Gabriela Limon Garcia

IPSec performance analysis for large-scale Radio Access Networks

Master’s Thesis
Espoo, July 30, 2008

Supervisors: Professor Sasu A O Tarkoma, Helsinki University of Technology
Professor Peter Sjödin, The Royal Institute of Technology

Instructor: Peter Sjödin, PhD, Royal Institute of Technology
Transition to IP based networks within the telecommunication world is a reality. IP based networks major feature is to enable the merging of wired and wireless networks. However, openness of the network introduces security threats. Therefore, there is the need to adopt solutions to secure transactions.

International standardization organizations have proposed the adoption of IPSec as the standard solution to implement. Previous research work has analyzed IPSec characteristics from both theoretical and practical perspective; however, little research has been done regarding IPSec practical characteristics when implementing in large scale radio access networks.

This thesis aims to evaluate IPSec implementation performance at the Radio Access Network part of large scale cellular systems. Results derive from Radio Access Networks emulations using realistic traffic characteristics.

It is shown that IPSec is suitable for large packet size traffic (512-1420 bytes) given the fact that it reduces overall performance in a 60-80% for small packet size traffic (64-500 bytes).

<table>
<thead>
<tr>
<th>Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec, Radio Access Network, Iub</td>
</tr>
</tbody>
</table>
Abstract

Transition to IP based networks within the telecommunication world is a reality. IP based networks major feature is to enable the merging of wired and wireless networks. However, openness of the network introduces security threats. Therefore, there is the need to adopt solutions to secure transactions.

International standardization organizations have proposed the adoption of IPSec as the standard solution to implement. Previous research work has analyzed IPSec characteristics from both theoretical and practical perspective; however, little research has been done regarding IPSec practical characteristics when implementing in large scale radio access networks.

This thesis aims to evaluate IPSec implementation performance at the Radio Access Network part of large scale cellular systems. Results derive from Radio Access Networks emulations using realistic traffic characteristics.

It is shown that IPSec is suitable for large packet size traffic (512-1420 bytes) given the fact that it reduces overall performance in a 60-80% for small packet size traffic (64-500 bytes).
Acknowledgments

First of all I would like to thank the European Commission and NordSecMob consortium for giving me the opportunity to make this dream possible and for providing support during the period of the master studies. I would like to thank the teaching staff at both universities. Specially, I want to express my gratitude to my supervisors PhD Peter Sjödin and Professor Sasu A O Tarkoma for their patience and support.

I would also like to thank my supervisor at Ericsson, Gunnar Forssell for his guidance and support not only for this work but also for daily life learning. Also, thanks to all the marvelous people at Ericsson WCDMA RAN systems, Ericsson Research department and Clavister for their invaluable help and support to make this project possible.

This work is dedicated to my beloved family and friends who support me and encourage me to continue despite the adverse circumstances. To my mother, for her warm words and wise advice. To my father for being a colleague and source of inspiration. To my siblings, nieces and nephews for feeding my heart with smiles.
List of Figures

Figure 1. 3G security architecture ................................................................. 14
Figure 2. UTRAN architecture ...................................................................... 19
Figure 3. RAN security infrastructure ............................................................ 23
Figure 4. Comparison WCDMA vs. LTE access architecture ....................... 24
Figure 5. Authentication Header overhead ................................................... 26
Figure 6. Encapsulation Security Payload overhead ...................................... 26
Figure 7. IPSec overhead for service and operation modes ......................... 27
Figure 8. Independent VPNs scenario ........................................................... 35
Figure 9. Test bed 1. One NodeB to one RNC .............................................. 36
Figure 10. Test bed 2. Four NodeB to one RNC ............................................ 36
Figure 11. Security gateway settings impact ............................................... 38
Figure 12. Latency for adjusted settings ....................................................... 39
Figure 13. Latency for default settings ......................................................... 39
Figure 14. Latency Default settings vs. Adjusted settings .............................. 40
Figure 15. Test duration impact. Default Settings ........................................ 41
Figure 16. Test duration impact. Adjusted Settings ....................................... 42
Figure 17. Rekey impact for default settings ............................................... 43
Figure 18. Rekey impact for adjusted settings .............................................. 44
Figure 19. Encryption algorithms performance for default settings ............... 45
Figure 20. Encryption algorithms performance for adjusted settings ............ 45
Figure 21. One common tunnel scenario ..................................................... 46
Figure 22. Independent tunnels. Flow throughput ........................................ 47
Figure 23. Independent tunnels. Tunnel throughput ..................................... 48
Figure 24. Common vs. Independent tunnel. Default settings ....................... 48
Figure 25. Common vs. Independent tunnel. Adjusted settings .................... 49
Figure 26. IPSec throughput for aggregated Security Associations ............... 50
Figure 27. IPSec throughput ................................................................. 51
Figure 28. IPSec bidirectional throughput ............................................... 52
Figure 29. IPSec latency. Default settings vs. Clear text .............................. 53
Figure 30. IPSec latency. Adjusted settings vs. Clear text ............................. 53
Figure 31. IPSec latency for packet size greater than 512 ............................ 54
Figure 32. IPSec Standard deviation ............................................................ 54
Figure 33. IPSec frame loss ................................................................. 55
Figure 34. IPSec frame loss behavior .......................................................... 56

Table 1. IPSec services overhead ................................................................. 29
Table 2. 3GPP specification for IPSec ......................................................... 30
Table 3. Iub latency requirements ............................................................... 32
Table 4. Configuration profiles ................................................................. 64
Contents

1 INTRODUCTION ............................................................................................................ 9
  1.1 BACKGROUND OVERVIEW .................................................................................. 9
  1.2 RESEARCH AREA .................................................................................................. 10
  1.3 PROBLEM STATEMENT ......................................................................................... 11
  1.4 OVERVIEW OF THE APPROACH ....................................................................... 11
  1.5 SCOPE .................................................................................................................. 11
  1.6 CHAPTER OUTLINE .............................................................................................. 12

2 BACKGROUND ............................................................................................................. 13
  2.1 RADIO ACCESS NETWORK SECURITY .................................................................. 13
  2.2 INTERNET SECURITY PROTOCOL PERFORMANCE ........................................... 15
  2.3 IPSec in RAN ........................................................................................................ 16

3 RADIO ACCESS NETWORKS ....................................................................................... 18
  3.1 WCDMA ................................................................................................................. 18
    3.1.1 3GPP Network architecture ............................................................................. 18
    3.1.2 IP in WCDMA RAN ......................................................................................... 20
      3.1.2.1 Traffic types ............................................................................................... 20
      3.1.2.2 Traffic segregation .................................................................................... 21
      3.1.2.3 Traffic protection ...................................................................................... 21
      3.1.2.4 Security architecture ............................................................................... 22
      3.1.2.5 Network architecture ............................................................................... 22
  3.2 LTE .......................................................................................................................... 23
    3.2.1 Network architecture ....................................................................................... 24
    3.2.2 Security ............................................................................................................ 24

4 INTERNET PROTOCOL SECURITY ............................................................................. 25
  4.1 IPSec SUITE ARCHITECTURE ................................................................................. 25
    4.1.1 Services ............................................................................................................ 25
      4.1.1.1 AH .............................................................................................................. 26
      4.1.1.2 ESP ............................................................................................................ 26
    4.1.2 Operation modes ............................................................................................. 27
      4.1.2.1 Transport Mode ......................................................................................... 27
      4.1.2.2 Tunnel Mode ............................................................................................ 27
  4.2 IKE .......................................................................................................................... 28
  4.3 PROTOCOL OVERHEAD ....................................................................................... 29
  4.4 IPSec as a Standard for Mobile Networks .............................................................. 29

5 THEORETICAL ASSESSMENT ..................................................................................... 31
  5.1 THROUGHPUT ......................................................................................................... 31
  5.2 LATENCY ................................................................................................................ 32
  5.3 FRAME LOSS RATE .............................................................................................. 33
  5.4 CAPACITY .............................................................................................................. 33

6 SYSTEM MODEL ......................................................................................................... 34
  6.1 IPSec Profile .......................................................................................................... 34
  6.2 SCENARIOS ........................................................................................................... 34
  6.3 TEST BED CONFIGURATION ................................................................................. 35
1 Introduction

The evolution of mobile networks has followed a fast development direction in terms of technology and services supported. First changes consisted in the adaptation from analog to digital services; recently, the paradigm has evolved from circuit switched to packet switched networks; As a result diverse technologies coexist to offer improved and new services. This explains the fact that current mobile networks do not only support voice services, but also data and multimedia applications. The overall tendency for next generation mobile networks is the convergence of technologies and services: a seamless integration of Internet protocol (IP) based services and mobile network services to conform an all-IP environment under expectations of best quality of service and high speed data connections. This section sets the context for this thesis finalizing with the goal of this work.

1.1 Background overview

The introduction to IP into mobile networks aims to provide a more efficient use of network resources. This derives on benefits for the main roles within a mobile network context: service providers, network operators and end-users. In one hand, for the end-user, the congregation of services and applications results in ease of access and availability of diverse applications by means of a single connection regardless the service provider. On the other hand, for mobile operators and service providers, introduction of all-IP based networks signifies an improvement in network efficiency and a reduction in the overall cost of transport networks.

Another benefit of the transition to an all-IP network approach is a continuous development and improvement of underlying technologies. As a consequence, standardization institutions release new and improved versions of systems implementation. Previous releases then derive on standards aiming to achieve backwards compatibility and consequently to smooth transition towards latest innovations.

The technology evolution scenario described above illustrates the evolution of Universal Mobile Telecommunication Systems (UMTS), a set of protocols defined by the European Telecommunications Standards Institute (ETSI) in January 1998.
[ETSI] as an approach to introduce what now is called Third-Generation of mobile systems (3G). After ETSI grounded the basis for UMTS cellular system, 3rd Generation Partnership Project (3GPP), a standardization consortium, defined an evolutionary roadmap for UMTS: from its initial deployment in 3GPP Release 99 [3GPP TS 33.102 1999] to the introduction of improved features in the latest 3GPP Release 8 such as Long Term Evolution (LTE) and System Architecture Evolution (SAE) initiatives [3GPP TR 33.821 2008].

The success of such evolving technologies relies on their ability to encompass the entire range of scenarios that main players: service providers, end-users and operators demand. Anywhere availability, efficient service, deployment flexibility and scalability are transcendent factors for all sectors. Furthermore, a successful foundation of these emerging technologies depends on the ability to overcome new challenges. Given the scenario in which the integration of Internet and mobile networks enables the sharing of public communication links it is obvious then that new vulnerabilities and potential threats represent such challenges. Therefore, the openness of next generation mobile networks not only translates in benefits and improvements in services and applications but it also introduces concerns in the security level offered by the underlying architecture.

1.2 Research Area

Despite the benefits an introduction of an all-IP approach to mobile networks implies, an all-IP approach also introduces the necessity for comprehensive security measures. Until now, mobile networks were mainly closed environments in which each operator configured its own infrastructure under its own policies. However, the transition to an all-IP approach enforces two elements: the openness of the network to share transport media; and the coexistence of different technologies into a single large scale network. Therefore, the main challenge the introduction of an all-IP approach confront relies in its very nature: IP-specific security vulnerabilities.

Vulnerabilities in IP based fixed networks are defeated by means of traditional security technologies such as firewalls and Virtual Private Networks (VPN). Since next generation mobile networks are moving towards an all-IP approach one important question arises: Is it possible to convey security solutions from fixed networks into a mobile network environment? Furthermore, which is the performance impact of implementing these technologies envisioned for large scale networks?

The answer for the first question is already a fact: for future all-IP mobile networks, standardization institutions such as 3GPP already defined the implementation of security protocols such as Internet Protocol Security (IPSec)[3GPP TS 33.203 2008]. The same case applies for current 3G mobile networks, where ongoing transition to
an all-IP approach is already a reality. For 3G mobile systems, 3GPP specifies the implementation of IPSec as the standard solution for the core network part of the mobile system [3GPP TS 33.210 2008]. However, 3GPP does not specify a mandatory IP based security mechanism for the access network part of a mobile system architecture. Therefore, the question mentioned previously can be rephrased into the following:

Is it viable to implement IP based security solutions such as IPSec at Radio Access Networks to securely transport traffic? And which are the impacts in relation to the high speed expected performance for all-IP next generation mobile networks?

1.3 Problem statement

Given both, the need for a secure transaction medium for IP based Radio Access Networks, specifically for unprotected data between fixed network elements, and the need for best performance in high-scale mobile network environments, the aim of this thesis is two folded:

i. To evaluate the performance and
ii. To analyze the impacts of IP Security Protocol as the security solution between fixed network elements of large scale Radio Access Networks.

1.4 Overview of the approach

Emulation scenarios for RAN implement IPSec between two security gateways as the endpoints an IPSec tunnel, emulating the network fixed elements of a Radio Access Network. A traffic generator emulates traffic loads that traverse the RAN. Stress testing emulates large-scale networks behavior which offers a comprehensive approximation of a real-world network scenario.

1.5 Scope

- This work focuses on security implemented at the fixed network segment of the Radio Access Network. Analysis of IPSec at wireless access link is out of scope of this research work.
- RAN architecture is limited to a specific composition of the main elements that constitute the fixed network. Nevertheless, given the fact that same mechanisms shall be implemented in future IP mobile networks, results apply to other radio access environments such as LTE.
- IPSec implementation settings are bound to a specific profile.
1.6 Chapter outline

The structure of this thesis is as follows. Chapter 2 presents existent literature work in the field of study. Chapter 3 and Chapter 4 introduce basic concepts of IPSec and RAN. Chapter 5 develops on relevant concepts for analyzing IPSec performance. Testing scenarios are included on Chapter 6. Results and analysis measurements can be found at Chapter 7 followed by overall conclusion in Chapter 8.
2 Background

Previous research is the basis for this work; therefore relevant information is grouped into three main streams: first, research on security mechanisms at Radio Access part of a mobile network followed by research on IPSec performance and finalizing with current state of art of the conjunction of both research fields. This section aims to present a logical sequence of facts to justify the need for this work.

2.1 Radio Access Network Security

Security within the context of mobile networks aims to protect two main elements: user related information; and resources and services provided by serving networks. Therefore, protection against misuse or misappropriation of this sensitive data and resources must be achieved.

An efficient implementation of security measures should be coherent with both the type of information being protected and the type of threats being defeated. Because of this, 3GPP, a telecommunication consortium, introduced a security architecture for 3G systems that differentiates mobile network elements’ interaction according to functionality. As a result, five security domains are defined: Network access security (I), Network domain security (II), User domain security (III), Application domain security (IV), Visibility and configurability of security (V) [3GPP TS 33.102 2006].
Figure 1 indicates the distribution of security domains in 3G architecture. Each security domain represents a network implementing a set of security mechanisms.

At network domain security (II), 3GPP specifies the use of the Internet Protocol Security (IPSec) as the security mechanism to offer confidentiality, integrity and authentication for communication between network elements [3GPP TS 33.210 2008]. In the case of Network access security (I), authentication algorithms and key generation functions provide user authentication, user identity confidentiality, and data integrity. Based on this, it is evident that Network access security (I) is a critical security area mainly because of the nature of the wireless link. Consequently, security mechanisms specified for this domain focus mostly on the air interface.

Early analysis on security mechanisms for 3G first release (Rel99) [3GPP TS 33.102 1999] outlined the absence of protection for the different types of traffic flows not only at the air interface but also at the fixed part of an IP RAN [Gopal 2001]. The same study by Gopal analyzes the viability of different security solutions and concludes that IPSec is the logic choice as a security method to implement at the IP RAN.

To overcome some of the evident security flaws, 3GPP later release [3GPP TS 35.201 2001] included standardized versions of encryption algorithms to provide integrity and confidentiality to signaling data. However, user plane data remains unprotected since 3GPP does not make mandatory the protection for user data traffic in 3G networks.

Current research on UMTS security also identifies the lack of protection for user plane data [Xenakis 2008]. To overcome this, the same author suggests two mechanisms for user data traffic protection: KiloByteSSL and IPSec. The main difference between the suggested solutions is the layer level of implementation.

---

1 Picture taken from [Xenakis 2008]
within an OSI layer model context; in one hand, at the application layer, Secure Sockets Layer (SSL) protocol is the foundation concept for the implementation of KiloByteSSL [Gupta et. al. 2001]. On the other hand, at the network layer, IPSec protocol is the preferred solution.

Clearly, state-of-art research on Radio Access Network security connotes the need of security solutions. Furthermore, they foresee the implementation of IPSec as the facto solution for secure access to a mobile environment. This is true for latest 3GPP releases [3GPP TS33.203 2008] [3GPP TS 33.210 2008], that is, in a pure all-IP mobile network environment, in which application of IPSec mechanisms at different network levels is mandatory.

2.2 Internet Security Protocol performance

Performance analysis of IPSec protocol has been extensively studied, for instance research in [Shue et al 2007] and [Zoltan 2006]. Due to the complex nature of the protocol, existent research on IPSec performance includes a wide range of diverse implementations in terms of protocol particularities (e.g. encryption algorithms, key management protocols) and technology contexts (e.g. wireline and wireless links, video applications, voice applications). Nevertheless, the common factor when analyzing IPSec performance concentrates in two basic aspects: space complexity and time complexity. The following paragraphs show some of the most relevant research on IPSec performance.

Work in [Barbieri et al 2002] measured the overall effects of encryption and decryption operations on throughput. By analyzing the performance of voice traffic transmitted over IPSec, their results show that IPSec causes a significant reduction in the expected bandwidth evidencing the cryptographic engine as the bottleneck for voice traffic.

A different approach by [Hadjichristofi et. al. 2003] focus on the overheads imposed by IPSec when transferring different file sizes by means of different protocols in both wireline and wireless scenarios. Two important findings are distinguished; first, file size has a significant impact in terms of time complexity being small file sizes the reason for longer transfer time values; secondly, computational capabilities are also related to time complexity in the sense that faster processors achieved better results.

Data length impact is also studied in [Mujinga et al 2006] and concludes that for smaller data packets IPSec overhead impact is higher in comparison to larger data packets. In regards to the impact of processing capabilities, [Ronan et al 2004] also determined that as processing capabilities increase the overall performance increase as well. Therefore, it should possible then to improve the overall performance by means of hardware cryptographic accelerators [Miltchev 2002].
Despite most of these works perform small-scale Emulations their contributions also apply when implementing IPSec in large scale environments.

Of particular interest for this work is performance of IPSec in large scale networks. Research by [Okhee 2003] measures the impact of different IPSec configurations in large scale networks. Obtained data offers a baseline framework for comparison with current speed connection values and current workload data for large scale networks. Nevertheless, his work offers a comprehensive framework for test modeling.

A more recent study [Wenlung et al 2006] analyzes the implementation of IPv6 protocol in a large-scale network environment. IPSec is part of IPv6 specification therefore the relevance of such study. Wenlung et al. findings suggest that performance for both IPv4 and IPv6 is almost the same.

By now, based on previous research, it is obvious that IPSec implementation implies a reduction on the overall performance of a system affecting space and time complexity factors. However, there is still the need to analyze IPSec behavior in mobile networks contexts since performance requirements in mobile networks differ from those in fixed networks.

### 2.3 IPSec in RAN

Within the context of cellular Radio Access Networks, IPSec research mainly focuses on future all-IP based network infrastructure and mobility protocols such as Mobile IP. This is explained by the fact that, until now, traditional transport methods for RAN such as Asynchronous Transfer Mode (ATM) offer full control of RAN data traffic [Peyravian et al 1997]. Therefore in a scenario where ATM and IP coexist there is not an urgent necessity for implementing security.

Current work [Zoltan et al 2006], analyze end-to-end IPSec protected mobility scenarios in heterogeneous access networks environments. Their findings show that adding IPSec security to mobility transactions does not represent a considerable increase in the response time. However, this research does not consider the processing overhead caused by key management protocols.

In future mobile networks such as the IP Multimedia Subsystem (IMS), access security is foreseen to be protected by means of IPSec security associations. Analysis work by [Agrawal et al 2008] identifies scalability issues due to the stateful nature of messages for establishing a secure transaction.

Recent research suggests the implementation of mobile Virtual Private Networks (VPN) for protection of user data in UMTS Networks. Three different schemes of VPN implementations are suggested: end-to-end [Xenakis & Merakos 2004],
network-wide [Xenakis & Merakos 2006], and border-based [Xenakis et al. 2006] VPNs. The main drawback for the end-to-end solutions is the isolation of the communication channel since neither the data itself or an external application can access the data. In the case of network-wide and border-based solutions, even though the actual end point of the tunnel is the UMTS infrastructure, the mobile system needs to implement a specific security client. Moreover, for user mobility, the VPN tunnel must be renegotiated [Xenakis et al 2004].

Given the existent state-of-art research for IPSec, there is still the need to verify performance of IPSec within RAN context. Furthermore, the implementation of security measures such as IPSec in large-scale network environments.
3 Radio Access Networks

Radio Access Networks main functionality is to provide a medium for the mobile user to register into the mobile network. Access network functionality then is conformed by a set of protocols that define this procedure; Telecom operators implement its own RAN infrastructure based on standard specifications. The following section describes the access technologies for two relevant mobile systems UMTS system and LTE project, and introduces the relevant network architecture for this work.

3.1 WCDMA

Wide Code Band Multiple Access (WCDMA) technology was developed in the beginning of 2000 by NTT DoCoMO, a Japanese telephone operator. Due to its success, WCDMA became the standard air interface for the International Telecommunications Union’s (ITU) cellular networks. Later on, 3GPP adopted the technology for its own 3G systems resulting in the UMTS system.

Universal Mobile Telecommunication systems (UMTS) technology specification defines UMTS Universal Terrestrial Radio Access Network (UTRAN) as its access system [3GPP TS 25.410 2002]. UTRAN implements Wide Code Band Multiple Access (WCDMA) radio interface to achieve high access rates of the order of 2Mbps to 14Mbps. In Europe, WCDMA has been widely adopted and developed as the radio access network for current networks.

3.1.1 3GPP Network architecture

3GPP, a standardization body, defines a network architecture for UMTS to serve as a common reference point mainly to achieve interoperability among operators that might differ in their implementations. Figure 2 shows the overall architecture for UMTS. UTRAN is the access network and serves as an interface between the User Element (UE) and the Core Network (CN).
As Figure 2 shows, UTRAN is composed by two main elements: Radio Network Controller (RNC) and NodeB (Base station). The former is in charge of controlling the resources for the allocated NodeBs. The latter supports radio cells to offer connectivity to mobile users.

Connectivity between network nodes is enabled by links named interfaces which implement protocols to achieve communication. There are three main interfaces at RAN that describe the links between the network elements:

- **Iub.** Interconnection point between the RNC and NodeB. It is possible to allocate more than one NodeB into the same RNC.
- **Iur.** Offers connectivity among RNC.
- **Uu.** Defines the radio interface between the user equipment and the access network.

In order to achieve communication the implementation of protocols at the interfaces are categorized in two groups:

- **i. Control plane protocols.** Provide access to network and services such as mobility, session and radio resource management.
- **ii. User plane protocols.** Related to user application data such as multimedia messaging, peer to peer applications, instant messaging, and location based services among others.

---

2 Picture taken from [Brännström 2007]
UTRAN 3GPP standard also specifies a layered model division for RAN: Radio Network Layer and Transport Network Layer. Nodes and Interfaces are part of the Radio Network Layer while Transport Network Layer provides transport services for signaling and user planes[3GPP TS 33.210 2008]

Based on this, communication procedures at RAN can be resumed as the exchange of signaling and user data between network elements by means of specific protocols associated with the type of data. The medium that facilitates the communication between these elements resides at the Transport Network Layer.

Traditionally, transport media was based on Asynchronous Transfer Mode (ATM) technology. With the advent of service convergence, transport media demanded new requirements. It is precisely through transport network layer where the introduction of IP is enabled.

### 3.1.2 IP in WCDMA RAN

Implementing IP as the transport protocol enables implementation of new applications and services; furthermore it enables the convergence of heterogeneous technologies into a single mobile network. For this to be possible, it is necessary an adequate configuration of the underlying architecture to achieve efficient transmission of data. Following sections describe a reference scenario for a Radio Access Network infrastructure implementing IP at the Iub interface.

#### 3.1.2.1 Traffic types

Data traffic types traversing the Radio Access Network map to plane components previously mentioned in section 3.1.1. The resulting traffic types are:

- User traffic, carrying end user data flows.
- Control traffic, signaling procedures for successful delivery of information and services

Additionally, two more traffic types are defined:

- Synchronization traffic such as Network Time Protocol (NTP) traffic for synchronization procedures between network elements and time server.
- Operation and Maintenance traffic, for proper functionality and availability of the network.
3. Radio Access Networks

3.1.2.2 Traffic segregation

With the concept of security on mind, separation of traffic in RAN is essential for both performance and security purposes. Different technologies such as Multiprotocol Label Switching (MPLS), Virtual LANs (VLANs), Generic Routing Encapsulation (GRE) and Virtual Private Networks (VPN) achieve this purpose. The later, Virtual Private Networks (VPN) technology, offers an adequate solution for distribution of data traffic flows according to two models:

- **Common virtual networks** where all the traffic flows are allocated within the same VPN; and
- **Independent virtual networks** where traffic flows are assigned to different VPNs.

For an independent virtual networks scenario, traffic flows are grouped in two VPNs. User, Control and Synchronization flows are allocated in one single VPN referenced as the “Iub traffic”. Operation and Maintenance traffic is allocated in a separate VPN, that is, “O&M traffic”.

3.1.2.3 Traffic protection

Most of the security mechanisms implemented at RAN networks reside at the radio interface part of the network since it is the first point of access to the network. At the Iub link, protection mechanisms should mimic those implemented at radio interface to offer the same quality of service each type of traffic demands. Therefore, IP based transport network should offer protection mechanisms to all the traffic flows based on performance requirements of each type of traffic. Following paragraphs analyze traffic flows’ security requirements at the Iub interface.

For most of the cases, O&M traffic is protected at the application level by means of Secure Socket Layer (SSL) and Secure FTP (SFTP) technologies. Adding extra protection at the transport layer would add redundancy and overhead. However, given the fact that availability of the service depends mostly on the system being manageable, compromise of O&M traffic has an important impact on the system. Therefore, it should be considered to add protection to O&M traffic.

A peculiar case is synchronization traffic flow as it is a critical element for accurate communication. Implementation of synchronization traffic attacks are unlikely to happen since it would require the attacker to introduce accurate illegitimate timestamps in a large scale basis. However, inconsistency in synchronization traffic leads to inability of the network and services; consequently authentication of synchronization traffic should be considered.
Despite the availability of solutions to protect control plane data such as confidentiality and integrity algorithms (f8 and f9 algorithms) [3GPP TS 35.201 2001], local encryption regulations might be an impediment to implement these solutions. Therefore, protection for control plane data should be offered by other means.

User plane data protection occurs at the radio interface by means of encryption algorithms [3GPP TS 35.201 2001]; however, at the Iub link there are no specific security measures to protect user plane data. Since user data traffic also contains sensitive information its protection should not be omitted.

### 3.1.2.4 Security architecture

An adequate security framework for any system should resemble the architecture it aims to protect. Therefore, an adequate security framework for mobile networks should map to a stratified model where security planes implement security services according to each plane requirements. ITU-T X.805 standard [ITU X805] provides such solution. This framework defines three security layers: infrastructure, service and applications; and three security planes: management, control and end-user. It also defines eight security dimensions that apply for both security layers and security planes. The overall goal is to segregate security planes functionality based on security policies and principles.

With this in mind, network security design should adopt ITU-T X.805 best practices. As a result, network infrastructure is divided into Security Domains. Each security domain manages specific traffic flows. Consequently, there is a correspondence between traffic segregation models (defined in section 3.1.2.2) and security domains. In addition, Virtual Private Network (VPN) technology should be implemented where necessary to ensure confidentiality of data.

### 3.1.2.5 Network architecture

Figure 3 shows the reference scenario for the described security infrastructure. In order to support IPSec, both nodes, RNC and NodeB, implement a standalone security gateway (SEGw) as termination point for IPSec tunnel. Therefore Iub implements IPSec gateway-to-gateway configuration.
Main elements to distinguish are: the Security Domains (SD) for which different access policies apply; the VPN tunnels that carry traffic O&M and Iub traffic flows; and the untrusted zone where connection of security gateways takes place.

### 3.2 LTE

Long Term Evolution (LTE) is the next evolutionary step for UMTS supporting not only improved services and applications but also higher data rates of the order of 100Mbps by means of radio techniques such as Orthogonal Frequency-Division Multiple Access (OFDMA) modulation [Chong et al 2006] and Multiple Input and Multiple Output (MIMO) [Zheng & Rao 2006].

Most relevant characteristics for LTE concern the low delay and latency requirements. For user plane, it is envisioned to have a round-trip delay time (RTT) less than 10ms which compared to current requirements for WCDMA of 200ms and 450ms[Gomez et. al. 2006] it is significantly faster.

Development of LTE technology is currently ongoing but it is already a reality and it is expected to reach a maturity level and commercial deployment by next year [3GAmericas]. Even though LTE is still in development, LTE foresees the integration of any access network technology which in practice represents a cost-effective solution for operators [Hoikkanen 2007].
3. Radio Access Networks

3.2.1 Network architecture

LTE delay stringent requirements are consequence of LTE’s flat network architecture approach. In such architecture, RNC functionality is redefined and integrated within the NodeB renamed eNodeB; therefore radio network functionality terminates at eNodeB. Figure 4 evidences the difference between WCDMA and LTE architecture.

![Figure 4. Comparison WCDMA vs. LTE access architecture](image)

3.2.2 Security

Due to simplification of network elements for LTE Radio Access Network architecture, entire radio access functionality, including access security methods, reside at eNodeB network element. According to latest documentation [3GPP TR 33.821 2008] signaling and user plane data protection reside at eNodeB; consequently, security measures should be adopted for the communication from eNodeB towards the core network. Even though details for implementing security at the link between eNodeB and LTE Core Network SAE are not specified, it is envisioned to apply network layer security solutions. Furthermore, future developments consider implementation of IPSec to achieve secure interconnection with non 3GPP standardized networks.

Because of this, the analysis of IPSec performance is also relevant for LTE environment. Of special interest is the delay impact of IPSec given the stringent delay requirements for LTE.
4 Internet Protocol security

Internet Protocol Security (IPSec) [Kent & Atkinson 1998] is a suite of protocols developed by Internet Engineering Task Force (IETF) research community in the late 90’s to provide data integrity, data confidentiality and data authentication at the IP layer; its main goal is to offer secure communication over insecure channels. The following sections briefly describe IPSec main elements as they introduce IPSec relevant parameters for this research work.

IPSec has been developed over the last years to conform a collection of subprotocols that offer three important concepts for a security solution: authentication, integrity and confidentiality. As a result, behind IPSec, there is a robust architecture that offers comprehensive security features. It is out of scope to describe all the implementation details for IPSec; for this reason this section presents the most relevant properties and briefly develops each of them.

4.1 IPSec suite architecture

IPSec functionality is based in two main elements:

i. A protocol to exchange security parameters (IKE) and

ii. IP header extensions to carry the cryptographic information (AH/ESP)

Briefly, IPSec operation is as follows; in order to create a cryptographically protected connection between two end-points, a session key must be established between an initiator and a responder side by means of the Internet Key Exchange Protocol (IKE). IKE protocol aims for end-points to exchange security parameters or proposals each of them support including: the type of service that is Authentication Header (AH) or Encapsulation Header (ESP); and the type of operation mode: Tunnel mode or Transport mode. Once both entities agree on the security features, they establish an active IPSec connection for the secured data.

4.1.1 Services

IPSec offers two types of services to secure a connection: AH and ESP. These services are IP headers to specify the cryptographic parameters they support. The election of a service is according to the end user needs.
4.1.1.1 AH

Authentication Header (AH) service provides integrity protection, authentication of origin and anti-replay attacks [Kent & Atkinson 1998a]. AH does not offer encryption services to the payload portion of the packet. Nevertheless, implementation of AH header might be suitable in scenarios where cryptography exportation restrictions exist. Latest implementation details for AH can be found at [Kent 2005].

![Figure 5. Authentication Header overhead](image1)

4.1.1.2 ESP

In contrast to AH, Encapsulation Service Payload (ESP) [Kent & Atkinson 1998a] not only provides integrity protection, optional authentication and anti-replay attacks services but also confidentiality by means of encryption. All services offered by ESP are configurable meaning that offered services can be activated or deactivated. A configuration mode of interest is ESP “Null Encryption” mode for which case confidentiality services are not offered. Under this configuration, ESP header has the same functionality as AH offering only integrity protection.

![Figure 6. Encapsulation Security Payload overhead](image2)
4.1.2 Operation modes

Configuration of IPSec services can be implemented either as a combination of both services or only one single service. Once the desired security level is selected, the actual transport of the data takes place according to the following connection modes.

4.1.2.1 Transport Mode

In transport mode, the original IP packet is segmented to allocate IPSec information between the IP header and the remainder of the data packet. Figure 7 represents the application of transport mode for both types of services. As the same figure shows, Transport mode protects the entire data packet. Because of this, transport mode is more suitable for end-to-end communications.

4.1.2.2 Tunnel Mode

In comparison with transport mode, Tunnel mode does not alter the original packet. In the contrary, it only adds a new IP header and IPSec information portions at the beginning of the IP packet. Therefore, tunnel mode is more suitable for connection between two networks or security gateways. Figure 7 shows Tunnel mode operation for both services.

Figure 7. IPSec overhead for service and operation modes
4.2 IKE

Internet Key Exchange (IKE) [Kaufman 2003] defines a robust protocol for mutual authentication and secret key setup between participating entities of a cryptographic secured connection. IKE specification differentiates three main tasks:

i. Endpoints mutual authentication
ii. Connection creation
iii. Keys and connection management

These three tasks are achieved in two exchange phases. IKE Phase 1 performs mutual authentication for the end-points by means of pre-shared keys, digital certificates or public key encryption. The output of this first phase is a session key to protect remaining IKE procedures. As next step, IKE Phase 2 performs once more mutual authentication based on IKE phase 1 session key. The output is an additional session key to protect the actual cryptographic connection.

The creation of a cryptographically protected connection is the most important outcome of IKE exchange phases. The protected connection named Security Association (SA) defines the configuration parameters such as IPSec service, encryption algorithm, key length, lifetime and granularity of the connection. There is one SA one for each phase of IKE exchange. Phase1 SA commonly called IKE SA; and phase2 SA called IPSec SA. In addition, there is one IPSec SA for each direction of the connection; consequently, two IPSec SA’s are associated with one secure connection.

Management of active connections is achieved by means of data structures that store information related to SAs properties and policy management such as security policies and filtering rules. By means of security policies, it is possible to create new SAs or to identify already established SAs through the SAI (Security Association Index). All this information is stored in the Security Association Database (SADB). In case a SA does not exist in the database, IKE negotiates a new SA. Renegotiation of a new SA originates each time a SA lifetime expires. This is called rekey procedure and it is specified in time (seconds) or data (kilobytes).

IKE exchange procedures work under two modes: aggressive and main mode. The main difference between them is the number messages they exchange. While main mode exchanges six modes, aggressive mode only exchanges three messages. Therefore aggressive mode is faster than main mode. However, faster resumption comes with a price since aggressive mode does not protect the identities of the endpoints. Therefore, aggressive mode is less secure than main mode.
4.3 Protocol overhead

Application of security methods has a direct impact in the overall performance for any system. This is also true for IPSec; several factors contribute to the detriment of the performance when applying IPSec. Reasons for this are grouped in two categories: time overhead and space overhead. The former is related to delay overheads introduced by cryptographic operations for encryption and authentication services. The latter is related to the increment on packets size by adding IPSec headers.

Space overhead imposed by IPSec to data packet size is mainly due to:
- Ciphering overhead for services
- Operation modes overhead

Ciphering overhead is proportional to the key length of cryptographic algorithms. For authentication operations, Keyed Hashing for Message Authentication (HMAC) is used in combination with either Message Digest Algorithm (MD5) or Security Hash Algorithm (SHA-1). The impact on size for authentication operations is of 12 bytes. Header size for both IPSec services (AH and ESP) is a fixed value of 12 bytes for AH and 10 bytes for ESP. In addition, ESP includes a variable padding field for confidentiality services of 12 bytes. Tunnel operation mode adds a new IP header of 20 bytes. The final result for header overhead is illustrated in Table 1 [Elkeelany et al 2002].

<table>
<thead>
<tr>
<th></th>
<th>AH</th>
<th>ESP</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Fixed</td>
<td>Variable</td>
<td>Total</td>
</tr>
<tr>
<td>Transport mode</td>
<td>12</td>
<td>12</td>
<td><strong>24</strong></td>
</tr>
<tr>
<td>Tunnel mode</td>
<td>12 + 20</td>
<td>12</td>
<td><strong>44</strong></td>
</tr>
</tbody>
</table>

Table 1. IPSec services overhead

4.4 IPSec as a standard for mobile networks

The main advantage of IPSec over other security protocols resides on its characteristic of transparent implementation for end users since it does not require any modification at the application level [Kaufman, Perlman & Speciner, 2002]. This means that IPSec is capable to protect any protocol residing above IP regardless the underlying medium supporting IP. This characteristic is of special interest given the introduction of heterogeneous environment enabled by an all-IP approach.
Because of this, IPSec is proposed as the security solution to implement in next generation mobile networks given. IPSec Specifications started in [3GPP TS 33.210] in Release5 specification set. Current [3GPP TS 33.210] Release7 specifies the use IPSec for the Network domain security only.

IPSec protocol suite robustness offers comprehensive security solutions. Diverse configuration settings enable different possibilities for security schemes. In order to implement a common solution that enables interoperability, 3GPP has limited IPSec settings according to Table 2. This profile applies to [3GPP TS 33.210] specification.

<table>
<thead>
<tr>
<th>IPSec parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transform</td>
<td>Encapsulating Security Payload (ESP)</td>
</tr>
<tr>
<td>Transport Mode</td>
<td>Tunnel Mode</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>3DES</td>
</tr>
<tr>
<td>Authentication Algorithm</td>
<td>HMAC with SHA-1</td>
</tr>
<tr>
<td>Key Exchange protocol</td>
<td>IKE main mode with pre-shared secrets</td>
</tr>
<tr>
<td>Diffie-Hellman group</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 2. 3GPP specification for IPSec

Even though, implementation of IPSec protection is not mandatory for 3G Access Network security, it is assumed that the same IPSec profile defined for Network Access Domain is applicable to Access Security. Therefore, IPSec profile described in Table 2 is the baseline profile for testing work.
5 Theoretical assessment

When analyzing the performance of network protocols it is important to focus in two main points: standard compliance and performance [Izquierdo et al. 2007]. To obtain relevant and reliable measurements for IPSec performance, four main concepts are developed. Following sections explain these concepts along with an approach from the IPSec implementation point of view. This section also introduces hypothesis for IPSec performance based on theoretical facts. In this way, predicted behavior can be compared against measured behavior.

5.1 Throughput

A key feature for next generation mobile networks is the ability to offer services and applications with high speed performance. The overall goal is to successfully deliver the data across the link. Because of this, it is important to measure the maximum possible quantity of data that successfully reaches its destination. Throughput is the maximum possible rate at which data can traverse a link without losing any information [Bradner 1991].

System throughput is dependent on different elements such as transmission media, link capacity, flow control, and the type of protocol being transmitted. The configuration of these elements directly affects the overall throughput.

In the case of IPSec, header overheads imposed by IPSec service modes contribute to the detriment of throughput. It is then cryptographic operations which mostly contribute to the total overheads [Okhee 2003]; IPSec offers the possibility to choose among different cryptographic algorithms. The selection of a specific algorithm impacts the performance. For instance, 3DES algorithm has poor throughput performance for encryption operations compared to its performance for authentication operations [Elkeelany et al 2002].

A characterization of the traffic load for a common scenario for UMTS suggest that maximum throughput can be achieved by means of larger packets size [Gomez et al 2006]. This is an important remark, since as previously described, only IPSec headers requires at least 44 bytes; Average packet sizes for UMTS traffic load range between 150 bytes and 800 bytes. Therefore, even though it is expected a decrease in throughput performance, results should still be acceptable for current UMTS traffic modeling.
5.2 Latency

Network latency, is the total amount of time that it takes for the data to traverse the network from its original point to its final destination. According to [Bradner 1991], latency measurement is based on the forwarding mechanisms of the devices under test. The results are store and forward latency and cut through latency; they differ on the packet’s reference point from where to start measurements. There is a wide range of reasons for high latency values. Usually, when processing a network packet, each process introduces an inherent latency: packetization delay, network transmission delay and packet delay variation; transmission delay is of main interest. In order to reduce the overall delay, traffic engineering and Quality of Service (QoS) mechanisms optimize traffic behavior. Therefore, it is critical a careful implementation of such mechanisms.

Latency requirements in mobile network environments are crucial for performance and it is expected to minimize latency values as much as possible. At RAN, low delay values are achieved by means of prioritized traffic. Such mechanisms should be homogeneous across the network. Because of this, synchronization traffic has the highest priority. By prioritizing synchronization traffic, delay and jitter requirements can be fulfilled. Therefore, at the Iub interface, synchronization traffic has the stringent requirement.

Table 3 shows the delay requirements for synchronization flows and user plane flows at the Iub interface.

<table>
<thead>
<tr>
<th>Traffic Flow</th>
<th>Recommended</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronization</td>
<td>20 microseconds</td>
<td></td>
</tr>
<tr>
<td>User plane</td>
<td>&lt; 5 milliseconds</td>
<td>30 milliseconds</td>
</tr>
</tbody>
</table>

Table 3. Iub latency requirements

Based on this, it is crucial then that IPSec protection for both synchronization flows and user plane flows, do not add a significant increment to delay. Even though IPSec inherent characteristics add latency there should be a threshold value for which it is acceptable to protect critical traffic flows (such as synchronization flows) by means of IPSec.

As in the same case as throughput, it is expected to observe an increment in latency values due to IPSec operation. Moreover, it is expected that IPSec surpass the
optimum value. In this way it could be possible to set a boundary for which IPSec is feasible to implement.

5.3 Frame Loss Rate

The ideal scenario in a network communication process is that one in which all transmitted data reaches its final destination in an accurate manner for the whole duration of the transaction. However, this scenario is not always possible due to facts such as delays, bandwidth, traffic congestion or other factors causing data traffic loss during the transmission. Frame loss values describe boundaries for acceptable performance for a particular system under overload conditions. Evidently, the fewer packets lost the best performance achieved. The main objective is to determine a threshold value for which loss rates values are minimum.

5.4 Capacity

Definition for capacity within a mobile network environment refers to the traffic load per network cell. In other words, capacity refers to the total number of simultaneous mobile subscribers able to acquire dedicated channels to establish a connection.

The Iub interface becomes a key factor to offer high capacity to end-users therefore it also determines the amount of supported users. Because of this, dimensioning procedures of Iub links either determine acceptable traffic loads for a given Iub configuration or determine the necessary Iub link configuration for a specific load [Xi et al 2006].

Since this work aims to find an acceptable load given a certain bandwidth when implementing IPSec, then, for purposes of this research, definition for capacity is in terms of the number of successful connections at the link between RNC and NodeB. Therefore, definition for a successful connection refers to a established communication in which no packet loss or at least minimum packet loss is achieved.

All the previous concepts referred in this section have an important contribution when defining the overall capacity. The overall goal is to find an acceptable configuration of the relation RNC-NodeB.
6 System Model

Given the implementation model of IP at the Iub interface detailed in section 3.1.2, following sections describe the architecture for emulation process based on previously described models.

6.1 IPSec Profile

Testing scenarios follow the IPSec profile defined by 3GPP (Table 1) which specifies the use of ESP header in tunnel mode and IKE protocol in main mode with pre-shared keys. The specification of the authentication and encryption algorithm is also predefined by 3GPP. For purposes of this work we will refer to the configuration in table as the “standard profile” for IPSec.

6.2 Scenarios

Scenario modeling takes into account two aspects: firstly, RAN implementation requirements for the introduction of IP at the Iub interface described in Chapter 3; secondly, the Benchmarking Methodology for Interconnect devices [Bradner 1999]. The later defines a framework to describe the performance of network interconnected devices. Chapter 5 develops further on the concepts relevant for this study.

As a result, Emulations focus on two testing scenarios. The first scenario implements a common virtual private network scenario described in Chapter 3 in which all traffic flows traverse the Iub link over a single IPSec tunnel. Therefore there is a single security association for bundle of traffic flows. (See Figure 3 in section 3.1.2.5)

The second scenario implements a dedicated IPSec tunnel per traffic flow that is an implementation of independent virtual private networks as Figure 8 shows.
6. System Model

Figure 8. Independent VPNs scenario

For both scenarios, measurements consider the connection of a single NodeB to the RNC. This aims to analyze performance for the relationship NodeB-RNC under ideal conditions.

A third scenario looks into the performance when more than one NodeB connects to the same RNC. The main goal is to analyze the response of the RNC under stress conditions.

6.3 Test bed configuration

Figures 9 and 10 illustrate the test bed configuration for scenarios emulation. The experiments use two security gateways as endpoints of the IPSec tunnel. Each gateway is the access point for RNC and NodeB sites. There is a connection between both security gateways to emulate the Iub link. Behind each gateway, there are emulated subnets which correspond to security domains for traffic flows. To emulate both, traffic traversing the Iub link and security domains, a single traffic generator is connected to both gateways. At the traffic generator there are transmit/receiver port pairs to register traffic behavior. For instance, traffic originates at the traffic generator port (transmit port) behind SecurityGateway1; then, traffic traverses the emulated Iub link and SecurityGateway2; finally, traffic reaches its destination at the traffic generator port (receiver port) behind SecurityGateway2. The receiver port registers the information describing traffic behavior. Links between network elements are 1 Gigabit Ethernet connections; therefore Iub traffic is carried over Gigabit Ethernet links.
Test bed 1 emulates a connection of a single NodeB to one RNC. Both testing scenarios, common VPN and independent VPN, use this configuration test bed. The VPN link between the security gateways is a persistent connection, that is, the VPN tunnel is already up and running for all test configurations. This means that performance measurements do not include tunnel setup times.

Test bed 2 aggregates NodeB connections to the RNC up to four NodeB. For each NodeB there is 1 GB link connection. Therefore the maximum amount of traffic load offered to the RNC does not surpass 4 GB.

For both scenarios, stress testing offers high loads of traffic consisting of frames from 64 to 1420 bytes. The range of packet sizes aims to avoid fragmentation since it can lower the throughput.
7 Results and Analysis

This section concentrates the results obtained for the conducted experiments. Results are presented in three groups. The first group comprises observations related to the performance impact of configuration settings derived from both IPSec protocol suite and third-party devices. These first results aim to find an acceptable configuration profile for a real-world network scenario. The second group includes the results obtained for the scenarios described in section 6.3. Lastly, the third group develops an impact analysis based on the concepts described on Chapter 5.

7.1 Configuration Impacts

Observations while measuring IPSec performance revealed the impact of configuration settings on IPSec performance coming not only from inherent IPSec properties but also from third-party equipment at the endpoints of the IPSec tunnel.

7.1.1 Equipment related

Despite it is out of scope to measure the performance of underlying devices, findings show an important impact for IPSec performance. The main objective is to segregate impacts from end-point devices from those related to IPSec. By doing this, it should be possible then to obtain more accurate results regarding IPSec performance impact independently of underlying devices.

7.1.1.1 Buffer and Ring size

Security gateways for conducted tests include two configuration properties which introduce significant impact on the results: buffer size and ring size parameters. The former relates to the number of packet buffers allocated to store data; the latter refers to the set of receive/transmit rings of the network interface controller (NIC) and their admissible packet buffer values to transmit and receive packets. By modifying these settings, throughput values dramatically increment compared to those values obtained when no modifications are performed at all, that is using default values. Figure 11 shows a comparison of IPSec throughput between two
configuration profiles: default settings and adjusted settings configuration. The default settings configuration does not include any change. The adjusted configuration maximizes the buffer size and optimizes the ring size for gigabit interfaces. Traffic load is unidirectional and frame size increments by a 64 bytes step. (Details for configuration profiles can be found at Appendix part Section C).

Figure 11. Security gateway settings impact

Figure 11 clearly shows that modifications on buffer and ring size improve throughput performance. This seems a logical behavior; under maximized configuration of the allocated space for packet flows, security gateways are able to process more packets in a timeline manner without frame loss. Therefore, when measuring throughput performance, the binary search algorithm for calculating the maximum throughput converges faster.

At this point, it might seem logic to set the configuration parameters of the security gateways to the maximum possible values to achieve the best performance. However, modifying buffer and ring values have a direct impact on latency values. Figure 12 and Figure 13 show average latency values obtained for two configuration profiles: adjusted settings (Figure 12) and default settings (Figure 13).
Two important observations derive from these results. First, the differences in latency patterns for each scenario (highlighted by a trendline); second, the actual latency values obtained (expressed in milliseconds). Latency pattern drastically changes among configuration profiles. In one hand, under adjusted settings configuration as Figure 12 shows, latency values for packet sizes smaller than 512 bytes are dissimilar from those values for packet sizes greater than 512 bytes.
After packet size of 512 bytes, latency values dramatically drop to less than 0.5 ms and maintain the same behavior for the rest of the frame sizes. In contrast, in a default settings configuration (Figure 13), latency values are smaller for packet sizes below 512 bytes and latency linearly increases as the packet size increase.

Figure 14 shows a comparison graph for both configuration settings scenarios. Latency behavior for both scenarios converges once packet size values are greater than 512 bytes.

![Figure 14. Latency Default settings vs. Adjusted settings](image)

Figure 14 also remarks the difference among latency values for both types of configuration. For default settings, latency values do not exceed 0.5 ms for all frame sizes. With adjusted settings, latency values dramatically increase to 3-4ms for frame sizes smaller than 512 bytes.

Adopting one configuration over the other depends on the traffic requirements for latency. Even though latency values obtained for adjusted settings configuration are relatively high in comparison to default settings configuration, values of 3-4ms are still acceptable for user plane traffic as Table 3 specifies. However, this is not true for latest technologies such as LTE, mentioned in section 3.2. LTE has stringent latency requirements in which it is expected to achieve a total round trip time of 10ms.

Since both configuration profiles are relevant, subsequent testing scenarios consider both configuration profiles.
7.1.1.2 Load period of time

The main characteristics of large-scale networks reside not only in the perimeter extension of the network but also in the amount of data being processed. In order to approximate to a real network traffic scenario, emulations should consist in stress testing by exposing the network configuration to heavy traffic loads during large periods.

In order to simulate large periods of traffic load, test duration maps to time periods of traffic. The larger the duration of the test the larger the amount of offered traffic load; in this way it is possible to achieve a better approximation to a real-world scenario. Figure 15 and Figure 16 describe throughput values for three periods of time (10, 15 and 60 seconds) and for both security gateways configuration profiles (default settings and adjusted settings). The offered traffic load is directly proportional to the duration of the transmission and it is automatically calculated by the traffic generator. The main purpose is to highlight throughput performance under high load conditions for different periods of time.

![Figure 15. Test duration impact. Default Settings](image-url)
Results for default settings (Figure 15) show a considerable variation in throughput performance as time period decrease. For small periods of traffic load, that is 10-15secs, throughput performance increase up to 10 times the results obtained for larger periods (60secs).

Despite the adjusted settings scenario registers the same behavior as default settings scenario, variation on the period of time for adjusted settings scenario does not signify an important difference on throughput performance. Still, the smaller the time period the larger the throughput achieved. This behavior is true for periods of time smaller than 60secs. For periods of time greater than 60secs obtained throughput values are approximately the same.

There are two reasons for difference on throughput values for smaller periods of time. The first one is related with security gateways internal processing capabilities. When performing a test, the offered traffic load increases as the configured period of time increases; this condition overloads security gateways processing capabilities and once the security gateway exceeds its processing thresholds incoming packets are dropped. This explains the fact that for adjusted settings scenario throughput performance does not differ as much as default settings scenario.

The second reason is related to traffic generator synchronization clock. In order to perform a test, the offered traffic load increases as the configured period of time increases; this condition overloads security gateways processing capabilities and once the security gateway exceeds its processing thresholds incoming packets are dropped. This explains the fact that for adjusted settings scenario throughput performance does not differ as much as default settings scenario. The second reason is related to traffic generator synchronization clock. In order to calculate throughput values, traffic generator merely compares sent frames against received frames based on a timestamp. Accuracy of calculations heavily depends on the port clocks at the traffic generator, influencing in some extent to the overall results.

It is important to remark that even though RFC 2544 [Bradner 1999] specifies a test duration value of 60 seconds for throughput testing, it was decided to test values below 60 seconds in order to emulate periods of short data transmission, that is
bursts of data. However, given the variability of results it was decided to set a default period of time of 60 seconds for the remaining test scenarios.

7.1.2 Protocol related

Even though 3GPP specification defines an IPSec standard profile, some implementation details are left open for user convenience. This section reviews only those parameters relevant for described scenarios implementing IPSec.

7.1.2.1 Rekeying

As mentioned in section 4.2, IPSec defines a rekey procedure to renegotiate keyed information once the SA lifetime value expires. From a security approach, a reasonable value for a SA lifetime considers small values. For instance, some default parameters range from 1200secs to 3600secs. However, an acceptable value depends on the type of information aiming to protect and applications requirements.

Figure 17 and Figure 18 show IPSec performance for two SA lifetime values. The first value sets a lifetime value of 3600s and 4096kb for both IP SA and IKE SA (With Rekey). The second scenario sets a zero value for both SA lifetimes; therefore, no rekey procedure is performed at all (No Rekey); By setting small values for SA lifetimes, rekey procedure is forced to trigger since traffic load exceeds the 4096kb value. The main reason for this is to evidence rekey procedures impact on performance.

Figure 17. Rekey impact for default settings
Presence of rekey procedures, within a default settings context (Figure 17), does not impact considerably throughput performance. However, there is a noticeable difference on throughput performance for an adjusted settings configuration (Figure 18), in which rekey procedure decrease the performance in 80%.

Acceptable SA lifetimes values are certainly a point of discussion. As mentioned before, from a security point of view, SA lifetime values should remain as low as possible to avoid situations in which an encrypted tunnel is unused for longer periods of time. This is mainly due to two reasons. Firstly, IPSec tunnel consumes resources; secondly large SA lifetime values enable a security vulnerability since the more encrypted information an attacker dispose the easier for her to decrypt information.

From a performance point of view, rekeying considerable degrades performance by increasing frame loss due to tunnel renegotiation. This property does not suit real-time applications in which packet loss degrades performance.

A possible solution is to configure a second tunnel as a backup. In this way when the first tunnel performs rekeying, the active connection should automatically shift to the backup tunnel. This method is called session resumption [Sheffer et al. 2008]. Because of this, subsequent tests configure SA lifetime values with zero values for both parameters (kilobytes and seconds) which specify that no rekey procedures should be performed. In this way, session resumption scenario is simulated to some extent. However, there is no implementation of the failover protocol at all. Nevertheless it gives a good approximation to a real-world scenario.
7.1.2.2 Cryptographic algorithm

In addition to performance evaluation of IPSec profile defined by 3GPP, performance evaluation of other encryption modes is relevant for new technologies such as LTE; specifically, IPSec null encryption mode and AES encryption algorithm.

Figure 19 and Figure 20 show comparison graphs when using 3DES, AES and null encryption modes for both configuration settings: default and adjusted settings.

For both scenarios, 3DES algorithm registers the smallest throughput values for all frame sizes. Nevertheless, 3DES and AES performance have almost identical values. This behavior is more evident in default settings scenario.
7. Results and Analysis

For an adjusted setting scenario, all the operation modes show almost similar throughput values until packet size value of 512. After this point AES and Null encryption performance surpass 3DES performance.

For LTE, relevant results refer to a default settings scenario since adjusted settings pose an important increment on latency (as described in section 7.1.1.1) which is not suitable for LTE. In this case, it stands out that even with null encryption throughput gets its maximum value for only 35% of the total line rate.

7.2 Scenarios Emulation

Lessons learned from previous section show that some configuration settings have an important impact on the overall performance. In order to achieve accurate results regarding IPSec performance, testing scenarios are aware of such settings.

7.2.1 Common IPSec Tunnel

Figure 21 shows throughput results when implementing one common tunnel for three flows. To achieve this, each flow includes VLAN tagging to differentiate traffic flows.

![One Common Tunnel](image)

**Figure 21. One common tunnel scenario**

The very first relevant observation while conducting one common tunnel test is related to security gateway behavior. As soon as the traffic generator begins to send the traffic for the first packet size (64 bytes), the security gateway registers high CPU loads and flooded buffers. After 5 seconds, an event called “dead peer” resumes the IPSec connection and reinitiates IKE exchange procedures.
Dead peer detection is a “keep alive” mechanism to detect a dead IKE peer. Once a peer is declared dead, IKE performs peer failover and declares lost resources [Huang et. al. 2004]. The event that triggers this mechanism is the high load condition. High loads on the security gateway introduce delays on its “heartbeat” pulses (a unidirectional message to prove liveness). After long enough time the peer is declared dead.

As the offered load decreases, the security gateway registers less dead peer events. This behavior is true for smaller packet sizes. Also, even though the very same behavior is present in both configuration settings profiles, it is less frequent in adjusted settings scenario due to optimized buffer space.

### 7.2.2 Independent IPSec Tunnel

In this scenario, there is one SA associated to each traffic flow. In total, there are three SA corresponding to the configured tunnels. Figure 22 and Figure 23 illustrate the throughput performance only for one flow and for one tunnel since the remaining flows and tunnels register the same values.

![Figure 22. Independent tunnels. Flow throughput.](image-url)
As in previous scenarios, adjusted settings scenarios register better performance in throughput when compared to default settings scenario. An interesting analysis derives from the comparison of both scenarios as shown in Figure 24 and Figure 25.
Throughput performance for both scenarios is very similar under default settings configuration. For this same configuration profile, common tunnel throughput values are slighter larger than independent tunnel scenario for frame values smaller than 512 bytes. The reason for this is high values related to the buffer space allocated.

An adjusted settings scenario registers a completely different behavior, in which independent tunnels performance significantly exceeds common tunnel scenario performance. The reason for this is mainly due to dead peer detection mechanism since such mechanism is applied in per tunnel basis. Therefore, even if one peer is declared as dead, the remaining tunnels will remain active. Consequently, the traffic generator registers a larger number of received packets.

### 7.2.3 Aggregated traffic

Test bed configuration 2 (section 6.3 Figure 10) shows the scenario emulating more than one NodeB connected to the same RNC. One port at securityGateway1 emulates one NodeB. The main goal is to measure the performance of IPSec for concurrent connections under high load traffic. SA granularity is implemented under a per host basis in order to achieve a greater number of connections. Each NodeB emulates traffic for 100 subnets; there are up to four NodeB connected to the RNC therefore the total amount of concurrent SA is 400. This scenario is implemented under adjusted settings profile. Figure 26 shows the results.
Evidently, presence of a major number of active SA signifies a detriment on performance. Throughput decreases to 50% less when compared to scenarios where there is only one SA active under adjusted settings (See figure 23). A meaningful observation is the presence of buffer overflows and high CPU utilization reported by the security gateway as the number of security associations increased.

7.3 Impact analysis

7.3.1 Throughput

The mechanism used to measure the highest rate at which the data can be forwarded is as follows. The traffic generator sends frames at the maximum theoretical throughput supported by the link, in this case 1000 Mbps. The receiving end compares the number of received frames to the number of sent frames, if they match then the offered frame rate corresponds to the maximum rate; otherwise, the test decrements the offered load by means of a binary search algorithm until there is no frame loss.

Figure 27 shows the results for IPSec throughput performance for a single security association implementing the IPSec standard profile for both configuration profiles: standard and adjusted.
When compared against clear text performance, it is obvious the overall reduction that IPSec implies. Throughput reduces until 80% for a default settings configuration. Even for adjusted settings scenario there is a significant reduction on the overall performance, especially for small size frames. This represents a significant detriment of performance considering that the offered load is only in one direction.

The most important observation is the low throughput values obtained for packet sizes below 512. A possible reason for this is that processing small size packets requires more CPU cycles than processing larger size packets. This is true regardless the type of data: clear-text or encrypted data.

These results match the theoretical analysis elaborated in Chapter 5: “throughput performance is highly associated with the packet size”. Testing results offer a quantification of this statement.

This affirmation reveals an important impact on RAN traffic. For instance, given that packet size for user data plane traffic depends on the application and assuming that average packet size for streaming applications range from 750 to 800 bytes; if traffic is IPSec protected, then packet size would increase up to 850 bytes; therefore, achieved throughput would range between 45% -60% of the link. This might not be suitable for streaming applications which require high throughput rates.

Previous scenario considers unidirectional traffic only. In the case of bidirectional traffic, there is also a significant reduction. Such reduction is more evident for an adjusted settings scenario, where throughput values are as equal as a default settings scenario. This means that there is a reduction on throughput performance for bidirectional traffic even with adjusted values.
7. Results and Analysis

7.3.2 Latency

Benchmarking technology for network interconnect devices defines two types of latency: for store and forward devices and for bit forwarding devices [Bradner 1991]. The main difference between the concepts is placement of the reference point to begin measurements. Store and forward latency is the used definition for latency given the fact that security gateways inspect the entire packet.

The mechanism applied to measure latency obtains the elapsed time between a packet is sent in one end and received at the other end by means of timestamps. In order to achieve the most accurate results as possible, latency tests were executed with a specific throughput value according to each frame size. The throughput value then should correspond to the maximum value for which there is no frame loss.

For purposes of a comprehensive latency analysis, clear text scenario is first analyzed. Latency observations in Figure 29 show the average latency for clear text compared against IPSec latency for default settings scenario and adjusted settings scenario.

Figure 28. IPSec bidirectional throughput
Clearly, latency values for IPSec double those values obtained for clear text. Moreover, after packet size value of 512, IPSec latency linearly increments while clear text latency registers a decrement. Nevertheless, latency values for default settings scenario are still lower than 0.5 ms as opposed to adjusted settings scenario.

IPSec latency behavior for adjusted settings scenario resembles to clear text latency behavior in the sense that both scenarios register an increment in delay values for packet sizes lower than 512 bytes and a decrement after this point. Figure 30 shows a comparison of clear text latency against IPSec adjusted settings scenario.
IPSec increments latency up to three times clear text values. An interesting observation is that after the threshold value of 512, adjusted settings scenario reports values almost as low as clear text and default settings scenario. A closer look for packets sizes greater than 512 reveals that even though adjusted settings scenario sees a significant decrease in latency after 512 packet size, it still registers higher values than clear text and default settings scenario as Figure 31 shows.

![IPSec Latency](image)

**Figure 31. IPSec latency for packet size greater than 512**

The variation of latency is used as a measure of irregularity. Figure 32 shows standard deviation measurements for IPSec default and adjusted settings. Regularity in latency values for default settings scenario describes a more stable behavior as opposed to adjusted settings scenario where peaks describe irregular behavior.

![IPSec Std Deviation](image)

**Figure 32. IPSec Standard deviation**

Results show that latency values are strongly related to buffer space. In one hand, latency values increase as the space allocated for buffer increase. On the other hand,
if buffer space does not consider large values, the lower the throughput obtained. The reason for this is that incoming packets are queue until they can be processed (authentication, encapsulation and forwarding). Therefore when offering high loads, buffers saturate and delay grows significantly.

Two important affirmations derive from comparing the obtained values against latency requirements for Iub link. First, none of the IPSec configuration scenarios (adjusted and default) meet the latency requirements for synchronization data plane traffic. Second, as opposed to synchronization traffic, IPSec latency values do meet user plane traffic delay requirements.

### 7.3.3 Frame Loss

Procedure to calculate frame loss is as follows: for each frame size, traffic generator offers an initial load rate based on the frame size. This process iterates until there is no frame loss. Figure 33 shows frame loss percentage per frame size when offered high loads of traffic. Traffic is expressed in millions of frames per second. Percentage scale starts from 10% for better readability. The main goal is to evidence system behavior under overload conditions.

![Figure 33. IPSec frame loss](image)

Evidently, the larger the packet size, the faster frame loss converges to a zero value therefore less iterations are needed. This explains the fact that for frame sizes of 1280 and 1480 bytes there is only one point value. In contrast 64 bytes needs a greater number of iterations to converge to zero value.

Both scenarios, default and adjusted settings, report the same behavior under stress conditions. Once the offered frame load decreases, adjusted settings scenario converges to zero faster than default settings. Figure 34 shows the values for frame
loss before converging to zero. Clearly, for the same traffic load, default settings scenario registers major frame loss than adjusted settings scenario.

Figure 34 also show behavior for zero frame loss. Evidently default settings scenario reports zero frame loss for lower values of frames received.

### 7.3.4 Capacity

Results for IPSec concurrent SAs tests (section 7.2.3), show that maximum achievable throughput equals to 20%-60% of the link capacity depending on the size of the packets. This is a significant detriment on throughput performance if it is assumed that total capacity at the Iub link is defined solely by the peak throughput.

Results on the same test show successful connectivity for all the 400 connections. However, even if the established connections are successful, each connection perceives a reduction on the available throughput meaning an impact to the service level offered to the end user.
Conclusions

This project aimed to evaluate and analyze IPSec performance as a protection scheme for Radio Access Networks at the Iub interface. Given the results, it has been showed that IPSec significantly reduces the overall performance and is not suitable for all type of traffic flows at Iub interface.

Given both, stringent delay requirements for synchronization traffic and high delay values for IPSec, it is not suitable to apply IPSec protection to synchronization traffic flow. Conversely, assuming equal delay requirements for control plane traffic and user plane traffic, it is suitable to protect Iub by means of IPSec for those applications which not require high throughput rates.

Clearly, there is a tradeoff between link capacity and delay variations. Emulation results showed that this behavior is tightly related to buffer space. High throughput values were obtained when optimizing settings for buffered data. However, this introduces larger values for latency. Consequently, IPSec at Iub is not suitable for delay sensitive applications.

Given the impact of configuration settings on delay performance, a possible solution is the adoption of cryptographic accelerators that enhance cryptographic capabilities improving performance of the system. However, analysis on performance impact of such configuration is left to future work.

Application of any security measure introduces inherent overhead. Final decision on implementation depends on security requirements for a given system.

At the end of the day, data revenues are key component for operators and they drive the need for higher bit rates. Therefore it is important to provide the best possible performance that includes both high data rates and lower latency. Furthermore, it is important to cover user demands with a security approach for availability and reliability of the system.
References


[3GPP TR 33.821 2008] 3rd Generation Partnership Project. TR 33.821 (V1.0.0.) Rationale and track of security decisions in Long Term Evolution (LTE) RAN/ 3GPP System Architecture Evolution (SAE), Release 8, April 2008


58


http://www.etsi.org/WebSite/homepage.aspx

[Gomez et. al. 2006] Gomez C; Catalan M; Viamonte D; Paradell J; Calaveras A; “Web browsing optimization over 2.5G and 3G; end-to-end mechanisms vs. usage of performance enhancing proxies” Wireless communication and Mobile computing. pp. 213-230 September 2006


[Huang et. al. 2004] Huang G.; Beaulieu S; Rochefort D. "A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers” RFC 3706. February 2004
[ITU X805] ITU-T Recommendation X.805. “Security architecture for systems providing end-to-end communications”. Available at: 
http://www.itu.int/itudoc/itu-t/aap/sg17aap/history/x805/x805.html


http://www.usenix.org/events/usenix02/tech/freenix/miltchev.html


[Xenakis & Merakos 2006] Xenakis C.; Merakos L.; “ Alternative schemes for dynamic secure VPN deployment over UMTS” Wireless personal communications. Volume 36 Issue 2, pp 163.194


Appendix

A. Hardware specifications

Security Gateways
Clavister Security Gateways 4200 series.
Processor: Intel Pentium 1599 MHz
RAM memory:

Traffic generator
IXIA Card 1 - 10/100/1000 ASM XMV12X
IXIA Card 2 - 10/100/1000 STXS4

B. Software specifications

IxExplorer 5.10.350 Build 9
IxAutomate 6.30.30.3 EASP1 Patch3

C. Configuration profiles

Default settings
Buffer size. Set to “Dynamic value” option which allocates approximately 1024 bytes for packet buffers in addition to 200 bytes as initial buffer size
Ring size. These settings apply for 1 GB interfaces
  Receiver (Rx). 64 bytes
  Transmitter (Tx). 256 bytes

Adjusted settings.
Buffer size. The maximum possible value according to RAM. In this case the maximum possible value is 200 000 bytes
Ring size. These settings apply for 1 GB interfaces
  Receiver (Rx). 512 bytes
  Transmitter (Tx). 1024 bytes
Due to availability reasons, two types of IXIA card were used for conducting testing. Results obtained for each card differ in some extent. This is mainly due to clock synchronization residing on the IXIA side. Even though the best performance results were obtained with IXIA Card1, due to software availability reasons, measurements presented in this report consider solely the use of IXIA Card 2.

Some of the proposed case scenarios could not be tested because of limitations of hardware. For instance testing of IPSec AH encapsulation mode; Clavister Security Gateways do not support AH. Also, it was not possible to measure the impact of not dropping the first SYN received packet when setting up the IPSec tunnel since this is not a configurable feature.

While performing testing, it was noticed that packet loss for security gateways ports is not uniform for all port pairs. In some extent, uneven forwarding rates at security gateways port had an impact on latency and throughput measurements.

### Table 4. Configuration profiles

<table>
<thead>
<tr>
<th>Configuration Profile</th>
<th>Buffer Size</th>
<th>Rx Ring Size</th>
<th>Tx Ring Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default settings</td>
<td>1024 bytes</td>
<td>64 bytes</td>
<td>256 bytes</td>
</tr>
<tr>
<td>Adjusted settings</td>
<td>200,000 bytes</td>
<td>512 bytes</td>
<td>1024 bytes</td>
</tr>
</tbody>
</table>