Vulnerabilities and Possible Attacks against the GPRS Backbone Network

Christos Xenakis, Lazaros Merakos

Security Group, Communication Networks Laboratory
Department of Informatics & Telecommunications, University of Athens
15784 Athens, Greece.
{xenakis, merakos}@di.uoa.gr
http://www.cnl.di.uoa.gr/

Abstract. This paper presents the security weaknesses and the possible attacks, which threaten the GPRS backbone network and the data that either reside at the network or are transferred through it. These attacks may be performed by malicious third parties, mobile users, network operators or network operator personnel, which exploit the weaknesses of the employed technology and the security measures applied to the GPRS backbone. The possible attacks against the GPRS backbone may result in the compromise of end-users security, the users over billing, the disclosure or alteration of critical information, the services unavailability, the network breakdown, etc. The analyzed attacks and their consequences increase the risks associated with the usage of GPRS, and, thus, influence its deployment that realizes the concept of the mobile Internet.

1 Introduction

The General Packet Radio Services (GPRS) [1] is a service that provides packet radio access for Global System for Mobile Communications (GSM) users. The GPRS network architecture, which constitutes a migration step toward third-generation (3G) communication systems, consists of an overlay network onto the GSM network. In the wireless part, the GPRS technology reserves radio resources only when there is data to be sent, thus, ensuring the optimized utilization of radio resources. The fixed part of the network employs the IP technology and is connected to the public Internet. Taking advantage of these features, GPRS enables the provision of a variety of packet-oriented multimedia applications and services to mobile users, realizing the concept of the mobile Internet.

For the successful implementation of the new emerging applications and services over GPRS, security is considered as a vital factor. In order to meet security objectives, GPRS uses a specific security architecture, which aims at protecting the network against unauthorized access and the privacy of users. This architecture is based on the security measures applied in GSM, since the GPRS system is built on the GSM infrastructure. However, GPRS is more exposed to intruders compared to GSM [2][3] because it uses the IP technology, which presents known vulnerabilities. Similarly to

IP networks, intruders to the GPRS system may attempt to breach the confidentiality, integrity, availability or otherwise attempt to abuse the system in order to compromise services, defraud users or any part of it.

This paper presents the security weaknesses and the possible attacks, which threaten the GPRS backbone network and the data that either reside at the network or are transferred through it. These attacks may be performed by malicious third parties, mobile users, network operators or network operator personnel, which exploit the weaknesses of the employed technology and the security measures applied to the GPRS backbone. The possible attacks against the GPRS backbone may result in the compromise of end-users security, the users over billing, the disclosure or alteration of critical information, the services unavailability, the network breakdown, etc. The analyzed attacks and their consequences increase the risks associated with the usage of GPRS, and, thus, influence its deployment that realizes the concept of the mobile Internet.

The rest of this article is organized as follows. Section 2 briefly describes the GPRS technology and the security measures applied to the GPRS backbone network. Section 3 presents the weaknesses of the security measures applied to the GPRS backbone. Section 4 analyzes the possible attacks that threaten the GPRS backbone and the data that either reside at the network or are transferred through it. Finally, section 5 contains the conclusions.

2 GPRS Technology

2.1 Network Architecture

The network architecture of GPRS [1] is presented in Fig.1. A GPRS user owns a Mobile Station (MS) that provides access to the wireless network. From the network side, the Base Station Subsystem (BSS) is a network part that is responsible for the control of the radio path. BSS consists of two types of nodes: the Base Station Controller (BSC) and the Base Transceiver Station (BTS). BTS is responsible for the radio coverage of a given geographical area, while BSC maintains radio connections towards MSs and terrestrial connections towards the fixed part of the network (core network).

The GPRS Core Network (CN) uses the network elements of GSM such as the Home Location Register (HLR), the Visitor Location Register (VLR), the Authentication Centre (AuC) and the Equipment Identity Register (EIR). HLR is a database used for the management of permanent data of mobile users. VLR is a database of the service area visited by an MS and contains all the related information required for the MS service handling. AuC maintains security information related to subscribers' identity, while EIR maintains information related to mobile equipments identity. Finally, the Mobile Service Switching Centre (MSC) is a network element responsible for circuit-switched services (e.g., voice call) [1].

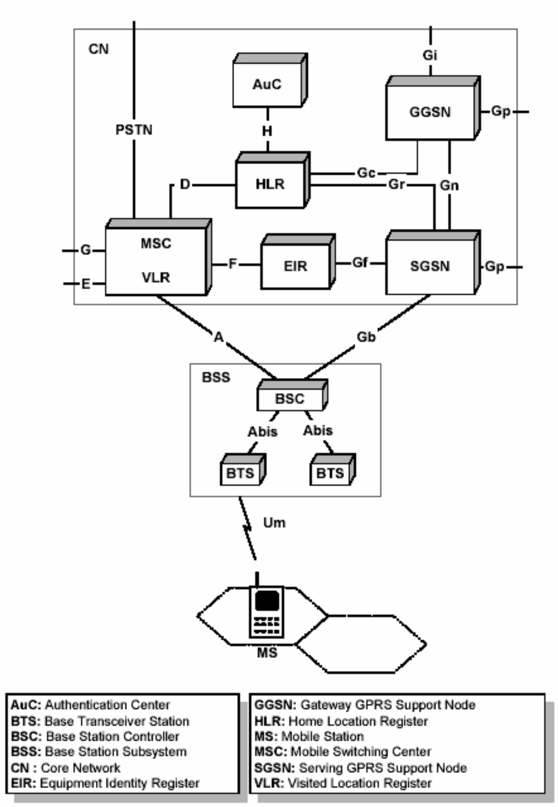
CN
PSTN
AuC
H
HLR
D
Gc
Gr
Gi
GGSN
Gp
Gn
MSC
VLR
G
E
F
EIR
Gf
SGSN
Gp
A
Gb
BSS
BSC
Abis
Abis
BTS
BTS
Um
MS
AuC: Authentication Center
BTS: Base Transceiver Station
BSC: Base Station Controller
BSS: Base Station Subsystem
CN : Core Network
EIR: Equipment Identity Register
GGSN: Gateway GPRS Support Node
HLR: Home Location Register
MS: Mobile Station
MSC: Mobile Switching Center
SGSN: Serving GPRS Support Node
VLR: Visited Location Register

Fig. 1. GPRS network architecture.

As presented previously, GPRS reuses the majority of the GSM network infrastructure. However, in order to build a packet-oriented mobile network some new network elements (nodes) are required, which handle packet-based traffic. The new class of nodes, called GPRS support nodes (GSN), is responsible for the delivery and routing of data packets between a MS and an external packet data network (PDN). More specifically, a Serving GSN (SGSN) is responsible for the delivery of data packets from, and to, a MS within its service area. Its tasks include packet routing and transfer, mobility management, logical link management, and authentication and charging functions. A Gateway GSN (GGSN) acts as an interface between the GPRS backbone and an external PDN. It converts the GPRS packets coming from the SGSN into the appropriate packet data protocol (PDP) format (e.g., IP), and forwards them to the corresponding PDN. Similar is the functionality of GGSN in the opposite direction.

Signaling exchange in the GPRS backbone is mainly based on the Signaling System 7 (SS7) technology [5], which does not support any security measure for the GPRS deployment. Similarly, the GPRS Tunneling Protocol (GTP) [4] that is employed for communication between GSNs does not support security. Thus, user data and signaling information in the GPRS backbone network are conveyed in clear-text exposing them to various security threats. In addition, inter-network communications (between different operators) are based on the public Internet, which enables IP spoofing to any malicious third party who gets access to it. In the sequel, the security measures applied to the GPRS backbone network are presented.

2.2 Security measures for the GPRS backbone

The responsibility for security protection of the GPRS backbone as well as inter-network communications belongs to mobile operators. An operator utilizes private IP addressing and Network Address Translation (NAT) [6] to restrict unauthorized access to the GPRS backbone. He may also apply firewalls at the borders of the GPRS backbone network in order to protect it from unauthorized penetrations. Firewalls protect the network by enforcing security policies (e.g., user traffic addressed to a network element is discard). Using security policies the GPRS operator may ensure that only traffic initiated from the MS and not from the Internet should pass through a firewall. This is done for two reasons: (a) to restrict traffic in order to protect the MS and the network elements from external attacks; and (b) to protect the MS from receiving un-requested traffic. Un-requested traffic may be unwanted for mobile subscribers since they pay for the traffic received as well. The GPRS operator may also want to disallow some bandwidth demanding protocols preventing a group of subscribers to consume so much bandwidth that other subscribers are noticeably affected. In addition, application level firewalls prevent direct access through the use of proxies for services, which analyze application commands, perform authentication and keep logs.

Since firewalls do not provide privacy and confidentiality, the Virtual Private Network (VPN) technology [7] has to complement them to protect data in transit. A VPN is used for the authentication and the authorization of user access to corporate resources, the establishment of secure tunnels between the communicating parties, and the encapsulation and protection of the data transmitted by the network. In the majority of GPRS implementations, pre-configured, static VPNs can be employed to protect data transfer between GPRS network elements (e.g., an SGSN and a GGSN that belong to the same backbone), between different GPRS backbone networks that belong to different mobile operators, or between a GPRS backbone and a remote corporate private network. The border gateway, which resides at the border of the GPRS backbone, is a network element that provides firewall capabilities and also maintains static, pre-configured VPNs to specific peers.

3 Security weaknesses of the GPRS backbone

Although GPRS have been designed with security in mind, it presents some essential security weaknesses, which may lead to the realization of security attacks that threaten network operation and data transfer through it. In the following, the security weaknesses of GPRS that are related to the GPRS backbone network for both signaling and data plane are presented and analyzed.

3.1 Signaling plane

As mentioned previously, the SS7 technology, used for signaling exchange in GPRS, does not support security protection. Specifically, it does not support any security measure that provides node and message authentication, data confidentiality and message integrity. Until recently, this was not perceived to be a problem, since SS7 networks belonged to a small number of large institutions (telecom operator). However, the rapid deployment of mobile systems and the liberalization of the telecommunication market have dramatically increased the number of operators (for both fixed and mobile networks) that are interconnected through the SS7 technology. This fact provokes a significant threat to the GPRS network security, since it increases the probability of an adversary to get access to the network or a legitimate operator to act maliciously.

The lack of security measures in the SS7 technology, used in GPRS, results also in the unprotected exchange of signaling messages between a VLR and a VLR/HLR, or a VLR and other fixed network nodes. Although these messages may include critical information for the mobile subscribers and the networks operation like ciphering keys, authentication data (e.g., authentication triplets), user subscription data (e.g., International Mobile Subscriber Identity - IMSI), user billing data, network billing data, etc., they are conveyed in a clear-text within the serving network, as well as between the home network and the serving network. For example, the VLR of a serving network may use the IMSI to request authentication data for a single user from its home network, and the latter forwards them to the requesting VLR without any security measure. Thus, the exchanges of signalling messages, which are based on SS7, may disclose sensitive data of mobile subscribers and networks, since they are conveyed over insecure network connections without security precautions.

3.2 Data plane

Similarly to the signaling plane, the data plane of the GPRS backbone presents significant security weaknesses, since the introduction of IP technology in the GPRS core shifts towards open and easily accessible network architectures (i.e., lack of authentication, confidentiality and integrity security measures). More specifically, the data encryption mechanism employed in GPRS does not extend far enough towards the core network, resulting also in a clear-text transmission of user data in it. Thus, a malicious, which gets access to the network, may either obtain access to sensitive data traffic or provide unauthorized/incorrect information to mobile users and network components. As presented previously, the security protection of users data in the fixed segment of the GPRS network mainly relies on two independent and complementary technologies, which are not undertaken by GPRS, but from the network operators. These technologies include firewalls that enforce security policies to the

GPRS backbone network that belongs to an operator, and pre-configured VPNs that protect specific network connections.

However, firewalls were originally conceived to address security issues for fixed networks, and, thus, are not seamlessly applicable in mobile networks. They attempt to protect the clear-text transmitted data in the GPRS backbone from external attacks, but they are inadequate against attacks that originate from malicious mobile subscribers, as well as from network operator personnel or any other third party that gets access to the GPRS core network. Another vital issue regarding the deployment of firewalls in GPRS has to do with the consequences of mobility. The mobility of a user may imply roaming between networks and operators, which possibly results in the changing of the user address. This fact in conjunction with the static configuration of firewalls may potentially lead to discontinuity of service connectivity for the mobile user. Moreover, in some cases the security value of firewalls is considered limited as they allow direct connection to ports without distinguishing services.

Similarly to firewalls, the VPN technology, in many cases, fails to provide the necessary flexibility required by typical mobile users. Currently, VPNs for a significant number of GPRS subscribers are established in a static manner between the border gateway of a GPRS network and a remote security gateway of a corporate private network. This fact allows the realization of VPNs only between a security gateway of a large organization and a mobile operator, when a considerable amount of traffic requires protection. Thus, this scheme can provide VPN services neither to individual mobile users that may require on demand VPN establishment, nor to enterprise users that may roam internationally. In addition, static VPNs have to be reconfigured every time the VPN topology or VPN parameters change.

4 Attacks on the GPRS backbone network

Based on the previous analysis, it can be perceived that the GPRS technology presents some essential security weaknesses. This fact may lead to the realization of attacks that threaten the GPRS network and the data that either reside at the network or are transferred through it. In the following, the possible attacks that target the backbone network of a GPRS operator (see Fig. 2), the interface between network operators (Gp interface) and the interface to the public Interne (Gi interface) are presented and analyzed.

4.1 Attacks on the backbone of a GPRS operator

The backbone network of a GPRS operator, which connects the fixed nodes of the GPRS architecture, is threatened by malicious actions. These actions refer to both IP and SS7 technologies that are employed to convey user data and signaling information in this part of the network. In the following, the security attacks against the backbone network of a GPRS operator, classified by the transmission technology used (IP and SS7), are presented and analyzed.

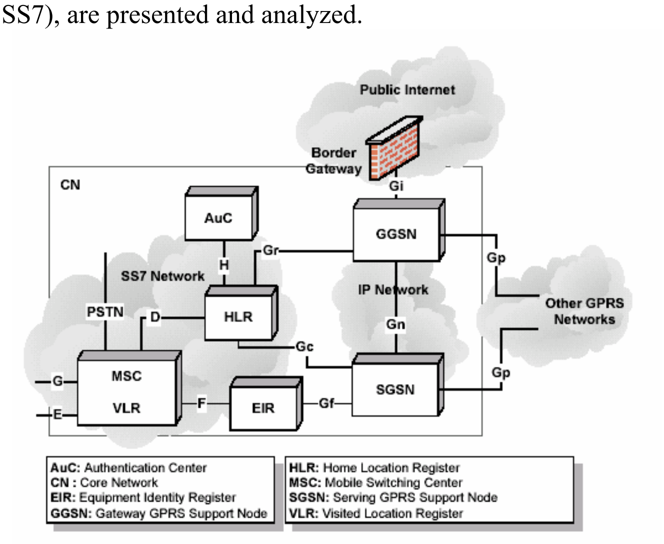
Public Internet
Border Gateway
Gi
CN
AuC
GGSN
Gr
H
SS7 Network
Gp
IP Network
Other GPRS Networks
PSTN
D
HLR
Gn
Gc
Gp
G
MSC
VLR
SGSN
E
F
EIR
Gf
AuC: Authentication Center
CN : Core Network
EIR: Equipment Identity Register
GGSN: Gateway GPRS Support Node
HLR: Home Location Register
MSC: Mobile Switching Center
SGSN: Serving GPRS Support Node
VLR: Visited Location Register

Fig. 2. GPRS backbone network.

4.1.1 Attacks on the IP technology (Gn Interface)

The IP technology is used to connect the SGSN and the GGSN of the same network operator (Gn interface) (see Fig.2). This connection may be built on the top of an already existing IP network, which is not dedicated to the GPRS traffic. Therefore, traffic that originates from outside of the GPRS network shares the GPRS backbone links with the GPRS traffic. The latter is conveyed in clear-text in the GPRS backbone since the GTP protocol, which is employed for both signaling and user data, does not support any security measure. The above situation might cause performance problems to the GPRS backbone (i.e., network overload) and expose the GPRS traffic to security threats (e.g., denial of service attacks, IP spoofing, compromise of confidentiality and privacy etc.) that the public Internet encounters. Therefore, the Gn Interface is vulnerable to attacks that can potentially lead to network downtime, loss of service, revenue loss and disgruntle customers. In the following, the most prominent security attacks that may be carried out against this part of the GPRS backbone network are presented.

Since the IP network that is used as a basis for the GPRS backbone is not dedicated to it, a malicious third party may masquerade as a legitimate part of the GPRS network by spoofing the address of a GPRS network component (e.g., GGSN or SGSN). Once the malicious party establishes himself as a legitimate network element, he is able to perform various actions that are detrimental to the mobile subscribers and the network operator. By executing commands that normally a legitimate network component does, the attack remains undetected until its results are noticeable. One of these attacks is related to the GTP protocol, and more specifically to the exploitation of the GTP commands like PDP context create, PDP context delete, PDP context update, etc. [4]. The attacker, who has access to the GPRS backbone network, is able to get information regarding the GTP tunneling by simply monitoring the GTP traffic, which is unencrypted. Without encryption, data carried by the GTP protocol can either be read or manipulated. Possessing the appropriate information, the attacker may create and forward to the GGSN of the network PDP context create, delete and update commands. These commands overload the GGSN under attack and change the servicing contexts of the mobile users that are currently served by the network, resulting in denial of service.

In addition to malicious third parties that get access to the GPRS backbone network, the mobile users (legitimate or not) may represent a threat to it. Since the MSs are behind the firewall, which is located between the GGSN and the public Internet, they may get access to the network elements of the GPRS backbone (i.e., SGSN, GGSN, DNS servers, O&M workstations, etc.). Having access to these elements, a malicious MS may perform various attacks such as denial of service, IP spoofing, compromise of confidentiality and privacy, etc. In addition, once the malicious MS gets access to the GPRS network, it may send massive amounts of data to unsuspecting users. Since the GPRS is a usage-based service, the mobile users under attack are over billed for content that they did not request for. Such an attack would be even more harmful than spam is for email, as it becomes much more than an annoyance.

Finally, a malicious MS in cooperation with a malicious server, which is located outside of the GPRS network, may also perform an over billing attack to a legitimate mobile subscriber. The malicious MS may hijack the IP address of the legitimate MS, and invokes a download from the malicious server. Once the downloading begins, the malicious MS exits the session. The legitimate MS (MS under attack) receives and gets charged for traffic that never requests for. The malicious parties could also execute this attack by sending broadcasts of unsolicited data to legitimate mobile subscribers. The result is still the same: the subscribers are billed for data that they did not solicited and might not have wanted.

4.1.2 Attacks on the SS7 technology

If an attacker gets access to the GPRS backbone, he may also gain access to the signaling part of the network, and consequently to the network components that are connected through it, such as the AuC, the HLR, the VLR, etc. Having access to the signaling part of the network, the attacker is able to listen to critical information for the mobile subscribers and the network operation such as the permanent identities of mobile users (IMSI), temporary identities (Temporary Mobile Subscriber Identity – TMSI, and Temporary Logical Link Identity - TLLI), location information, authentication triplets, charging and billing data, etc [1]. This is feasible because the signaling network (SS7), used in GPRS, does not support security measures. Except for listening to the critical information exchanged, the attacker may either perform denial of service attacks to the GPRS signaling components or try to retrieve the sensitive information that they hold. For example, the AuC contains authentication information of the subscribed home users. A similar attack to that performed to retrieve the unique subscriber key, Ki, from a SIM-card can also be carried out to retrieve the Ki from the AuC. The AuC has to answer to a request made by a GPRS network component and returns valid authentication triples to be used in the authentication procedure of the involved MS. Thus, exploiting the absence of authentication and integrity protection mechanisms in SS7, a malicious party may masquerade as a network element and retrieve critical information that should be kept confidential.

4.2 Attacks on the interface between network operators (Gp Interface)

The Gp Interface (see Fig. 2), which provides connectivity between GPRS networks that belong to different operators, is also vulnerable to malicious actions. This interface supports users roaming and conveys: (a) GTP traffic between a local network and the home network of a roaming user; (b) roaming information between a GPRS network and a GPRS Routing Exchange (GRX) operator, which provides roaming services to cooperating networks; and (c) Domain Name Server (DNS) information. The security threats to the Gp interface mainly concern with the availability of resources and services, the authentication and authorization of users and actions, and the integrity and confidentiality of the data transferred. A vital security issue of the Gp interface is the lack of security measures in the GTP protocol. In the following, the most important security attacks that target the Gp interface are presented and analyzed.

Trust and reliability between the cooperating GPRS network operators influence the level of security that each operator supports. A malicious operator has the ability to generate a sufficient amount of traffic (either IP or GTP) directed at the border gateway, the SGSN or the GGSN of an operator under attack. In this way, the GPRS nodes are flooded with useless and unwanted traffic that consumes the majority of processing and communication resources. This may result in preventing subscribers from being able to roam, to be attached to the GPRS network, to forward data to external networks (i.e., Internet), etc. In addition, the attacker (the malicious operator) might perform attacks that target the GTP protocol, such as deleting or updating PDP contexts. These actions remove or modify the GTP tunnels between the SGSN and the GGSN (of an operator under attack) that are used for user data transfer, and, thus, denying users service.

Since the GTP protocol provides no authentication for SGSNs and GGSNs, a malicious operator or an attacker with access to the Gp Interface may create a bogus SGSN. Using information regarding users subscription, which can be captured from the GTP traffic (GTP messages are conveyed unencrypted), the bogus SGSN may create GTP tunnels between itself and a legitimate GGSN. After the establishment of such tunnels, the network, where the legitimate GGSN belongs to, provides unauthorized Internet access to the attacker and, possibly, access to cooperating networks. In addition, the bogus SGSN may send Update PDP context request messages [1] to a legitimate SGSN, which is handling the GTP sessions of a mobile subscriber. In this way, the bogus SGSN takes the responsibility for handling the GTP sessions of the user. Thus, the attacker may intercept the user data exchanged by the sessions, compromising end-user security.

4.3 Attacks on the interface to the public Internet (Gi Interface)

The network of a GPRS operator is not only threatened by attacks that originate from inside of it and the networks of cooperating operators, but also from outside of them. The Gi interface (see Fig. 2) connects the GPRS network to the public Internet and service providers that provide services to mobile subscribers. Since the applications of mobile subscribers can be whatever is carried by the Internet technology, the Gi interface may carry any type of traffic. This fact exposes the GPRS network elements and the mobile subscribers to a variety of threats that the public Internet encounters, such as viruses, worms, Trojan horses, denial of service attacks, and other malicious network traffic.

Similarly to the Gp interface, denial of service attacks represent the largest threat to the Gi interface. Attackers may be able to flood the links that connect the GPRS network to external packet data networks with useless traffic, thereby, prohibiting legitimate traffic to pass. The flood traffic might target to the MSs or the network elements causing availability problems to the followed network paths and the involved components.

Apart from harm to the network availability, the GPRS data are conveyed unprotected over the public Internet enabling anyone to read and/or manipulate them, and, thus, compromising user data confidentiality and integrity. In addition, an adversary may exploit the unprotected user related information causing huge bills to the GPRS users. This is feasible because the GPRS billing system is based on the amount of traffic transmitted and received. The over billing attack can be achieved by sending large emails from a malicious external network to the MSs, or by creating viruses that are transferred to the MSs. A virus may have the property to send dummy packets from the infected MS to a malicious server, without any notice to the user.

5 Conclusions

This paper has presented the security weaknesses and the possible attacks, which threaten the backbone network of a GPRS operator and the data that either reside at the network or are transferred through it. The identified weaknesses can be exploited by malicious third parties, mobile users, network operators or network operator personnel, which target both IP and SS7 technologies that are employed to convey user data and signaling information in the GPRS backbone network. The results of possible attacks might be the monitoring of MS usage, the downloading of unwanted files, the realization of unwanted session calls, the availability of resources and services, the authentication and authorization of users and actions, and the integrity and confidentiality of the data transferred. The analyzed attacks and their consequences increase the risks associated with the usage of GPRS, and, thus, influence its deployment that realizes the concept of the mobile Internet. In order to defeat these risks and the inabilities of the GPRS technology, research activities on the identified security issues should be triggered and specific security measures should be designed and applied.

Acknowledgement

This paper is part of the 03ED910 research project, implemented within the framework of the "Reinforcement Programme of Human Research Manpower" (PENED) and co-financed by National and Community Funds (75% from E.U.-European Social Fund and 25% from the Greek Ministry of Development-General Secretariat of Research and Technology).

References

[1] 3GPP TS 03.6 (V7.9.0), "GPRS Service Description, Stage 2", Sept. 2002.
[2] P. Pagliusi, "A Contemporary Foreword on GSM Security", Proc. Infrastructure Security International Conference (InfraSec 2002), LNCS 2437, Springer-Verlag, 2002, pp 129-144.
[3] C. Mitchell, "The security of the GSM air Interface protocol", Technical Report, Royal Holloway University of London, Aug. 2001, http://www.ma.rhul.ac.uk/techreports/
[4] 3GPP TS 09.60 (V7.10.0), "GPRS Tunneling Protocol (GTP) across the Gn and Gp Interface", Dec. 2002.
[5] 3GPP TS 09.02 (v7.15.0) "Mobile Application Part (MAP) specification", March 2004.
[6] P. Srisuresh, M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, Aug. 1999.
[7] B. Gleeson, A. Lin, J. Heinanen, G. Armitage, A. Malis, "A Framework for IP Based Virtual Private Networks", RFC 2764, Feb. 2000.
[8] C. Xenakis and L. Merakos, "Security in third Generation Mobile Networks", Computer Communications, Vol. 27, No. 7, May 2004, pp. 638-650.