UNIVERSITY OF VAASA

FACULTY OF TECHNOLOGY

TELECOMUNICATION ENGINEERING

Bahaa Eltahawy

SECURITY AND PRIVACY ISSUES IN MOBILE NETWORKS, DIFFICULTIES AND SOLUTIONS

Master's thesis for the degree of Master of Science in Technology submitted for inspection, Vaasa, 1 October, 2014.

Supervisor	Professor Timo Mantere
Instructors	Professor Hannu Kari M.Sc. Reino Virrankoski

ACKNOWLEDGEMENT

First of all, I would like to express my deepest appreciation to all my professors, who really provided me with their valuable times, advices, and helped me throughout my studies. I would like to thank my advisor Professor Timo Mantere for the great opportunity he gave me by supervising this thesis. My sincere appreciation and thanks to my first instructor Professor Hannu Kari for firstly inspiring me about this special field, and secondly for encouraging my research with the valuable times, comments and ideas he provided me. Special thanks to my teacher and my second instructor Senior Researcher Reino Virrankoski for all the effort and facilities he gave me, which I believe without him this work would never have been done. At last, but not least, I would like to thank my teacher Professor Mohammed Elmusrati for his help and for sharing the knowledge.

Secondly I would like to thank my family. Words cannot express how grateful I am to my mother, father and my brothers for all the sacrifices they have made on my behalf. I also would like to thank my dear friend Anita Ratajczyk whom I dedicate this work to, for her support, encouragement and being always by my side. Special thanks to my dear friend Maria Castela, as well as to all my friends.

TABLE OF CONTENTS

ABBREVIATIONS

3DES	Triple DES algorithm
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard algorithm
AH	Authentication Header Protocol
AK	Anonymity Key, in UMTS
AKA	Authentication and Key Agreement
AMF	Authentication Management Field
ARM	Anonymous Routing Protocol for Mobile Ad hoc Networks
AuC	Authentication Center
AUTN	Authentication Token
BSC	Base Station Controller
BTS	Base Transceiver Station
CBC	Cipher Block Chaining
CIA	Confidentiality, Integrity and Availability
CK	Ciphering Key, in UMTS
CN	Core Network
CS	Circuit Switched domain
CTR	Counter mode
DCH	Dedicated Channel
DDoS	Distributed Denial of Service
DES	Data Encryption Standard algorithm
DH	Diffie Hellman algorithm
DHE	Ephemeral Diffie Hellman algorithm
DNS	Domain Name System
DNSSEC	Secured DNS
DoS	Denial of Service

DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
DTLS	Datagram Transport Layer Security Protocol
E2EE	End to End Encryption
ECDH	Elliptic Curve Diffie Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EDE	Encrypt-Decrypt-Encrypt mode
EK	Encryption Key
ESK	Encrypted Session Key
ESP	Encapsulating Security Payload Protocol
FACH	Forward Access Channel
FQDN	Fully Qualified Domain Name
GCM	Galois/ Counter Mode
GOST	Gosudarstvennyy Standart (Russian)
HE	Home Environment
HI	Host ID
HIP	Host Identity Protocol
HIT	Host Identity Tag
HLR	Home Location Register
HMAC	Hash Message Authentication Code algorithm
HTTP	Hypertext Transfer Protocol
ICV	Integrity Check Value
ID	Identification/ Identity
IDEA	International Data Encryption Algorithm
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IK	Integrity Key, in UMTS
IKE	Internet Key Exchange Protocol
IMS	Internet Multimedia Subsystem

IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPSec	Internet Protocol Layer Security
ISAAC	Internet Security, Applications, Authentication and Cryptography group
ISAKMP	Internet Security Association and Key Management Protocol
ISO	International Organization for Standardization
IV	Initialization Vector
K	Secret Key, in UMTS
KAC	Key Administration Center
K_c	Ciphering Key, in GSM
KDC	Key Distribution Center
KEA	Key Exchange Algorithm
KEYMGT	Key Management Protocol
K_i	Integrity/Authentication Key, in GSM
KRB	Kerberos algorithm
LBS	Location Based Services
MAC	Message Authentication Code
MAC	Media Access Control
MAP	Mobile Application Part
MAPSec	Mobile Application Part Security Layer Protocol
MD5	Message Digest 5 algorithm
MIKEY	Multimedia Internet Keying Protocol
MitM	Man in the Middle
MKI	Master Key Identifier
MS	Mobile Station
MSISDN	Mobile Station International Subscriber Directory Number
MTP	Message Transfer Part
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization

NE	Network Element
OR	Onion Routing
OSI	Open Systems Interconnection model
PCH	Paging Channel
PDA	Packet Data Network
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKA	Public Key Authority
PRF	Pseudorandom Function
PS	Packet Switched domain
PSK	Pre-Shared Key algorithm
RAND	Random Number
RC	Ron’s Code algorithm
RES	Response
RFC	Request for Comments
RLC	Radio Link Controller
RNC	Radio Network Controller
RSA	Ron **R**ivest, Adi **S**hamir and Len **A**dleman algorithm
RTCP	Real Time Transport Control Protocol
RTP	Real Time Transport Protocol
SA	Security Association
SCTP	Stream Control Transmission Protocol
SDA	Smartcard Developer Association
SDAR	Secure Distributed Anonymous Routing Protocol
SEED	national standard encryption algorithm in South Korea
SEG	Security Gateway
SGW	Signaling Gateway
SHA-1	Secure Hash Algorithm 1
SIM	Subscriber Identity Module

SIP	Session Initiation Protocol
SKEME	Secure Key Exchange Mechanism Protocol
SN	Serving Network
SP	Switching Point
SPD	Security Policy Database
SPI	Security Parameters Index
SQN	Sequence Number
SRES	Signed Response, in GSM
SRP	Secure Remote Password Protocol
SRTCP	Secure Real Time Transport Control Protocol
SRTP	Secure Real Time Transport Protocol
SS7	Signaling System No. 7
SSL	Secure Socket Layer protocol
STP	Signaling Transfer Point
TCP	Transport Control Protocol
TLS	Transport Layer Security protocol
TMSI	Temporary Mobile Subscriber Identity
TTL	Time to Live
UDP	User Datagram Protocol
UE	User Equipment
U-LU	Uplink Location Update
USIM	Universal Subscriber Identity Module, in UMTS
UTRAN	Universal Terrestrial Radio Access Network
VLR	Visitor Location Register
VoIP	Voice over IP
VPN	Virtual Private Networking
XRES	Authenticated Response
ZRTP	Zimmermann Real Time Transport Protocol

UNIVERSITY OF VAASA
Faculty of Technology

Author:	Bahaa Eltahawy
Topic of the Thesis:	Security and Privacy Issues in Mobile Networks, Difficulties and Solutions
Supervisor:	Prof. Timo Mantere
Instructors:	Prof. Hannu Kari M.Sc. ReinoVirrankoski
Degree:	Master of Science in Technology
Department:	Department of Computer Science
Degree Program:	Master´s Programme in Telecommunication Engineering
Major Subject:	Telecommunication Engineering
Year of completing the Master's thesis:	2014 **Pages:** 106

ABSTRACT

Mobile communication is playing a vital role in the daily life for the last two decades; in turn its fields gained the research attention, which led to the introduction of new technologies, services and applications. These new added facilities aimed to ease the connectivity and reachability; on the other hand, many security and privacy concerns were not taken into consideration. This opened the door for the malicious activities to threaten the deployed systems and caused vulnerabilities for users, translated in the loss of valuable data and major privacy invasions. Recently, many attempts have been carried out to handle these concerns, such as improving systems' security and implementing different privacy enhancing mechanisms. This research addresses these problems and provides a mean to preserve privacy in particular. In this research, a detailed description and analysis of the current security and privacy situation in the deployed systems is given. As a result, the existing shortages within these systems are pointed out, to be mitigated in development. Finally a privacy preserving prototype model is proposed. This research has been conducted as an extensive literature review about the most relevant references and researches in the field, using the descriptive and evaluative research methodologies. The main security models, parameters, modules and protocols are presented, also a detailed description of privacy and its related arguments, dimensions and factors is given. The findings include that mobile networks' security along with users are vulnerable due to the weaknesses of the key exchange procedures, the difficulties that face possession, repudiation, standardization, compatibility drawbacks and lack of configurability. It also includes the need to implement new mechanisms to protect security and preserve privacy, which include public key cryptography, HIP servers, IPSec, TLS, NAT and DTLS-SRTP. Last but not least, it shows that privacy is not absolute and it has many conflicts, also privacy requires sophisticated systems, which increase the load and cost of the system.

KEYWORDS: Privacy, Anonymity, End to end encryption, IPSec, DTLS-SRTP.

1. INTRODUCTION

Safety, security and privacy are basic rights for humankind; they are declared and guaranteed in all credible constitutions. These rights aim protecting individuals and their freedom, which is one of the most valuable privileges of humanity. With the introduction of new technologies and the evolution, demands and dependencies they caused, these rights got affected. Technology is playing a major role with human rights; it can provide a means for protecting these rights, or on the other hand can be misused and abused maliciously to violate them. With this double role, it is important to guarantee that the deployed technologies are utilized in the right way to serve the exact purposes, and to protect against all sorts of abuse.

The information age started around 1970s, with new facilities that serve the information availability and accessibility, and supported by an enormous technological revolution in the information and telecommunication industries. These technologies helped making the world closer, by mostly connecting the whole globe, and by providing services that ease the communication process. In turn, an enormous amount of data was exchanged between the communicating entities, through the different networks and infrastructures, with all levels of trustworthiness and security. Though the many benefits these entities gained out of this evolution, the situation was also worrying, since they do not hold control on their own data and its spread within such environment.

With these considerations, the general meanings of security and privacy have significantly changed; since the concerns exceeded the individuals to include their data, and hence certain requirements and measures are needed to afford the protection facilities. On the other hand, these requirements are of many conflicts with the other communication parties, which include operators and authority organizations. These parties have their own requirements, which by default do not match with individuals, since they require a level of data disclosure and accessing certain information according to the situation and the afforded protection level. These conflicts raise the complexity of these systems; furthermore they cause a dilemma of the system design, implementation and the means to meet the different parties' demands.

Technically, the most widely used mobile telecommunication system GSM succeeded in providing the needed connectivity; also it included the basic level of security measures. However, with the introduction and availability of new technologies, its security got completely broken, that is because GSM did not include but limited security services, also these fast technological changes were not expected. For the next generation of mobile networks, 3G CDMA/UMTS, it could benefit from the success of the GSM system, and it could avoid its security shortages by providing an advanced level and improved security mechanisms. This generation introduced new services and applications for users, which consequently led to sharing more data, including information about users and their identities, locations, payments, and the other activities. For such growth, the protection needs to be taken to a further level, to protect users' data from all sorts of illegal intrusion, either from outsiders or from inside of the malicious networks.

The classical security model, with its parameters confidentiality, integrity and availability, or what is collectively known as the CIA triad was the main security architecture for computer security and information security generally since 1975 (Saltzer & Schroeder 1975: 1278 – 1308). This model was acceptable for the older systems with the limited services; however, this model is no longer sufficient for the new challenges the current systems face. The Parkerian hexad model dealt with this issue by expanding the security model to include the necessary parameters utility, authenticity, and possession to the CIA ones (Parker 1998). In application, it was also found that non-repudiation is an important parameter to consider when building the security model, due to its consequences in the communication environment. This new model could cover mostly all aspects of security measures that are needed to build a robust system.

The main goal of this thesis is to study and evaluate these models as well as the associated security measures deployed in the mobile networks. The target is to find out the different shortages these systems face and how they affect end users and their privacy. This leads to providing suggested solutions for these shortages, also providing a prototype model to preserve privacy in mobile communication. For these purposes, a distinction between security and privacy needed to get well defined; also the different parameters and different perspectives were considered. The thesis was built upon the suggested privacy preserving model shown in Figure 1, which combines the basic parameters that are needed to maintain privacy, i.e. security and anonymity.

This thesis is organized in six chapters; the first three chapters explain the general security parameters and evaluate them in the different parts of the network, also they describe the mechanisms and protocols used in the security procedure. The fourth chapter provides the definitions, dimensions and arguments needed for privacy description. Finally, the fifth chapter presents suggested solutions to improve the security and privacy situation, and the sixth chapter proposes the suggested privacy preserving prototype model.

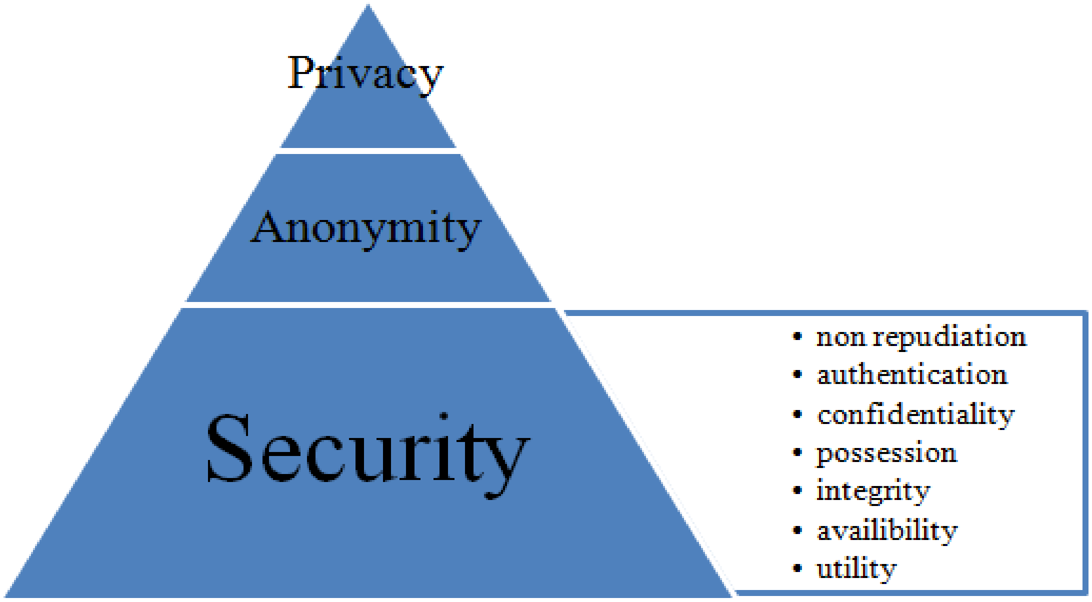


Figure 1: The fundamental privacy model.

2. SECURITY

According to the Oxford English Dictionary, security is “the freedom from danger or threat” (Oxford 2013). This definition is general and applicable to all systems; however, the specific definition of security depends on the system upon description. Security concerns providing the needed level of protection for the deployed systems; security categories include physical security, personal security, operations security, communications security, network security and information security (Whitman & Mattord 2010: 10). Since the telecommunication field is a part of the information technology category, its security is defined by the information security measures. Information security aims securing data and information within the employed systems. According to Straub, “Information security protects the availability, integrity, confidentiality, and authenticity of information and underpins such societal goods as privacy, the protection of digital identity, and the protection of intellectual property. Information security comprises a dynamic system of measures taken to protect data, information, and information systems from unauthorized use or a disruption due to a human agency or a natural threat” (Straub & Goodman 2008: viii).

To provide the adequate protection level, the different security parameters need to be fulfilled. In 1998, Donn B. Parker proposed a security model modifying the traditional CIA model. In his model, he included parameters of high importance that are needed to protect and control information; these parameters included utility, authenticity, and data possession (Parker 1998). Furthermore, non-repudiation as well is an important parameter that needs to be considered for building a complete security model; this parameter was mentioned in the earlier security model of the International Organization for Standardization (ISO) in 1989 (ISO 1989).

In the following sections, the different security parameters that constitute the base of the proposed model are discussed.

2.1. Utility

Utility is a new security parameter that was included by Donn B. Parker in his security model. Utility refers to the usefulness, and worthiness of the exchanged data (Andress 2011: 8). Though utility is one of the basic security concerns, it is not of much consideration from the network's and operation's point of view, since they view it as an abstract concept. The reason is that because utility has many levels, and it depends on the deployed applications and data formats these applications utilize, which is out of control of the communication facility. For example, if end users would utilize special encryption schemes or special data formats, that deployment might cause difficulties for data extraction at the other side, in other words, data might be useless for the other party. This is an important issue since it consumes the bandwidth and resources as well as costs for no clear advantage.

The utility issue lies within the application layer, and it can be described as the lack of standardization between the communicating peers. To solve this problem, the standards with their formats have to be followed, also if special formats would be utilized in special cases, e.g. confidentiality reasons, these formats have to be agreed upon before data exchange.

2.2. Availability

Availability is the readiness and reliability for resources to be accessed and used when needed (Stamp 2006: 2). This parameter is of high importance within the security model, since the different resources and assets have to be accessed for utilization to establish a communication session. These resources include Identifications/ Identities (IDs), addresses, locations, databases and users' privileges. Availability plays the base role in the security structure, since the above given resources should be available and reachable; otherwise the communication process will be meaningless. Also, shortages that might face one of these resources would affect the whole deployed system; and it might cause system failure.

Difficulties that resources mainly face are categorized in two categories; the first is the internal unintentional shortages while the other is the external intentional attacks. The first difficulty can be caused out of the unexpected resources' shortage, system failure due to certain actions or being not ready to handle some cases, and also natural disasters. This issue is related to the readiness of operators mainly to maintain safety measures, and it is their responsibility to take the different scenarios into consideration. This issue can be mitigated easily by affording parallel links, operating backup servers in addition to using higher speed links to avoid bottleneck problems.

The other difficulty is caused by the outer attacks that target the network to occupy its resources causing shortage of resources. This type of attack is called Denial of Service (DoS) and also can be performed by Distributed Denial of Service (DDoS) scheme. These attacks are the main problem that faces the availability. DoS attacks tend to bring the network down and to block the authorized traffic by occupying the resources. This normally occurs when a large amount of junk data is sent to fold up the servers and bottleneck the network. When service seekers demand a certain service, servers will not be able to handle or reply their query, or at the best case, they will suffer large delays and slow response (Needham 1993).

When it comes to mobile networks, DoS attack takes different forms. From the early GSM, the attack is performed by occupying the signaling channels by means of sending requests from unauthenticated Mobile Station (MS) devices in a specific Base Station Controller (BSC) (Bocan & Cretu 2004). This leads to shortage of resources for legitimate users as shown in Figure 2. Another technique is as early as connecting the GSM backbone to the Internet gateway; it is by sending a large number of SMSs to the active users within the network. Delivering this data is a complex scenario, and it consumes the network resources, and might cause failing the network (Enck, Traynor, McDaniel & Porta 2005). Normally because sending SMS does have a cost, this case occurs due to free of charge SMSs being sent from Internet server, or by malware infected phones.

A proposed solution (Spatscheck & Peterson 1999) for the DoS problem relies on three key factors, namely accounting, detection and containment. Resources of a user have to be accounted, that would help to detect the resources consumption caused by the user. When the user exceeds some certain threshold limits, he receives a dedicated extra server resources to handle the tasks in operation, thus the DoS case is avoided (Bocan & Cretu 2004).

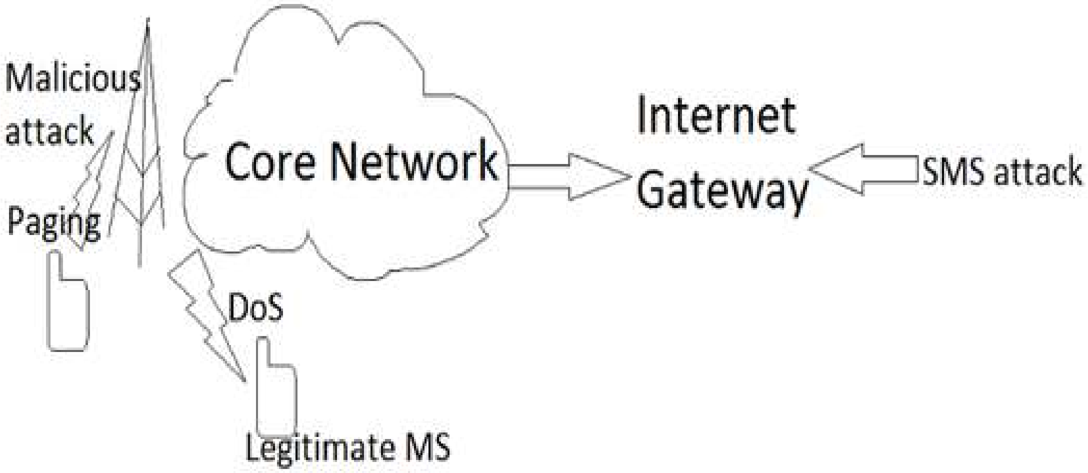


Figure 2: DoS attacks in GSM networks.

For 3G networks and beyond, networks rely on the Internet Protocol (IP) for communication and for the different services. The deployment of the IP increases the complexity against the DoS attacks, as the network becomes rich of signaling. One of the most DoS common attacks is the paging attack (Serror, Zang & Bolot 2006). This attack exists when the operator’s firewall is unable to detect the unwanted traffic. The attack occurs by sending data packets to an MS, which in turn triggers the paging channel and overloads it; additionally the MS resources get occupied. This situation causes the MS to fluctuate between the different states, which requires more signaling with the attached network, also it can make the device unreachable.

Figure 3 shows the mobile transition states in GPRS, which is similar in concept with the 3G but with only differences in the used terminologies (Ricciato, Coluccia & Alconzo 2010: 551−558). An MS has three states; idle, ready and standby. In the idle state, MS is not attached to the network, either out of coverage or powered off. In the ready state, the MS is attached to the network and it updates its location. Finally in the standby state, the MS is within the same cell and does not perform any updates. Within the standby state, the MS keeps listening to the network for paging requests; when it receives a request, it moves to the ready state. Between the ready and standby states, there is a timeout which changes the state of the MS if not transmitting data or receiving paging to the standby state, thus saving radio resources and the MS's battery.

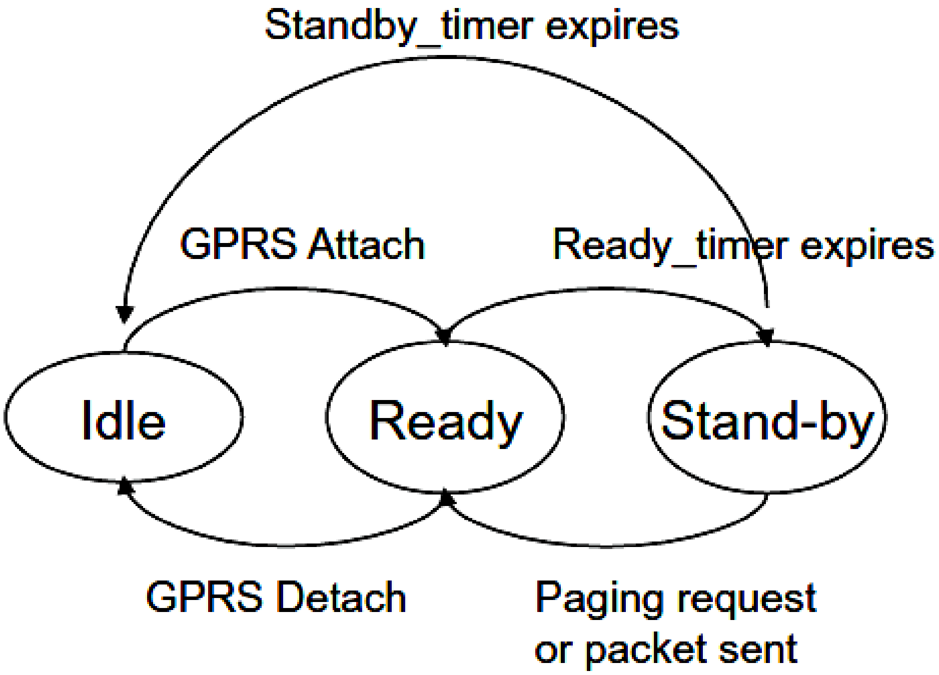


Figure 3: MS transitions in GPRS (Ricciato *et al.* 2010).

The other type of the DoS attacks on 3G is the signaling attack (Lee, Bu & Woo 2007). An MS normally switches between two channels, the Dedicated Channel (DCH) in the download/upload mode and the Forward Access Channel (FACH) in the silent mode, where the timeout in between is 30 to 120 seconds (Chandra, Kumar, Gupta, Kumar, Chaurasia & Srivastav 2011: 407). The attack is taking two scenarios; the first is either by triggering the MS at times larger than the timeout period, so that it switches back to the DCH channel again which causes signaling overload to the network. The second scenario is on the contrary to the first one, performs triggering with times shorter than the timeout period, so that the DCH channel does not get released, which shortens the resources of the other service seekers.

These signaling and paging attacks form malicious DoS attacks as they leave the legitimate users with short resource. The solution for these attacks lies in two levels, namely randomization and fragmentation of the paging channels (Chandra *et al.* 2011: 406 – 410). Randomization of the timeout increases the probability of defense against the paging attacks made at certain time values. If the timeout would be longer than the attack frequency, the Paging Channel (PCH) will not get occupied; also if it would be short enough, the DCH will be free. However, with this solution, MSs would suffer from triggering between the different states; also staying longer time in the ready state is not feasible for MS's battery consumption and the radio resources.

In the second solution, the IP addresses along with the PCH channels are fragmented into subsets. With this solution, when a certain PCH channel receives a paging attack, the other PCH channels with their subsets do not get affected and they still function properly. This solution increases the probability of resistance against the paging attacks. However, to practically implement this solution without causing negative impacts on the addresses of the same PCH subset, addresses should be divided in a way that does not overburden the associated PCH channel. This can be done by equally dividing the addresses and the PCH channels. However, if equal division is not applicable, then the bigger subsets acquire higher priority.

2.3. Integrity

Integrity concerns the delivery of data as it was originally sent with the exact accuracy. Information integrity refers to freedom, trustworthiness and dependability of information (Geisler, Prabhaker & Nayar 2003: 217, 221). In other words, integrity is the consistency and the assurance of data against any sort of modification or alternation (Lei & Ting 2009: 238 –241), either by the communication operation, or by malicious intrusions. This definition comprises data integrity and system integrity, since both constitute the information integrity.

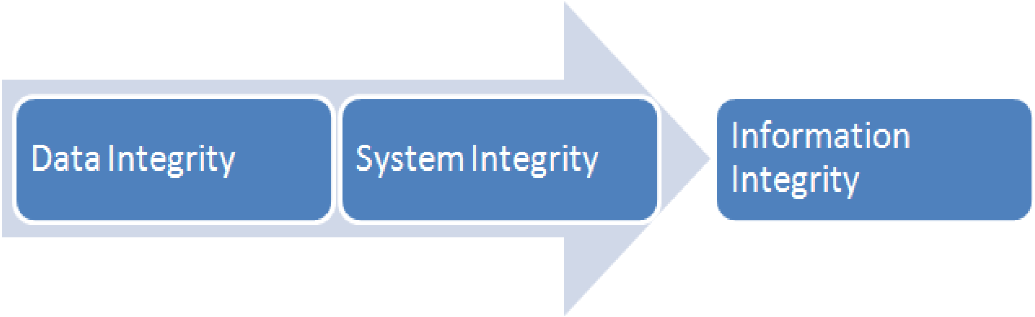


Figure 4: Composition of information security.

In the telecommunications field, integrity protection mechanisms are performed by the serving networks. Operators apply different mechanisms to detect the alternation caused to the exchanged data, regardless of its content. These deployed mechanisms utilize the authentication procedure, since authentication is required for the signaling to perform integrity. The employed mechanisms vary from as simple as using checksums to perform data check, to utilizing sophisticated cryptographic algorithms. Typically the cryptographic algorithms are preferred due to the robustness they provide. These algorithms include symmetric cryptography, e.g. Message Authentication Code (MAC), also using asymmetric cryptography techniques, e.g. digital signature and public key cryptography (Mao 2003: 356 – 385). Figure 5 illustrates the integrity procedure between the source and the receiver. In this figure, the system utilizes the transformation function f with the encoding key K_e at the source side, while it utilizes the transformation function g with the verification code K_v at the receiver's side. When both transformations match, it gives an indication that integrity is preserved. In this procedure, keys $K_{e,}$ K_v with transformations f and g specify whether the mechanism utilizes symmetric or asymmetric cryptography scheme.

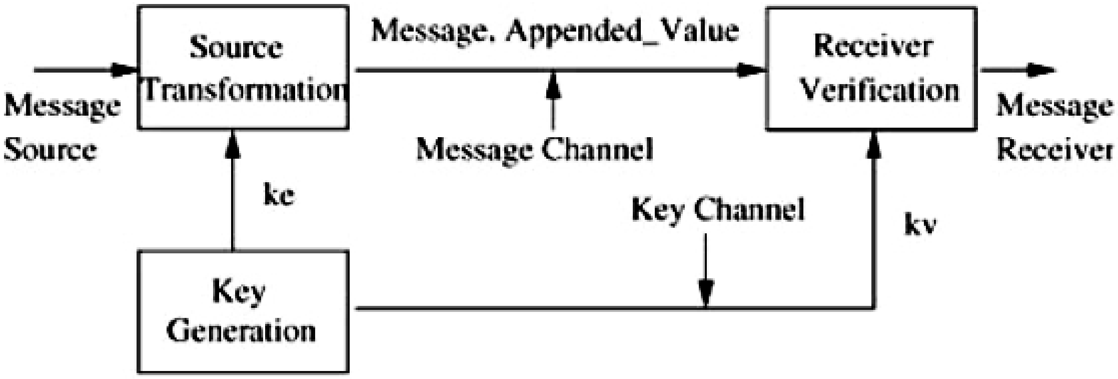


Figure 5: Data integrity systems (Mao 2003: 357).

In practice, one of the main criticisms of the GSM network is that authentication is unidirectional from the network's side, which in turn prevents the MSs from authenticating the network (Walker & Wright 2002: 385 – 406). Additionally, integrity protection is not provided for control messages (Chanadra 2005). Though, GSM provides integrity protection by the use of ciphering, which is applied according to the following algorithms:

1. A5/0: No encryption.
2. A5/2: For export, it is the weaker version and it is used mostly in Asia.
3. A5/1: The original ciphering algorithm, it is the stronger version and it is used in Europe and the US.

These algorithms are known with many weaknesses (Barkan, Biham & Keller 2003: 600 – 616). Several trials have been made and succeeded in breaking the stronger version A5/1 (Biryukov, Shamir & Wagner 2001); it can take from several hours to few seconds to cryptanalysis the algorithm according to the used techniques. Similarly is the case for the weaker version A5/2 (Goldberg, Wagner & Green 1999: 239 – 255), which was reverse engineered within only one second. Moreover, because of the security lack of the GSM architecture, an attacker can perform a Man in the Middle (MitM) attack and enforce the MS to use the weaker algorithm A5/2. This can be done by performing impersonation attack, to impersonate a false base station for the user while personating a fake MS for the network, and thus controlling the ciphering algorithms used within the session. Additionally, because A5/2 and A5/1 utilize the same key, an attacker can perform a malicious eavesdropping attack by deciphering the exchanged messages and revealing their content.

Along with the UMTS, integrity and confidentiality procedures are performed by the use of f9 and f8 ciphering algorithms respectively. Unlike GSM, UMTS integrity measures protects from false base station attacks; this is achieved by providing "in call authentication independent of ciphering" (Pütz, Schmitz & Martin 2001). The utilized algorithms f8 and f9 belong to the Kasumi algorithms family, also the newer GSM algorithm A5/3, and EDGE with GEA3 for the GPRS (Quirke 2004: 1 – 26). Kasumi (3GPP 2001b) is an open ciphering algorithm defined by the 3rd Generation Partnership Project (3GPP), it uses 128 bit keys and 64 bit block cipher, that is where it gets its robustness. However, several trials targeted breaking Kasumi algorithm, and they could succeed in breaking it theoretically to some extent. (Biham, Dunkelman & Keller 2005: 443 – 461) (Dunkelman, Keller & Shamir 2010: 393 – 410).

Figure 6 illustrates the procedure of integrity check in UMTS. In this figure, the Integrity Key (IK) is used as an input, in conjunction with the integrity sequence number COUNT-I, random number FRESH, and the integrity direction (uplink or downlink) DIRECTION. These values are utilized by the f9 function to calculate the Integrity code MAC-I for both systems of the sender and the receiver. These codes are compared to indicate whether integrity is achieved or compromised. It is worth mentioning that with this structure, replay and reflection attacks are prevented.

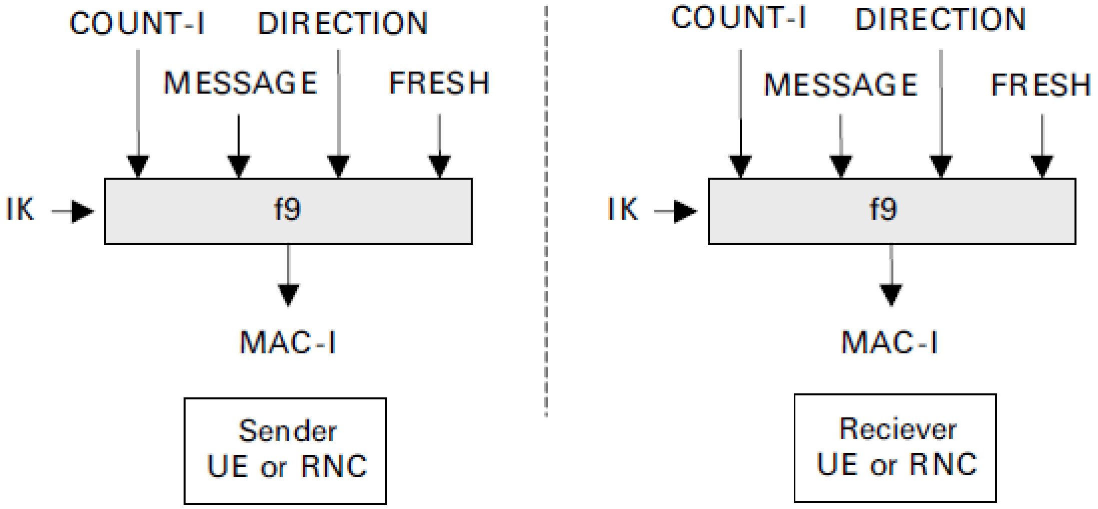


Figure 6: Integrity mechanism in UMTS (Niemi & Nyberg 2003: 140).

Many solutions are afforded to solve the issues regarding integrity (Lei & Ting 2009: 238 – 241); the typical ones include separation between the different domains, i.e., the network access, the network security, the user domain security and the application security. Also they include mutual authentication with the network, using temporary identities, enhancing routing and end to end security solutions.

2.4. Possession

Data possession or control protection is a new concept that was firstly introduced in the Parkerian security model. This concept concerns protecting and controlling information in the physical assets, i.e. communication devices (Ateniese, Pietro, Mancini & Tsudik 2008). Communication devices typically store contacts, logs information, and also can be used to store other valuable information, e.g. notes, pictures, emails and calendars. An example of the possession issue is that confidentiality is compromised when communication devices are lost, which directly affects users' privacy. The concept of possession is completely independent of the network and its security standards, since it concerns the mobile devices themselves. Upon that, possession is rather dependent on the platform, and its embedded security features; however, it can be enhanced by using adds-on services by the service provider.

A default solution to protect data at end devices is by using passwords to restrict the access to these devices; however, passwords can be broken or reset by several methods. Still, using passwords is the first step to protect the user's device. A more feasible solution is by encrypting the devices' data storage. Even though encryption provides robustness, it could be broken by using dedicated programs for that task. Advanced solutions include using remote storage service to store the valuable information rather than locally in the device. Also, implementing a three way authentication mechanism between the user, device and the network to control the device and its stored data, which in case of authentication failure, it performs a predefined action concerning these data, i.e. data erase. A very important issue to consider here as well is that mobile devices became commonly susceptible to attacks, due to the smart phones' spread and the facilities they provide. Hence, installing anti-intrusion and malware protection programs is no longer an option to protect these devices.

2.5. Confidentiality

Confidentiality is the most important fundamental concept in the security model; its importance comes from the fact that confidentiality concerns the content and the access to the data, which is directly related to users' privacy. "Confidentiality is the property of information that is not made available or disclosed to unauthorized individuals, entities, or processes” (IEEE Std 802.10 1998). This means that data has to be restricted and protected against all sorts of intrusion. Accessing data by unauthorized entities can put a threat for its owners, since data might disclose their personal, businesses, or other sorts of critical information.

In GSM, the system implements different measures to protect users’ confidentiality against intrusion; since the core network was assumed to be trustworthy, these measures are applicable only to the radio interface part of the network, i.e. access network (Horn, Mueller & Vinck 1999: 495 – 500). Therefore, the radio link between the base station and the User Equipment (UE) is encrypted, while data is transferred in clear inside the network (Kulkarni, Bhide & Chaudhari 2013). Confidentiality measures in GSM include hiding users’ identities, and encrypting the exchanged data. The MS’ Subscriber Identity Module (SIM) plays the main role in the security procedure since it stores the parameters needed throughout the communication process. The SIM card stores the main communication identities, the Mobile Station International Subscriber Directory Number (MSISDN), the International Mobile Subscriber Identity (IMSI) and the Temporary Mobile Subscriber Identity (TMSI) (Scourias 1995). MSISDN is the MS’s phone number; this number is used to call a user, also it is used by operators to route a call to its destination. IMSI is a unique number used by operators to identify and authenticate a user’s SIM card; this number is stored at the network’s side, and it is used when a SIM needs to authenticate itself to the network. However, during the different authentication procedures, IMSI is rarely used and all sessions are created by the use of the TMSI; thus it protects the confidentiality of the IMSI (Rahnema 1993: 92 – 100) (Vedder 1998: 224 – 240).

The SIM card as well includes the needed keys and algorithms utilized by the different security procedures. The SIM stores the authentication/integrity 64 bit key K_i, the ciphering key K_c, in addition to the algorithms A8, A3 and A5. A8 algorithm is used for key generation, while A3 algorithm is used for authentication and integrity check. Both algorithms are used in combination with the ciphering algorithm A5 to maintain voice confidentiality protection (Joshi 2008: 208). Though the benefits encryption provides to protect confidentiality, encryption is not standardized in the GSM model (Boman, Horn, Howard & Niemi 2002: 191 – 204). This lack of restrictions gives the choice for operators to design their own mechanisms, and to optionally implement them. However, mostly all operators make use of the COMP128 algorithm for the GSM authentication /confidentiality encryption (Pesonen 1999).

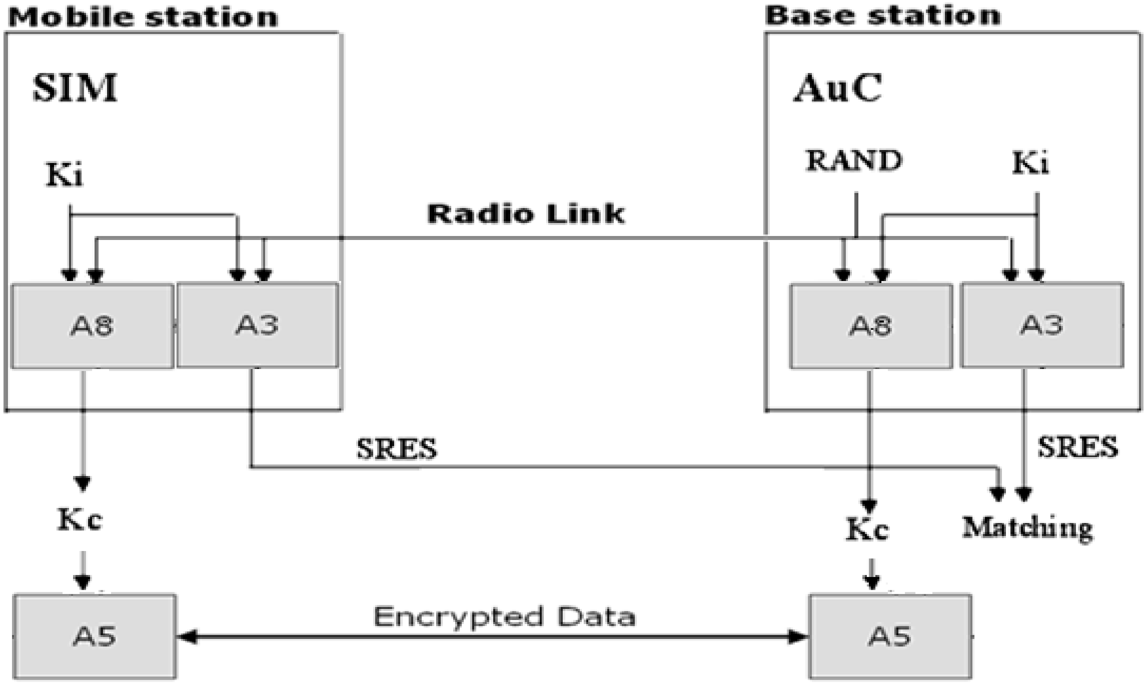


Figure 7: Encryption in GSM, modified from (Brookson 1994).

Figure 7 illustrates the encryption mechanism in GSM. In this figure, the authentication key K_i with the Random Number (RAND) are fed to the A3 algorithm at both ends, the SIM and the Authentication Center (AuC). Results of the generated Signed Response (SRES) are compared; when matched, they indicate that the session is authenticated. Similarly, the RAND is fed to the A8 algorithm to generate the session ciphering key K_c, this key is utilized by the ciphering algorithm A5/x to encrypt the exchanged data, thus maintaining confidentiality (Vedder 1998: 224 – 240).

Even though the GSM system is implementing several encryption mechanisms, it does not provide the required protection level due to several drawbacks. Firstly the key used is a 64 bit key, with the first 10 bits set to 0, which means that the active key length is only 54 bits (Boman *et al.* 2002: 191 – 204). Secondly, the first two versions of the COMP128 are known with weaknesses. In 1998 (Wagner, Goldberg & Briceno 1998), a group of Berkeley research cracked the COMP128. Additionally, the encryption algorithms A5/x are mostly cracked as mentioned before. In 2002 (Rao, Rohatgi, Scherzer & Tinguely 2002) IBM research could extract the COMP128 keys by the use of side channels attack. Thirdly, the encryption is only implemented over the radio link.

In the UMTS, these shortages facing the GSM security have been considered to improve the security situation (Niemi & Nyberg 2003). UMTS deploys ciphering algorithms to maintain data confidentiality; in contrast to GSM, ciphering is extended to the Radio Network Controller (RNC). Also, encryption is done over the Media Access Control (MAC) layer and the Radio Link Control (RLC) sublayer of the data layer, which extends the protection. In UMTS, the ciphering function f8 is utilized to maintain data and signaling confidentiality, which in contrast to GSM is included in the standard (3GPP 2001a). Also, the key length was increased to 128 bit. Moreover, the UMTS Universal SIM (USIM) keeps tracking of the amount of data by a certain ciphering/integrity key, so it can trigger the procedure to establish a new authentication session. Also, the Serving Network (SN) controls the lifetime of the ciphering/integrity key to guarantee its freshness (Pütz *et al.* 2001).

Figure 8 illustrates the UMTS ciphering mechanism and its implementation by the function f8. In this figure, f8 is fed by the Ciphering Key (CK), the cipher sequence number COUNT-C, the session/bearer ID BEARER, the direction of the stream DIRECTION, and the length of the stream LENGTH. The result of this process is the KEYSTREAM BLOCK which is used to encrypt the data by applying the bitwise XOR operation. This procedure is reversible, i.e. data can be extracted at the receiver's side by applying the same mechanism.

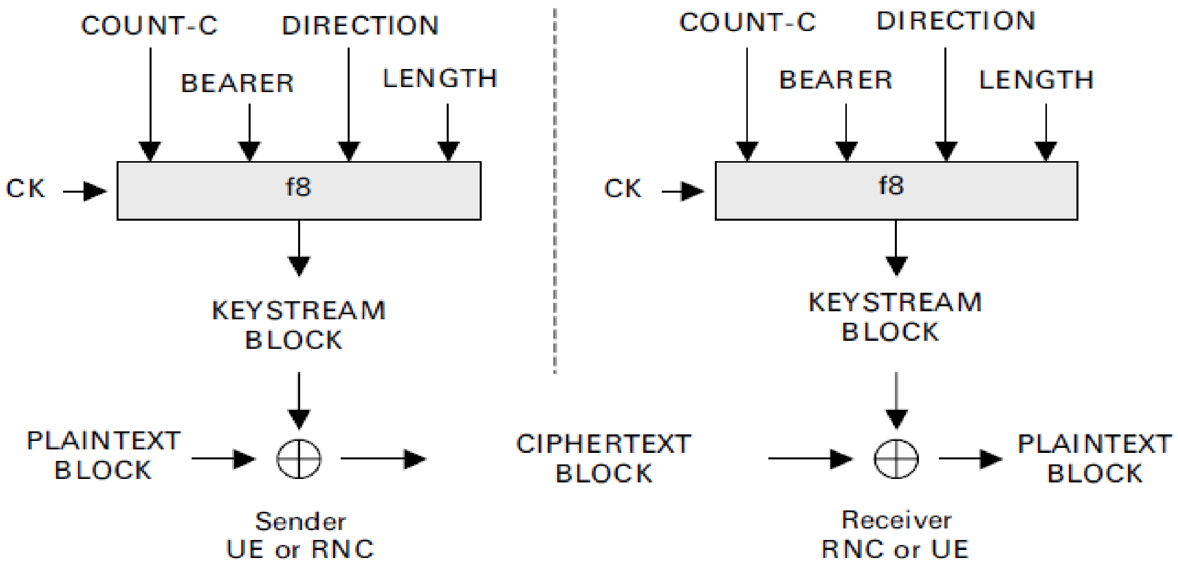


Figure 8: Ciphering mechanism in UMTS. (Niemi & Nyberg 2003: 137).

Even with these configurations and the robustness they provide, UMTS systems experience security drawbacks because of their compatibility with the GSM network part (Meyer & Wetzel 2004). When roaming to GSM network or when using a GSM device, due to the differences of the ciphering, integrity and authentication mechanisms, the system downgrades to the compatible version. This prevents the hybrid networks and devices from taking advantage of the higher security mechanisms; also it leaves a chance for malicious attacks to exploit the system.

2.6. Authentication

Authentication, Authorization, and Accounting (AAA) concepts provide means to identify users and to approve their permissible activities. Authentication mechanisms validate the user's identity. Authorization validates the privileges, services, permissions and resources assigned to the user, which is by default authenticated. Accounting keeps tracking of the user's activity, for further considerations including billing and security countermeasures (Stamp 2006: 153 – 154) (Convery 2007). In the telecommunication systems, the authentication procedure is performed along with the integrity and the ciphering procedures. That is because data integrity provides a means to ensure that the authentication procedure is consistent, i.e. integrity protected, while ciphering protects the exchanged authentication data (Tanenbaum & Van Steen 2007: 397). This was shown in Figure 7 previously, where authentication was performed between the SIM and the AuC.

As mentioned before, the authentication algorithm A3 is utilized by the non-standardized algorithm COMP128, which is known with many weaknesses. The Internet Security, Applications, Authentication and Cryptography (ISAAC) group along with the Smartcard Developer Association (SDA) succeeded in performing GSM cloning, where they could retrieve the K_i from the SIM and they proposed that the same attack can be done over the air interface. Also, they proposed that they could retrieve the K_i from the AuC itself (Wagner *et al.* 1998). This issue is very critical, since knowing the K_i breaks the GSM security, as K_i is the main input for the different cryptographic functions performing the different security procedures. Furthermore, the one-way authentication scheme is a main weakness for GSM, since it leaves a chance for impersonation attacks that impersonate false base stations.

The situation has been improved significantly in the UMTS phase; that is by implementing separate authentication functions, in addition to modifying the authentication mechanism. Firstly, the new standardized algorithm MILENAGE was implemented; with its constituent functions, MILENAGE provides the needed means for authentication between the USIM and the AuC. Figure 9 shows the structure of MILENAGE algorithm. In this figure, the left hand part of the algorithm performs the synchronization procedures while the right hand part handles authentication. Here, the different functions perform the following tasks: f0 is the RAND generator function, f1 is the network authentication function that provides the network authentication code MAC-A or the authenticated reply XMAC-A, f1* is the resynchronization message authentication function, and it generates the resynchronization authentication code MAC-S or the authenticated resynchronization reply XMAC-S , f2 generates the response RES or the authenticated response XRES, f3 generates the CK, f4 generates the IK, f5 generates the Anonymity Key (AK), and finally f5* is for the anonymity key derivation resynchronization messages. These functions utilize the secret key K, the RAND, the Authentication Management Field (AMF), and the Sequence Number (SQN) to perform their tasks.

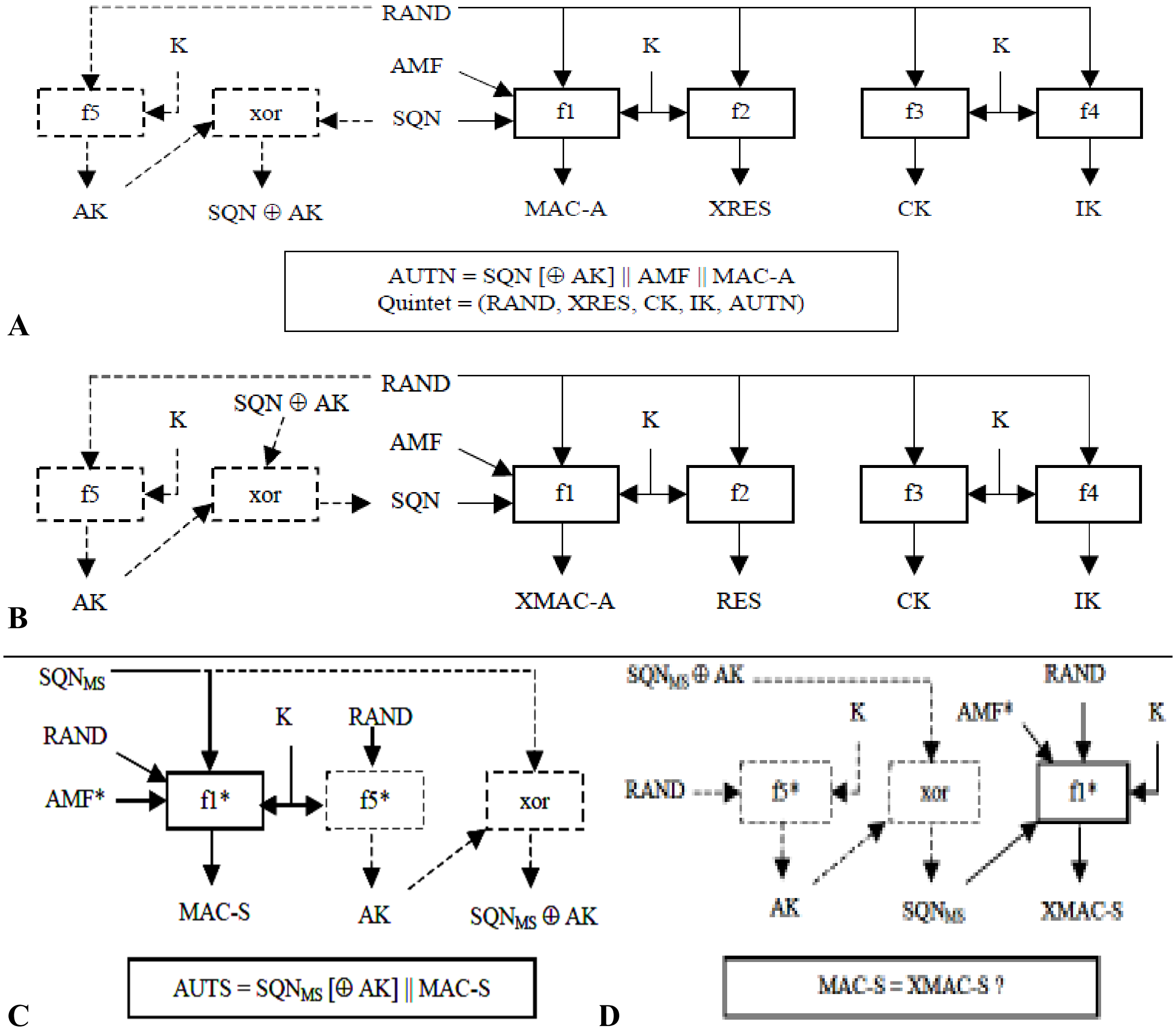


Figure 9: MILENAGE authentication algorithm, A) Authentication at the AuC, B) Authentication at the USIM, C) Synchronization at the USIM, and D) Synchronization at the HLR/AuC (3GPP 2010).

MILENAGE algorithm is implemented as a part of the Authentication and Key Agreement (AKA) procedure, which is illustrated in Figure 10. Here in the figure, the UMTS performs a mutual authentication mechanism between the SN and the USIM (Niemi & Nyberg 2003: 30).

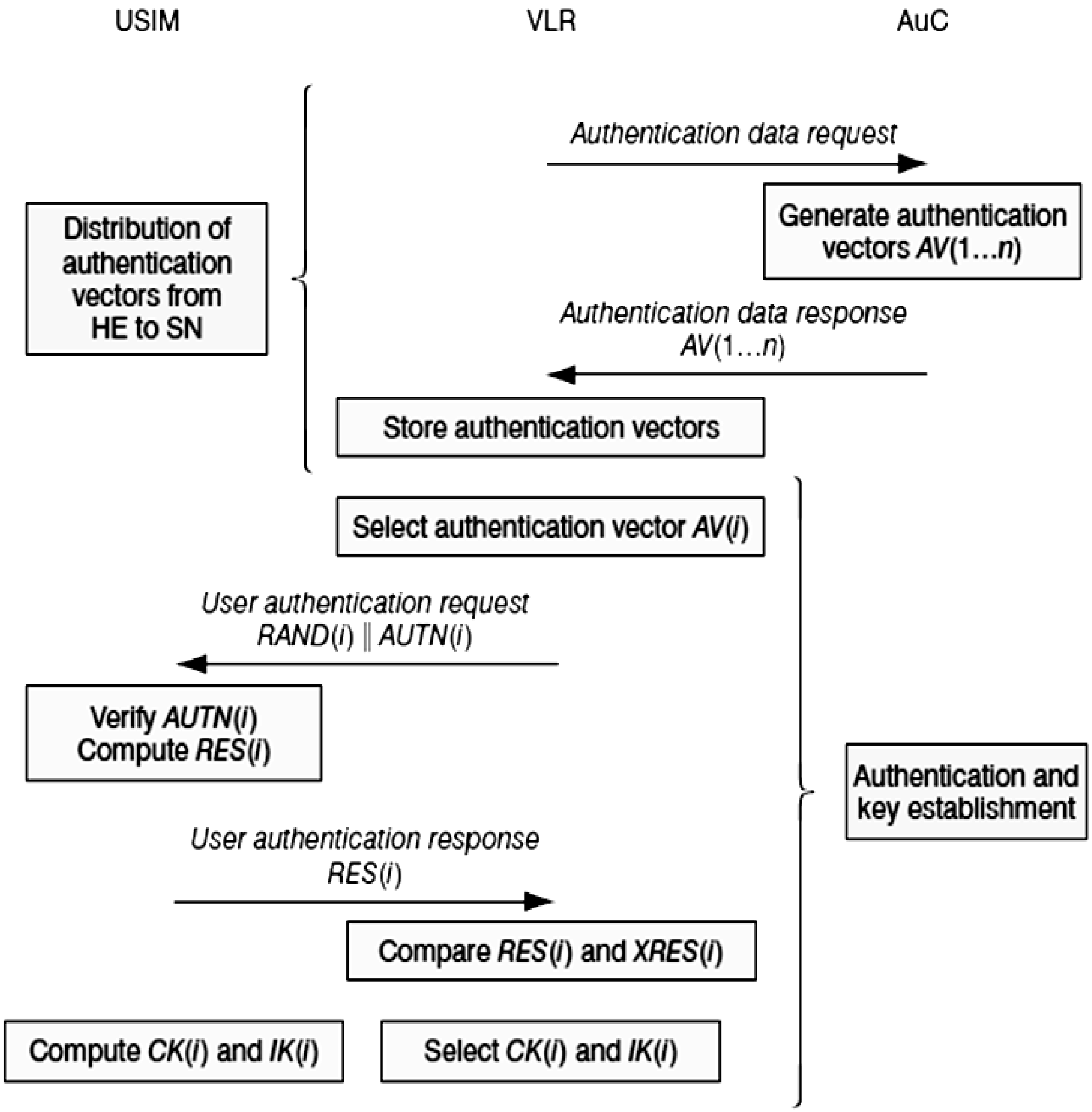

USIM
VLR
AuC
Authentication data request
Generate authentication vectors *AV*(1…*n*)
Distribution of authentication vectors from HE to SN
Authentication data response *AV*(1…*n*)
Store authentication vectors
Select authentication vector *AV*(*i*)
User authentication request *RAND*(*i*) ‖ *AUTN*(*i*)
Verify *AUTN*(*i*) Compute *RES*(*i*)
Authentication and key establishment
User authentication response *RES*(*i*)
Compare *RES*(*i*) and *XRES*(*i*)
Compute *CK*(*i*) and *IK*(*i*)
Select *CK*(*i*) and *IK*(*i*)

Figure 10: AKA procedure in UMTS (Boman *et al*. 2002).

Still, some minor weaknesses exist in the system after these modifications. They include the four unprotected messages of the AKA, which can be a target for intruders' attacks to either modify, or eavesdrop the exchanged messages (Mobarhan, Mobarhan & Shahbahrami 2012). Also, as mentioned before, compatibility with GSM is a major drawback to the UMTS system.

2.7. Non repudiation

The concept of non-repudiation has received high attention recently in the telecommunication environment, because of its importance to the different businesses since businesses are more dependent on the telecommunication facilities and the far communication services. Also because the effects the repudiation cause and their relation to the legal considerations. "Repudiation is the denial by one of the entities involved in a communication of having participated in all or part of the communication" (ISO 2009). Non repudiation is required to prevent an entity from denying a communication activity, since it concerns the transmitted messages from point to point, and the verification of their origin. A scenario (Stamp 2011: 77) can occur by an entity sending a message then denying it was sent by him under different circumstances, pretending to be vulnerable to some sort of attack. SMS messages for example are currently used and involved in different businesses, for example bank notifications, money transfers and work orders. Repudiation in such cases can cause serious problems to either the sender or the receiver.

In GSM non-repudiation was not considered in the design phase (Chikomo, Chong, Arnab & Hutchison 2006), which caused problems with bills in addition to masquerading and cloning users' IDs to send information in their names. The same issue arises with the UMTS as well (Hwang, Chong &Ou 2011: 99 – 112). The only implemented measures for non repudiation are through the logs information within the home network; however, in case of roaming non repudiation is not protected. The non repudiation issue belongs to the application layer's security, and it can be mitigated by the use of cryptography mechanisms, i.e. digital signatures. By adding the user's digital signature to the sent messages, it proves that messages are sent by the user who really signed them. In application, each module has to have its own digital signature, and third party authority is needed in the process to guarantee the repudiation free (Coffey & Saidha 1996: 6 – 17).

2.8. Analysis

Firstly, GSM was successful in its main task, providing connectivity; however, many security issues were not considered when it was first designed and the system was susceptible to different types of attacks. Secondly, in its design phase, UMTS security took these security shortages into consideration. Although many improvements have been made, avoiding all threats could not be achieved. Thirdly, the security architecture depends mainly on encryption mechanisms; however, other factors including the key management and key exchange procedures' enhancement should be considered, since it is the weakest part of the security association. Fourthly, the security level is independent of the end user and it lacks configurability. This means that a roaming user in an unsecured network is consequently not secured. End users need to configure and control the security level meeting their requirements. Fifthly, for both GSM and UMTS systems, encryption terminates at the outer part of the network, as the core network is considered trustworthy. However, for further protection, security has to be extended within the whole parts of the network. Sixthly; the GSM/UMTS compatibility is of many drawbacks, since the network downgrades to the compatible version, which in turn prevents it from applying the higher security measures. Finally, some parameters still need more consideration, e.g. possession and repudiation.

On the threat level, Mobarhan *et al.* evaluated the security attacks on UMTS according to its level, and according to the type of threat as shown in Table 1.

Table 1: Security attacks in UMTS.

Attack	Threat probability: Protection
Replay Attack	Low: Authentication
Man In The Middle	High: Authentication, Confidentiality, Integrity
Brute Force Attack	Medium: Authentication, Integrity
Eavesdropping Attack	Low: Confidentiality
Impersonation of The User Attack	Low: Authentication
Dictionary Attack	Low: Authentication
Impersonation of The Network Attack	Low: Authentication
Compromising AV In The Network Attack	Low: Authentication
Denial of Service (DoS) Attack	High: Authentication, Confidentiality, Integrity
Identity Catching Attack	High: Authentication, Confidentiality, Integrity
Redirection Attack	High: Authentication, Confidentiality, Integrity
Sequence Number Depletion Attack	Low: Authentication
Roaming Attack	High: Authentication, Confidentiality, Integrity
Bidding Down Attack	Medium: Confidentiality, Integrity
Guessing Attack	Medium: Authentication, Confidentiality
Substitution Attack	High: Authentication, Confidentiality, Integrity
Disclosure Of User Identity(IMSI) Attack	Low: Authentication
Packets Injection Attack	Low: Integrity
Content Modification Attack	Low: Integrity

It is clear from this table that the security measures of the UMTS need revision.

3. CORE NETWORK SECURITY

3.1. Background

In the first phase of mobile networks, networks could only afford limited services as voice, short messages and later limited data. With the 3G introduction, new services including multimedia and high speed packet data services were implemented to the network. This required installing new components to the network, in addition to upgrading the different parts of the network so that it can deal with the new functions (Wisely, Eardley & Burness 2002: 10 – 17).

Generally, mobile networks consist of two main parts, access network and Core Network (CN). The access network part is the outer part of the network; this part is responsible for users' access to the network since it holds the radio interface and performs the direct communication between the user and network. This part is represented by the Base Transceiver Station (BTS) and the BSC in GSM, or the Universal Terrestrial Radio Access Network (UTRAN) and Node B with RNC in UMTS. On the other side, the core network is the central part of the network. In this part, all the needed functions regarding services, management, switching, routing, authentication, and quality control measures are held. To perform these tasks, the CN is connected to all the needed registries and databases concerning users (Niemi & Nyberg 2003: 14 – 19). Figure 11 shows the basic components and concepts of the UMTS network architecture.

In GSM, the CN performs its tasks using the Circuit Switched (CS) domain. In UMTS, for the added services and facilities, more domains were included. UMTS' CN consists of three domains, CS domain, Packet Switched domain (PS), and Internet Multimedia Subsystem domain (IMS) (3GPP 2006). The CS part is responsible for handling the switching and signaling of the voice and the critical real time services between the UTRAN and the other network components. The PS part is responsible for data switching and signaling between Packet Data Networks (PDAs). Finally, the IMS provides the added multimedia services. These different domains use different signaling schemes for communication between the different network components.

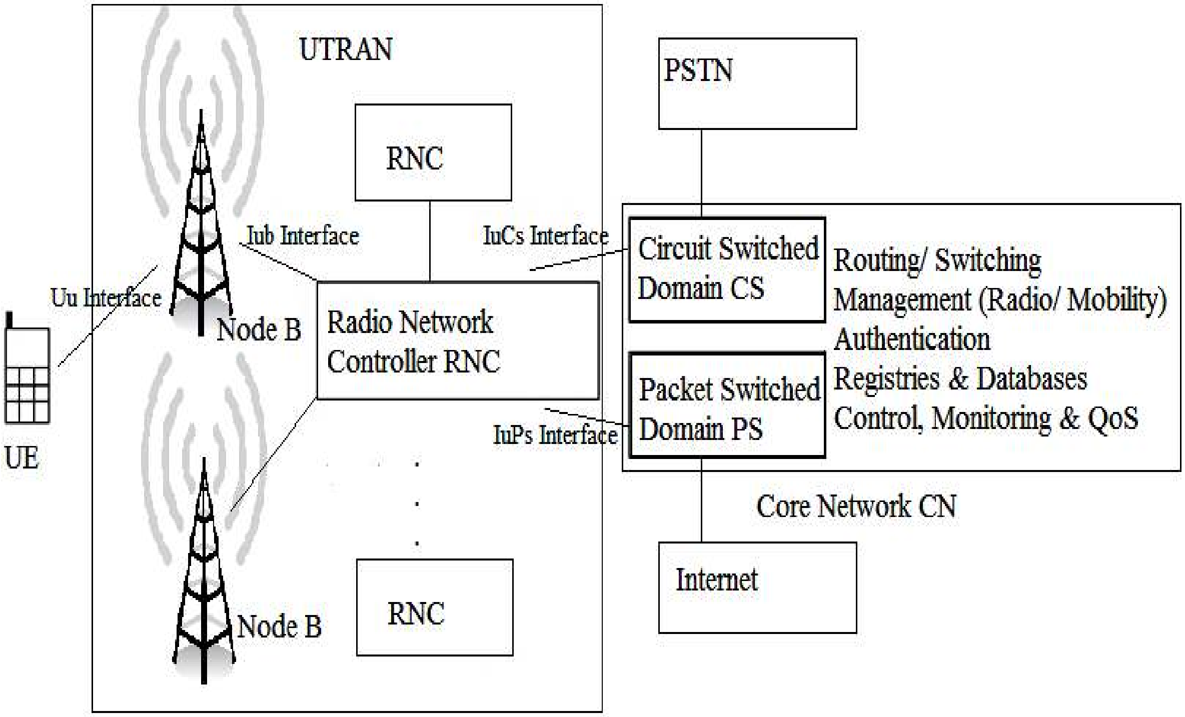


Figure 11: UMTS architecture simplified, modified from (Zheng *et al.* 2009: 31).

Signaling and communication between the different nodes of UMTS networks use two main schemes, the IP protocol and the older Signaling System No. 7 (SS7) (Niemi & Nyberg 2003: 19). Though the network release 5 standard (3GPP 2002a) published in 2002 planned for a pure IP connection between the different nodes (Walke, Seidenberg & Althoff 2003: 82), SS7 will keep in use for some years. A report (GSMA Intelligence 2012) showed that by 2017 half of global subscribers will keep on 2G while the other half will be using either 3G or 4G services. Figure 12 shows the growth of the global connections by technology between the years 2000 and 2017.

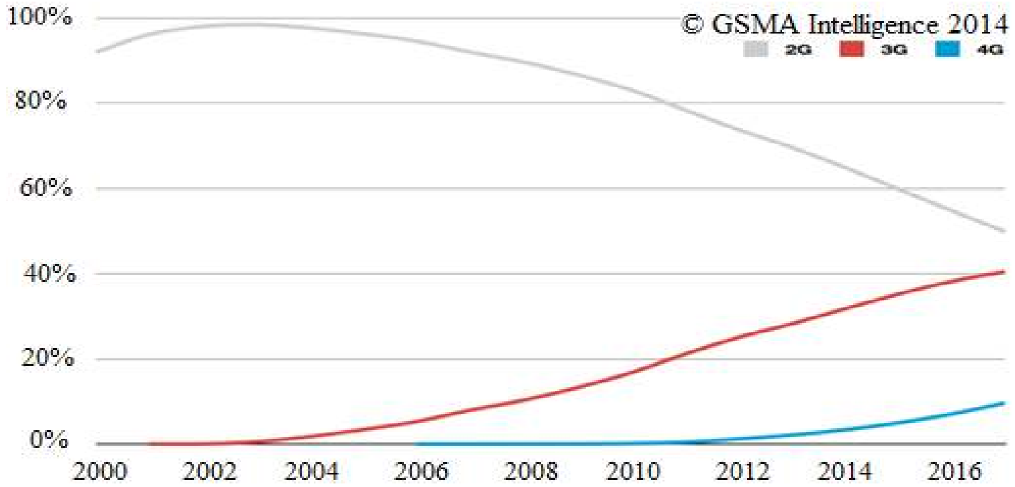


Figure 12: Global connections by technology (GSMA Intelligence 2012).

Out of this report, the IP will be the main signaling scheme wherever applicable within the network, while the SS7 will be kept in use for the older nodes. In this case, a Signaling Gateway (SGW) function is employed to perform the translation between the different protocols as shown in Figure 13. In this figure, the signaling between the IP network to the SGW is carried by the Stream Control Transmission Protocol (SCTP) over the IP protocol, while in the other side, the SS7 network sends its messages via the Message Transfer Part (MTP) which is a part of the SS7 signaling.

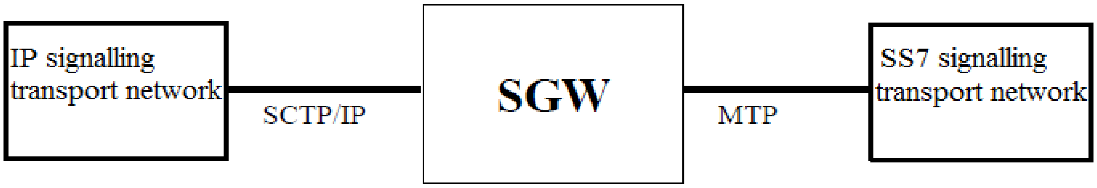

IP signalling transport network
SCTP/IP
SGW
MTP
SS7 signalling transport network

Figure 13: Signaling Gateway function configuration (3GPP 2006: 39).

In brief, SS7 (Modarressi & Skoog 1990) is a signaling standard and the predominant signaling scheme for GSM; it is analogous to the first three layers of the Open Systems Interconnection (OSI) model (Heine & Horrer 1999: 125 – 127). It specifies the signaling and protocols needed to connect the direct Switching Points/nodes (SP) or the indirect ones through using Signaling Transfer Points (STP). SS7 is an outbound scheme, thus it provides a distinction between the signaling plane and the users' plane as shown in Figure 14. The SPs and STPs negotiate for a set up to establish a communication link between end users.

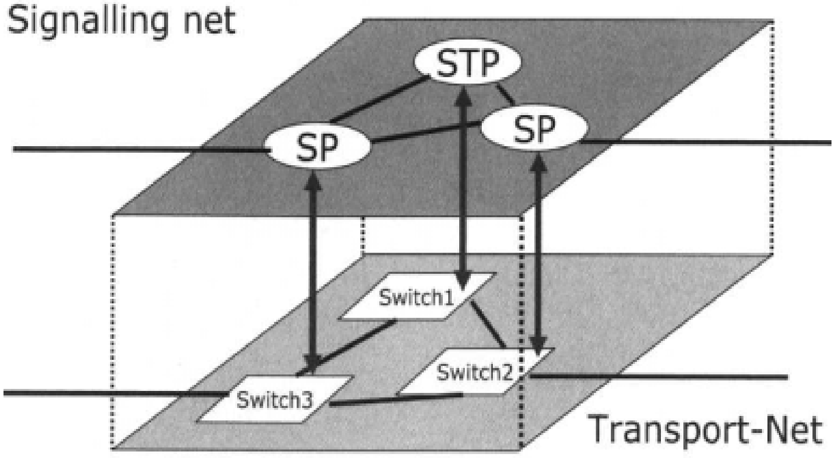


Figure 14: SS7 planes, Signaling and Transport Nets (Walke *et al.* 2003: 76).

For the different nodes to establish a communication session they need to access certain databases; this is done by the use of the Mobile Application Part (MAP) protocol (Bosse 1998: 478 – 529). MAP is the associated part of the SS7 in GSM networks, also it is known as GSM-MAP. MAP runs over the SS7 and has access to the different registries and nodes. As a result, MAP provides an application layer capability to the different nodes enabling them to perform their tasks.

3.2. Security Domains

Concerning UMTS security, in its 1999 release, the 3GPP group divided the UMTS security features into five domains (3GPP 2001b):

1. Network access security: users' secured accessibility to the UMTS services. Chapter 2 discussed this domain. In brief, access security is performed by the use of the

different measures of authentication, authorization, integrity, availability and confidentiality.

2. Network domain security: secure connection between the different network nodes. This chapter will focus on this domain.
3. User domain security: secure access to the mobile station. It is performed by implementing two mechanisms, firstly the USIM – user authentication by providing a key, namely the Personal Identification Number (PIN). Secondly the USIM – terminal authentication by providing a shared secret key.
4. Application domain security: secure data exchange between applications within the provider and the user. It secures the exchanged messages between the service provider and the USIM toolkit application within the user terminal.
5. Visibility and configurability: The end user will be informed about the security level, whether calls are encrypted or not, and whether it is 2G or 3G connection. Also it allows configuring the protection level, e.g. accepting or rejecting non ciphered calls, enabling/disabling USIM authentication, and choosing the ciphering algorithms.

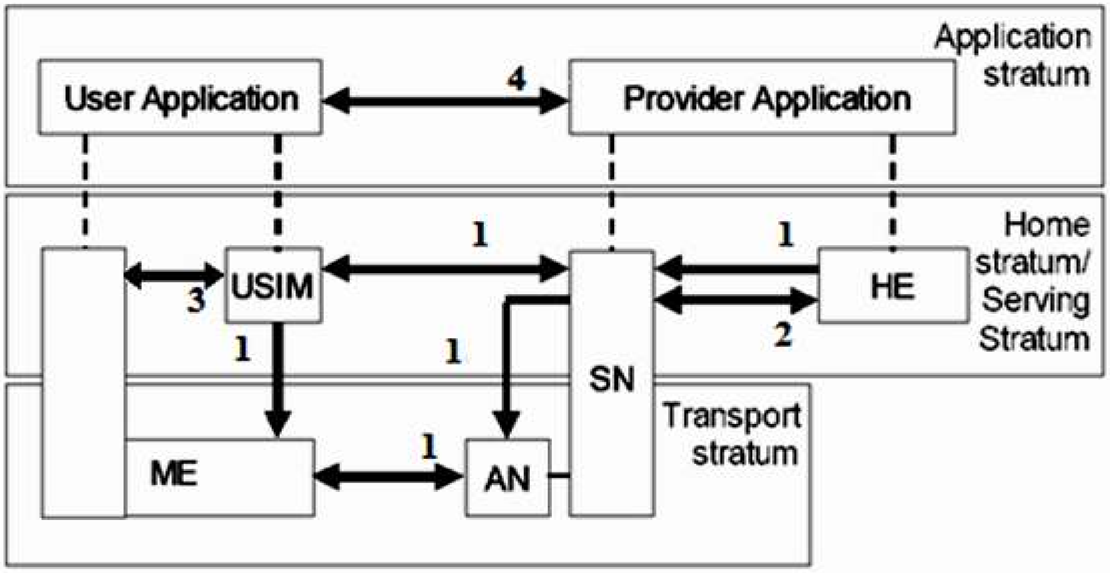


Figure 15: Security architecture in UMTS (3GPP 2001b).

Figure 15 shows the different security domains and its deployment with the different components. In this figure, numbers refer to the applied security domain and arrows refer to its direction. These domains are applied with the USIM, the UE, the access network, the SN, the Home Environment (HE) and finally to the different applications between users and the providing network.

3.3. Network Domain Security

Network domain concerns the communication between the different nodes within the core network. The communication is done using various protocols between the different nodes as mentioned before. The IP protocol is used for the new services of the UMTS with both Transport Control Protocol (TCP) and User Datagram Protocol (UDP), preferences are to the UDP due to the wireless communication nature. SS7 is also used to perform the communication with the outer nodes which have not been upgraded.

Regarding security, even though the IP protocol is promising for SS7 replacement due to its afforded facilities, all the security risks that face the IP protocol in the traditional networks as well as Internet will move to the new network. Thus, deploying IP needs high security considerations because of the higher risks. With SS7, it is also a similar situation, since SS7 has not any security features upon design. SS7 was assumed to be accessible only by very few institutions; as a result security was not considered in its design (3GPP 2002b). Also with the changes of the situation and the advanced techniques attackers hold, SS7 become weaker. For GSM, It is essential to protect the SS7 and its associated MAP part, since it performs the critical signaling between the different nodes. Thus, the 3GPP group developed a new protocol to include some security features to protect MAP signaling, introducing the MAP Security Layer (MAPSec).

In the next sections, MAPSec and the different IP security mechanisms are discussed.

3.4. Mobile Application Part Security Layer

The Mobile Application Part Security Layer MAPSec (3GPP 2002b) is a security protocol developed by the 3GPP to solve the security lack issue of the MAP protocol, to protect the exchanged messages between the network nodes. MAPSec adds a cryptographic layer to the MAP messages. The concept of MAPSec is by encrypting the plaintext MAP messages between Network Elements (NE) then enclosing it in another MAP messages before sending them. This is done by the use of encryption keys which is provided during the Security Association (SA). This mechanism was borrowed from the Internet Protocol Layer Security (IPSec) concept which will be discussed later in this chapter. For the different networks using MAPSec, a new element called the Key Administration Center (KAC) is needed. This element handles the automatic SA negotiation tasks which includes the keys, the lifetime and the needed security factors. Figure 16 shows the MAPSec operation between two arbitrary networks A and B; in this figure both KAC_A and KAC_B negotiate about the SA parameters by using of the Internet Key Exchange (IKE) protocol. After that, MAP messages get ciphered with the agreed keys according to the SA and the security level as will be mentioned later.

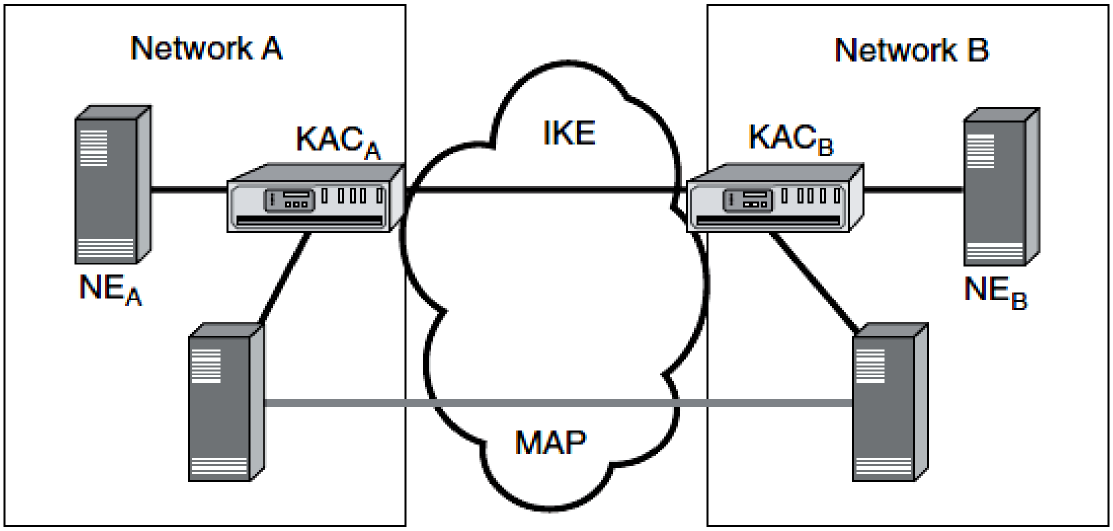


Figure 16: MAPSec operation (Niemi & Nyberg 2003: 75).

Unlike MAP which lacks the basic security, MAPSec uses separate functions for encryption and for integrity, respectively f6 and f7. f6 uses the Advanced Encryption Standard (AES) while f7 uses AES in Cipher Block Chaining Message Authentication Code (CBC-MAC) mode. Also, MAPSec uses interfaces with the NEs in the same network different than the ones of the NEs in other networks. That is because the KAC distributes the SA within the same network, enabling the network nodes to share the same rules and policies. For the other networks, KACs investigate the Security Policy Database (SPD) to check whether to apply the security mechanisms with the remote network or not.

MAPSec operates in three modes, 0, 1 and 2. In mode 0, no security is provided and the exchanged messages are identical to the original MAP ones. In mode 1, integrity and authenticity are provided while mode 2 additionally supports confidentially. Figure 17 shows the message format of MAPSec and protection procedures of modes 1 and 2. In this figure, Cleartext is the original MAP message, f6 and f7 functions are used with concatenation to provide the required protection procedure. It is worth mentioning that for all protection modes, the security header is sent in clear text. Also, MAPSec does not by default protect all exchanged messages, but it uses protection profiles that specify the protection level and the protection modes needed in operation.

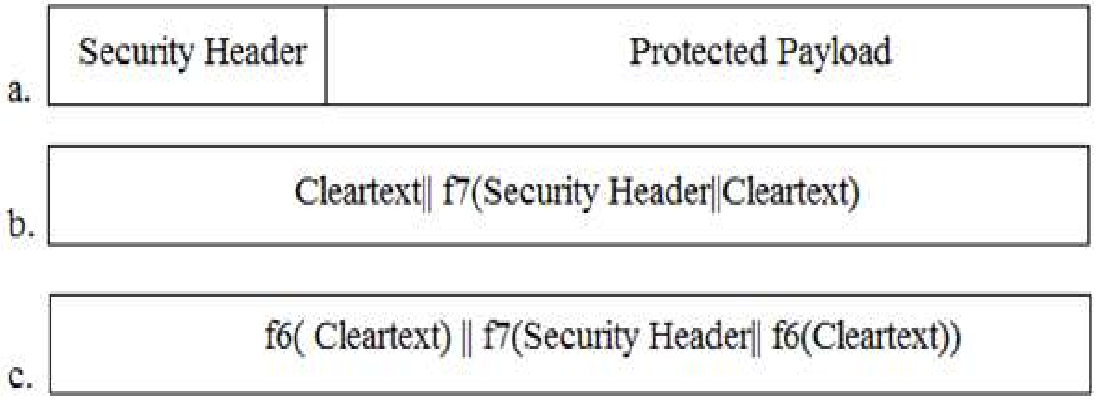

a.
Security Header
Protected Payload
b.
Cleartext|| f7(Security Header||Cleartext)
c.
f6(Cleartext) || f7(Security Header|| f6(Cleartext))

Figure 17: a. MAPSec format b. Protection mode 1 c. Protection mode 2 (3GPP 2002b: 11 – 12).

MAPSec faces three challenges, key management and standardization (Niemi & Nyberg 2003: 74 – 76, 80, 81). The former challenge is the need for a mechanism to renew the used keys during the SA. SAs can be configured manually, which gives the chance for operators to run their own mechanisms for key management. This will lead to longer lifetimes for the used keys. In releases 5, 6 (3GPP 2004) and 7 (3GPP 2007), the specifications of automatic key management was not included. A mechanism for automatic key management is needed to provide freshness for keys to enhance the protection mechanism. The other challenge is the standardization; as for these networks that do not support MAPSec, the other communicating networks should automatically downgrade to send only MAP messages. This case increases the probability of active attacks. Also the transition between MAP to MAPSec increases the probability of eavesdropping passive attacks which try to get knowledge of the authentication vectors.

3.5. Internet Protocol Layer Security

The Internet Protocol Layer Security IPSec is a network protocol developed by the Internet Engineering Task Force (IETF) specified in “RFC2401” (Kent & Atkinson 1998a), and adopted by the 3GPP (3GPP 2005) to provide protection for the IP communication. Since many protocols utilize the IP protocol, also because of the IP replacement to the SS7 in the legacy nodes of the core networks, high protection against outer attacks targeting IP systems is required, which is provided by IPSec.

IPSec specifications are given in the IETF’s Request for Comments (RFC) 2401 – 2412 series (Niemi & Nyberg 2003: 81). IPSec is a set of protocols that address the different security issues to provide the needed security layer for the IP communication. IPSec can be used also to protect MAP signaling to protect SS7 systems (Niemi & Nyberg 2003: 84 – 86) as shown in Figure 18, where the KAC is replaced by Security Gateway (SEG) performing the SAs operations.

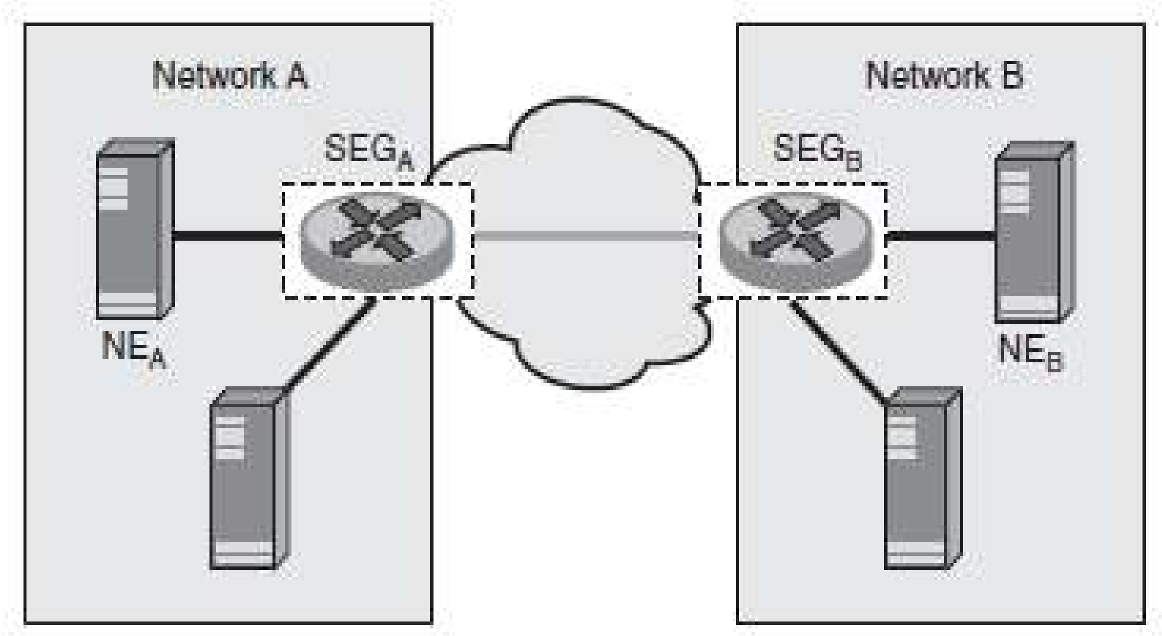


Figure 18: MAP over IPSec (Niemi & Nyberg 2003: 85).

IPSec lies in the third layer of the OSI model, where it can provide Virtual Private Networking (VPN) scheme between the communicating entities (Frankel, Kent, Lewkowski, Orebaugh, Ritchey & Sharma 2005), thus protecting them from outer attacks. Figure 19 in the next page shows the IPSec private network function; as shown, IPSec creates a cryptographic tunnel between the IP layers of the communicating systems. Also the figure shows that the IPSec can be implemented within a firewall or a router in conjunction with the host. This implementation within the network layer distributes the security mechanisms since it is application independent, and hence it guarantees the authentication, integrity and confidentiality for all deployed applications.

IPSec is a flexible protocol as it can adopt more protocols; also it supports different cryptographic schemes, hence it proves to be the base for secure communication. On the other hand, the protocol is not complete and it still needs more enhancements. It lacks mobility support; also its configuration is of high complexity compared to other protocols, which needs to be considered (Ferguson & Schneier 2000).

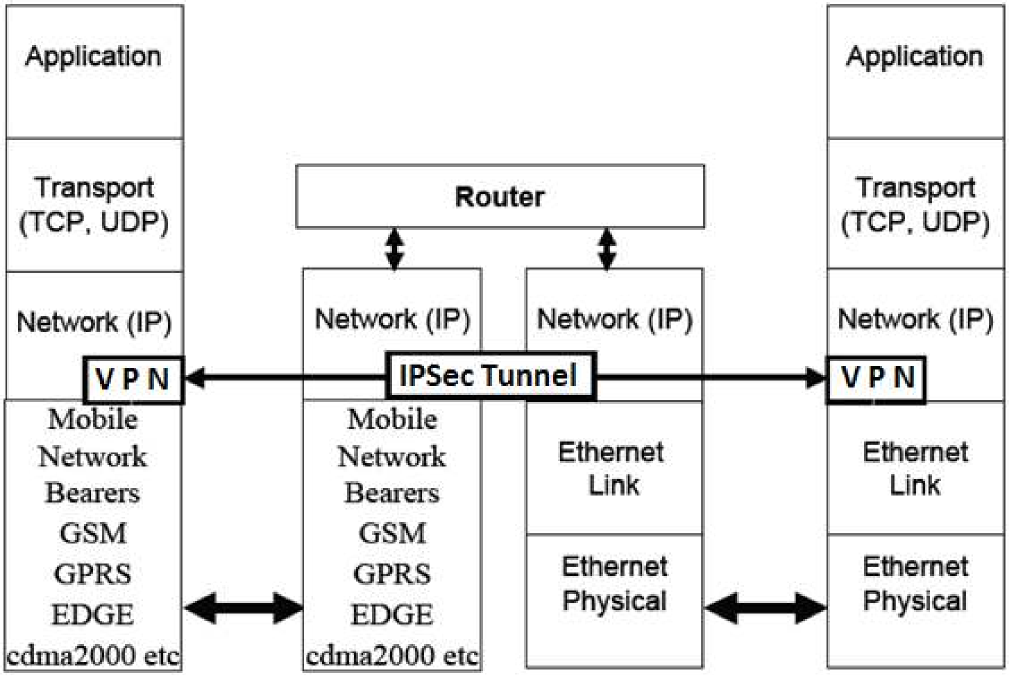
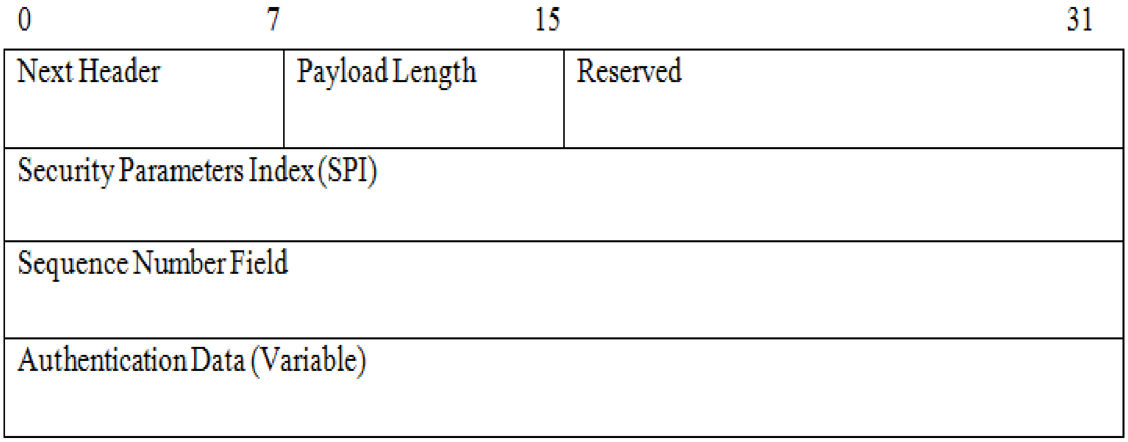


Figure 19: IPSec and VPN architecture in 3G (Ray 2006).

IPSec consists mainly of 3 protocols with their associated protocols, the Authentication Header (AH) protocol, the Encapsulating Security Payload (ESP) protocol and the IKE protocol. These protocols are discussed in the next sections.

3.5.1. Authentication Header Protocol

The Authentication Header Protocol AH “RFC2402” (Kent & Atkinson 1998b), “RFC4302” (Kent 2005a) is a protocol developed by the IETF; it is one of the deployed protocols within IPSec architecture to provide security services. AH provides protection for the IP headers, by means of providing data integrity and sender authentication services, also it optionally provides replay attacks protection. Figure 20 shows the stack of the AH protocol; in this figure the next header field indicates the next protocol dealing with the protected data, the payload length is the length of the AH datagram, and the reserved field is left optionally for future use. These three fields preserve the first 32 bits of the stack. The Security Parameters Index (SPI) is used for the SA options for the datagram. Sequence Number Field is a counter value for the sent messages. Finally, the Authentication Data field contains the Integrity Check Value (ICV) for the sent packets. As can be seen, there is no field for data here in this stack.



0 7 15 31

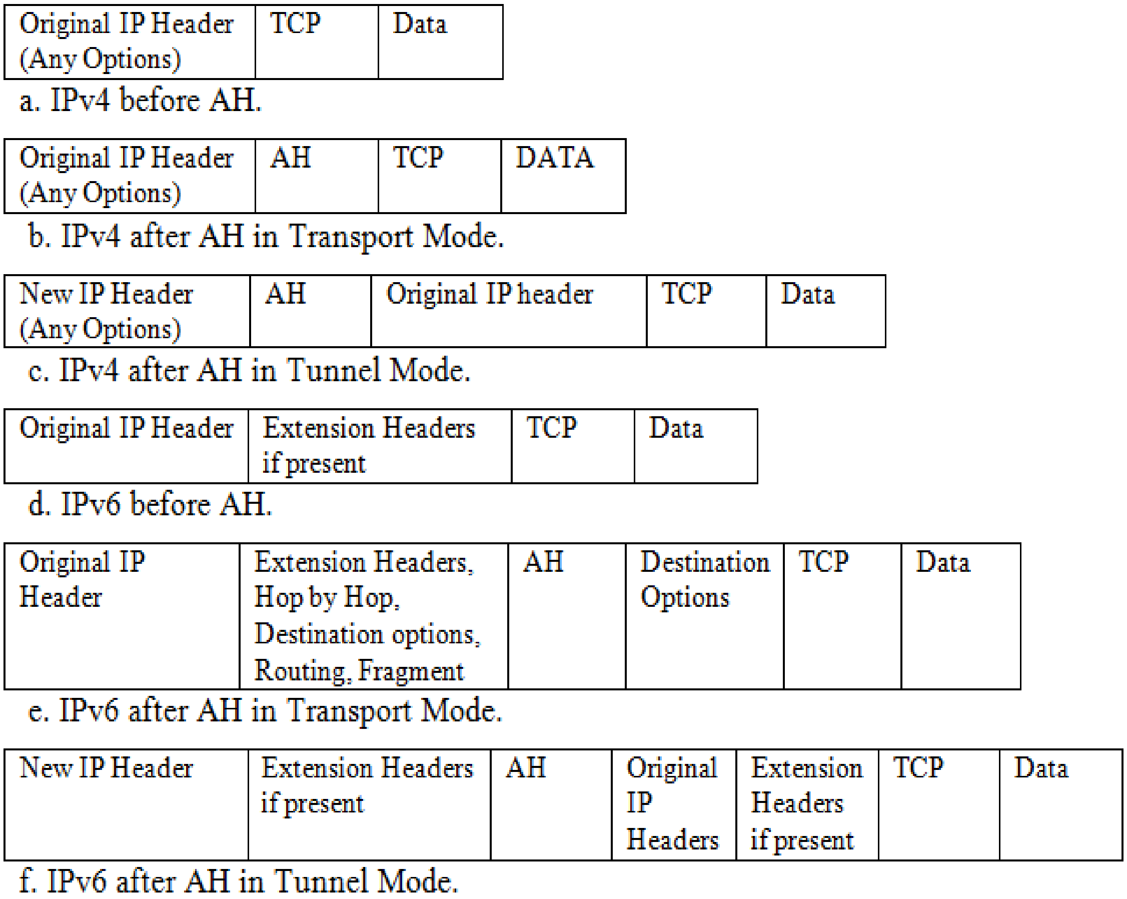
Next Header	Payload Length	Reserved
Security Parameters Index (SPI)		
Sequence Number Field		
Authentication Data (Variable)		

Figure 20: Authentication Header Protocol stack “RFC2401” (Kent & Atkinson 1998a: 2).

Concerning security; AH provides integrity by the use of checksums and sequence numbers, also guarantees authentication by providing keyed MAC for the exchanged messages. In the case of sending unicast between peers, it uses symmetric encryption functions like Data Encryption Standard (DES) algorithm, or one way hash functions like the Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1). For multicasting, it uses one way hash algorithm in addition to asymmetric signatures. Also, AH protects against replay attacks, this is done by resetting the sequence number field between the sender and receiver and checking to prevent numbers’ recycling. This option is allowed when the receiver enable it at the SA establishment.

AH operates in 2 modes, transport and tunnel. In its transport mode, it is deployed between hosts of a selected IP addresses. In that mode, the AH protocol is located directly after the IP header. In its tunnel mode, it is deployed between hosts, also between security gateways.

The tunnel mode requires creation of inner and outer IP addresses. The inner addresses are the ultimate addresses for the source and destination, while the outer ones are used for tunneling and protection, since they carry the addresses of the security gateways. Also, in this mode, AH is located after the IP header relative to the outer IP addresses. Figure 21 shows the IP datagram before and after applying AH protocol in its both modes for both IPv4 and IPv6.



Original IP Header (Any Options)	TCP	Data

a. IPv4 before AH.

Original IP Header (Any Options)	AH	TCP	DATA

b. IPv4 after AH in Transport Mode.

New IP Header (Any Options)	AH	Original IP header	TCP	Data

c. IPv4 after AH in Tunnel Mode.

Original IP Header	Extension Headers if present	TCP	Data

d. IPv6 before AH.

Original IP Header	Extension Headers, Hop by Hop, Destination options, Routing, Fragment	AH	Destination Options	TCP	Data

e. IPv6 after AH in Transport Mode.

New IP Header	Extension Headers if present	AH	Original IP Headers	Extension Headers if present	TCP	Data

f. IPv6 after AH in Tunnel Mode.

Figure 21: The IP datagram before and after applying AH protocol "RFC2401" (Kent & Atkinson 1998a: 5 – 6).

Despite the fact that AH supports integrity and authenticity, it does not afford confidentiality services for the transmitted data. AH does not provide encryption for data, and hence it is not a complete option to protect the transmitted data (Frankel *et al.* 2000: 28 – 31). ESP protocol as will be discussed later can handle this issue.

3.5.2. Encapsulating Security Payload Protocol

The Encapsulating Security Payload Protocol ESP “RFC2406” (Kent & Atkinson 1998c), “RFC4303” (Kent 2005b) (Frankel *et al.* 2000: 31 – 36) is a security protocol used within IPSec to provide confidentiality, integrity, anti replay protection and origin authentication. These services are similar to the ones of the AH protocol; however, ESP uses ciphering to protect the exchanged traffic; on the contrary, ESP does not protect the IP header as AH does. The number of the implemented services is agreed upon during the SA session. ESP is deployed between hosts, security gateways, or between a host and a security gateway. Figure 22 shows the format stack of ESP. As can be seen, there are similar fields with AH, these fields perform the same services. The differences are about the Payload Data field which holds the encrypted data, and the Padding field which is used for encryption purposes depending on the used encryption algorithm.

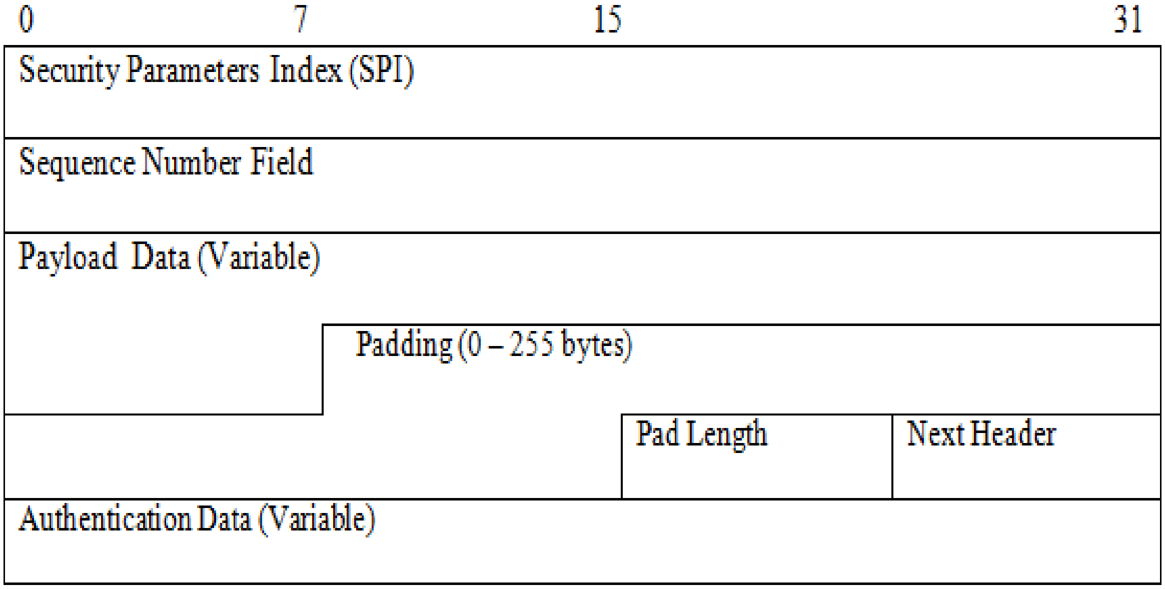


Figure 22: ESP stack format “RFC2406” (Kent & Atkinson 1998c: 2).

ESP supports a variety of cryptographic protocols for both encryption and authentication. It supports NULL algorithm by default for encryption and authentication, as well as 3DES-

CBC with keys of 192 bits, BLOWFISH-CBC with 128 bits “RFC2451” (Pereira & Adams 1998), AES-CBC with keys from 128 up to 256 bit “RFC3602” (Frankel, Glenn & Kelly 2003), AES-CTR with 192 up to 320 bits minus 32 for nonce value “RFC3686” (Housley 2004), and DES-CBC with 64 bits “RFC2405” (Madson & Doraswamy 1998) for encryption. For authentication it supports HMAC-SHA1-96 “RFC2404” (Madson & Glenn 1998b), HMAC-MD5-96 “RFC2403” (Madson & Glenn 1998a) and finally HMAC-SHA-256/384/512 “RFC4868” (Kelly & Frankel 2007). Also other algorithms can be implemented as well.

Similarly, ESP operates in two modes, tunnel and transport, depending on the afforded services and the level of security. The transport mode is deployed between hosts and it protects the upper protocols, while in contrast, tunnel mode can be between hosts or security gateways. In the transport mode, the ESP header lies between the IP header and the upper layer protocol. It is clear that the IP header is not protected with this mode. In the tunnel mode, an outer IP is created between security gateways, and the ultimate original IP headers are protected. The outer IP header is of the same position as the transport mode. Figure 23 shows the IP stack before and after ESP. As seen, ESP has a trailer field unlike the case with AH

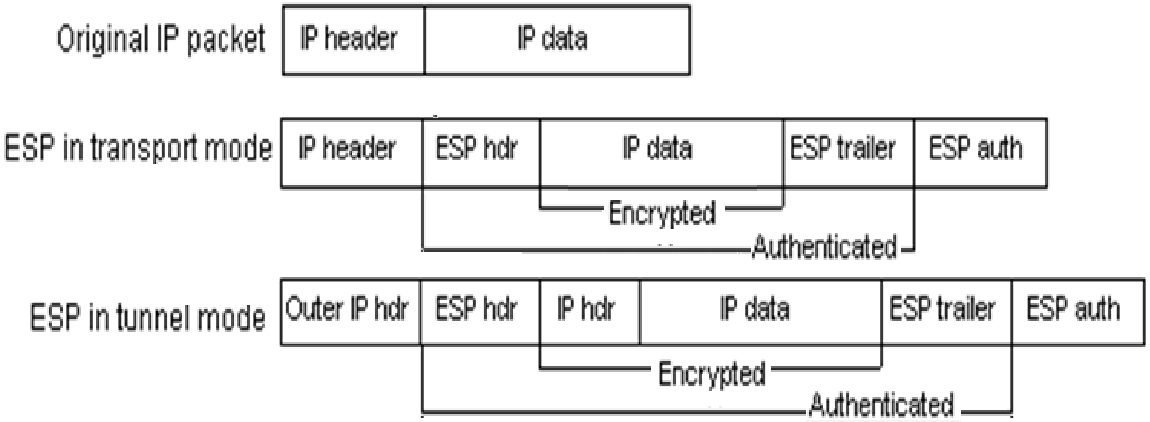


Figure 23: IP stack after ESP (Kent 2005).

3.5.3. AH-ESP

AH and ESP protocols can be employed together to provide more robustness security mechanism. Since both protocols are of overlapping security services, this configuration requires a precise definition of the SA; it needs to specify which services will be handled by each protocol. This agreement needs to meet the system requirements and the desired performance, to afford the needed level of protection without overlapping.

3.5.4. Transport Mode and Tunnel Mode

IPSec operates in one of two modes, transport and tunnel, since it is composed mainly of AH and ESP protocols which operate using these modes. These modes perform different functions to provide the needed security level between the different network parts, yet they differ significantly. Transport mode supports end to end security between the intra-network devices. In this case, these devices should support IPSec while intermediate ones do not need to. On the other hand, tunnel mode supports creation of VPN, and it is deployed between security gateways, though it does not afford end to end security.

3.5.5. Internet Key Exchange Protocol

The Internet Key Exchange protocol IKE “RFC2409” (Harkins & Carrel 1998) is a hybrid protocol for key management and SA negotiation. It is of high importance for IPSec, since AH and ESP protocols do not have a mechanism for key exchange, so it assists them performing their functions. IKE establishes a mutual authenticated secure communication and provides a mechanism for key exchange.

IKE combines features of Oakley Key Determination Protocol (Oakley) “RFC2412” (Orman 1998), Secure Key Exchange Mechanism Protocol (SKEME) (Krawczyk 1996) and the Internet Security Association and Key Management Protocol (ISAKMP) “RFC2408” (Maughan, Schertler, Schneider & Turner 1998). ISAKMP handles the SA negotiation including the encryption algorithms, hash algorithm, the authentication method and the exchange method which is a part of Diffie-Hellman (DH) key exchange algorithm. ISAKMP operates in one of two phases; the first phase establishes a secure channel and agrees about the SA, while in the second phase it negotiates about the SA parameters and services. These phases operate in three modes borrowed from Oakley protocol, explicitly, main mode, aggressive mode and quick mode. The main mode is responsible for identity protection. The aggressive mode is used for speeding up the process by reducing round trips; however it does not support identity protection by default, but only with further configurations. These two modes are employed within the first phase of the ISAKMP. In its second phase, the quick mode is utilized, which is used for fresh keying generation. SKEME protocol is also used with IKE to provide fast key exchange means based on public key, key distribution center or manual installation. This protocol provides fast key refreshment, also less complexity and realistic exchange scenarios, in addition to variety of services including anonymity and repudiability.

3.6. Transport Layer Security Protocol and Secure Socket Layer Protocol

The Transport Layer Security (TLS) protocol and its former version the Secure Socket Layer (SSL) protocol or what is collectively known as TLS/SSL is one of the major protocols for network security. TLS/SSL is used for tunneling and providing VPN between a user and a server. That is similar to IPSec function; however, TLS/SSL is network layer independent as it is applied within the upper layers, and hence it does not protect the whole exchanged traffic as IPSec. Furthermore, TLS/SSL is of high popularity because of its simplicity and the fact that it does not require complicated configurations and hard work compared to IPSec.

SSL protocol (Hickman & Elgamal 1995) (Stamp 2006: 235 – 239) was first introduced by Netscape to cover the security concerns of growing networks. It aimed protecting end users, providing an adequate level of communication privacy, preventing eavesdropping, tamper and message forgery. This is achieved by providing end to end security regardless of the intermediate networks' situation, also by performing mutual authentication between servers and clients to protect the exchanged traffic. SSL is a transport layer connection oriented protocol; therefore it provides security services for the upper layers' reliable applications. Figure 24 shows the position of the SSL protocol within the OSI stack. SSL operates by establishing socket to socket secure communication between the peer applications. This requires protocol negotiation to agree about the SA parameters, which is performed by the SSL constituent protocols, SSL Record protocol and SSL Handshake protocol. The SSL Record protocol is responsible for encryption and the unique keys for the different connections; also it concerns integrity and message checking, while the SSL Handshake protocol deals with the negotiation tasks, authentication and security parameters agreement.

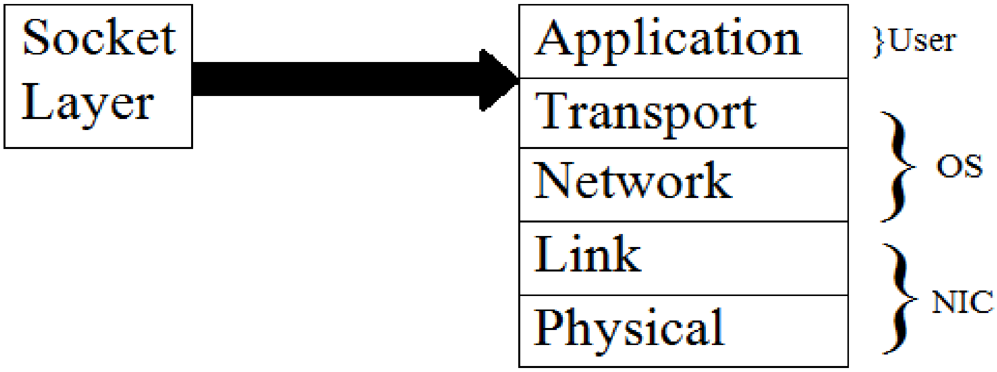


Figure 24: SSL position (Stamp 2006: 235).

TLS protocol "RFC 2246" (Allen & Dierks 1999) was introduced in 1999 by the IETF as the new standardization for SSL. TLS is a fourth layer security protocol, it runs over the

TCP/IP and it requires reliable data transmission and reception. TLS provides tunneling between applications, integrity and authentication. TLS is based on the same architecture of the SSL 3.0, with many similarities that it is rather considered SSL version 3.1. Though, these similarities with SSL exist, both protocols are not identical. Therefore, TLS has the facility to downgrade to SSL with a system not supporting TLS. Table 2 (Thomas 2000: 118) (Horms & Horman 2005: 3) shows the differences between both protocols.

Table 2: TLS and SSL differences

Property	SSL 3.0	TLS 1.0
Protocol version in messages	3.0	3.1
Alert protocol message types	12	23
"No certificate" Alert message	Not needed	Needed
Message Authentication Code MAC	Not supported	Supported
Authentication	MD5, SHA	HMAC
Key generation	Ad hoc: Non-standard	HMAC with Pseudorandom Function (PRF): Standard
Implementation and Baseline cipher suites	Supports Diffie- Hellman DH and RSA. Supports FORTEZZA crypto systems	Required to support Diffie Hellman- Digital Signature Standard (DSS) DH/DSS key exchange with 3DES. Does not include FORTEZZA
Certificate Verify	Complex	Simple
Finished messages	Ad hoc: Non-standard	PRF: Standard

TLS as well as SSL consists of two protocol layers, Record Layer and Handshake layer. As shown in Figure 25, the Handshake layer combines three protocols, Handshake protocol, Change Cipher Spec protocol and Alert protocol. Protocols within both layers are explained in the next sections.

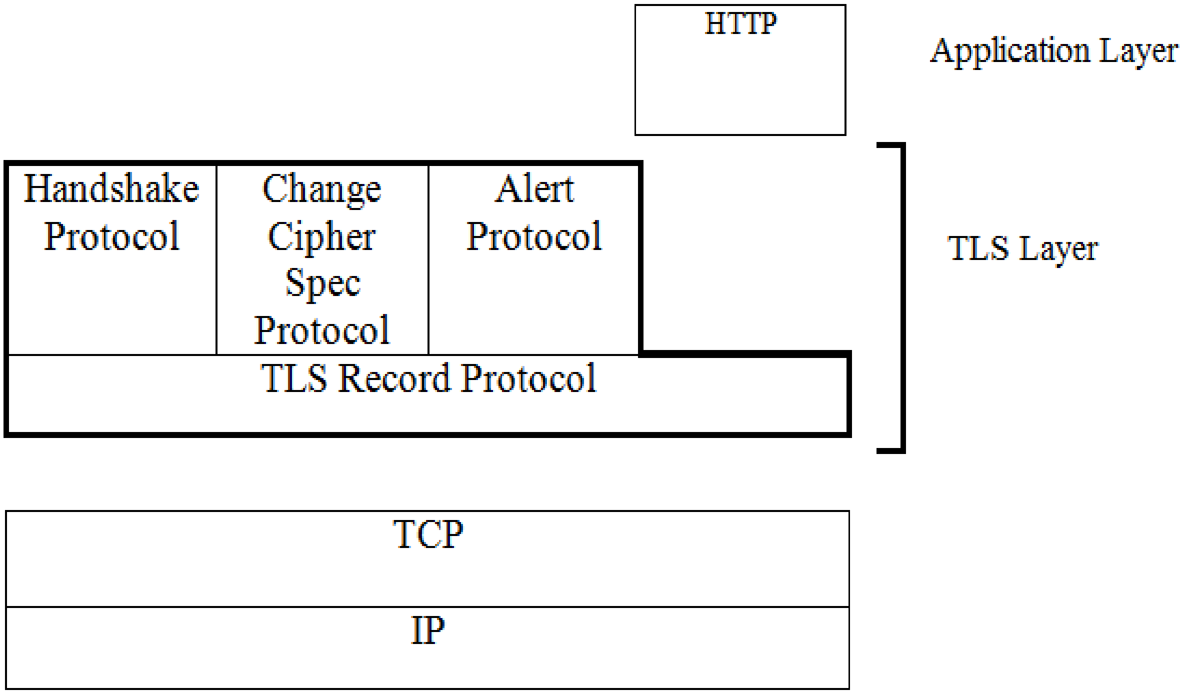


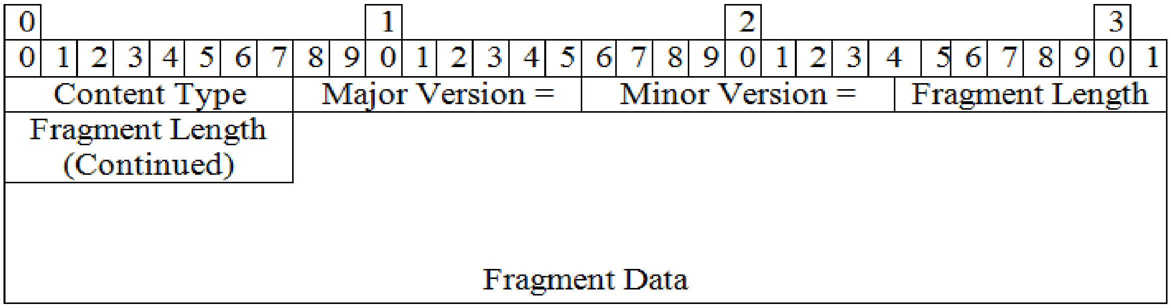
Figure 25: TLS protocol stack, modified from (Mahboob & Ikram 2004).

3.6.1. TLS Record Protocol

TLS Record protocol (Joshi 2008: 125 – 132) is a layered protocol performing the base functions for TLS. It is utilized by the higher protocols as shown in Figure 25, as it specifies the needed parameters for the operation of these protocols. TLS works in records, these records need declaration for the data format, data length, fragmentation, compression if applicable, MAC procedure, encryption and ciphering; these records are performed by the Record protocol.

TLS has four connection states, currently read/write and pending read/write. TLS Record performs its procedures within only the first two states. On the other hand, the pending states turn into currently states after being initialized with the needed security factors, otherwise it will not proceed. These states need to state the type of the entity (client or server), the PRF algorithm, the bulk encryption algorithm, MAC authentication algorithm, compression algorithm, master keys, and the random values for each entity. The Record layer uses this information to generate the needed security parameters, including the entity MAC key, encryption key and the Initialization Vector (IV). These parameters are used by the server and the client for communication. When connected, both entities have to declare the compression state, the cipher state, the MAC key and the sequence number.

The Record protocol stack as shown in Figure 26 consists of Content Type field, Major Version, Minor Version, Fragment Length, and Fragment Data. Content Type field specifies the higher layer protocol in action. A value of 22 is assigned to Handshake protocol, 21 for Alert protocol, 20 for Change Cipher Spec protocol, and during data transmission, the content type value changes to 23. Also, for these higher protocols, their control messages have different numbers specified by the deployed protocol. Major Version and Minor Version fields specify whether it is SSL or TLS, and which subversion it is. SSL has versions 1, 2 and 3, while TLS starts with 3.1 for TLS version 1. TLS Record protocol can carry data size up to 2^{14} bytes within its Fragment Data field; the size of the data is given in the Fragment Length field. Moreover, for data of larger sizes, fragmentation and compression are applicable.



0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Content Type								Major Version =								Minor Version =								Fragment Length							
Fragment Length (Continued)																															
Fragment Data																															

Figure 26: Record layer (Joshi 2008: 126).

3.6.2. Handshake Protocol

For TLS to perform its tasks; it needs to agree about the parameters and configurations used within the session, these agreements are made by the Handshake protocol. The Handshake protocol (Joshi 2008: 125 – 132) is responsible for the negotiation tasks needed by both communication entities. It handles the different security algorithms, the cryptographic parameters, keys, authentication, certificates, and closure notifications. Figure 27 illustrates the procedure of the Handshake protocol. As observed, the protocol utilizes the Change Cipher Spec protocol to finalize the session. When the Handshake protocol completes the negotiation process, the agreed parameters get carried by the Record protocol.

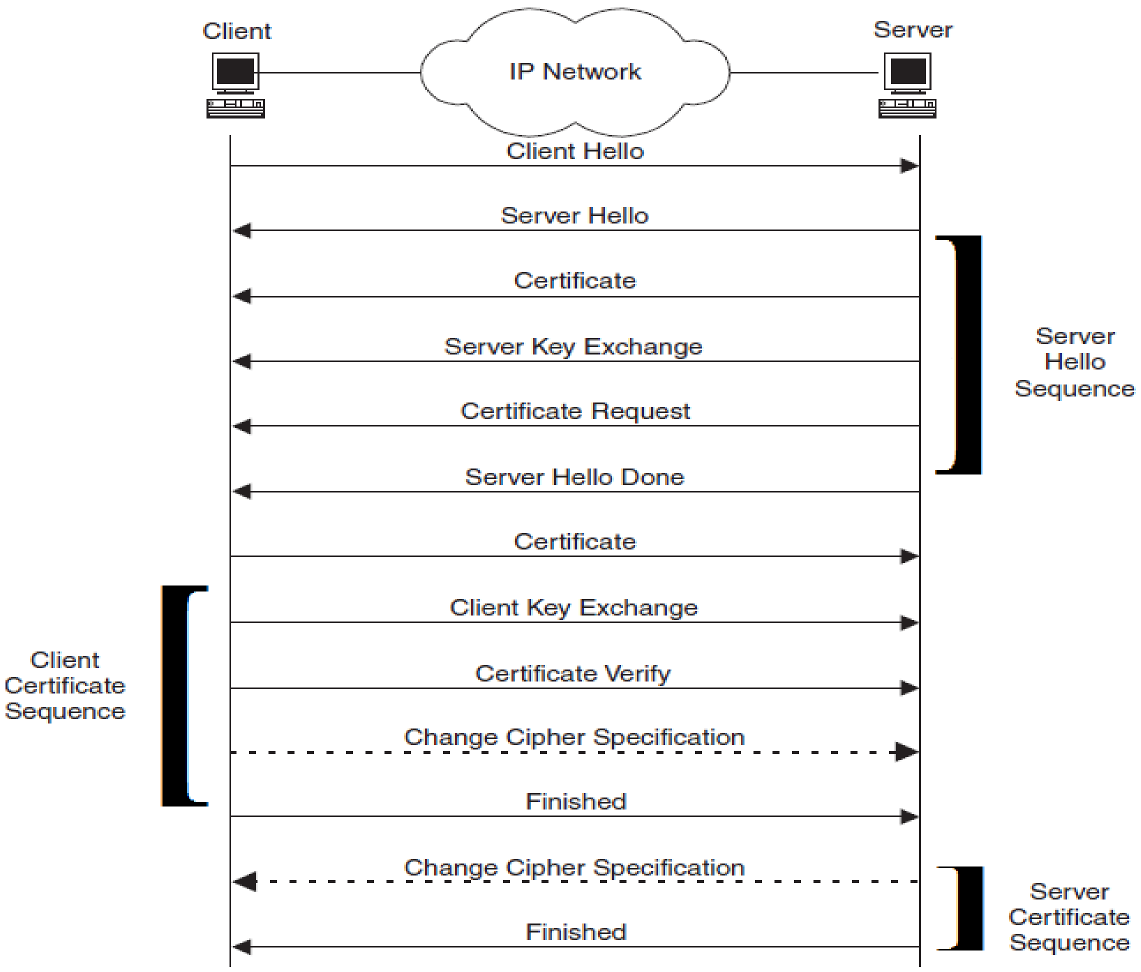


Figure 27: Handshake message exchange (Joshi 2008: 128).

3.6.3. Change Cipher Spec Protocol

Change Cipher Spec protocol (Joshi 2008: 125 – 132) is a one message protocol at the end of the Handshake protocol procedure. This message is compressed and encrypted under the current security parameters. It is sent to inform the communication entities that the new security parameters have been agreed, and that the new messages will be protected by the newly agreed parameters. Change Cipher Spec protocol sends a message of value 1 of one byte, this message is utilized by the Handshake protocol to instruct the Record protocol to change to the new configurations.

3.6.4. Alert Protocol

Alert messages are supported by the Record protocol; these messages are carried out by the Alert protocol. TLS Alert protocol (Joshi 2008: 125 – 132) protects the content and the exchanged messages from either errors or severe messages. The protocol sends warning messages informing about the level of severity, these messages are carried within its two bytes header. Moreover, the protocol assigns the first byte to inform about the level of severity, while the second byte indicates exactly which error or threat has been occurred. In the high risk cases, the TLS is instructed to terminate the connection. Table 3 specifies the different error messages, their values within messages, and their severity level.

Alert protocol provides protection against the truncation attacks; that is by setting up a disclosure mechanism between both ends. When a connection experiences a discontinuity without a termination notify, the session will be ceased, and in such situation, new session will have to be established with new agreed parameters.

Table 3: Alert messages and their severity level.

Severity	Message and Value	
Warning	close_notify: 0	bad_certificate: 42
	unsupported_certificate: 43	certificate_revoked: 44
	certificate_expired: 45	certificate_unkown: 46
	decrypt_error: 51	user_canceled: 90
	no_negotiation: 100.	
Fatal	unexpected_messagage: 10	bad_record_mac: 20
	decryption_failed: 21	record_overflow: 22
	decompression_failure: 30	handshake_failure: 40
	illegal_parameter: 47	unknown_ca: 48
	access_denied: 49	decode_error: 50
	export_restriction: 60	protection_version: 70
	insufficient_security:71	internal_error: 80.

3.6.5. Cipher Suites

One of the main strengths of TLS is supporting a vast variety of cipher suits. These suits are utilized by the different procedures including key exchange algorithms, authentication, encryption, effective key bits and MAC. TLS also supports different key lengths; it supports from 40 up to 256 bit keys, in addition to supporting different modes of operation. The selection of the appropriate cipher suite, keys and modes depends on the compatibility and readiness of the communicating entities. This is agreed upon within the negotiation session of the Handshake protocol. Table 4 (Kacherginsky 2009) gives more details about the supported ciphering parameters by TLS. It is worth mentioning that at the beginning of the negotiation session, TLS by default operates using NULL identifiers for the given parameters.

Table 4: The different cipher suits.

Procedure	Supported schemes
Key Exchange Algorithm (KEA) and authentication	RSA, DH, DHE, ECDH, KRB5, SRP, PSK, DSA, ECDSA, DSS.
Encryption and MAC algorithms	3DES, AES, Camellia, DES, IDEA, GOST, RC2, RC4, SEED, SHA, MD5.
Modes	CBC, GCM, EDE.
Active Bits	0, 40, 56, 80, 128, 168, 192, 256.

Example: TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA, it has a cipher ID of 0x00004A and it uses ECDH for KEA, ECDSA for authentication, 3DES with modes EDE CBC for encryption, SHA for MAC, and 168 active bits.

3.7. Datagram Transport Layer Security Protocol

TLS is a connection oriented protocol, as aforementioned, which means that it runs only over a TCP environment. As communication in certain cases experiences significant delays and packets loss, which causes more delay due to the TCP retransmit feature, UDP is preferred. UDP is faster as it is unreliable connectionless protocol; it does not require acknowledgments, error check, flow control, packets orders, and recovery options, additionally it has a smaller header compared to the TCP one. Thus, UDP is preferable for some certain applications and protocols that require faster communication, e.g. the Session Initiation Protocol (SIP) and gaming protocols. SIP is used for signaling and one typical application of it is the Voice over IP (VoIP) services. TLS for signaling applications in such cases is not preferred because of its latency.

Datagram Transport Layer Security (DTLS) “RFC6347” (Rescorla & Modadugu 2012) protocol was introduced to cover these shortages of the TLS, since it is a UDP connectionless protocol. DTLS is roughly similar to TLS regarding to its security mechanisms; however, DTLS performs extra functions to guarantee the reliability of the communication, thus adding up TCP features while sustaining the UDP performance and speed. The differences between DTLS and TLS include:

1. Sequence numbers are explicitly added to datagrams; this allows reordering.
2. The use of a simple time packet reordering scheme.
3. Data is handled as records; these records are not transparent for applications anymore. This means that either a record arrives or not, also a record can be discarded.
4. Data size is limited, as the size of the UDP; so the maximum record size is only 1500 bytes. Otherwise, data has to be fragmented to several records.
5. Stream ciphers are not supported; as a result RC4 ciphering is not acceptable anymore.
6. Termination notification is not used anymore; this error is mostly acceptable.
7. DoS counter measures are considered. It uses a cookie mechanism for the handshake, and the reply must include it to validate the session.

3.8. Real Time Transport Protocol and Secure Real Time Transport Protocol

TLS and DTLS protocols can be used to secure the signaling between the communicating entities. For the payload and media content, these protocols cannot be used, as these contents require real time delivery while these protocols only support non-real-time transmission. For such cases, the Real Time Transport Protocol (RTP) is used.

RTP “RFC3550” (Schulzrinne, Casner, Fredrick & Jacobson 2003) protocol provides real time end to end transport delivery services; where it is used for unicast as well as multicast streams. RTP runs over the UDP layer, as a result it does not guarantee the delivery or the quality of the transmitted payload. For this reason RTP utilizes the Real Time Transport Control Protocol (RTCP) to perform these monitoring and quality control functions. RTCP is responsible for handling reports, controlling the encoding schemes and media formats depending on the quality, synchronization and the deployed ports. Unlike UDP, RTP header contains sequence numbers and timing information. This is so important for media transfer because it allows the receiver system to construct the received segments in the right order. Also for the case of lost segments, RTP sends resend requests. RTP and RTCP each operate using one port, one for the media and the other for control. When the media is audio combined with video, both protocols operate using two ports for each, since coupling between the different media is not provided. By default if not configured otherwise, RTP uses an even port, while RTCP uses the next higher available odd port. Regarding security, RTP does not include security features; however these features are included in its secure version, the Secure Real-Time Transport Protocol (SRTP).

SRTP “RFC3711” (Baugher, McGrew, Naslund, Carrara & Norrman 2004) provides the same functions as RTP, as it provides real-time transport between the different applications. In contrast, SRTP provides optional confidentiality and authentication features, in addition to a mandatory messages integrity. Similarly as RTP, SRTP uses a protocol called the Secure Real Time Transport Control Protocol (SRTCP) to monitor its performance. This protocol acts as RTCP but rather with protected messages. SRTP provides its security services by means of using a recommended authentication tag field and an optional Master Key Identifier (MKI) field. The purpose of the authentication tag is to protect the header and the payload, which is maintained by authenticating the data. Likewise, SRTP uses keying schemes to provide confidentiality; this is performed by utilizing the MKI field to derive the keys needed for the session. However, SRTP does not have a facility for key management; for that reason it normally depends on some other protocols to perform these operations, e.g. ZRTP, MIKEY, KEYMGT, as well as other protocols.

3.9. DTLS-SRTP

DTLS and SRTP could be used simultaneously to successfully achieve a complete protected content. This extension for SRTP was given by the IETF, where it utilizes the DTLS for keying schemes instead of using external protocols. This allows managing the keying procedure during the media session rather than signaling. DTLS-SRTP “RFC5764” (McGrew & Rescorla 2010) combines the security features of SRTP regarding encryption, authentication and protection with the DTLS key management facilities. DTLS performs the negotiation and key management by the use of its Handshake protocols. These parameters are utilized to protect the Record layer as well as the SRTP application data. When DTLS-SRTP is combined with SIP or VoIP, due to their integrity protected signaling services, DTLS-SRTP provides a complete end-to-end security scheme for the exchanged payload (Fischer 2008).

4. PRIVACY CONSIDERATIONS, ARGUMENTS AND SOLUTIONS

4.1. Introduction

In the previous chapters, the different security considerations, dimensions, and parameters needed to build a secure system were discussed, also the faced problems were mentioned. The main target behind this study was to find the advantages, drawbacks and the main shortages the telecommunication systems encounter. This study helped providing a better overview about the security situation. As noticed, security concerns protecting the employed systems and the communication facilities from all means of the intentional harm; also it includes measures to maintain the system's safety to protect against the unintentional harm. In telecommunications, security means protecting the data from all sorts of alternation. On the other hand, maintaining security does not mean protecting the communication entities and their data. In a worst case scenario, these data can be wiretapped, mined and analyzed to extract information about the communicating entities. This situation arises the need to answer the following questions: Who is allowed accessing an entity's data? What are the purposes? Also, under what circumstances it is allowed? The answers for these questions are a part of the bigger term privacy, which is defined and discussed hereafter.

4.2. Privacy, Definitions and Theories

Privacy is a new interest in the research field; within the last two decades, the number of researches that includes the word "Privacy" has increased dramatically than before; this is shown in Figure 28. The reason behind this growth is the new demands and concerns in privacy and the moral issues regarding technology and sciences.

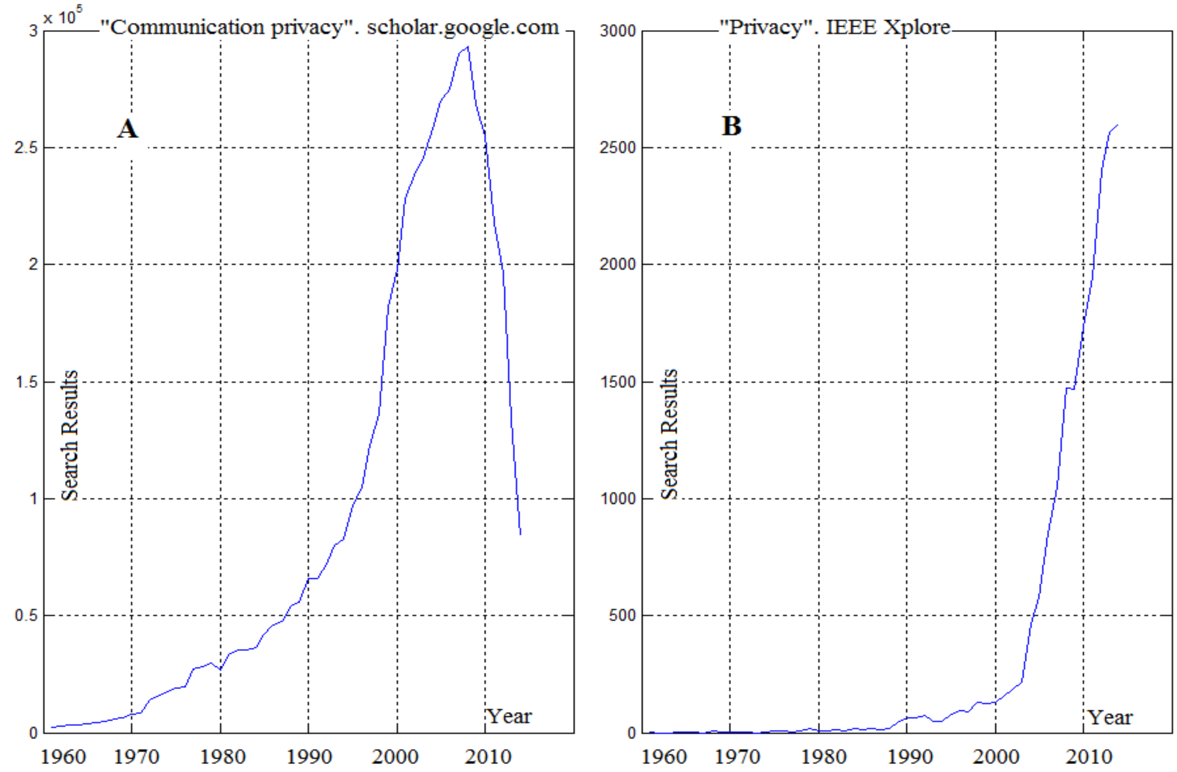


Figure 28: The number of the published articles, journals, papers and books between 1960 and 2013, including the search term: A) "Communication privacy", extracted from scholar.google.com B) "Privacy", extracted from IEEE Xplore Digital Library [Cited 14 Sept. 2014].

Privacy as a term goes beyond the security meaning. Privacy protects users' private data from being disclosed, or connected to draw a figure about their activities and their personalities (Horniak 2004: 15). These unwanted activities can cause harm if being used against users; also it can be used in a way threatening their lives. However, privacy is not absolute, as there are some lines where privacy needs to be revealed under some criteria and by the right entities. These criteria and entities will be discussed later on.

Privacy can be explained according to two theories, control theory and restricted access theory (Spinello 2010: 150 – 153). The control theory was given by Professor Charles Fried; in his theory he proposed that privacy can be preserved if a person has control over his information and its spread. On the contrary, the restricted access theory of Professor Ruth Gavison implied that, privacy can be preserved on a condition of restricting what others can access, based on secrecy, anonymity and solitude. Both theories were contradicted by Professor and philosopher James Moor; in his control/restricted access theory (Moor 1997: 27 – 32). He stated that controlling information in the cyberspace is unfeasible; however, it is a must that the right entity at the right time can access the information. This comprises both advantages of both previous theories, that an entity can control information, and restrict others from accessing it, while it is still accessible by the right entities whenever needed under the right conditions. Moreover, the concept of privacy-policies was given, where it is flexible to be set according to the situation.

The above mentioned theories summarize the privacy definition as: privacy is a right for individuals, as they hold the right to control their own information and the right to restrict others from accessing it, as long as no harm can be caused to others with this information.

4.3. Privacy Dimensions

To preserve privacy, its dimensions need firstly to get well defined. Privacy includes five dimensions, explicitly, data and traffic, identities, locations and mobility, time, and existence (Candolin 2005: 98 – 104). These factors collectively preserve a complete privacy scheme for the communicating entities. Traffic and exchanged data between entities should be protected against others; luckily, the cryptographic functions of the security procedures perform these tasks. However, data suffers from the internal malicious intrusion and the external attacks targeting the cryptographic algorithms.

Identity is how a person defines oneself to the world (Hogg & Abrams 1988: 2), describing his individuality, sort and relation among others. In telecommunications, an identity is used to relate a user to his own activities, interests and privileges. Thus, telecommunication systems should take considerations to protect against revealing users' communication identities. This case is practically unfeasible since the communication identities are used for session establishment. A feasible solution is by using temporal identities than using the real ones, also by deploying a level of randomization. This later is the concept of anonymity. A person can protect himself by the use of pseudonyms and different identities for the different sessions, these identities should be independent of any other factors. However, the absolute anonymity solution faces a difficulty with the lawful interception consideration.

Location and mobility privacy is one of the most crucial concerns when talking about privacy. Systems and new applications by default keep tracking records about their users; these records are used to provide users with the services they demand. However, there is no enough transparency on the process of such data collection and usage. Location can draw a general picture about a person’s behavior, interests, and activities. This situation threatens users upon information disclosure or any unwanted actions regarding their own data. The current challenges are concerning the Location Based Services (LBS), which users require themselves, or share with others. Not only LBS, but also other unwanted applications and mistrustful networks collect location data about users.

Time privacy intends to protect against disclosure of transactions and its associated times. Time can be used with the other dimensions above to precisely detect users’ activities. However, hiding the time of occurrence is not an easy task for implementation. One of the afforded solutions to hide the real time of transactions is by randomly sending junk data at random instances, this will cause a sort of illusion about the exact times of events. On the other hand, this solution overloads the network resources.

The last dimension is existence privacy. Existence privacy tries to protect the communicating entities by hiding them, so that a surveillance system cannot detect them. This issue also is not easy for implementation, since nodes and users need to publish themselves for the communication procedure. However, there are different solutions that can afford such level; these solutions include nodes’ visibility control, and the continuous use of pseudonyms.

4.4. Privacy Relations

Privacy can be viewed as a set of relations; it can be described as the collection of anonymity, unlinkability, unobservability and undetectability (Pfitzmann & Hansen 2005: 4 – 13). These relations provide users with the needed privacy level by hiding their identities, as well as any indication, relation or connection about their activities. Thus, these relations protect users from information leakage caused by the deployed systems.

In brief, pseudonymity is the use of traceable anonymous identities rather than the real ones. Anonymity is the ability to combine an anonymous identity with a recognizable one, in a way that an identity cannot be identified from a set of identities. This can be achieved by the continuous use of pseudonyms, or providing less information than the needed for identification. Unlinkability is the inability to draw a link or relation between two identities or between two activities. Undetectability is the inability to detect the existence of an identity or its participation in an activity. Finally, unobservability is the inability to observe a user and its activities, this implies undetectability and anonymity.

Anonymity in general is classified into three categories, sender anonymity, receiver anonymity and relationship anonymity. The former two categories protect sender's and receiver's identities, while the later one rather does not give information about the communication and whether users are involved in an activity or not, i.e. unlinkablility. Also it is the weaker version and can be maintained by sender or receiver anonymity.

The given parameters can be rewritten as a set of relations as following:

Unobservability → Undetectability
Unobservability → Anonymity → Pseudonymity
Sender/Receiver anonymity → Relationship anonymity.
Sender/Receiver unobservability → Relationship anonymity.

It is clear that the needed sufficient condition to preserve privacy is by maintaining unobservability. Unobservability on the other hand is difficult to be achieved in application as it requires systems of high complexity. However, a simple mechanism to implement unobservability is by providing anonymity, in addition to spreading dummy meaningless traffic. The dummy traffic provides the needed undetectability to the exchanged messages.

4.5. Privacy Levels

The given arguments about privacy are conceptual; in turn absolute privacy cannot be achieved in reality (Chao 2009). However, to a certain level privacy can be achieved by applying some mechanisms as discussed earlier. In Figure 29, six states are used to evaluate the privacy situation; in this figure beyond suspicion would be the best affordable solution in reality, while in contrast exposed or provably exposed are the worst cases, and they are common in web and some of the VoIP applications.

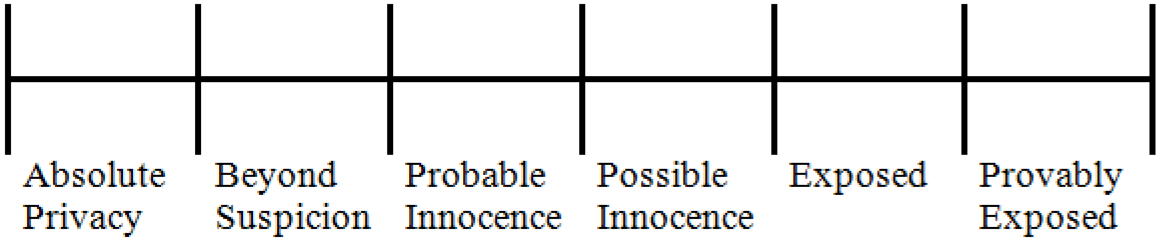


Figure 29: Anonymity degree (Chao 2009).

4.6. Parties, Rights and Responsibilities

The word “party” has been used within this research several times, including communication parties and third party organization terms. Within a communication session, there are four parties included; these parties have different rights and responsibilities according to their nature (Mason 2004). First and second parties are individuals or entities that establish the communication session. By default, these parties are users who do not hold control on any of the communication factors; they basically use the provided service. The third party is the one managing the communication environment; though, it is not a part of the communication session and does not have access to that session by default. This party can be the operator network, a monitoring organization, the governmental authorities and policy officials. The fourth party is all the other entities, which as well do not participate in the communication session and do not get any information about it by default; they only get the information allowed for them. This party can be the public, or in a worst case, a malicious attacker. With this clearance, it is obvious that the first and the second parties hold accountability, while the third and the fourth do not.

These parties have different rights and responsibilities. The first party has the right to privacy. According to the privacy theories, the first party entities hold control over their own information, and they have the right to restrict others access to their information. This party has to take considerations while spreading their own information, and they hold the responsibility for the type of information they spread. Additionally, this party holds the right to acquire the level of privacy it suits them, upon their understanding of the different levels and the benefits they gain or the threat they might face (Graham 1999). However, this party as a part of the society holds a right to not cause harm with the right they hold, which again means that privacy is not absolute. Officials under the legal considerations can break into an individual’s privacy, if it would cause a sort of danger.

Second party is by default a replicate to the first one, they have the same rights, as they are sharing a communication relation. By default, the first party trusts the second party, which gives the second party the responsibility for not spreading the first party’s information. That is the reason that the first party has a responsibility on what they share and with whomever they share it.

Third party is the most important in the privacy process, as they have access to the resources of the communication facility. Third party has the responsibility to protect the communication between the first and second parties. Also third party has to protect other parties' data, in addition to the stored personal data. Additionally, this party holds a right to protect the society from any sort of danger that other parties might cause, and therefore they have to take their own considerations.

Fourth party on contrast to the previous parties has the least responsibilities and rights. They have the right to access the authorized data only, and they are not authorized to interfere in the communication session between the previous parties.

4.7. Privacy Conflicts and Costs

The meaning of privacy is not consistent for all parties, it rather has so many conflicts; here are some of these conflicts (Noam 1995: 52 – 59).

1. Cultural conflicts: it depends on the culture and its understanding and acceptance for the privacy values. Some cultures and societies value individuals' privacy while others see it as a right for the whole society.
2. Organizational conflicts: in organizations, such as work places, governments, policy officials, they see a different meaning for privacy. They consider it a right for the organization rather than individuals. That causes actions like surveillance and monitoring.
3. Individual conflicts and conflict of interest: individuals also have different opinions about privacy considerations. There is no common opinion about it.
4. Structural conflicts: the structure and design of privacy preserving systems might conflict with the security and safety models, as the type of information that needs to be accessed will face a sort of difficulty.

5. Communication conflicts: tracking, mobility and other services will face difficulties also.
6. Price conflicts: the cost to afford privacy will increase the prices of the services, since systems will be more complex.
7. Efficiency and quality conflicts: information collecting is used to measure the quality of the provided services; this will suffer with the privacy rules.
8. Operational conflicts: networks share resources and information, with the limitation of this information, the operational ease will be affected.
9. Standardization conflicts: to come to a widely agreed vision and to an acceptable standard, this will not be an easy task, and it will consume time.
10. Expansion conflicts: once agreed, all current and new networks have to follow the new standard.

In addition to the previous conflicts, crime fighting and privacy is an important issue to take into consideration. Privacy as all rights can be misused, that is because of the coverage privacy provides against information collection, which in turn can encourage the illegal actions. This later increases the criminal activities and certainly causes harm to the society (Spinello 2006: 186 – 188).

All the given conflicts increase the complexity of the system design, and in turn they increase the cost of privacy; as well they cause a rise in the information costs.

5. SUGGESTED SOLUTIONS

In this chapter, different solutions for the difficulties that have been mentioned previously are proposed and evaluated. These solutions are used to enhance the security situation inside the network; also they help maintaining users' privacy scheme.

5.1. End To End Encryption

In mobile networks encryption and integrity tasks terminate at the RNC; this implies that data and voice are transmitted in the blank inside the CN. The outer part of the network protects users from the interception by others. However, there is no mechanism to protect against the internal interception. Here, by interception, it refers to the malicious one. The abovementioned security procedures are performed at the link layer, and they are controlled by the serving networks. In turn, they can enable/disable and control these functions according to the situation, and the provided security level. This provider fully controlled mechanism is called Link Encryption (Lin & Dam 1996: 274) (Smith 1997: 63 – 83). A typical example of link encryption is by implementing an in-line encryptor device, e.g. Fortezza crypto cards. With link encryption mechanisms, governments and authority organizations can have the means to access users' traffic, either through their own equipments or by means of the SN. This is a concern for users since it leaves a chance for the illegal actions targeting their privacy. The provided solution for the latter case is by utilizing the higher encryption scheme, End to End Encryption (E2EE).

E2EE (Lin & Dam 1996: 275 – 276) deals with the privacy threat by providing a security mechanism independent of the security standards afforded by the service provider; it rather depends on the users' security preferences. E2EE allows the use of own encryption schemes between end users. E2EE performs its tasks at the application layer, which means that it is independent of the network and the other intermediate devices. A typical example of E2EE is the Pretty Good Privacy (PGP) software which is used to secure emails by providing end-to-end public key encryption level (Lin & Dam 1996: 163 – 165). When E2EE is applied, third party entities will not be aware of the exchanged content since it is encrypted, thus the content will be meaningless for all other parties rather than the communicating peers. This deployment can afford absolute privacy scheme, and therefore users have to hold the responsibility upon the exchanged content. However, implementing such mechanism arises the lawful interception problem, since it leaves authorities unable to intercept users' traffic (Dohmen & Olaussen 2001: 49). On the other hand, authorities still have the ability to monitor the communicating parties, know their locations, activities and the exact times.

Generally, there exist three solutions to implement E2EE over cellular networks (Chumchu, Phayak & Dokpikul 2012: 210 – 214). The first solution is by using external module to digitize then encrypt the voice signal. A special modem with the GSM serving network will be used after for transmission. The second solution replaces the modem used in the first solution by the GSM or 3G voice channel for transmission. The third solution also replaces the voice channel by the data channel to establish the encrypted communication. The typical affordable solutions in the market rely on the third solution; they use the data channel to implement the encrypted communication. The main reasons for choosing the data channel over the voice channel are the ease of implementation, the security algorithms and protocols are applicable, tunneling is affordable, and the configurability of the data channel by end users' applications.

The main challenges the voice channel face are the nature of the speech coding mechanisms, the quality of the encrypted voice and the key exchange algorithms. In GSM, vocoders are designed to encode human speech, with human voice characteristics (Kaiugampala, Villette & Kondoz 2003). When encryption is applied to human voice, it loses its characteristics and becomes scrambled. This problem causes the voice to behave like noise, and hence vocoders cannot perform their functions to handle it anymore. The reason for this problem is the limited bit rate that the GSM affords, which affects the quality of the digitized voice. . Holub and Street applied the E2EE to GSM voice channel and the result was an acceptable degradation in the voice's quality (Holub & Street 2004). The degradation problem almost vanishes when using the data channel, or the wideband/3G because of the higher bit rates available. Figure 30 shows the typical architecture for that applied system.

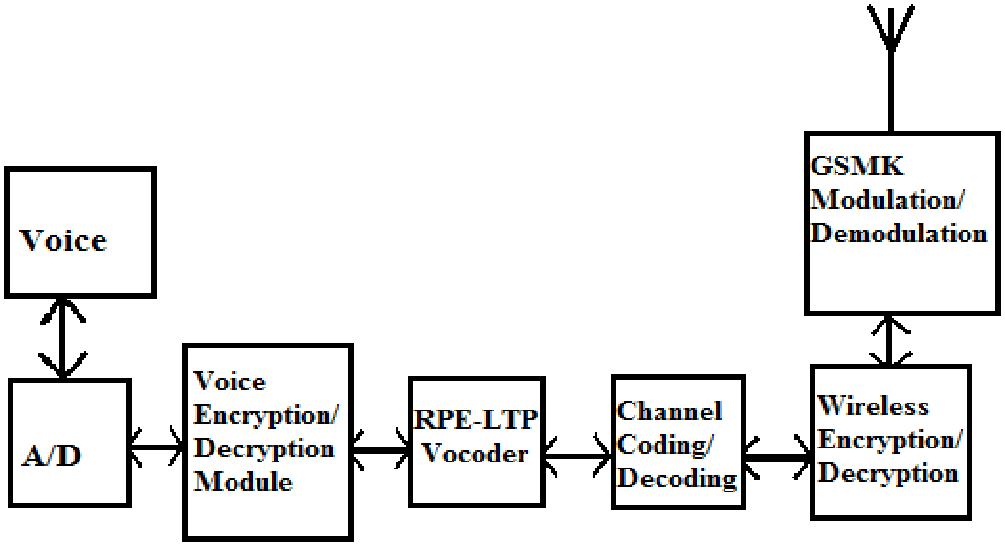

GSMK Modulation/ Demodulation
Voice
A/D
Voice Encryption/ Decryption Module
RPE-LTP Vocoder
Channel Coding/ Decoding
Wireless Encryption/ Decryption

Figure 30: Voice Encryption module (Qi, Yang, Jiang, Liang & Zhou 2008).

In the previous figure, the module Voice Encryption/ Decryption consists of an encoder/decoder and a modulator/demodulator to modulate the encrypted voice to a human characteristic signal as shown in Figure 31 below.

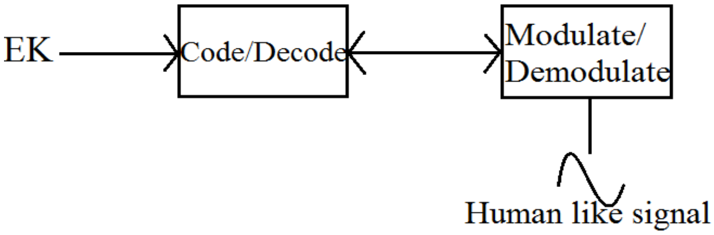


Figure 31: Voice Encryption/Decryption module.

In E2EE, the communicating parties need to have the same secret shared Encryption Key (EK) (Wang, Jiang, Li, Niu &Yang 2009: 1, 7, 12 – 14). The concept of the PGP and its standard OpenPGP "RFC4880" (Callas, Donnerhacke, Finney, Shaw & Thayer 2007) can be used as a means for key exchange, since it allows entities without prior knowledge of each others to exchange the shared keys. In this procedure, the Encrypted Session Key (ESK) which is created during the authentication and identification phases will be used in symmetric cryptography scheme for encryption and decryption.

Other mechanisms as well can be used for the shared key exchange procedure, these mechanisms include pre-shard key or live exchange key. The pre-shared key system is one of the typical solutions; it can be employed within an organization or special officials by distributing the keys that they will use for encryption. Also, this distribution can be done over a secure link, e.g. encrypted email service. In their prototype, Chumchu *et al.* used the Bluetooth module for the key exchange procedure. In this solution, the users' contact list was extended to have an EK field for each contact. This later configuration can be generalized to have different EK fields for the same person with the other contacts. In other words, encryption will be unique between every pair of contacts. This later configuration provides a higher level of privacy between users. However, the drawback of this given solution and the pre-shared keys in general is that they need a direct contact to exchange the EK, or a trusted encrypted service to exchange the key. Typical market products use the pre-shared key system, and mostly they use the AES cryptography algorithms for the EK. It is worth mentioning that the highest security level provided for these systems is AES with 256-bit key; this system is implemented by BlackBerry systems (Hewitt 2014) and approved for North Atlantic Treaty Organization (NATO) communication.

The other mechanism for key distribution is live key exchange. In this mechanism, users will need to have public and private keys. Public and private keys belong to the asymmetric cryptography systems (Stallings 2011: 267 – 277). In these systems, the public key is only used for encryption; this key can be shared with the other users. On the other hand, the private key is the one used for decryption, and it is only stored at the user's side. When implementing a live key exchange scheme, users will need to connect to a trusted Key Distribution Center (KDC) which can be a Public Key Authority (PKA) (Stallings 2011: 412 – 429). Users need to acquire the public keys for each others to establish an encrypted session; these public keys are stored in the KDC. The KDC performs authentication and identification procedures with users then it sends the requested public keys. Using such scenario for key distribution strengths the security of the system, as it protects against the MitM attacks and eavesdropping. That is because of the fact that only the user with the right private key can decrypt the intended message. Figure 32 illustrates the process of the public key distribution. Here, the KDC is operated by PKA.

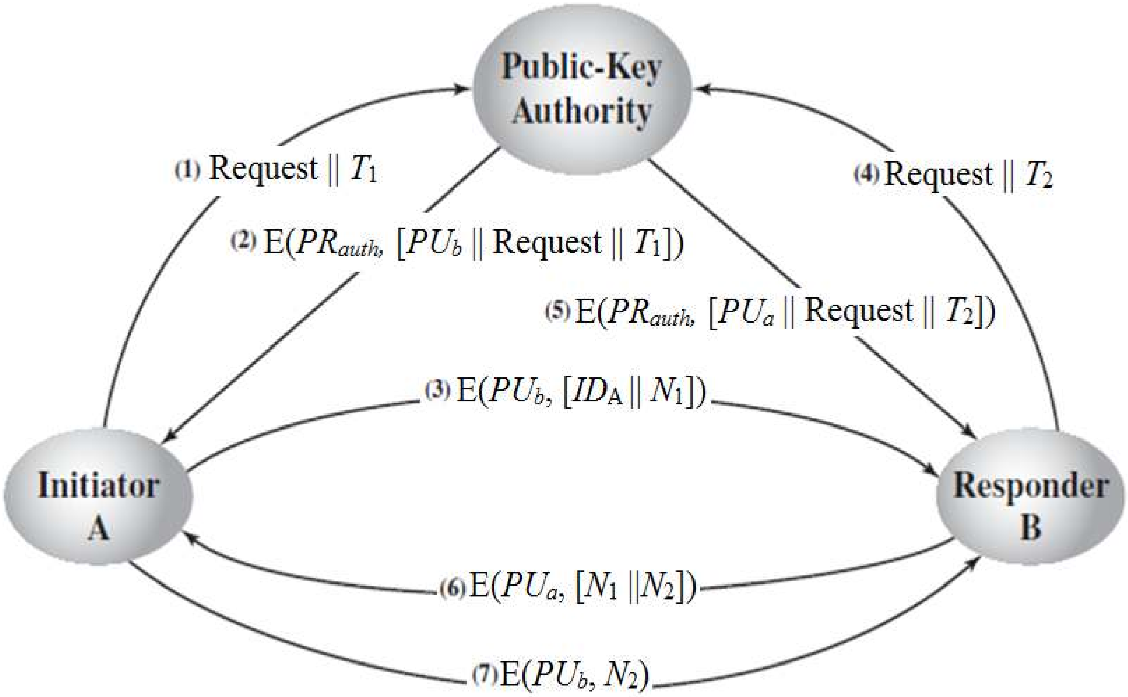

Public-Key Authority
(1) Request || T_1
(2) E(PR_{auth}, [PU_b || Request || T_1])
(4) Request || T_2
(5) E(PR_{auth}, [PU_a || Request || T_2])
(3) E(PU_b, [ID_A || N_1])
Initiator A
Responder B
(6) E(PU_a, [N_1 ||N_2])
(7) E(PU_b, N_2)

Figure 32: Public Key Distribution (Stallings 2011: 427).

In this figure, A to communicate with B needs to have her public key, which is acquired from the PKA. The process of the key exchange is done through seven messages. A sends a timestamp T_1 with the request for B's public key, the PKA replies with an encrypted authenticated PR_{auth} message to prove its identity, the reply includes the original timestamp T_1, and the public key of B. A sends an encrypted message to B using her public key PU_b, with his identifier ID_A and a unique nonce N_1. B identifies A, however, she requests his parameters from the PKA for security reasons; this request is done in the same manner. By that message, B and A know about each others. After that, B sends an encrypted message using A's public key PU_a, this message includes A's nonce N_1 and her unique nonce N_2. A in turn decrypts the message and sends back the N_2 nonce. By these later messages, A and B are sure that they are the only participants in the communication session.

This given solution of using public/private key systems has an important feature, which is the lawful interception. If the distributed keys within the KDC/PKA are controlled by only the authority, it will guarantee that the lawful interception is allowed. This means that only the authority but not any other party will be able to intercept the traffic. In turn, this also means that any other malicious interception will not be allowed, because keys will not be available and hence the communication will be fully encrypted.

5.2. Key management and key distribution

Chapter 2 presented the difficulties the key distribution, and the AKA mechanisms face. It is clear that this part is the weakest parts of the security system of the mobile network (Table 1, chapter 2) (Tang, Naumann & Wetzel 2013: 2). For that reason, using public key systems is a better alternative, since encryption and decryption keys are different. Also, private keys are stored at end devices, either the user device or the serving node. This later means that decryption keys do not need to be exchanged, which improves the system's security. Also, a suggestion of generating the RAND locally at the end devices than centrally at the network side would guarantee the freshness of the RANDs since they will not be correlated.

5.3. Location Privacy Protection

Location is a quasi-identifier and a major dimension in the privacy issue (Joshi 2008: 257 – 258). Location can be used to give information about the user's current situation, it can give a figure about own interests, or connected to the visited places to identify a user's identity. Location information is of high importance, it can be used to afford users many services, also for post-disastrous, rescuing, and crime fighting. On the other hand, this information can be misused to invade a user's privacy by getting information about his personal and public activities. In mobile communication, data protection has received the most of the attention, by many security measures, on the contrary; location privacy protection is still in need for more effort to provide an acceptable solution. Fortunately, the IETF is currently working on this issue with their project Geographic Location/Privacy "GEOPRIV" to afford the needed level of location privacy.

When users establish a session, they by default do not receive location information about each others; however they can share this information only upon their permission. This means that the protection scheme is needed against these activities performed out of users' permission, control and awareness. Generally, information is generated, processed, exchanged and stored mostly without users' awareness (Rechert, Meier, Zahoransky, Wehrle, von Suchodoletz, Greschbach, Wohlgemuth & Echizen 2013: 211 – 222). This information is used for many purposes as previously mentioned. From an operator' perspective, some parameters and information are needed for communication purposes, in other words, it is not feasible to hide the location information from an operator. These include the Uplink Location Updates (U-LU) and the availability of the paging area information in the local Visitor Location Register (VLR), and the availability of the VLR information in the Home Location Register (HLR).

Typical applications concerning and utilizing location information are the LBS (Schiller & Voisard 2004: 15 – 26) (Gruteser & Grunwald 2003) (Snekkenes 2001). LBS applications provide users with navigation, and information about the associated activities within an area of interest. Thus, LBS providers need to access users' locations upon their permission to afford them the required services. Even though LBS by law and policies do not share users' information with other parties, there are no guarantees for these actions. That is the reason that LBS are included in the semi-honest services category.

Generally, to protect the location information, the first step is by establishing transparent policies with the network and service providers regarding location data. Secondly, by implementing solutions which assist providing an adequate level of location privacy. A typical solution makes use of blurring and obfuscation techniques to hide the exact location from the serving network; this is done by sending slightly modified inaccurate location data. In their paper, Rechert *et al.* proposed the following suggestions:

1. Observation frequency: a mobile device with a software installed to detect the operator's control messages used for location updates. Such software can control the frequency of updates, additionally informs the user about the network activity.
2. Observation accuracy: this means reducing the accuracy of observation by the network, it can be achieved as follows:
   a. Sending empty UL-U messages
   b. Sending less accurate UL-U messages.
   c. Using time offset with the sent reports, to avoid connecting a place with time observation.

Figure 33 illustrates the update mechanism and its relation with the location accuracy. In these figures, update measurements were increased from one in A to six in C. Figures B and C show that more updates give higher accuracy of the user's location. It is clear that, increasing the number of updates reveals user's exact location, thus violates his location privacy.

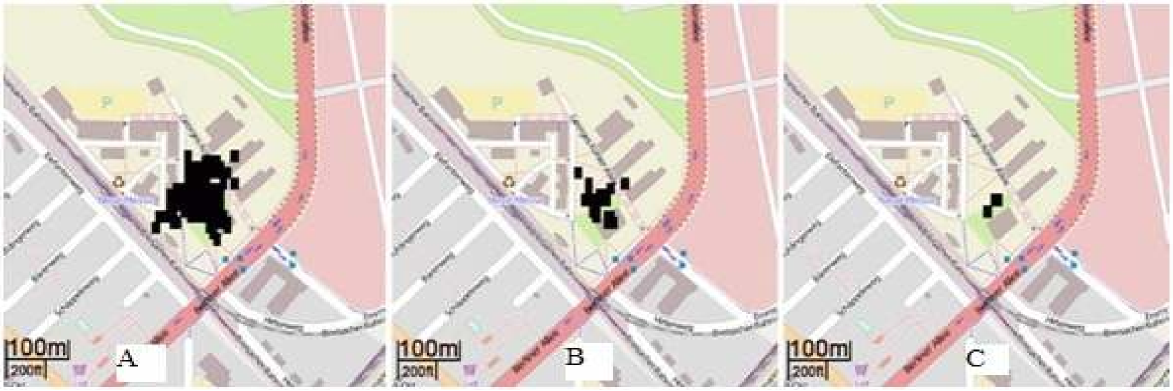


Figure 33: Location accuracy with different set of measurements (Rechert *et al.* 2013).
A) One measurement B) Four measurements C) Six measurements

The second solution concerns the LBS services. With LBS, the security situation is better since they do not have direct access to users, and they operate through the data network part. Solutions to protect users from localization include using K anonymity servers and mix zones. A mix zone is similar to a mix node (Chaum 1981: 84 – 88), where in a spatial area, user activities before and after crossing the mix zone cannot be linked (Bettini, Wang & Jajodia 2005: 185 – 199). In a mix zone, users' identities get mixed so their activities get anonymized. To choose a mix zone, it has to be smaller than the coverage area of a location update; otherwise the given mixing procedure will not be sufficient to provide the needed anonymization (Beresford & Stajano 2003: 46 – 55). This is illustrated in Figure 34.

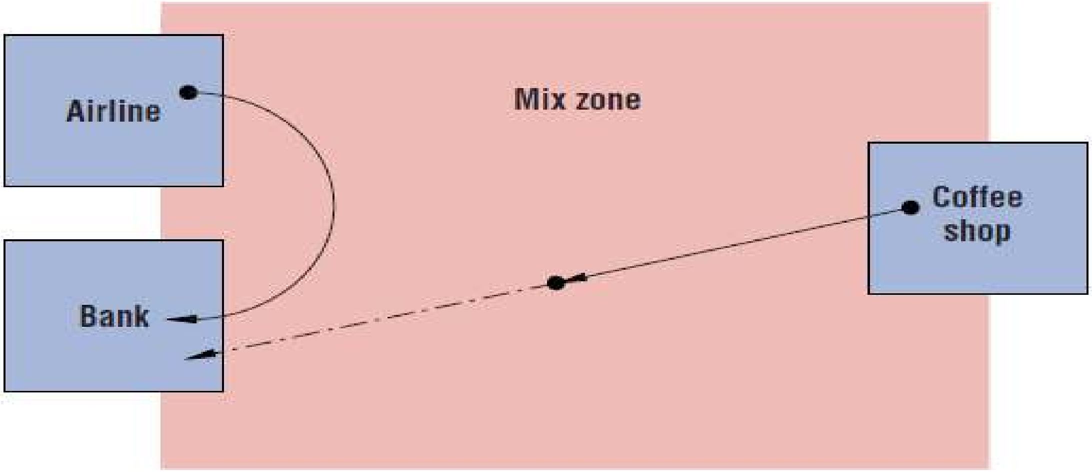


Figure 34: 4 mix zones, Coffee shop, Airline, Bank and the whole combined area (Beresford & Stajano 2003).

Another solution is by implementing K-anonymity identity server (Gedik & Liu 2008: 1 – 18) (Zuberi, Lall & Ahmad 2012: 196 – 201). In this scenario a user's identity will be mixed with K-1 identities within the area of interest. K value specifies the accuracy and anonymity level, large values of K insures high anonymity level with low accuracy while a small value gives a low anonymity level with high considerable location accuracy. K values are controllable, thus they can be different from a user to another. Figure 35 illustrates the idea of K anonymity technique.

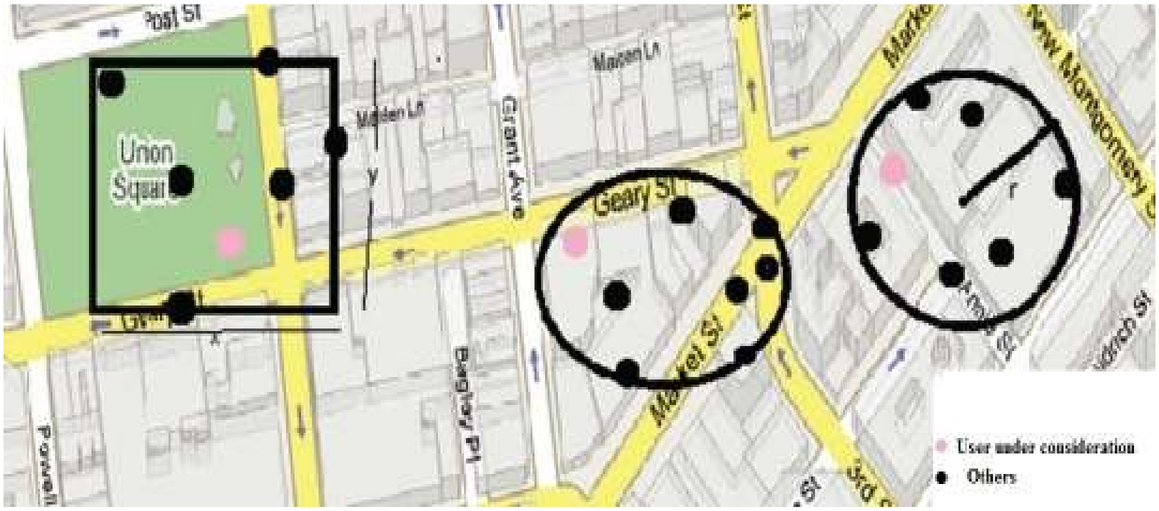


Figure 35: Data/distance cloaking, K-anonymity (Zuberi *et al.* 2012).

Another similar solution is by using of Network Address Translation (NAT) routers. In IP communication, NAT "RFC1631" (Egevang & Francis 1994) "RFC2663" (Srisuresh & Holdrege 1999) is used to connect a set of dynamically assigned IP addresses to the WAN network via a static IP address; thus NAT internal addresses by default are not visible to the other WAN applications and protocols. This configuration provides an advanced level of anonymity since service providers will not be able to identify the users' real addresses. Additionally, encrypting the traffic between users and the serving network protects users from the network surveillance. However, NAT systems do not support end to end encryption schemes like IPSec in general, but this difficulty can be overcome by applying application layer encryption, e.g. TLS/SSL.

5.4. Routing protection

Routing is analogous to location in IP networks, since IP addresses are indicators to the physical location of the communicating peers. This means that routing and location protection complete each other and both are mandatory for privacy protection. When packets move to their destination, the intermediate nodes perform the needed routing tasks for packet delivery. In a non-tunnel mode, data packets contain the ultimate source and destination addresses in their headers, thus within the delivery process sensitive information about activity, relation, sender and receiver can be extracted (Boukerche, El-Khatib, Xu & Korba 2004). This information can be improperly utilized, depending on the level of trustfulness of the intermediate infrastructures.

There are several solutions to protect a user's route from the unwanted activities including traffic analysis and global adversaries' surveillance; these solutions require (Seys & Preneel 2009: 145 – 155):

1. Preventing leakage of the ultimate destination information.
2. Preventing leakage of information about the participating nodes in a certain communication.

However, these requirements cannot be feasibly implemented in a normal mode routing. That is because of the routing nature and the fact that both ends need to be known for the routing process. Thus, only cryptographic routing and mixing schemes can be used to achieve these demands. The most basic solution to implement routing protection is by implementing IPSec in its tunneling mode as mentioned in chapter 3. IPSec protects the addresses of the sender and the receiver by sending the traffic within a VPN, thus the visible addresses within its header are the ones of the security gateways. Implementing IPSec benefits from its simplicity and lightweight, though advanced solutions can be used. These solutions include on demand cryptographic routing schemes, e.g. Onion Routing, Anonymous Routing Protocol (ARM) to hide the traffic, or IP addresses anonymity mechanism, e.g. Host Identity Protocol (HIP).

5.4.1. Onion Routing

Onion routing (OR) (Kaviya 2009: 339 – 342) is a cryptographic routing scheme that provides end to end secure routing by means of tunneling, where it employs an extendible principle to the IPSec. OR is an efficient method to hide the route information from the other intermediate nodes, since it relies on encrypted routes. OR encrypts the source and the destination addresses, then it adds an encrypted layer for every intermediate node; thus it creates an onion like cryptographic layered structure. When a packet arrives to an intermediate node, it decrypts its cryptographic layer with its own key, so that it can only see the information about the next hop of the route. This process is similar to peeling an onion layer. For the route creation process, OR employs special nodes to create unpredictable routes, these nodes are called agent routers (Fang, Liu & Zhou 2010). Only agent routers know about the ultimate destination, while intermediate ones know only about the next hop. These OR general concepts are adopted by the Secure Distributed Anonymous Routing Protocol (SDAR) (Boukerche, El-Khatib, Xu & Korba 2004), this protocol provides routing anonymity scheme and it proves resilience against active and passive attacks.

Figure 36 shows the principle of the onion like cryptographic layer creating. However, in application, Figure 36 is not the typical case since the cryptographic layers peel and build up, which means that it is not an absolute cryptographic structure between the communication ends.

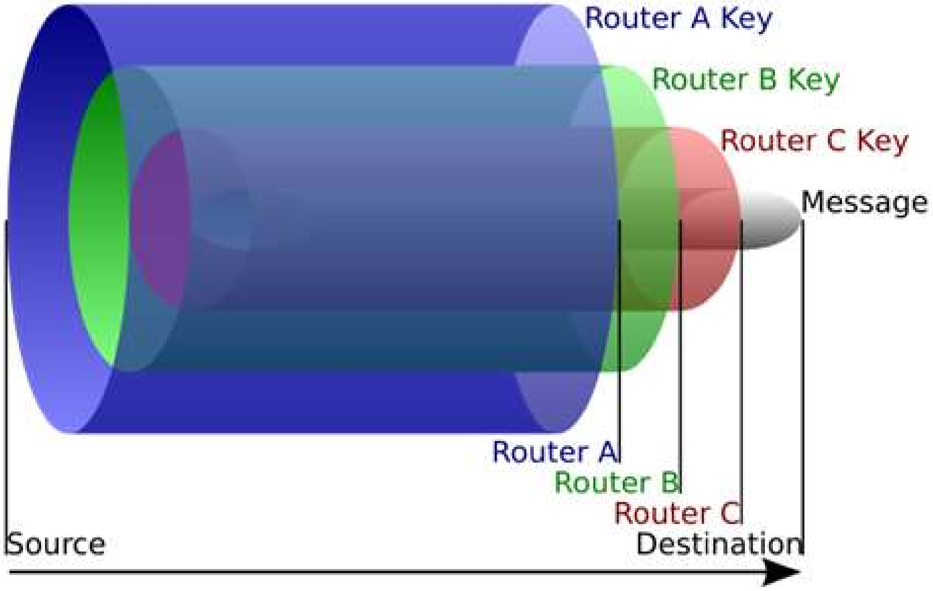


Figure 36: The onion routing structure (Kaviya 2009: 340).

Due to its cryptographic structure; OR proves robustness against traffic analysis (Backes, Goldberg, Kate & Mohammadi 2012) (Syverson 2003: 108, 110). On the other hand, OR is a heavy deployment for the network resources and it causes significant delays. That is because of the real time encryption/decryption process and its associated load to the intermediate nodes, also the longer unoptimized routes it uses. Another important issue to consider is the passive global adversaries monitoring schemes (Kaviya 2009: 339), where nodes' activities are monitored to predict an active route. This issue can be overcome by implementing a mechanism to hide the nodes' activities; which is discussed in the next section.

5.4.2. Anonymous Routing Protocol

Anonymous Routing Protocol for Mobile Ad hoc Networks (ARM) (Seys & Preneel 2009: 145 – 155) is a routing protocol used for routing traffic anonymization. ARM achieves its goal by adding a random Time to Live (TTL) value to the routing table of all ports of a node. ARM functions as follows: when a packet arrives to a specific node, all ports forward it according to their assigned TTL value rather than discarding it. When a node receives a packet, decryption is performed, where it fails if that packet is not intended to that node. Still, the packet is forwarded to the other nodes till the TTL value reaches zero. For route discovery, ARM rather depends on the route in demand and source routing schemes than the ordinary routing ones. In these schemes, the network keeps in silent mode till it receives a demand for a session establishment. The network responds by sending route discovery messages to explore the network, and then it decides the optimum route that might be used.

These mechanisms of ARM prove protection against the surveillance activities since all ports of a monitored node will be active, thus it hides the original route. On the contrary, ARM causes heavy loads to the network, since it circulates meaningless junk data around the network. Also, the use of in demand routing schemes dramatically explode the routing tables, additionally it might lead to unoptimized routes selection. Aside of these shortages, ARM can be combined with OR to provide a complete robust protection scheme against the global adversaries. In this configuration, the OR performs the encryption and tunneling procedures while the ARM maintains the routing anonymity. This configuration achieves the desired level of routing secrecy. However, this deployment is not feasible for implementation in large or slow networks, also not for real time data sessions due to the considerable delays.

5.4.3. Host Identity Protocol

Unlike the previously mentioned SDAR and ARM protocols that protect the routing data by performing encryption, Host Identity Protocol (HIP) protects the routing data by performing anonymity procedures (Nikander, Gurtov & Henderson 2010: 186 – 204). HIP "RFC5201" (Moskowitz, Nikander, Jokela & Henderson 2008) is a protocol operating between the network and transport layers as shown in Figure 37. It adds a cryptographic name space field between these layers, where it separates the locator and identification functions of the current IP addresses. With this deployment, IP addresses are only used as locators in the network layer; this benefits mobility, multi-homing and provides a base for end-to-end security.

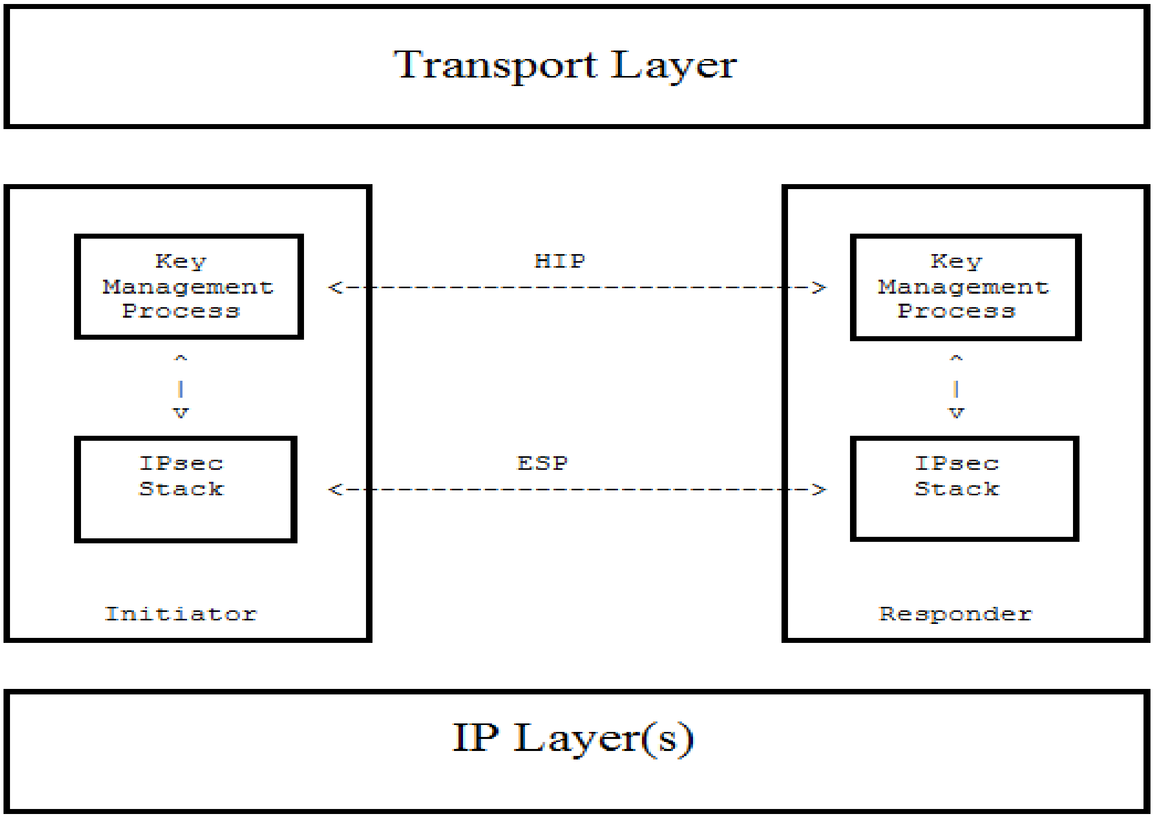


Figure 37: HIP architecture, modified from (Nikander *et al.* 2010: 192) (Nikander, Henderson, Vogt & Arkko 2008: 4).

HIP is compatible with both IP versions; for IPv6, HIP sets a global unique Host Identity Tag (HIT) identifier of 132 bits, while for IPv4 it sets a Local Scope Identity (LSI) of 32 bits. HIP also incorporates the security functions of IPSec, since it employs its ESP protocol for authentication and SAs. In the handshake procedure, communicating peers agree about a set of name spaces, as well as the associated algorithms and keys needed for the process. HIP supports RSA public key cryptosystems and the Digital Signature Algorithm (DSA), with variety of key lengths from 512 up to 2048 bits.

The main feature of HIP is that it does support multi-homing; this allows users to connect to more than one IP address simultaneously. This configuration introduces anonymity and improves the routing privacy since the data can be split over the set of the utilized IP addresses; which also improves the reliability of the connection. To perform these functions, HIP modifies the current routing tables' lookup procedure. HIP separates between the Fully Qualified Domain Name (FQDN) and the IP addresses by inserting the Host ID (HI) field in between. FQDN with this deployment performs a Domain Name System (DNS) lookup to resolve for the HIs, which in turn performs HIP lookup to resolve for the associated IP addresses. These two steps can be combined together upon upgrading to the Secured DNS (DNSSEC), which will store the HIs with their IPs in the same record.

However, aside of HIP strengths, it does not provide a complete solution for routing privacy and location protection. HIP provides anonymity against the remote peers while it does not provide it to the closer ones inside its domain; that is because of the ability to correlate the host keys. Secondly, in the application layer, name spaces can be correlated. Thirdly, in its extension, HIP DNS, it does not support direct communication with anonymous unnamed peers; also it depends on the DNSSEC. Regarding these points, it is clear that HIP provides a means for anonymity and incorporates encrypted host names, but it does not provide a scheme for privacy preserving or location protection.

6. PRIVACY MODEL

Based on the presented literature overview and analysis, we ended up formulating the privacy model shown in Figure 38. This proposed model combines the essential components that are required to preserve privacy in the telecommunication system. It also considers the needs of each party of the system. The model has two perspectives, hypothetical and practical. The hypothetical perspective defines the parameters that should be considered to preserve privacy, while the practical one specifies how to implement these parameters in the system.

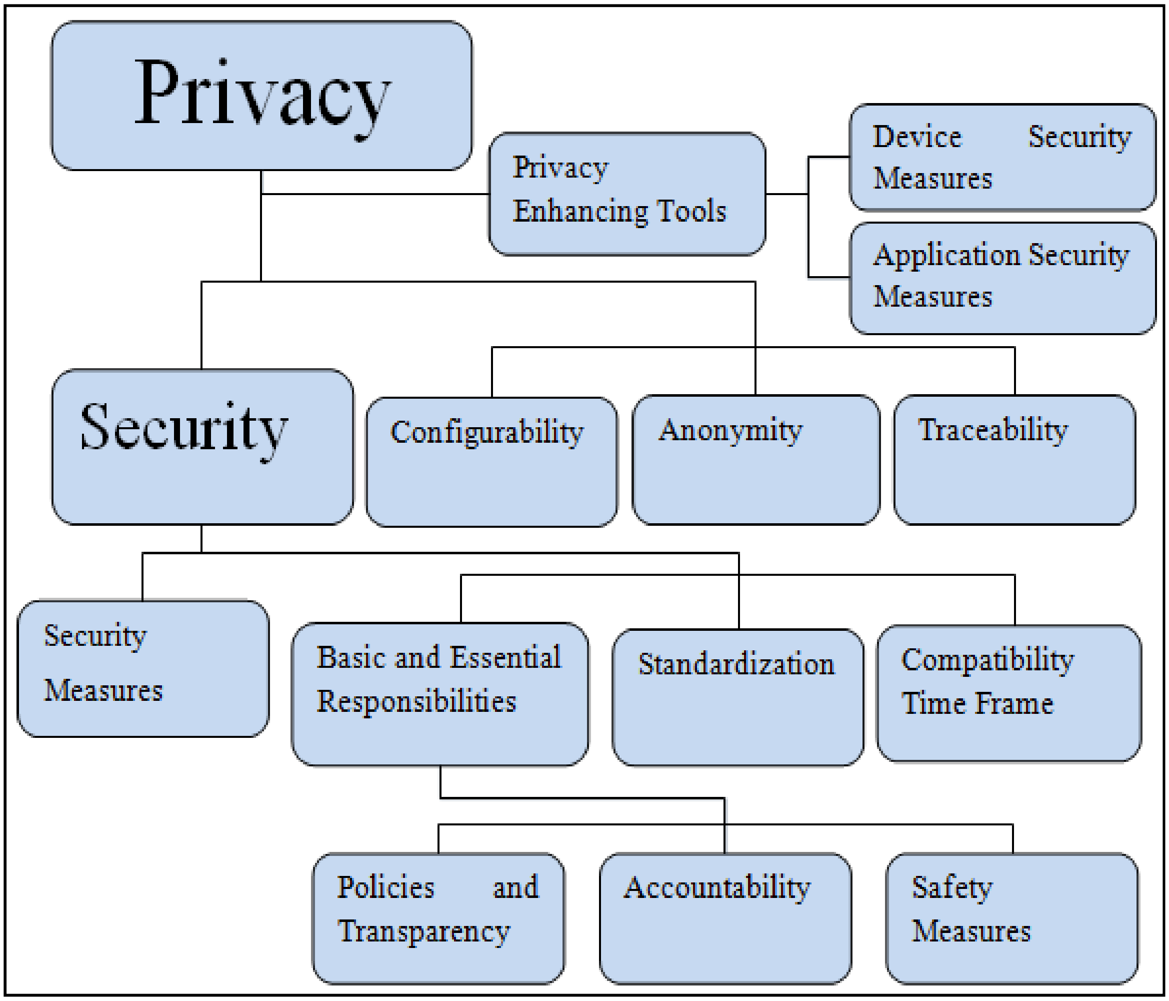


Figure 38: The proposed privacy model.

The proposed model includes the following parameters according to their position and importance in the model's hierarchy:

1. Policies transparency: Clear policies for users, operators and authorities are needed, where well defined procedures and actions are clearly stated. Policies have to clarify the disclosure situations, purposes and responsibilities upon disclosure. Also, changes of the deployed policies need to be acknowledged and agreed upon before coming to application.
2. Accountability: Holding the responsibility for own actions.
3. Safety measures: Operators handle the responsibility for the data and systems safety, thus they can apply the right actions to fully protect them against all sorts of danger.

These three parameters compose the fundamental responsibilities of the communicating parties, where they are essential to build a trusted communication plan.

4. Standardization: Security measures and standards need to be agreed upon. The deployed mechanisms cannot be left optionally implemented as a free choice of operators.
5. Compatibility: Time frame for the legacy systems, applications and protocols upgrade needs to be clearly declared.
6. Security measures: Operators need to consider actions targeting users, systems and data, and by applying the main security measures discussed in chapter 2, they can assure a secure communication. Authorities and governments on the other hand also hold responsibility against the harm that might be caused to or by users, thus considerations need to be taken in the legal form.

The abovementioned parameters form the basic structure to build a trusted secure communication.

7. Configurability: Users need to hold control on their own data; hence systems need to provide users the needed flexibility and options to configure and control the different parameters according to their preferences and the privacy level they seek.
8. Anonymity: Anonymity is needed to protect users and to hide their activities.
9. Traceability: Unlike anonymity, linkage is allowed but only controlled by authorities in its legal form.

Security, Anonymity, and Configurability provide the means to preserve privacy in a system, while traceability provides a means to restrict this privacy in a legal form so that no harm can be caused out of it.

10. Application Security measures: Applications by default are not allowed to gather, store, or exchange data about users without declaration and usage transparency. Also, anonymity needs to be applied upon collecting data.
11. Device Security: Mechanisms to restrict access to devices and their stored data in case of being lost. Also, mechanisms for controlling devices remotely by means of a legal form.

These last two parameters are used to assist and enhance privacy for end users.

From the practical perspective, implementations need to consider the following:

1. Upgrading the non-standard functions and algorithms in the GSM, and its older nodes to the standardized ones.
2. Old networks and the legacy nodes explicitly GSM and SS7, need time frame to be upgraded. Also, hybrid networks compatibility and downgrading to the weaker security standards actions need revising.
3. Access network and key management mechanisms need revising also, since the access network and its associated AKA phase are the weaker in the mobile system.

4. Digital Signatures are needed for data origin authentication and non-repudiation guarantees.
5. Public Keys implementation is needed to provide confidentiality and to protect against eavesdropping. Also, public keys systems provide a facility for lawful interception, thus the PKA needs to be only controlled by authorities.
6. Multi-homing since it provides anonymity, and communication reliability.
7. IPv6 implementation is needed since it affords a means for multi-homing, also some security services and procedures do not function with IPv4.
8. HIP implementation services anonymity, multi-homing, and by implementing it by the authorities officials, it provides a means for lawful traceability.
9. IPSec and TLS/SSL for different connections, since this configuration provides tunneling and application security. For applications employing NAT, IPSec cannot be used, thus a link or more will be protected by only using TLS/SSL.
10. Application Security is needed to protect users from malwares, viruses, and the different attack schemes.
11. Device Security can be implemented by encrypting the device's memory, also by applying a higher deployment, a device can be controlled remotely by its owner under the legal conditions.

7. CONCLUSIONS

The main contribution of this thesis is a proposal of privacy model with certain priorities; this was based on the presented literature and analysis. To achieve that, a detailed study was conducted on the security and users' privacy situation in mobile networks. Different parameters and protocols of security were reviewed to build an overall security evaluation. Additionally, different considerations and arguments of privacy were studied to fully define privacy and its dimensions.

From security and privacy point of view, it is clear that algorithms, standards and security countermeasures need modification. Since systems are susceptible to number of attacks which also leave users vulnerable to valuable data loss. For example, different encryption mechanisms are already broken while still being employed; also short length keys need to be exchanged to more robust longer ones. Additionally, for the purpose of integrity and confidentiality, the randomness of the generated random numbers has to be fully guaranteed so that the applied algorithms can perform their tasks in the right way. Another important issue to consider is the data origin authentication and the repudiation. This can be simply solved by implementing digital signatures by the mobile devices.

The main findings of this thesis regarding security and privacy emphasize possession, standardization, compatibility and configurability. Firstly, possession and data control concepts are of high importance, since losing a device is a common action that might reveal a lot of valuable stored information. Typical solutions for device control include encrypting the data storage, also, some applications enable accessing a lost device remotely once it is connected to the Internet. However, advanced solutions can be afforded to include mutual device-user authentication procedure performed by the serving network, thus in a case of losing a device, it is inaccessible. Also, another solution is by using a remote storage facility like cloud technology instead of local storage.

Secondly, from the GSM experience, non-standardized procedures and functions are a facility to break into a system. Therefore, standardization should be the concept, and all implemented elements should follow a predefined strict standard to not be left as an option in operators' hands. Thirdly, compatibility as well is a very important issue regarding security. Even though the compatibility many advantages, it may also weaken the system's security. In hybrid systems, systems can switch back to the older standards to be compatible with the other older systems and devices. However, this configuration gives a chance for attackers and infected nodes to access these systems by utilizing the weaker security schemes. One must remember that the system's security is as good as the weakest part of its subsystems. Thus, an action needs to be taken against the older weaker systems, to schedule a time for either upgrading them or cutting their support. Finally, configurability is a demand to achieve a controllable privacy scheme by users. It allows users to configure the systems' flexible parameters to fully achieve the privacy level they seek.

At the privacy level, privacy faces many challenges; because of its many dimensions and the less commons between the communication parties. Also, users' absolute privacy is unfeasible in reality because of several reasons including legal and operational drawbacks. Privacy has two main cores; the first concerns policies and regulations while the second concerns trustfulness and credibility. Generally, well defined transparent policies have to be established between governments, operators and users. These policies should specify the rights of all parties, their responsibilities and the legal actions. Also, there is a required level of trustfulness and credibility needs by users, so that they can trust the service and make sure that they receive the adequate privacy level according to the given policies. For this purpose, a trustworthy organization is needed. This organization will hold control on the private data and its access, also it will hold technical duties and control on some parameters that can disclose the privacy of an entity, e.g. private keys, digital signatures and identity traceability. However, the description of this organization differs according to the place and the applied policies and regulations. It can be for example an independent authority organization such as the administrative control authority, the telecommunication regulatory authority, a legal independent authority or in some other cases governments themselves.

In application, privacy can be preserved to an acceptable level by employing mechanisms that hide users' traffic, location, and activities from surveillances. These mechanisms include utilizing end-to-end encryption schemes, e.g. asymmetric encryption to protect the exchanged data, upgrading systems to IPv6 to provide multi-homing, also to assist the other security services, installing HIP servers to provide multi-homing and anonymity, in addition to utilizing NAT boxes for anonymity. It is highly recommended to employ IPSec since it provides end-to-end secure dedicated channel between users, by means of utilizing its modes; transport mode between end devices and tunnel mode between network nodes. Additionally, TLS/SSL can be combined with NAT to provide the needed location protection and traffic anonymity at the application level. Finally, implementing SRTP over TLS in conjunction with SIP over TLS provides the needed protection for the voice services. However, the main challenge here is that these technologies are complex and require high processing power, thus they add costs and loads to the whole system. The right configuration should consider all these factors, to keep the balance between service efficiency, quality, customer satisfaction and costs.

REFERENCES

3GPP (2001a). *Cryptographic Algorithm Requirements (3GPP TS 33.105 version 4.1.0 Release 4)*. Available from World Wide Web: <URL: http://www.etsi.org/deliver/etsi_ts/133100_133199/133105/04.01.00_60/ts_133105v040100p.pdf>.

3GPP (2001b). *Security Architecture (3GPP TS version 33.102 Release 4)*. Available from World Wide Web: <URL: http://www.etsi.org/deliver/etsi_ts/133100_133199/133102/04.01.00_60/ts_133102v040100p.pdf>.

3GPP (2002a). *Network Architecture (3GPP TS 23.002 version 5.6.0 Release 5).* Available from World Wide Web: <URL: http://www.etsi.org/deliver/etsi_ts/123000_123099/123002/05.06.00_60/ts_123002v050600p.pdf>.

3GPP (2002b). *Network Domain Security - MAP (3GPP TS 33.200 version 5.0.0 Release 5).* Available from World Wide Web: <URL: http://www.etsi.org/deliver/etsi_ts/133200_133299/133200/05.00.00_60/ts_133200v050000p.pdf>.

3GPP (2004). *Network Domain Security - MAP (3GPP TS 33.200 version 6.0.0 Release 6).* Available from World Wide Web: <URL: http://www.etsi.org/deliver/etsi_ts/133200_133299/133200/06.00.00_60/ts_133200v060000p.pdf>.

3GPP (2005). *IP Network Layer Security (3GPP TS 33.210 version 7.0.0 Release 7).* Available from World Wide Web: <URL: http://www.etsi.org/deliver/etsi_ts/133200_133299/133210/07.00.00_60/ts_133210v070000p.pdf>.

3GPP (2006). *Network Architecture (3GPP TS 23.002 version 7.1.0 Release 7).* Available from World Wide Web: <URL: http://www.etsi.org/deliver/etsi_ts/123000_123099/123002/07.01.00_60/ts_123002v070100p.pdf>.

3GPP (2007). *Network Domain Security - MAP (3GPP TS 33.200 version 7.0.0 Release 7).* Available from World Wide Web: <URL: http://www.etsi.org/deliver/etsi_ts/133200_133299/133200/07.00.00_60/ts_133200v070000p.pdf>.

3GPP (2010). *Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1∗, f2, f3, f4, f5 and f5∗; Document 1: General (3GPP TS 35.205 version 9.0.0 Release 9).* Available from World Wide Web: <URL: http://www.etsi.org/deliver/etsi_ts/135200_135299/135205/ 09.00.00_60/ts_135205v090000p.pdf>.

Andress, Jason (2011). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Massachusetts: Elsevier.

Ateniese, Giuseppe, Roberto Di Pietro, Luigi V. Mancini & Gene Tsudik (2008). Scalable and efficient provable data possession. In: *Proceedings of the 4th international conference on Security and privacy in communication networks.* ACM, 2008.

Backes, Michael, Ian Goldberg, Aniket Kate & Esfandiar Mohammadi (2012). Provably secure and practical onion routing. In: *2012 IEEE 25th Computer Security Foundations Symposium (CSF).* IEEE, 2012.

BARKAN, Elad, Eli BIHAM & Nathan KELLER (2003). Instant ciphertext-only cryptanalysis of GSM encrypted communication. In: *Advances in Cryptology-CRYPTO 2003*. Springer Berlin Heidelberg, 2003. 600-616.

Baugher, Mark, D. McGrew, M. Naslund, E. Carrara & K. Norrman (2004). *The secure real-time transport protocol (SRTP) (RFC3711)*. Available from World Wide Web: <URL: http://www.hjp.at/doc/rfc/rfc3711.html>.

Beresford, Alastair R. & Frank Stajano (2003). Location privacy in pervasive computing. *Pervasive Computing, IEEE*, 2003, 2.1: 46-55.

Bettini, Claudio, X. Sean Wang & Sushil Jajodia (2005). Protecting privacy against location-based personal identification. In: *Secure Data Management.* Springer Berlin Heidelberg, 2005. 185-199.

Biham, Eli, Orr Dunkelman & Nathan Keller (2005). A related-key rectangle attack on the full KASUMI. In: *Advances in Cryptology-ASIACRYPT 2005*. Springer Berlin Heidelberg, 2005. 443-461.

Biryukov, Alex, Adi Shamir & David Wagner (2001). Real Time Cryptanalysis of A5/1 on a PC. In: *Fast Software Encryption*. Springer Berlin Heidelberg, 2001. 1-18.

Bocan, Valer & Vladimir Cretu (2004). Security and denial of service threats in GSM networks. *PERIODICA POLITECHNICA, Transactions on AUTOMATIC CONTROL and COMPUTER SCIENCE,* 2004, 49.63.

Boman, K., G. Horn, P. Howard & V. Niemi (2002). UMTS security. *Electronics & Communication Engineering Journal*, 2002, 14.5: 191-204.

Bosse, John G. (1998). *Signaling in telecommunication networks*. New York: John Wiley & Sons, Inc.

Boukerche, Azzedine, Khalil El-Khatib, Li Xu & Lary Korba (2004). A novel solution for achieving anonymity in wireless ad hoc networks. In: *Proceedings of the 1st ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks.* ACM, 2004. 30-38.

Boukerche, Azzedine, Khalil El-Khatib, Li Xu & Lary Korba (2004). SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks. In: *Local Computer Networks, 2004. 29th Annual IEEE International Conference on.* IEEE, 2004. 618-624.

Brookson, Charles (1994). GSM (and PCN) Security and Encryption. *GSM Opportunities*.

Callas, J., L. Donnerhacke, H. Finney, D. Shaw & R. Thayer (2007). *OpenPGP message format (RFC4880)*. Available on World Wide Web: <URL: http://www.hjp.at/doc/rfc/rfc4880.html>.

Candolin, Catharina (2005). *Securing military decision making in a network-centric environment*. Available on World Wide Web: <URL: http://lib.tkk.fi/Diss/2005/isbn9512279819/isbn9512279819.pdf>.

Chandra, Mukesh, N. Kumar, R. Gupta, S. Kumar, V.K. Chaurasia & V. Srivastav (2011). Protection from paging and signaling attack in 3G CDMA networks. In: *Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference on.* IEEE, 2011. 406-410.

Chao, Gao (2009). Study on Privacy Protection and Anonymous Communication in Peer-to-Peer Networks. In: *Multimedia Information Networking and Security, 2009. MINES'09. International Conference on.* IEEE, 2009. 522-525.

Chaum, David L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 1981, 24.2: 84-90.

Chikomo, Kelvin, Ming Ki Chong, Alapan Arnab & Andrew Hutchison (2006). Security of mobile banking. *University of Cape Town, South Africa, Tech. Rep.,* Nov, 2006, 1.

Chumchu, Prawit, Attaphon Phayak & Prakaidao Dokpikul (2012). A simple and cheap end-to-end voice encryption framework over GSM-based networks. In: *Computing, Communications and Applications Conference (ComComAp), 2012.* IEEE, 2012. 210-214.

Coffey, Tom & Puneet Saidha (1996). Non-repudiation with Mandatory Proof of Receipt. *ACM computer Communication Review*, 26, 1996. 6-17.

Convery, Sean (2007). Network Authentication, Authorization, and Accounting: Part One. *The Internet Protocol Journal* [online] 10:1 [cited 2 Oct. 2013] Available from Internet: <URL: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-1/101_aaa-part1.html>.

Dierks, Tim & Allen Christopher (1999). *The TLS protocol version 1.0. (RFC2246).* Available from World Wide Web: <URL: https://www.ietf.org/rfc/rfc2246.txt>.

Dohmen, Jon Robert & Lars Olaussen (2001). UMTS Authentication and Key Agreement. *Graduate Thesis, Agder University College—2001*, on line available at http://siving.hia.no/ikt01/ikt6400/jrdohm99.

Dunkelman, Orr, Nathan Keller & Adi Shamir (2010). A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. In: *Advances in Cryptology–CRYPTO 2010*. Springer Berlin Heidelberg, 2010. 393-410.

Egevang, Kjeld & Paul Francis (1994). *The IP Network Address Translator (NAT) (RFC1631)*. Available from Word Wide Web: <URL: http://www.hjp.at/doc/rfc/rfc1631.html>.

Enck, William, Patrick Traynor, Patrick McDaniel & Thomas La Porta (2005). Exploiting open functionality in SMS-capable cellular networks. In: *Proceedings of the 12th ACM conference on Computer and communications security*. ACM, 2005. 393-404.

Ér émy Serror, J., Hui Zang & Jean C. Bolot (2006). Impact of paging channel overloads or attacks on a cellular network. In: *Proceedings of the ACM Workshop on Wireless Security (WiSe),* 2006. 75-84.

Ferguson, Niels & Bruce Schneier (2000). A cryptographic evaluation of IPsec. *Counterpane Internet Security, Inc,* 2000, 3031.

Fischer, Kai (2008). *End-to-End security for DTLS-SRTP*. Available from World Wide Web: <URL: https://tools.ietf.org/html/draft-fischer-sip-e2e-sec-media-00>.

Frankel, Sheila, Karen Kent, Ryan Lewkowski, Angela D. Orebaugh, Ronald W. Ritchey & Steven R. Sharma (2005). Guide to IPsec VPNs. *NIST Special Publication, 2005,* 800-77.

Frankel, Sheila, R. Glenn & S. Kelly (2003). *The AES-CBC Cipher Algorithm and Its Use with IPsec (RFC3602)*. Available from World Wide Web: <URL: http://www.hjp.at/doc/rfc/rfc3602.html>.

Gedik, Bugra & Ling Liu (2008). Protecting location privacy with personalized k-anonymity: Architecture and algorithms. *Mobile Computing, IEEE Transactions on*, 2008, 7.1: 1-18.

Geisler, Eliezer, Paul Prabhaker & Madhavan Nayar (2003). Information integrity: an emerging field and the state of knowledge. In: *Management of Engineering and Technology, 2003. PICMET'03. Technology Management for Reshaping the World. Portland International Conference on*. IEEE, 2003. 217-221.

Goldberg, Ian, David Wagner & Lucky Green (1999). The real-time cryptanalysis of A5/2. *Rump session of Crypto* '99, 1999: 239-255.

Gruteser, Marco & Dirk Grunwald (2003). Anonymous usage of location-based services through spatial and temporal cloaking. In: *Proceedings of the 1st international conference on Mobile systems, applications and services*. ACM, 2003. 31-42.

GSMA Intelligence (2012). *Half of All Mobile Connections Running on 3G/4G Networks by 2017*. [Cited 7 July 2014]. Available from World Wide Web: <URL: https://gsmaintelligence.com/analysis/2012/11/half-of-all-mobile-connections-running-on-3g-4g-networks-by-2017/359/>.

Harkins, Dan & Dave Carrel (1998). *The internet key exchange (IKE) (RFC2409).* Available from World Wide Web: <URL: http://www.hjp.at/doc/rfc/rfc2409.html>.

Heine, Gunnar & Matt Horrer (1999). *GSM networks: protocols, terminology, and implementation*. Norwood, MA: Artech House, Inc.

Hewitt, Milena (2013). *BlackBerry 10 Receives NATO Approval for Restricted Communications.* Available from World Wide Web: <URL: http://press.blackberry.com/press/2013/blackberry-10-receives-nato-approval-for-restricted-communicatio.html>.

Hickman, Kipp & Taher Elgamal (1995). The SSL protocol. *Netscape Communications Corp,* 501. Available from World Wide Web: <URL: http://www.webstart.com/jed/papers/HRM/references/ssl.html>.

Hogg, Michael A. & Dominic Abrams (1988). *Social Identifications: A Social Psychology of Intergroup Relations and Group Processes.* New York: Routledge.

Holub, J. & M. D. Street (2004). Impact of end to end encryption on GSM speech transmission quality-a case study. In: *IET Conference Proceedings, 2004*: 6-6.

Horms aka, Simon Horman (2005). *SSL and TLS*. Available from World Wide Web: <URL: https://lca2009.linux.org.au/conf/2005/security_miniconf/presentations/ssl_ and_ tls .pdf>.

Horn, Günther, Klaus Muellerand & Bart Vinck (1999). Towards a UMTS security architecture. *ITG FACHBERICHT* ,1999: 495-500.

Horniak, Virginia (2004). Privacy Of Communication-Ethics And Technology. *Master Thesis, Mälardalen University, 2004*. Available from World Wide Web: <URL: http://www.idt.mdh.se/utbildning/exjobb/files/TR0390.pdf>.

Housley, Russell (2004). Using advanced encryption standard (AES) counter mode with ipsec encapsulating security payload (ESP) (RFC3686). Available from World Wide Web: <URL: https://tools.ietf.org/html/rfc3686>.

Hunt, Ray (2006). Security in Mobile and Wireless Networks, *University of Canterbury, New Zealand*. Available from World Wide Web: <URL: http://www.apricot.net/apricot2006/slides/tutorial/monday/mobile-security.pdf>.

Hwang, Min-Shiang, Song-Kong Chong & Hsia-Hung Ou (2011). On the security of an enhanced UMTS authentication and key agreement protocol. *European Transactions on Telecommunications*, 2011, 22.3: 99-112.

IEEE (1998). *IEEE standards for local and metropolitan area networks: standard for interoperable LAN/MAN security (SILS) specification; IEEE standard 802.10*. IEEE Standard Press.

ISO (1989). ISO 7498-2, Information processing systems-Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture. *ISO. Geneva, Switzerland.*

ISO (2009). ISO/IEC 13888-1: Information Technology Security Techniques-Non repudiation-Part 1: General. Available from World Wide Web: <URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:13888:-1:ed-3:v1:en>.

Joshi, James (2008). *Network Security: Know It All: Know It All*. Burlington, MA: Morgan Kaufmann.

Kacherginsky, Peter (2009). *TLS and SSL Cipher Suites*. [Cited 02 Nov. 2013]. Available from World Wide Web: <URL: http://www.thesprawl.org/research/tls-and-ssl-cipher-suites/>.

Katugampala, Nilantha, Stephane Villette & A. M. Kondoz (2003). Secure voice over GSM and other low bit rate systems. In: *IET Conference Proceedings,* 2003: 3-3.

Kaviya, K. (2009). Network security implementation by onion routing. In: *Information and Multimedia Technology, 2009. ICIMT'09. International Conference on*. IEEE, 2009: 339-342.

Kelly, Scott & Sheila Frankel (2007). *Using HMAC-SHA-256. HMAC-SHA-384, and HMAC-SHA-512 with IPsec* (*RFC4868)*. Available from World Wide Web: <URL: http://www.ietf.org/rfc/rfc4868.txt>.

Kent, Stephan & Randall Atkinson (1998a). *Security Architecture for the Internet Protocol (RFC2401)*. Available from World Wide Web: <URL: http://www.ietf.org/rfc/rfc2401.txt>.

Kent, Stephen & Randall Atkinson (1998b). *IP authentication header (RFC 2402)*. Available from World Wide Web: <URL: http://www.ietf.org/rfc/rfc2402.txt>.

Kent, Stephen & Randall Atkinson (1998c). *IP encapsulating security payload (RFC2406)*. Available from World Wide Web: <URL: http://www.ietf.org/rfc/rfc2406.txt>.

Kent, Stephen (2005a). *IP authentication header (RFC4302)*. Available from World Wide Web: <URL: http://tools.ietf.org/html/rfc4302.html>.

Kent, Stephen (2005b). *IP encapsulating security payload (ESP) (RFC4303)*. Available from World Wide Web: <URL: http://tools.ietf.org/html/rfc4303.html>.

Krawczyk, Hugo (1996). SKEME: A Versatile Secure Key Exchange Mechanism for Internet. In: *Network and Distributed System Security, 1996. Proceedings of the Symposium on*. IEEE, 1996: 114-127.

Kulkarni, Mandar M., A. S. Bhide & Mr Prafull P. Chaudhari (2013). Encryption Algorithm Addressing GSM Security Issues-A Review. *International Journal of Latest Trends in Engineering and Technology (IJLTET)*, V. 2 Issue 2, March 2013.

Lee, Patrick P. C., Tian Bu & Thomas Woo (2007). On the detection of signaling DoS attacks on 3G wireless networks. In: *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*. IEEE, 2007. 1289-1297.

Lei, Wu & Song Xiao Ting (2009). Information integrity and its protection in networks. In: *2009 5th Asia-Pacific Conference on Environmental Electromagnetics*. 2009. 238-241.

Lin, Herbert S. & Kenneth W. Dam, Ed. (1996). *Cryptography's role in securing the information society*. Washington: National Academies Press.

Madson, Cheryl & N. Doraswamy (1998). *The ESP DES-CBC cipher algorithm with explicit IV (RFC2405)*. Available from World Wide Web: <URL: http://www.hjp.at/doc/rfc/rfc2405.html>.

Madson, Cheryl & R. Glenn (1998). *The use of HMAC-MD5-96 within ESP and AH (RFC2403)*. Available from World Wide Web: <URL: http://www.hjp.at/doc/rfc/ rfc2403.html>.

Madson, Cheryl & R. Glenn (1998). *The use of hmac-sha-1-96 within ESP and AH (RFC2404)*. Available from World Wide Web: <URL: http://www.hjp.at/doc/rfc/ rfc2404.html>.

Mahboob, Athar & Nassar Ikram (2004). Transport Layer Security (TLS)–A Network Security Protocol for E-commerce. *PNEC Research Journal*.

Mao, Wenbo (2003). *Modern Cryptography: Theory and Practice*. Upper Saddle River, New Jersey: Prentice-Hall PTR.

Mason, Richard O. (2000). *A tapestry of privacy, A meta-discussion*.

Maughan, D., M. Schertler, M. Schneider & J. Turner (1998). *Internet Security Association and Key Management Protocol (RFC2408)*. Available from World Wide Web: <URL: http://tools.ietf.org/html/rfc2408>.

McGrew, David & Eric Rescorla (2010). *Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP) (RFC5764)*. Available from World Wide Web: < URL: https://tools.ietf.org/html/rfc5764>.

Meyer, Ulrike & Susanne Wetzel (2004). On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating GSM/UMTS networks. In: *Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004. 15th IEEE International Symposium on.* IEEE, 2004. 2876-2883.

Mobarhan, Mojtaba Ayoubi, Mostafa Ayoubi Mobarhan & Asadollah Shahbahrami (2012). Evaluation of security attacks on UMTS authentication mechanism. *International Journal of Network Security & Its Applications,* 2012, 4.4.

Modarressi, Abdi R. & Ronald A. Skoog (1990). Signaling system no. 7: A tutorial. *Communications Magazine, IEEE*, 1990, 28.7:19-20.

Moor, James H. (1997). Towards a Theory of Privacy I1', in the Information Age. *Computers and Society*, 1997, 27.3: 27-32.

Moskowitz, R., P. Nikander, P. Jokela, Ed. & T. Henderson (2008). *Host Identity Protocol (RFC5201)*. Available from World Wide Web: < URL: https://tools.ietf.org/html/rfc5201>.

Needham, Roger M. (1994). Denial of service: an example. *Communications of the ACM*, 1994, 37.11: 42-46.

Niemi, Valtteri & Kaisa Nyberg (2003). *Front Matter, in UMTS Security*. Chichester: Wiley & Sons, Inc.

Nikander, P., T. Henderson, Ed., C. Vogt & J. Arkko (2008). *End-host mobility and multihoming with the host identity protocol.* Available from World Wide Web: < URL: http://www.hjp.at/doc/rfc/rfc5206.html>.

Nikander, Pekka, Andrei Gurtov & Thomas R. Henderson (2010). Host identity protocol (HIP): Connectivity, mobility, multi-homing, security, and privacy over IPv4 and IPv6 networks. *Communications Surveys & Tutorials, IEEE*, 2010, 12.2: 186-204.

Noam, Eli M. (1995). Privacy in Telecommunications: Markets, Rights, and Regulations. Part I. *New Telecom Quarterly*, 3.2: 52-59.

Orman, Hilarie (1998). *The OAKLEY key determination protocol (RFC2412)*. Available from World Wide Web: <URL: https://tools.ietf.org/html/rfc2412>.

Oxford Dictionaries. *Security*. [Cited 30 July 2013]. Available from World Wide Web: <URL: http://www.oxforddictionaries.com/definition/english/security>.

Parker, Donn B. (1998). *Fighting computer crime: A new framework for protecting information.* New York: John Wiley & Sons, Inc.

Pereira, Roy & Rob Adams (1998). *The ESP CBC-Mode Cipher Algorithms (RFC2451).* Available from World Wide Web: <URL: http://www.hjp.at/doc/rfc/rfc2451.html>.

Pesonen, Lauri (1999). *GSM interception*. Available from World Wide Web: <URL:http://www.tml.tkk.fi/Opinnot/Tik-110.501/1999/papers/gsminterception/netsec.html >.

Pfitzmann, Andreas & Marit Hansen (2005). *Anonymity, unlinkability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology.* Available from World Wide Web: <URL: *http://dud.inf.tu-dresden.de/literatur/ Anon_Terminology_v0.28.pdf*>.

Pütz, Stefan, Roland Schmitz & Tobias Martin (2001). Security mechanisms in UMTS. *Datenschutz und Datensicherheit*, 2001, 25.6.

Qi, H. F., X. H. Yang, R. Jiang, B. Liang & S. J. Zhou (2008). Novel End-to-End Voice Encryption Method in GSM System. In: *Networking, Sensing and Control, 2008. ICNSC 2008. IEEE International Conference on.* IEEE, 2008. 217-220.

Quirke, Jeremy (2004). Security in the GSM system. *AusMobile*, May, 2004.

Rahnema, Moe (1993). Overview of the GSM system and protocol architecture. *Communications Magazine, IEEE*, 1993, 31.4: 92-100.

Rao, J. R., P. Rohatgi, H. Scherzer & S. Tinguely (2002). Partitioning attacks: or how to rapidly clone some GSM cards. In: *Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on.* IEEE, 2002. 31-41.

Rechert, Klaus, K. Meier, R. Zahoransk, D. Wehrle, D. von Suchodoletz, B. Greschbach, S. Wohlgemuth & I. Echizen (2013). Reclaiming location privacy in mobile telephony networks—effects and consequences for providers and subscribers. *Systems Journal, IEEE*, 2013, 7.2: 211-222.

Rescorla, Eric & Nagendra Modadugu (2012). *Datagram Transport Layer Security Version 1.2 (RFC6347).* Available from World Wide Web: <URL: https://tools.ietf.org/html/ rfc6347>.

Ricciato, Fabio, Angelo Coluccia & Alessandro D'Alconzo (2010). A review of DoS attack models for 3G cellular networks from a system-design perspective. *Computer Communications*, 2010, 33.5:551-558.

Saltzer, Jerome H. & Michael D. Schroeder (1975). The protection of information in computer systems. *Proceedings of the IEEE*, 1975, 63.9: 1278-1308.

Schiller, Jochen & Agnès Voisard, Ed. (2004). *Location-based services*. San Francisco: Elsevier.

Schulzrinne, H., S. Casner, R. Fredrick & V. Jacobson (2003). *RTP: A Transport Protocol for Real-Time Applications (RFC3550*). Available from World Wide Web: <URL: http://tools.ietf.org/html/rfc3550.html>.

Scourias, John (1995). Overview of the global system for mobile communications. *University of Waterloo*, 1995, 4.

Seys, Stefaan & Bart Preneel (2009). ARM: Anonymous routing protocol for mobile ad hoc networks. *International Journal of Wireless and Mobile Computing*, 2009, 3.3: 145-155.

Smith, Richard E. (1997). *Internet cryptography*. MA: Addison-Wesley.

Snekkenes, Einar (2001). Concepts for personal location privacy policies. In: *Proceedings of the 3rd ACM conference on Electronic Commerce.* ACM, 2001. 48-57.

Spatscheck, Oliver & Larry L. Peterson (1999). Defending against denial of service attacks in Scout. In: *OSDI*. 1999. 59-72.

Spinello, Richard (2006). *Cyberethics: Morality and law in cyberspace*. Massachusetts: Jones & Bartlett Learning.

Srisuresh, Pyda & Matt Holdrege (1999). *IP network address translator (NAT) terminology and considerations (RFC2663).* Available from World Wide Web: <URL: https://tools.ietf.org/html/rfc2663>.

Stallings, William (2011). *Cryptography and Network Security, Principles and Practice*. 5/E. New York: Pearson Education, Inc.

Stamp, Mark (2006). *Information Security Principles And Practice*. Hoboken, New Jersey: John Wiley & Sons.

Straub, Detmar W., Seymour E. Goodman & Richard Baskerville (2008). *Information security: policy, processes, and practices*. New York: M.E. Sharpe.

Syverson, Paul (2003). Onion routing for resistance to traffic analysis. In: *DARPA Information Survivability Conference and Exposition, 2003. Proceedings.* IEEE, 2003. 108-110.

Tanenbaum, Andrew S. & Maarten Van Steen (2007). *Distributed systems principles and paradigms*. Ed 2. New Jersey: Prentice Hall.

Tang, Chunyu, David A. Naumann & Susanne Wetzel (2007). Analysis of authentication and key establishment in inter-generational mobile telephony. *IACR Cryptology ePrint Archive 2013*, 2013: 227.

Thomas, Stephen (2000). *SSL and TLS essentials*. New York: John Wiley & Sons, Inc.

Vedder, Klaus (1998). *GSM: Security, services, and the SIM. State of the art in Applied Cryptography*. Springer Berlin Heidelberg.

Wagner, David, Ian Goldberg & Marc Briceno (1998). GSM cloning. *Web page about COMP-128 version 1*. Available from World Wide Web: <URL: http://www.isaac.cs.berkeley.edu/isaac/gsm.html>.

Walke, Bernhard H., Peter Seidenberg & Marc Peter Althoff (2003). *UMTS: the fundamentals*. Chichester: John Wiley & Sons.

Walker M. & T. Wright. Security. In F. Hillebrand, Ed. (2002). *GSM and UMTS: The Creation of Global Mobile Communication*. Chapter 15. Chichester: John Wiley & Sons.

Wang Jian, Nan Jiang, Hui Li, Xinxin Niu & Yixian Yang (2009). Novel key management for 3G end-to-end encryption. In: *Global Mobile Congress 2009*. IEEE, 2009. 1-7.

Whitman, Michael E. & Herbert J. Mattord (2010). *Principles of information security*. Boston: Cengage Learning.

Wisely D., P. Eardley & L. Burness (2002). *IP for 3G—Networking Technologies for Mobile Communications*. New York: John Wiley & Sons.

Zuberi, Rubina Shahin, Brejesh Lall & Syed Naseem Ahmad (2012). Privacy Protection Through k-anonymity in Location-based Services. *IETE Technical Review (Medknow Publications & Media Pvt. Ltd.),* 2012, 29.3.