
CID	Connection Identifier
CMAC	Cipher-based Message Authentication Code
COA	Care of Address
COCR	Communications Operating Concept and Requirements
COTS	Commerial Of The Shelf
CPS	Common Part Sublayer

Term	Definition
CRAMM	Risk Analysis and Management Method
CS	Convergence Sublayer
CSN	Connection Service Network
CVSS	Common Vulnerability Scoring System
DBPC_REQ	Downlink Burst Profile Change Request
DEP	Departure
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DLC	Departure Clearance
DNS	Domain Name Server
DOS	Denial of Service
EAP	Extended Authentication Protocol
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
EMSK	Extended Master Session Key
ETSI	European Telecommunications Standards Institute
EUROCAE	European Organization for Civil Aviation Equipment
FA	Foreign Agent
FBSS	Fast Base Station Switching
FH	Frequency Hopping
FL	Forward Link
FPC	Fast Power Control
FTP	File Transfer Protocol
GKEK	Group Key Encryption Key
GRE	Generic Routing Encapsulation
GTEK	Group Traffic Encryption Key
GW	Gateway
H-NSP	Home Network Service Provider

Term	Definition
HA	Home Agent
HHO	Hard Handover
HMAC	Hash-based Message Authentication Code
HTTP	Hyper Text Transfer Protocol
ICAO	International Civil Aviation Organization
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IFE	In-Flight entertainment
IP	Internet Protocol
IPSEC	IP Security
ISO	International Organization for Standardization
KEK	Key Encryption Key
LAN	Local Area Network
MAC	Message Authentication Code
MANET	Mobile Adhoc Network
MBRA	Multicast and Broadcast Rekeying Algorithm
MD5	Message Digest 5
MDHO	Macro Diversity Handover
MIP	Mobile IP
MOB_ASC-REP	Mobile Association Report
MOB_NBR-ADV	Mobile Neighbor Advertisement
MS	Mobile Station
MSID	Mobile Station Identifier
MSK	Master Secret Key
NAP	Network Access Provider
NBR-ADV	Neighbor Advertisement
NGN	Next

Term	Definition
NIST	National Institute of Standards and Technology
NSP	Network Service Provider
NVD	National Vulnerability Database
NWG	Network Working Group
OCTAVE	Operationally Critical Threat Asset and Vulnerability Evaluation
OFDM	Orthogonal frequency-division multiplexing
OSI	Open Systems Interconnection
P2MP	Point to Multi Point
PDU	Payload Data Unit
PHY	Physical Layer
PID	Priority Identifier
PIESD	Passenger Information and Entertainment Services Domain
PKI	Public Key Infrastructure
PKM	Privacy Key Management
PKM-REQ	PKM Request
PMIP	Proxy Mobile IP
QOS	Quality of Service
QPSK	Quadrature phase-shift keying
RADIUS	Remote Authentication Dial-In User Service
REG-REQ	Registration Request
RES-CMD	Reset Command
RFC	Request For Comment
RL	Return Link
RNG-REQ	Ranging Request
RNG-RSP	Ranging Response
RP	Reference Point
RSA	Rivest Shamir Aldman

Term	Definition
RTCA	Radio Technical Commission for Aeronautics
SA	Security Association
SAID	SA Identifier
SAP	Service Access Point
SDU	Service Data Unit
SESAR	Single European Sky ATM Research Program
SFA	Service Flow Authorization
SGKEK	Sub Group Key Encryption Key
SIM	Subscriber Identity Module
SITA	Société Internationale des Télécommunications Aéronautiques
SLA	Service Level Agreement
SRQC	Service based Risk Quantitative Calculation
SS	Subscriber Station
TEK	Traffic Encryption Key
TLS	Transport Layer Security
TMA	Terminal Aera
UL-MAP	Uplink MAP
URL	Uniform Resource Locator
V-NSP	Visited-Network Service Provider
WIMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WP	Working Package

2 BACKGROUND ON WiMAX

2.1 WIMAX PROTOCOL ARCHITECTURE

The WiMAX protocol stack is composed of two main layers: the PHY and the MAC layers, which is itself, composed of three sub-layers as shown in Figure 1. The first layer is the service specific CS (Convergence Sublayer) which communicates with higher layers through the CS SAP (Service Access Point), acquires external network data and transforms them into MAC SDUs (Segment Data Units). The second layer is the CPS (Common Part Sublayer) responsible for the system access, bandwidth allocation, connection management, and MAC SDUs fragmentation into MAC PDUs (Protocol Data Units).

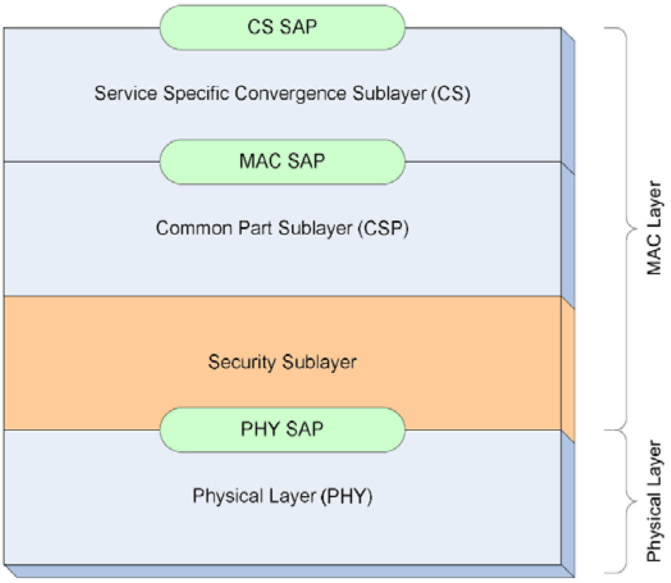


Figure 1: WiMAX Protocol stack

As shown in Figure 1, security is handled at the security sublayer. It addresses many security services such as authentication, authorization, key establishment, and encryption/decryption of data between the PHY and MAC layers. In fact, after the weaknesses that restricted the early IEEE 802.11 networks, security has been seriously considered in the WiMAX standards (and consequently AeroMACS) and was built in (rather than built on) the 802.16 protocol architecture since the first standard release in 2001. The security sublayer provides several mechanisms designed to protect both service providers and users/customers from unauthorized access or information disclosure.

However, this is not sufficient to build in a broadband wireless airport network: end-to-end services such as QoS, security, mobility management or IP connectivity are a requisite and should be provided beyond the WiMAX scope (*i.e.* at higher layers of the protocol stack). In this context, an WiMAX network reference model has been developed. Besides, security in section 3 will be discussed from two points of view: WiMAX privacy sublayer security and WiMAX network security (*i.e.* security considerations above the MAC layer).

2.2 WiMAX NETWORK REFERENCE MODEL

In order to understand better the interconnection security considerations discussed in section 3.2, a logical representation of a WiMAX reference network must be first introduced. Such a scheme distinguishes between the logical domains, the functional entities, and the RPs (Reference Points) as reported in Figure 2. This reference network model is used to define topology scenarios for a later deployment of the AeroMACS system.

The main depicted functional entities are:

- MSs and SSs which could be aircraft, surface vehicles, or passenger personal generic devices;
- The ASN (Access Service Network) network represents the boundary for functional interoperability between MSs and WiMAX connectivity services. The ASN integrates many functions such as forwarding AAA (Authorization, Authentication, Accounting) messages between MSs and the H-NSP (Home Network service Provider), relaying network service messages (*e.g.* DHCP request/response), etc;
- The CSN (Connectivity Service Network) network provides connectivity to public networks such as the Internet.

The logical domains, which are basically set of functions associated to a single domain, and considered in the network reference architecture, are:

- The NAP (Network Access Point) is the physical point used by MSs to access the network;
- The H-NSP (Home Network Service Provider) is the AeroMACS service provider, which provides SLA (Service Level Agreement) to the MSs such as IP connectivity and core network services. These NSPs could be for instance, SITA, ARINC, or even the airlines depending on the provided service;
- The V-NSP (Visited Network service Provider) is visited by the MSs to access the network in a roaming scenario (which usually depends on the roaming agreement made between the MSs H-NSP and the V-NSP).

Referring to Figure 2, RPs (Reference Points) are the communication end-points between functional entities and represent the interfaces that ensure the interoperability between WiMAX related components.

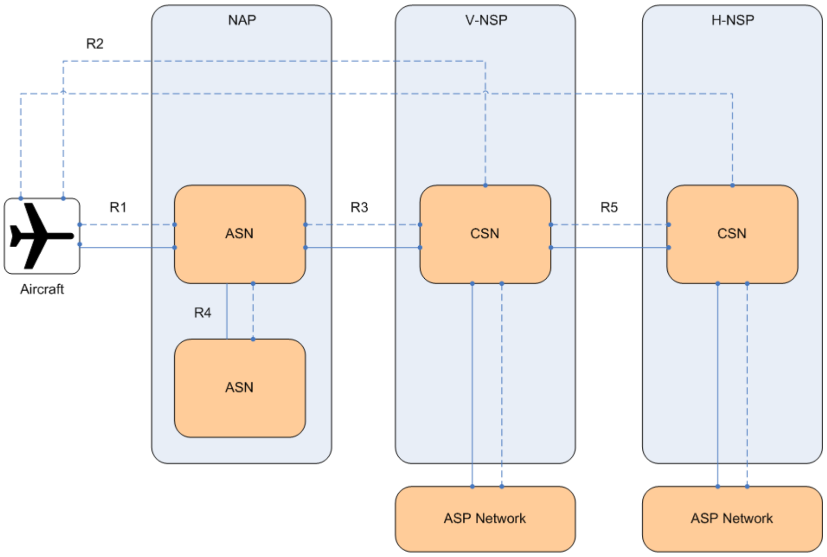


Figure 2: WiMAX Network Reference Model

Table 1 gives a description of all the reference network architecture interfaces:

RP	Interface	Functionality
R1	Between MSs and BSs	Air interface
R2	Between MSs and the CSN	IP host configuration, IP mobility, Authentication, Authorization
R3	Between the ASN and the CSN	Mobility management, Authentication, Authorization, tunneling
R4	Between ASNs	Mobility management, ASNs interworking
R5	Between CSNs	Roaming and interworking between the V-NSP and the H-NSP

Table 1: WiMAX Reference Point Interface Description

3 WiMAX SECURITY FEATURES

Even if the WiMAX security sublayer relies on several security protocols and constitutes a complex and heterogeneous security framework, security weaknesses still exist and an end-to-end WiMAX network should be strengthened by using other security mechanisms.

The WiMAX security is then divided into two categories:

- The WiMAX security framework integrated into the MAC layer (*i.e.* Privacy sublayer);
- The WiMAX interworking security, meaning the security mechanisms used in addition to the built-in WiMAX MAC security.

These two categories of WiMAX security features are analyzed in this part of the document in order to derive guidance's for AeroMACS standardization and implementation.

It has to be noted that the end-to-end communication infrastructure integrating the AeroMACS system as an Access network was not fully defined at the time this document is issued. The analysis done in this document is based on WiMAX Forum documentation assuming it will be deemed relevant for the Aeronautical world.

3.1 WiMAX PRIVACY SUBLAYER SECURITY

The WiMAX security weaknesses proper to the MAC privacy sublayer can be categorized as the following:

- PKMv2 weaknesses;
- Management traffic weaknesses;
- Multicast and broadcast service weaknesses;
- Handover weaknesses[1].

3.1.1 PKM WEAKNESSES

The second version of the PKM protocol tries to overlap vulnerabilities found in the original version of the protocol (i.e. PKMv1 defined in the early versions of the WiMAX IEEE 802.16 standard) but still, some of them remains exploitable in PKMv2.

The possible attacks on the second version of the PKM protocol are:

- ***Attacks on the authorization phase:*** the aim of these attacks is to impersonate both legitimate MS and BS in two different sessions, in order to lead to a denial of access (meaning the BS does not authorize the legitimate MS accessing the network while it should accept it). This is typically an interleaving attack[2] where the MS is used as an oracle and the attacker impersonates, first a legitimate MS toward the BS, then a legitimate BS toward the MS (which is called also a rogue BS attack). Figure 3 shows how this interleaving attack on the authorization phase of the PKMv2 protocol is possible:

[1] Handover weaknesses could be placed in the AeroMACS network security section, but the described vulnerabilities are relevant to design issues in the handover management scheme provided in the AeroMACS MAC layer.

[2] A masquerade attack that uses information derived from ongoing or previous authenticate exchanges.

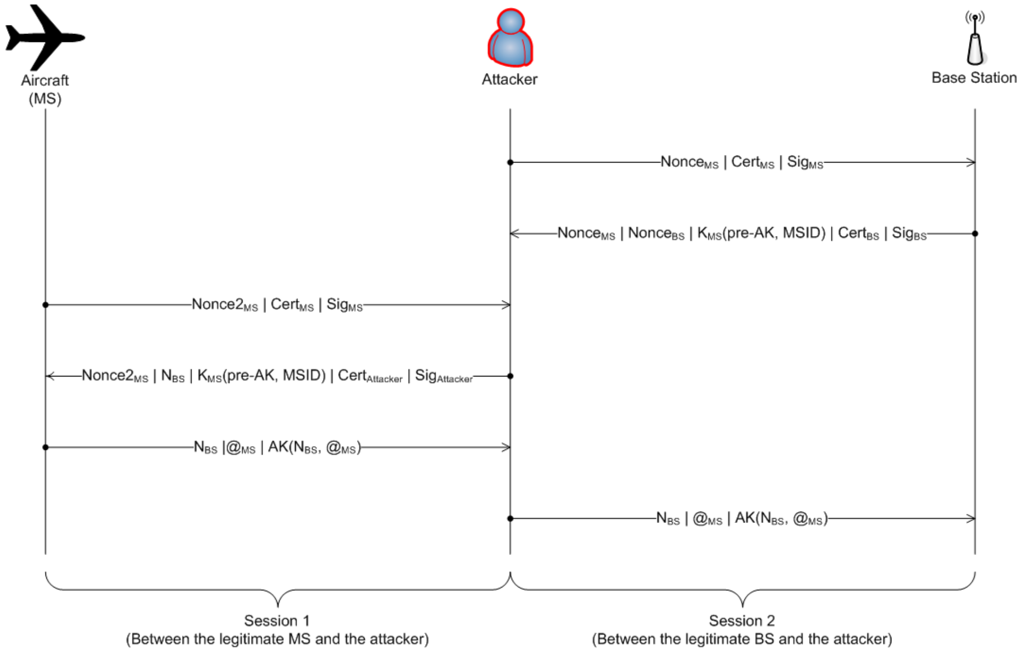

Aircraft
(MS)
Attacker
Base Station
Nonce$_{MS}$ | Cert$_{MS}$ | Sig$_{MS}$
Nonce$_{MS}$ | Nonce$_{BS}$ | K$_{MS}$(pre-AK, MSID) | Cert$_{BS}$ | Sig$_{BS}$
Nonce2$_{MS}$ | Cert$_{MS}$ | Sig$_{MS}$
Nonce2$_{MS}$ | N$_{BS}$ | K$_{MS}$(pre-AK, MSID) | Cert$_{Attacker}$ | Sig$_{Attacker}$
N$_{BS}$ |@$_{MS}$ | AK(N$_{BS}$, @$_{MS}$)
N$_{BS}$ | @$_{MS}$ | AK(N$_{BS}$, @$_{MS}$)
Session 1
(Between the legitimate MS and the attacker)
Session 2
(Between the legitimate BS and the attacker)

Figure 3: Attack on the authorization phase of the PKMv2 protocol

One session involves the legitimate BS and the attacker that impersonates a legitimate MS while the other session involves the legitimate MS and the attacker that impersonates a legitimate BS:

- The attacker begins by replaying an authorization request message previously sent by a legitimate MS;
- Being unable to decrypt the pre-AK key included in the BS response message (encrypted using the legitimate MS public key) and send back the authorization acknowledgment (as it should encrypt the BS address and nonce with the right AK key), the attacker attracts the MS to connect to it (in a second session) and use it as an oracle to generate the correct acknowledgment message;
- The MS sends the signed authorization request message to the rogue BS (meaning the attacker), which replies using the BS nonce and the pre-AK key concatenated to the MSID encrypted with the MS public key received from the first session. However, this message is signed using the private key of the attacker this time;
- As the AK key generated at the legitimate MS and legitimate BS should be the same (and uses both the MS and BS addresses), the attacker needs the BS address which could be retrieved easily by eavesdropping the traffic related to the legitimate BS;
- The legitimate MS replies by sending the BS nonce, its address, and an encryption of both values using the AK key he generated on his own side;
- The attacker has just to replay the received message to correctly impersonate the legitimate MS and finish the first session with the legitimate BS. This message could be after sent repeatedly in order to cause a denial of access of the legitimate MS.

In order to avoid this kind of attacks on the authorization phase of the PKMv2 protocol, two solutions can be foreseen:

- The first approach is to add the BSID (i.e. BS Identifier) to the last message in the authorization phase and encrypt it together to the BS nonce and MS address using the AK key;

- The second approach is to use both nonces and timestamps in parallel: while nonces guarantee the correct sequentiality of exchanged messages, timestamps guarantee message freshness even if the attacker tries to synchronize his clock with the legitimate MS or the legitimate BS.
- ***Attacks on the SA-TEK three-way handshake phase:*** The SA-TEK three-way handshake phase of PKMv2 is secure in it self, but it is still poss ble to conduct a replay attack on the first message (i.e. the SA-TEK challenge) of the protocol. Adding timestamps to the SA-TEK challenge message would be sufficient to protect against this replay attack.

3.1.2 MANAGEMENT TRAFFIC WEAKNESSES

During the Initial network entry many critical parameters are negotiated between the MS and BS. From a security point of view the entire procedure is extremely receptive to violations since all the security measures contemplated by the specification have not taken place and important negotiation parameters are transmitted in clear text.

The network entry procedure, executed by a MS to attach itself to a corresponding BS is not protect at all allowing several attacks:

- The RNG-REQ (Ranging Request) and RNG-RSP (Ranging Response) messages are not encrypted neither authenticated, then an attacker is able to listen to these messages and forge false RNG-REQ (e.g. by modifying the preferred downlink burst profile) and RNG-RSP (e.g. by setting the MS emission power to the minimum, which forces it to repeatedly trigger the ranging procedure from the beginning in order to reach the BS) messages to mislead the MSs which are unable to authenticate the source of the sending node;
- The WiMAX technology allows two different connectivity modes: the Point to Multi-Point (P2MP) mode where a MS can reach a BS in one hop, and a Mesh mode (similar to Ah-hoc networks) where MSs are connected together and packets are sent hop-by-hop until they reach the BS. In the Mesh connectivity mode, when a MS is about to enter the network, it listens for a network descriptor message to generate a list of potential neighbors and available BSs to connect with, then select a sponsoring node. This node will be responsible for tunneling the PKM-REQ (authentication request) and REG-REQ (registration request) messages from the new MS to respectively the BS and the registration node. Then, it forwards back the received response messages to the MS which is able to establish direct connections with it neighbors. In this topology, common vulnerabilities known in MANETs and sensor networks (e.g. Sybil attacks, Sinkhole attacks) are likely to occur. Indeed, the network descriptor message is not encrypted neither authenticated which open the path to several attacks. For instance, a malicious node can claim a shorter path to the BS in order to be the sponsoring node and create a sinkhole attack in order to attract all the network traffic to it.

Besides, many other management messages are not authenticated:

- MOB_NBR-ADV (Mobile Neighbor Advertisement) message is sent by the anchored BS currently linked to the MS in order to give a map of the neighbor BSs. An attacker could send false characteristics of the neighbor BSs to the MS in order to re-directed the MS to a rogue BS or to deny it from accessing the network;
- FPC (Fast Power Control) messages sent by the BS to ask the MS to adjust its transmission power could be forged by an attacker to force the MS transmission power to its minimum or to conduct a water torture attack. In order to reach the BS, the MS needs then to send repeatedly cumulated power adjustment messages. If the attack is conducted on several MSs at the same time, it could induce packet collisions in the uplink bandwidth request contention slots. Another consequence is a drain of the MS battery preventing it from communicating with the BS;
- DBPC-REQ (Downlink Burst Profile Change Request) messages sent by the BS to the MS to adjust the burst profile in order to cope with a variation of the distance between them (caused

by the MS node mobility) could be forged by an attacker to modify the encoding scheme used by the BS and preventing the communication between them;

- AUTH-INVALID (Authentication invalid) messages are sent by the BS to the MS if the shared AK key lifetime is no longer valid or if some management messages (containing HMAC or CMAC digests) in the authorization phase are not correctly authenticated. An attacker could forge such a message and send it the MS to deny it from accessing the network;
- MOB_ASC-REP (Mobile Association Report) messages are composed of an aggregation of all the neighbor BS identities that are likely to be connected to a MS when it performs a handover operation. This message is sent by the current (serving) BS to the MS, which chooses the best candidate to be the following (target) BS. An attacker could forge such a message with false information (e.g. unavailable services) in order to mislead the MS and prevents it from being anchored to the best BS candidate.

These unauthenticated management messages should then use some integrity protection techniques (*e.g.* HMAC, CMAC digest) or key agreement protocols such as Diffie-Hellman early in the initial ranging procedure. For some management messages, despite the fact they are authenticated, attacks may occur. For instance, the RES-CMD (Reset Command) message is sent by the BS to MSs that do not respond in order to ask them resetting their MAC state machine. As the message is authenticated, instead of sending a forged RES-CMD message, the attacker will force the BS to send itself the message. This is accomplished by synchronizing with the network and getting the UL-MAP (Uplink MAP) message, which contains a set of information that defines the entire access for all MSs during a scheduling interval. Thus, the attacker is able to choose a CID (Connection Identifier) and a burst profile related to the target MS. Then, it transmits a signal at the time scheduled for that node with transmission power strength higher than the one used by the legitimate MS, which force the BS sending the RES-CMD. The attacker is obviously able to repeat this procedure several times in order to prevent a stable connection to the MS in the network.

3.1.3 MULTICAST AND BROADCAST SERVICE WEAKNESSES

Multicast and broadcast services have several weaknesses that can be classified as it follows:

- ***Attacks on the GTEK multicast group keys:*** Multicast and broadcast messages are encrypted and authenticated using a symmetric shared key GTEK (Group Traffic Encryption Key) between a BS and all MSs belonging to the same group: this is an issue in the sense that any MS may impersonate the original BS by forging false multicast or broadcast messages and sending them to other MSs in the same group. The same attack is likely to happen when the BS wants to update the GTEK keys of all members of a multicast group: the BS sends the GTEK keys by encrypting it using the shared GKEK key. When received, each MS decrypts the message using the shared GKEK and update the used GTEK. Since the GKEK key is known by all the members of the multicast group, a malicious MS is able to distribute a false GTEK key with a valid encryption and authentication code, which forces the remaining MSs to update their active and valid GTEK key with a forged and false GTEK key. The direct consequence is that when the BS sends an encrypted message to the multicast group, MSs will be unable to decrypted it because their use a different GTEK key. However this vulnerability will be avoided when the legitimate BS sends the group key update message to update the current GTEK of the multicast group. In order to mitigate these vulnerabilities, the GTEK should be distributed separately by the BS to each MS securely using the shared KEK key. Another alternative would be to sign the key update message used to distribute the GTEK. Secure distr bution and key management in multicast groups have been widely investigated and several solutions could be used to avoid such weaknesses in the AeroMACS (e.g. the group-based key distribution algorithm proposed in [21]);
- ***Attacks on the MBRA protocol:*** The MBRA (Multicast and Broadcast Rekeying Algorithm) does not guarantee forward and backward secrecy:
    - o ***Attack on Backward Secrecy:*** When a new MS joins the multicast group, it receives the GTEK key from the BS and is able to decrypt all the previous messages that were

multicasted in the group using the same GTEK key (but only if the GTEK lifetime is still valid when the MS joins the group);

- ***Attack on Forward Secrecy:*** After leaving a multicast group, a MS remains able to receive the next GKEK (Group Key Encryption Key) and/or decrypt the next GTEK key while it should not be allowed to have such capabilities.

If the GTEK lifetime is optimized, it should help avoiding such backward and forward secrecy attacks. The default value is 12 hours while the standard recommends a value ranging between 30 minutes to 7 days. A low value should be privileged in order to renew the GTEK key as much as possible but induces an additional overhead on the anchor BS. [21] proposed a solution based on a hierarchy of Sub-Groups KEKs (SGKEKs) where MSs are regrouped into equal size sub-groups.

3.1.4 HANDOVER WEAKNESSES

Three different handover schemes are provided within the AeroMACS specifications, namely:

- ***Hard Handover (HHO):*** This is probably the simplest AeroMACS handover scheme where the MS communicates with a single BS at a time (i.e. establishes a connection with the following BS only if it breaks the previous connection with the old BS). In this handover scheme, the BS broadcasts periodically a NBR-ADV (Neighbor Advertisement) message which includes information about the neighbor BSs. When the connection with the following BS has been established, the MS is required to restart all the procedures related to ranging, authentication, and registration which could not be adapted for ATS since continuity of service is critical ;
- ***Macro Diversity Handover (MDHO):*** In this case, the MS is able to connect to several BSs instead of a single one. The set of BSs involved in the handover scheme (and called a diversity set) share MAC-context based information (e.g. encryption or authentication keys) used by the established connections. All the BSs in the diversity set send data to the MS which perform selection diversity;
- ***Fast Base Station Switching (FBSS):*** This the same handover scheme as MDHO except that the BS are not required to maintain the connection with the MS, meaning data are exchanged only with the anchor BS.

For each handover scenario, three different security settings are allowed by the WiMAX specifications and defined by two Handover optimizations bits in the RNG-RSP (Ranging Response) message. These security settings are the following:

- ***Bit_1=0 and Bit_2=0:*** Re-authentication and three-way TEK handshake are required. From a security point of view, this configuration provides the best protection against backward and forward secrecy attacks;
- ***Bit_1=1 and Bit_2=0:*** Re-authentication is not needed but TEKs are updated for all SAs (Security Associations), meaning that TEKs will be updated during the handover but the AK key will remains the same. Since the AK key is used to derive the KEK key and then obtain the corresponding TEKs, an impersonated BS could use the unchanged AK to determine the updated TEK of the following BSs;
- ***Bit_1=1 and Bit_2=1:*** neither re-authentication nor three-way TEK handshake are required, meaning that the MS keeps using the same TEKs established with the serving BS. This is obviously awkward in the case a malicious MS has impersonated the serving BS, it could comprise all the previous and following BSs.

In handover schemes, a trade-off between QoS and security should be discussed in order to provide a good protection against security attacks while latency (which is a crucial metric in operational traffic, essentially ATS) should be minimized.

3.2 WiMAX NETWORK SECURITY

From a security point of view, the central element of an WiMAX network is probably the AAA server which performs many functionalities beyond its main purposes (meaning authentication, authorization, and accounting). Indeed, the AAA server is widely used to supply user related information l ke QoS parameters or ASN network configuration, but it is also involved in IP mobility procedures (such as handover procedures) or even IP host configuration. DHCP is also important from a security point of view because some attacks can be conducted, but fortunately could be avoided as depicted in the following sub-sections.

3.2.1 DHCP SECURITY

In a WiMAX network, the DHCP protocol can be configured in two ways using either a DHCP proxy or a DHCP relay. Note that the DHCP protocol is solicited when the first packet sent by the MS is a DHCP_DISCOVER frame:

- When using a DHCP proxy, the ASN answers to the DHCP_REQUEST frame sent by the MS and assign him the IP address. In most cases, if a seamless handover is required, meaning that the session has to be kept alive, the assigned IP address should be the same before and after the handover. In order to do this, the MS puts the IP address he was already using in a specific option of the DHCP_DISCOVER frame. However, the DHCP_DISCOVER frames are not signed (i.e. unauthenticated) which means that a malicious MS could be trying to obtain the IP address of a legitimate MS. In order to avoid this security issue, the AAA server is involved in the IP address assignment procedure, meaning that the effective IP address to be assigned to the MS will be included into a specific RADIUS[3] (Remote Authentication Dial In User Service) attribute, part of the ACCESS_ACCEPT packet coming from the AAA server in the CSN;

- When using a DHCP relay, the ASN does not answer to the MS but forwards the request to a remote server. If the DHCP relay does not know the IP address of the remote server, this information has to be included in a RADIUS attr bute when received by the ASN at the end of the authentication (note that the remote server must be the same one used by the MS to be authenticated for the first time). Using a DHCP relay to communicate with a remote DHCP server is a tricky procedure as far as both integrity and packet authentication are not provided, leading to several attacks such as DNS spoofing (this can be done by modifying the DNS server address in order to redirect MSs to fake URLs) or Man-in-The-Middle attacks by changing the default gateway address. In order to address this security issue, the DHCP protocol introduces a security extension [22] to authenticate the frames exchanged between the DHCP relay agent and the DHCP server using a pre-configured symmetric key between them. This key, called DHCP_RK is used to derive other keys to secure each single session. In order to dynamically redirect the DHCP_REQUEST frames, the DHCP_RK must be also dynamically moved into the DHCP relay and the DHCP server when need. In order to do so, the AAA server is once again involved using RADIUS attributes. Figure 4 shows the DHCP protocol key exchange when a DHCP relay is used:

[3] Note that RADIUS is considered as the in-facto by-default AAA server to be used in the AeroMACS network, however this should be discussed further, specially for security purposes.

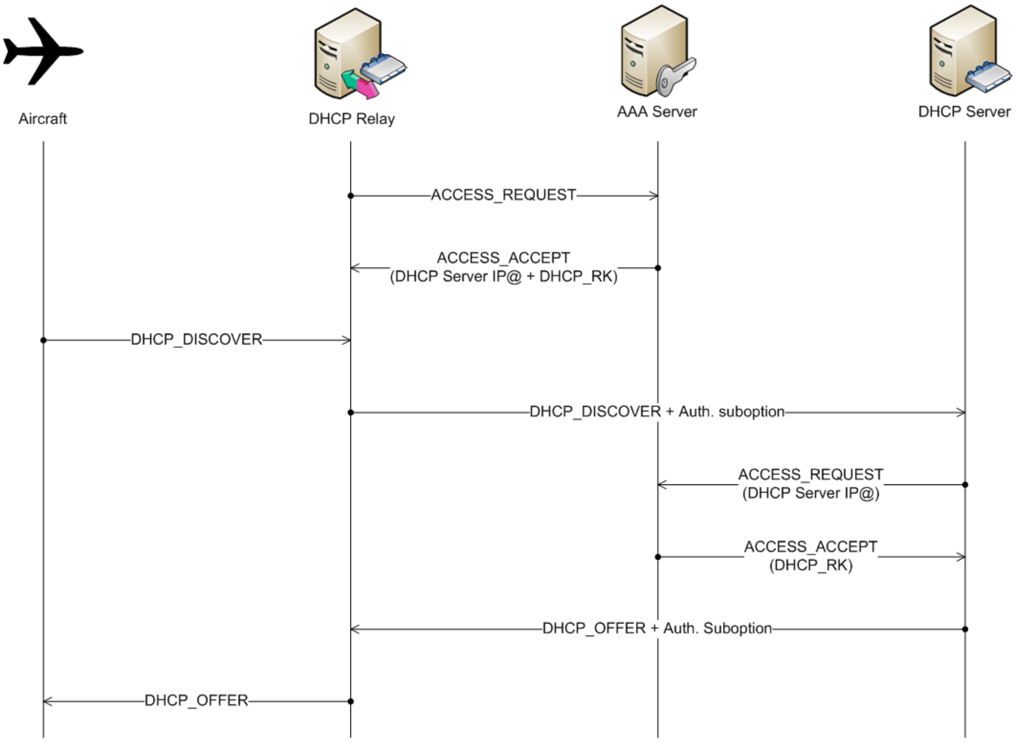


Figure 4: DHCP Key Management using a DHCP Relay

The exchange scheme shown in Figure 4 works as the following:

- When a MS is being authenticated, the CSN generates a random key and assigns it to the AAA server. The random key is a 64 bit random number used to generate IVs (Initiation Vectors) and keys used later in the exchange (DHCP_RK). Recommended practices for generating random numbers for use within cryptographic systems are provided in IETF RFC 1750. For more details, see Figure 8;
- The DHCP relay sends an ACCESS_REQUEST to the AAA server, which responds using an ACCESS_ACCEPT packet containing the DHCP server IP in the CSN, the DHCP_RK key, its lifetime, and a unique ID, all encapsulated into a RADIUS attribute;
- When the ACCESS_ACCEPT packet is received by the DHCP relay, he use it to sign the DHCP_DISCOVER frame sent to the DHCP server in the CSN;
- If the DHCP server does not already know the DHCP_RK key, he asks it from the AAA server, otherwise he uses it to verify the signature of the DHCP_DISCOV7.3.6ER frame sent by the DHCP relay.
- If the signature verification is correct, the DHCP server sends back a DHCP_OFFER packet, which will be forwarded by the DHCP relay to the MS.

Note that a RADIUS client has to be implemented on both DHCP relay and server in order to communicate correctly with the AAA server (RADIUS operates in a pure client-server paradigm, meaning the server does not initiate any messages but only replies to client requests).

3.2.2 MOBILE IP SECURITY

WiMAX uses the Mobile IP (MIP) protocol [23][24] to provide seamless, transparent and flexible IP addressing in the network. The main intent is to allow a MS having a permanent IP address while moving from one point of access to another, especially in roaming scenarios. Using DHCP allows the MS to keep a session alive and the same IP address before and after a handover, but this works in one way, meaning that the other communication party will receive IP packets but its responses will be routed to the home network of the MS. The MIP protocol is then used to forward these packets from the home network to the visited network.

When using the MIP protocol, a MS has two IP addresses:

- a home address (also called Home of Address – HOA) which is the IP address assigned by the Home Agent (HA) in the home network. This address remains fixed while the MS is roaming and is always used as long as the MS remains under its home network coverage;
- a Care of Address (COA) given to the MS by a Foreign Agent (FA) in the visited network. After receiving the COA address, the MS sends a REGISTRATION_REQUEST (Mobile IP RRQ) to his HA that contains its COA address, needed to reach the MS in the visited network. The HA confirms the reception by sending back a REGISTRATION_REPLY (Mobile IP RRP). When the MS is communicating from the visited network with a correspondent end entity, it uses a direct route from the visited network to reach the destination. However, when the correspondent node wants to communicate with that MS, it has to sends the IP packets using the MS home address. When the HA receives these packets, he looks to the associated COA address, sends the packets to the adequate FA, which finally forwards the packets to the MS.

Security issues related to MIP depend on how Mobile IP is supported on the MS side. There are two kinds of MIP support on the MS:

- Proxy MIP (PMIP): used for MSs that are not MIP compliant but still need persistent connections and seamless roaming when moving from a home network to a visited network. In this case, a third party entity called PMP Mobility Manager is in charge of handling the Mobile IP registration procedure for the MS toward the FA by intercepting the DHCP_DISCOVER frame sent by the MS (in order to get the COA address in the visited network), and performs the MIP registration with the HA. When the registration is finished, the PMIP Mobility Manager uses the DHCP protocol to assign the COA IP address to the MS. Again, the AAA server is involved in this procedure as the PMIP Mobility Manager receives several information (such as the MS HOA or the HA IP address) encapsulated in specific RADIUS attributes. Figure 5 shows all the logical entities involved when a MS is PMIP compliant:

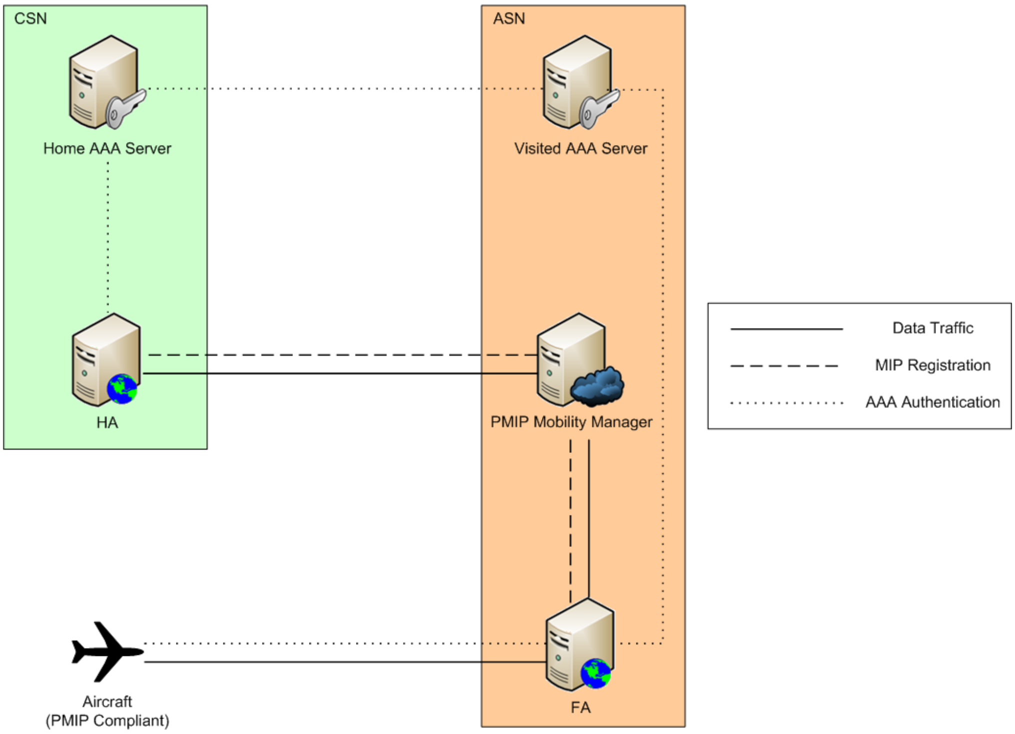


Figure 5: Mobile IP registration – PMIP Case

When a MS receives beaconing traffic from a foreign network it wants to access, he starts an authentication process with the H-NSP as depicted in Figure 6:

- The authenticator[4] (which is co-located with the PMIP Mobility Manager) intercepts the ACCESS_REQUEST sent by the MS and forwards it to the Home AAA server;
- The AAA server sends back an ACCESS_ACCEPT packet that contains information needed by the authenticator to contact the HA (i.e. IP address) and encrypt the MIP registration messages (i.e. the Master Session or MSK key produced by the AAA server);
- The authenticator communicates the MSK key to the PMIP Mobility Manager, which uses it later to derive the MIP_RK and the HA_RK keys needed to generate respectively the MS_HA key (to secure the MIP_RRQ message) and the FA_HA key (to secure the messages between the FA and the HA agents). Note that there is no need in this case for the MS_FA key because the MS and the FA are located in the same ASN. The complete AeroMACS key generation tree is detailed later;
- The PMIP Mobility Manager is now able to proceed to a Mobile IP registration on behalf of the MS by sending a signed MIP_RRQ packet to the HA using the MN_HA key;
- In order to verify the MIP_RRQ packet signature and continue the Mobile IP registration process, the HA sends an ACCESS_REQUEST packet to the AAA server asking for the needed keys (i.e. MN_HA and HA_RK keys);

[4] PKMv2 uses the IEEE 802.1X port-based access control standard which defines three basic roles that performs the authentication: a supplicant which is the client, an authenticator located in the ASN, and an authentication server (the AAA server) located in the CSN.

- The AAA server responds with an ACCESS_ACCEPT RADIUS packet that contains the required keys for the signature verification.

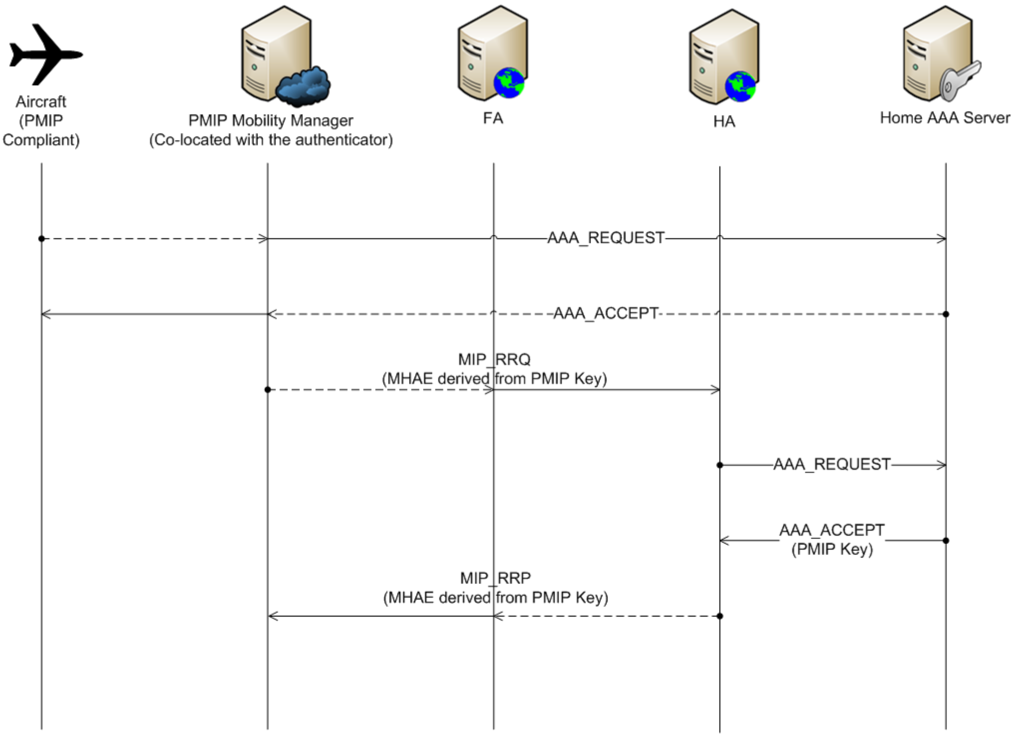


Figure 6: Mobile IP Key Management – PMIP Case

- Client MIP (CMIP): used for MSs that completely support Mobile IP. Figure 7 shows the Mobile IP registration for CMIP compliant MSs, which does not need a Mobility Manager in this case. Besides, the FA is able to distinguish between PMIP and CMIP clients depending on the first packet they send respectively (PMIP clients send a DHCP_DISCOVER packet whereas CMIP clients send a MIP_RRQ packet instead):

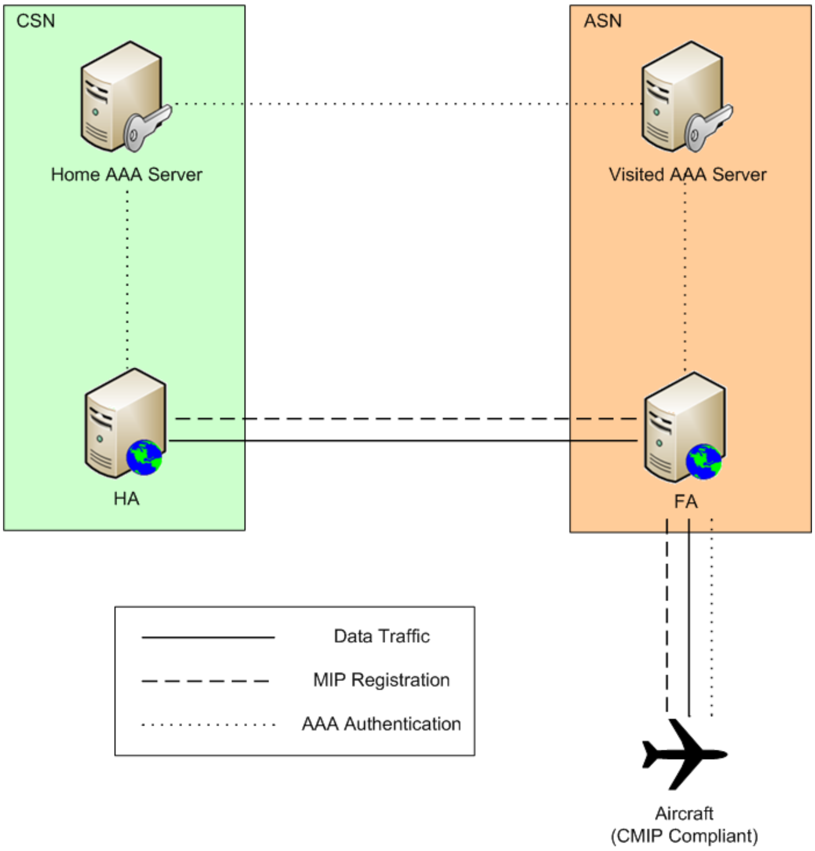


Figure 7: Mobile IP registration – CMIP Case

The security procedure is practically the same as for the PMIP clients except the usage of the FA_RK key needed to derive the MS_FA key (which is used to provide integrity and message authentication between the MS and the FA).

3.3 AEROMACS KEY GENERATION TREE

Figure 8 shows the overall AeroMACS key generation tree:

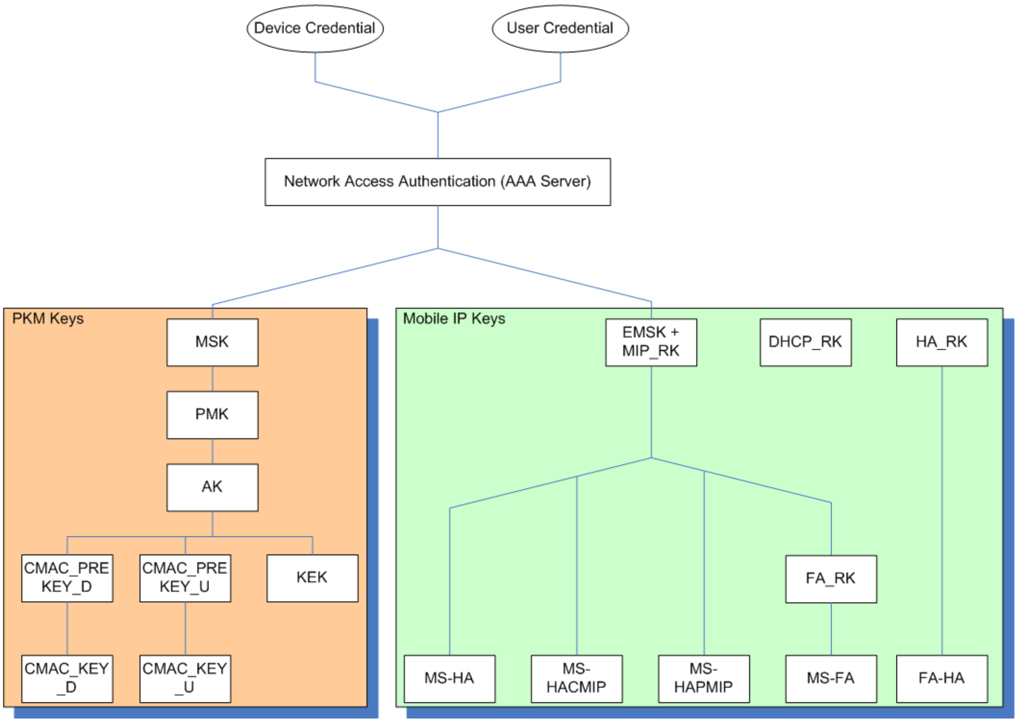


Figure 8 : AeroMACS Key Generation Tree

Two keys are generated into the MS and the AAA server after a successful EAP authentication:

- The MSK (Master Session Key) key is derived by the AAA server and sent to the authenticator using an ACCESS_ACCEPT packet. This key is used by the AeroMACS privacy sub-layer at the MAC layer to generate the keys needed by the PKMv2 framework (left branch of the tree in Figure 8);
- The EMSK (Extended Master Session Key) key used to generate MIP sessions keys (right branch of the tree), namely the MS_HA and FA_RK keys:
    - The MS_HA key will be sent to the HA when the HA sends an ACCESS_REQUEST packet to the server;
    - The FA_RK key will be sent to the authenticator and used to generate the MS_FA session key when the MS is CMIP compliant (remind that the MS_FA key is not needed when the MS is PMIP compliant).
- The DHCP_RK and HA_RK keys are not related to the MSK nor the EMSK keys as far as the (FA-HA) and (DHCP relay - DHCP server) paths do not depend on the MS authentication. Both keys are generated by the AAA server and sent respectively to the DHCP server and the HA when they are needed.

3.4 AEROMACS SECURITY TAXONOMY

In Table 2, a summary of possible security attacks on AeroMACS is provided through a taxonomy showing characteristics of those attacks and likely solutions to be used or privileged in order to face them.

Layer	Weaknesses location		Vulnerabilities	Attacks	Solutions
MAC Layer	PKM Protocol	Authorization phase	Message sequentiality and freshness not always guaranteed	- Rogue BS - Interleaving attacks - Denial of access	- Add the BSID in he last message - Use nonces for sequentiality - Use timestamps for freshness
		SA-TEK hree-way handshake	SA-TEK challenge message not imestamped	Replay attacks	Add timestamps
	Management Messages	Network entry procedure	RNG-REQ and RNG-RSP not encrypted neither au henticated	- Eavesdropping attacks - DoS attacks -Water torture attacks	Add HMAC/CMAC digest unauthenticated messages
			Using the Mesh mode, the network descriptor message is not encrypted neither authenticated	- Sinkhole attacks - Sybil attacks	
		Neighbor BS mapping	MOB_NBR-ADV message not authenticated	- Rogue BS attacks - Denial of access	
		Transmission power management	FPC message not authenticated	- Water torture attacks - DoS attacks	
		Burst profile management	DBPC-REQ message not authenticated	- Wrong encoding scheme - Dos Attacks	
		AK key lifetime management	AUTH-INVALID message not authen icated	Denial of access	
		Anchor BS selection in handover operations	MOB-ASC_RSP not au henticated	- Rogue BS attacks - DoS attacks	
		Reset of not responding MSs	BS forced to send a RES-CMD message to MSs	- Denial of access	Use a key agreement protocol in the ini ial

			which work correctly	- DoS attacks	ranging procedure (DH)
	Multicast and Broadcast Services	GTEK multicast group key sharing	- GTEK keys are symmetrically used in the same multicast group - GTEK keys are updated and encrypted using a shared GKEK key	- Rogue BS attacks - DoS attacks	- Distribute the GTEK key separately using the shared KEK key. - BS must sign key update messages - Group-based key distribution algorithms
		MBRA protocol	- GTEK and GKEK keys lifetime not optimized	Backward/forward secrecy attacks	- Optimize GTEK/GKEK key lifetime - Use a hierarchy of sub-GKEKs
Network Layer	DHCP Protocol	DHCP Proxy	DHCP_DISCOVER not authenticated	IP@ impersonation	Use ACCESS_ACCEPT to deliver IP@
		DHCP Relay	DHCP_DISCOVER and DHCP_OFFER not au henticated	- DNS Spoofing - MITM attacks	Use au h. sub-option in DHCP + AAA attributes
	Mobile IP Protocol	MIP registration procedure	MIP_RRQ and MIP_RRP not authenticated PMIP manager forwards the MIP registra ion	- Denial of access - DoS attacks	Use the AEE (Authentication Enabling Extension) in MIP_RRQ/MIP_RRP
	Handover Schemes	Handover op imization bits	Re-authen ica ion and/or TEK three-way handshake are not required in the [01] and [11] bit configuration	- Backward and forward secrecy attacks - DoS attacks	Use he [00] bit configuration (Re-authentication and TEK handshake are required)

Table 2: AeroMACS security Taxonomy

4 A QUANTITATIVE NETWORK RISK ASSESSMENT MODEL BASED ON RISK PROPAGATION APPLIED TO AEROMACS NETWORK

In this part of the document, we apply to the AeroMACS infrastructure a new approach for network security assessment that measures quantitatively the network risk level based on critical aspects such as the impact of a successful attack on a node and the risk propagation of that attack within the network. This method helps in analyzing easily different scenarios of implementation in order to derive guidances for manufacturers and AeroMACS future operators.

The proposed evaluation approach helps in comparing security policies in order to define an optimal policy and thus improve the global security of the network. This approach can also help administrators to estimate the effect of any topological change in the network architecture (*e.g.* adding or deleting a node) on the security of the global system. All the parameters involved in the network risk measurement are explained and quantified: threat l kelihood, risk impact (*i.e.* cost of damages), individual network risk (*i.e.* specific to a single node), and the total risk induced by the interconnection between the network components. The proposed security assessment framework is original as most existing methodologies and tools only identify vulnerabilities and evaluate risk in a given network node by node. They do not consider the relations between nodes. The results obtained are usually quite specific and it is difficult to apply the findings to others networks or fields of application.

Note: The risk assessment methodology has been conducted on AeroMACS using real statistics and vulnerability data about WiMAX implementation (and other network nodes) from the National Vulnerability Database (NVD) published by the National Institute of Standards and Technology (NIST)[5]. The NVD provides information about vulnerabilities such as type, severity class and score, extended description, products and versions affected, etc. To be more specific, it uses the NVD Common Vulnerability Scoring System (CVSS)[6] (which is basically a database containing scores for each vulnerability) combined with the well-known network vulnerability scanning tool NESSUS[7] to build the assessment security framework. For further information on CVSS scores, refer to annex A.

This part of the document is structured as follows:

- First, a survey of existing risk assessment methodologies is provided. Their advantages and drawbacks are discussed in order to introduce the new methodology;
- Secondly, a detailed description of the proposed methodology is provided;
- Finally, the methodology is applied to several AeroMACS implementation scenarios in order to derive recommendations for manufacturers and ASN/CSN operators to secure the AeroMACS network.

[5] http://web nvd nist gov/view/vuln/search

[6] http://www first org/cvss

[7] http://www nessus org/

4.1 AN ALTERNATIVE RISK ASSESSMENT METHODOLOGY

4.1.1 RISK MANAGEMENT STANDARDS AND METHODS

Risk assessment process is a mandatory step in traditional risk management methods such as CCTA Risk Analysis and Management Method (CRAMM), Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)[1] or “Expression des Besoins et Identification des Objectifs de Sécurité” (EBIOS)[2]. These risk management tools are compliant with information security standards proposed by the International Organization for Standardization (ISO)[5]. ISO defined lots of standards related to information security such as ISO 15408 (also known as Common Criteria - CC) [3] which is basically a certification framework able to evaluate information security. Based on this standard, ISO 27001 has been introduced in 2005 [4] to provide guidance for designing an information security management system. In this global process of security management, the risk assessment process has been specified with ISO 27005 [5] but it still relies on qualitative risk evaluation.

Those standards and methods are related to information security in general and thus, are perfectly well suited to a specific context such as aeronautical area. This is one reason why Aeronautical Radio Incorporated (ARINC) introduced in 2005 [6] a risk management framework for aeronautical information and network security (*i.e.* document entitled ARINC 811). ARINC 811 provides additional guidance to deal with physical and operational constraints of aeronautical hardware and software assets relative to companies, airports, aircraft or flights.

The risk assessment approaches used in the risk management methods mentioned above are mostly static and evaluate damage produced by threats qualitatively, making results somehow subjective. In the next subsection, are presented the advantages of quantitative over qualitative approaches, and then the most significant models that use formal representations in network security risk assessment are presented.

4.1.2 QUANTITATIVE AND QUALITATIVE RISK ASSESSMENT APPROACHES

As it has been underlined before, risk assessment can be performed either qualitatively or quantitatively. Typically, qualitative risk techniques lack of theoretical bases. These models rely on security specialist’s expertise and, usually questionnaires are used to gather their opinions like in [7]. This is an essential issue as security expertise costs money to companies. Also, data collection process is considered complex, as it requires much time and effort. Finally, the qualitative results could not be substantially evaluated because of their subjective nature. Indeed, these measures are mostly based on a ranking scale: it is then poss ble to compare two security levels (for instance, between high and low) but impossible to estimate the distance between these measures (for instance, between two security levels ranked as high).

Quantitative risk assessment allows a more granular analysis of risk events compared to qualitative techniques. In fact, a plethora of parameters involved in the risk assessment process can be used and designed in many ways thanks to mathematical and theoretical models. The results are accurate and can be understood easily by administrators and engineers in order to enhance the security of the network. Automated tools are developed for this purpose and present the advantage of accelerating the assessment process and avoiding some computation errors. These errors may occur with qualitative techniques, which are usually performed manually.

Quantitative risk assessment techniques can be used either for preventive risk analysis, or reactive risk analysis depending on the context of the study. Preventive risk analyses often rely on the Annual Loss Expectancy (ALE)[8]. ALE is the expected monetary loss that can be expected for an asset due to a risk over one year period. As ALE is an important feature that can be used directly in cost-benefit analysis, quantitative risk assessment methods are considered more relevant than qualitative ones (note that ALE is out of scope of this report). Reactive risk analysis is generally conducted to define a set of countermeasures when an alert corresponding to an attack is triggered by a monitoring system, using, for instance, an Intruder Detection System (IDS). For this purpose, several decision criteria are used and modeled in various ways. The most prominent models are detection and reaction cost models (number of security countermeasures to deploy, percentage of intrusion into the supervised network, monetary or processing resources required to face an attack, etc), attack models (scenarios-based or tree-based graphs, etc), threat impact models (impact distribution laws, impact progression over the network, etc), and so on. Some examples of such mathematical and formal models can be found respectively in [9], [10] and [11].

4.1.3 NETWORK RISK PROPAGATION CONCEPT

When an attack occurs on a network node, it is highly likely that the intruder will try to attack the interconnected nodes when this is allowed by the network topology. The attacker would be able to do so if there are some system assets that could help him to break into a connected node. These assets could be applications, services (intruded on an associated port), user logins (*e.g.* root privilege access), or database access accounts. Furthermore, the dependency between these system facilities implies some kind of transitivity in the network risk propagation process: if a node *i* has some vulnerabilities, it might transmit its correlative risk to a connected node *j*. This risk will propagate to the different nodes connected with node *j*.

4.1.4 RELATED WORK

There are lots of studies about network and information security risk quantification. [12] gives out hierarchical threat assessment models for network security and quantify the information system security parameters. [13] prompts a service-based risk quantitative calculation method (SRQC) for Next Generation Networks (NGN), which includes a layered risk assessment model (quantification of assets, vulnerabilities, threats and risk). [14] proposed a three-dimensional security architecture model in NGN and focused on threat, vulnerability, stability and survivability parameters. [15] used a multi-criteria decision making algorithm to weight the security parameters used in the risk evaluation process. However, authors asked some security experts to give values to these weights, which make the model somehow subjective and unsuitable with others environments. [16] proposed a security metric framework combined with NVD databases to quantify the most relevant security risk parameters used in the assessment procedure. The authors made a considerable effort to model some specific parameters such as vulnerabilities, but they did not cover most of network security attributes. [17] and [18] proposed some evaluation methods by formalizing and modeling attacks to find out how intruders proceed, and illustrate all the likely paths from origins to targets.

[19] and [20] proposed two risk assessment approaches for network information systems based on node correlation. These are two of the few studies that take into account node dependency and risk propagation concepts. However, all the risk parameters are not well-defined in both papers: there are no indications on how some of these parameters are computed, which lead to some misunderstanding of the global assessment process. For instance, it has been told that likelihood is estimated on the analysis of attack frequency and complexity without any additional details. Also, authors said that attack impacts are evaluated based on analysis of severity results. They chose to let users decide about the ranking of these baseline risk parameters, which is totally subjective and incompatible with a quantitative risk assessment methodology. Also, as both studies emphasize their efforts on network risk assessment, rough assumptions have been made for host risk assessments (i.e. individual risk for each node)..

4.2 PRESENTATION OF THE QUANTITATIVE NETWORK RISK ASSESSMENT MODEL BASED ON RISK PROPAGATION

4.2.1 TERMINOLOGY

Table 3 shows the nomenclature used in the quantitative network risk assessment model:

Notation	Description
ɹ ,	Function value of a node *i*
ʅ ,	Class value of a node *i*
\ ,	Total value of a node *i*
ɹ pu! ,	Individual risk evaluated on node *i*
ɹ oɹd ,	Propagated risk evaluated on node *i*
ɹ ,	Total risk evaluated on node *i*
ɹ ʇəu	Total network risk
,	Total number of nodes in the network
ı ,	Number of nodes connected with a node *i*
' ,	Total number of vulnerabilities detected on node *i*
ɹ ,)ı(	Likelihood of occurrence of vulnerability *t* on node *i*
ı ,)ı(	Impact induced by a vulnerability *t* on node *i*
ɹ ,)ı(	Motivation of an attacker to exploit a threat *t*
,)ı(	Technical difficulty level to exploit vulnerability *t* on node *i*
ɂ ,	Number of security mechanisms used to protect a node *i*
$\sum$	Mathematical sum
ɿ ,	Number of information required to exploit vulnerability *t*
ı ,)ı ‘ ʃ(	Propagated impact of *t* from node *i* to node *j*
ɹ ɩ,	Number of total flows between two correlated nodes *i* and *j*
ı ɩ,	Number of detected flows between two correlated nodes *i* and *j*
ɹ ,)ı ‘ ʃ(	Propagation likelihood of *t* from node *i* to node *j*
ʅ !	Scalar vector

	Security features provided for node *i*
	Security requirements related to a security service *s*

Table 3: Terminology

4.2.2 RISK PARAMETERS

In this section, we explain how we compute every involved network parameters in the risk assessment process. The first step is to estimate the network risk for each node. As a node is connected to other nodes in the network, we evaluate the total risk for a given node *i* as the product between node value and the individual plus propagated risk:

(1)

[illegible]

Considering that network nodes have not the same functionalities, we can assume their importance degree (or value *Value$_i$*) in the network may vary. For instance, it is clear that a gateway or a firewall is more important, from a security point of view, than a simple host or a user terminal: for instance, the function value of a firewall (1.0) is greater than the function value of a terminal (0.1). For the aeronautical context, we have considered, besides the node functionality (*FunctionValue$_i$* in (2)), the traffic generated by this node. In fact, there are mainly four traffic classes in the aeronautical network: the Air Traffic Services (ATS) class for communications between pilot and tower control, the Aeronautical Operational Communications (AOC) class which is relevant to airline information (flight plans for instance), the New Generation AOC class (AOC NG) represented mainly by new services such as telemedicine[10] and video surveillance[11], and the Aeronautical Passenger Communication (APC) class for passenger entertainment (e.g. broadband Internet access, IFE[12]). For safety and regularity of flight considerations, the following priority scale has been respected as required in [BLD10]: and respectively traffic class values are 1.0 > 0.7 > 0.4 > 0.1. Thus, the value of a node *i* is given by:

(2)

$$Value_i = n_i * FunctionValue_i * ClassValue_i$$

Besides function and class values, we have also considered the total number of connected nodes *n$_i$* to node *i*. Indeed, the total value *Value$_i$* increases when a node is logically connected to an important number of nodes in the network (for instance, an email server or Internet proxy). The matrix resulting from the combination of the function and class values is detailed in Table 4.

	Traffic Class Value			
Node (function value)	**ATS**	**AOC**	**AOC NG**	**APC**
	1.0	0.7	0.4	0.1
Firewall or Gateway (1.0)	1.0	0.7	0.4	0.1
Router (0.7)	0.7	0.49	0.28	0.07
Switch or Hub (0.5)	0.5	0.35	0.2	0.05

Server (0.3)	0.3	0.21	0.12	0.03
Terminal (0.1)	0.1	0.07	0.04	0.01

Table 4: Function and class values matrix for Aeronautical Network Nodes

Both functions and classes values have been ranged between 0.0 and 1.0. The function and class nodes values are the only parameters requiring a 'human in the loop' since there are no means to quantify them in practice. The second parameter considered in equation (1) is the individual risk, namely the host risk specific to a node. The following formula is used to compute the individual risk for a node *i:*

(3)

$$Risk_i^- = \sum_{t=0}^{T_i} P_t(i) * I_t(i)$$

For each node, the total number of vulnerabilities T_i and the estimated impact I_t relative to a specific vulnerability *t* (namely, the t^{th} threat identified on that node) are gathered using the NESSUS[8] vulnerability scanning tool. In practice, NESSUS provides a set of known vulnerabilities stored in the CVSS database. Among the output information, we retrieve the score (i.e. impact) associated to each vulnerability occurring on that node. These scores are ranged from 1 to 10. The number of vulnerabilities T_i is a simple addition on the existing vulnerability for that node.

The likelihood $P_t(i)$ represents the possibility that attacks associated with the vulnerability *t* are conducted. The likelihood of occurrence evaluation is driven by an existing threat analysis methodology [24] proposed by the European Telecommunications Standards Institute (ETSI). However, as the likelihood values are qualitative, we slightly modified this part of the methodology in order to quantify the involved parameters. Indeed, as described in [24], the evaluation of the likelihood is based on two factors: the technical difficulties that have to be resolved and the motivation for an attacker to carry out an attack.

The methodology associates three values to the likelihood function: (1) *unlikely*, if the motivation for conducting an attack is *low* (*e.g.* no financial interest or technical challenges) and there are *strong* technical difficulties to overcome (*e.g.* major unknowns to achieve the attack); (2) *possible*, if the motivation is *moderate* (*e.g.* reasonable financial gains) and the technical difficulties are *solvable* (*e.g.* information required to exploit the vulnerability are available); and (3) *likely*, if there is a *high* attacker motivation (*e.g.* inducing a denial of service on the network, important financial gains) and technical difficulties are almost *inexistent* (*e.g.* no security protection). In our algorithm, we made some modifications in the ETSI likelihood evaluation process to replace the qualitative values by quantitative values. First, the likelihood is computed using the motivation and technical difficulties values as shown in equation (4):

(4)

$$P_t(i) = \frac{Motivation_t(i)}{TechnicalDifficulty_t(i)}$$

[8] Note that any scanning tool providing the same features than NESSUS can be used.

In fact, we think that likelihood of occurrence of a vulnerability *t* increases when the motivation also increases; otherwise, the likelihood decreases when the technical difficulties that must be resolved increase. The motivation for an attacker to exploit a vulnerability *t* on a node *i* is:

(5)

$$Motivation_t(i) = Value_i * T_i$$

The equation (5) shows that the motivation increases when the node value is important and when the number of known vulnerabilities is high. Finally, technical difficulties get stronger when security features (*e.g.* Firewalls) are reinforced (*e.g.* increasing their number of enhancing the security policies) or the number of information required to exploit a vulnerability t is high:

(6)

$$TechnicalDifficulty_t(i) = S_i + B_t$$

Comment [m1]: Are Si and Bt informed in he CVSS tool?

Comment [m2]: How is it normalized.

Comment [m3]: Si is not defined in this section

Meaning that in order to exploit a vulnerability, some information must at least be available to conduct an attack. Indeed, we make the assumption that an attacker cannot do anything if a minimum of data is not available to start the attacking process (*e.g.* opened port IDs, user's logins, target addresses, etc). As the resulting probability value must be ranged between 0 and 1, both motivation and technical difficulties values have been normalized to 1. Finally, the last parameter of formula (1), namely the propagated risk, is evaluated as the following:

(7)

$$Risk_i^+ = \sum_{j=0}^{n_i} \sum_{t=0}^{T_j} P_t(i,j) * I_t(i,j)$$

The idea is quite the same as the one used in equation (3), the main difference is that the propagated likelihood and impact are induced by all the vulnerable nodes connected with node *i*. The propagation likelihood of vulnerability *t* from a node *j* to a node *i* is given by:

(8)

$$P_t(i,j) = P_t(j) * P(i,j)$$

In fact, the propagation likelihood depends on the likelihood of vulnerability *t* on the issuing node *j* and the likelihood of correlation *P(i,j)* between the two nodes, given by:

(9)

$$P(i,j) = \frac{f_{ij}}{F_{ij}}$$

The number of detected (relative to a service concerned by this vulnerability) and total data flows exchanged (which is basically an aggregation of all detected data flows) between two nodes *i* and *j* can be directly deduced using some network statistic tools l ke NETSTAT[9] or raw data from */proc/net/dev*. The propagated impact from a vulnerability *t* from node *j* to a node *i* is:

(10)

[9] http://linux-ip net/html/tools-netstat html

$$I_t(i,j) = Value_i * W_S^i * I_t(j)$$

The propagated impact depends on the affected node value, namely *Value*$_i$, the impact of *t* on the issuing node *j* (cf. CVSS database which provides vulnerability scores), and the targeted service *s*. The service can be either an ATS or AOC data-based service as defined in the COCR (*e.g.* Departure Clearance – DCL). is a scalar value deduced as the following :

(11)

$$W_S^i = SecurityFeatureIndicator_i * (SecurityObjectiveVector_S)^T$$

Where *SecurityFeatureIndicator*$_i$ is a binary indicator function that defines the security features provided by security mechanisms and countermeasures to protect all the services on the node *i*. For instance, if the data flows are only encrypted, the associated binary indicator function is [0 1 1]. It could seem abnormal to associate the zero binary value to express a "YES", but this is used in order to respect the impact function behavior (*cf.* equation (10)).

Indeed, the impact grows when less security features are available. Thus, mapping the one binary value to a "YES" is then inadequate. In this specific case, the more we have security features, the bigger would be the propagated impact, which would not be logical with the impact function we previously defined. The second part of the equation (11) is a 3-dimension vector containing the security objectives per service (the transpose of the vector is used here in order to obtain a scalar value result). *SecurityObjectiveVector*$_S$ is deduced from the COCR document where security objectives are expressed using a qualitative scale. In order to compute the network risk and get quantitative values, we suggest the following mapping:

Qualitative values	Quantitative values
None	0
Low	1
Medium	2
High	3
High-Severe	4
High-Catastrophic	5

Table 5: COCR Quantitative Value Mapping

For instance, for DCL service, the *SecurityObjectiveVector*$_{DCL}$ = [0 5 5] in as defined in the COCR.

Finally, we deduce the total risk as a sum of all the network risk relevant to each node on the network:

(12)

$$R_{net} = \sum_{i=0}^{N} Risk_i$$

Finally, since we defined all the parameters involved in the network risk computation process, we can then implement our risk assessment algorithm.

4.2.3 RISK ASSESSMENT PROCESS

In this section, we describe the 6 steps leading to the final network risk evaluation using our assessment approach:

Network Risk Assessment Algorithm (Pseudo-code)

```
//Step 0: initiation step
; //initiate a set of vulnerable nodes
//initiate a set of processed nodes
For each node i network Do{
    ; //initiate a set of the correlated nodes with node i
} End For


//Step 1: scan and identify vulnerable nodes
For each node i network Do{
    Run NESSUS client;//identify vulnerabilities
    If any vulnerability is detected Then{
        Add node i to V;
    }End If
    For each vulnerability t Do{
        Store t and associated CVSS score;
    }End For
}End For


//Step 2: compute individual risk for each identified vulnerable node
For each node i Do{
    Store correlated nodes with node i in ;
    For each vulnerability t Do{
    }End For
}End For

//Step 3: compute the propagated risk for nodes correlated with vulnerable nodes
While Do{
    For each node j Do{
        For each node i Do{
            For each vulnerability t Do{
                ;
                //s is the service targeted by t
                //update the vulnerability probability for the infected node
                If Then{
                    //update the probability of occurrence of vulnerability t
                }End If
            }End For
            If the node i and Then{
                Store node i in V; // this node is now infected and must be treated
            }End If
        }End For
        Copy node j to NVD and remove it from V; //this node has been processed
    }End For
}End While

//Step 4: compute the total risk for each node in the network
```

```
For each node i network Do{

}End For


//Step 5: compute the whole network risk level

For each node i network Do{

}End For
```

Note: In annex, an algorigram presents this risk assessment process.

4.3 APPLICATION TO AEROMACS NETWORK

4.3.1 TRAFFIC FLOW SPECIFICATION

Traffic flows are grouped according to the nature of the service and the affected network entities. In the following sections, a classification of the services extracted from COCR (ATC, AOC and NET) is performed. In addition, access network management flows are considered, according to WiMAX profile and NWG specifications.

For each service, a set of information is given in order to describe its features that can be used in risk analysis:

- **Security level:** a description of the needs in terms of confidentiality, integrity and/or availability according to COCRv2, or to a different hypothesis when stated specifically;
- **End to end:** an indication of the nodes that represent the communication ends of the flow (source and/or destination, depending on the flow directionality). It also indicates whether the service is unicast (one to one) or multicast/broadcast (one to many);
- **Direction:** an indication of the directionality of the flow. It can be unidirectional, originated in Ground or Air domains, or bidirectional;
- **Traffic volume:** the volume of traffic generated by the aggregated instances of services of this class. It considers that every service of the class is instantiated once. It is calculated as sum(#messages per dialog * message size in Bytes * 8);
- **Traffic pattern:** an indication on whether the traffic is periodic (messages are sent in a deterministic frequency) or bursty (non predictable pattern of message transmission). Periodic services are assumed to be executed during the whole simulation time (departure + arrival = 65 minutes according to COCRv2).

4.3.2 ATS

Air Traffic Service (ATS) are executed by Air Traffic Management Systems and Aircraft. They may be instantiated in any of the operational APT areas (RAMP, GROUND or TOWER) at both arrival and departure phases. They support safety-critical traffic control operations and clearances.

For the purpose of the security analysis, the different traffic flows identified can be classified as follow:

- **ATS addressed:** represents the majority of ATS that are addressed between Air traffic controller and Aircraft and generate a bidirectional message exchange used for aircraft control and monitoring on the surface.
- **ATC SURV:** refers to the specific ATC surveillance service. This service, when active, generates a message periodically from the aircraft that informs the ground system on the latest surveillance events.
- **ATS multicast:** represents a set of ATS that instantiate between the Air traffic controller and a group of subscribers. These services are used to send reports to the aircrafts, but the services are bidirectional as they include an ACK message from the aircraft.

Service name	Security level	End to end	Direction	Traffic volume (bits)	Traffic pattern
ATS addressed	Confidentiality (low) Integrity (high-severe) Availability (high-severe)	ATC server ATC client	G<->A	99592 (FL) 86848 (RL)	Bursty
ATC SURV	Confidentiality (low) Integrity (high-severe) Availability (medium)	ATC server ATC client	G<-A	530400 (RL)	Periodic (2 s/msg)
ATS multicast	Integrity (high-severe) Availability (medium)	ATC server Group (ATC client)	G<->A	75336 (FL) 14760 (RL)	Bursty

Table 6: Specification of ATS traffic flows

4.3.3 AOC

Air Operation Control (AOC) services are executed by Airline Controller and Aircraft. Most of them are instantiated while the aircraft is in the RAMP area, but some of them can also be present in the phase of the flights (while taxiing, or in TMA and En-route). They support monitoring and operation services that provide aircraft maintenance and boarding actions.

The different traffic flows identified are the following:

- **A/C report**: represents the services that are instantiated in Aircraft and generate reports and logs to the ground AOC (CABINLOG, FLTLOG, FLTJOURNAL, LOADDOC). The nature of these services is informative, and so they need to guarantee a certain level of confidentiality.
- **A/C monitoring**: represents the services that are instantiated in Aircraft and generate monitoring or operation messages that provide the ground AOC with quick information on the aircraft status in order to undertake the appropriate actions (DOOR, HANDLING, PREFLT-INS, AUTOLAND-REG). These services affect safety and regularity of flight, and thus integrity and availability are critical aspects. These services are not defined by COCR, but, due to their direct effect on traffic control, these services are granted the same security needs as addressed ATC services.

- **Controller notification**: refers to the services instantiated in the ground AOC that send an order or notification to the aircraft (UPLIB, NOTAM, NOTOC, AIRWORTH). These can combine reports and air operation data.
- **AOC bidirectional**: refers to the majority of services executed between Airlines Operation Centre and aircraft or handling vehicle and manage most of the AOC flight operations in surface (AOCDLL, FLTPLAN, LOADSHT, WXGRAPH, WXTEXT, EFF, FLOWCON, SWCONF, and TAKEOF-CALC).
- **FOQA**: the specific Flight Operations Quality Assurance is a method for gathering flight data and providing to the ground AOC for its treatment, analysis and monitoring. The information sent by the aircraft after a flight is variable and generally of considerable size. As FOQA is not an implemented service yet, best information on security levels required can be extracted from the COCR, in which there is an insistence on preserving Confidentiality and Integrity over the service.
- **ECHARTS**: the specific Electronic Charts Update is a service by which ground AOC sends the aircraft the updated Navigation Maps after a certain number of flights. Charts have a big size and are thus not generally updated in a single turn-around phase. There is no security information for this future service yet, so the security levels from FOQA are translated here since both services transmit flight data for the crew or operators.
- **Technical log updates**: includes the TECHLOG and ACLOG services that are used to request the aircraft to check the status of the aircraft technical log and update it in the maintenance base if necessary. These services must be done quickly and reliably since remedial actions may need to be taken according to the log information.
- **WXRT**: The specific Real-time Weather Reports for Met Office is used by the aircraft to periodically derive the environment on which it is operating, and send it to ground AOC.

Service name	Security level	End to end	Direction	Traffic volume (bits)	Traffic pattern
A/C report	Confidentiality (medium) Integrity (low) Availability (low)	AOC server AOC client	G<-A	160042648 (RL)	Bursty
A/C monitoring	Confidentiality (low) Integrity (high-severe) Availability (high-severe)	AOC server AOC client	G<-A	29600 (RL)	Bursty
Controller notification	Confidentiality (medium) Integrity (high-severe)	AOC server AOC client	G->A	320120000 (FL)	Bursty

	Availability (high-severe)				
AOC bidirectional	Confidentiality (medium) Integrity (high-severe) Availability (high)	AOC server AOC client or AOC client (vehicle)	G<->A	241340256 (FL) 48251680 (RL)	Bursty
FOQA	Confidentiality (high) Integrity (high)	AOC server AOC client	G<-A	800000000 (RL)	Bursty
ECHARTS	Confidentiality (high) Integrity (high)	AOC server AOC client	G->A	1200000000 (FL)	Bursty
Technical log updates	Confidentiality (medium) Integrity (medium) Availability (medium)	AOC server AOC client	G<->A	32704 (FL) 643816 (RL)	Bursty
WXRT	Integrity (medium) Availability (medium)	AOC server AOC client	G<-A	780E06 (RL)	Periodic (0.6 s/msg)

Table 7: Specifications of AOC traffic flows

4.3.4 VEHICULAR SERVICES

This set of services is executed between a controller and an assisting vehicle operating on the airport surface.

- **Airport operation:** refers to informative services between airport server or supervisor, and vehicle in the airport surface. They refer to applications strictly in the airport domain (V-PLAN, ADLI, DMSG), and are absolutely not considered in the COCR as security critical to provide safety of life or regularity of flight. Thus, no clear security level can be issued for them.
- **Airport Operation Centers Clearance (AOPCL) service** that is used to authorize the vehicle to enter areas controlled by ATC (e.g. runway).

AOPCL	Confidentiality (low) Integrity (high-severe) Availability (high-severe)	ATC server AP client (vehicle)	G<->A	1488 (FL) 1488 (RL)	Bursty

Airport operation		AP server AP client (vehicle)	G<->A	16000 (FL) 16000 (RL)	Bursty

Table 8: Specifications of Vehicular Service Traffic Flows

4.3.5 MANAGEMENT

Management traffic flows include all the non-operational message flows that keep signalization for network functions. Unlike ATS and AOC services, there is no COCR defined security level for these traffic flows.

The following flows have been identified:

- NETCONN/NETKEEP: the services that guarantee network connection and keep-alive are instantiated once per pair of aircraft and ATC/AOC server. They make service flow establishment and maintenance possible.
- Authentication protocol: during the AeroMACS registration phase, every MS proceeds to an authentication procedure. Here, an EAP method is assumed, which is established between the MS and the AAA server. Although authentication delays depend on the network performance, a conservative figure of 5 seconds authentication time is proposed. In order to calculate the data volume, we assume RADIUS messaging over EAP-TLS exchange, with a message size equal to the maximum RADIUS packet (4096 Bytes).
- DHCP protocol: if a DHCP architecture is present in the network, the AeroMACS MS needs to perform IP configuration during network entry prior to registration. A conservative figure of 5 seconds DHCP time is proposed. We assume a normal DHCP operation (discover – offer – request – ack) with 342 Byte messages.
- Handover signalization: in the frequent situation that a subscriber changes its anchor BS, due to terminal movement or channel degradation, a handover process is necessary. Such process is managed by the ASN-GW and signaled in the air interface between the MS and the two affected BSs (serving and target). We assume an ASN-anchored mobility procedure encapsulated in R6 packets with explicit source and destination TLV (176 Bytes) as message size. This information is exchanged in the non-secured basic or primary CID. In order to calculate the total data volume exchanged during a turn-around time, we assume a normal operation in which 3 handovers on average are performed.
- MAC signalization: represents all the message exchange in the air interface level that affect the link management between a given MS and its anchor BS (Power control, Burst profile configuration, etc). This information is exchanged in the non-secured basic or primary CID. A 2-way message exchange with 10 Bytes message on average is assumed.

Service name	Security level	End to end	Direction	Traffic volume (bits)	Traffic pattern
NETCONN / NETKEEP		ATC/AOC server ATC/AOC client	G<->A	401 (FL) 389 (RL)	Bursty
Authentication protocol		AAA server	G<->A	98304 (FL)	Bursty

		MS		65536 (RL)	
DHCP protocol		DHCP server MS	G<->A	5472 (FL) 5472 (RL)	Bursty
Handover signalization		ASN-GW 2 BS MS	G<->A	8448 (FL) 8448 (RL)	Bursty
MAC signalization		BS MS	G<->A	62400000 (FL) 62400000 (RL)	Periodic (0.005s/mg)

Table 9: Specifications of Management Traffic flows

4.3.6 Characterization of data volume exchanged per pair of nodes

The table below displays the total volume exchanged between two contiguous nodes of the topology. The size of the volume is given in bits, on a per service manner. A total simulation time of 46.5 (DEP) + 18.5 (ARR) minutes is assumed as chosen for phase 2 High Density airport is used.

Service \ pair	AAA – ASN gateway		DHCP server – ASN gateway		ATC server – ASN gateway		AOC server – ASN gateway		AP server – ASN gateway	
Direction	→	←	→	←	→	←	→	←	→	←
ATS addr	-	-	-	-	99592	86848	-	-	-	
ATC SURV	-	-	-	-	-	530400	-	-	-	-
ATS multicast	-	-	-	-	75336	14760	-	-	-	-
AOC report	-	-	-	-	-	-	-	160042648	-	-
AOC monitor	-	-	-	-	-	-	-	29600	-	-
C. notification	-	-	-	-	-	-	320120000	-	-	-
AOC bidirect.	-	-	-	-	-	-	241340256	48251680	-	-
FOQA	-	-	-	-	-	-	-	800E06	-	-
ECHARTS	-	-	-	-	-	-	1200E06	-	-	-
Technical log	-	-	-	-	-	-	32704	643816	-	-
WXRT	-	-	-	-	-	-	-	780E06	-	-
AP operation	-	-	-	-	-	-	-	-	16000	16000
AOPCL					1488	1488				
NET	-	-	-	-	-	-	401	389	-	-

Authentication	98304	65536	-	-	-	-	-	-	-	-
DHCP protocol	-	-	5472	5472	-	-	-	-	-	-
Handover	-	-	-	-	-	-	-	-	-	-
MAC signal	-	-	-	-	-	-	-	-	-	-
TOTAL	**98304**	**65536**	**5472**	**5472**	**175E03**	**632E03**	**1760E06**	**1790E06**	**16000**	**16000**

Table 10: Amount of Data Exchanged between Nodes Pair per Service - Part 1

Service \ pair	ASN gateway – BS		BS – MS		MS – AP client (vehicle)		MS – ACD/AISD firewall		ACD firewall – ACD ATC client	
Direction	→	←	→	←	→	←	→	←	→	←
ATS addr	99592	86848	99592	86848	-	-	86848	99592	99592	86848
ATC SURV	-	530400	-	530400	-	-	530400	-	-	530400
ATS multicast	75336	14760	75336	14760	-	-	14760	75336	75336	14760
AOC report	-	160042648	-	160042648	-	-	160042648	-	-	-
AOC monitor	-	29600	-	29600	-	-	29600	-	-	-
C. notification	320120000	-	320120000	-	-	-	-	320120000	-	-
AOC bidirect.	241340256	48251680	241340256	48251680	-	-	48251680	241340256	-	-
FOQA	-	800E06	-	800E06	-	-	800E06	-	-	-
ECHARTS	1200E06	-	1200E06	-	-	-	-	1200E06	-	-

Technical log	32704	643816	32704	643816	-	-	643816	32704	-	-
WXRT	-	780E06	-	780E06	-	-	780E06	-	-	-
AP operation	16000	16000	16000	16000	16000	16000	-	-	-	-
AOPCL	1488	1488	1488	1488	1488	1488	-	-	-	-
NET	401	389	401	389	-	-	389	401	-	-
Authentication	98304	65536	98304	65536	-	-	-	-	-	-
DHCP protocol	5472	5472	5472	5472	-	-	-	-	-	-
Handover	8448	8448	8448	8448	-	-	-	-	-	-
MAC signal	-	-	62400000	62400000	-	-	-	-	-	-
TOTAL	**1778E06**	**1807E06**	**1843E06**	**1866E06**	**17488**	**17488**	**1790E06**	**1760E06**	**632E03**	**175E03**

Table 11: Amount of Data Exchanged Between Nodes Pair per Service - Part 2

Service \ pair	ACD firewall – ACD AOC client		AISD firewall – AISD AOC client		AISD firewall – ACD firewall	
Direction	→	←	→	←	→	←
ATS addr	-	-	-	-	99592	86848
ATC SURV	-	-	-	-	-	530400
ATS multicast	-	-	-	-	75336	14760
AOC report	160042648	-	160042648	-	-	-
AOC monitor	29600	-	29600	-	-	-
C. notification	-	320120000	-	320120000	-	-
AOC bidirect.	48251680	241340256	48251680	241340256	-	-
FOQA	800E06	-	800E06	-	-	-
ECHARTS	-	1200E06	-	1200E06	-	-
Technical log	643816	32704	643816	32704	-	-
WXRT	780E06	-	780E06	-	-	-
AP operation	-	-	-	-	-	-
AOPCL	-	-	-	-	-	-
NET	389	401	389	401	-	-
Authen ication	-	-	-	-	-	-
DHCP protocol	-	-	-	-	-	-
Handover	-	-	-	-	-	-
MAC signal	-	-	-	-	-	-
TOTAL	**1790E06**	**1760E06**	**1790E06**	**1760E06**	**632E03**	**175E03**

Table 12 : Amount of Data Exchanged Between Nodes Pair per Service - Part 3

4.3.7 NODE INTERCONNEXION MATRIX

The table below depicts the total amount of data exchanged between every pair of nodes in the topology.

Tx / Rx	AAA	DHCP server	ATC server	AOC server	AP server	ASN gateway	BS	MS	AP client	ACD firewall	AISD firewall	ACD ATC client	ACD AOC client	AISD AOC client
AAA	-	-	-	-		98304	-	-	-	-	-	-	-	-
DHCP server		-				5472								
ATC server			-			175E03								
AOC server				-		1760E06								
AP server					-	16000								
ASN gateway	65536	5472	632E03	1790E06	16000	-	1778E06							
BS						1807E06	-	1843E06						
MS							1866E06	-	17488	1790E06	1790E06			
AP client								17488	-					
ACD[10] firewall								1760E06		-	175E03	632E03	1790E06	
AISD firewall								1760E06		632E03	-			1790E06
ACD ATC cli										175E03		-		

[10] ACD, AISD are airborne domains according to ARINC 664. More details can be found in section 7.4.1.1.1.2.2.1

ACD AOC cli										1760E06			-	
AISD AOC cli											1760E06			-

Table 13: Total Amount of Data Exchanged Between Nodes

4.4 RISK ANALYSIS SCENARIOS

In this section, different risk analysis scenarios are presented:

- Section 4.4.1: Isolated AeroMACS scenario with operational server vulnerabilities. Operational servers are non-COTS servers, designed for operational services (mainly ATC and AOC services). Isolated means that the basic topology assumes the existence of a standalone service network supported by an AeroMACS access network in the airport. Consequently, all the services are provided by components inside the AeroMACS network (AAA, DHCP, and application servers) and placed within the airport backbone;
- Section 4.4.2.1: Isolated AeroMACS scenario without operational server vulnerabilities. This is the same scenario as the one above except that vulnerabilities related to operational servers are not considered;
- Section 4.4.2.2: Isolated AeroMACS scenario without operational server vulnerabilities using Two ASN Gateways. In this scenario, the results of previous simulations are retained and 2 AeroMACS gateways are deployed in the ASN instead of one;
- Section 4.4.3: End-to-End AeroMACS scenario. Finally, the overall architecture is considered, including non-AeroMACS devices such as firewalls and home agents.

At the end of this section, a comparison is made between all the results.

4.4.1 ISOLATED AEROMACS SCENARIO WITH OPERATIONAL SERVER VULNERABILITIES

4.4.1.1 NETWORK TOPOLOGY

Figure 9 depicts the isolated AeroMACS network topology, three main portions can be identified, namely the AeroMACS ASN, the AeroMACS Core Service Network (CSN), and the mobile stations (aircraft or surface vehicles). This basic topology assumes the existence of a standalone service network supported by an AeroMACS access network in the airport. Consequently, all the services are provided by components inside the airport network (AAA, DHCP and application servers) and placed within the airport backbone.

The AeroMACS (additionally to the AAA server) segment is the only system supporting security features and the AAA server will be directly reachable through a dedicated gateway between the AeroMACS network and the others Airport networks. The APC server of the Figure 9 refers to the AirPort Communications server (and not to the Airline Passenger Communication Server as it is the case in other documents).

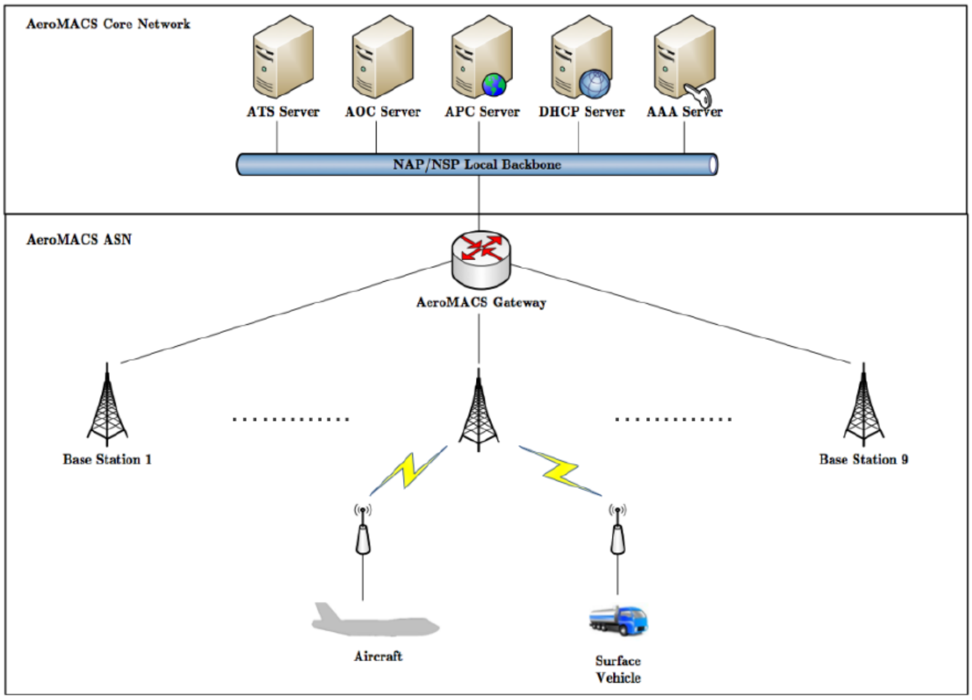


Figure 9: AeroMACS Network Topology : Extended Isolated Scenario

4.4.1.1.1 NODE SPECIFICATION

In this section, a description of the different nodes identified in the topology is given from a point of view of security. That is, the security measures that can be implemented are given per node. If there are options, these will be specified in a later stage when defining the scenarios. The nodes can be split up in three sections according to the section of the topology they are part of:

- AeroMACS ASN: BS, MS, ASN-GW. This is the focus of the study as it makes reference to the logical devices used for AeroMACS radio communication that support ATC/AOC services.
- Airborne network: the number of nodes and connections that are part of the A/C communications infrastructure. This part is relevant to aircraft.
- Ground network: the set of devices and connections that compose the airport network, extensible to the WAN connectivity. The ground network includes the AeroMACS gateways, the AeroMACS base stations, and the surface vehicles.

4.4.1.1.1.1 AEROMACS GROUND INFRASTRUCTURE

4.4.1.1.1.1.1 BASE STATION

4.4.1.1.1.1.1.1 NODE DEFINITION

The Base Station (BS) manages the radio link with Mobile Stations (MS) in the coverage area of the Access Service Network (ASN). It controls and assists all the procedures at local level to ensure link connectivity, service flow creation and signal quality. It relays the data path from the user side to the network, together with the related security methods. It manages security at local level and relays to the authenticator in the network.

4.4.1.1.1.1.1.2 SECURITY FEATURES

Regarding RF protection, AeroMACS uses inherently OFDM and subcarrier permutation schemes in order to provide frequency diversity. It also provides an adaptive modulation/coding and power control mechanism to improve the link quality. However, no standard Frequency Hopping (FH) or Spread Spectrum (SS) techniques are available. Also, Dynamic Frequency Selection (DFS, defined in ITU-R Recommendation M.1652) is at this moment not eligible for AeroMACS, since this technique switches the system off and changes channel in order to avoid interference from a license-exempt radio to critical application radars. This is not the case in AeroMACS since it is a safety-critical system and a cell cannot be switched off (this is the consequence to be avoided).

The BS manages the authentication and assists authorization of the subscriber credentials. During authentication process, PKMv2 key exchange and authorization is used. This algorithm is done bilaterally, so BS-MS authentication is mutual. There are two poss ble methods:

- If RSA based on X.509 certificate (PKI) is used, it applies only to the air interface between MS and BS;
- If EAP is used for PKMv2, it is an end-to-end security protocol, the endpoints being the BS and the MS, where the BS acts as authentication relay and key receiver/generator.

Private AKs are generated in both BS and MS from shared pre-PAK[11] or MSK and MS MAC address. In the process of key generation, function DOT16KDF that employs CMAC algorithm is used in order to guarantee the cryptographic independence of AK at every MS. Once AK is generated, a pair of TEKs is generated per BS-MS pair. These TEK are periodically refreshed (according to an implementation-dependent timer). Optionally multicast group keys can be supported.

Algorithms to encrypt data and TEK are negotiated during the PKMv2 phase. A limited combination of cryptographic solutions is allowed, and currently only one supported by WiMAX: CCM-Mode 128-bit AES data encryption, CCM-Mode (CMAC) data authentication, and AES Key Wrap with 128-bit key for TEK encryption.

Basic and primary connections, which carry management messages, do not cipher, nor authenticate messages. Transport connections can be handled independently and be assigned security associations (SA). SA associates key material and connection, *i.e.* every service flow is mapped to a SA if it supports security. A BS can share a SA with one MSs (or several for multicast connections), and identifier (SAID) is unique within every BS, pairs being represented by {MS MAC address, SAID}. SA information includes cryptographic suite, current used TEK, KEK, PN and associated lifetimes. SAID is updated in the BS via the backbone during handover.

At authentication, every MS establishes a primary SA with the BS. The rest of SAs are static as they are provisioned by the BS. The BS ensures that every MS has only information on the SAs authorized for them. If a pair BS/MS has no authorization policy, there is no related SA.

Service admission control is performed on a per-subscr ber basis. There is a Service Flow Manager (SFM) function in the BS that admits/rejects new service flows depending on radio occupation of the cell. It is also SFM role to forward to the ASN-GW the information on the user profile in order to perform a second decision level depending on user permissions.

4.4.1.1.1.1.2 AEROMACS ASN GATEWAY

4.4.1.1.1.1.2.1 NODE DEFINITION

The ASN Gateway (ASN-GW) performs routing or bridging function and relays the data path. It also aggregates the control functions that are paired with corresponding functions instantiated by MSs and BSs, plus resident functions in the network. Every BS is associated with one default ASN-GW.

[11] Pre-PAK is a random Pre-Primary Authentication Key used to generate the actual authentication AK key.

4.4.1.1.1.1.2.2 SECURITY FEATURES

The ASN-GW does not have a physical air interface. Its reference points involve an IP/Ethernet interface to the network, and an unsecured GRE protocol interface with the associated BSs.

ASN-GW acts as authenticator for every MS, i.e. it is the AAA client and relays EAP protocol to AAA server. If RSA authentication is performed, ASN-GW does not play any role in it. ASN-GW as AAA client and server use RADIUS or Diameter protocol to support EAP for device/user authentication, and service authorization.

In the PKMv2 process, the ASN-GW is in charge of distributing the shared keys among the BSs. No key generation is performed in ASN-GW.

Service admission control is performed on a per-subscriber basis. Depending on the QoS profile of a given registered MS in the registration server (AAA), there is a Service Flow Authorization (SFA) function in the ASN-GW that checks the QoS policy of the users at service flow initiation request. User policies are stored in AAA server and loaded in SFA when necessary.

4.4.1.1.1.1.3 GROUND NETWORK BEYOND AEROMACS NODES

4.4.1.1.1.1.3.1 NODE DEFINITION

The ground network allows the end-to-end connection of the AeroMACS ASN to the service provider network, and is composed by Ethernet IP routers, AAA server, DHCP server, Mobile IP related nodes and firewall.

4.4.1.1.1.1.3.2 SECURITY FEATURES

Interconnection ground network cannot be easily characterized as is fully out of the scope of AeroMACS. It is up to every airport operator to deploy a certain deployment with a level of security. However it can be assumed that all the connections will be encapsulated using IPsec between different domain of responsibilities.

Servers are treated separately in the following sections.

4.4.1.1.1.1.4 AAA SERVERS AND PROXIES

4.4.1.1.1.1.4.1 NODE DEFINITION

The AAA Server implements a framework, based on IETF protocols (RADIUS or Diameter), that specifies the protocols and procedures for authentication, authorization, and accounting associated with the user, MS, and subscribed services across different access technologies.

The AAA Server could provide the following services to the AeroMACS networks:

- Authentication Services. These include device, user, or combined device and user authentication.
- Authorization Services. These include the delivery of information to configure the session for access, mobility, QoS and other applications.
- Accounting Services. These include the delivery of information for the purpose of billing (both prepaid and post paid billing) and information that can be used to audit session activity by both the home NSP and visited NSP.

An AAA server in the topology can act as an AAA proxy if the user that proceeds with registration belongs to a different domain, in a roaming context since the two servers are placed in different entities.

4.4.1.1.1.1.4.2 SECURITY FEATURES

The IETF AAA protocols are hop-by-hop secure and the AAA nodes are assumed to be trustworthy. RADIUS is assumed for this set of scenarios.

Note: RADIUS protocol has been for long time been considered as the “defacto” AAA protocol for WiMAX. However, according to WiMAX forum documentation, the DIAMETER protocol could be also considered. A comparison between those two AAA implementations is provided in Annex B.

The AAA protocols provide protection against multiple types of external threats e.g. man-in-middle attacks. In RADIUS the protocol provides a mechanism to provide integrity protection, privacy, and protection against replay attacks. This mechanism is protected by a key that is shared between the RADIUS hops. Using this procedure is usually accepted when the registration is performed within the same network, however, it can have some security concerns in roaming (in our case, between AAA server and AAA proxy) since the MD5 hash built into RADIUS is considered insecure. In order to avoid this, a secure end-to-end connection (Ipsec) between the RADIUS servers can be established to ensure that users' credentials cannot be intercepted while being proxied across the non-trusted network, IPsec is not part of the RADIUS protocol and the decision on a specific protection method remains a deployment-specific decision. We will assume IPSec is only used for the connection between AAA proxy and AAA server, not inside the airport network.

RADIUS uses a number of data stores. These include the user’s identity store, policy stores, and an accounting store that contains accounting information collected for a period of time. These stores must be secured and maintained but the decision on specific mechanisms is manufacturer Dependant.

4.4.1.1.1.1.5 DHCP SERVER

4.4.1.1.1.1.5.1 NODE DEFINITION

Each AeroMACS MS owns a univocal IP address, it is the main way for the network to identify it and the only way for the MS to send & receive data. In the AeroMACS Network Entry procedure the last phase is the “establish IP connectivity”. To obtain an IP address the MS shall find the right DHCP Server and once located the DHCP server it will assign a unique IP address to the MS.

Even in scenarios where IPv6 architecture is deployed and auto configuration is used, a DHCP server is still present and used for DNS allocation. When IPv6 will be analyzed for AeroMACS network, this scenario will be considered. In this study, the existence of a DHCP server is assumed.

4.4.1.1.1.1.5.2 SECURITY FEATURES

The standard procedure to obtain an IP address is quite insecure. The DHCP client (MS) broadcast discovery messages (DHCPDISCOVER) containing own MAC address and DHCP servers respond by offering (DHCPOFFER) to lease an IP address and other TCP/IP settings that the MS can use to communicate on the network. The client responds (DHCPREQUEST) to the first lease offer it receives and the server acknowledges (DHCPACK) the request and marks the address as leased in its DHCP database. In AeroMACS there are two different DHCP deployment modes possible:

- DHCP proxy is in the ASN, in the ASN-GW for the FAD;
- DHCP relay in the ASN (in the ASN-GW for the FAD) and DHCP server is located in the CSN.

In the first case the ASN-GW receives the DHPC Discover from the MS and it will answer directly. In this case the DHCP Server is the ASN-GW. On air the communication is protected with radio encryption and on R6 only if the GRE tunnels are ciphered (e.g. with IPSEC).

In the second case the DHCP relay sends messages to the external DHCP server, it is in the CSN, on R3 interface. This interface is insecure and not standardized in AeroMACS networks and it could be protected using IPSec.

The DHCP Server has a pool of IP addresses to manage and these IP Addresses are allocated to the AeroMACS MSs. This pool must be secured and maintained but the decision on specific mechanisms is manufacturer Dependant.

4.4.1.1.1.2 AIRBORNE TOPOLOGY

4.4.1.1.1.2.1 AEROMACS MOBILE STATION

4.4.1.1.1.2.1.1 NODE DEFINITION

Mobile Station (MS) is the subscr ber side of the service flows in the air interface. It is also a host or a CPE supporting multiple hosts. The link connectivity and resource allocation for every MS are managed by the corresponding BS. An MS can initiate a network entry or handover, but final decision and authorization comes from BS.

4.4.1.1.1.2.1.2 SECURITY FEATURES

Regarding RF protection, AeroMACS uses inherently OFDM and subcarrier permutation schemes in order to provide frequency diversity. It also provides an adaptive modulation/coding and power control mechanism to improve the link quality. However, this improvement has a limit (most robust modulation scheme can be QPSK1/2, and transmitted power is limited by regulation in airport). At a signal loss, MS stores the operational information and tries to reacquire the lost channel for a while (implementation-dependent). If no re-acquisition is possible, it performs a complete re-entry to the system by scanning for possible channels with reachable BSs.

The MS performs authentication with the BS (if RSA used) or with AAA server (if EAP is used). During authentication process, PKMv2 key exchange and authorization is used that provides mutual authentication. There are two possible methods:

- If EAP is used for PKMv2, both device and user authentication are possible. EAP is an end-to-end security protocol. For device authentication, X.509 over EAP-TLS is used. For user authentication, either EAP-AKA or EAP-TTLS are used. Also, EAP-SIM, EAP-PEAP are optionally supported. MS normally checks the revocation status of AAA server X.509 certificate at the time of authentication in order to provide end-to-end authentication.
- If RSA based on X.509 certificate (PKI) is used, only device authentication is possible, there are no user authentication related procedures. RSA applies only to the air interface between MS and BS.

If user and device credentials are distinct and both need to be authenticated, either a tunnelling EAP method (EAP-TTLS) or a credential combining can be used in a single EAP session. However, this is only feasible if the AAA server for user and device authentication is the same. If AAA servers that authenticate user and device are different, a double authentication must be used. In current standard, only RSA+EAP is supported. In IEEE802.16e standard, also EAP+authenticated EAP and RSA+authenticated EAP are possible.

During authentication, MS receives the shared keys pre-PAK or MSK from BS in order to generate the AK and TEK together with its MAC address. In the process of key generation, function DOT16KDF that employs CMAC algorithm is used in order to guarantee the cryptographic independence of AK at every MS. At every TEK refresh, the MS requests the BS for the new key.

Optionally multicast group keying can be supported. For group multicast connections, shared keys are generated among all MSs. Also GKEK (from which GTEK is generated) is sent to all MSs. Multicast connections must use different SA than unicast connections.

Basic and primary connections, which carry management messages, do not cipher, nor authenticate messages. Transport connections can be handled independently and be assigned security associations (SA). Security Association (SA) associates key material and connection, *i.e.* every CID is mapped to a SAID if it supports security. Every MS must be able to support at least 2 transport SAs according to WiMAX. SA information includes current cryptographic suite, used TEK, KEK, PN and associated lifetimes. SAID is updated in the MS by the target BS during handover.

Every MS establishes a primary SA with the BS. The rest of SAs are static as they are provisioned by the BS. If a pair BS/MS has no authorization policy, there is no related SA.

4.4.1.1.1.2.2 AIRBORNE TOPOLOGY BEYOND THE AEROMACS MOBILE STATION

4.4.1.1.1.2.2.1 NODE DEFINITION

The airborne topology can be divided in three domains. ACD (Aircraft Control Domain), AISD (Airline Information Service Domain) and PIESD (Passenger Information and Entertainment Services Domain) are the three main domains in the aircraft. From a security point of view, they are represented from left to right, left being the most secure domain and right less secure domain. The ACD is the heart of the aircraft, it contains the most critical functions of the aircraft and that is why it is much more secure than AISD and PIESD.

There are two possible ways to connect AeroMACS inside the aircraft:

- Option 1: AeroMACS is connected to the ACD;
- Option 2: AeroMACS is connected to the AISD.

4.4.1.1.1.2.3 SECURITY FEATURES

The onboard router does not implement security functions, the latters are provided by firewalls. Firewalls filter flows passing through them. But, an important thing to know is that firewalls always allow flow going from the most secured domain to a less secure domain (e.g. ACD to AISD). This is called segregation between domains and the main reason why there is two way of connection of the AeroMACS to the aircraft.

For example, communications between ACD and AISD are very restricted in the way AISD to ACD, the firewall between both domains filters every packet going from AISD to ACD but not all coming from ACD to AISD. This is the same between sub-domains Flight Domain and Flight IS Domain. Others firewalls also implement rules of filtering, firewalls that are implemented inside routers with connection of AeroMACS filter flows coming from the ground. Moreover, a security feature that is not shown in the figure is robustness of the applications inside the ACD.

The only router able to support an encrypted connection (type is not defined nowadays) is the AISD router, option 2, which is the embedded router connected to the AISD domain (as it is the case for the all the embedded domains such as the ACD for instance).

4.4.1.2 SIMULATION INPUTS

Table 14 summarizes the main simulation inputs that we used in this study:

Node ID	Function value	Class value	# Connected nodes	# security protection	# vulnerabilities
Base Stations	1	1	3 / 4 / 5	8	1
Aircraft	0.7	1	1	2	0
Surface vehicles	0.7	1	1	2	0
AAA Server	0.3	1	1	3	20
DHCP Server	0.3	1	1	1	64
ASN Gateway	0.3	1	14	2	1
ATS Server	0.3	1	1	1	47
AOC Server	0.3	0.7	1	1	47
APC Server	0.3	0.1	1	1	13

Table 14: Simulation parameters

Function values and class values are explained in section 4.2.2. Number of connected nodes and security protections are derived from the topologies all the partners agreed on. Number of vulnerabilities is based on realistic hypothesis made for COTS products from the NVD database.

4.4.1.3 VULNERABILITY STATISTICS

The following table illustrates the repartition of the CVSS score for each node in the network (please note that the terminology and taxonomy used in the NVD database has been respected):

CVSS score	Number of total vulnerabilities	Percentage

[0,1]	0	0%
[1,2]	2	0.995%
[2,3]	1	0.498%
[3,4]	0	0%
[4,5]	7	3.483%
[5,6]	11	5.473%
[6,7]	4	1.990%
[7,8]	111	55.224%
[8,9]	0	0%
[9,10]	65	32.338%
Total	**201**	**-**
Average score	**7.938**	

Table 15: Vulnerability CVSS statistics

The most part of the scores are ranked in the [7,8] NVD CVSS interval (and represent 55.224% of the total vulnerability scores). The maximum CVSS scores ranked between 9 and 10 are in most cases relative to the DHCP server node, which explains why this node has the highest individual risk value among the network. The average CVSS score has been measured to 7.938.

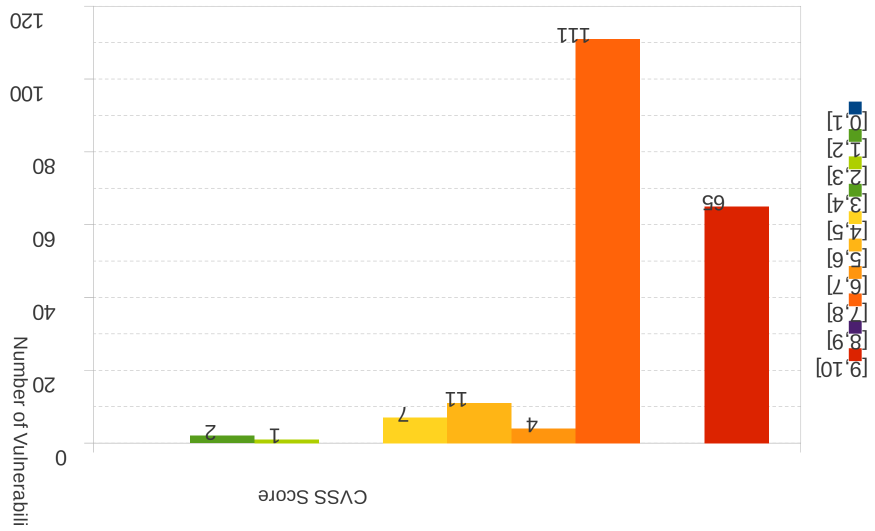


Figure 10 : Vulnerability CVSS score distribution for all nodes

4.4.1.4 INDIVIDUAL RISK RESULTS

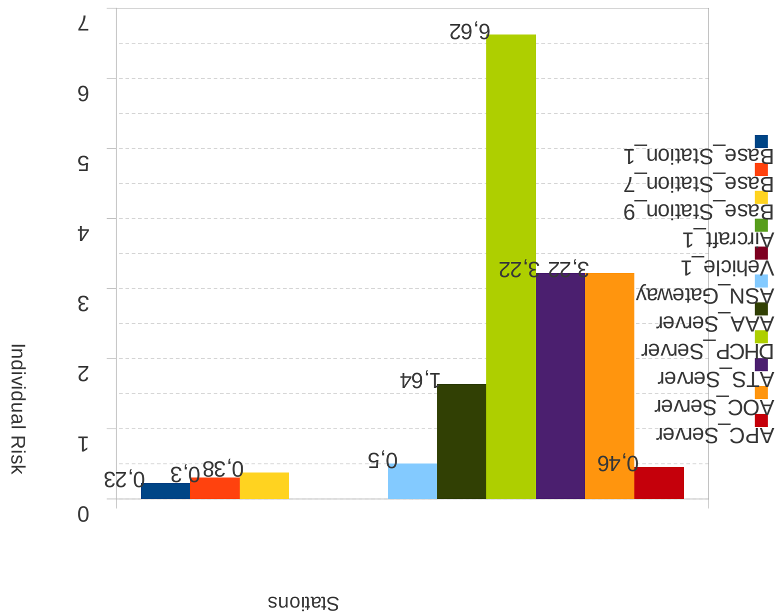


Figure 11: Individual risks for all network nodes

As we can see in the Figure 11, base stations and ASN Gateway individual risks are relatively low because there is only a single vulnerability for these nodes. Despite having the same specific vulnerability (CVE-2008-1542), there is a difference (evaluated from 0.075 to 0.15) between Base_Station_8, Base_Station_9 and the seven first base stations individual risks. This is mainly due to the higher number of connected nodes of Base_Station_8 and Base_Station_9, which increases their node values. Another interesting fact is that APC_Server and ASN Gateway individual risks are nearly close (respectively 0.5 and 0.46) despite a big difference in the number of intrinsic vulnerabilities on each of them (respectively 1 and 13). Indeed, we shall expect a higher individual risk for the APC_Server node as long as it has more vulnerabilities, however the ASN Gateway compensates the gap with the highest node value in the network (equal to 14) whereas the APC_Server, giving it functionality and traffic class value is the lowest one (equal to 0.03). The DHCP_Server node is the most vulnerable node in the network, and consequently has the highest individual risk out there (assessed to 6.62). The FreeRadius server is the most vulnerable node in the network with 64 vulnerabilities and very high CVSS scores: 92.12% of these them have top CVSS score (meaning 10, the highest score in the NVD database). Even the lowest CVSS score is relatively high (9.3) if we compared to base stations or ASN Gateway vulnerability scores (respectively 7.5 and 5.0). Finally AAA_Server, ATS and AOC servers, regarding the assumptions made in the inputs, are quite logical and get medium individual risk values due to a considerable number of intrinsic vulnerabilities. Except the ASN Gateway individual risk value which is considerably impacted by the high value of the node, all the individual risk values we measured seem to grow with the number of exploitable vulnerabilities per node taken from the NVD database (according the the different vulnerabilities provided by the inputs):

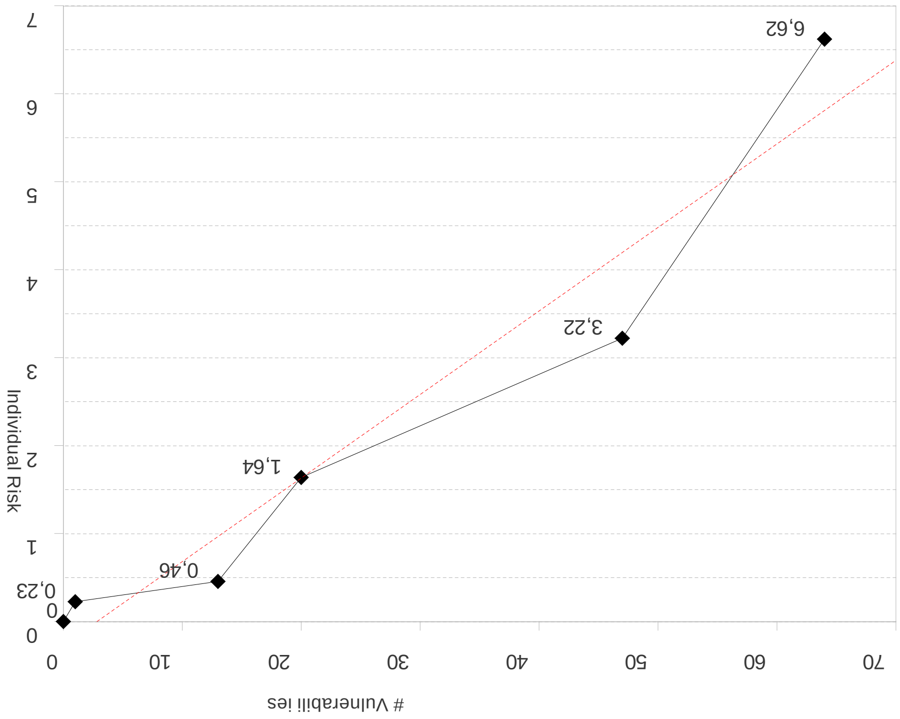


Figure 12: Individual risk evolution as a function of the number of vulnerabilities for all nodes.

Regarding the assumptions made for the inputs of the current simulation; we can say that the individual risk depends on the number of vulnerabilities per nodes.

4.4.1.5 PROPAGATED RISK RESULTS

Here are the propagated risk values for the nodes in the network:

Node	Propagated risk
Base stations (1 to 6)	7.474
Base stations 7 and 8	9.965
Base station 9	12.456
Aircraft (1 to 6)	0.812
Aircraft (7 to 12)	1.082
Vehicle (1 to 6)	0.812
Vehicles 7 and 8	1.082
Vehicles 9 and 10	1.353

ASN Gateway	538.998
DHCP and AAA server	1.2
ATS server	0.398
AOC server	0.750
APC server	0.135

Table 16: Propagated risk values for all nodes

The propagated risk results are mainly impacted by the importance of the connected node number parameter in the algorithm. For instance, we have made assumptions regarding the topology of this scenario for the base stations: the first 6 base stations are connected to three nodes (*i.e.* one aircraft, one vehicle, and the ASN gateway), base stations 7 and 8 are connected to four nodes (+ another vehicle) and the last base station to five nodes. The remaining parameters (security protection, offered service, exchanged data, of NVD vulnerabilities) are always the same. However, the propagated risk values are slightly different (ranging from 7.474 to 12.456) because of different correlation density in the network.

The propagated risk for the aircraft also deserves to be deeply discussed. Indeed, as we can see, it is not the same for the 6 first aircraft (equal to 0.812) as the 6 last ones (equal to 1.082). However, the justification does not lay in the connected node parameter this time as far as all aircraft are connected to a single base station. The difference between propagated risk for the aircraft (assessed to 0.27) is due to intrinsic vulnerabilities and the individual risk specific to the base station to which the aircraft is connected to. DHCP, AAA, ATS, AOC, and APC servers have all low propagated risk values (ranging from 0.135 to 1.2) because all of them are connected to a single node (the ASN gateway) which has a very low individual risk (equal to 0.5).

As we can see, the most important result in this simulation is the propagated risk value of the ASN gateway, which supersedes all the remaining nodes. This is likely due to a high node correlation for the ASN gateway: as far as it is the 'core' of the topology where all node exchanges have to pass through the gateway, it is logically impacted by the other nodes and their specific vulnerabilities. The concept of propagated risk lies in the importance of the connected node number parameter as we can see in the following figure:

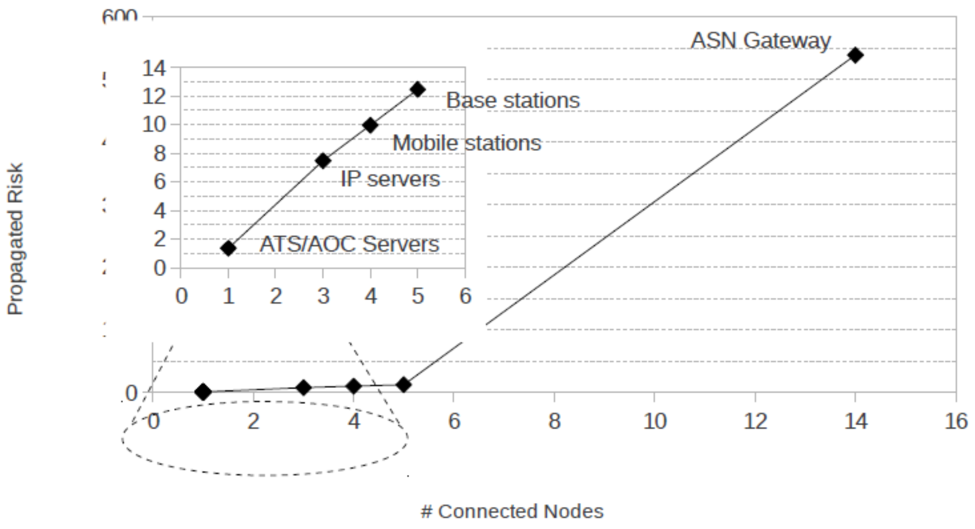


Figure 13: Propagated risk evaluation as function of connected nodes for all network nodes

4.4.1.6 NODE AND NETWORK RISK RESULTS

The node risk of the ASN Gateway is hardly impacted by the high-propagated risk of the node (cf. the formula of node risk evaluation). Besides, the high node value of the ASN Gateway plays a major role in the growth of the node risk value: even the highest node risk (which is relevant to the Base Station 9) is 117 times smaller than the ASN Gateway node risk.

Consequently, as the network risk is given by the sum of the node risk, the network risk is mainly represented by the ASN Gateway node risk as we can see in the following chart:

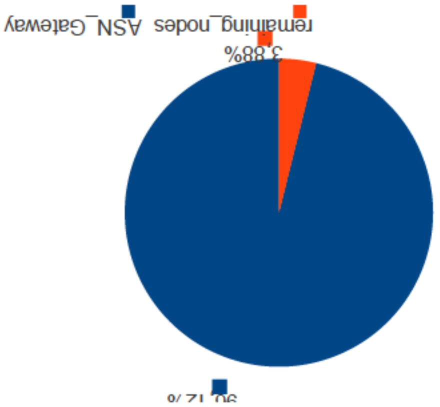


Figure 14: Percentage of network risk per node risk

The detailed node risk repartition compared to the network risk is given in the following table:

Node	Node risk	% of network risk
All base stations	284,866	3,63%
All aircraft	8,337	0,11%
All vehicles	6,821	0,09%
AAA server	0,851	0,01%
DHCP server	2,346	0,03%
ATS server	1,085	0 ,01%
AOC server	0,833	0,01%
APC server	0,017	0%
ASN Gateway	7552,98	96,12%

Table 17: Node risk statisctics

Here is the contribution (%) of each connected node with the ASN_Gateway propagated risk:

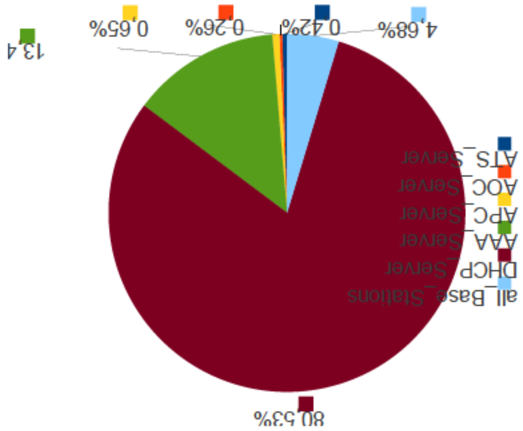


Figure 15: ASN Gateway propagated risk contribution per connected node

It is clear that the DHCP server represents the biggest contribution in the propagated risk of the ASN Gateway node and is the main actor of this high-risk value. This means that if we want to get the ASN Gateway node risk lower (and consequently the network risk) we should tweak two related parameters:

1. The number of connected nodes is really important and should be limited per node as much as poss ble. This can be first done by some topological considerations that allows the network risk to be less higher than in this first simulation;
2. The ASN Gateway is the bottleneck of this risk analysis as we already saw in the previous results. Despites its high node connectivity, its high propagated risk value is not directly due the number of interconnected nodes, but rather to the high individual DHCP server individual risk, the high correlation that exists between the two nodes (the ASN Gateway is the only node connected with the DHCP server node) and the high node value of the ASN Gateway.

4.4.1.7 ISOLATED AEROMACS SCENARIO: EAP VS. RSA SIMULATIONS

As it has been previously mentioned, AeroMACS privacy sublayer is able to support both EAP and RSA for device and user authentication and authorization. The aim of this scenario is to compare the effects of these security options on the AeroMACS air interface on the global network. Currently, only one option can be chosen, which is using RSA or EAP as authentication and authorization protocol. Many vulnerabilities have been found for both security mechanisms. It is worthy to notice that EAP has several methods defined in IETF RFCs (EAP-TLS, EAP-AKA, EAP-SIM, etc), however the NVD vulnerability database does not give much information on these methods: it is only mentioned that the vulnerability is relevant to the EAP protocol. The NVD database clearly indicates a higher number of vulnerabilities for RSA (i.e. 33 vulnerabilities) compared to EAP (only 4 vulnerabilities). Indeed, RSA is much more known and used over all IT systems in the world. Then, it is quite logical to find more vulnerabilities inputs in the database compared to EAP. Moreover, the vulnerability statistics we made in this simulation shows again that the number of vulnerabilities is not the only indicator on what is the security mechanism we should privilege. Indeed, despite a higher number of vulnerabilities (+29 vulnerabilities), RSA remains more secure than EAP: as we have seen in the global simulation, the average CVSS score is a safer criteria if we want to compare two or more security mechanisms in the NVD database. The average CVSS score (on the total vulnerabilities in the AeroMACS network) has been evaluated to 6.325 for RSA and 7.795 for EAP. Table 18 gives more details on the vulnerabilities statistics for the EAP vs. RSA scenario simulations:

CVSS score	EAP		RSA	
	# Vulnerabilities	Percentage	# Vulnerabilities	Percentage

[0,1]	0	0	0	0
[1,2]	2	0.83	12	2.26
[2,3]	1	0.415	11	2.072
[3,4]	0	0	10	1.883
[4,5]	7	2.905	107	20.151
[5,6]	31	12.863	121	22.787
[6,7]	4	1.66	24	4.52
[7,8]	121	50.207	161	30.32
[8,9]	0	0	0	0
[9,10]	75	31.12	85	16.008
Total	**241**	-	**531**	-
Average Score	**7.795**		**6.325**	

Table 18: EAP vs. RSA Vulnerability Statistics

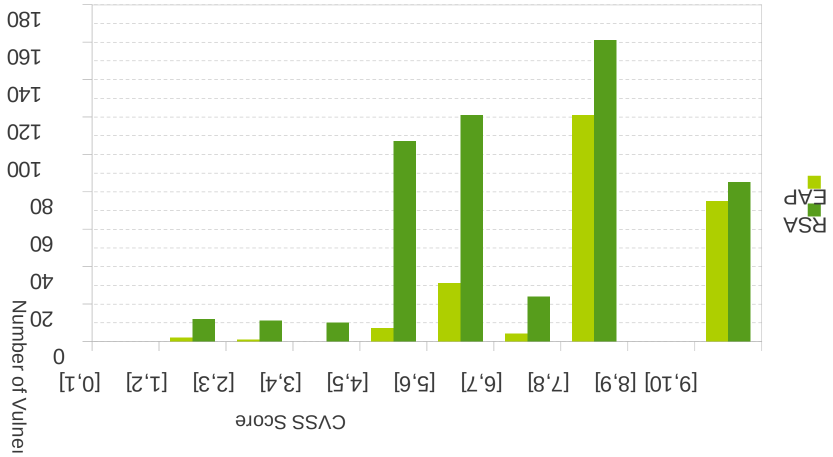


Figure 16: Vulnerability CVSS Score Distribution for EAP and RSA

However, the average CVSS score should be weighted accordingly to the individual risk values obtained after the simulation. Indeed, Figure 17 shows the individual risk values updated for the base stations and the ASN Gateway (all the remaining nodes are not represented since there is no change to notice on them). The higher number of vulnerabilities for RSA makes naturally the individual risk higher than EAP for both base stations and the ASN Gateway (+16.35 and +14.8 respectively for RSA and EAP). These results suggest first that the number of vulnerabilities remains important parameters because the individual risk is computed as a sum of likelihood of occurrence of a threat and its impact on the total number of vulnerabilities: since RSA has much more inputs in the NVD database, the individual risk relevant to EAP is lower.

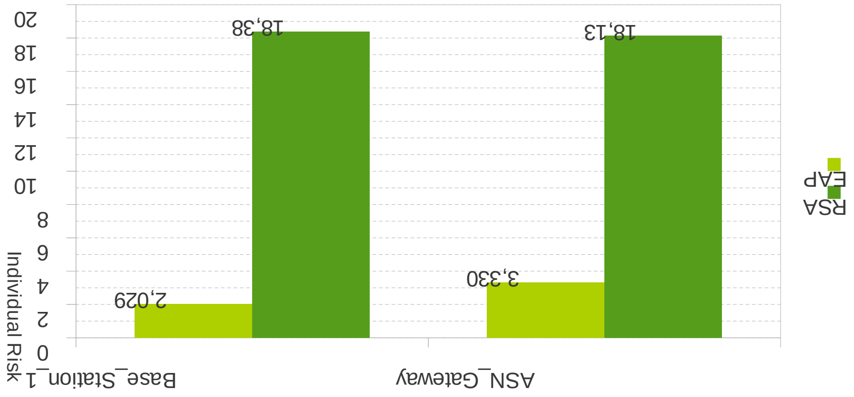


Figure 17: Individual risk for base stations and the ASN Gateway (EAP vs. RSA)

As a conclusion, if we want to take the risk individually by node, it is clear that EAP should be used for authentication and authorization in the AeroMACS nodes. However, the propagated risk results should be also considered to effectively make final guidances on the use of EAP or RSA protocols.

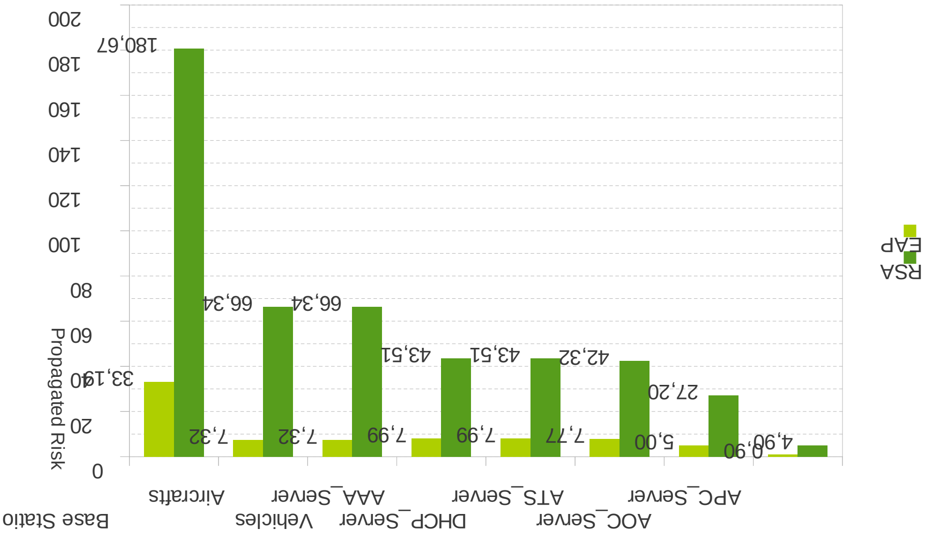


Figure 18: Propagated risk for all nodes (EAP vs RSA)

Figure 18 shows the propagated risk values using EAP or RSA protocols for all network nodes (except the ASN Gateway which has a very big propagated risk value and is not represented for clarity matters).

The same comments for the individual risks remain true here: the EAP authentication protocol induces a lower propagated risk compared to the RSA protocol. The ASN Gateway is still the bottleneck in both sub-scenarios since it has the largest propagated risk among all the network nodes (1042.64 and 2499.87

respectively for EAP and RSA). It still has the biggest contribution in the global network risk (either for EAP or RSA) as illustrated in Table 19:

Node	% of network risk	
	EAP	RSA
All base stations	6.867%	14.509%
All aircraft	0.386%	1.310%
All vehicles	0.322%	1.091%
AAA server	92.118%	82.888%
DHCP server	0.03%	0.038%
ATS server	0.135%	0.0755%
AOC server	0.081%	0.0546%
APC server	0.053%	0.030%
ASN Gateway	0%	0%

Table 19: Node risk statistics (EAP vs. RSA)

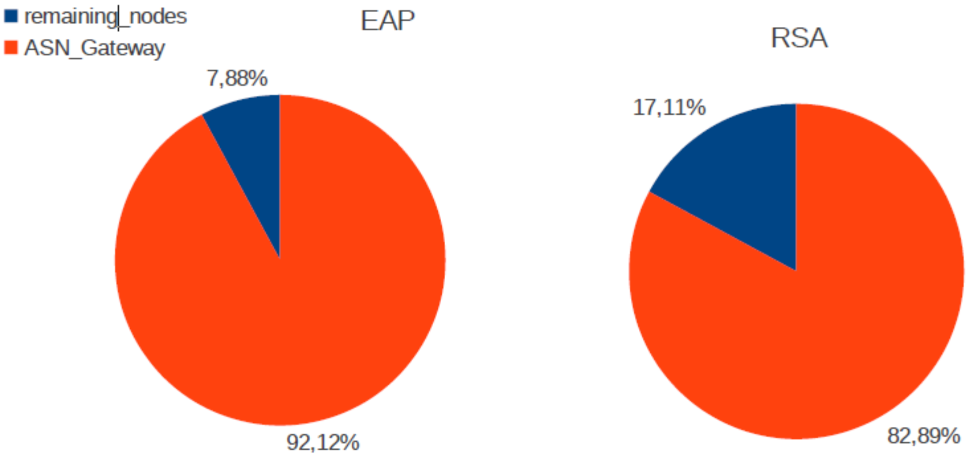


Figure 19: Percentage of network risk per node risk (EAP vs. RSA)

4.4.1.8 PRELIMINARY GUIDANCES

Even if the results of this first scenario should be discussed again regarding the end-to-end AeroMACS topology simulation results, we can already draw the big lines of the guidances that should allow us to decrease the risk level for the different network nodes:

1. **Implementation guidances:** Network nodes should be chosen wisely with a minimum of intrinsic vulnerabilities. IP COTS nodes (AAA Server, DHCP Server) should be discussed regarding the number of the exploitable vulnerabilities and their respective CVSS scores. It could be interesting to establish a state-of-the-art of the potentially usable IP nodes (particularly the DHCP server node),

classify them by number of vulnerabilities and CVSS scores and see how the individual risk per node is affected. The nodes to be preferred are obviously the nodes with the lowest individual risks. Also the simulations of the RSA vs. EAP scenario showed that EAP induces a lower risk (individual, propagated, and network risk) for the isolated AeroMACS topology.

2. **Topological guidances:** as we have seen, the global network risk is highly impacted by the propagated risk values (more than the individual risk values) because the node connectivity is taken into account at this step of the risk assessment process. It is clear that the ASN Gateway is the main issue in this topology and some countermeasures should be taken to avoid this problem. For instance, it could be interesting to select two ASN Gateways, each connected to a set of base stations and IP nodes. This will likely provides less node correlation between the ASN Gateway (then a lower l kelihood of correlation) and highly impacted IP nodes (such as the DHCP server) and consequently decreases the network risk. Using two GWs (or more) allows dispatching the connected nodes, and then reduces both the l kelihood of propagation and impact of threat from COTS nodes (which are highly vulnerable) to the GW. Another advantage is to introduce dissymmetry of devices, meaning having different implementations of the GWs, which allows to have different level of risks;

3. **Security guidances:** now that we clearly identified the most constraining node in the network and their respective contribution in the global network risk, some security mechanisms should be deployed to limit the propagated risk. A particular attention should be given to the connectivity between the ASN Gateway and the IP nodes such as the DHCP server. To deal with this connectivity problem, firewalls should be privileged. Indeed, they can limit the data exchanges between a highly vulnerable node and the ASN Gateway. Also, maximizing security protections at a layer-2 (typically AeroMACS security) should also help the propagated node risk decrease for AeroMACS-based nodes (*i.e.* base stations and mobile stations).

4.4.2 ISOLATED AEROMACS EXTENDED SCENARIOS

After the preliminary guidance provided by the first simulation campaign, we decided to extend the isolated scenario simulations. The first idea is to start again the simulation with the same parameters except for the operational aeronautical servers (*i.e.* ATS, AOC, and APC servers), for whom we remove the intrinsic vulnerabilities (because they relied on COTS products, which have been considered not much realistic). The second idea is to take into consideration the topological guidance, namely using two ASN gateways instead of one in order to reduce the propagated risk between the network nodes.

The results presented in this section are (in most cases) compared to the first simulation results with the aim to tell if the new assumptions are helpful or not.

4.4.2.1 SCENARIO WITHOUT OPERATIONAL SERVER VULNERABILITIES

4.4.2.1.1 NETWORK TOPOLOGY

The network topology is depicted in the previous scenario. Basically, it remains the same, as there is no added or removed node in the network:

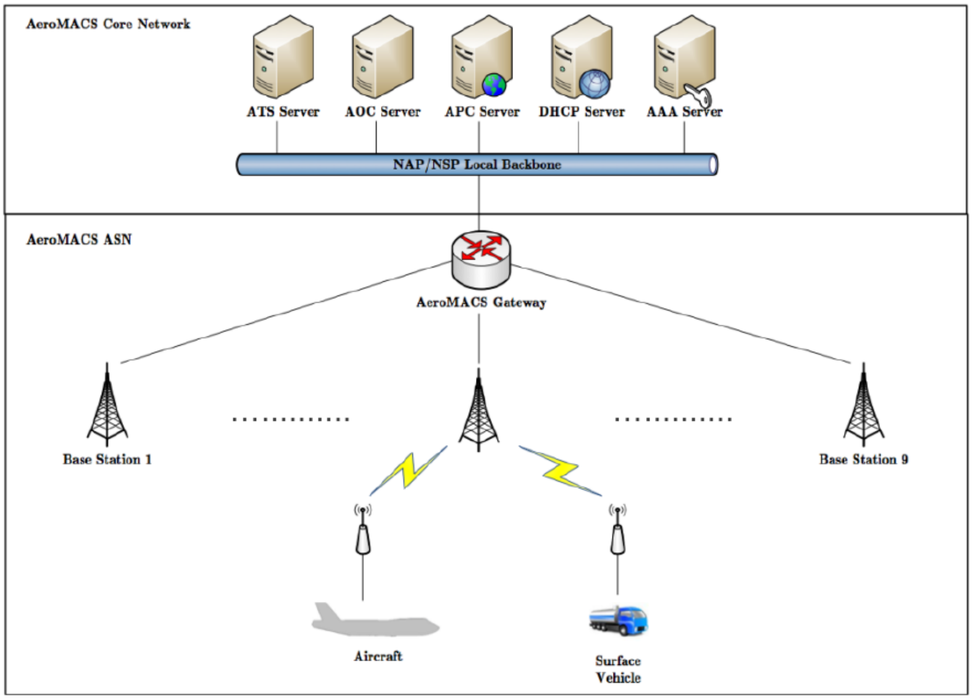


Figure 20: AeroMACS Network Topology : extended Isolated Scenario

4.4.2.1.2 SIMULATION INPUTS

Table 20 summarizes the main simulation inputs we used in this study. Parameters are kept unchanged except for the "# vulnerabilities" parameter relevant to the operational servers:

Node ID	Function value	Class value	#Connected nodes	#Security protection	# Vulnerabilities
Base Stations	1	1	3 / 4 / 5	8	1
Aircraft	0.7	1	1	2	0
Surface vehicles	0.7	1	1	2	0
AAA Server	0.3	1	1	3	20
DHCP Server	0.3	1	1	1	64
ASN Gateway	0.3	1	14	2	1
ATS Server	0.3	1	1	1	0
AOC Server	0.3	0.7	1	1	0
APC Server	0.3	0.1	1	1	0

Table 20 : Simulation parameters (without operational server vulnerabilities)

4.4.2.1.3 VULNERABILITY STATISTICS

Table 21 shows the updated vulnerability CVSS statistics after removing the operational aeronautical server vulnerabilities:

CVSS score	Number of total vulnerabilities	Percentage
[0,1]	0	0%
[1,2]	0	0%
[2,3]	0	0%
[3,4]	0	0%
[4,5]	2	2.127%
[5,6]	9	9.574%
[6,7]	2	2.127%
[7,8]	16	17.021%
[8,9]	0	0%
[9,10]	65	69.148%
Total	**94**	**-**
Average score	**8.859**	

Table 21: Updated Vulnerability CVSS statistics

The most interesting result here is probably the fact that even if we reduced the total number of vulnerabilities (from 201 to 94), the average CVSS score is higher in this extended scenario (8.859 against 7.938). This result is mainly due to the new distribution of CVSS scores which put a higher emphasis on the critical vulnerabilities (*i.e.* [9,10] CVSS score range) in this scenario compared to the previous one. This has obviously an impact on the individual risk results, but should not alter the propagated risk values, as this type of risk is more sensitive to the node correlation parameter. Figure 21 shows the distr bution of CVSS scores in each scenario:

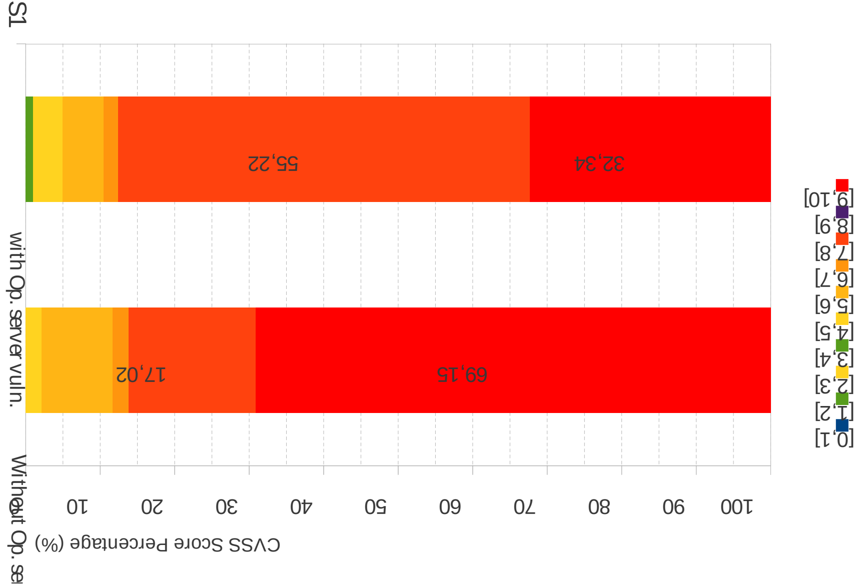


Figure 21: Comparison of CVSS score distribution (with and without operational server vulnerabilities

4.4.2.1.4 INDIVIDUAL RISK RESULTS

Except for the operational servers, individual risk results are not altered. Indeed, beside the number of connected nodes (with is taken into account in the node value parameter), there is no consideration for node correlation in the individual risk. That being said, removing the operational server vulnerabilities does not have any impact on the other individual risk results relevant to remaining network nodes (even those directly connected to them such as the ASN GW).

Node ID	Individual risk
Base stations (1 to 6)	0.23
Base stations 7 and 8	0.3
Base station 9	0.38
Aircraft (all)	0
Vehicle (all)	0
ASN Gateway	0.5
DHCP server	6.62
AAA server	1.64
ATS server	0
AOC server	0
APC server	0

Table 22: Updated Individual risk results

4.4.2.1.5 PROPAGATED RISK RESULTS

Removing the operational server vulnerabilities undeniably has a impact on the propagated risk values for all nodes in the network. As we can see, updated propagated risk values have decreased compared to values in Table 16:

Node	Propagated risk
Base stations (1 to 6)	5.471
Base stations 7 and 8	8.012
Base station 9	9.586
Aircraft (1 to 6)	0.355
Aircraft (7 to 12)	0.941
Vehicle (1 to 6)	0.355
Vehicles 7 and 8	0.670
Vehicles 9 and 10	0.941
ASN Gateway	417.013
DHCP and AAA server	0.66
ATS server	0.182
AOC server	0.551
APC server	0.054

Table 23: Updated Propagated Risk Results

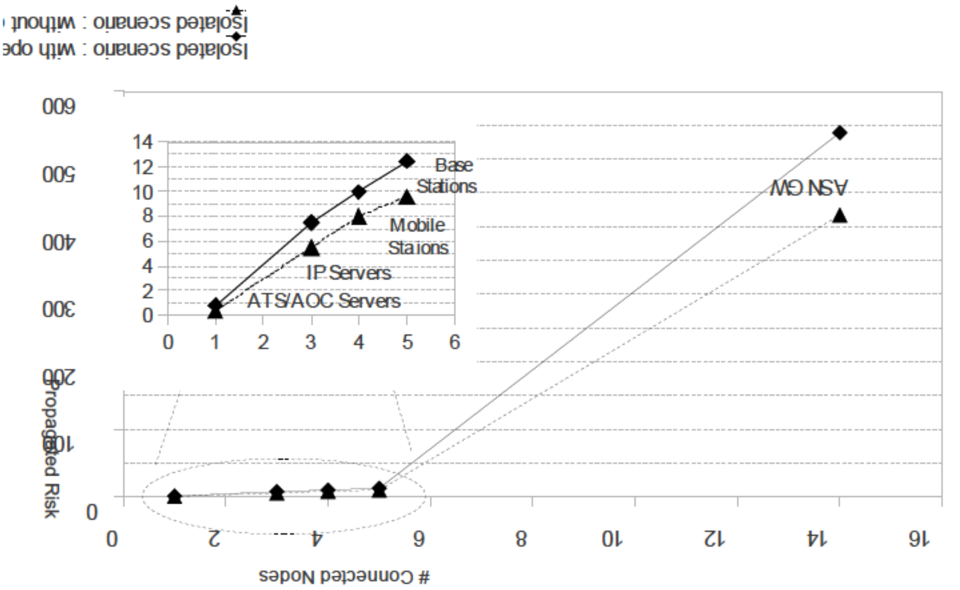


Figure 22: Comparison of Propagated Risks as a Function of the Number of Connected Nodes (with and without operational server vulnerabilities)

This difference is clearer when we compare the propagated risk evolution as a function of the number of connected nodes for both scenarios: for all network nodes, propagated risk values are lower and decrease in the new scenario (i.e. without operational server vulnerabilities). This is an important result because it shows that even if we make some assumptions regarding a node individually (for instance by updating its exploitable vulnerabilities or CVSS scores), we impact the propagated risk values relevant to nodes connected logically (i.e. there is a data flow exchange between them) to that specific node.

4.4.2.1.6 NODE AND NETWORK RISK RESULTS

The network risk results are impact the same way as the propagated risk results, the new values are resumed in Table 24:

Node	Node risk	% of network risk
All base stations	218.838	3.601
All aircraft	4.687	0.077
All vehicles	3.748	0.061
AAA server	0.689	0.011
DHCP server	2.184	0.03
ATS server	0.054	0
AOC server	0.115	0.001
APC server	0.001	0
ASN Gateway	5845.192	96.209

Table 24: Updated Network and Node Risk Results

Despite a decrease of every node risk value, the ASN Gateway has always the biggest node risk among all nodes and its contribution in the network risk always over-seeds the other nodes. Figure 23 shows a comparison between node contributions in the network risk for both scenarios:

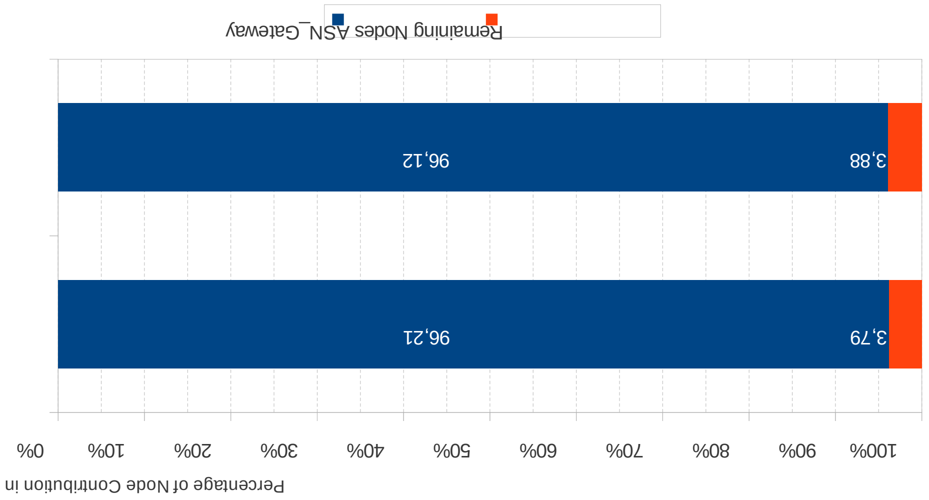


Figure 23 : Comparison of the Percentage of network risk per node risk (With and Without Operational Server Vulnerabilities)

As a conclusion, we can say that removing the operational server vulnerabilities has an impact on both individual risk (relevant to ATS, AOC, and APC servers) and propagated risk values but the network risk value remains high because the node correlation was not modified, and then the ASN Gateway is still the Achille's Heel of the of isolated topology. In order to address this issue, we propose in the next section another simulation campaign, this time using two ASN Gateways, instead of one, by keeping the assumptions made in this section for the operational server vulnerabilities.

4.4.2.2 SCENARIO WITH TWO ASN GATEWAYS

4.4.2.2.1 NETWORK TOPOLOGY

The network topology has changed with the addition of the second ASN gateway as depicted in the following figure:

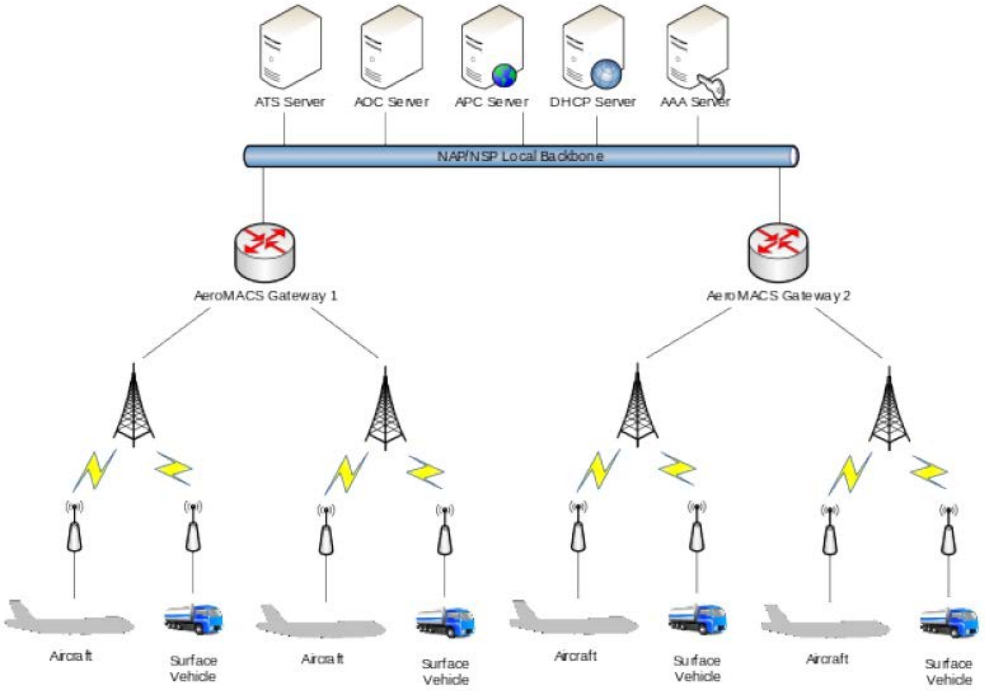


Figure 24: The New Isolated Network Topology using Two ASN Gateways

This topological amendment will likely reduce the correlation between a single ASN Gateway and connected nodes, as it has been considered as the central hub and point of failure in the first topology. With the introduction of a second ASN Gateway and removing the operational server vulnerabilities, the risk values should decrease.

4.4.2.2.2 SIMULATION INPUTS

Table 25 summarizes the main simulation inputs that we used in this study. The impact of the new topology resulting from the integration of a second ASN gateway implies many changes:

- Servers behind the backbone are now connected to two ASN gateways (instead of only one);
- The node correlation for ASN gateways is now reduced to 9 (or 10 depending on the connected BSs) instead of 14 in the first simulation;
- The assumptions made for operational servers in the previous simulation (i.e. no COTS vulnerabilities) are maintained.

Node ID	Function value	Class value	#Connected nodes	#Security protection	# Vulnerabilities
Base Stations	1	1	3 / 4 / 5	8	1
Aircraft	0.7	1	1	2	0
Surface vehicles	0.7	1	1	2	0
AAA Server	0.3	1	2	3	20
DHCP Server	0.3	1	2	1	64

ASN Gateway 1	0.3	1	9	2	1
ASN Gateway 2	0.3	1	10	2	1
ATS Server	0.3	1	2	1	0
AOC Server	0.3	0.7	2	1	0
APC Server	0.3	0.1	2	1	0

Table 25: Simulation parameters (Scenario with Two ASN GWs)

4.4.2.2.3 VULNERABILITY STATISTICS

Same as the vulnerability statistics in the previous scenario.

4.4.2.2.4 INDIVIDUAL RISK RESULTS

As for the individual risk results in the previous scenario, the altered values are relevant to nodes that have been impacted by the new topology. Then, the individual risk results remain the same for all nodes except the IP servers (i.e. AAA and DHCP servers) and both ASN Gateways:

Node ID	Individual risk
Base stations (1 to 6)	0.23
Base stations 7 and 8	0.3
Base station 9	0.38
Aircraft (all)	0
Vehicle (all)	0
ASN Gateway 1	0.32
ASN Gateway 2	0.29
DHCP server	13.24
AAA server	3.26
ATS server	0
AOC server	0
APC server	0

Table 26: Updated Individual Risk Values (Isolated Scenario With 2 ASN GWs)

As we can see in Table 26, the ASN GW risk values are lower compared to the scenario with one Gateway: indeed, the vulnerabilities (and their respective scores) are the same whereas the node connectivity has decreased (from 14 to either 9 or 10). The difference between the individual risk values for the two ASN Gateways is due to the number of connected nodes.

Moreover, we can see that the IP server individual risk values have doubled compared to the scenario with just one ASN Gateway: the DHCP and AAA servers where connected to one node (which is the ASN GW) while in the second scenario they are connected to two nodes (both ASN Gws). As all the parameters relevant to IP servers have not changed except the node connectivity ni, which is taken into account in the likelihood of occurrence of a threat formula (c.f. The first deliverable for more details), the individual risks have been multiplied by a factor of 2.

Quantitatively speaking, these new individual risk values show that globally, the risk is getting higher: we added an additional node and the intrinsic risk for IP servers has increased. But conclusions should be drawn after analyzing the propagated risk results, and more importantly, the overall network risk. That's why these results should be confronted to the propagated risk values (and later the node risk values) presented in the following section.

4.4.2.2.5 PROPAGATED RISK RESULTS

As expected, adding another ASN Gateway makes the propagated risk values increase or decrease, depending on the node correlation in the new topology as shown in Table 27:

Node	Propagated risk
Base stations (1 to 4)	4.469
Base stations 5 and 6	4.589
Base stations 7 and 8	6.062
Base station 9	7.518
Aircraft (1 to 4)	0.316
Aircraft 5 and 6	0.329
Aircraft (7 to 12)	0.549
Vehicle (1 to 6)	0.754
Vehicles 7 and 8	0.549
Vehicles 9 and 10	0.754
ASN Gateway 1	268.21
ASN Gateway 2	260.019
DHCP and AAA server	0.691
ATS server	0.250
AOC server	0.785
APC server	0.093

Table 27: Updated Propagated risk values (2 ASN GWs)

Unlike the previous simulation scenarios, base stations 1 to 6 do not have the same propagated risk values. Indeed, base stations 5 and 6 are connected to the ASN GW 2 (with a higher node correlation), which explains the higher propagated risk values for these base stations compared to base stations 1 to 4 (connected to the first ASN GW 1). Propagated risk values for base stations 7 to 9 have also decreased.

The observation is made for the propagated risk values relevant to the aircraft 1 to 6. In the previous scenarios, as they were connected to the same GW, they have the same propagated risk values (*cf.* Also tables 3 and 8), but in this case, despites having the same node correlation, aircraft 5 and 6 have slightly different propagated risk values as they are connected to the second GW.

Note that the DHCP and AAA server propagated risk values are the only results that have increased because of the higher node correlation in this scenario (two instead of one). For the ASN GWs, ss the node correlation has decreased (from 14 nodes to 9 and 10) in this scenario compared to the previous one, it is quite logical to obtain a lower propagated risk for both ASN GWs.

As a summary, propagated risk values relevant to nodes behind the backbone (belonging to the AeroMACS core network) have slightly increased whereas those relevant to nodes in the AeroMACS access service network have significantly decreased. These unbalanced changes in the propagated risk values have an impact on the network risk results as depicted in the next sub-section.

4.4.2.2.6 NODE AND NETWORK RISK RESULTS

Table 28 resumes the values for the node risks of all nodes in the new topology:

Node	Node risk
Base stations (1 to 4)	14.082
Base stations 5 and 6	14.433
Base stations 7 and 8	25.449
Base station 9	39.469
Aircraft (1 to 4)	0.221
Aircraft 5 and 6	0.230
Aircraft (7 to 12)	0.384
Vehicle (1 to 6)	0.221
Vehicles 7 and 8	0.384
Vehicles 9 and 10	0.527
ASN Gateway 1	725.031
ASN Gateway 2	780.927
DHCP server	8.358
AAA server	2.370
ATS server	0.15
AOC server	0.329
APC server	0.00

Table 28: Updated Node risk values (2 ASN GWs)

As expected, the node risk values have substantially decreased compared to those relevant to scenarios using a single GW, except for nodes in the AeroMACS core network (namely servers), but their respective contributions in the network risk are not really significant to be emphasized. Figure 24 shows a comparison between the network risk values for the three different simulations conducted at this stage of the study:

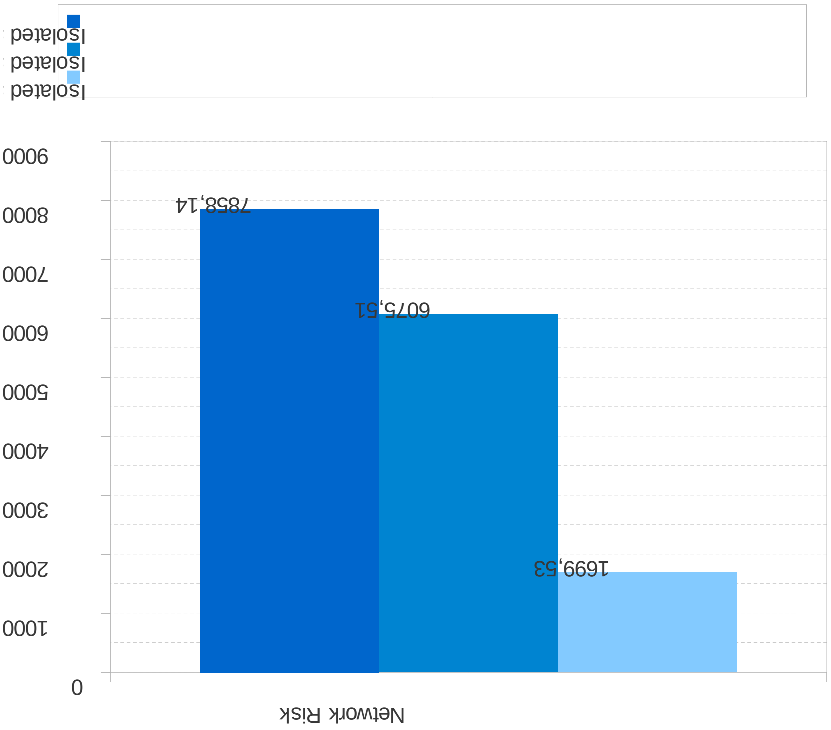


Figure 25: Comparison of Network Risk Values

It is clear that the isolated scenario using two ASN GWs without operational server vulnerabilities gives better results regarding the risk assessment simulations. The main observations that can be made about this scenario using the new topology with two ASN GWs are the following:

- Individual risk values remained unchanged or decreased except for IP servers because of a higher node value (and then a higher likelihood of occurrence of a threat on these nodes);
- Propagated risk values relevant to nodes at the AeroMACS core network have slightly increased whereas those relevant to nodes at the AeroMACS access service network have considerably decreased;
- The overall network risk value of the new topology is lower compared to the scenario results using a single ASN GW. This result shows that duplicating the ASN GWs and dispatching as much as poss ble the BSs among them reduces the propagated risk and consequently the overall network risk.

In the next simulation scenario, we focus on the end-to-end topology and analyze the evolution of the different types of risks.

4.4.3 END-TO-END AEROMACS SCENARIO

4.4.3.1 SIMULATION INPUTS

Table 29 summarizes the main simulation inputs we used in this integrated topology. With the addition of the Firewall and the Home agent nodes, several parameters have been modified such as number of connected nodes and security protections:

Node ID	Function value	Class value	# Connected nodes	# security protection	# vulnerabilities
Base Stations	1	1	3 / 4 / 5	8	1
Aircraft	0.7	1	1	2	0
Surface vehicles	0.7	1	1	2	0
AAA Server	0.3	1	2	4	20
DHCP Server	0.3	1	1	2	64
ASN Gateway 1	0.3	1	5	3	1
ASN Gateway 2	0.3	1	6	3	1
ATS Server	0.3	1	1	2	0
AOC Server	0.3	0.7	1	2	0
APC Server	0.3	0.1	1	2	0
Home Agent	1	1	2	1	4
Firewalls	1	1	2 / 3 / 6	1	1

Table 29: Simulation parameters (Integrated AeroMACS Topology)

4.4.3.2 NETWORK TOPOLOGY

As we can see in Figure 26, we added to the previous network topology (which contains two ASN GWs):

- A mobile IP Home Agent (HA) node that essentially handles the following tasks:
  - Registration of mobile stations;
  - Routing and forwarding of mobile station traffic.
- Firewalls (FW) to provide protection to:
  - ASN GWs at the entry of the AeroMACS ASN;
  - Operational and IP servers;
- The Home Agent.

Note that with the introduction of the HA to support IP mobility, the data flow exchanges have completely been reevaluated mainly because of the mobile IP subscriber (could be an aircraft of a surface vehicle) registration process as it follows:

1. The ASN GW sends the subscriber registration request from the mobile station to the mobile IP HA. The sought ASN GW is obviously the one connected to concerned mobile stations;

2. HA requests that the AAA server (which is now directly connected to the HA node) send the cryptographic keys for the Mobile IP session. The HA announces to the AAA server that it would like to source IP session-based accounting messages;
3. The AAA server agrees to use IP session-based accounting, provides the requested cryptographic keys, and sends the AAA-Session-ID for this session;
4. The HA replies to the Mobile IP registration request.

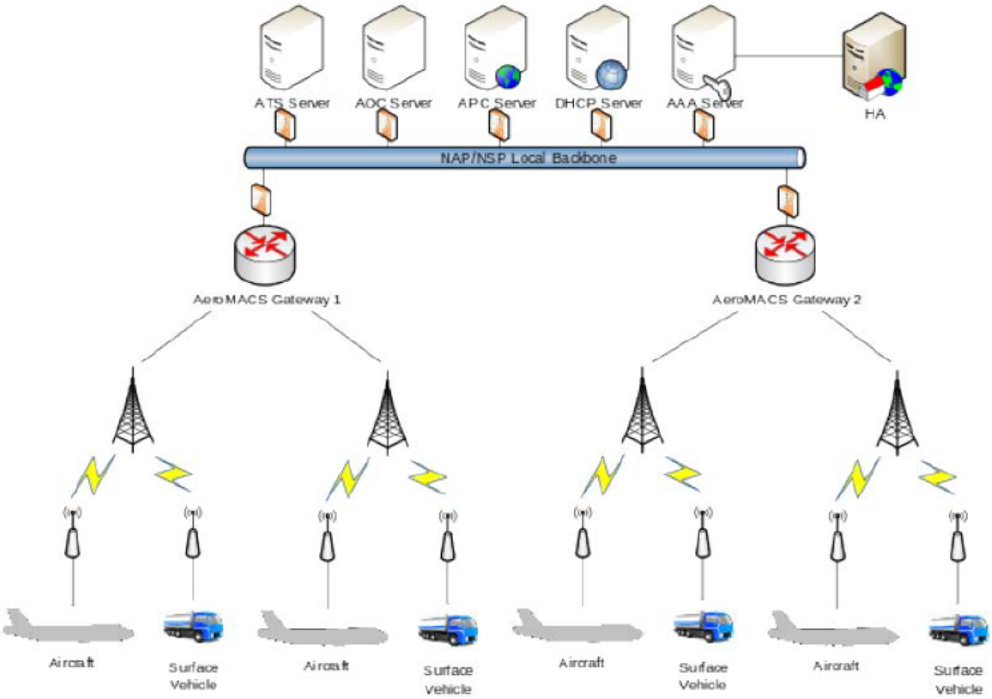


Figure 26: Integrated AeroMACS Network Topology

Note that the network topology provided in Figure 26 has been provided to match as close as possible the WiMAX end-to-end network model provided by the WiMAX Forum Network Working Group (NWG) as shown in Figure 27:

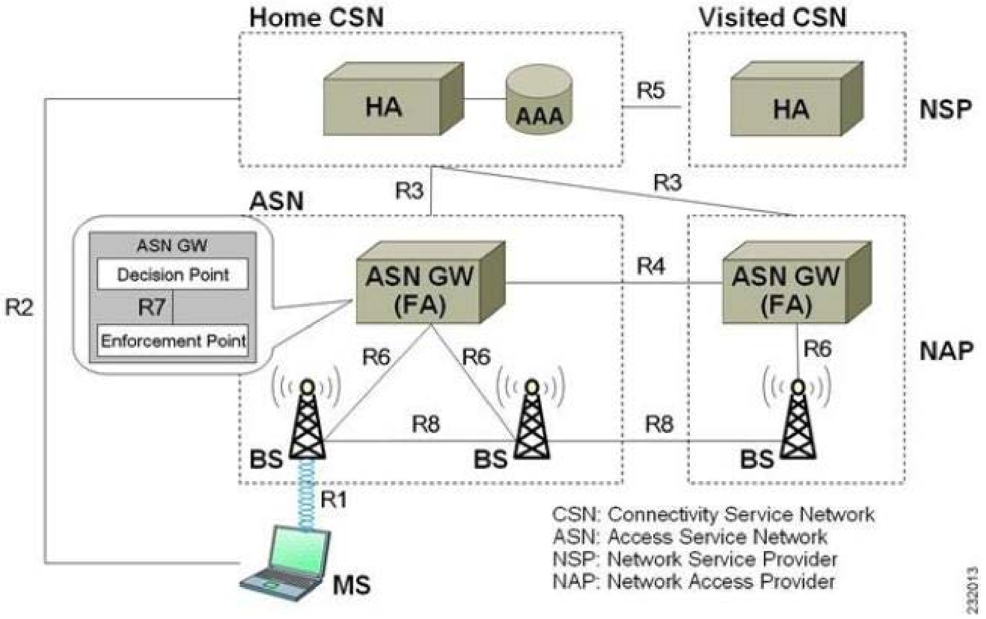


Figure 27: WiMAX Forum NWG end-to-end Network Model

4.4.3.3 VULNERABILITY STATISTICS

Table 30 shows the updated vulnerability CVSS statistics of the integrated network topology:

CVSS score	Number of total vulnerabilities	Percentage
[0,1]	0	0%
[1,2]	0	0%
[2,3]	0	0%
[3,4]	0	0%
[4,5]	2	1.980%
[5,6]	9	8.910%
[6,7]	2	1.980%
[7,8]	22	21.782%
[8,9]	0	0%
[9,10]	66	65.346%
Total	**94**	**-**
Average score	**8.651**	

Table 30: Updated Vulnerability CVSS statistics (Integrated Network topology)

The CVSS distribution is not really very different from the one presented in the previous scenario: there are few vulnerabilities added to the final statistics (*i.e.* 1 vulnerability per Firewall and 4 for the HA) which made the distribution more balanced, mainly between the highest CVSS score ranges (namely [8,9] and [9, 10]). A Comparison between the CVSS score distributions in all simulation scenarios is presented in Figure 28:

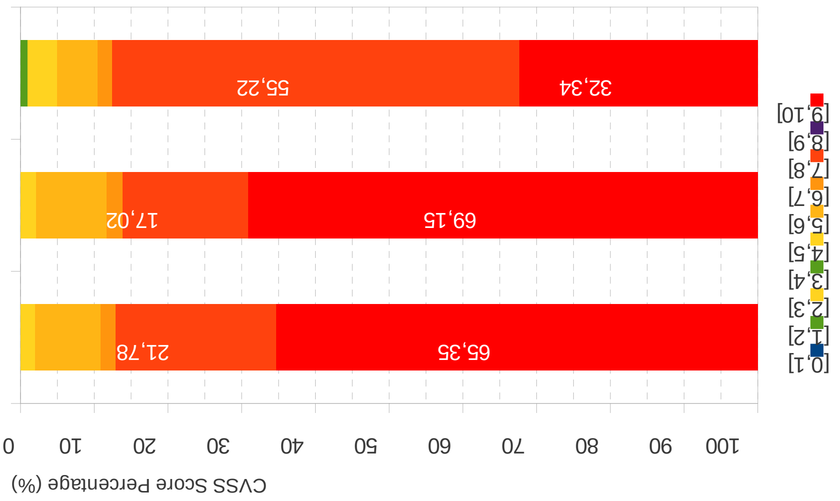


Figure 28: Final Comparison of CVSS Scores Distribution

The total number of vulnerabilities has naturally increased with the addition of the HA and Firewalls as shown in Figure 29:

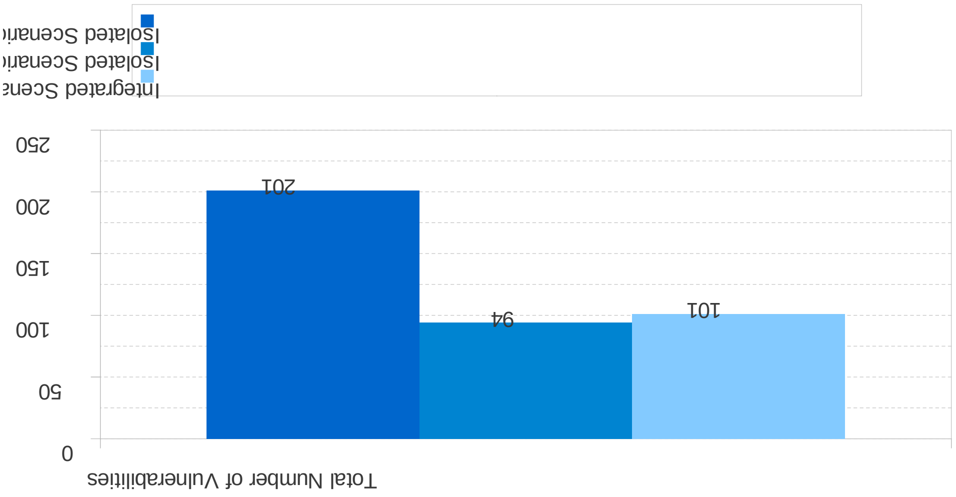


Figure 29: Final Comparison of Total Number of Vulnerabilities

The results are quite expected and relevant to the assumptions made in each scenario. However, the most interesting part is probably the comparison between the average CVSS scores which seems to evolve at the opposite of the total number of vulnerabilities: when the total number of vulnerabilities increases, the average CVSS score is likely decreasing as we can see in the results presented in Figure 30:

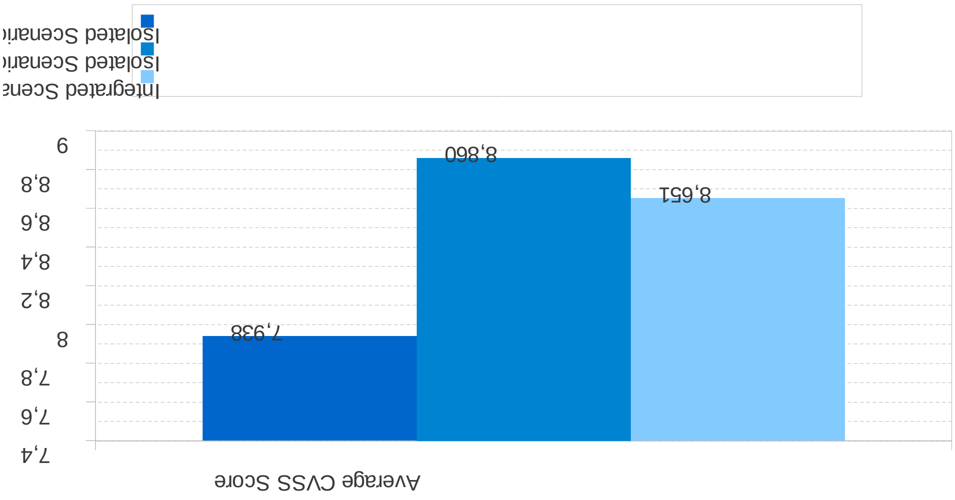


Figure 30 : Final Comparison of Average CVSS Score

This result is important as it helps the security managers choosing the adequate COTS products when it comes to implement their solution and designing the network. In the next sections, we analyze the final individual, propagated, and network risk results, and compare them to the previous scenarios.

4.4.3.4 INDIVIDUAL RISK RESULTS

As presented in Table 31, the individual risk results are practically the apparition of the HA and Firewalls, but also values relevant to nodes for which the node connectivity or the security protection parameter has changed (taken into account respectively in the value of the node and the likelihood of occurrence of a threat):

Node ID	Individual risk
Base stations (1 to 6)	0.23
Base stations 7 and 8	0.3
Base station 9	0.38
Aircraft (all)	0
Vehicle (all)	0
ASN Gateway 1	0.24
ASN Gateway 2	0.18
DHCP server	12.99

AAA server	3.07
ATS server	0
AOC server	0
APC server	0
Home Agent	1.88
Firewall 1	3.9
Firewalls (2 to 6)	5.85
Firewalls 7 and 8	11.7

Table 31: Updated Individual Risk Values (Integrated Scenario)

The nodes in the AeroMACS access service network have not been impacted by the addition of the new nodes, except the ASN Gateways protected by a firewall at the entry of the sub-network. However, all nodes in the AeroMACS CSN have either the number of security protections increased (because of the addition of the firewalls), or the number of connected nodes decreased. Firewalls do not have the same individual risk values because they are connected to the same nodes (depending where there are deployed and what node they protect).

Nevertheless, the DHCP server remains the most vulnerable node in the network mainly because of its high and critical COTS vulnerabilities. The individual risk values for the ASN Gateways have also decreased because their lower value in this scenario (connected to a lower number of nodes compared to the previous scenarios. Unlike the propagated or the network risk, it is useless here to compare the values between the different nodes because individual risks characterize the node itself, and are not related to the topological assumptions made in each simulation. However, the individual risks slightly vary, depending on the connected nodes.

Comparison is more relevant for propagated and network risk results where the addition of the firewalls is going to reduce the data flow exchanges between connected nodes (and consequently the likelihood of propagation of threats between them). The node connectivity has been also impacted because of the deployment of Firewalls at the entry of the AeroMACS access service network: in this way, ASN GWs are connected to a lower number of nodes and should have their propagated risk values decreased.

4.4.3.5 PROPAGATED RISK RESULTS

As expected, adding the Firewalls to the integrated AeroMACS topology has the advantage to get lower propagated risk values for the connected nodes as shown in the following table:

Node	Propagated risk
Base stations (1 to 4)	2.429
Base stations 5 and 6	2.576
Base stations 7 and 8	5.587
Base station 9	5.911
Aircraft (1 to 4)	0.093
Aircraft 5 and 6	0.095
Aircraft (7 to 12)	0.121
Vehicle (1 to 6)	0.093

Vehicles 7 and 8	0.121
Vehicles 9 and 10	0.394
ASN Gateway 1	87.225
ASN Gateway 2	79.452
DHCP server	0.341
AAA server	0.215
ATS server	0.056
AOC server	0.221
APC server	0.008
Home Agent	0.216
Firewall 1	0.015
Firewalls (2 to 6)	15.120
Firewalls 7 and 8	45.781

Table 32: Updated Propagated risk values (Integrated Scenario)

The most important part here is obviously the decrease of the ASN Gateway propagated risk values, which are no more the points of failure of the integrated topology. Indeed, the addition of the firewalls changed completely the connectivity between nodes. In one hand, Firewalls are deployed now between the servers and the ASN Gateways, reducing the connectivity from 9 and 10 to respectively 5 and 6. In the other hand, data flows are reduced, inducing a lower likelihood of propagated between nodes.

4.4.3.6 NODE AND NETWORK RISK RESULTS

The following table resumes the final node risk results for the integrated AeroMACS scenario:

Node	**Propagated risk**
Base stations (1 to 4)	2.429
Base stations 5 and 6	2.576
Base stations 7 and 8	5.587
Base station 9	5.911
Aircraft (1 to 4)	0.093
Aircraft 5 and 6	0.095
Aircraft (7 to 12)	0.121
Vehicle (1 to 6)	0.093
Vehicles 7 and 8	0.121
Vehicles 9 and 10	0.394
ASN Gateway 1	87.225
ASN Gateway 2	79.452

DHCP server	0.341
AAA server	0.215
ATS server	0.056
AOC server	0.221
APC server	0.008
Home Agent	0.216
Firewall 1	0.015
Firewalls (2 to 6)	15.120
Firewalls 7 and 8	44.781

Table 33: Updated Network Risk Values (Integrated Scenario)

As both the individual and propagated risk values decreased, so do the node risk for all nodes. Obviously, the resulting overall network risk is lower in this scenario compared to all the previous scenarios. The network results are clearly better in the integrated scenario as depicted in Figure 31:

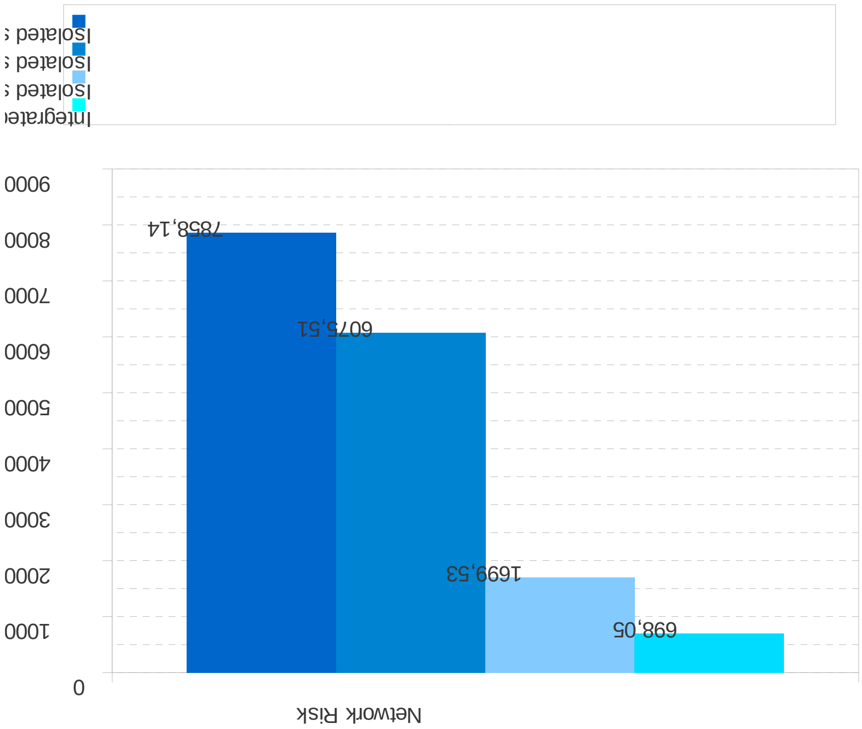


Figure 31: Final Comparison of Network Risk Values

Also, the ASN GW contribution in the network risk is now more balanced than in the previous scenario as shown in figure:

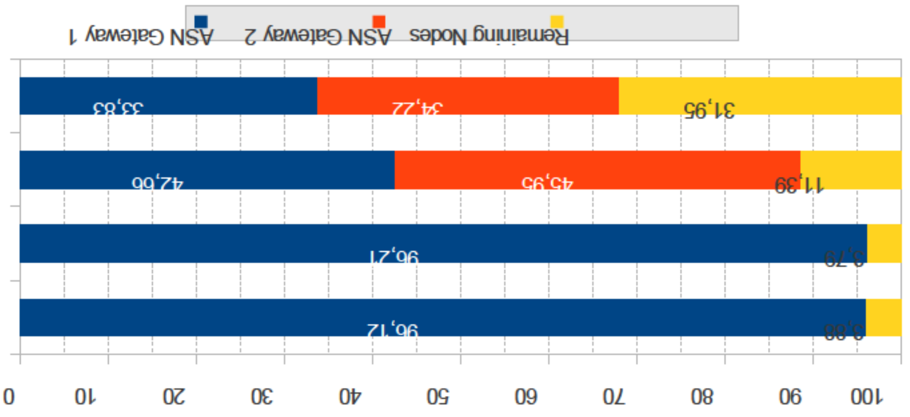


Figure 32: Final Comparison of the Percentage of Network Risk per Node Risk

In conclusion, this figure summarizes the approach we had in our work and in the simulation campaign: at each step, we tried to enhance the results by making the adequate assumptions and by learning what should be learnt from the previous simulation results, using the risk methodology as a decision making tool. It was quite useful to reduce the network risk from 7858.14 (first scenario) to 698.05 (last scenario), showing that our predictions, guidance, and assumptions were rightly done.

4.4.3.7 FINAL GUIDANCES

The risk propagation approach we relied on in this study shows that recommendations made after the first simulation campaign (i.e. the isolated scenario – with operational server vulnerabilities) are justified and effective. The network risk has been divided by a factor of 11, which is a significant and substantial gain in term of security. The guidance's we made in section 4.4.1.8 remain obviously effective and applicable. However, the duplication of the GW seems to have the heavier impact on the performances. The number of GWs to be deployed should be considered according to the network size and the overall number of connected nodes (BS, aircraft, surface vehicles). COTS products should be also chosen wisely, and a survey of the related vulnerabilities should be conducted uninterruptedly. Firewalls are also the best ways to avoid unwanted risk propagation between nodes, which is the main reason for high-risk levels measured in the first simulation.

5 References

[1] C. J. Alberts and A. J. Dorofee, Managing Information Security Risks: The OCTAVE Approach. 2002.

[2] DCSSI, “EBIOS : Introduction, démarche, techniques, outillage.” 2004.

[3] ISO, “ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation.” 1999.

[4] ISO, “ISO/IEC 27001: Information Technology, security techniques, information security management systems requirements.” 2005.

[5] ISO, “ISO/IEC 27005: Information Technology, Information Security Techniques, Information Security Risk Management.” 2008.

[6] M. L. Olive, R. T. Oishi, and S. Arentz, “Commercial Aircraft Information Security : an Overview of Arinc Report 811,” in 25th Digital Avionics Systems Conference, 2006 IEEE/AIAA, 2006, pp. 1–12.

[7] S. P. Bennett and M. P. Kailay, “An application of qualitative risk analysis to computer security for the commercial sector,” in Proc. Eighth Annual Computer Security Applications Conf., 1992, pp. 64–73.

[8] Microsoft, “The Security Risk Management Guide.” 2004.

[9] A. Barth, B. I. P. Rubinstein, M. Sundararajan, J. C. Mitchell, D. X. Song, and P. L. Bartlett, “A Learning-Based Approach to Reactive Security,” CoRR, vol. abs/0912.1, 2009.

[10] J. M. Wing, “Scenario Graphs Applied to Network Security,” in Information Assurance, Burlington: Morgan Kaufmann, 2008.

[11] G. Lao and L. Wang, “The Quantification Management of Information Security Risk,” in Proc. 4th Int. Conf. Wireless Communications, Networking and Mobile Computing WiCOM '08, 2008, pp. 1–4.

[12] X. Chen and Q. Zheng, “Quantitative Hierarchical Threat Evaluation Model for Network Security,” Journal of Software, vol. 17, no. 4, pp. pp.885–897, Apr. 2006.

[13] Y. Danfeng, Y. Fangchun, and L. Yu, “Service-based quantitative calculation of risk for NGN,” in Proc. 2nd IEEE Int. Conf. Broadband Network & Multimedia Technology IC-BNMT '09, 2009, pp. 306–310.

[14] R. Huang, D. Yan, and F. Yang, “Research of security metric architecture for Next Generation Network,” in Network Infrastructure and Digital Content, 2009. IC-NIDC 2009. IEEE International Conference on, 2009, pp. 207–212.

[15] T. Yongli, X. Guoai, and Y. Yixian, “Information Security Management Measurement Model based on AHP,” Journal of Liaoning Technical University, vol. 27, 2008.

[16] M. S. Ahmed, E. Al-Shaer, and L. Khan, “A Novel Quantitative Approach For Measuring Network Security,” in Proc. INFOCOM 2008. The 27th Conf. Computer Communications. IEEE, 2008, pp. 1957–1965.

[17] Q. Meng, M. H. Dong, Y. Li, and Z. W. Ming, “Network Security Analysis Model based on Logic Exploitation Graph,” in Computer Engineering, 2009, vol. 9, pp. 147–149.

[18] L. Jing, “Risk Evaluation Process Model of Information Security,” in Proc. Int. Conf. Measuring Technology and Mechatronics Automation ICMTMA '09, 2009, vol. 2, pp. 321–324.

[19] S. S. Yau and X. Zhang, “Computer network intrusion detection, assessment and prevention based on security dependency relation,” in Proc. Twenty-Third Annual Int. Computer Software and Applications Conf. COMPSAC '99, 1999, pp. 86–91.

[20] Y.-Z. Zhang, B.-X. Fang, and X.-C. Yun, “A risk assessment approach for network information system,” in Machine Learning and Cybernetics, 2004. Proceedings of 2004 International Conference on, 2004, vol. 5, pp. 2949 – 2952 vol.5.

[21] H. Li, G. Fan, and J. Qiu, “GKDA: A group-based key distribution algorithm for WiMAX MBS security,” Advances in Multimedia Information Processing, pp. 310–318, 2006.

[22] Y. T’Joens, C. Hublet, and P. D. Schr jver, “DHCP reconfigure extension,” no. 3203. IETF, Dec-2001.

[23] C. Perkins, “IP Mobility Support for IPv4,” no. 3344. IETF, Aug-2002.

[24] ETSI, “Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis.” 2003.

[25] C. Perkins, “IP Mobility Support,” no. 2002. IETF, Oct-1996.

[26] P. Eronen, T. Hiller, and G. Zorn, “Diameter Extensible Authentication Protocol (EAP) Application,” no. 4072. IETF, Aug-2005.

[27] C. Rigney, S. Willens, A. Rubens, and W. Simpson, “Remote Authentication Dial In User Service (RADIUS),” no. 2865. IETF, Jun-2000.

[28] B. Aboba and P. Calhoun, “RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP),” no. 3579. IETF, Sep-2003.

[29] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, and A. Sastry, “The COPS (Common Open Policy Service) Protocol,” no. 2748. IETF, Jan-2000.

[30] J. D. Case, M. Fedor, M. L. Schoffstall, and J. Davin, “Simple Network Management Protocol (SNMP),” no. 1157. IETF, May-1990.

[31] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, “The Kerberos Network Authentication Service (V5),” no. 4120. IETF, Jul-2005.

[32] B. Lloyd and W. Simpson, “PPP Authentication Protocols,” no. 1334. IETF, Oct-1992.

[33] W. Simpson, “PPP Challenge Handshake Authentication Protocol (CHAP),” no. 1994. IETF, Aug-1996.

[34] D. Simon, B. Aboba, and R. Hurst, “The EAP-TLS Authentication Protocol,” no. 5216. IETF, Mar-2008.

[35] J. Arkko and H. Haverinen, “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA),” no. 4187. IETF, Jan-2006.

[36] P. Funk and S. Blake-Wilson, “Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0),” no. 5281. IETF, Aug-2008.

[37] C. Rigney, “RADIUS Accounting,” no. 2139. IETF, Apr-1997.

[38] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, and B. Palter, “Layer Two Tunneling Protocol ``L2TP'',” no. 2661. IETF, Aug-1999.

[39] S. Krishnan, D. Thaler, and J. Hoagland, “Security Concerns with IP Tunneling,” no. 6169. IETF, Apr-2011.

[40] [16] K. Zeilenga, “Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map,” no. 4510. IETF, Jun-2006.

[41] W. Forum, “Network Architecture Stage 3: Detailed Protocols and Procedures,” vol. 05, 2010.

[42] Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. H. Drielsma, P. C. Heam, J. Mantovani, S. Modersheim, D. von Oheimb, M. Rusinowitch, J. S. Santiago, M. Turuani, and L. Vigano, “The AVISPA Tool for the automated validation of internet security protocols and applications,” in *Proceedings of CAV 2005: 17th International Conference on Computer Aided Verification*, 2005.

[43] R. M. Needham and M. D. Schroeder, “Using encryption for authentication in large networks of computers,” *Commun. ACM*, vol. 21, no. 12, pp. 993–999, Dec. 1978.

[44] G. Lowe, “An attack on the Needham-Schroeder public-key authentication protocol,” *Information Processing Letters*, vol. 56, no. 3, pp. 131–133, 1995.

[45] M. Burrows, M. Abadi, and R. Needham, “A logic of authentication,” *ACM TRANSACTIONS ON COMPUTER SYSTEMS*, vol. 8, pp. 18–36, 1990.

[46] Y. Chevalier, L. Compagna, J. Cuellar, P. H. Drielsma, J. Mantovani, S. Modersheim, and L. Vigneron, “A High Level Protocol Specification Language for Industrial Security-Sensitive Protocols,” in *Austrian Computer Society*, 2004.

[47] D. Basin, S. Modersheim, and L. Vigano, “Technical Report No. 450 OFMC: A Symbolic Model-Checker for Security Protocols.” 2004.

[48] D. A. Basin, “Lazy Infinite-State Analysis of Security Protocols,” in *Proceedings of the International Exhibition and Congress on Secure Networking - CQRE (Secure) ’99*, 1999, pp. 30–42.

[49] A. Armando and L. Compagna, “SATMC: A SAT-Based Model Checker for Security Protocols,” in *Logics in Artificial Intelligence*, 2004, pp. 730–733.

[50] O. K. Boichut Y. P.-C. Heam and F. Oehl, “Improvements on the Genet and Klay Technique to Automatically Verify Security Protocols,” in *In Proceedings of Int. Ws. on Automated Verification of Infinite-State Systems (AVIS’2004), joint to ETAPS'04, Barcelona (Spain)*, 2004.

[51] V. Fajardo, Ed., J. Arkko, J. Loughney, and G. Zorn, Ed., « Diameter Base Protocol », no. 6733, IETF, October 2012.

[52] M. Schiffman, “A Complete Guide to the Common Vulnerability Scoring System (CVSS).” Jun-2005.

[53] M. S. Ben Mahmoud, N. Larrieu, and A. Pirovano, “Quantitative risk assessment to enhance aeromacs security in SESAR,” in *2012 Integrated Communications, Navigation and Surveillance Conference*, 2012, pp. C7–1–C7–15.

Appendix A Introduction to CVSS

CVE (Common Vulnerabilities and Exposures) is a dictionary of publicly known information security vulnerabilities and exposures. CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services. One of the most important component of CVE databases is the CVSS (Common Vulnerability Scoring System) which is a universal means to asset a vulnerability impact and help in finding the right countermeasures. It can be seen as an aggregation of several metrics and formulas to solve the problem of multiplicity and incompatibility between vulnerability scoring systems used in the IT industry as shown in Figure 33.

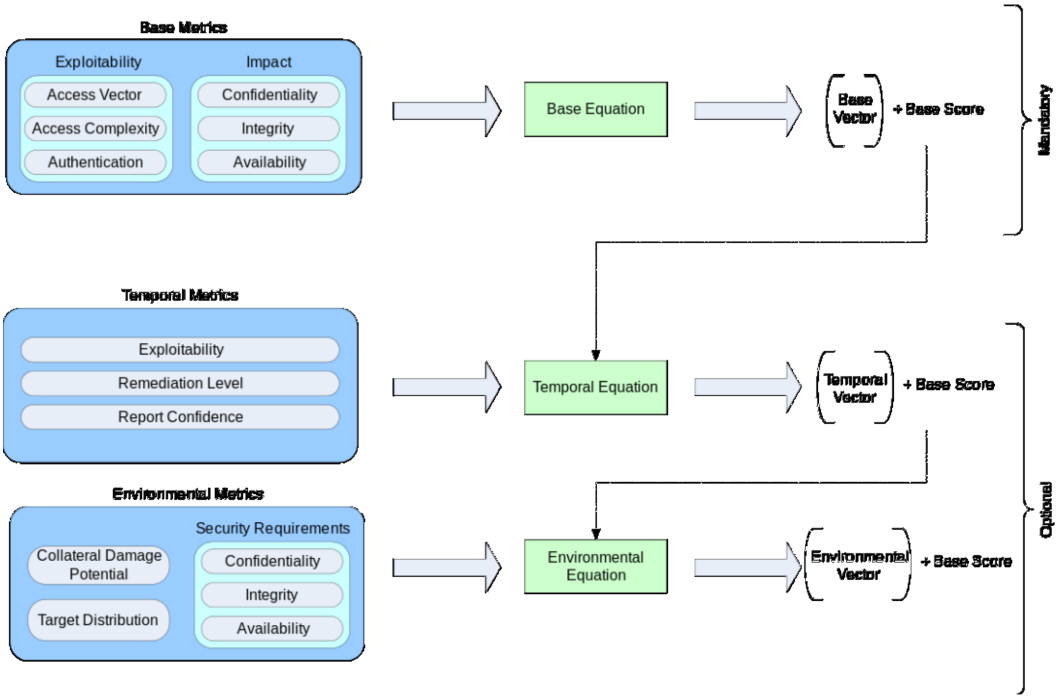


Figure 33: CVSS Metrics and Framework

Indeed, every day, several vulnerabilities are discovered for products and technologies used across world-wide networks and systems. All the actors involved in the use, development, or maintenance of such technologies have to be aware of those vulnerabilities and need a common way to communicate efficiently about them.

Historically, product vendors used own proprietary scoring systems to asset the severity of the discovered vulnerabilities, however past experience has shown that for the same vulnerability, and using different scoring systems by these actors, the impact is not the same which involves a significant uncertainty in the evaluation of vulnerability impacts.

The CVSS scoring system has been then developed to unique, open, usable, and understandable framework for all the IT actors. This framework relies on a set of metrics and equations designed to be complete, accurate, and easy to use by everyone as shown in Figure 33. For more details about CVSS, refer to [52].

Appendix B Risk Assessment Process Algorigram

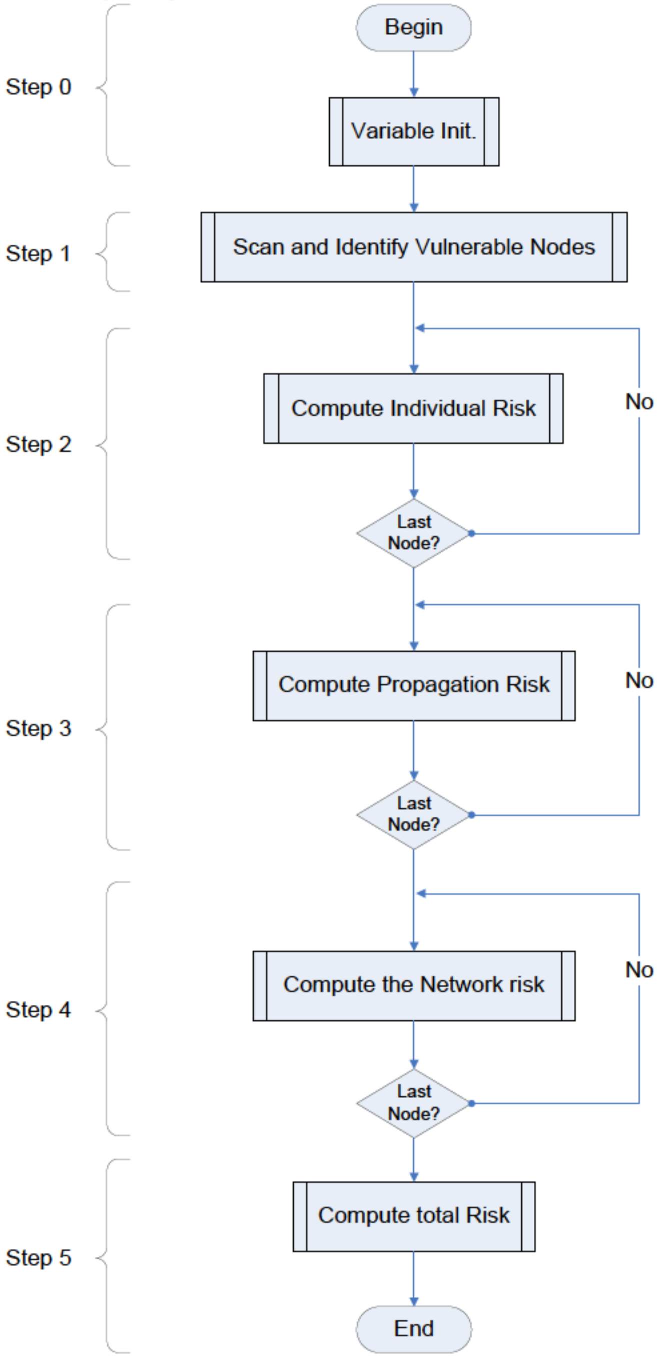


Figure 34: Risk Assessment Process Algorigram

Appendix C AAA RADIUS and DIAMETER implementation

The AAA (Authentication Authorization Accounting) term generally refers to a set of protocols, mechanisms, and architectures used to conduct three major services within a service provider network:

- Authentication is the operation of identifying the sender or the receiver involved in the communication and prove his identity when required by the other entity he is talking to ;
- Authorization is the operation to allow an entity to access/use network resources or services;
- Accounting is the operation of collecting data and statistics about the consumptions of resources by a user within the network.

These services are fundamental for an efficient and smooth operation of the network. AAA servers, which are supposed to ensure these services properly, should be then strongly protected and invulnerable against network attacks. Thus, security is a primary concern in AAA environments, particularly those related to the aviation when the AeroMACS protocol is used for airport communications. This annex provides a general overview of AAA along with a security comparison between two AAA protocols: RADIUS and DIAMETER. Two security analysis have been adopted: formal verification of both AAA protocols and vulnerability assessment using NVD and CVSS scores.

A.1 General Overview of AAA

The AAA term has initially appeared in the 90's within the IEEE (Institute of Electrical and Electronics Engineers) and IETF (Internet Engineering Task Force) working group (AAA WG)[12] in order to develop new AAA standards and applications.

A.1.1 AAA Architecture

With the increase of users of Internet services and subscribers, ISP's (Internet Service Provider) began to deploy more NAS's (Network Access Server). Basically, a NAS is an intermediate equipment that plays the role of an interface between the ASN (Access Service Network) and the CSN (Connectivity Service Network). It could be a router, a terminal server, or a gateway. As the number of these NAS's was increasing day by day, ISP's tried to alleviate their administration by using AAA servers. These servers provide three basic services, namely authentication, authorization, and accounting. Figure 35 shows a general AAA architecture that uses a NAS and a AAA server within the ISP network:

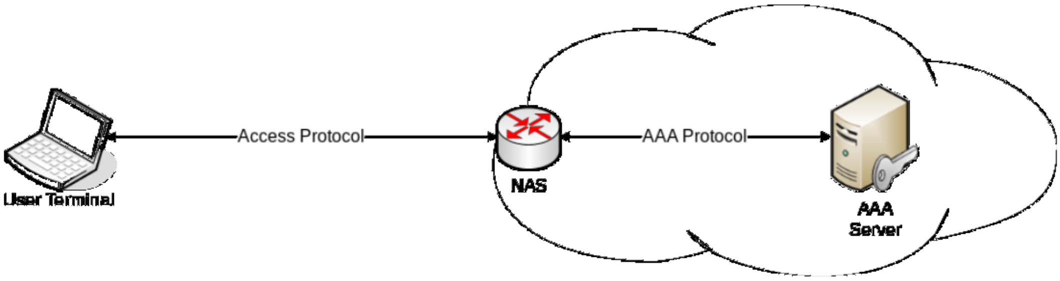


Figure 35: General AAA Architecture

When a user tries to access the ISP network, the NAS does the authentication and authorization for the user with the AAA server. Two protocols are used: an access protocol such as PPP (Point to Point Protocol) between the user terminal and the NAS, and a AAA protocol between the NAS and the AAA server. When a

[12] http://tools.ietf.org/wg/aaa/

user is moving from an ISP network to another (*i.e.* mobility scenario), another AAA server is involved in the AAA operations as shown in Figure 36. Two networks are represented:

- The H-NSP (Home Network Service Provider) which is the home network of the user;
- The V-NSP (Visited Network Service Provider) which is the visited network in a roaming scenario.

The NAS could be for instance, a router, a gateway, or a WAP (Wireless Access Point), depending on the access protocol as described in Figure 35. Note that depending on the AAA protocol used within the V-NSP, the AAA client could be merged with the NAS. AAA clients could be:

- a relay agent routes the access request sent by the user;
- a redirection agent asks the AAA client to redirect the traffic to another IP address if the VAAA server IP address is no longer valid;
- a translation agent translates the access request sent by the user is the AAA server does not use the same AAA protocol as the AAA client.

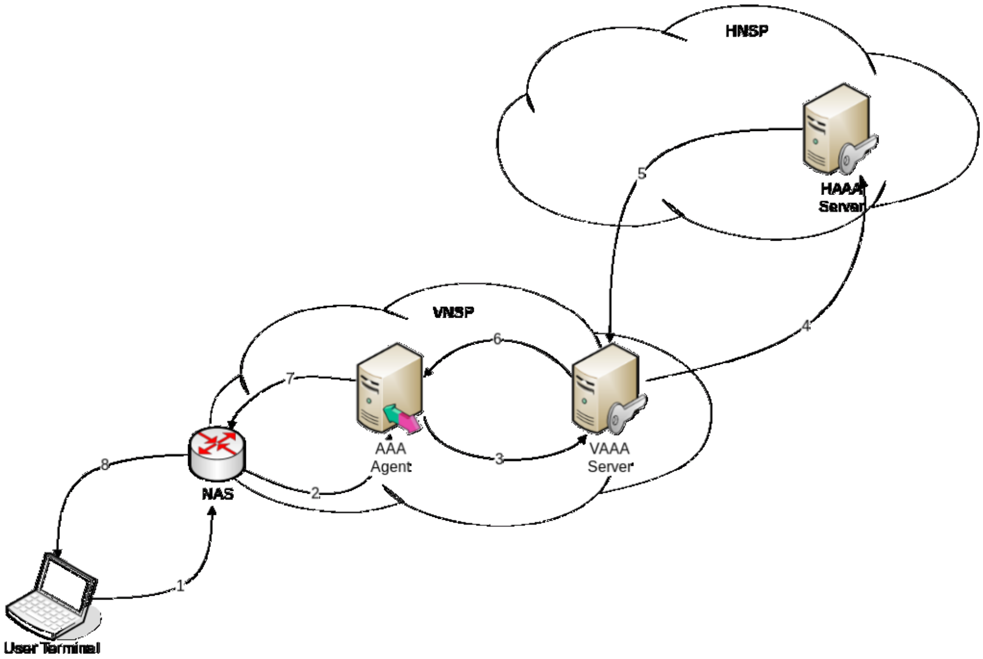


Figure 36: AAA Architecture Model for Mobility

When the user tries to access the V-NSP (message 1), his request is handled by the NAS then sent toward the HAAA server. After receiving the request (message 2), the AAA agent sends it the VAAA server (message 3), which is unable to authenticate the user as it does not registered in the V-NSP. Thus, it sends it the HAAA server (message 4), and then the access response is sent hop-by-hop to the user terminal (messages 5, 6, 7, and 8). Note that an EP (Enforcement Point) could be merged with the NAS. This EP is basically responsible for applying the control access techniques used in the V-NSP. Besides, IP mobility [25] is usually used in such mobility scenarios above access protocols (*e.g.* WiMAX, AeroMACS).

A.1.2 AAA Process Flow Chart

Figure 37 shows a high abstraction level data flow diagram of AAA operations:

- **Registration**: or *enrolment* is the process of subscr bing the entity to the services offered by the NSP. Several information are given to the subscriber for later use such as IP addresses (*e.g.* NAS, DNS server, DHCP server), CA (Certificate Authority) identity, supported cryptographic algorithms, access privileges for instance;
- **Initialization**: or *bootstrapping* is the process of starting the network entry. This process encompasses a set of actions such as the neighbour discovery or IP address configuration;
- **Authentication**: is the first security step of the AAA data flow chart. The authentication can be mutual (both the client and the server) or not (and in this case, the user is the only one to authenticate himself). AAA protocols do not provide an authentication protocol literally speaking, but they rather use an existing one. For a purpose of commodity and convenience, the EAP (Extens ble Authentication Protocol) [26] has been developed by the IETF to the AAA concept. As shown in Figure 37, it's a middleware layer between AAA protocol layer and the authentication method layer. The idea is to adapt any authentication method to the AAA context;

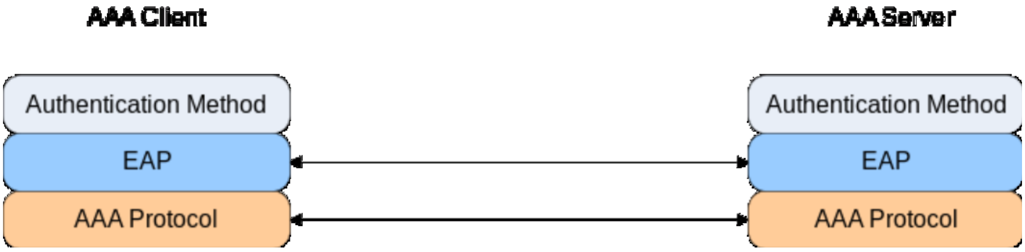


Figure 37: AAA Protocol Architecture Using EAP

- **Session Key Establishment**: is the process of creating a session key between the client and the NAS in order to secure later exchanges. A negotiation phase, could be needed between the client and the NAS, and uses security credentials established at the initialization phase;
- **Authorization**: when the client has been correctly identified and session keys generated, the AAA server sends the access privileges to the NAS which is responsible for applying and verifying them when the client tries to access to service resources;
- **Revocation**: if the client does not respect the NSP policy or rules established at the registration phase beforehand, he could be denied from accessing the NSP resources. This is generally done by revoking some identity credentials, such as his certificate, which is added to a CRL (Certificate Revocation List). Also, the NAS could simply apply some filtering rules on the data traffic generated by the client;
- **Authorized Session**: at this step, the client actually uses the services it is allowed to access by the NAS. His consumptions are monitored, registered, and sent by the NAS to the H-AAA server periodically (accounting phase). When the session is active, the NAS controls continuously the validity of the security credentials used by the client and asks for new ones if they have been misused, or have simply expired. *Tracing* is also part of the NAS role: the behaviour of the client is always monitored; the aim is to verify that access rules are respected and not violated by the user.

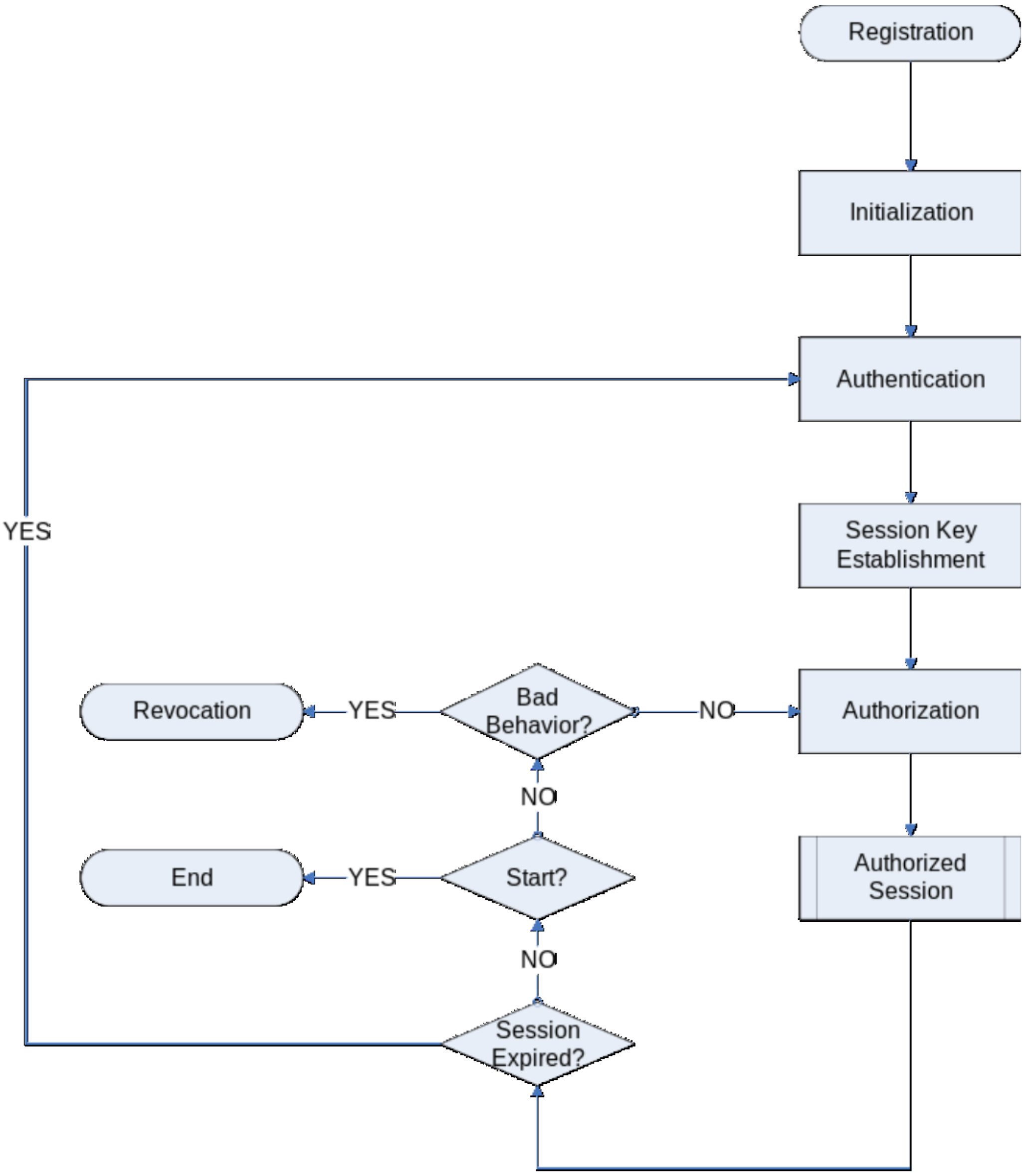


Figure 38: AAA Process Flow Chart

A.1.3 AAA Concepts

AAA components are very heterogeneous and differences between their roles have to be well understood. Figure 39 shows a taxonomy of AAA concepts, three main categories can be distinguished:

- **AAA Mechanisms**: are the methods to perform authentication, authorization, and accounting;
- **AAA Protocols**: specify the MSC (Message Sequence Chart) between the AAA client and the AAA server;
- **AAA Architectures**: refer to the interconnection and interworking between AAA network components.

A.2 AAA Mechanisms

AAA mechanisms are divided into three categories:

- **Authentication mechanisms**: the credentials used to make the entity authentication could be of different natures such as IP address, MAC (Medium Access Control) address, IMSI (Internet Mobile Subscriber Identity), or IMEI (International Mobile Equipment Identity) for instance, different authentication mechanisms classes exist:
  - ✓ Knowledge-based mechanisms;
  - ✓ Cryptography-based mechanisms;
  - ✓ Biometrics-based mechanisms;
  - ✓ Secure tokens-based mechanisms.
- **Authorization mechanisms**: As for authentication mechanisms, authorization mechanisms could be of different natures:
  - ✓ Authentication-based mechanisms which means that correct authentication of an entity implies its authorization to access the NSP services;
  - ✓ Credential-based mechanisms which mean that credentials initially negotiated as shown in Figure 38.
- **Accounting mechanisms**: covers either collection of data from monitoring systems or storage of these data into accounting records. Depending on the data structure used within the NSP network, those records are triggered and generated periodically according to one or several metrics (*e.g.* IP packets). In such a case, records are called IPDRs (IP Detail Record).

A.3 AAA Protocols

Several AAA protocols have been defined; the most relevant and world-wide used are those discussed within the IETF AAA WG, namely RADIUS (Remote Authentication Dial-In User Service) [27] [28] DIAMETER [26]. AAA Protocols could be categorized into two families:

- Protocols developed specifically for AAA context such as RADIUS and DIAMETER;
- Protocols developed for others purposes but could be used or adapted to the AAA context such as COPS (Common Open Policy Service) [29] SNMP (Simple Network Management Protocol) [30] or Kerberos [31] (these protocols are out of scope of this document).

If PPP is the data link technology used for the network access, several authentication protocols could be used, the most common are:

- PAP (PPP Password Authentication Protocol) [32];
- CHAP (PPP Challenge Handshake Authentication Protocol) [32];
- EAP which could itself rely on different authentication credentials:
  - ✓ EAP-TLS which is a device-based authentication using X.509 certificates [34];

- ✓ EAP-AKA which is a SIM Card [35] based authentication;
- ✓ EAP-TTLS, which is use both X.509 certificates and password [36].

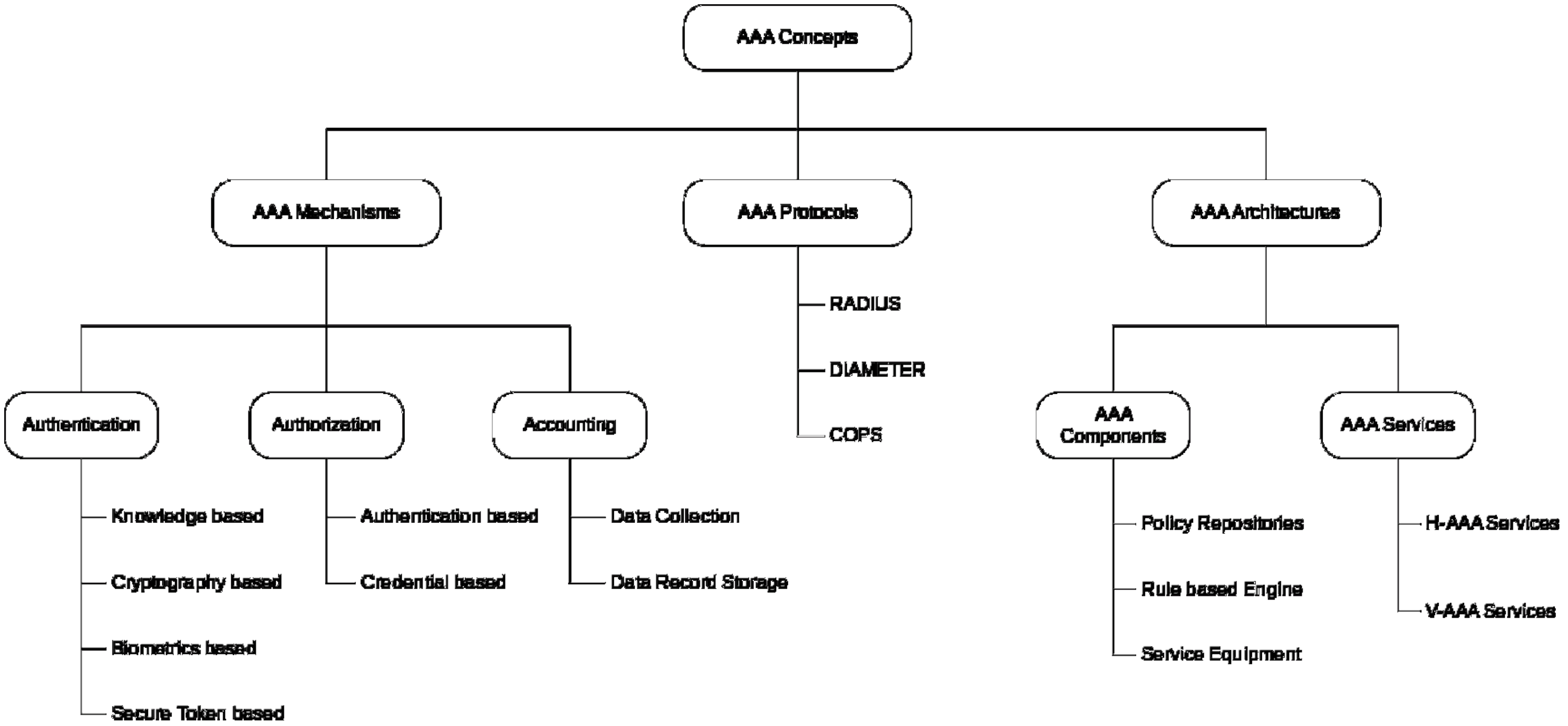

AAA Concepts
AAA Mechanisms
AAA Protocols
AAA Architectures
Authentication
Authorization
Accounting
RADIUS
DIAMETER
COPS
AAA Components
AAA Services
Knowledge based
Cryptography based
Biometrics based
Secure Token based
Authentication based
Credential based
Data Collection
Data Record Storage
Policy Repositories
Rule based Engine
Service Equipment
H-AAA Services
V-AAA Services

Figure 39: AAA Concepts Taxonomy

A.4 RADIUS

RADIUS is probably the most used AAA server in today networks. It has been originally designed to support dial-up connections, but over time, it has been adapted to several context and environments. From an architecture point of view, RADIUS is a pure client-server paradigm, meaning it relies on client requests and server responses to work. In a RADIUS-based AAA architecture, the NAS plays the role of the RADIUS client which make the authentication and authorization on behalf the user toward the RADIUS server. Those servers could also play the role of RADIUS clients toward other RADIUS servers (*i.e.* proxy clients). Messages exchanged between the RADIUS client and servers are authenticated using a pre-shared key and users password sent in those messages are encrypted. RADIUS messages carry AAA information encoded in type length value fields called attributes or AVPs (Attribute Value Pairs). AVPs contain several information such as IP addresses, user password, or user name. These AVPs can be defined by vendors selling RADIUS equipment.

Accounting was not initially planned as a RADIUS server, but it has been added later in protocol amendments [37]. The NAS forwards an ACCOUTING-REQUEST (with an AVP called Acct-Status-Type with a value equal to START) message to the RADIUS server as soon as the connection has been established. Then it begins accounting process by collecting information such as input/output packets, session lifetime, and session termination. When the session is finished, the NAS sends an ACCOUTING-REQUEST (Acct-Status-Type = STOP) message to the RADIUS server to finish the accounting process. RADIUS might also be used to establish VPNs (Virtual Private Networks) in order to enhance the network security. Tunnelling protocols such as L2TP (Layer 2 Tunnelling Protocol) [38] or IPSec (IP Security) [39] could be used to create tunnels through IP networks and carry PPP connections.

Figure 40 shows a AAA architecture similar to Figure 35 but adapted to the RADIUS protocol. The user asks the NAS that supports a RADIUS client to access the network services. Using the PPP protocol, the NAS collects the information needed by the RADIUS server (*e.g.* user name and password) and then forwards an encrypted ACCESS-REQUEST message using UDP[13] (User Diagram Protocol) to the server (authentication phase). Other AVPs may be added such as the NAS port ID or its IP address. Then, the RADIUS server checks the validity of these information using authentication mechanisms such as CHAP, EAP, PAP, or by comparing them with its own local database. Note also that these information could be possibly stored into external sources such as Active Directories or LDAP (Lightweight Directory Access Protocol) [40] servers.

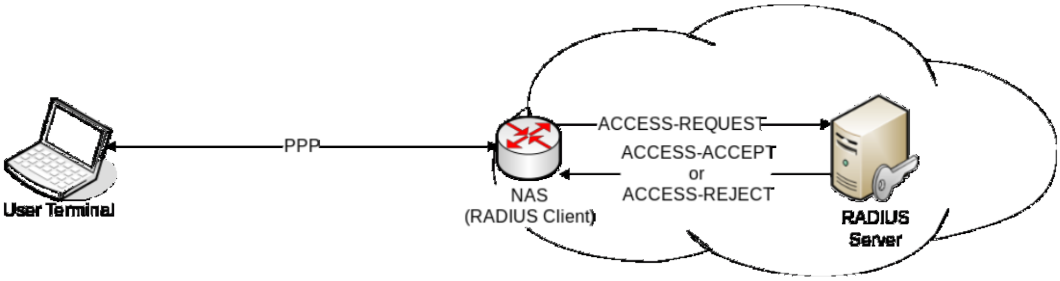


Figure 40: RADIUS AAA Architecture

If the users or the passwords are not recognized, the RADIUS server sends back an ACCESS-REJECT message to the NAS with an optional text field indicating the reason for the access failure (authorization

[13] RADIUS uses ports 1812 and 1813 respectively for authentication and accouting (or ports 1645 and 1646 for older versions of the protocol).

phase). The NAS then notifies the end user of the RADIUS server decision. If the user credentials are correct, an ACCESS-ACCEPT message is sent to the NAS along with a request for additional information about the user to complete the network connection such as a valid IP address for the end user (in this case an ACCESS-CHALLENGE message is sent). Each of these responses (*i.e.* ACCESS-ACCEPT, ACCESS-REJECT, ACCESS-CHALLENGE) could optionally contain a special attribute called "replay-message" in order to inform the NAS and the user about the reason for the acceptance, rejection or the additional challenge. Authorization attributes are also added such as the IP address to be given to the user (or an IP address pool to choose from), the session maximum lifetime, VLAN or QoS (Quality of Service) parameters.

The NAS sends then an ACCOUNTING-REQUEST in order to inform the server that the user is now connected. The RADIUS server sends back an ACCOUNTING-RESPONSE in order to indicate which metrics should be monitored (accounting phase). An ACCOUTING-REQUEST with the Acct-Status-Type=Interim-update is periodically sent to the server in order to monitor the current active session. When the session is finished, the NAS sends an ACCOUNTING-RESQUEST (STOP) to the server along with information collected in the accounting phase (e.g. input/output packets, input/output data, session lifetime, session termination conditions).

Figure 41 shows the RADIUS packet format:

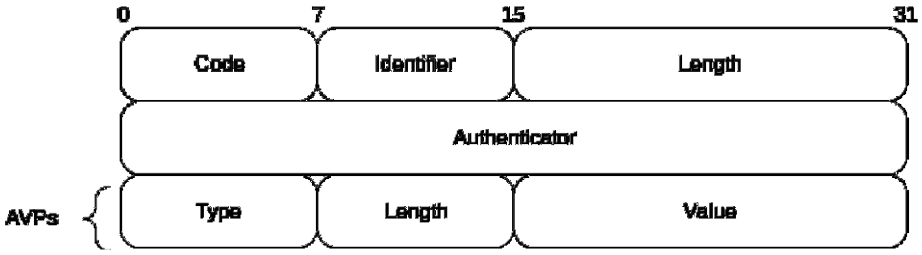


Figure 41: RADIUS Packet Format

The packet fields are:

- **Code** corresponds to the RADIUS request and response (1 Byte) as stated in Table 34:

Table 34: RADIUS Packet Fields

Code	Description
1	ACCESS-REQUEST
2	ACCESS-ACCEPT
3	ACCESS-REJECT
4	ACCOUNTING-ACCEPT
5	ACCOUNTING-RESPONSE
11	ACCESS-CHALLENGE
12	STATUS-SERVER
13	STATUS-CLIENT
255	RESERVED

- **Identifier** is used to compare the request and the response (1 Byte);
- **Length** is RADIUS packet length (2 Bytes);
- **Authenticator** corresponds to the value used to authenticate the RADIUS server response;
- **AVPs** are the attributes corresponding to the request or the response.

A.5 DIAMETER

DIAMETER is the successor of RADIUS and has been defined to mainly deal with RADIUS weaknesses (see section A.6.2.2 for more details about advantages and drawbacks of each AAA protocol). Indeed, RADIUS has been originally designed for small networks, which is, by now, out-of-date considering the wide networks and the heterogeneity of the used technologies and protocols. DIAMETER is then a lightweight and scalable P2P (Peer to Peer) AAA protocol. Indeed, unlike RADIUS, which is a client-server protocol, DIAMATER is a peer-based protocol, meaning every entity is a client and a server at the same time. The protocol relies on TCP (Transmission Control Protocol) (unlike RADIUS which uses UDP) or SCTP (Stream Control Transmission Protocol) and uses AVPs to exchange information between the DIAMETER peers. The DIAMETER protocol is continuously improved and currently it supports RADIUS-based peers, EAP, IP Mobility, etc.

DIAMETER has been improved over time to deal with RADIUS inherent limitations. Scalability is probably the most important improvement as RADIUS AVPs were initially limited to 255 Bytes. Beside, RADIUS component, such as a NAS RADIUS client, was unable to handle more than 255 messages before an acknowledgement was necessary. DIAMETER supports much larger AVPs length and uses a reliable transport protocol to establish the connection between the peers. It uses either TCP (Transmission Control Protocol) or SCTP (Stream Control Transmission Protocol), which are obviously more reliable than UDP, which is used by RADIUS. Besides, a DIAMETER server is able to send unsolicited commands to the client when needed (*e.g.* ask the NAS to perform additional accounting functions), which is impossible when RADIUS. The second purpose behind the design of DIAMETER is the support of mobility and roaming scenarios (see Figure 36). RADIUS has support for mobility (based on implicit possibility of forwarding requests). RADIUS mobility architectures rely on a network of trusted RADIUS servers by proxy chains. However, DIAMETER brings a more sophisticated support of mobility (*e.g.* discovery of DIAMETER peers, IP mobility). DIAMETER supports also CMS (Cryptographic Message Syntax) data within AVPs for security purposes. CMS are like SA (Security Association) in IPSec: they are established by two peers through agents in order to provide authentication, integrity, and confidentiality. Besides, CMSs are able to carry the X.509 certificates.

The DIAMETER packet format is presented in Figure 42:

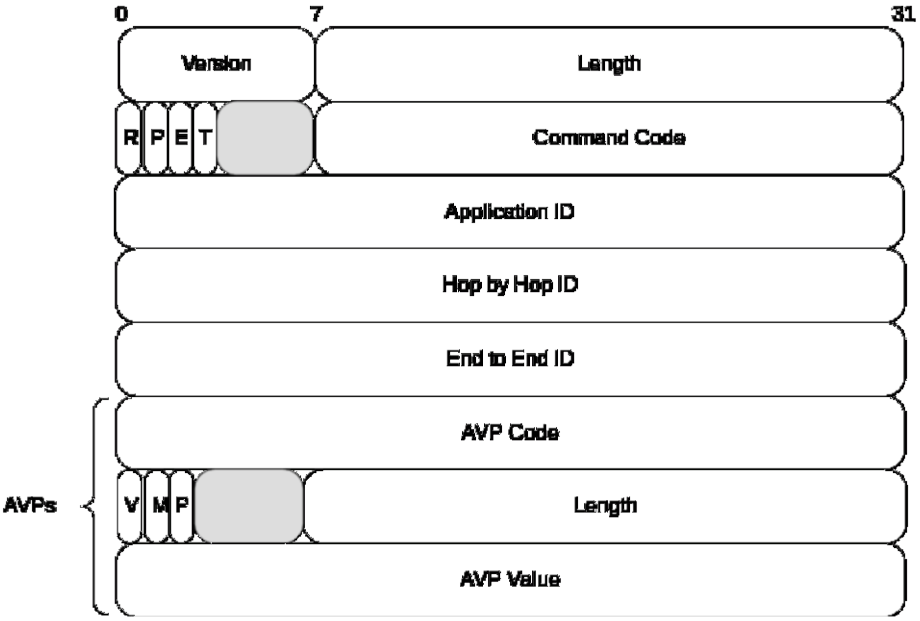


Figure 42: DIAMETER Packet format

the packet fields are:

- **Version** is the DIAMETER used version;
- **Length** is the length of the DIAMETER packet;
- The “**R**” bit (for Request) is set to 1 for a request message, otherwise it is set to 0;
- The “**P**” bit (for Proxiable) is set to 1 if the message is relayed or redirected;
- The “**E**” bit (for Error) is set to 1 if the message contains an error;
- The “**T**” bit (for retransmitting) is set to 1 for a retransmitted message.

As for the RADIUS protocol, each message is associated to a command, which is assigned to a specific code. For the AVP fields:

- The “**M**” bit (for mandatory) is set to 1 in order to indicate the necessity for AVP support;
- The “**V**” bit (for vendor specific) is set to 1 in order to indicate that the optional Vendor ID field is required;
- The “**P**” bit is set to 1 when encryption is needed.

For more details about the DIAMETER packet format and the dedicated RFC 4072 [26]

A.6 Comparison between RADIUS and DIAMETER Protocols

In this section, we provide a short comparison between the RADIUS and DIAMETER AAA protocols. Theoretically, Diameter is an improved extension of RADIUS and should provide better authentication, authorization, and accounting services. Despite several drawbacks such as a limited size of attribute data, a limited session control, a low fault tolerance because of UDP, and a lack of end-to-end security, RADIUS remains the worldwide AAA server that is used currently in the real world. In classical networks, Diameter is used mainly in the GSM telecommunication world, for IMS authorization policies. However, its use for authentication and accounting is currently limited outside the scope of GSM. Here are some examples that illustrate the current deployment of Diameter in the network market (and shows also the supremacy of RADIUS):

- DIAMETER is not supported in the Cisco IOS software[14], HP products and Juniper products. Indeed, the main use of Diameter today is somewhat more limited than originally envisioned. DIAMETER products are progressively growing, but the main use of the protocol is in the GSM world, for exchanging IMS (IP Multimedia Subsystem) authorization policies. Then deployments of DIAMETER for authentication and accounting is extremely limited, and currently there is no large-scale systems that use this protocol for authentication or accounting;
- For the same scalability and usability reasons, the American NSP SPRINT attempted to use DIAMETER for its WiMAX systems without success and resigned to replace all the DIAMETER systems by RADIUS;
- The WiMAX Forum allows the use of both RADIUS and Diameter AAA servers: « AAA **SHALL** support RADIUS and **MAY** support Diameter AAA protocols » [41] but RADIUS is strongly recommended;
- In aeronautical systems and networks, SITA is currently using RADIUS for gatelink.

The comparison between RADIUS and DIAMETER protocols is conducted upon two axes:

- A formal verification of RADIUS and DIAMETER security using the AVISPA tool [42]. This technique shows the logical inconsistencies leading to an attack. More details are given in section A.6.1;
- A vulnerability analysis of both AAA protocols based on statistics and exploits identified in public vulnerability databases (section A.6.2).

A.6.1 Formal Verification of RADIUS and DIAMETER Protocols

It has been shown in the past that security protocols can never be considered 100% safe even after many years of deployment. The best example is the Needham-Schroeder authentication protocol [43], which has been used in public and private networks for 16 years before Lowes discovered a security hole in the protocol specification [44].

A.6.1.1 Benefits from Formation Verification of Security Protocols

In order to make these protocols more robust and secure, security protocol verification techniques allow the designer to verify if the security specification actually reaches the security requirements fixed beforehand. Automatic tools provide systematic approaches to verify the security protocol properties without losing much time and being confronted to computation errors. Generally, these tools use two approaches:

- **Computational approaches**: rely on Turing machine-based intruder models. Security properties are considered as a string of bits and are verified regarding the computational resources used by the intruder to find the decryption key;
- **Formal method approaches**: assume that the intruder cannot conduct cryptanalysis attack like in computational approaches, meaning that they assume perfect cryptography in the verification process (*i.e.* the original message can only be decrypted if the intruder has the appropriate decryption key). Several formal model-checking tools have been provided to automate the verification procedure. Usually they use either the BAN (Burrows Abadi Neddham) logic [45], or a state exploration approach where all possible execution paths are reached and each visited state is tested regarding a set of preconditions. If security properties are not reached at a particular state, an exploit trace of the attack is built from the initial state to the vulnerable state. The verification process can be bounded (fixed and finite number of states and sessions) or unbounded (infinite number of users or sessions) depending on the purpose of the verification.

[14] http://www.cisco.com/en/US/products/ps6638/products_data_sheet09186a00804fe332.html

A.6.1.2 The AVISPA Formal Verification Tool

In order to verify the RADIUS and DIAMETER protocols, the formal automatic security analyser AVISPA is used. The formal verification procedure is divided into two steps:

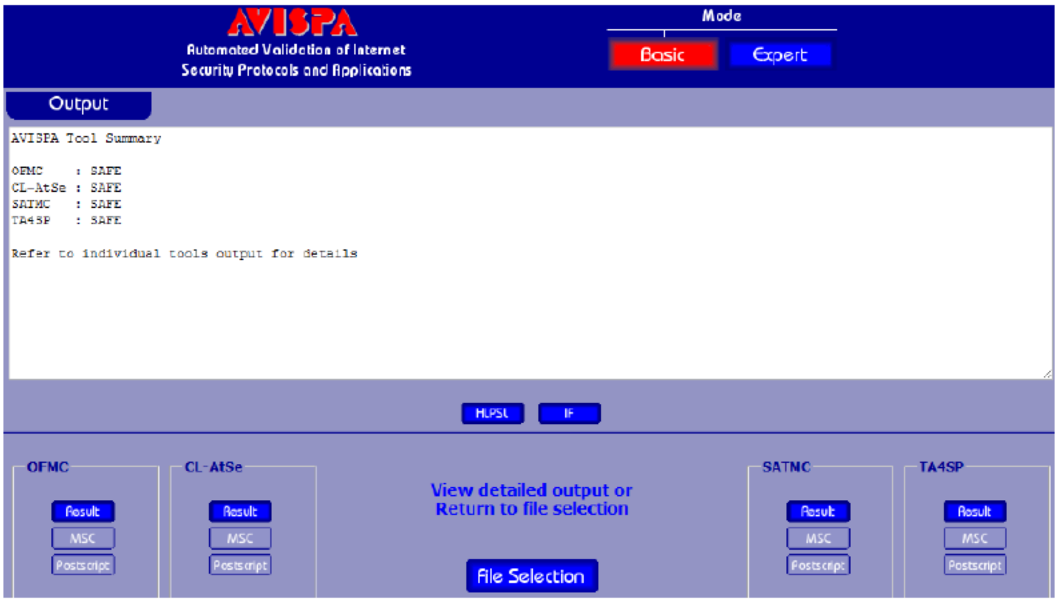
- **Protocol specification using high-level languages**: in this phase, a high level language is used, namely HLPSL (High Level Protocol Specification Language) [46] to specify the RADIUS and DIAMETER messages. This language offers a high level of abstraction and allows a very detailed specification of every security protocol aspects (*e.g.* roles, cryptographic operators, intruder models). Specifications are then automatically translated into a lower level language, named IF (Intermediate Format) using the HLPSL2IF translator;
- **Verification of RADIUS and DIAMETER specifications using the AVISPA back-ends**: in this step, the RADIUS and DIAMETER specifications are used by the AVISPA tool to check if the security requirements are respected or not. AVISPA uses 4 different verification back-ends. In software architecture, "*back-end*" is a generic term used to refer to programs called indirectly by users. In the case of AVISPA, these back-ends are formal checking model tools receiving the translated protocol specifications for security verification.

The AVISPA formal verification tool has many advantages, namely:

- It is freely and publicly available and provides a friendly GUI tool called SPAN (Security Protocol ANimator for AVISPA) which has been very useful in the intruder simulation;
- It is supported by 4 different back-ends, which provide several possibilities to verify one security protocol from different perspectives: OFMC (On the Fly Model Checker) [47], CL- Atse (Constraint Logic based Attack Searcher) [48], SATMC (SAT based Model Checker) [49], and TA4SP (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols) [50].

A.6.1.3 Formal Verification of DIAMETER and RADIUS Protocols

The RADIUS protocol has been verified according to RFC 2865 [27]. Results of the intrusion simulation are safe using the four AVISPA back-ends as shown in Figure 43:



AVISPA
Automated Validation of Internet Security Protocols and Applications
Mode
Basic
Expert
Output
HLPSL
IF
OFMC
CL-AtSe
SATMC
TA4SP
Result
MSC
Postscript
View detailed output or Return to file selection
File Selection

```
AVISPA Tool Summary

OFMC    : SAFE
CL-AtSe : SAFE
SATMC   : SAFE
TA4SP   : SAFE

Refer to individual tools output for details
```

Figure 43: AVISPA Backend Results for RADIUS

The DIAMETER protocol has been verified according to RFC 6733 [51]. The intrusion simulation has shown that a Man-in-the-middle attack is possible. The corresponding attack trace is the following:

```
I → mn: fa,fa
mn → I: fa,mn,aaah,{fa,mn,aaah}k mn aaah
i → mn: {fa,mn,aaah}k_mn_aaah,{{fa,mn,aaah}k_mn_aaah}(mn,aaah)
```

The intruder (denoted I) is able to forge a false encryption key and used to produce a message that is unreadable by the mobile node (denoted mn) since he knows both mobile node and aaah agent names. Nevertheless, this vulnerability has been rapidly patched and corrected before implementation as shown later in the vulnerability statistics.

A.6.2 Vulnerability Statistics

A.6.2.1 RADIUS Vulnerability Assessments

Several implementations of the RADIUS protocol have been provided worldwide. According to the NVD database, it seems that depending on the RADIUS implementation or the product vendor, the number of vulnerabilities varies between 1 and 21.

From all the implementation provided by industry vendors, FreeRADIUS is the most used RADIUS server ever. On the official website, FreeRADIUS is presented as *"...the most widely deployed RADIUS server in the world. It is the basis for multiple commercial offerings. It supplies the AAA needs of many Fortune 500 companies and Tier 1 ISPs. It is also widely used in the academic community. The server is fast, feature-rich, modular, and scalable."* Consequently, the RADIUS vulnerability analysis is based on FreeRADIUS CVE inputs.

Figure 44 and Figure 45 show the distribution of freeRADIUS vulnerabilities by type and the vulnerability distribution by CVSS scores. As shown in these results, DoS attacks are the most represented type of attacks. CVSS scores are not really high as shown in the vulnerability distr bution by CVSS scores (only one vulnerability ranked in [9 – 10]). Then, the distribution of the CVSS score is more balanced on low scores than high scores, which means that the weighted average CVSS score will have a medium criticality. The weighted average CVSS score is a good indicator of the security related to an IT product as it combines all the vulnerabilities (meaning their total number) and their relative CVSS scores.

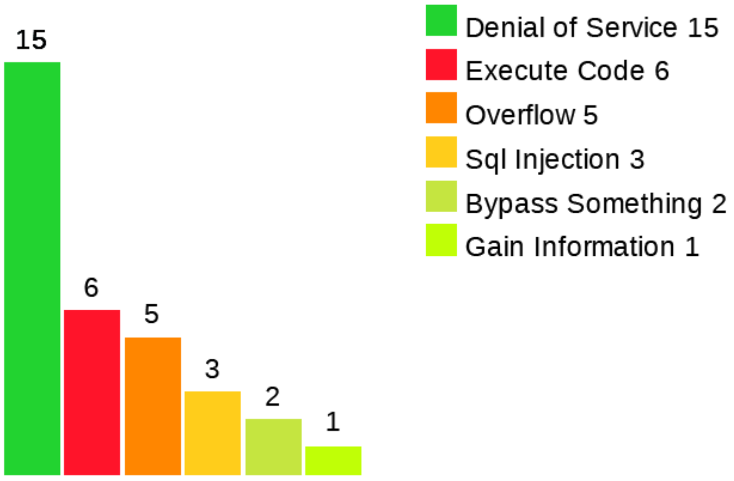


Figure 44: FreeRADIUS Vulnerabilities by Type

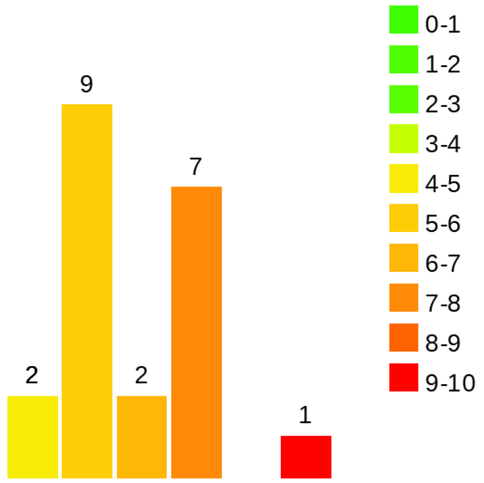


Figure 45: Vulnerability Distribution by CVSS Scores

Table 35 gives a deeper insight of FreeRADIUS vulnerabilities and their distribution using CVSS score. The weighted average CVSS score is equal to 6.9, which is considered as a medium score.

Table 35: Distribution of all FreeRADIUS Vulnerabilities by CVSS Scores

CVSS Score	Number of Vulnerabilities	Percentage (%)
[0 - 1]	0	0 %
[1 - 2]	0	0 %
[2 - 3]	0	0 %
[3 - 4]	0	0 %
[4 - 5]	2	9.5 %
[5 - 6]	9	42.9 %
[6 - 7]	2	9.5 %
[7 - 8]	7	33.3 %
[8 - 9]	0	0 %
[9 - 10]	1	4.8 %
Total Number of Vulnerabilities		**21**
Weighted Average CVSS Score		**6.9**

A.6.2.2 DIAMETER Vulnerability Assessments

There is no vulnerability publicly known on DIAMETER protocol implementations. Searching on CVE databases for DIAMETER vulnerabilities forwards to a Wireshark (a network traffic analyser) vulnerability, which is related to the DIAMETER packet dissector implemented in Wireshark (CVE-2012-2393). Consequently, this is absolutely not a DIAMETER security issue, which means that practically, DIAMETER has no vulnerability to be quoted in this section. This is probably due to the fact that DIAMETER is poorly implemented compared to RADIUS, which is massively used in the industry.

A.6.3 Comparison Summary Between RADIUS and DIAMETER Protocols

Table 36 summarises the characteristics of both AAA protocols as discussed earlier:

Table 36: Comparative Summary between RADIUS and DIAMETER Protocols

	RADIUS	Diameter
Operation Paradigm	Client-Server	Peer to Peer
Packet Formats	Figure 41	Figure 42
Transport Protocol	UDP	TCP and SCTP
Proxies and Agents	Proxies	Relay Agents, Proxy Agents, Redirection Agents, Translation Agents
Authentication Mechanisms	NAI, CHAP, PAP, EAP	NAI, CHAP, PAP, EAP
Authorization Mechanisms	Authentication-based, Credential-based	Authentication-based, Credential-based
Accounting Mechanisms	Real-time, timestamps, dynamic accounting	Real-time, timestamps, dynamic accounting

Authorization without Authentication	Possible	Supported
Server-initiated Messages	No (work in progress)	Yes
Error Messages	No	Yes
Compatibility	Low (only with other RADIUS versions)	High (RADIUS and Diameter)
Extensibility	Vendor-specific AVPs	Public-specific AVPs
Reliability	Implementation-specific	Transport failure in the specifications
Scalability	Low	High
Congestion Control	No (UDP)	Yes (TCP and SCTP)
IPv6 Support	Yes (Extension)	Yes (Natively)
Firewalls Friendliness	Yes (Known 1812 port)	Partially (if SCTP is used)
IPSec Support	Supported (Extension)	Mandatory on clients and Servers
End-to-end Security Framework	No (only Hop-by-Hop)	Diameter CMS Security Application (Hop-by-Hop and End-to-End)
Negotiation Capabilities	No	Yes (supported applications and security level)
Number of Vulnerabilities	21 (for FreeRADIUS)	None

A.7 AAA Architectures

AAA architectures are discussed within two working groups:

- The IETF AAA WG defines short term requirements for AAA protocols that support current services such as Mobile IP or NASREQ (NAS Server Requirements)[15];
- The IRTF AAAarch RG (Research Group)[16] defines long-term requirements for AAA protocols that support interconnected generic AAA architectures for inter-organizational AAA operations.

Note that both WG are concluded and are not longer active.

A.7.1 AAA Components

The AAA architecture defined within the IRTF RG is based on a policy approach (the IETF defines a policy as an aggregation of policy rules made up of policy conditions and policy actions). Three AAA components are defined:

- PRs (Policy Repositories) where authorization and accounting policies are stored;
- RBE (Rule Based Engine) takes policy decisions and executes adequate policy actions depending on policy conditions. RBE is generally located at AAA servers;
- SE (Service Equipment) performs policy actions belonging to requested services jointly to other network components. SE may also perform policy actions belonging to support services (*e.g.* accounting) jointly to AAA servers. The NAS is considered as the SE when it performs such policy actions.

[15] NASREQ is an extension that covers the support of PPP EAP and RADIUS by NAS services.

[16] http://irtf.org/concluded/aaaarch

A.7.2 AAA Services

As described in section A.1.1, AAA architectures offer user authentication, authorization, and accounting services. In order to perform these services in an efficient and secured way, trusted relationships between AAA components must be guaranteed. When a user register for AAA services (see section A.1.2), he establishes by contract a trust relationship with its H-NSP. When the user tries to access the V-NSP services, a chain of trust between the relaying proxy AAA servers, the user, and its H-NSP has to be correctly resolved.

The AAA server receives the services requests from the SE (pull sequence) via an ASM (Application Specific Module), the service users or the AAA proxy servers (pull and agent sequence). Then the services requests are evaluated by the RBE which is located inside the AAA server according to the policies stored within the PR. Policy conditions are evaluated by consulting other AAA servers and the SE status: requests are sent to other AAA servers first, then to the ASM which is needed to enforce policy actions. The role of the ASM is then to configure the SE in order to provide a service.

A.7.3 AAA in AeroMACS: Conclusions

The analysis provided in this Annex shows that from a strict security point of view, DIAMETER is more secure compared to RADIUS. Indeed, RADIUS messages are not protected originally (*i.e.* without security extensions) whereas DIAMETER uses CMS to protect its messages.

However, if other considerations have to be taken into account (*e.g. operability, interconnection with existing AAA-equipped devices, existing implementations),* it seems that RADIUS is recommended. The vulnerability study provided here shows that some implementations have minor vulnerabilities that can be patched and corrected easily, which makes the use of RADIUS more receivable.

Appendix D SESAR Paper at ICAO ACP WG W

SESAR P15.2.7 submitted at ICAO ACP WG-W a paper to address the need for an appropriate AAA framework for AeroMACS to be chosen for standardisation.

In addition, the working paper proposed a solution to provide services from different application domains to the same AeroMACS mobile station. Indeed, the standard WiMAX forum procedure does not provide such capabilities to the AeroMACS subscr bers (a MS is able to use services supplied by its home CSN only). An AeroMACS MS could receive services from different Application Domains and it is necessary that the MS is authenticated from each of them. The MS is authenticated by its Home CSN using the standard WiMAX Forum procedure and in this way it is able to use services supplied directly by the Home CSN. The WMF Forum procedures do not consider additional authentication procedures for services supplied from other Application Domains.

In order to get more information, the reader can find the paper at: http://legacy.icao.int/anb/panels/acp/wg/w/wgw4/ACP-WGW04-WP18_AAA_v10.doc

-END OF DOCUMENT-