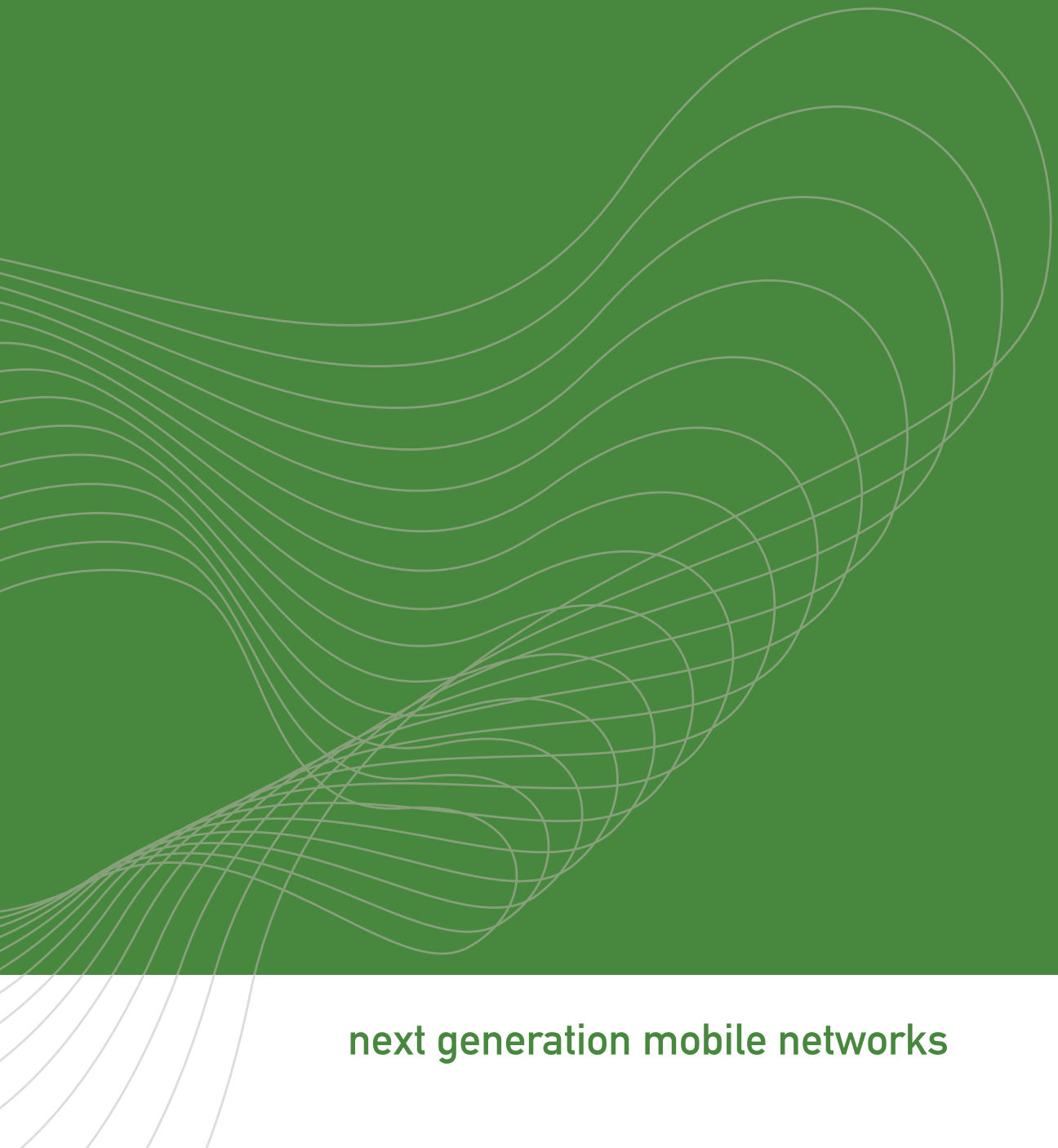
ngmn
the engine of broadband wireless innovation

A White Paper by the NGMN Alliance

Security in LTE backhauling



next generation mobile networks

Security in LTE backhauling

by NGMN Alliance

Version:	**1.0 Final**
Date:	**29 February 2012**
Document Type:	**Final Deliverable (approved)**
Confidentiality Class:	**P – Public**
Authorised Recipients:	**N/A**

Project:	**P-OSB: Optimised Backhaul**
Editor / Submitter:	**Miguel Angel Alvarez, Frederic Jounay, Paolo Volpato**
Contributors:	**NGMN Optimized Backhaul Project Group**
Approved by / Date:	**NGMN Board** **29 February 2012**

Abstract

The adoption of packet based architecture for the LTE backhaul has brought to an increased attention to security matters, often considered as critical issues to be addressed for the deployment of LTE networks.

This paper is an NGMN informative contribution on the subject and aims to provide a common terminology and some high-level scenarios to introduce to Industry a few possible implementations for security in LTE backhauling.

The attention has been put on the ways to assemble security mechanisms in a few scenarios suitable to address the security requirements of an LTE network. The “per interface” approach has been adopted to analyze every scenario presented. The term “per interface” refers to LTE interfaces (S1, X2), the core of this analysis, and the approach undertaken considers what happens to every LTE interface when crossing some defined points in the backhaul network. This is covered in chapter 5

The scenarios described in chapter 6 do not aim to be exhaustive; they should be taken as high level guidelines for Operators to define their own requirements and to what degree of security they are looking at. To this extent, an overview of the meaning of trusted versus un-trusted networks is also given.

Table of Contents

1. Introduction

Scope of this paper is to present some alternative security architectures (scenarios) to be considered in LTE backhauling. The content of this paper is informative; nevertheless some functions or mechanisms needed for the good implementation or operation of a network are addressed. As such sometimes the term “requirement” is used to indicate a functional or logical element to be evaluated when dealing with an end-to-end security architecture in backhauling.

This paper has been developed under the NGMN TWG P11 - P-OSB scope and relates to the other papers already published by the same workgroup.

2. Definitions and abbreviations

Abis	Logical interface between 2G BTS and BSC	**PHB**	Per Hop Behaviour
ATM	Asynchronous Transfer Mode	**PDH**	Plesiochronous Digital Hierarchy
BGP	Border Gateway Protocol	**POS**	Packet Over Sonet
CAC	Call Admission Control	**PPP**	Point to Point Protocol
CE	Customer Edge	**QoS**	Quality of Service
CPE	Customer Premises Equipment	**S1**	Logical interface between LTE BTS and packet core
CSG	Cell Site Gateway	**SDH**	Synchronous Digital Hierarchy
DSCP	Differentiated Service Code Point	**SecGW**	Security Gateway
EPC	Evolved Packet Core	**SGSN**	Serving GPRS Support Nodes
GGSN	Gateway GPRS Support Node	**S-GW**	Serving Gateway
GPRS	General Packet Radio Service	**TDM**	Time division Multiplex
GW	Gateway	**TE**	Traffic Engineering
HSPA	High Speed Packet Access	**UMTS**	Universal Mobile Telecommunication Service
Iub	Logical interface between 3G BTS and RNC	**VC**	Virtual Circuit
LSP	Label Switched Path	**VLAN**	Virtual LAN
LTE	Long Term Evolution	**VPLS**	Virtual Private LAN Service
MPLS	Multi Protocol Label Switching	**VPN**	Virtual Private Network
MASG	Mobile Aggregation Site Gateway	**VRF**	Virtual Routing and Forwarding
OSPF	Open Shortest Path First	**VSI**	Virtual Switching Instance
P	Provider (Router)	**X2**	Logical interface between LTE BTS
PE	Provider Edge (Router)		

3. References

1. **NGMN Alliance, “Next Generation Mobile Networks Beyond HSPA & EVDO – A white paper”, V3.0, December 2006 [available at www.ngmn.org]**
2. **NGMN Alliance, “Next Generation Mobile Networks Optimized Backhaul Requirements”, August 14th, 2008 [available at www.ngmn.org]**
3. **NGMN Alliance, “LTE backhauling deployment scenarios”, paper under publication**
4. **ITU-T X.800, “Security architecture for Open Systems Interconnection for CCITT applications”, March 1991**
5. **ITU-T X.805, “Security architecture for systems providing end-to-end communications”, October 2003**
6. **3GPP TS 33.102: "3G security; Security architecture", March 2010**
7. **3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security", June 2009**
8. **3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)", June 2010**
9. **3GPP TR 33.401, “3GPP System Architecture Evolution (SAE); Security architecture”,**
10. **IETF RFC 4303, "IP Encapsulating Security Payload (ESP)", December 2005**

4. Scope of the work

Compared to the second and third generation of mobile services (2G/3G), the LTE security requires a different system protection. The adoption of a packet-based architecture for the LTE backhaul network, the sometimes recognized lack of expertise when handling packet networks in contrast to circuit switched networks, this even worsened by a widespread know-how on attack methods and availability of hacking tools have found an answer in the work done by 3GPP in some relevant technical specifications, such as the TR 33.401 [9] and related documents.

TR 33.401 and the related documents define the security architecture for LTE as well as the set of features and mechanisms to be implemented in the different network and service domains to obtain a level of security suitable for the support of the control and data plane of LTE by a backhaul network. As an example the LTE flat architecture moves some functions previously in the controller (BSC and RNC respectively) directly into the eNodeB, exposing the service and the underlying packet backhaul network to potential security threats. Unlike in traditional radio networks which had their own physical infrastructure, this is particularly perceived as an issue when a shared network infrastructure is employed, for example in case of coexistence of fixed and mobile services on the same packet network. Moreover, the presence of the X2 interface, that supports direct handover among the vicinity eNodeBs, involves stronger security requirements on the nodes.

Scope of this work is to discuss the security deployments in an LTE backhaul network and propose some guidelines for the implementation of a security architecture compliant with the backhaul scenarios defined in other NGMN papers, specifically [3].

After discussing, in chapter 5, how the analysis on LTE backhaul security has been performed and the resulting requirements, chapter 6 introduces some architectures that operators might consider for their own implementation of security. Chapter 7 also provides an high-level description security for OAM.

4.1. ITU-T X.800 series recommendations

To address the need of having a common security related terminology, the ITU-T recommendations belonging to the X.800 family, and in particular X.805, have been extensively referenced throughout this paper. They have been specifically used to group the requirements into security areas, define the security threats, and map for every area and possible threats some security mechanisms.

Please refer to [4] and [5] for the classification and terminology used.

4.2. Approach taken

Among the several available methods to define and assess the LTE backhaul security architecture the current analysis took the “per interface” approach. Every LTE flow/interface (S1, X2) has been matched against the security requirements at every point into the backhaul network, as explained later.

For each of the architectures presented in chapter 3 a table summarizes the degree of fulfilment of the security requirements, as defined by ITU-T X.805 and the mechanisms that could be implemented to obtain that level of security.

4.3. Trusted and un-trusted networks

One of the basic questions to answer before evaluating what architecture is most suitable for a backhaul network is whether that network is considered trusted or un-trusted. This is key since, as stated by 3GPP in [9], for an un-trusted network it is mandatory to implement an increased layer of security than in trusted environments.

Trusted (or un-trusted) networks can be defined in many different ways. One possible definition is based on criteria related to the property or control of physical site locations, owing of the network, operation managed by a single administrative authority, but more remains (e.g. what degree of network security one operator wants to reach, assessment to define the cost to reach it, etc.).

As a start point to support operators to evaluate how trusted their network is, a very high-level decision tree is proposed, without pretending of being exhaustive.

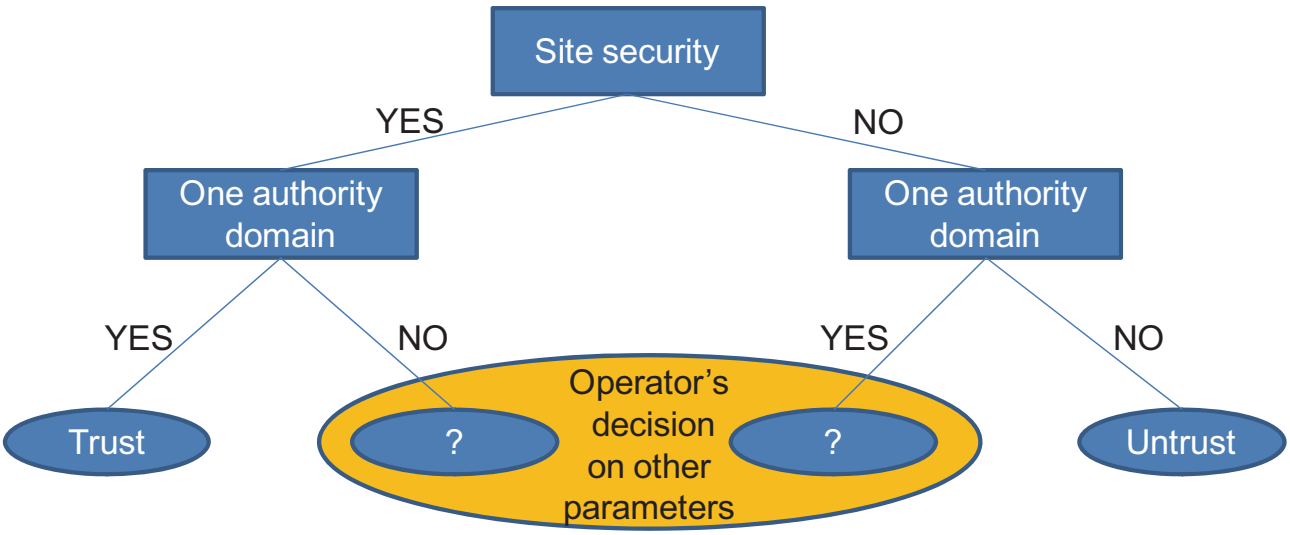


Figure 1 – Decision tree for a trusted / un-trusted network based on physical aspects

An high level decision strategy might start from the physical security of a site (cell site, central office), including the ownership and/or a tight control of it (access, policies, etc.). A second step considers whether a single organization manages the network, or, put in different terms, the network can be organized as a single domain.

If the two previous questions give a positive answer then it is likely that a network can be considered "trusted". On the opposite, two negative answers might lead to an "un-trusted" network, not compliant with the two criteria of physical/logical security.

In between there is a grey area where the definition of trusted or un-trusted network might depend on other parameters, ranging from the operator's attitude to deal with network security, market requirements or law enforcement policies, and a cost versus benefit assessment.

In any case it is recognized that beyond the physical security aspects for any deployment it would be necessary to run a dedicated assessment to assess risk, identify the mitigation needs, plan and deploy controls and accept the residual risk.

5. LTE backhauling security

3GPP has extensively analyzed the security for LTE services across an entire set of specifications (see as an example [6], [7], [8], [9]). Specifically [9] details the features that should be applied into every single function or service stratum to obtain a full-fledged security implementations.

Whilst 3GPP mandates the implementation of those features into a backhaul network, considered in general as a non-secure connectivity medium, Operators have the freedom either to enable the features referenced by the specifications or leave them disabled.

Depending on the willingness of Operators to enable such features, their attitude and many other factors, several security architectures can be found in backhauling, each with advantages and disadvantages. To assess the degree of security of some possible implementations scenarios, this work starts analyzing the impact of security threats over the LTE traffic at the main backhauling interfaces, to detect which are the most suitable mechanisms to mitigate or block a possible attack.

5.1. Architecture and security points

The general description of the LTE backhauling architecture has been detailed in [3]. For sake of clarity, the same diagram is referenced here with the addition of the points (network elements or connections) where backhaul security is analyzed.

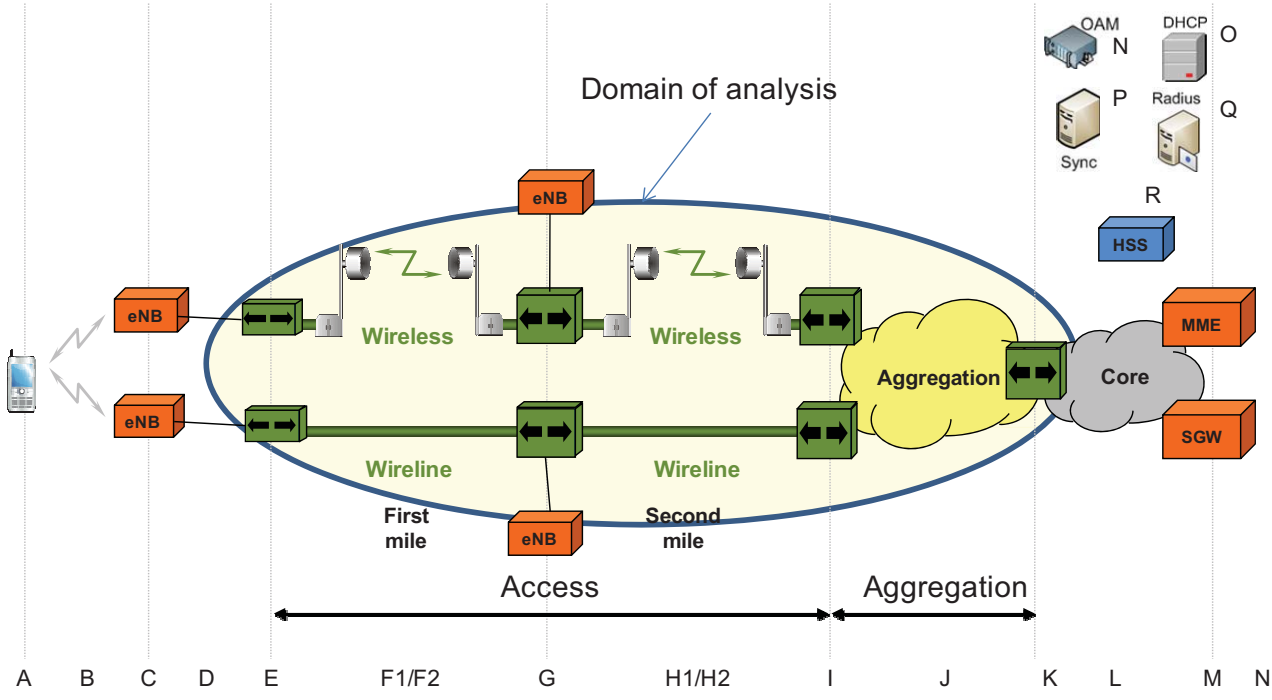


Figure 2 – Network points considered in the analysis

The security points are listed and explained in the following table.

Interface	Network point	Comments
A	User equipment	Delivery of service to user – Out of scope
B	Radio access link	Radio access and transport – Out of scope
C	eNB	Point of ingress to the network and service – Out of scope
D	MEF UNI (eNB – Demarcation node link)	Transit of Ethernet frames
E	Demarcation node	Switching/routing of traffic
F1	Wireless (microwave) first mile	Transit of Ethernet frames (on air, often scrambled and/or proprietary format)
F2	Wireline (fiber, copper) first mile	Transit of Ethernet frames
G	Packet node	Switching/routing of traffic
H1/H2	Second mile - See F1/F2	As F1/F2
I	Packet node	Switching/routing of traffic
J	Aggregation network	Ethernet transport
K	MASG	Switching/routing of traffic
L	Core	Any transport technology – Out of scope
M	Controller	Service control and handling – Out of scope
N	OAM	Log alarms and events, SW distribution, configuration parameters – Out of scope
O	DHCP Server	IP address – Out of scope
P	Sync Master	Network clock – Out of scope
Q	Radius server	Authentication server – Out of scope
R	HSS	Subscriber data, authentication vectors – Out of scope

Table 1 – List of network points

5.2. LTE flows

The “per flow” is the approach taken to analyze the backhaul security; it follows the previous statement of 3GPP and considers the impact, in the security domain, of every LTE flows when they cross some defined points into the backhaul network, as shown in the next paragraph.

The key LTE interfaces considered are listed in the following table.

Interface	Scope	Detail
S1-U	S1 User data	Defines the user plane between eNB and Serving GateWays
S1-C	S1 Control pane	Used for signaling between the eNB and the MME
X2-U	X2 User data	Data plane distributed among eNBs
X2-C	X2 Control plane	Supports inter-eNB handoff with no packet loss
OAM	Management plane	Management traffic exchanged with network elements belonging to backhauling

Table 2 – List of interfaces

5.3. Threats

There are many standards and documents that describe the attacks and risks in telecommunications networks. As mentioned earlier, this paper uses the security framework defined by the ITU-T X.800/X.805 recommendations. The ITU-T X.800 threats model is summarized in the table below.

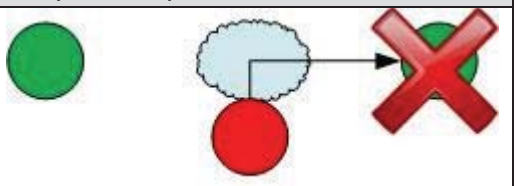
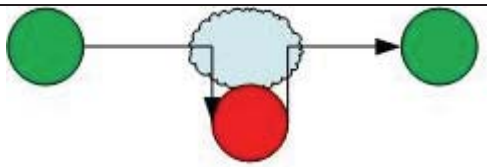
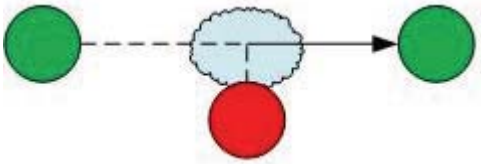
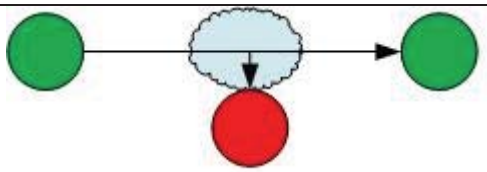
Threats	Description	Graphical representation
Destruction	Destruction of information and/or network resource (DoS Denial-of-Service)	
Corruption/Modification	Unauthorized tampering with an asset	
Removal	Theft, removal or loss of information and other resource	
Disclosure/Interception	Unauthorized access to an asset (eavesdropping)	
Interruption	Network becomes unavailable or unusable	

Table 3 - Threats model

The focus of the threats analysis is on intentional attacks and in particular:

- Insider attacks - abuse of administrator rights (eNB/CSG access)
- External attacks via networks – from Internet or other PDN, from GPRS roaming exchange or other PLMN, from an external transport network or external non-3GPP access network;
- External attacks on physical access to the network – on the radio interfaces, tampering with easily accessible devices (e.g. small cells), unauthorized physical access to network ports;
- Attacks from mobiles.

5.4. Per interface application of threats to security points

Matching the threats defined in the previous paragraph with the LTE flows crossing the network points shown in Figure 2, we obtain a first result described into the next table.

Network point	S1-U	S1-C	OAM	X2-U	X2-C
D	Tampering, traffic hijacking, eavesdropping, destruction	Tampering, traffic hijacking, inject wrong/false control data, eavesdropping, destruction	Spoofing of eNB identity, eNB impersonation, eavesdropping of management activities, management intrusion	Tampering, traffic hijacking, eavesdropping, destruction	Tampering, traffic hijacking, inject wrong/false control data, destruction
E		Unauthorized access, loss of accountability of control plane activities	Unauthorized access to CSG, impact on traffic steering, DoS attacks against node manageability, unauthorized modification of configuration data, loss of configuration data and accountability of management activities	Traffic hijacking, if X2 routed/switched here	Traffic hijacking, if X2 routed/switched here
F1/F2	Tampering, traffic hijacking, eavesdropping, destruction	Tampering, traffic hijacking, inject wrong/false control data, eavesdropping, destruction	Spoofing of eNB identity, eNB impersonation, eavesdropping of management activities, management intrusion	Tampering, traffic hijacking, eavesdropping, destruction	Tampering, traffic hijacking, inject wrong/false control data, destruction
G		Unauthorized access, loss of accountability of control plane activities	As point E, loss of configuration data and accountability of management activities	Depending on topology and backhauling scenarios X2 steering might be impacted, denial of service	Depending on topology and backhauling scenarios X2 steering might be impacted, denial of service

H1/H2	Tampering, traffic hijacking, eavesdropping, destruction	Tampering, traffic hijacking, inject wrong/false control data, eavesdropping, destruction	Spoofing of eNB identity, eNB impersonation, eavesdropping of management activities, management intrusion	Tampering, traffic hijacking, eavesdropping, destruction	Tampering, traffic hijacking, inject wrong/false control data, destruction
I		Unauthorized access, loss of accountability of control plane activities	See E, , loss of configuration data and accountability of management activities	Depending on topology and backhauling scenarios X2 steering might be impacted, denial of service	Depending on topology and backhauling scenarios X2 steering might be impacted, denial of service
J	Tampering, traffic hijacking, eavesdropping, destruction	Tampering, traffic hijacking, inject wrong/false control data, eavesdropping, destruction	Spoofing of eNB identity, eNB impersonation, eavesdropping of management activities, management intrusion	Tampering, traffic hijacking, eavesdropping, destruction	Tampering, traffic hijacking, inject wrong/false control data, destruction
K		Unauthorized access, loss of accountability of control plane activities	See E, loss of configuration data and accountability of management activities	Depending on topology and backhauling scenarios X2 steering might be impacted, denial of service	Depending on topology and backhauling scenarios X2 steering might be impacted, denial of service

Table 4 – List of threats per network point

In general, the closer the potential attack is to the core network, the less physical access methods are required. In other words physical access methods are more involved to deal with potential attacks brought from positions close to eNBs.

This is a security focus for LTE features. The operator shall also manage security backhauling networks form networks point of view. All access point shall have sufficient security rule to insure backhauling security.

5.5. Security areas

Security services can be grouped, according to ITU-T X.800/X.805, into a few categories whose scope is described in the next table.

Area	Description
Authentication	This area provides for the authentication of a communicating peer entity and the source of data
Access Control	This service provides protection against unauthorized use of resources
Traffic confidentiality and integrity	Data cannot be read by unauthorized parties or modified during transit
Replay Protection	Data should not delivered multiple times, out of order
Availability	Avoid impacts over services, network elements and application due to (un)intentional reason such injection of false traffic, attacks, spoofing, (D)DoS
Accountability	Prevent ability to deny that an activity on the network occurred
Communication security	Ensure information only flows from source to destination
Privacy	Ensure identification and the network usage is kept private

Table 5 – Security areas

The possibility of addressing one or more of the eight security areas defined in the previous table depends on what security mechanisms are available in a network. Literature often groups the security methods in nine major categories, as shown in the columns of the next table. The table aims at matching the security mechanisms with the areas described before. If an operator wishes to address one security area, then one or more security mechanisms have to be selected, to obtain the implementation of the proper counter-measures to the threats listed in paragraph 5.4.

The green cells in the table highlight that for addressing the service in one of the eight rows the security mechanisms belonging to one of the nine categories need to be enabled. For sake of clarity some examples, not exhaustive, of security mechanisms are listed into the green cells.

Service/ mechanism	Ciphering (1)	Digital signature	ACL	Data Integrity	Authentication exchange	Traffic padding	Routing control	Notarization	Recovery
Authentication		DSA, RSA		MAC	PKI, X.509, Radius				
Access control			VLAN ID, MAC addr.						
Confidentiality	AES, 3DES, A5/3					Many encyph. algorithms	VLAN, VRF		
Data integrity		Asymmetric encyph.		SHA1, SHA-256					
Privacy	IPsec					Many encyph. algorithms	VLAN, VRF		
Availability				IPsec	PKI, X.509, Radius				Redundancy, backup, alarms
Communication security	IPsec, SSH						VLAN, VRF		
Accountability		DSA, RSA, ElGamal		IPsec				LOG activity	

Table 6 – Examples of security mechanisms per area

1. The common term to indicate this function is "ciphering" (which also includes "deciphering"). The name "encipherment" has been also maintained in this paper as it is referenced by ITU-T X.800 [4]

As an example, if one operator needs to enable the authentication of the network elements part of the backhauling, then some mechanisms belonging to the "Digital signature", "Data integrity" or "Authentication exchange" have to be enabled. From an implementation point of view, this corresponds to the usage of one or more mechanisms often related to the IPsec framework: algorithms for digital signature (i.e. DSA, RSA), for data integrity (e.g. MAC), certificate-based methods, etc.

This table will be applied in the next chapter when dealing with network scenarios. For every scenario, some examples of security mechanisms will be examined and explained.

6. Security scenarios

The scenarios presented in this chapter aim at highlighting different ways to combine the security mechanisms introduced in the previous section to obtain a secure LTE backhauling.

Three high-level scenarios are introduced:

- A first scenario tries to answer to the necessity of a light security implementation, meaning without IPsec, leveraging on mechanisms already available in packet networks
- The second presents IPsec for protecting the LTE control traffic (S1-C, X2-C), often considered as the most sensible for the service continuity
- The third analyzes a full IPsec protection, both for control and user traffics.

One point that will be discussed is the position of the Security Gateway (SecGW) applied to the topologies described in [3].

6.1. Scenario 1: Trusted domain

The key characteristic of this scenario is the absence of IPsec.

This scenario might be considered by Operators perceiving their backhaul network as “trusted”. There may exist several motivations for that. One example, based on the decision tree presented in paragraph 4.3, is given by an operator who relies on the “physical” aspects of security (e.g. entirely owns the backhaul infrastructure and relies on tight control policies to access sites). Another example could be represented by operators who are not willing to handle extra operation due to the introduction of a security layer or that, after performing a risk assessment, determine the risk reduction that could be achieved by introducing IPsec does not justify the associated expenses.

Also, this scenario might be considered for first LTE deployments provided that one operator is aware of the implications for enabling a security architecture afterwards, as pointes out in the pros/cons discussion.

The scenario is shown in the next picture.

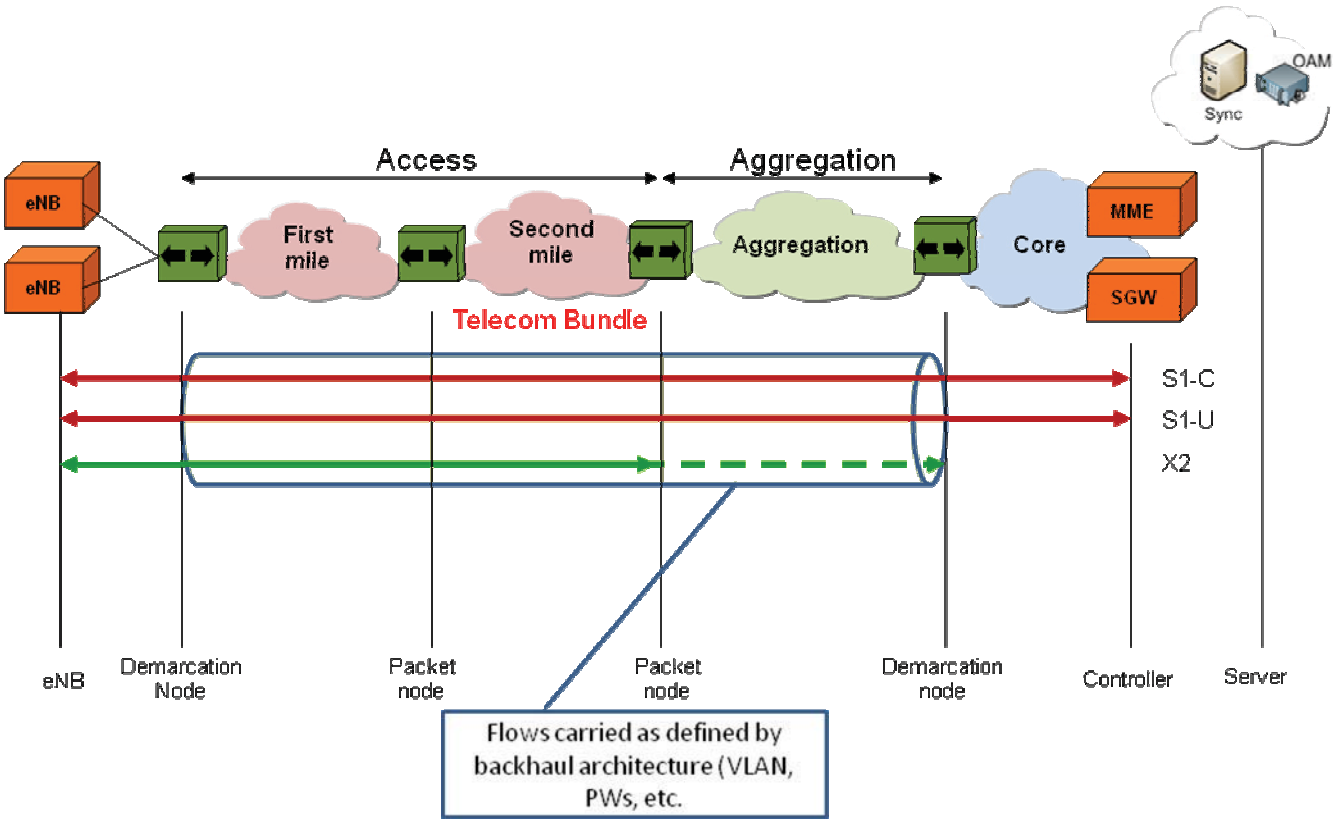


Figure 3: Scenario 1 logical architecture

Transport of LTE flows relies on the same mechanisms and architectures shown in [3]. In the example above a VLAN is considered to carry the Telecom bundle, but the case could be generalized for pseudowires, L2 or L3 VPNs.

Security should focus on:

- Requirements against physical access;
- Restricted access, strong authentication.

Even if not widely implemented, some techniques for supporting ciphering/integrity at L2 could be enabled (e.g. 802.1AE MACsec for authentication and confidentiality of each packet exchanged link by link). Those solutions are not commonly found in deployed networks.

The next picture highlights the degree of security reachable by this scenario and shows some of the mechanisms that can be enabled to achieve it. It is worth noting that without encryption or digital signatures techniques the services of authentication or confidentiality cannot be fulfilled (reason why the corresponding cells are filled with solid yellow, as a reminder for attention).

Service/ mechanism	Ciphering	Digital signature	ACL	Data Integrity	Authentication exchange	Traffic padding	Routing control	Notarization	Recovery
Authentication		(1)		(1)	Radius, password, smartcard (2)				
Access control			VLAN ID, MAC@. IP@						
Confidentiality	(1)					Many encyph. algorithms	VLAN, VRF, PW, firewall		
Data integrity		(1)		(1)					
Privacy	(1)					Many encyph. algorithms	VLAN, VRF, PW firewall		
Availability				(1)	Radius, password, smartcard (2)				IDS/IPS, backup, alarms
Communication security	(1)						VLAN, VRF, PW, firewall		
Accountability		(1)		(1)				LOG activity	

Table 7 – Degree of security of scenario 1 and available mechanisms

1. Security not applicable, unless mechanisms different from IPsec are enabled (e.g. MACsec protocol)
2. Smartcards are included as an example for the storage of a certificate

6.1.1. Pros & Cons

The simplest advantage is that no operational burden is imposed by a security layer. IPsec is sometimes perceived as impacting the network (extra processing requested to eNBs, extra overhead in transmission, etc.) leading, in ultimate analysis, to an extra cost. The usage of standard security mechanisms (i.e. ACLs, Firewalls, etc.) falls within the average skill of network operation teams.

It is a scenario that perfectly fits any network topology, and does not require the planning of a detailed addressing (i.e. one IP address is associated to the transport pipe).

On the other hand, the missing security features might have to be compensated at the service/application layer. The bottom line is that both the control and data traffic flows are neither encrypted nor integrity protected, so in theory exposed to any form of listening and/or modification, particularly important for signaling. Unless the elements of backhauling are strongly controlled, some attacks from within the network are possible.

Another issue could be the adoption, in a second step, of some form of security as explained by the next scenarios; this might force the operator to considering a re-planning of the LTE flows transport.

The adoption of L2 mechanisms still does not completely solve the problem. Protection is provided on the link only, traffic is still vulnerable while being processed in network nodes. Also, the hop-by-hop security realized through them requires authentication credentials to be deployed and managed in every packet node.

6.2. Scenario 2: IPsec for control plane

In this case IPsec is enabled for protecting the LTE control traffic.

It might be considered by Operators with self-built backhauling or with eNBs in areas secure enough to let Operators just encrypt the signaling traffic.

As such the S1-C and X2-C flows are based on IPsec-ESP (encryption and integrity control, tunnel mode), whilst S1-U and X2-U remain based on the transport technology chosen for backhauling (as per [3]).

Two different variants of this scenario can be considered.

In the first case one VLAN only is used to carry both the encrypted control traffic and the un-encrypted user traffic. In the second case two transport constructs are needed, to differentiate control from data traffic (VLANs, PWs, or any other solution based on a mix of L2 and L3 VPNs). The next picture shows the latter case, as it can be considered as an extension of the former.

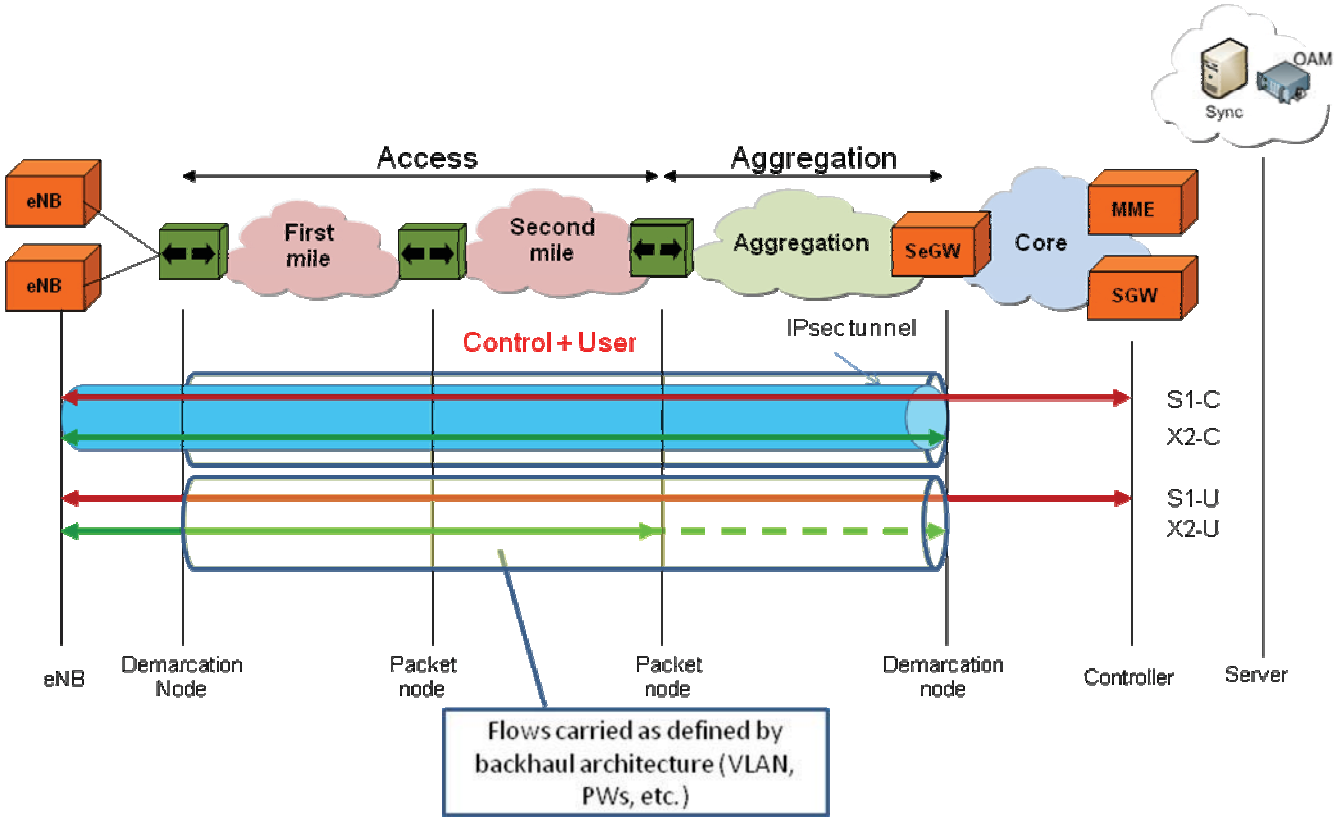


Figure 4: Scenario 2 logical architecture

This scenario could implement the same security mechanisms of the previous one (e.g. the demarcation node at the cell site may act as PAE, supporting 802.1x). It has to be noted however that this scenario enables the security level described in [8]: the eNB is authenticated to/by the MME. In other terms a tunnel is established from the eNB and the MME, to cope with the requirements of authentication and confidentiality.

In doing that both S1-C and X2-C are carried within an IPsec tunnel, characterized by the Encapsulating Security Payload (ESP) mode [10] and profiled following 3GPP specifications [7], [8], [9]. Also, [8] further profiles a certificate based network authentication based on a public key exchange. The typical deployment then sees the presence of a Security Gateway (SecGW) in front of the Evolved Packet Core (EPC).

As a result, the next table shows the security level obtainable through this scenario. The usage of several mechanisms belonging to the IPsec framework raised the level of security, yet the lack of data integrity, authentication and encryption for the user plane has the consequence of having some cells half-colored.

Service/ mechanism	Ciphering	Digital signature	ACL	Data Integrity	Authentication exchange	Traffic padding	Routing control	Notarization	Recovery
Authentication		DSA, RSA (1)		MAC (1)	Radius, password, smartcard (2)				
Access control			VLAN ID, MAC@. IP@						
Confidentiality	AES, 3DES, A5/3 (1)					Many encyph. algorithms	VLAN, VRF, PW, firewall		
Data integrity		Asymmetric encyph. (1)		SHA1, SHA-256 (1)					
Privacy	IPsec (1)					Many encyph. algorithms	VLAN, VRF, PW firewall		
Availability				IPsec (1)	Radius, password, smartcard (2)				IDS/IPS, backup, alarms
Communication security	IPsec, SSH (1)						VLAN, VRF, PW, firewall		
Accountability		DSA, RSA, ElGamal (1)		IPsec (1)				LOG activity	

Table 8 - Degree of security of scenario 2 and available mechanisms

1. IPsec framework is applied only on control plane
2. Smartcards are included as an example for the storage of a certificate

6.2.1. Pros & Cons

The main advantage is clearly the protection offered to the control traffic, at a price of some limited overhead and performance impact.

Also, it offers an easy path to eventually include S1-U and X2-U into the IPsec tunnel (Tunnel mode)[1].

There is, probably, one major drawback related to the topology that could be chosen to support this scenario. eNBs communicate directly to the SGW (the address plan is “visible” from backhauling, so in theory more exposed and require hub and spoke topologies), whilst SecGW will be the check point to reach MME.

For X2-U, this has to be steered up to the first Transport node allowing local switching/routing. The SecGW assume also check point and manage the control plane connectivity between neighbour eNodeBs. The SecGW position shall be compatible with maximal latency supported by X2-C.

[1] 3GPP used IPSec Tunnel Mode to protect IP interface.

6.3. Scenario 3: IPsec for all telecom flows (Control Plane, User Plane)

The last scenario could be adopted by those Operators that want to extend the same security features of the previous one also to the data plane. One example is represented by mobile Operators that lease backhaul resources from other carriers or consider everything as un-trusted.

The control traffic is then transported as in scenario 2, with S1-C and X2-C based on IPsec-ESP in tunnel mode (to support both encryption and integrity). S1-U and X2-U are based on IPsec as well, with the only difference that might be with or without integrity protection. This latter case is just for the support of authentication and confidentiality.

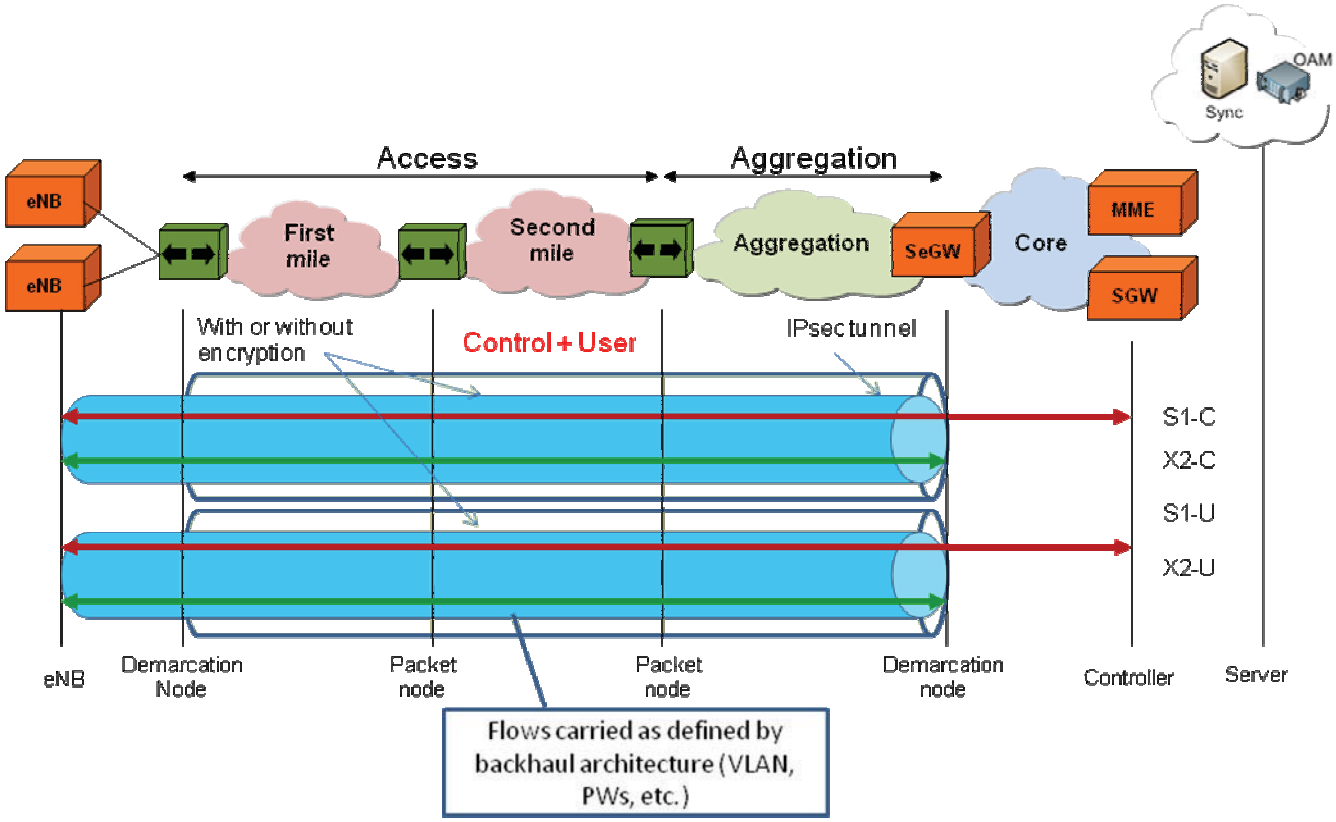


Figure 5: Scenario 3 logical architecture

The most notable difference with the previous scenario is IPsec used to carry the data plane. The picture shows two IPsec tunnels, but this is left to the Operator's decision (one tunnel may suffice).

As a result, the next table shows the level of fulfilment of the security requirements.

Service/ mechanism	Ciphering	Digital signature	ACL	Data Integrity	Authentication exchange	Traffic padding	Routing control	Notarization	Recovery
Authentication		DSA, RSA (1)		MAC (1)	PKI, X.509, Radius smartcard (2)				
Access control			VLAN ID, MAC@. IP@						
Confidentiality	AES, 3DES, A5/3 (1)					Many encyph. algorithms	VLAN, VRF, PW, firewall		
Data integrity		Asymmetric encyph. (1)		SHA1, SHA-256 (1)					
Privacy	IPsec (1)					Many encyph. algorithms	VLAN, VRF, PW, firewall		
Availability				IPsec (1)	PKI, X.509, Radius smartcard (2)				IDS/IPS, backup, alarms
Communication security	IPsec, SSH (1)						VLAN, VRF, PW, firewall		
Accountability		DSA, RSA, ElGamal (1)		IPsec (1)				LOG activity	

Table 9 - Degree of security of scenario 3 and available mechanisms

1. IPsec framework is applied to all planes
2. Smartcards are included as an example for the storage of a certificate

6.3.1. Pros & Cons

The main advantage is clearly the protection offered to all of the traffic with no distinction. The S1-U interface has the same level of security of S1-C.

On the other hand, this scenario has an increased computational impact on eNB and imposes a bigger overhead at L1 transmission, bringing to some capacity waste as in the case of microwave links.

Depending on the position of the SecGW some impact on switching/routing of X2 could be caused.

6.4. The position of SecGW

The Security Gateway (SecGW) comes into play whenever the transport of LTE flows is protected by IPsec. The position SecGW can assume in the network depends on several factors among which:

- Topology chosen by Operators for their network infrastructure (L2, L3 or a mix of the two, as shown in [ref. stream #1]);

- Network requirements (e.g. scalability, performance, density of cell sites);
- Operation constraints (different teams handle different network domains).
- Wholesale offer (leased line)

Following the definition of backhauling as given by [3], three main positions are suited for SecGW:

- Very close to the eNB, or at the cell site;
- At the point of decoupling between two network domains (for the scope of [ref. stream #1] this could be between the access and the aggregation). This can be considered as a distributed position of SecGW;
- In front of the Evolved Packet Core (EPC), or directly connected either to MME or S/P-GW. This could be referred to as a centralized position for SecGW.

The first of the three, close to or even at the cell site, can be considered as a case of "collapsed backhauling". As it is not likely to be found in the field, this case is not treated here.

For the two remaining positions, "distributed" and "centralized", an high level comparison is given in the next table.

	Distributed SecGW	Centralized SecGW
Pro	Flexibility in adapting to the underlying network domains topology (i.e. point-to-point L2 access, L3 VPN aggregation)	Less equipment requested (depends on scalability), cost effective solution
	Lower latency is achieved for X2 (scenario 3, control and user planes carried in IPsec).	Increased flexibility when dealing with redundancy. Please note with optical networks, the networks latency is less than 10 ms [2].
	Lower latency is achieved for X2 also in scenario 2 (control carried in IPsec), whilst for the user plane the same performance could be achieved by decoupling the SecGW from the transport function (two different network elements)	More flexible in handling scenario 2
Con	For scenario 2 if two NEs are used for the decoupling mentioned above there could be an increased provisioning and configuration burden	Higher latency for X2 in scenario 3

[2] Current latency measure is ~10ms for 2250 km and 10 hops

	The number of SecGWs can be potentially high, depending on factors such as scalability and degree of distribution	Access and aggregation more exposed to threats
	Increased overall operation	

Table 10 – Distributed versus centralized SecGW

It is not the intent of this paper to suggest which position should be adopted by SecGW. On a high level basis, it is likely that a centralized approach could be suitable for Operators willing to minimize the effort for operation. One redundant SecGW should be enough for connecting a few hundreds of eNBs, if the model based on one IPsec tunnel per site is chosen.

If eNBs manage more than one IPsec tunnels (e.g. for decoupling every LTE flow), a tunnel providing integrity protection and encryption for the Control Plan and a second tunnel providing encryption only for the User Plan can be foreseen. The usage of two tunnels saves computational processing if compared to the usage of one tunnel only where integrity and encryption are enabled for both planes. It can be reminded that the Control Plan requires less processing than the User Plan.

7. OAM security

For completeness, this section highlights a security scenario for OAM. This is not directly related to any of the three scenarios presented earlier in this paper, but can be considered common to them.

The next picture shows a possible implementation based on two VLANs (they could be collapsed into one), respectively carrying Access Control traffic and Management traffic.

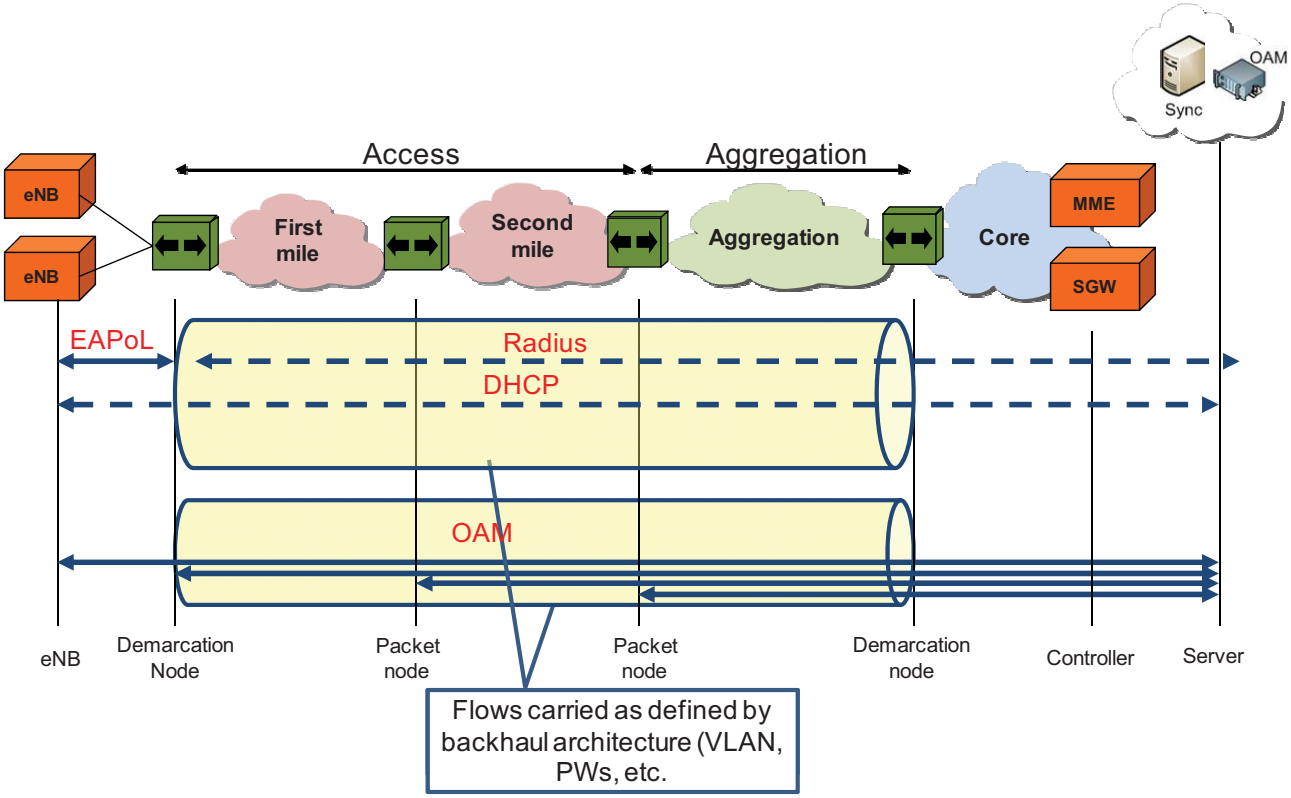


Figure 6 – OAM example

The reason to base OAM on two VLANs comes from a functional split:

- A first VLAN may transport the data exchanged for the authentication of an eNB and can include the 802.1x support based on EAPOL and Radius/Diameter, plus the DHCP traffic for the address assignment to the same eNB;
- A second VLAN may be used for management (FCAPS function). OAM security is primarily concerned with accountability and handling of privileges of operators. An example of usage is to limit access to OAM interfaces to what is necessary for an individual user to carry out assigned tasks.

The authentication of an eNB based on PAE (at the demarcation entity) could be considered anyway as a base level to start with. 3GPP specifies eNB authentication is done within IKEv2, through certificates, when initializing the IPsec connectivity [8].

For eNB management, only secure protocols could be employed: SNMPv3 (authentication, integrity and encryption packets), SSH or TLS for local or remote access, HTTPS for web interface, Secure FTP for data transfer. It should be noted that the use of TLS and HTTPS requires a PKI and provisioning of X.509 OAM certificates. The support of these protocols is mandated by 3GPP specifications such as [8] and [9].

The scenario could be simplified through the usage of one VLAN only. Also to be noted, IPsec can be used to tunnel OAM packets.

8. Other Requirements

8.1. Security on synchronization plane

The synchronization features is a main mandatory features for every mobile networks. A loss of synchronisation will have large radio link QoS impact. This may also be applicable for those security mechanisms that rely on the usage of time-stamps (e.g. certificates). As such it needs to be secured.

Among the several approaches that can be considered the most likely:

- Handling the synchronization traffic in a separate and dedicated VLAN;
- Transport this traffic together with the control flows;
- Choose to transport synchronization traffic together with the user data;
- Bundle synchronization with some OAM traffic

Independently from the chosen method, it is worth noting that the synchronization traffic is likely not to be encrypted. This is for two reasons: encryption could impact the overall performance of synchronization protocols such as the IEEE 1588v2 and avoid the operational burden imposed by IPsec when network elements receive a synch packet.

Nevertheless, the need for master authentication and data integrity is envisioned. In addition, internal attacks that enable, for instance, to insert delays or cause quality of service degradation, should be avoided.

9. Conclusion

Defining an end-to-end, integrated security architecture for the LTE backhaul network is not trivial and many different aspects have to be considered.

On the technical side a security architecture cannot be disjoint from the logical topology of the backhaul network. On top of that an Operator can choose what security services have to be enabled to reach a satisfactory degree of security. In the end, much of the technical design depends on aspects such as the Operator's expertise in dealing with the concepts presented through the three high-level security scenarios described in chapter 6.

Apart from the technical side of the problem, security has to be also tackled from an economic standpoint (cost of the solution, management complexity) and from a performance point of view (match the security architecture with the transport architecture to avoid impairment on some traffic flows).

In ultimate analysis the scope of this paper should be to introduce architectures that have be assessed by more detailed cost/benefit analyses that only Operators can run for their own network.