**İÇİNDEKİLER**

Sayfa

## KISALTMA LİSTESİ

| | |
|---|---|
| 1G | First Generation – Birinci nesil |
| 2G | Second Generation - İkinci nesil |
| 3DES | 3 x Data Encryption Standard – Üç katlı veri şifreleme standardı (168bit) |
| 3G | Third Generation - Üçüncü nesil |
| 3GPP | Third Generation Partnership Project - Üçüncü nesil ortaklık projesi |
| 8PSK | 8 Phase-Shifted Keying - 8 faz kaymalı anahtarlama |
| AES | Advanced Encryption Standard - Gelişmiş şifreleme standardı |
| AH | Authentication Header - Doğrulama başlığı |
| AMPS | Advanced Mobile Phone System - Gelişmiş mobil telefon sistemi |
| APN | Access Point Name - Erişim noktası adı |
| AuC | Authentication Center - Doğrulama merkezi |
| BGP | Border Gateway Protocol - Sınır ağ geçidi protokolü |
| BSC | Base Station Controller - Baz istasyonu kontrol merkezi |
| BSS | Base Station Sub-System - Baz istasyonu alt sistemi |
| BTS | Base Transceiver Station - Baz istasyonu |
| CCU | Channel Codec Unit - Kanal kodlama birimi |
| CDMA | Code Division Multiple Access - Kod bölmeli çoklu erişim |
| DDoS | Distributed Denial-of-Service - Dağıtık hizmet dışı bırakma |
| DES | Data Encryption Standard - Veri şifreleme standardı (56 bit) |
| DLCI | The Data Link Connection Identifier - Veri bağlantı noktası belirteci |
| DNS | Domain Name System - Alan adı sistemi |
| DoS | Denial of Service - Hizmet dışı bırakma |
| EDGE | Enhanced Data rates for GSM Evolution – GSM evrimi için geliştirilmiş veri hızları |
| EIR | Equipment Identity Register - Mobil cihaz kimlik tanımı veritabanı |
| ESP | Encapsulating Security Payload - Veri kapsülleme |
| ETSI | European Telecommunications and Standards Institute – Avrupa haberleşme standartları enstitüsü |
| FAC | Final Assembly Code - Final birleştirme kodu |
| GEA | GPRS Encryption Algorithm - GPRS şifreleme algoritması |
| GGSN | Gateway GPRS Support Node - Ağ geçidi GPRS destek düğümü |
| GMM | GPRS Mobility Management - GPRS hareketlilik yönetimi |
| GMSC | Gateway Mobile Switching Center - Mobil anahtarlama merkezi ağ geçidi |
| GMSK | Gaussian Minimum-Shifted Keying - Gaussian minimum kaymalı anahtarlama |
| GPL | General Public License - Genel kamu lisansı |
| GPRS | General Packet Radio Service - Paket anahtarlamalı radyo hizmeti |
| GR | GPRS Register - GPRS veritabanı |
| GRX | GPRS Roaming EXchange - GPRS dolaşım şebekesi |
| GSM | Global System for Mobile Communications - Küresel mobil haberleşme sistemi |
| GTP | GPRS Tunnelling Protocol - GPRS tünelleme protokolü |
| HLR | Home Location Register - Abone bilgileri kalıcı veritabanı |
| HSCSD | High Speed Circuit Switched Data - Yüksek hızlı devre anahtarlamalı veri iletimi |
| ICMP | Internet Control Message Protocol - İnternet mesaj kontrol protokolü |
| IETF | Internet Engineering Task Force - Internet mühendisliği görev gücü |
| IKMP | Internet Key Management Protocol - Internet anahtar yönetim protokolü |
| IMEI | International Mobile Equipment Identity - Uluslararası mobil cihaz bilgisi |
| IMSI | International Mobile Subscriber Identity - Uluslararası mobil abone numarası |
| IP | Internet Protocol - İnternet protokolü |

| | |
|---|---|
| IPS | Intrusion Prevension System - Saldırı önleme sistemi |
| IPSec | IP Security Protocol - IP güvenlik protokolü |
| ISDN | Integrated Services Digital Network - Tümleşik hizmetler sayısal ağı |
| ISO | International Standards Organization - Uluslararası standartlar organizasyonu |
| ITU | International Telecommunications Union - Uluslararası telekomünikasyon birliği |
| LA | Location Areas - Konum alanı |
| LAI | Location Area Identifier - Konum alanı belirteci |
| LLC | Logical Link Control - Mantıksal link kontrolü |
| MAP | Mobile Application Part - Mobil uygulama kısmı |
| MCC | Mobile Country Code - Mobil şebekeye ait ülke kodu |
| MM | Mobility Management - Serbest hareketlilik yönetimi |
| MNC | Mobile Network Code - Mobil şebeke kodu |
| MS | Mobile Station - Mobil istasyon |
| MSC | Mobile Switching Center - Mobil anahtarlama merkezi |
| MSIN | Mobil Station Identification Number - Mobil istasyon kimlik numarası |
| MSISDN | Mobile Station International Service Digital Network - Mobil istasyon uluslararası sayısal servis şebekesi |
| MSRN | Mobile Station Roaming Number - Mobil istasyon dolaşım numarası |
| NAT | Network Adress Translation - Ağ adresi çevrimi |
| NIST | National Institute of Standards and Technology - Ulusal standartlar ve teknoloji enstitüsü |
| NLSP | Network Layer Security Protocol - Ağ katmanı güvenlik protokolü |
| NMC | Network Management Center - Şebeke yönetim merkezi |
| NMSI | National MS Identification number - Ulusal mobil istasyon tanımlama numarası |
| NSA | National Security Agency - Ulusal güvenlik ajansı |
| NSAP | Network Service Access Point - Ağ servisi erişim noktası |
| NSAPI | Network Service Point Identifier - Ağ servis noktası belirteci |
| OSI | Open System Interconnection - Açık sistem ara bağlaşımı |
| PCU | Packet Control Unit - Paket kontrol birimi |
| PDN | Packet Data Network - Paket veri şebekesi |
| PDP | Packet Data Protocol - Paket veri protokolü |
| PDU | Packet Data Unit - Paket veri birimi |
| PLMN | Public Land Mobile Network - Kamu mobil telefon şebekesi |
| PSTN | Public Switched Telephony Network - Kamu telefon şebekesi |
| PTM | Point to Multipoint - Bir noktadan çok noktaya |
| P-TMSI | The Packet Temporary Mobile Subscriber Identity - Mobil abone geçici kimlik paketi |
| PTP | Point to Point - Noktadan noktaya |
| QoS | The Quality of Service - Servis kalitesi |
| RA | Routing Area - Yönlendirme alanı |
| RAI | Routing Area Identity - Yönlendirme alanı kimliği |
| RAN | Radio Access Network - Radyo erişim şebekesi |
| RAND | Random Number - Rastgele numara |
| RPC | Remote Procedure Call - Uzaktan yordam çağrısı |
| RSS | Radio Subsystem - Radyo alt sistemi |
| SA | Security Associations - Güvenlik birliği |
| SAPI | Service Access Point Identifier - Servis erişim noktası belirteci |
| SDNS | Secure Data Network System - Güvenli veri ağ sistemi |
| SGSN | Serving GPRS Support Node - GPRS servis düğümü |
| SIM | Subscriber Identity Module - Abone kimlik modülü |
| SLR | SGSN Location Register - SGSN konum veritabanı |

| | |
|---|---|
| SM | Session Managament - Oturum yönetimi |
| SMS | Short Message Service - Kısa mesaj servisi |
| SNDCP | Sub Network Dependent Convergence Protocol – Alt ağ bağımlı yaklaşım protokolü |
| SNR | Serial Number - Seri numarası |
| SOHO | Small Office / Home Office - Küçük ofis / ev ofisi |
| SPI | Secure Parameter Index - Güvenlik parametre indeksi |
| SRES | Signed Response - Mobil istasyonun sayısal imzası |
| SS | Switching System - Anahtarlama sistemi |
| SS7 | Signalling System Number 7 - Sinyalleşme sistemi 7 |
| TAC | Type Approval Code - Tür onay kodu |
| TACS | Total Access Control System - Bütünsel erişimli haberleşme sistemi |
| TDMA | Time Division Multiple Access - Zaman bölmeli çoklu erişim |
| TI | Transaction Identifier - İşlem belirteci |
| TID | Tunnel Identifier - Tünel belirteci |
| TLLI | Temporary Logical Link Identifier - Geçici mantıksal bağlantı belirteci |
| TMN | Telecomunication Management Network - Telekomünikasyon yönetim şebekesi |
| TMSI | Temporary Mobile Subscriber Identity - Mobil abone geçici kimliği |
| UDP | User Datagram Protocol - Kullanıcı datagram protokolü |
| UMTS | Universal Mobile Telecommunications System – Evrensel mobil haberleşme sistemi |
| VLR | Visitor Location Register - Ziyaretçi abone bilgileri veritabanı |
| VPN | Virtual Private Network - Sanal özel ağ |

## ŞEKİL LİSTESİ

## ÇİZELGE LİSTESİ

## ÖNSÖZ

İletişim teknolojilerindeki gelişmeler hiç şüphesiz son yüzyıla damgasını vurmuştur. Bu gelişmeler günümüz insanının yaşayış biçimini, günümüz firmalarının iş yapış şeklini değiştirmiştir. Internet ve mobil haberleşme teknolojileri bu değişimin en önemli basamaklarındandır. Küreselleşen bilgi toplumunun bireyleri de haber almak, ürün satın almak, yazılı veya sözlü iletişimde bulunmak, banka işlemleri yapmak için klasik yöntemlerden vazgeçerek bu ihtiyaçlarını internet veya mobil telefon kullanarak karşılama eğilimine girmişlerdir. Internet hizmetinin mobil telefonlar üzerinden verilmeye başlanması ile birlikte bu yöne eğilim daha da artmıştır. Bunun yanı sıra daha önce firmalar için büyük sorun olan saha personeli ile hızlı ve ekonomik iletişim sorunu çözülmüş, işlem süreleri kısalmıştır. Özetle, sağladıkları kolaylıklar nedeni ile mobil sistemler ve bununla bağlantılı olarak mobil internet hayatımızın vazgeçilmez bir parçası olmuştur.

Kullanımı gittikçe artan mobil internet ortamı sağladığı kolaylıkların yanında bazı güvenlik risklerini de beraberinde getirmektedir. Özellikle işlemlerini mobil olarak gerçekleştiren kuruluşlar ve finans işlemlerini yapan bireyler için mobil internet bağlantısının güvenliği son derece önemlidir. Mobil internet üzerinden kurumsal ağlara erişim, gerekli güvenlik önlemleri alınmadığında başkalarının kurum ağına erişebilmesi veya kurum ağı ile yapılan haberleşmenin dinlenmesine neden olabilmektedir. Gizliliğin büyük bir rekabet avantajı getirdiği günümüzde erişim için hangi teknoloji kullanılırsa kullanılsın gerekli önlemlerin alınması kaçınılmazdır.

Tez kapsamında mobil internet erişim tekniklerinden yaygın olarak kullanılan GPRS'in (General Packet Radio Service) taşıdığı riskler saptanmış, sahip olduğu güvenlik fonksiyonları ele alınmıştır. GPRS şebekesinde güvenlik sağlanması için gerekli güvenlik önlemleri belirlenmiş ve operatörlerin dikkat etmesi gereken konular belirtilmiştir. GPRS şebekelerinde kullanılmak üzere güvenlik testleri geliştirilmiş ve örnek bir GPRS şebekesi üzerinde test edilerek güvenlik açıklıkları saptanmıştır.

Bu çalışma boyunca yardımlarını, dostluğunu ve kıymetli vaktini esirgemeyen, engin tecrübelerinden faydalandığım değerli hocam Aktül KAVAS'a, tezin geliştirilmesi sırasında Ericsson Mobility World (EMW) GPRS şebekesini kullanmamıza olanak sağlayan Mobil Internet İş Koordinatörü Dağhan FELLAHOĞLU'na, güvenlik testleri süresince yardımlarını esirgemeyen Teknoloji Müdürü Murat ERDEM'e ve Ericsson Destek Mühendisi Noyan KAZAZ'a en içten teşekkürlerimi sunarım.

Ayrıca, akademik çalışmalarımız için destek sağlayan Tübitak UEKAE yönetimine, proje yöneticim Mert ÜNERİ'ye, çalışmalarımı gerçekleştirirken bana sağladığı huzurlu ortam ve manevi destek için eşim Nilay DİNÇKAN'a ve bugünlere gelmemi sağlayan aileme teşekkür ederim.

## ÖZET

İnsanoğlu yüzyıllardır bulunduğu yer ve zamandan bağımsız olarak iletişim sağlayabilmeyi hayal etmiştir. Bu hayal mobil haberleşme fikrini doğurmuştur. Elektronik sistemlerin küçülmesi ve teknolojinin ilerlemesi neticesinde önceleri sadece evlerimizde ve işyerlerimizde bulunan telefonlar artık hepimizin ceplerinde bulunmaktadır. Mobil haberleşme konusunda yapılan çalışmalar sadece ses haberleşmesi ile sınırlı kalmamış, ihtiyaç duyulan veri haberleşmesinin de mobil olarak verilmesine olanak sağlamıştır. Bu sayede daha önce klasik yöntemler ile karşılanan ihtiyaçlar mobil cihazlar üzerinden karşılanmaya başlanmıştır. Verilen hizmetlerden en önemlisi mobil internet hizmetidir. Mobil internet alışverişten kurumsal ağlara bağlanmaya kadar birçok hizmeti kapsayan bir teknolojidir. Bu teknoloji mobil cihazlarımıza GSM sistemi üzerinde çalışan GPRS ve EDGE teknolojileri ile verilmektedir. Dünya üzerinde aynı hizmeti üçüncü nesil GSM sistemleri kullanarak veren operatörler bulunmakla birlikte Türkiye'de henüz deneme çalışmaları sürmektedir.

Bu çalışmada; GSM operatörlerinin mobil internet hizmeti vermek üzere çok yaygın olarak kullandığı GPRS sisteminin güvenlik konuları ele alınmıştır. GPRS sisteminin korunmaya ihtiyacı olan bilgileri, potansiyel saldırganları ve GPRS sistemi güvenlik tehditleri ortaya konmuştur. Tehditlerden korunmak amacıyla alınması gereken güvenlik önlemleri geliştirilmiştir. Ayrıca, GPRS operatörlerinin güvenli hizmet verebilmeleri için gerekli kıstaslar belirlenmiş ve bu kıstaslar canlı bir GPRS şebekesi üzerinde test edilmiştir. Canlı şebeke üzerine uygulanan testlerin geliştirilmesi için örnek bir GPRS şebekesi kurulmuş ve güvenlik testleri tekrarlanmıştır. Örnek GPRS test sistemi için GPRS operatörlerinin de kullanabileceği bir güvenlik politikası geliştirilmiştir.



**Anahtar kelimeler:** Mobil internet, GSM, GPRS, Güvenlik, (A3, GPRS-A5, A8) Doğrulama ve şifreleme algoritmaları, güvenlik politikası, EDGE

**ABSTRACT**

Human beings had always dreamed of being able to communicate freely without the limitations of time and place. This dream led the idea of mobile communication. Thanks to the electronic systems, getting smaller, and the development of technology, telephones, which we had only in our homes and offices in the past, are now in our pockets. Mobile communication studies have not been limited to voice communication, but it provided the needed mobile data transmission. Thanks to this improvement the needs which used to be met by traditional means have started to be met with mobile devices. The most important service provided is the mobile internet service. Mobile internet is a technology that includes services varying from shopping to corporate networks. This technology is added to our mobile devices with GPRS and EDGE technologies which work over GSM system. There are operators in the world which provide the same service by using the third generation GSM systems; however, only trial studies have been going on in Turkey.

The work in this study is the security issues of the GPRS system which is very commonly used by the GSM operators to provide mobile internet service. The information needed to be protected, the potential attackers, and the security threats of the GPRS system are presented. Security countermeasures are developed in order to be protected against the threats. Moreover, criteria needed by the GPRS operators to provide a secure service are determined, and they are tested on a live GPRS network. In order to develop these tests, a sample GPRS network has been constructed and the security tests have been repeated. For this sample GPRS test system, a security policy which can also be used by GPRS operators has been developed.

**Key Words:** Mobile internet, GSM, GPRS, Security, (A3, GPRS-A5, A8) Authentication and ciphering algorithms, security policy, EDGE

# 1. GİRİŞ

GPRS sistemi, abonelerine, paket anahtarlamalı haberleşme tekniğini kullanarak, GSM şebekesi üzerinden, standart veri şebekelerine yüksek hızlarda erişim hizmeti sağlamaktadır. GPRS sistemi, üçüncü nesil (3G) teknolojilere geçiş aşaması olarak kullanılmaktadır. Ülkemizde üçüncü nesile ne zaman geçileceği konusu henüz netlik kazanmamıştır. Lisansların 2006 yılında verilmesi yönünde çalışmalar başlatılmıştır[1]. Üçüncü nesil lisans ve altyapı bedellerinin yüksek olması, GPRS'in en azından önümüzdeki senelerde önemli bir erişim altyapısı olacağını göstermektedir. Üçüncü nesil iletişim ile ilgili lisans ve altyapı maliyeti sorunları aşılsa dahi yaygınlaşma dönemi, kapsama alanı, 3G hizmetlerini sunan operatör sayıları gibi kısıtlamalar, GPRS hizmetlerinin bundan sonra da uzun süre devam edeceğinin göstergesidir.

GPRS servisleri abonelerine, küçük ofis / ev ofisi (SOHO), bankacılık, elektronik ticaret, mobil veri toplama, reklam ve pazarlama gibi işlemlerde kolaylıklar getirmektedir. Internet üzerinden gerçekleştirilebilecek her türlü işlem GPRS şebekeleri üzerinden gerçekleştirilebilmektedir.

Kurumlar ve aboneler her ortamdan iletişim ihtiyaçlarının giderebildikleri için GPRS'in kullanım oranı her geçen gün artmaktadır. GPRS sistemi üzerinden akan kurumsal veri kurumların işi ile doğrudan ilgili olduğundan maddi değere sahiptir, aynı şekilde abonelerin internet bankacılığı veya elektronik ticaret gibi faaliyetleri de doğrudan para ile ilgilidir. GPRS sistemi popülerliği ve üzerinden nakit işlemlerinin geçmesi nedeni ile kötü niyetli kişilerin hedefi haline gelmiştir. Her sistemde olduğu gibi GPRS sisteminin de güvenli olarak kullanılması mümkündür. Bunun için hem operatörler hem de aboneler tarafından gerekli önlemler alınmalıdır. Tez kapsamında GPRS sisteminin taşıdığı riskler, tehditler ve potansiyel saldırganlar anlatılmış, ilgili tehditlere karşı uygulanabilecek önlemler verilmiştir.

## 1.1 Tezin Konusu ve Amacı

Tez kapsamında GPRS sistemlerinde güvenlik konusu incelenmiştir. Tezin amacı; GPRS sisteminde bulunan güvenlik açıklıklarını saptamak ve bu açıklıkları kullanarak sisteme zarar verebilecek tehditleri ortaya koymak, örnek bir sistem için güvenlik testi yaparak tehditlere karşı güvenlik önerileri geliştirmektir.

[1] Telekomünikasyon Kurumu, "Türkiye İçin Genişbantta Yeni Teknolojiler (3G)"

### 1.2 Daha Önce Yapılan Çalışmalar

1999 ve 2000 yılları arasında GSM operatörleri deneme amaçlı olmak üzere ilk ticari GPRS altyapılarını kurmuşlardır. 2000 yılının yazında deneme amaçlı ilk GPRS servisi T-Mobil tarafından Expo2000 fuarında 28 kbit/sn hızında verilmiştir. 2001 yılında GPRS destekli terminaller satışa sunulmuştur. 2001 yılından itibaren birçok operatör abonelerine GPRS hizmeti sağlamaya başlamıştır[1].

GPRS sistemleri güvenliği ile ilgili akademik olarak yapılan çalışmalardan ilki 1998 yılında *Stephane Piot* tarafından *University College London*'da Elektrik ve Elektronik Mühendisliği bölümünde yapılan "*Security over GPRS"* isimli yüksek lisans tezidir. *Piot* bu çalışmasında 1998 yılında GPRS uygulamalarının henüz başlamamış olması nedeni ile GPRS sistemlerinde güvenlik konusunu kavramsal olarak incelemiştir. Tezde özellikle GPRS kavramları ve hava arayüzünün güvenliği ile ilgili konular işlenmiştir.

GPRS sistemleri güvenliği konusundaki bir diğer çalışma 2001 yılında *Geir Stian Bjåen* ve *Erling Kaasin* tarafından *Agder Univerisity College* Bilgi ve haberleşme teknolojileri bölümünde yapılan "*Security in GPRS"* isimli yüksek lisans tezidir. Bu tezde 2001 yılı itibari ile GPRS siteminde bulunan olası açıklıklar ele alınmış ve çeşitli senaryolar için güvenlik testi yapılarak sonuçları yorumlanmıştır.

Bu çalışmalara ek olarak @stake firmasının 2002 yılında yayınladığı "*GPRS Wireless Security"* ve 2004 yılında yayınladığı "*Attacks and counter measures in 2.5G and 3G Cellular IP networks*" araştırma raporları bulunmaktadır.

Son olarak GPRS sistemlerinde uçtan uca güvenlik sağlamak amacı ile kullanılan Sanal Özel Ağların (Virtual Private Networks - VPNs) kullanımına yönelik Atina Üniversitesi Haberleşme Bölümü'nden *Christos Xenakis* ve *Lazaros Merakos* "*Secure VPN Deployment in GPRS Mobile Networks*" isimli bir makale yayınlamışlardır. Bu makalede VPN teknolojisinin GPRS şebekesinde nasıl uygulanacağı detaylı olarak ele alınmıştır. Aynı konuda Lucent Technologies firmasının da 2000 yılında yayınlamış olduğu "Mobile VPNs for Next Generation GPRS and UMTS Networks" isimli bir çalışması bulunmaktadır.

---

[1] GSM Association, "What is General Packet Radio Service"

# 2. TEMEL BİLGİLER

Bu bölümde GPRS sisteminin anlaşılabilmesi için gerekli temel bilgiler verilmiştir. İlk olarak veri haberleşme türleri tanıtılmış, daha sonra mobil haberleşme sistemlerinin gelişimi hakkında bilgi verilmiştir. Son olarak GPRS hizmetinin verilmesi için zemin hazırlayan GSM sisteminin çalışma prensipleri anlatılmıştır.

## 2.1 Veri Haberleşmesi Türleri

Veri haberleşmesi iki ana bölümde incelenmektedir. Bunlardan ilki, haberleşme süresince sabit bir hatta sahip olan ve bütün verinin aynı devre üzerinden aktığı devre anahtarlamalı haberleşmedir. Diğeri ise verinin paketlere ayrılarak birbirinden bağımsız olarak alıcı uca iletildiği paket anahtarlamalı haberleşme sistemidir. GSM sistemi devre anahtarlamalı haberleşme sistemlerine, GPRS sistemi ise paket anahtarlamalı haberleşme sistemlerine örnek olarak verilebilir.

### 2.1.1 Devre Anahtarlamalı Haberleşme

Devre anahtarlamalı haberleşme sisteminde veri, bir veya daha fazla santral üzerinden geçerek, kullanıcılar arasında zamanda ya da frekans uzayında (domain) bağlantı kurularak iletilmektedir. Haberleşme taraflar arasında yol kurulunca başlamakta ve kurulan yol görüşme süresince kullanılmaktadır. Görüşme sona erdiğinde alıcı ve verici arasında kurulan bağlantı çözülmekte ve imkanlar başka kullanıcılara tahsis edilmektedir (Heine,2003).

GSM sisteminde veri iletilmek istendiğinde, şebeke mobil istasyona (MS) bir radyo kanalı tahsis ederek hava arayüzü bağlantısı kurmaktadır. Transfer edilen veri miktarından bağımsız olarak kanal haberleşme süresince tahsis edilmektedir. Abone genelde toplam bağlantı süresi için ödeme yapmak zorundadır (Ericsson, 2000).

Devre anahtarlamalı haberleşme tekniği aşağıdaki durumlara sahip veri trafiği için uygundur:

- Sabit bant genişlikli veri akışı durumlarında
- Veri küçük bağlantı gecikmelerine duyarlı olduğunda. (örnek: Gerçek zamanlı ve interaktif uygulamalar zamana duyarlıdır. İnteraktif uygulamalarda kullanıcının girdiği değere sistemin geç yanıt vermesi müşteri memnuniyetini azaltır. Buna karşın SMS zamana duyarlı bir uygulama değildir. Gecikme dakikalar mertebesinde bile olsa kullanıcı genelde farkında olmayacaktır)

### 2.1.2 Paket Anahtarlamalı Haberleşme

Bir uç noktasından başka bir uç noktasına iletilmek üzere bir mesaj gönderildiğinde, sistem mesajı paket adı verilen belli bir uzunluğu olan parçalara ayırmaktadır. Noktadan noktaya kurulan bağlantıya "Sanal Bağlantı" adı verilmektedir. Oluşturulan paketler ayrık olarak iletilmekte ve her bir pakete, ulaşması istenen uç noktanın adresi eklenmektedir. Bir mesaja ait paketler farklı yollar izleyerek farklı gecikmelerle alıcısına ulaşabilmektedir. Alıcının mesajı doğru değerlendirebilmesi için paketin sıra numarası da taşıması gerekmektedir (Heine,2003).

GSM sisteminde bir radyo kanalı TDMA (Zaman bölmeli çoklu erişim) yöntemi ile sekiz zaman kanalına ayrılmaktadır. Bu zaman kanalları devre anahtarlamalı haberleşmede ses taşımak için kullanılmaktadır. Aynı kanallar GPRS şebekesi için veri taşımak amacı ile kullanılmaktadır. Paket anahtarlamalı haberleşme için şebeke, ihtiyaç olduğunda paketlere ayrılmış olan veriyi zaman kanallarına dağıtmaktadır. Bu yüzden bir radyo kanalı birden fazla mobil istasyon tarafından eşzamanlı olarak paylaşılabilmektedir. GPRS şebekesinde bir mobil istasyon gerektiğinde sekiz radyo zaman kanalını aynı anda kullanabilmektedir. Bir mobil istasyon veri paketi oluşturduğunda, şebeke, paketi adresine uygun olan ilk radyo kanalı üzerinden göndermektedir. Veri trafiği, veri patlamaları içerdiğinden radyo kanalları verimli bir şekilde kullanılmaktadır. Radyo kanallarının paylaşımında yapılan çoğullama işlemi sırasında gecikme oluşabilmektedir. Bu gecikmenin kabul edilebilir seviyede olması için kullanıcı ile hizmet sağlayıcı arasında "Servis Kalitesi" (QoS) tanımlanmaktadır. GPRS şebekesinde tanımlanabilecek dört farklı gecikme sınıfı vardır. En iyi gecikme sınıfında, paket uzunluğunun 128 oktet olması durumunda ortalama gecikme 0.5 saniyenin altındadır, paket uzunluğunun 1024 oktet olması durumunda ortalama gecikme 2 saniyenin altındadır. Bu değerler ikinci en iyi gecikme sınıfında sırasıyla 5 ve 15 saniye, üçüncü en iyi gecikme sınıfında 50 ve 75 saniyedir. Dördüncü gecikme sınıfı için ise bu tür değerler tanımlanmamıştır (Sanders,2003). Paket anahtarlamasında bant genişliği, devre anahtarlamasında yapıldığının aksine, sürekli olarak tahsis edilmemektedir. Bunun yerine gerekli olduğunda bant genişliği tahsis edilmekte ve ihtiyaç olmadığında serbest bırakılmaktadır.

GPRS, X.25, Çerçeve Aktarma (Frame Relay) ve IP protokolünün bulunduğu sistemler paket anahtarlama teknolojisini kullanmaktadır.

Paket anahtarlama tekniği aşağıdaki durumlara sahip veri trafiği için uygundur (Ericsson, 2000):

- Veri patlamalar halinde gönderiliyor ise
- Veri hatalara karşı duyarlı ise

## 2.2 Mobil Haberleşme Sistemlerinin Gelişimi

Mobil haberleşme 1940'lı yıllarda A.B.D. 'de ve 1950 yıllarında Avrupa'da tek hücreli analog araç telefonlarının kullanılmasıyla başlamıştır. Daha sonra 1970'lerin sonlarına doğru birinci nesil (1G) diye adlandırılan hücresel analog mobil telefonlar kullanılmıştır. Analog haberleşme teknolojisini kullanan birinci nesil (1G) mobil haberleşme sistemi, ses kalitesi, kapasite, kapsama alanı artırılması ve veri iletim isteklerini karşılayamamıştır. Bu problemlerin çözümü için sayısal haberleşme teknolojisini kullanan ikinci nesil (2G) mobil haberleşme sistemi geliştirilmiştir. İkinci nesil sistemlerde esas olarak ses haberleşmesi hizmetlerini sağlamak hedeflenmiştir. Bu nedenle bu sistemler devre anahtarlamalı radyo haberleşmesini kullanmaktadırlar. Küresel mobil haberleşme sistemi (GSM) ikinci nesil mobil haberleşme sistemidir ve yüksek hızda hareket eden abonelerin kesintisiz iletişim halinde kalabilmeleri için dinamik olarak baz istasyonu değiştirme ve girişim giderme yetenekleri ile donatılmıştır (Özdemir, 2001).

Devre anahtarlamalı sistemler, ses haberleşmesi için etkin olmakla birlikte internet üzerinden haberleşmede olduğu gibi patlamalı tip veri trafiği için yetersiz kalmıştır. Bunun nedeni devre anahtarlamalı sistemlerin trafik kanalını tüm oturum boyunca veri haberleşmesi yapmak isteyen kullanıcıya tahsis etmesidir. Devre anahtarlamalı sistemlerde patlamalı veri iletimi yapılması durumunda, trafik kanalı zamanın büyük bir bölümünde boş kalmaktadır. Veri hizmetlerine olan taleplerin giderek artması, yeni protokollerin geliştirilmesi ihtiyacını doğurmuştur. Bu da sayısal teknolojiyi ve paket anahtarlamalı radyo haberleşmesini daha verimli bir şekilde destekleyebilen üçüncü nesil sistemlerin geliştirilmesine yol açmıştır. 3. nesil (3G) mobil haberleşme sistemleri, gerçek zamanlı çoklu ortam (multimedya) hizmetleri sunan bir hücresel haberleşme sistemidir. Üçüncü nesil mobil haberleşme sistemlerinde yüksek hızda internet erişimi sağlanarak, hareketli resim, ses, veri ve grafik bilgileri de iletilmektedir. Bu hizmetleri sunabilmek için sabit erişimde 2 Mbit/sn, yaya hızında 384 kbit/sn, taşıtla seyahat hızlarında 144 kbit/sn bilgi hızlarına gereksinim vardır. (Özdemir, 2001)

### 2.2.1 Mobil Haberleşme Sistemlerinde Veri Haberleşmesi

GSM servisi ile ilgili ilk gelişme, var olan devre anahtarlamalı veri hızının 9.6 kbit/sn'den 14.4 kbit/sn'ye çıkartılmasıdır. Bu aşamadan sonra 1998 yılında, veri iletim hızını arttırmak amacıyla devre anahtarlamalı veri kapasitesine sahip mevcut ikinci nesil GSM şebekelerinin gelişmiş bir uygulaması olan HSCSD (Yüksek hızlı devre anahtarlamalı veri iletimi) yapısı oluşturulmuştur. HSCSD kullanımı ile 57.6 kbps hızına kadar veri iletimi gerçekleştirmek mümkündür. Temelde yüksek hızlara ulaşmak çoklu GSM zaman kanalı ile mümkündür. Bir zaman kanalı ile 14.4 kbit/sn hızında veri iletimi gerçekleştirilebilmektedir. HSCSD'de 57.6 kbit/sn hızına ulaşmak için 4 zaman kanalı kullanılmaktadır (Candan,2002).

HSCSD'den sonra GPRS teknolojisi gelmektedir. GPRS sistemi ile teorik olarak 171.2 kbit/sn hız desteklenmektedir. Yüksek hızda bir GPRS bağlantısının kurulma süresi sadece 1-2 saniye almakta ve yalnız bir kez bağlantı kurulması yeterli olmaktır. Bu aşamada, son kullanıcı herhangi bir şebeke kaynağını kullanmadan sürekli hatta kalabilmekte ve kapasiteye ihtiyaç duyulduğunda erişim gecikmeleri sadece birkaç yüz milisaniye olmaktadır.

GPRS teknolojisinden sonra ve üçüncü nesilden önce EDGE (GSM evrimi için geliştirilmiş veri hızları) teknolojisi gelmektedir ve geliştirilmiş modülasyon teknikleri kullanılarak 384 kbit/sn'lik bir maksimum teorik hız desteklenmektedir.

EDGE teknolojisinden sonra veri haberleşmesini 2 Mbit/sn hızlara çıkarabilen üçüncü nesil hücresel sistemler gelmektedir. GSA (GSM Supplier Association) internet sitesinden 23 ekim 2005 itibari ile alınan bilgiye göre üçüncü nesil sistemler için 146 adet lisans verilmiş ve bu lisanslar ile 37 ülkede 82 operatör faaliyete geçmiştir. Üçüncü nesil sistemleri kullanan operatörlerden 55 tanesi aynı zamanda EDGE hizmeti de vermektedir.

**Çizelge 2-1 Mobil haberleşme sistemleri veri haberleşme hızları**

| **Teknolojinin Adı** | **Yetenekleri ve Hızı** | **Notlar** |
|---|---|---|
| GSM | 9.6 kbit/sn hızında devre anahtarlamalı veri ve faks | Çoğu GSM operatöründe mümkün |
| GSM | 14.4 kbit/sn hızında devre anahtarlamalı veri ve faks | 9.6 kbit/sn servisi ile benzer şekilde, daha yüksek hızda çalışır. |
| HSCSD | 57.6 kbit/sn'ye kadar yüksek hız | Pahalı altyapı gerektirmez, taşıyıcılar için sadece yazılım geliştirmesi yapılır. |

| | | |
|---|---|---|
| GPRS | Teorik olarak 171.2 kbit/sn hızında paket veri iletimi | Son derece yetenekli ve esnek mobil haberleşme |
| EDGE | GPRS ile mümkün olan hızı 3 kat daha artıran yüksek hızlı paket veri iletimi | Var olan GSM şebekesi için son yüksek hızlı veri şebekesi |
| 3.Nesil Hücresel Sistemler | 2 Mbit/sn'lik yüksek hızlı paket veri iletimi | Tamamen yeni bir hava arayüzü |

### 2.3 GSM Sisteminin Gelişimi

Avrupa devletleri 1980'li yılların başlarından itibaren birbirlerinden bağımsız olarak kendi özel hücresel sistemlerini geliştirmişlerdir. Bunun en büyük dezavantajı bu sistemlerin birbirleri ile uyumsuz olmalarıdır. ETSI (Avrupa haberleşme standartları enstitüsü) 1990 yılında Avrupa 'da uluslararası dolaşımı sağlayabilmek için GSM standardının 1. fazını yayınlamıştır. GSM iyi bir konuşma kalitesi, düşük terminal ve hizmet maliyeti, kendisinden önceki sistemlere göre daha yüksek bant verimliliği, ISDN (tümleşik hizmetler sayısal ağı) ile uyumluluk ve ilk aşamada Avrupa ülkelerinde uluslararası dolaşım sağlamak amacıyla geliştirilmiş bir sistemdir. GSM, devreye girdikten sonra tahmin edilenin ötesinde ilgi görmüş, bunun sonucunda da tüm dünyaya yayılmıştır[1].

ETSI bu amaçları destekleyebilmek için GSM'in devre anahtarlaması kullanan sayısal ve hücresel bir sistem olarak geliştirilmesine karar vermiştir. Hücresel sistemlerde tanımlı olan sınırlı frekans bandında milyonlarca aboneyi konuşturabilmek için frekansın tekrar kullanılması zorunluluktur, bu da sistemin verimliliğini ve kapasitesini arttıran bir etkendir. Ancak bu durum, sistemde düşük güçlü vericiler kullanılmasını gerektirmektedir. Devre anahtarlaması tekniğinin ses haberleşmesini etkin bir biçimde desteklemesinden dolayı GSM' de devre anahtarlamalı iletim tekniği seçilmiştir.

### 2.4 GPRS Sisteminin Gelişimi

İnternetin giderek yaygınlaşması ve gün geçtikçe daha fazla kullanım alanına sahip olması ile GSM'in veri haberleşmesi ihtiyaçlarını karşılamakta yetersiz kaldığı görülmüştür. Bu nedenle ETSI 1997 yılında GSM Faz 2+ standardını yayınlamıştır. İkinci nesil sistemler ile üçüncü

[1] http://www.symbiandev.net/node/32

nesil sistemler arasında geçiş görevi gören bu sistem paket anahtarlamalı radyo hizmeti (GPRS) olarak adlandırılmaktadır.

Paket anahtarlamalı haberleşme sistemlerinde, veri trafiğinin patlamalı olması (örnek: internet) durumlarında radyo kaynakları daha verimli kullanılmaktadır. GSM sistemi üzerine geliştirilen GPRS ile GSM'in paket veri iletim yeteneğinin geliştirilmesi amaçlanmıştır. GPRS orijinal olarak paket anahtarlamalı bir sistem olduğundan patlamalı veri iletimini etkin bir biçimde destekleyebilmektedir. GPRS'in ücretlendirme yapısı GSM'den farklıdır. GSM'de aboneler şebekeye bağlı oldukları süreye göre ücretlendirilirken GPRS'te aboneler genelde gönderdikleri ve aldıkları veriye göre ücretlendirilirler.

GPRS'te abone mobil cihazı açık olduğu sürece şebeke ile mobil cihaz arasında her zaman pasif bir bağlantı bulunmaktadır. Böylece e-posta hizmeti gibi arka planda çalışan hizmetler desteklenirken gerektiğinde veri iletimi için şebeke ile mobil cihaz arasındaki bağlantının en kısa zamanda aktif hale gelmesi sağlanmaktadır. GPRS, mevcut GSM altyapısına paket haberleşmesi için yeni cihazlar ekleyerek bu hizmeti vermektedir. Bu sebeple GPRS ile GSM aynı frekans bantlarını, aynı çerçeve yapısını ve aynı modülasyon tekniklerini kullanmaktadır.

### 2.5 EDGE Sisteminin Gelişimi

3G sistemlerine doğru giden yolda en son adımı oluşturan EDGE (GSM evrimi için geliştirilmiş veri hızları), 3G lisansı alması zor olan veya alamamış mobil şebeke operatörlerinin yararlanması amacıyla geliştirilmiştir. EDGE, GSM operatörlerine, 3G şebekeleri üzerinde sunulan servislere yakın hızlarda hizmet sunma olanağı vermektedir. Aynı zamanda EDGE, daha sonra 3G kullanımında gerekli olacak modülasyon değişikliklerinin şimdiden yapılarak, GSM'den 3G'ye geçiş dönemi sürecinde de yardımcı olmaktadır.

EDGE sistemi şebeke operatörleri tarafından, kurulumu basit olarak gerçekleştirilebilecek şekilde tasarlanmıştır. Kurulum için EDGE verici birimi her hücreye eklenmekte, baz istasyonu kontrol merkezlerinde ve baz istasyonlarında yazılım yenilemeleri yapılmaktadır. Yeni EDGE vericileri, standart GSM trafiğini taşıyabilecekleri gibi gerekli durumlarda vericiler otomatik olarak EDGE modunda çalışabilmektedir. Abonelerin bu hizmetten faydalanabilmeleri için mobil cihazlarının EDGE sistemini destekliyor olması gereklidir.

EDGE kullanımına başlanması, teknolojisinin büyük oranda GSM temelli olması nedeniyle operatörlere yatırım açısından çok büyük külfet getirmemektedir. EDGE çekirdek şebeke ve hücre kapsama açısından mevcut GSM mimarisi ile uyumludur. EDGE'nin arkasındaki fikir,

mevcut devre (ve paket) anahtarlama tekniklerini kullanarak 200 kHz GSM bant genişliğinde daha hızlı veri iletimini sağlamaktır. EDGE, GSM ile aynı TDMA yapısını ve 200 kHz bant genişliğini kullanması nedeniyle aynı anda 900-1800 MHz frekans bandı bölgesinde mevcut GSM şebekeleri ile birlikte kullanılabilmektedir (Hannikainen, 2002).

EDGE, 384 kbps veri hızına ulaşımda alternatif bir modülasyon tekniği kullanmaktadır. HSCSD ve GPRS her bir zaman kanalı üzerine düşen bit hızını arttıran GMSK (Gaussian minimum kaymalı anahtarlama) modülasyon tekniğini kullanmaktadır. EDGE ise hava arayüzü içinde daha yüksek hızlara ulaşabilen 8PSK (8 faz kaymalı anahtarlama) adı verilen bir modülasyon tekniği kullanmaktadır. Zaman kanalı başına düşen bit hızının ulaştığı maksimum 48 kbit/sn veri hızının mevcut veri iletim servislerinin sağlayabildiği bit hızından daha yüksek olması nedeniyle, hava arayüzü teknolojileri içinde en önemli gelişme olarak değerlendirilmektedir (Hannikainen, 2002).

## 2.6 Üçüncü Nesil Mobil Haberleşme Sistemi

### 2.6.1 Üçüncü Nesil Standartlarının Gelişimi

Uluslararası Telekomünikasyon Birliği (ITU) birbiri ile uyumsuz standartlara sahip hücresel haberleşme sistemlerinin hızlı gelişimini takiben 1985 yılında "3G" diye tabir edilen üçüncü nesil haberleşme standartlarını geliştirmek için çalışmalara başlamıştır.

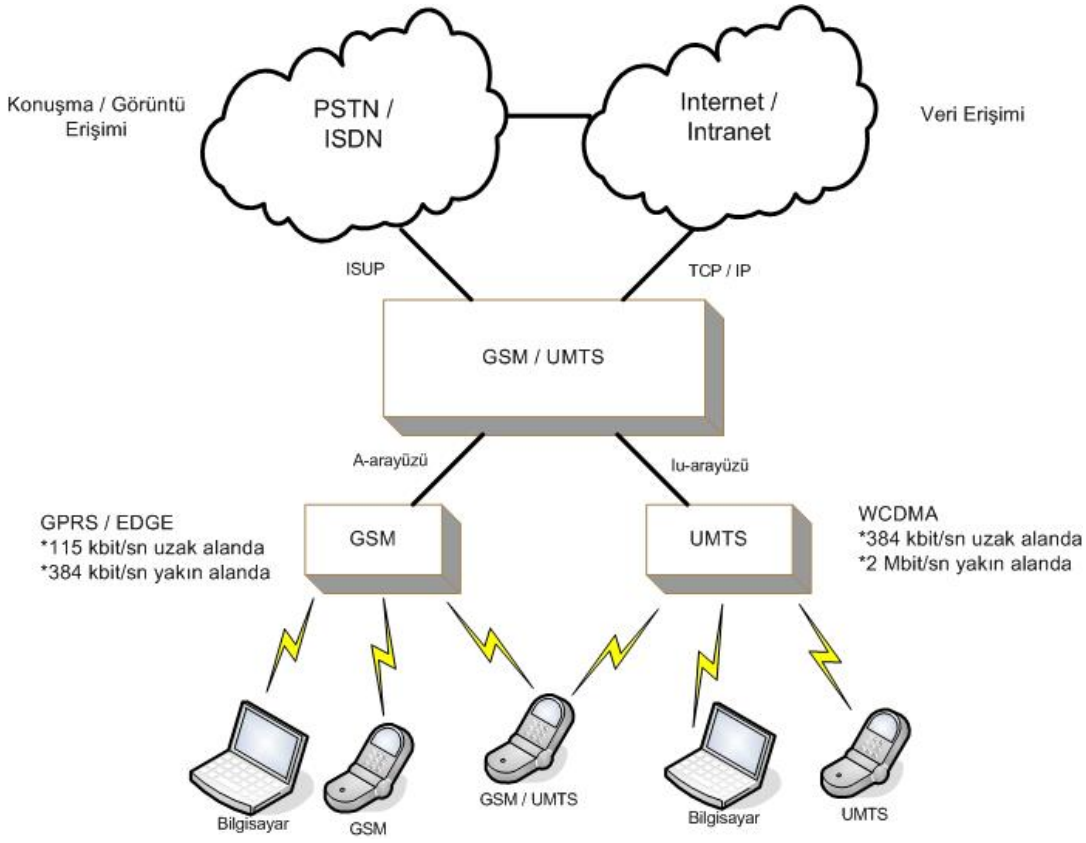
ITU, 1998 yılında üçüncü nesil mobil haberleşme standartlarının genel adı olarak IMT-2000'i (International Mobile Telecommunications Year 2000) kabul etmiş, aynı yıl Avrupa haberleşme standartları enstitüsü (ETSI) Avrupa'da üçüncü nesil sistemler için kullanılacak standartları evrensel mobil haberleşme sistemi (UMTS) adı altında ITU'ye evrensel standart önerisi olarak sunmuştur. ABD ise, Kuzey Amerika'da kullanılmakta olan hücresel sistemlerden AMPS (Gelişmiş mobil telefon sistemi) ve CDMA (Kod bölmeli çoklu erişim) ile uyumlu olan CDMA-2000'i 3G küresel standardı olarak önermiştir (Özdemir, 2001).

1998 yılı Aralık ayında Avrupa'dan ETSI, Japonya'dan ARIB ve TIC, ABD'den ANSI ve Kore'den TTA gibi dünyanın önde gelen standart enstitülerinin altı tanesi üçüncü nesil mobil haberleşme siteminin mevcut GSM alt yapısı ile uyumlu olmasını sağlayacak teknik özellik ve standartları belirlemek amacı ile bir araya gelerek; üçüncü nesil ortaklık projesi 3GPP'i (3G Partnership Project) oluşturmuşlardır. Daha sonraki gelişmeler ile IMT-2000 bir dünya standardı haline gelmiştir. Bu gelişmeler sonucunda IMT-2000 her biri GSM ve IS-41 şebeke mimarisine uyumlu üç işletim modelini kapsayan CDMA tabanlı bir standart haline gelmiştir.

### 2.6.2 Evrensel Mobil Haberleşme Sistemi (UMTS)

UMTS, yüksek hızlı veri iletimine ve gerçek küresel gezinmeye olanak tanıyan IMT-2000'nin standartlarına uygun olarak Avrupa'da kabul edilen üçüncü nesil bir haberleşme sistemidir.

Yeni UMTS şebekesinin mevcut GSM işleticilerinin kullandıkları şebeke alt yapısı üzerine kurulması işleticiler tarafından tercih edilmektedir. 2. nesil ve 3. nesil sistemlerinin bir arada çalışması düşüncesi Şekil 2-1'de verilmiştir (Özdemir, 2001).




**Şekil 2-1 İkinci ve üçüncü nesil sistemlerinin bir arada çalışması**

UMTS' in sağlayacağı özellikler aşağıdadır;

- Ses kalitesinde artış
- Bireye özel uygulamalar (isteğe bağlı olarak oyun oynamak, müzik dinlemek)
- Kaplama alanın genişlemesi ve hücre sayısında azalma
- Sistem planlama, kurulum ve işletme masraflarında azalma
- Diğer elektronik cihazlarla olan elektromanyetik etkide azalma
- Aktarmadan kaynaklanan çağrı kayıplarında azalma

- Kablosuz güvenli veri transferi
- Eski teknolojilerle uyumluluk

### 2.6.3 UMTS Hizmetleri ve Uygulamaları

UMTS talebe göre hizmet sunmaktadır. Yüksek kalitede eğlence hizmetleri, büyük dosyaları indirme ve internette dolaşma bu kavram içinde sunulan hizmet türleri arasındadır. Çoklu ortam hizmetlerinin sunumuna ilave olarak, kullanıcıların gereksinim duyduğu mevcut iletişim hizmetleri UMTS sistemi içinde verilmektedir.

Aşağıda UMTS tarafından desteklenen hizmet ve uygulama örnekleri verilmektedir. Belirtilen büyük pazar hizmetlerinden bazıları sabit ya da GSM şebekeleri üzerinden halen sunulmaktadır. Ancak UMTS bu konularda hem hizmet vermede hem de hizmet verme performansında önemli yenilik ve gelişmeler sağlamaktadır (UMTS Forum,1997).

**Bilişim**

- WEB sayfalarında dolaşma
- İnteraktif alışveriş
- Gazetelere ya da yazılı medya ürünlerine internet üzerinden erişim
- Internet üzerinden anında çeviri
- Geliştirilmiş tarama ve filtreleme yeteneği

**Eğitim**

- Sanal okul
- Internet üzerinden bilimsel laboratuarlara erişim
- Internet üzerinden kütüphane hizmeti
- Internet üzerinden dil eğitimi
- Çeşitli eğitimler

**Eğlence**

- İsteğe bağlı müzik ( CD, kaset ve radyolara alternatif olarak)
- İsteğe bağlı oyunlar
- Video klipler
- Sanal manzara görüntüleri

**Toplum Hizmetleri**

- Acil servis hizmetleri
- İdari prosedürler (Government procedure)

**İş Uygulamaları**

- Mobil ofis
- Sanal çalışma grupları

**Kişiler Arası İletişim Hizmetleri**

- Görüntülü telefon
- Video konferans
- Sesli cevap ve tanıma
- Kişisel konum belirleme

**Ticari Ve Finansal Hizmetler**

- Sanal banka
- Internet üzerinden fatura ödeme

**Karayolu Ulaşım İzleme Hizmeti**

- Hastane veya tıp hizmetlerine uzaktan erişim (telemedecine)
- Güvenlik kamerası hizmeti
- Acil yardım hattı
- Telefon konuşmalarında gizli bağlantı kurma yeteneği

# 3. GSM SİSTEMİ

GSM sözcüğü, Türkçe anlamı "Küresel Mobil İletişim Sistemi" anlamına gelen *"Global Ssystem for Mobile Communications"* tanımlamasının baş harflerinden oluşmuştur. Bu sistem, kullanıcılarına daha güvenli ve kaliteli bir iletişim hizmeti sunmakla birlikte, uluslararası seyahat serbestliği ve mekan özgürlüğü sağlamaktadır. GSM aboneleri, dünyanın neresinde olurlarsa olsunlar GSM kapsam alanı içinde bulundukları sürece, dünyanın herhangi bir yerinde mobil ya da sabit bir telefonu arayabilirler. Aynı şekilde dünyanın herhangi bir yerinden rahatça aranabilirler. Kapsama alanı içinde oldukları sürece GPRS veya EDGE gibi teknolojiler sayesinde veri şebekelerine bağlantı kurabilirler.

## 3.1 Çalışma Prensipleri

Hücresel yapıya sahip olan GSM şebekesi, servis alanını birçok hücrenin tekrarlamasıyla kapsamaktadır. Her hücre belirli bir coğrafi alanı kapsamakta ve her hücrede, abonelerin mobil şebekeye erişimleri için bir ana alıcı-verici istasyon bulunmaktadır. Bu istasyon ileride baz istasyonu (BTS) olarak anılacaktır. Hücrelerde bulunan baz istasyonları gruplar halinde baz istasyonu kontrol merkezlerine (BSC) bağlıdır. Baz istasyonu kontrol merkezleri ise görüşme hatlarının kurulacağı mobil anahtarlama merkezine (MSC) bağlıdır. Bu merkez tüm telefon görüşmelerinin kurulmasını ve görüşme bittiğinde sonlandırılmasını gerçekleştirmektedir.

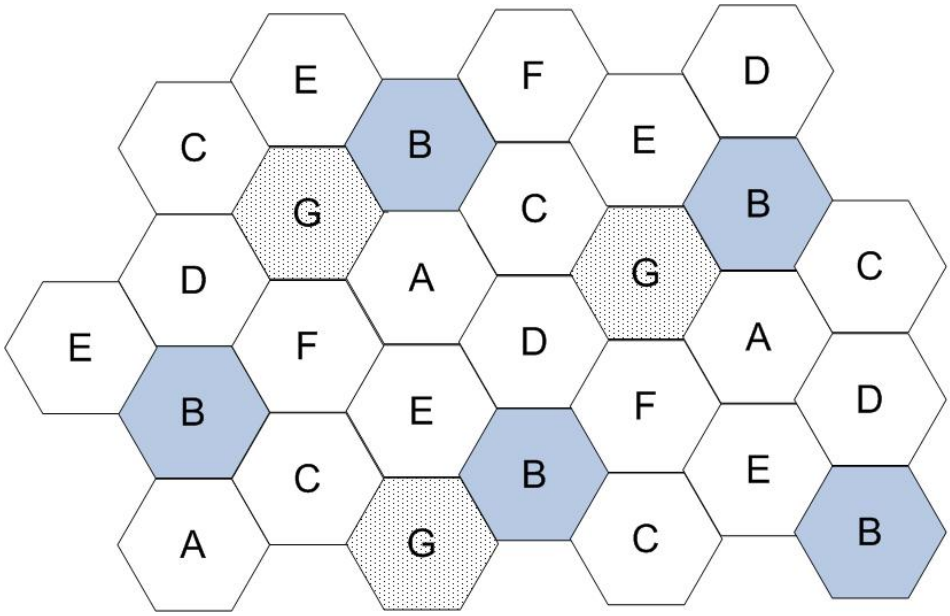
GSM sisteminde evlerimizde kullandığımız alışılageldik sabit telefon yerine, mobil telefon kullanılmaktadır. Mobil telefon pille çalışan ufak bir radyo alıcı verici istasyonu olarak düşünülmelidir. Ufak radyo istasyonu açık olduğu sürece, GSM şebekesinden en güçlü sinyali aldığı baz istasyonu ile devamlı irtibat halindedir. Tez kapsamında özellikle veri iletişimi söz konusu olduğunda, üzerinde abone kimlik modülü (SIM kart) bulunan mobil telefon mobil istasyon olarak anılacaktır.

Mobil telefon ile serbest olarak hareket edildiğinde, sistem aboneyi bulunduğu hücre ve konum alanı olarak takip etmektedir. Telefon görüşmesi sırasında bir hücreden diğerine hareket edildiğinde, sistem otomatik olarak görüşmeyi yeni hücreye yönlendirmektedir. Bu işlem saniyeden çok daha ufak sürelerde geçekleştirildiğinden aboneler tarafından fark edilmemektedir.

### 3.2 Hücresel Sistem

Mobil telefon sistemleri için sınırlayıcı faktör, kullanılan radyo frekans bandıdır ve GSM sisteminde aboneden şebekeye 25 MHz, şebekeden aboneye 25 Mhz'lik frekans bantları kullanılmaktadır. 25 MHz'lik bant GSM şebekelerinde kullanılmak üzere 200KHz'lik kanallara ayrılmaktadır. Bu kanallar ülkede kullanılan GSM operatörlerine dağıtılmaktadır.

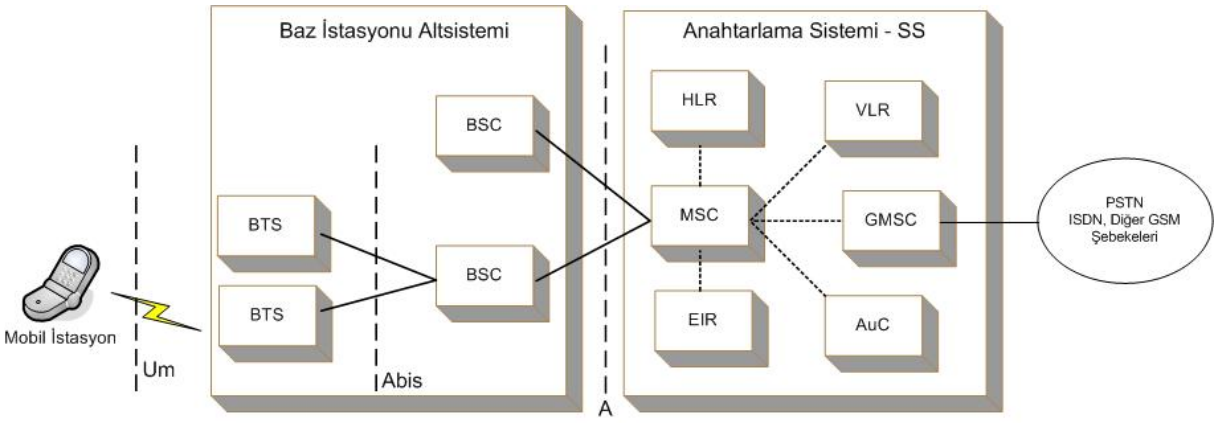
Şehirlerde aynı anda yapılan birçok görüşme için yeterli kapasiteyi sağlamanın tek yolu şebekenin bazı bölümlerinde aynı radyo frekanslarını tekrar kullanmaktır. Bu amaçla sistem, bal peteği gibi birbirine bitişik olarak çalışan hücrelerden oluşmaktadır. Her hücre düşük çıkış gücü ve kısa mesafeli radyo sinyalleri ile haberleşen baz istasyonu ile çalışmaktadır. Bu sayede aynı frekanslar değişik hücrelerde tekrar kullanılmakta ve aynı frekans daha fazla sayıdaki telefon görüşmeleri için kullanılmış olmaktadır (Steele,2001).




**Şekil 3-1 Frekans grupları : A, B, C, D, E, F, G**

Büyük şehirlerde ve aynı anda birçok görüşme yoğunluğu taşıyan bölgelerde hücreler daha küçük ve daha sık yapıda kullanılmaktadır. Hücre küçültme durumunda önemli olan birbirine komşu olan hücrelere farklı frekans kanalı vererek konuşma sırasında aynı verimi sağlamaktır. Şekil 3-1'de görüldüğü gibi bütün frekans grupları birbirine belirli bir uzaklıktadır. Kolay anlaşılabilmesi için B ve G hücreleri renklendirilmiştir.

## 3.3 GSM Şebekesi




**Şekil 3-2 GSM sitem modeli**

Temel olarak GSM, Anahtarlama Sistemi (SS) ve Baz İstasyonu Altsistemi (BSS) olarak iki bölüme ayrılmaktadır. Anahtarlama sistemi (SS) aşağıdaki fonksiyonel üniteleri içermektedir:

- Mobil anahtarlama merkezi (MSC)
- Ziyaretçi abone bilgileri veritabanı (VLR)
- Abone bilgileri kalıcı veritabanı (HLR)
- Doğrulama merkezi (AUC)
- Mobil cihaz kimlik tanımı veritabanı (EIR)
- Mobil anahtarlama merkezi ağ geçidi (GMSC)

Baz istasyonu altsistemi (BSS) ise aşağıdaki fonksiyonel üniteleri içermektedir:

- Baz istasyonu kontrol merkezi (BSC)
- Baz istasyonu (BTS)

GSM sistemi, kapsama alanının tamamını oluşturan radyo hücrelerinin bir araya gelmesi şeklinde gerçekleştirilmiştir. Her hücre, bir grup radyo kanalı üzerinde çalışan bir ana baz istasyonuna (BTS) sahiptir. Bu kanallar, girişimi önlemek amacı ile komşu hücrelerde kullanılan kanallardan farklı olurlar. Bir BTS grubu, bir baz istasyonu kontrol merkezi (BSC) tarafından kontrol edilmektedir. BSC bu gibi fonksiyonları verim ve güç kontrolü şeklinde idare etmektedir. Bir kaç adet baz istasyonu denetleyicisine bir mobil anahtarlama merkezi

(MSC) hizmet vermektedir. MSC'ler mobil anahtarlama merkezi ağ geçidi (GMSC) üzerinden, kamu telefon şebekesi (PSTN), tümleşik hizmetler sayısal ağı (ISDN), kamu mobil telefon şebekesi (PLMN) ve birçok özel şebekelerle yapılan karşılıklı görüşmeleri kontrol etmektedir.

Yukarıda belirtilen ünitelerin tümü bir mobil istasyon ile sabit ağ (örneğin bir PSTN abonesi ) arasındaki konuşmayı taşımak için kullanılmaktadır. Eğer sabit şebekedeki bir abonenin mobil aboneyi arama olasılığı bulunmasaydı daha fazla bir donanıma ihtiyaç olmayacaktı. Sabit şebekeden arayan kişinin mobil istasyonun nerede olduğunu bilmesi pek mümkün değildir. Buna bağlı olarak, ağın içerisinde mobil istasyonu dikkatle takip eden bir takım veri tabanlarına ihtiyaç duyulmaktadır. Bu veri tabanlarından en önemli olanı abone bilgileri kalıcı veritabanıdır (HLR). Bir kişi GSM operatörlerinden birine abone olduğunda o operatörün HLR'sine kaydedilmektedir. HLR aboneye ait bütünleyici servisler ve doğrulama parametreleri gibi bilgileri içermektedir. Bundan başka mobil istasyonun yerleşimi ile ilgili bilgiler yani mobil istasyonun o anda hangi MSC bölgesinde bulunduğu hakkında bilgiler bulunmaktadır. Bu bilgi mobil istasyon hareket ettikçe değişmektedir. Mobil istasyon kendine ilişkin HLR'ye MSC/VLR üzerinden arayan kişilerle görüşme olanağını sağlamak amacı ile yerleşim bilgilerini göndermektedir (Steele,2001).

Abonenin şebekeye girişinde doğrulanması için doğrulama merkezi (AuC) adı verilen bir ünite HLR ile irtibatlandırılmıştır. AuC'nin işlevi, güvenlik nedeni ile kullanılan doğrulama parametrelerini ve şifreleme anahtarlarını HLR'ye ulaştırmaktır.

Ziyaretçi abone bilgileri veritabanı (VLR) o sırada MSC bölgesinde bulunan tüm mobil istasyonlar ile ilgili bilgileri içeren bir veri tabanıdır. Bir mobil istasyon yeni bir MSC bölgesine girer girmez, o MSC'ye bağlı VLR, HLR'den mobil istasyon ile ilgili bilgi istemektedir. Bu şekilde mobil istasyon daha sonra bir görüşme yapmak istediğinde, VLR her defasında HLR'ye başvurmak zorunda kalmaksızın görüşmenin sağlanması için gerekli tüm bilgiye sahip olmaktadır. VLR aynı zamanda mobil istasyonun MSC içerisindeki yerleşimi ile ilgili daha fazla ve kesin bilgi içermektedir.

Eğer sabit şebekedeki (PSTN) bir kimse bir GSM abonesi ile görüşmek isterse, PSTN'deki telefon santrali görüşmeyi geçit fonksiyonu adlı bir fonksiyonla donatılmış MSC'ye iletmektedir. Bu MSC mobil anahtarlama merkezi ağ geçidi (GMSC) olarak bilinmekte ve GSM ağındaki MSC'lerden herhangi biri olabilmektedir. GMSC aranan mobil istasyonun yerini bulmak durumundadır. Bu ise mobil istasyonun kayıtlı olduğu HLR'ye başvurularak

yapılmaktadır. HLR cevap olarak o anki MSC bölgesine ilişkin adresi göndermektedir. GMSC aldığı adresi kullanarak çağrıyı ilgili MSC'ye yönlendirmektedir. Görüşme isteği ilgili MSC'ye ulaştığında VLR mobil istasyonun yeri hakkında detaylı bilgiye sahip olduğundan çağrı kurulabilmektedir (Weber,1998).

Mobil istasyonda SIM kartın bulunmadığı durumda mobil istasyon GSM ağına sadece acil çağrı yapmak üzere giriş yapabilmektedir. Eğer abone SIM kartına sahip fakat mobil telefona sahip değilse başka bir mobil telefonu kendi telefonu gibi kullanabilmektedir. Bu durum cihaz çalındığında hırsızın çalıntı mobil telefonu kullanabileceğini veya satabileceğini göstermektedir. Bu sorunun üstesinden gelebilmek için telefonun kendine özel donanım kimliğini içeren bir veri tabanına, mobil cihaz kimlik tanımı veritabanına (EIR) ihtiyaç vardır. EIR bir işaretleşme arayüzü üzerinden MSC'ye bağlanmıştır. Bu arayüz MSC'nin donanım geçerliliğini kontrol etmesini mümkün kılmaktadır. Abonenin doğrulanmasının doğrulama merkezi (AuC) üzerinde bulunan bilgiler ile yapıldığı hatırlanmalıdır.

## 3.4 Temel GSM Kavramları

### 3.4.1 Radyo Altsistemi (RSS)

Radyo alt sistemi baz istasyonundan ve mobil telefondan oluşmaktadır. Bir çok baz istasyonu alt sisteminden (BSS) oluşan GSM şebekesine radyo erişim şebekesi (Radio Access Network-RAN) denilmektedir. Bu altyapı, GSM sistemi üzerinden konuşma ve veri iletimi için kullanılmaktadır.

### 3.4.2 Mobil İstasyon (MS)

Mobil istasyon halk arasında genelde "cep telefonu" olarak bilinmektedir. Mobil istasyon iki bileşenden oluşmaktadır:

- Mobil Telefon - MT
- Abone Kimlik Modülü (SIM kart)

### 3.4.3 Mobil Telefon (MT )

MT tüm teknik fonksiyonları sunan cep telefonundan oluşmaktadır. Bir cep telefonu tek başına konuşma yapabilecek yeterlilikte değildir ve sadece uluslararası **112** ilk yardım numarasına ulaşabilmektedir. Telefon görüşmesi yapabilmesi için bir GSM operatörünün SIM kartına ihtiyacı vardır. Bu kart telefona yerleştirildikten sonra telefonla görüşme

yapılabilmektedir.

### 3.4.4 Radyo Erişim Şebekesi (RAN)

RAN'ın görevi mobil telefondan gelen ve mobil telefona giden sinyalleri GSM şebekesi içinde ve dışında yönlendirici ara birimlere sunmaktır. RAN birden çok baz istasyonunun birleşiminden oluşan şebekenin ismidir. Bir baz istasyonu kontrol merkezleri ve bunlara bağlı baz istasyonlarından oluşmaktadır.

### 3.4.5 Baz İstasyonu Kontrol Merkezi (BSC)

BSC birçok hücrenin ön saha konsantrasyonudur ve ona bağlı hücrelerin sinyallerini düzenlemektedir. BSC hücreler için bir tür veritabanıdır ve bilgileri hücrelerden MSC'ye iletmekten sorumludur.

Görüldüğü gibi BSC yeni bir görüşmeyi boş bir kanala yönlendirmek için tüm hücrelerinin frekans kanallarını ve zaman dilimlerini denetleyip yönetmektedir. MSC bir telefon görüşmesi için bir kanala ihtiyacı olduğunda BSC'yi boş kanal var mı diye sorgulamaktadır. BSC'nin diğer önemli görevi telefon ve baz istasyonun güç denetimini yapmaktır. Kendi hücreleri içindeki aktarma (handover) da BSC'nin görevlerinden birisidir (Steele,2001).

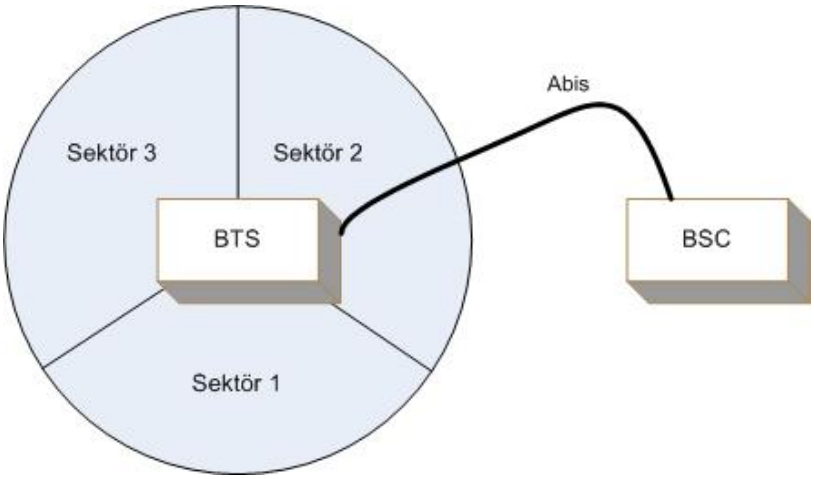
### 3.4.6 Baz İstasyonu (BTS)

BTS bir hücre içindeki haberleşmeden sorumludur. Mobil istasyon ile bağlantıyı sağlamak, verileri yüksek frekansa çevirmek ve TDMA zaman çerçevesini uygulamak BTS'nin görevlerindendir. BTS aboneyle Um arayüzü ve BSC ile de Abis arayüzü üzerinden iletişim kurmaktadır.

### 3.4.7 Sektörleme

Normal durumda BTS'ye hizmet vermesi için 1 değil, sektörlere ayrılmış 3 hücre tahsis edilmektedir;

Bunun için 120º (derece) verici/alıcı karakteristiğine sahip antenler kullanılmaktadır. Böylece 3 hücreyi beslemek için BSC'ye tek bir Abis arayüzü çekmek yeterlidir. Bu şekilde maliyet tasarrufu sağlamak mümkündür. Diğer bir maliyet düşürücü unsurda 3 hücre için 3 antenin tek ayağa monte edilmesidir.




**Şekil 3-3 120 Derece sektörleme**

### 3.4.8 Mobil Anahtarlama Merkezi (MSC)

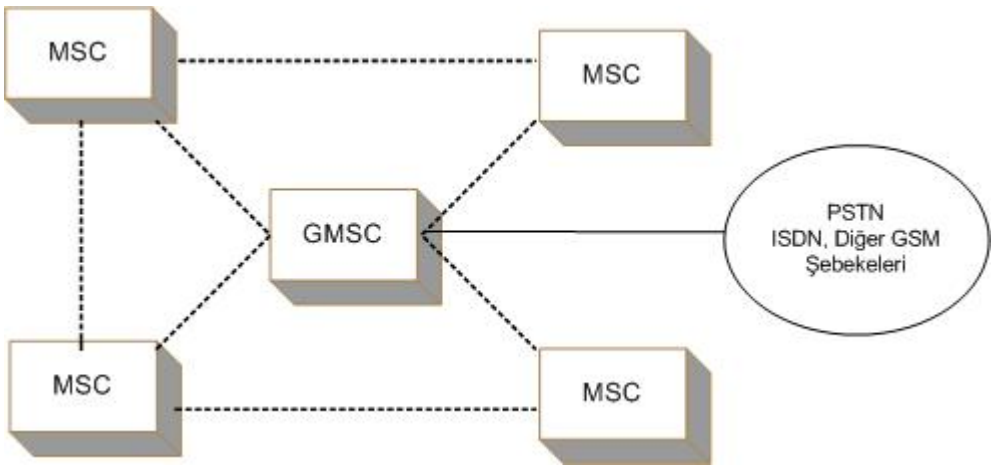
MSC sabit şebekenin santrali ile aynı görevi yapmaktadır. Sabit şebekeden farklı olarak, birbirlerine kablo ile bağlı olan kullanıcılar yerine coğrafi olarak özgür dolaşan mobil kullanıcıların görüşmelerine imkan sağlamaktadır. MSC'nin görevleri aşağıda belirtilmiştir;

- Diğer anahtarlama merkezlerine gerektiğinde bağlantı kurmak
- Diğer şebekelere bağlantı kurmak (sabit şebeke ve mobil şebeke)
- Devre anahtarlamalı hizmetler için serbest hareketlilik yönetimi (MM) sağlamak
- Servis hizmetlerinin yüklenmesini yapmak
- Kullanıcıların VLR'ye kaydedilmesi
- Dahili veya harici aktarmalarda BSC'ler arası geçişi sağlamak.
- Mobil şebekeyle sabit şebekenin arasında olabilecek yankıları gidermek
- Verilerin modem üstünden PSTN şebekelerine uyumunu sağlamak
- Bağlantı ve sinyallerin idare edilmesini sağlamak
- Sistem verileri, sistem kayıtları, ücretlendirme verilerinin kayıt edilmesini sağlamak

### 3.4.9 Mobil Anahtarlama Merkezi Ağ Geçidi (GMSC)

Mobil anahtarlama merkezi ağ geçidi, mobil anahtarlama merkezi gibi çalışmaktadır. Ayrıca ISDN ve PSTN şebekelerine veya PLMN şebekesine haberleşme için gereken fonksiyonları

da sunmaktadır. Aynı anda GMSC kendi GSM şebekesi ve diğer şebekelerin arasında giriş ve çıkış kapısı olarak çalışmaktadır. GMSC'nin görevlerinden bir tanesi gelen çağrının telefon numarasında (MSISDN numarası - Mobil istasyon uluslararası sayısal servis şebekesi numarası ) iletilen verileri veritabanlarının yardımıyla (HLR ve VLR) aranan mobil kullanıcının şebekesine iletmektir. Dışarıdan gelen çağrılarda mobil istasyonun bulunduğu hücreye doğru giden çağrı için ilk adımı GMSC atmaktadır.



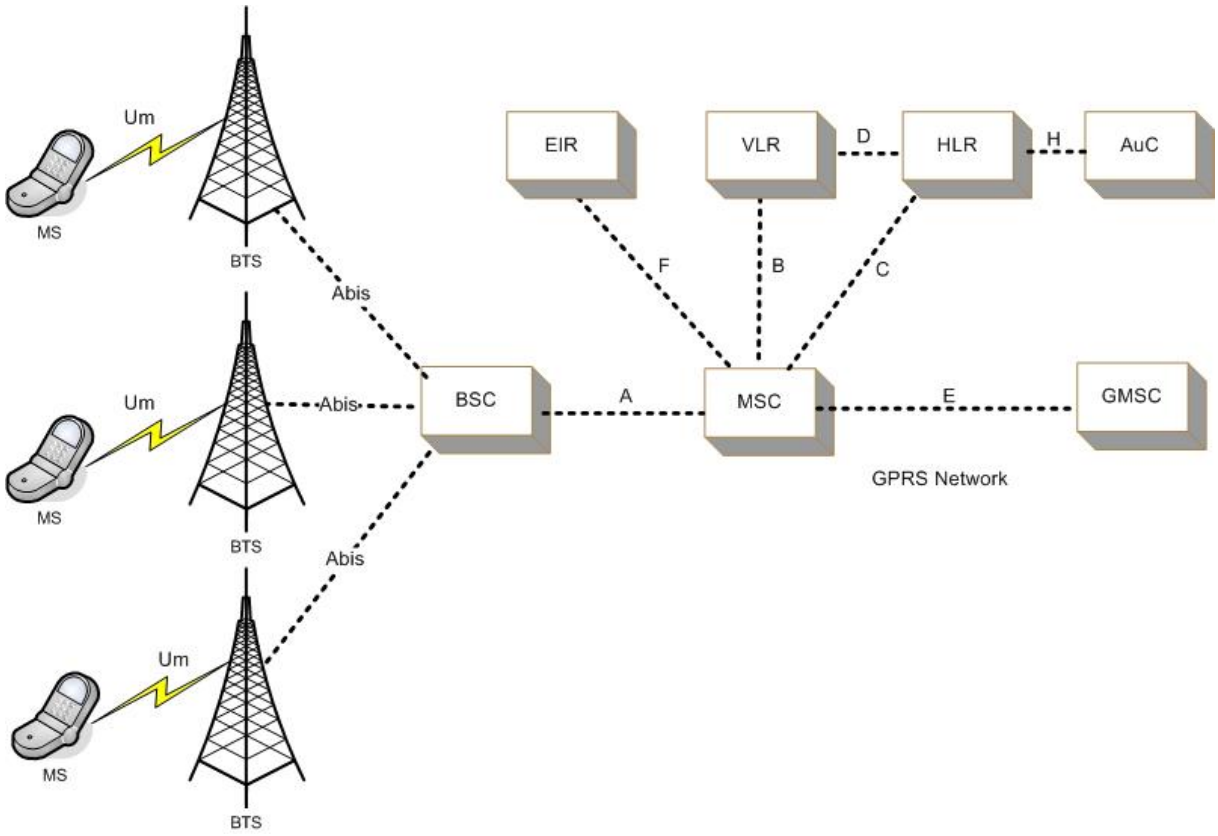

**Şekil 3-4 GSM sistemi PSTN bağlantısı**

MSISDN numarası şebekeden şebekeye değişebilmektedir. Şebekenin kendi GMSC'si MSISDN numarasının bileşenini tanımakta ve HLR'yi serbest hareketlilik yönetimi (MM) için gereken bilgileri almak üzere yönlendirmektedir.

### 3.4.10 Abone Bilgileri Kalıcı Veritabanı (HLR)

HLR, GSM mimarisinin merkezinde kurulmuş bir veri bankasıdır. MSC, HLR'ye C arayüzü üzerinden MAP (Mobil uygulama kısmı) protokolü ile sinyalleşme sistemi 7'yi kullanarak (SS7) ulaşmaktadır. Sinyalleşme sistemi 7 şebeke bileşenleri arasında mesaj aktarımı için kullanılan bir sinyalleşme standardıdır. HLR aynı zamanda ziyaretçi abone bilgileri veritabanına D arayüzü ile bağlıdır. HLR, bu arayüz üzerinden VLR'ye güvenlik verileri sağlamaktadır. HLR şebekenin tüm kullanıcılarının daimi verilerinin ve bazı geçici verilerinin kayıtlı olduğu veritabanıdır. Sözü edilen arayüzler Şekil 3-5'te gösterilmiştir (Sanders,2003).

HLR yoğun veri işleyen bir veritabanı olduğu için donanımı genelde aynı yerde bulunan birçok modülden oluşmaktadır. Her HLR modülüne bir numara verilmekte ve her HLR modülü alt parçalara bölünüp numaralandırılmaktadır. Bu HLR numaraları hem MSISDN hem de uluslararası mobil abone numarasında (IMSI) bulunmaktadır.




**Şekil 3-5 GSM arayüzleri**

### 3.4.11 Ziyaretçi Abone Bilgileri Veritabanı (VLR)

Bir veritabanı olan VLR mobil kullanıcıların geçici verilerini kayıt etmekle görevlidir. Sürekli dolaşım halinde bulunan mobil abonelerin yönetimi, serbest hareketlilik yönetimi ile sağlanmaktadır. Serbest hareketlilik yönetimi mobil istasyonların şebeke içerisindeki yerlerini ilgili veritabanlarında doğru olarak tutmak üzere kullanılan bir prosedürdür. Bu geçici veriler bir yandan serbest hareketlilik yönetimi için, diğer yandan da güvenlik fonksiyonları için kullanılmaktadır. MSC ile VLR birbirleriyle yoğun şekilde veri alış verişi yaptığından şebekede bulunan her MSC'de kendine ait bir VLR bulunmaktadır. Böylece MSC ve VLR bütünleşik biçimde hizmet vermektedir (Yousef,2004).

MSC ile VLR arasında bulunan arayüz B arayüzü olarak adlandırılmaktadır. VLR'nin gerektiğinde HLR' de kayıtlı bilgilere ulaşabilmesi için VLR ile HLR arasında bir bağlantı vardır. Bir cep telefonu birkaç gün kapalı tutulursa bu telefona ait bilgiler VLR'den silinmektedir. Telefonun yeniden açılışında VLR'de yeni bir kayıt açılmaktadır. Kayıt için gerekli bilgilerin büyük bir bölümü HLR ve AuC'den alınmaktadır. HLR burada MSC tarafından hangi servislerin uygulanacağını ve hangilerinin uygulanmayacağını bildiren verileri sunmaktadır. Bunun için VLR ve HLR, D arayüzünden sürekli iletişim halindedir.

Aşağıda VLR üzerinde kayıt edilen önemli veriler sıralanmıştır.

- Mobil abone geçici kimliği (TMSI)
- Konum alanı belirteci (LAI)
- Doğrulama merkezinden alınan güvenlik verileri (RAND/ SRES ve Kc)
- Desteklenen servislerin verileri
- Cep telefonunun durum bilgisi (aktif, pasif, meşgul)
- Mobil istasyon uluslararası sayısal servis şebekesi (MSISDN) numarası
- Uluslararası mobil abone numarası (IMSI numarası)
- Mobil istasyon dolaşım numarası (MSRN)

TMSI ve LAI numaraları çağrı bağlantısını kurmak ve kullanıcıya ulaşmak için gerekmektedir. LAI mobil kullanıcının BSS'nin (BSC'nin yönetim bölgesi) hangi hücre grubunda bulunduğunu tarif etmektedir. Bu hücre gurubuna konum alanı (LA) denilmektedir. Bir kullanıcının o an hangi hücrede bulunduğu değil, hangi konum alanında bulunduğu kayıt edilmektedir. Bunun avantajı abonenin telefonu pasif olduğu sürece aynı konum alanında bulunursa VLR'de konum güncellemesine ihtiyaç bulunmamasıdır. Böylece GSM şebekesinde sinyal tasarrufu sağlanmaktadır. TMSI numarası mobil telefonun şebekeye erişmesi sırasında IMSI numarasının görünmemesi amacıyla kullanılmaktadır

Güvenlik verileri kullanıcının tanımlanması ve iletişim sırasında veri şifrelemesi yapmak için gerekmektedir. GSM şebekesinde mobil telefonun sayısal imzasının oluşturulması için A3, şifreleme anahtarının oluşturulması için A8 isimli algoritmalar kullanılmaktadır. Bu algoritmalar şebeke tarafında doğrulama merkezinde ve abone tarafında SIM kart üzerinde çalışmaktadır. Doğrulama merkezinde ayrıca abonenin SIM kartı üzerinde Ki kişisel kimlik anahtarı bulunmaktadır. Bir abonenin doğrulanması mobil istasyonun imzasının (SRES) şebeke tarafında karşılaştırılması ile yapılmaktadır. Bu imzanın oluşturulması için doğrulama merkezi RAND isminde rastgele bir sayı üretmekte ve mobil istasyona iletmektedir. Şifreleme sırasında kullanılacak anahtarın (Kc) üretilmesinde de aynı rastgele sayı (RAND) kullanılmaktadır. RAND, SRES ve Kc üçlüsüne GSM sisteminde üçüz denilmektedir (Yousef, 2004). Bu kavramlar GPRS güvenlik prosedürleri kısmında ayrıca ele alınacaktır. GSM ve GPRS sisteminde kullanılan A3 ve A8 algoritmaları aynı algoritmalardır.

Mobil istasyon uluslararası sayısal servis şebekesi (MSISDN) numarası telefonun tuşları kullanılarak girilen numaradır. Örnek olarak +90 532 1234567 numarası alınırsa +90 Türkiye'nin uluslararası alan kodudur, 532 "Türkcell" şebekesinin alan kodu, 12 ilgili HLR'yi gösteren numara ve 34567 aranılmış kullanıcının HLR bilgilerinin hangi kayıt yerinde bulunduğunu gösteren numaradır.

Uluslararası mobil abone numarası (IMSI) uluslararası normlara uygun olup GSM kullanıcısının dünyanın her yerinde tanımlanmasını sağlamaktadır. Bu özellikle uluslararası dolaşım için önem arz etmektedir. Örnek IMSI numarası olarak 286 01 20 123456 alınırsa 286 numaranın Türkiye'ye ait olduğunu, 01 "Türkcell" şebekesinde bulunduğunu, 20 hangi HLR'de kayıtlı olduğunu belirtmektedir. 123456 ise mobil istasyon kimlik numarasıdır (MSIN).

Mobil istasyon dolaşım numarası (MSRN) aktarılan aboneye aramanın kurulması süresince atanan geçici bir numaradır. MSRN numarası sabit şebekeden gelen bir çağrının doğru coğrafi MSC'ye yönlendirilmesini sağlar. Coğrafi MSC dünya üzerinde GSM şebekesi olan her hangi bir yerde olabilmektedir.

# 4. GPRS SİSTEMİ

Bu bölümde GPRS sisteminin genel mimarisi ve GPRS hizmeti verebilmek için gerekli bileşenler tanıtılacaktır.

## 4.1 Tanım

GPRS, mobil kullanıcılara GSM şebekesi üzerinden herhangi bir zamanda ve herhangi bir yerden veri ağlarına ulaşma hizmeti sağlamaktadır. GPRS sistemi, devre anahtarlamalı GSM sistemi üzerinde paket anahtarlamalı olarak çalışarak şebekenin ve radyo kaynaklarının etkin kullanımını sağlamaktadır. GPRS servisi verebilmek için şebeke üzerinde yeni radyo kanalları tanımlanmakta ve bu kanalların abonelere atanması ihtiyaca göre dinamik olarak yapılmaktadır. Haberleşmede kullanılan her bir TDMA çerçevesindeki 1–8 arası radyo arayüzü zaman kanalları aktif kullanıcılar tarafından kullanılabilmekte, bu kanallar konuşma ve veri servisleri arasında dinamik olarak paylaşılmaktadır(Sanders,2003). Bir zaman kanalı ile ulaşılabilecek en yüksek hız 21.4 kbit/sn'dir. Bir abonenin bütün zaman kanallarını aynı anda kullanması durumunda erişebileceği maksimum teorik hız 171.2 kbit/sn olmaktadır.

GPRS, aşağıdaki karakteristiklere sahip uygulamalar için şebeke kaynaklarının verimli ve ekonomik kullanımına olanak sağlamaktadır;

- Aralıklı, periyodik olmayan (örneğin patlamalı) veri iletimi

Örnek: Internet üzerinden mail göndermek veya almak.

- Küçük veri miktarlarının sık iletimi

Örnek: Internet (Web) sitelerinin ziyareti.

- Büyük veri miktarlarının sık olmayan iletimi

Örnek: Büyük boyutta dosya indirme veya yükleme işlemi.

## 4.2 GPRS Uygulamaları

GPRS için mümkün olan uygulamalar bir diz üstü bilgisayardaki haberleşme imkanlarından (Örn: Internet) düşük iletim hızlı özel uygulamalara (Örn: sahadan veri toplama) kadar yayılabilmektedir. Bazı uygulamalar zaten devre anahtarlamalı GSM veri servisleri ile kullanılmaktadır, fakat bu servisler GPRS kullanımı ile gerçekleştirildiğinde daha ekonomik hale gelmektedir. Bu tür bir haberleşmeye en tipik örnek kredi kartı ile yapılan ödemelerde provizyon alımı için yapılan haberleşmedir. Çok sık provizyon alınması gereken iş yerlerinde telefon maliyetleri çok yüksek çıkabilmektedir. Bu işlemin GPRS destekli cihazlar ile GPRS

şebekesi üzerinden paket anahtarlamalı olarak yapılması önemli ölçüde tasarruf sağlamaktadır.

Bir diğer önemli mobil uygulama uzak ofis (remote office) çalışmalarıdır. Günümüz iş dünyasının gereği olarak çalışanların her nerede olurlarsa olsunlar kurum ağlarına bağlanarak çalışabilme ihtiyacı vardır. GPRS gibi teknolojilerden önce bu ihtiyaç kiralık hat veya internet üzerinden yapılan sanal özel ağ bağlantıları (VPN) ile yapılabilmekteydi. GPRS sayesinde kurum çalışanları yer bağımsız olarak kurum ağlarına bağlanabilir duruma gelmiş oldular. Yer bağımsız olarak kurum ağına bağlanma imkanı sahada satış yapan çalışanların stok veya kuruma özel bilgileri anında görebilmesine ve daha sağlıklı bir satış yapabilmesine imkan tanımış oldu.

GPRS şebekesine bir defa bağlantı kurulması ve bir daha bağlantı kurma ihtiyacı olmaması nedeni ile kurum ağından veya internet üzerinden küçük dosya transferi gerektiğinde zaman kaybedilmemekte ve ücretlendirmenin süre yerine veri miktarı üzerinden olması nedeni ile maliyet avantajı sağlanmaktadır.

Internet üzerindeki adreslerin ziyaretinde genelde transfer edilen veri, sayfa isteğine ait paketler iken, geri dönen veri istek yapılan sayfanın kendisidir. Bir sayfa geldiğinde bir sonraki sayfa isteğine kadar herhangi bir haberleşme olmamaktadır. GPRS sisteminde ücretlendirmenin iletilen ve alınan veriye göre yapılmasından dolayı önemli bir maliyet avantajı sağlanmaktadır.

GPRS küçük veri miktarlarının sık olmayan iletimini gerçekleştiren uygulamalar için büyük bir pazar oluşturmaktadır. Bu tip haberleşme imkanlarından yararlanacak pek çok cihaz vardır. Hırsız alarmları ve periyodik istatistiksel hata bildirimleri yapan sistemler GPRS vericisi kullanarak çalışabilmektedir. GPRS mobil bir servis olduğu için cihaz mobil veya sabit olabilmektedir.

Elektronik ticaret ve bankacılık uygulamaları GPRS servisinin kullanıldığı diğer uygulamalara örnek olarak verilebilir. GPRS sayesinde internet üzerinden gerçekleştirilen elektronik ticaret işlemlerini mobil olarak yapmak mümkün olmuştur. Aynı biçimde bankacılık işlemleri de yer bağımsız olarak bankaların internet siteleri üzerinden yapılabilmektedir.

Fotoğraf, resim, statik internet sayfaları gibi hareketsiz görüntüler sabit telefon şebekelerinde olduğu gibi mobil telefon şebekeleri üzerinden de alınıp gönderilebilmektedir. Bu durum,

GPRS cihazına bağlanmış bir sayısal kameradan bir internet sitesine görüntüleri göndermek suretiyle mümkün olmaktadır.

GPRS sistemi son zamanlarda mobil saha satış otomasyonu, mobil veri toplama, mobil ürün dağıtım yönetimi ve mobil bilgi servisleri gibi alanlarda kullanılmaya başlanmıştır. Bu sektörlerde iş yapan firmalar GPRS kullanımı sayesinde aşağıdaki avantajları elde edebilmektedir;

- Yer bağımsız haberleşme nedeni ile iş süreçleri hızlanmaktadır
- Saha ile merkez arasındaki anlık bütünleştirme ile iş akış süreçleri hızlandığı için verimlilik artmaktadır.
- Telefon ve faks trafiğini azaltarak tasarruf sağlamaktadır.
- Anlık stok paylaşımı ile daha etkin satış ve daha iyi stok yönetimi sağlamaktadır.
- En önemlisi müşteri memnuniyeti ve rekabet avantajı sağlamaktadır.

Sayılan bu uygulamalara ek olarak ev otomasyonu, mobil reklam, anlık yer takibi, beyaz eşyaların internet'e bağlı olması gibi daha birçok uygulama saymak mümkündür.

### 4.3 GPRS Kodlama Teknikleri

Bu bölümde GPRS üzerinden gerçekleşen veri transferi detaylandırılacaktır. Bilindiği üzere GSM sistemi, her bir taşıyıcı frekans için 8 adet zaman kanalına sahiptir. Konuşma sırasında bu kanallardan bir tanesi mobil istasyona atanır ve konuşma bitinceye kadar mobil istasyon tarafından kullanılır. GSM şebekesi üzerinden devre anahtarlamalı veri aktarımı içinde aynı durum söz konusudur. Mobil istasyon veri aktarımı için bir adet zaman kanalına sahiptir. Bu zaman kanalının hızı gerçekte 21.8 kbit/sn'dir. Fakat transfer edilen verinin doğru ve tam biçimde transfer edildiğinden emin olmak için transfer edilen verinin bir kopyası başka zaman kanalları tarafından iletilir. Sonuçta her zaman kanalı kendisine ve diğer zaman kanallarına ait yedek verinin iletimini gerçekleştirir. Bu çalışma biçimi devre anahtarlamalı veri aktarımı hızını 9.6kbit/sn hızına düşürmektedir (Sanders,2003).

GSM şebekesinden yüksek veri hızlarına ulaşmanın bir yolu gönderilen net veri miktarının birden fazla zaman kanalı kullanılarak arttırılmasıdır. Yüksek veri hızına ulaşmak için bir diğer yol ise yeni bir kodlama tekniği kullanmaktır. Bu tekniğin daha fazla orijinal veri gönderip daha az yedek veri göndermesi, kısacası daha az güvenilirlik ile yüksek veri

hızlarına imkan tanıması beklenir.

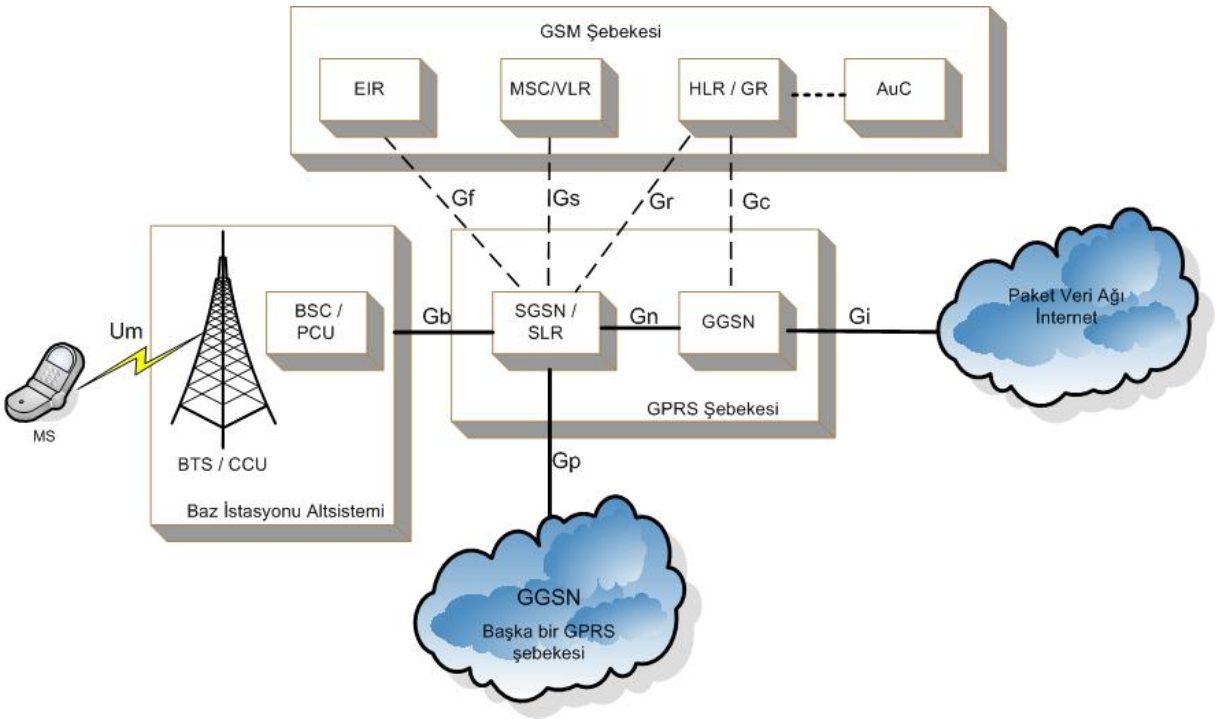
Yukarıda sayılan teknikler GSM şebekesinde uygulanmıştır ve sonuçları HSCSD olarak bilinmektedir. HSCSD ile bir zaman kanalı üzerinden 14.4 kbit/sn veri aktarmak mümkündür. Sekiz zaman kanalının beraber kullanımı durumunda 8x14.4 kbit/sn (115.2 kbit/sn) hıza ulaşılması beklenir. Fakat veri iletimi sırasında GSM şebekesinin klasik düğümleri üzerinden geçildiğinden (BTS→BSC→MSC→…) ve mobil anahtarlama merkezinin (MSC) her bir bağlantı için 64 kbit/sn'den daha yüksek bir hıza izin vermemesinden dolayı HSCSD pratik olarak 57.6 kbit/sn hızında sınırlanmıştır. Bu hız için HSCSD dört zaman kanalı kullanmaktadır (Candan,2002).

GPRS sistemi de yüksek veri hızlarına ulaşabilmek için HSCSD'nin kullandığı teknikleri kullanmaktadır. Bunlara ek olarak sekiz zaman kanalının tamamını bir oturum için kullanabilmekte ve her bir zaman kanalı üzerinden gönderebileceği veri miktarını güvenilirlikten ödün vererek 21.4 kbit/sn hızına çıkarmaktadır.

GPRS sistemi, tasarımı gereği hava arayüzünü ve hava arayüzünün iletim kalitesine olan etkisini dikkate almaktadır. Hava arayüzünün iyi iletim karakteristiği gösterdiği durumlarda çok düşük yeniden gönderme oranı yeterli olmaktadır. Mobil istasyonun baz istasyona olan uzaklığı, haberleşme ortamının durumu hava arayüzü üzerinden gönderilen verinin düzgün biçimde yerine ulaşıp ulaşmadığını etkileyen unsurlardandır. Sonuç olarak GPRS şebekesinde farklı durumlarda kullanılmak üzere dört farklı kodlama tekniği tasarlanmıştır. Kodlama teknikleri CS–1 (Coding Scheme-1), CS-2, CS-3 ve CS-4 olarak adlandırılmaktadır. Bu tekniklerden CS–1 net olarak 9.05 kbit/sn iletim hızına sahiptir. Bu hız devre anahtarlamalı veri iletim hızından (9.6 kbit/sn) bile daha düşüktür. CS–1 kodlama tekniği kodlama teknikleri arasında en sağlam olan tekniktir. Çok kötü hava şartlarında bile kullandığı yüksek yedekli konvolüsyon tekniği ile iletişim sağlayabilmektedir. CS–2, CS–3 ve CS–4 kodlama teknikleri sırası ile 13.4 kbit/sn, 15.6 kbit/sn ve 21.4 kbit/sn hızlarına sahiptir. Çıkılabilecek maksimum veri iletim hızının 21.8 kbit/sn olması nedeni ile CS–4 kodlama tekniğinin hiçbir güvenilirlik sunmadığı anlaşılmalıdır. Bu nedenle CS–4 kodlama tekniği hava arayüzünün mükemmele yakın olduğu durumlarda veya abonenin baz istasyonuna çok yakın ve durağan ya da yavaş hareketli olduğu durumlarda kullanılır (Sanders,2003).

## 4.4 GPRS Mimarisi

Devre anahtarlamalı GSM şebekesi üzerinden paket anahtarlamalı biçimde haberleşebilmek için GSM şebekesine kanal kodlama birimi (CCU), paket kontrol birimi (PCU), GPRS servis düğümü (SGSN), SGSN konum veritabanı (SLR), ağ geçidi GPRS destek düğümü (GGSN) ve GPRS veritabanı (GR) eklenmektedir (Şekil 4-1).




**Şekil 4-1GPRS Mimarisi**

### 4.4.1 CCU (Kanal kodlama birimi)

Kanal kodlama birimi, kanal kodlama tekniklerini (CS 1-4) kullanarak mobil istasyonun şebeke ile haberleşmesini sağlayan birimdir. Kanal kodlama birimi her zaman baz istasyonu üzerinde gerçeklenmektedir.

### 4.4.2 PCU (Paket kontrol birimi)

Paket kontrol birimi, kanal erişim kontrolü, trafik ve güç kontrolü, paket veri birimlerinin (PDU) parçalanması / yeniden birleştirilmesi ve paket veri kanallarının kontrolü görevlerini yerine getirmektedir. Bu birim BTS, BSC veya SGSN' de gerçeklenmektedir.

### 4.4.3 SGSN (GPRS servis düğümü) ve SLR (SGSN konum veritabanı)

SGSN bünyesinde SLR isimli bir veritabanı bulunmakta ve abone ile ilgili bilgiler bu veritabanında tutulmaktadır. GSM mimarisinde bulunan MSC/VLR ikilisi GPRS sisteminde SGSN/SLR ikilisine karşılık düşmektedir.

**SGSN Fonksiyonları;**

- Belirli bir alan içerisindeki bütün mobil istasyonlara hizmet verir.
- Konum yönetimi yapar. Mobil istasyonun yer bilgisini tutar.
- Doğrulama kontrolü yapar. Mobil istasyonun GPRS hizmetine erişme hakkı olup olmadığını kontrol eder.
- Mobil istasyon ile GPRS şebekesi arasında mantıksal bağlantı kurulmasını sağlar.
- Sisteme bağlanma, kopma, yönlendirme alanı güncellemesi gibi serbest hareketlilik yönetimi fonksiyonlarını yerine getirir.
- Oturumun açılması/sonlandırılması, PDP (Paket veri protokolü) oturum etkinleştirmesi ve iptali gibi oturum yönetimi fonksiyonlarını yerine getirir.
- Paket kontrol ünitesinden gelen veriyi GGSN'e gönderme gibi paket işleme fonksiyonlarını yerine getirir.
- SGSN'ler arası yönlendirme alanı güncellemelerini kontrol eder
- Ücretlendirme verisi toplama görevini yerine getirir.
- Performans ve hata yönetimi gerçekleştirir. Transmisyon anında ortaya çıkan problemlerin tespitini yapar.

### 4.4.4 GGSN (Ağ geçidi GPRS destek düğümü) ve GR (GPRS veritabanı)

Paket veri şebekesi (PDN- En genel anlamda internet) ve GPRS sistemi arasında bulunan ağ geçit cihazıdır. GGSN bir yönlendirici gibi davranmakta ve trafik kontrolü yapmaktadır. GGSN aynı zamanda mobil istasyonun izlenmesini sağlamaktadır. PDN tarafından sadece GGSN görülmekte ve mobil istasyonun hareketliliği iletişimin sürekliliğini etkilememektedir. GPRS veritabanı (GR) GSM şebekesinde bulunan HLR'ın karşılığıdır. GR mobil istasyonların adres bilgilerini ve veri servislerine ait bilgileri tutmaktadır (Sanders,2003).

Mobil istasyon tarafından bakıldığında internet'e erişim için iki önemli adım vardır.

1. GPRS şebekesine bağlanmak. Bu işlem mobil istasyonun CCU ve PCU üzerinden geçerek SGSN'e bağlanmasıdır.

2. SGSN ve GGSN arasında PDP bağlantısının kurulması.

GGSN, GSM şebekesinde bulunan ve başka devre anahtarlamalı sistemlere bağlantıyı sağlayan GMSC'ye karşılık gelmekte ve paket anahtarlamalı dış şebekelere bağlantıyı sağlamaktadır.

**GGSN Fonksiyonları;**

- SGSN'den gelen veriyi dış veri şebekelerine gönderme fonksiyonunu gerçekleştirir.
- PDP oturum etkinleştirmesi ve iptali, belirli bir SGSN'ye bağlantı kurulması veya bırakılması gibi oturum yönetimi fonksiyonlarını yerine getirir.
- GPRS şebekesine giren yeni mobil istasyonlar için DNS ve IP adresi atamalarını yapar.
- Ücretlendirme verisi toplama görevini yerine getirir.
- GPRS şebekesinin kendi bulunduğu bölüm için trafik ölçümü yapar.
- Veri transferi sırasında oluşan problemleri tespit eder. Hata yönetimi gerçekleştirir.

## 4.5 GPRS Arayüzleri

GPRS sistemlerinin arayüzleri, sinyalleşme ve kullanıcı verisi taşıyan arayüzler ile sadece sinyalleşme verisi taşıyan arayüzler olmak üzere iki ana başlık altında incelenmektedir.

### 4.5.1 Sinyalleşme ve kullanıcı verisi taşıyan arayüzler

**Çizelge 4-1 Sinyalleşme ve kullanıcı verisi taşıyan arayüzler**

| Arayüz Adı | Görevi |
|---|---|
| **Gb** | BSC ve SGSN cihazları arasındaki arayüzdür. |
| **Gi** | GGSN ve dış veri şebekesi (PDN) arasındaki arayüzdür. |
| **Gn** | SGSN ve GGSN (veya SGSN ve SGSN) cihazları arasındaki arayüzdür. |
| **Gp** | Gn arayüzü gibidir ancak farklı iki mobil şebeke arasındadır. |
| **Um** | Mobil istasyon ve baz istasyonu arasında bulunan hava arayüzüdür. |

### 4.5.2 Sadece sinyalleşme verisi taşıyan arayüzler

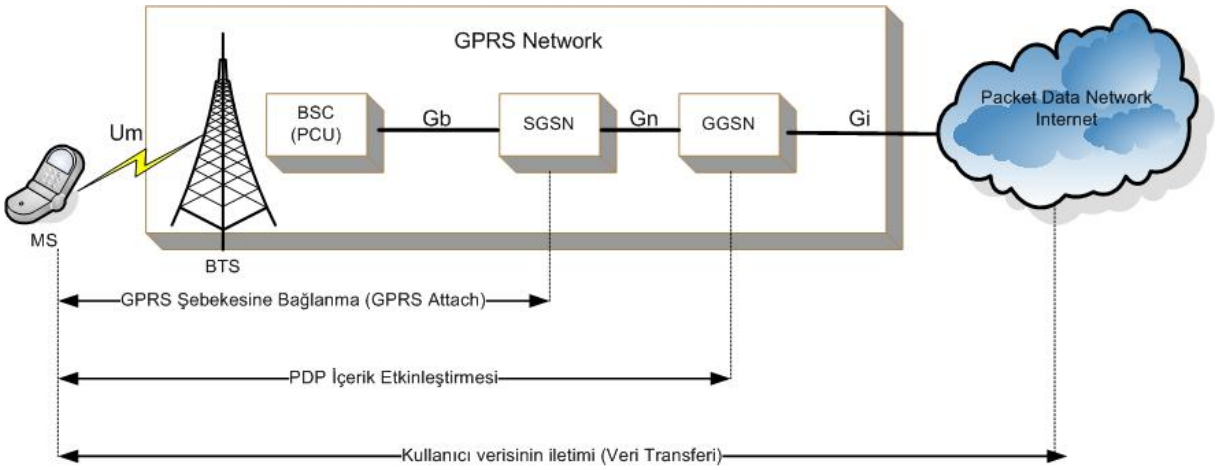
**Çizelge 4-2 Sadece sinyalleşme verisi taşıyan arayüzler**

| Arayüz Adı | Görevi |
|---|---|
| **Gc** | GGSN ve HLR/GR cihazları arasındaki arayüzdür |
| **Gf** | SGSN ve EIR cihazları arasındaki arayüzdür. |
| **Gr** | SGSN ve HLR/GR cihazları arasındaki arayüzdür. |
| **Gs** | SGSN/SLR ve MSC/VLR cihazları arasındaki arayüzdür. |

## 4.6 GPRS Şebekesi Üzerinden Veri İletişimi

Mobil istasyon ile dış veri şebekesi arasında paket alış verişi başlamadan önce GPRS şebekesi üzerinde üç ana işlemin yapılması gereklidir (Sanders,2003).

- İlk olarak mobil istasyonun GPRS şebekesine bağlanması gereklidir. Bu işlem mobil istasyon ve SGSN arasında gerçekleştirilen GPRS bağlanma (GPRS attach) prosedürü ile yerine getirilmektedir (Şekil 4-2).
- GPRS şebekesine bağlantı yapılmasının ardından şebeke içerisinde akacak olan IP paketlerinin yolu tanımlanmalıdır. Bu amaçla mobil istasyon ile SGSN arasında mantıksal bir bağlantı kurulur. Bu bağlantı PDP içerik etkinleştirmesi olarak anılacaktır.
- GPRS bağlantısı gerçekleşip iletilecek IP paketlerinin yolu belirlendikten sonra mobil istasyon tarafından oluşturulan bilgiler şebeke boyunca iletilir.




**Şekil 4-2 GPRS prosedürleri**

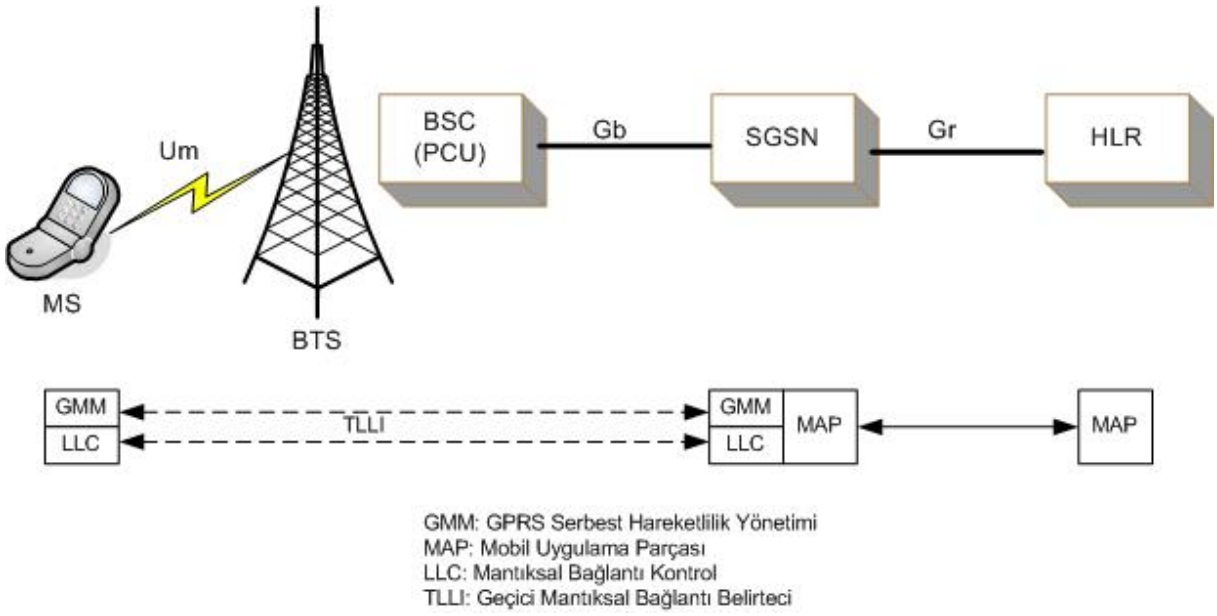
### 4.6.1 GPRS Şebekesine Bağlanma

Bir abone GPRS şebekesinden hizmet alacağı zaman GPRS şebekesine bağlanma prosedürünü çalıştırmaktadır. Bu prosedür sonucunda SGSN, mobil istasyonun GPRS servisini aktif duruma getirdiğini öğrenmektedir. Eğer mobil istasyon daha önce başka bir SGSN'ye bağlı ise, yeni bağlandığı SGSN GPRS veritabanını (GR) güncellemektedir. GR mobil istasyonun GPRS'e özel bilgilerini yeni SGSN'e göndermektedir. GPRS'e özel bu bilgiler kullanılarak mobil istasyon için farklı bir PDP içerik bilgisi oluşturulmaktadır. PDP içerik bilgisi bir mobil istasyon için GPRS veri bağlantısını tanımlamaktadır. Bu bilgiler GR tarafından gönderilmekte ve aşağıdaki bilgileri içermektedir (Sanders,2003);

- Erişim noktası adı (APN): İletişime geçilecek veri şebekesinin mantıksal adı. Örnek: internet
- Servis kalitesi (QoS): İstenen uygulama için gereken öncelikler, gecikmeler ve güvenilirlik ihtiyaçları. Örnek: konuşma, video, internet gezintisi, dosya indirme vb.
- PDP protokolü: Mobil istasyon ve dış veri şebekesi arasında kullanılan protokol. PDP protokolü genellikle IP protokolüdür.
- Mobil istasyonun IP adresi: Eğer mobil istasyon sabit bir IP adresi kullanarak GPRS şebekesine bağlanıyorsa gönderilmektedir.

Bir mobil istasyonun farklı IP şebekelerine bağlantısı için farklı servis kalitesi seviyelerinde birçok PDP içerik bilgisi oluşturulabilir. Ayrıca farklı servisleri farklı servis kalitesi seviyesinde verebilmek için aynı şebekeye birçok erişim noktası adı verilebilir.

Bir mobil istasyon ve SGSN arasındaki GPRS şebekesine bağlanma prosedürü GMM (GPRS serbest hareketlilik yönetimi) protokolü tarafından işletilmektedir (Şekil 4-3).




**Şekil 4-3 GPRS şebekesine bağlanma prosedürü**

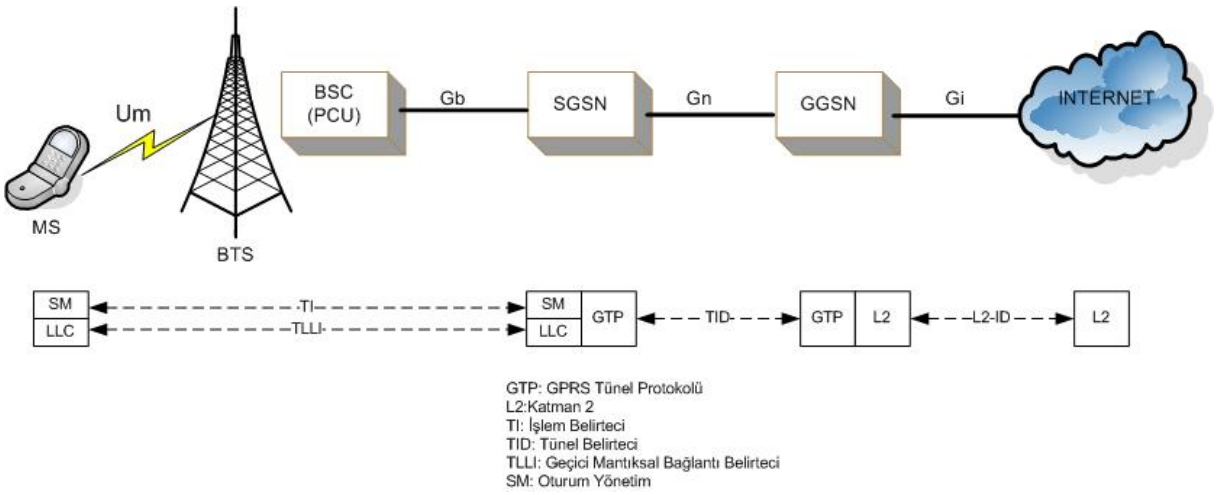
Mobil istasyon ve SGSN arasında bulunan bir diğer önemli protokol mantıksal link kontrolü (LLC) protokolüdür. Bu protokol servis erişim noktası belirteci (SAPI) ve geçici mantıksal bağlantı belirtecini (TLLI) içeren veri bağlantı noktası belirteci (DLCI) ile tanımlanmaktadır. TLLI belirli bir mobil istasyonu ve SAPI servis erişim noktasını (Örn: SNDCP, GMM/SM, veya SMS) tanımlamaktadır. LLC protokolü aynı zamanda mobil istasyon ile SGSN arasında bulunan bağlantının şifrelenmesinden sorumludur. Devre anahtarlamalı olan GSM sisteminde şifreleme sadece mobil istasyon ve BTS arasında yapılmakta iken GPRS şebekesinde mobil istasyon ile SGSN arasında yapılmaktadır. HLR ve SGSN arasındaki Gr arayüzü, GSM şebekesi omurgasındaki sinyalleşme arayüzünün uygulama kaymanı olan MAP protokolüne dayanmaktadır (Sanders,2003).

### 4.6.2 PDP İçerik Etkinleştirmesi

Bir abone GPRS hizmetini kullanmaya başlayacağı zaman şebekeden PDP içerik etkinleştirmesi talep etmektedir. Bu istek aşamasında abone APN ismini ve talep ettiği servis kalitesini bildirmektedir. PDP içerik etkinleştirmesinde hangi protokollerin yer aldığı Şekil 4-4'te görülmektedir.

Bu prosedürün işletimi sonucunda GPRS şebekesi ilgili IP paketlerini nasıl yönlendireceğini öğrenmektedir. Mobil istasyondan GGSN'e olan yol PDP içerik etkinleştirilmesinden sonra

belirlenmiş olmaktadır.




**Şekil 4-4 PDP içerik etkinleştirmesi**

Mobil istasyon ile SGSN arasındaki yolun kurulması oturum yönetimi (SM) protokolünün görevidir. Oturumun tanımlanması amacı ile işlem belirteci (TI) kullanılmaktadır. Oturum yönetimi protokolünün bir diğer görevi PDP etkinleştirmesinin sonlandırılmasıdır.

PDP içerik etkinleştirmesi sonucunda şebeke üzerinden aktarılacak bilgiler SGSN ve GGSN arasında GPRS tünel protokolü (GTP) kullanılarak aktarılmaktadır. Her bir PDP içerik etkinleştirmesinde SGSN ve GGSN arasında GTP protokolünde kullanılmak üzere tünel belirteci (TID) oluşturulmaktadır. Tünel belirteci numarası IMSI (Uluslararası mobil abone numarası) ve NSAPI (Ağ servis noktası belirteci) numaralarından oluşmaktadır. IMSI bir mobil istasyonun sabit numarasıdır ve NSAPI şebeke servisini tanımlamaktadır (Sanders,2003).

GGSN'in ek olarak iki görevi daha vardır. Bunlardan ilki ilgili PDP içeriğine ilişkin doğru fiziksel katman protokolüne (Layer 2) karar vermektir. Bu protokoller Ethernet, Frame Relay veya ATM gibi ikinci katman protokolleri olabilmektedir. İkinci görevi mobil istasyon için bir IP adresi istemek ve bunu mobil istasyona göndermektir.

### 4.6.3 Veri Transferi

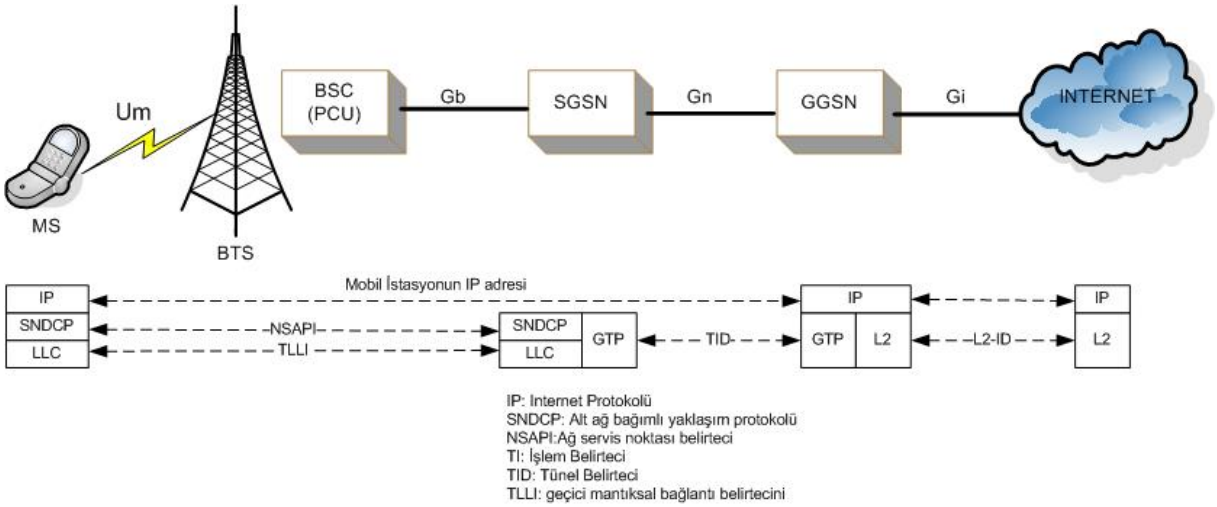
Mobil istasyon tarafından seçilmiş APN için PDP içerik etkinleştirmesi yapıldıktan sonra veri transferi başlamaktadır.

- Mobil istasyon dış IP şebekesinden geçici bir IP adresi alarak haberleşeceği IP şebekesinin bir üyesi olur.

- Mobil istasyon SGSN'e doğru TLLI numarası ile PDP içeriği ise SNDCP katmanında NSAPI numarası ile belirtilir.
- SGSN ve GGSN arasında her bir mobil istasyon ve bu mobil istasyona bağlı içerik etkinleştirmesi TID ile belirtilir.
- GGSN Gi arayüzü üzerinde PDP içeriği için doğru ikinci katman protokolünü kurar.

Bu işlemler sonucunda PDP içeriği üzerinden içeri veya dışarı yönde yönlendirilecek IP paketleri tanımlanmış olmaktadır. Son olarak SGSN, GGSN ile arasında akacak IP paketlerinin hangi TID numarası ile işaretlendiğini, mobil istasyon ile kendisi arasındaki iletişimde hangi TLLI numarasını kullanacağını öğrenmektedir. Dış IP şebekesinin bu olaylardan haberi yoktur. GGSN sadece erişim noktası olarak görünmektedir.

Mobil istasyon ve SGSN arasında veri trafiği başladığında SNDCP protokolü IP paketlerini sıkıştırır ve parçalara (segment) ayırır. Mobil istasyon veya SGSN bu veriyi aldığında SNDCP parçaları (segmentleri) yeniden birleştirir ve IP paketlerini elde etmek için LLC paketlerini açar (Şekil 4-5).




**Şekil 4-5 mantıksal veri transferi**

## 4.7 GPRS Fonksiyonları

Bu bölümde GPRS sisteminin temel çalışma yapısının anlaşılabilmesi için GPRS fonksiyonları anlatılmaktadır. Fonksiyon tanımları için ETSI GSM 03.60 standardı referans alınmıştır.

### 4.7.1 Şebeke Erişim Kontrol Fonksiyonları

Şebeke erişimi bir kullanıcının ilgili hizmete erişebilmek amacı ile haberleşme şebekesine bağlanması anlamına gelmektedir. GPRS şebekesi IP, X.25 gibi birçok protokolü desteklemektedir. GPRS şebekesine erişimde yüksek seviyede gizliliği sağlayabilmek için IMSI veya IMEI (Uluslararası mobil cihaz bilgisi) numaraları kullanılmamaktadır.

#### 4.7.1.1 Kayıt Fonksiyonu

Bir mobil istasyonun şebeke tarafından bilinmesi için şebekeye kayıt olması gereklidir. Başarılı bir kayıt işleminden sonra şebeke abonenin mevcut yönlendirme alanını, IP adresini ve erişim noktası adını (APN) bilmektedir. Şebeke içerisinde bir mobil istasyonun IP adresi abonenin tanımlanmış profili ile ilişkilidir. Bu ilişki statik veya dinamik olabilmektedir. Statik ise GPRS veritabanında (GR) kayıtlıdır, dinamik ise her ihtiyaç duyulduğunda tahsis edilmektedir.

#### 4.7.1.2 Doğrulama ve Yetkilendirme Fonksiyonu

Bu fonksiyon servis talebinde bulunan abonenin doğrulama ve yetkilendirme işlemlerini yapmaktadır. Doğrulama işlemi ile abonenin şebekeye erişim izninin olup olmadığı kontrol edilmektedir. Doğrulama işlemi serbest hareketlilik yönetim fonksiyonları ile birlikte uygulanmaktadır. Yetkilendirme işlemi ile de şebekeye erişim izni olan abonenin hangi şebeke servislerini kullanabileceği belirlenmektedir.

#### 4.7.1.3 Mesaj Perdeleme Fonksiyonu

Mesaj perdeleme yetkisiz mesajları filtreleme amacı ile kullanılmaktadır. Bu fonksiyon bir güvenlik duvarı üzerinde her paket için yapılmalıdır. İstenmeyen bir kaynaktan veya istenmeyen içerikte bir paket geldiğinde basit filtreleme işlemi ile paket imha edilmelidir. Mesaj perdeleme uygulama seviyesinde bulunan zararlı kodlara veya internet ya da iç ağdan gelecek muhtemel saldırılara doğrudan çere bulamamaktadır.

#### 4.7.1.4 Paket Adaptasyon Fonksiyonu

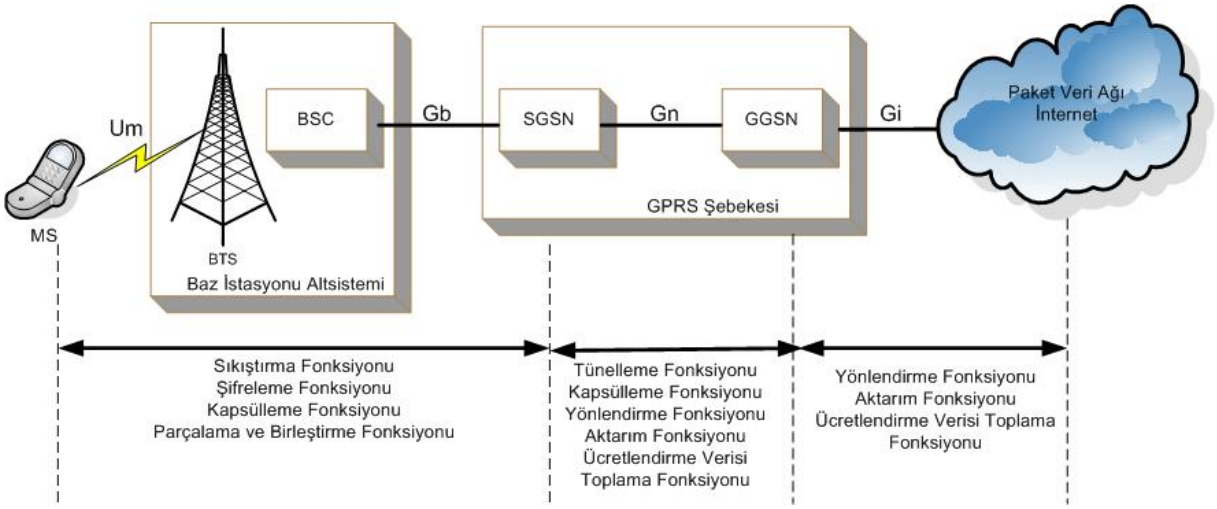
Mobil istasyon genellikle harici bir terminale (örneğin bilgisayar) bağlanarak kullanılmaktadır. Bu harici cihaz ile kendisi arasında veri alışverişi yapılabilmesi için mobil istasyonun çeşitli arayüzleri (örneğin seri arayüz) desteklemesi gereklidir. Mobil istasyon şebeke ile haberleşme sırasında IP protokolü kullanılırken harici cihaz ile mobil istasyonun seri arayüzü üzerinden haberleşme yapabilmektedir. Aradaki geçişi sağlama işlemini paket adaptasyon fonksiyonu gerçekleştirmektedir.

#### 4.7.1.5 Ücretlendirme Verisi Toplama Fonksiyonu

Bu fonksiyon şebeke üzerinden ücretlendirme için gerekli veriyi toplamaktadır. GPRS şebekesinin kullanımına dair ücretlendirme çeşitli modellere göre yapılmaktadır. En yaygın ücretlendirme metodu abonenin transfer ettiği veri miktarına göre yapılan ücretlendirmedir. GPRS şebekesine bağlı aboneler için ücretlendirme verisi SGSN/SLR düğümü tarafından sağlanmaktadır. Diğer tür ücretlendirme metodu dış şebekelerin (örneğin internetin) kullanımına göredir ve farklı kriterler olabilir. Transfer edilen içeriğe göre ücretlendirme bu kriterlere bir örnektir. Dış ağlara ulaşım için ücretlendirme verisini GGSN cihazı toplamaktadır.

### 4.7.2 Paket Yönlendirme ve Transfer Fonksiyonları

Paket yönlendirme, GPRS şebekesi içerisinde mesajların bir noktadan başka bir noktaya transferi amacı ile kullanılmaktadır. Bir noktadan başka bir noktaya belirli düğümler üzerinden geçilerek ulaşılmaktadır. Düğümlerden oluşan bu yola rota denilmektedir. Her rotanın başlangıç düğümü, sıfır veya daha fazla aktarım düğümü ve hedef düğümü vardır. Yönlendirme, GPRS şebekesi içerisinde hangi rotanın kullanılacağının belirlenmesidir. İlgili paket yönlendirme ve transfer fonksiyonları aşağıda açıklanmıştır (Şekil 4-6).




**Şekil 4-6 Paket Yönlendirme ve Transfer Fonksiyonları**

#### 4.7.2.1 Aktarım Fonksiyonu

GPRS şebekesi içerisinde veriyi bir düğümden alıp başka bir düğüme aktaran fonksiyon aktarım fonksiyonudur. Rota üzerindeki ara düğümler tarafından yerine getirilen bir fonksiyondur.

#### 4.7.2.2 Yönlendirme Fonksiyonu

Mesajın hedef adresine bakarak hangi düğüme gönderileceğine karar veren, dolayısı ile mesajın rotasını belirleyen fonksiyondur. Bu fonksiyon GPRS Destek Düğümlerinin (SGSN ve GGSN) temelini oluşturmaktadır.

#### 4.7.2.3 Adres Çevrimi ve Eşleştirme Fonksiyonları

Adres çevrimi bir adresin farklı tipte bir adrese dönüşümünü sağlamaktadır. GPRS şebekesinde üretilen bir mesaj farklı bir şebekeye veya dış bir şebekede üretilen trafik GPRS şebekesine yönlendirilmektedir. Şebeke protokollerinin farklı olması durumunda adres çevrimi gerçekleştirilmektedir. Adres eşleştirme ise bir adresi yönlendirme veya aktarım amaçlı olarak aynı tür başka bir adrese eşleştirmek için kullanılmaktadır.

#### 4.7.2.4 Kapsülleme Fonksiyonu

Kapsülleme fonksiyonu yönlendirilen paketleri yeniden paketlemek amacı ile kullanılmaktadır. Yeni paketleme işlemi ile pakete ek kontrol bilgisi ve yeni adres bilgisi yerleştirilmektedir. Karşı uçta kapsüllemenin tersi işlemi yapılarak orijinal paket yeniden oluşturulmaktadır. Kapsülleme ve kapsülden çıkarma olarak adlandırılabilecek bu fonksiyonlar GPRS destek düğümleri arasında veya SGSN ile mobil istasyon arasında yapılmaktadır.

#### 4.7.2.5 Parçalama ve Birleştirme Fonksiyonu

Şebeke üzerinden gönderilecek veri bir defada gönderilemeyecek kadar büyük olduğunda parçalama ve karşı uçta birleştirme işlemi yapılmaktadır. Parçalama işleminde veri küçük parçalara ayrılmakta ve karşı uçta birleştirme işlemi yapılabilmesi için bir başlık eklenmektedir. Parçalama işlemine bir örnek verecek olursak, IP paketlerinin hava arayüzünden gönderilebilmesi için gerekli işlemi yapan protokol, paketleri küçük parçalara (segment) ayırmaktadır. Bu parçalar LLC çerçevesi olarak adlandırılmaktadır. Daha sonra bu parçalar radyo bloklarına ve radyo blokları da gönderilmek üzere zaman kanallarına ayrılmaktadır. Karşı uçta zaman kanallarında alınan bilgilerden radyo blokları çıkarılmakta ve bu bloklardan yararlanarak LLC çerçeveleri oluşturulmaktadır. LLC çerçevelerinin birleştirilmesi ile de IP paketleri elde edilmektedir

#### 4.7.2.6 Tünel Fonksiyonu

GPRS şebekesi içerisinde kapsüllenmiş paketleri transfer etmek amacı ile kullanılan fonksiyondur. Tünel iki yönlü ve noktadan noktaya bir yoldur. Tünel kurulma aşamasında

tünelin ucunda bulunan düğümler belirtilmektedir. GPRS şebekesi içerisinde SGSN ve GGSN arasında GTP protokolü kullanılarak tünel oluşturulmaktadır.

#### 4.7.2.7 Sıkıştırma Fonksiyonu

Sıkıştırma fonksiyonu mesajları sıkıştırarak bant genişliğinin daha verimli kullanımını sağlamaktadır. IP paketleri parçalanmadan, şifrelenmeden ve iletilmeden önce sıkıştırılmaktadır. Sıkıştırma tekrar eden sıfır ve birlerin minimize edilmesi işlemidir. Bu işlem sonucunda transfer edilecek veri boyutunun düşmesi, fakat karşı uçta orijinal veriye dönüşümün mümkün olması beklenmektedir.

#### 4.7.2.8 Şifreleme Fonksiyonu

Şifreleme fonksiyonu radyo kanalları üzerinden akan kullanıcı verisi ve sinyalleşme trafiğinin gizliliğini ve bütünlüğünü sağlamaktadır. Bu fonksiyon sadece haberleşen uçların bildiği bir bit dizisi ile veriye ait bitlerin kombinasyonunu yapmaktadır. Bu sayede uçlar arasında akan trafiğin gizliliği korunmaktadır. GPRS şebekesinde şifreleme işleminden LLC katmanı sorumludur.

#### 4.7.2.9 Alan Adı Servisi

Mobil istasyon veri ağına ulaşmak istediği zaman ulaşmak isteği ağın adını (APN) SGSN'e göndermektedir. IP haberleşmesinin sağlanabilmesi için APN adının IP adresine dönüştürülmesi gerekmektedir. SGSN, DNS sunucusuna APN adını göndererek IP adresini sormakta ve DNS sunucusunun gönderdiği yanıta (IP adresine) göre iletişime geçmesi gerektiği GGSN'i belirlemektedir.

### 4.7.3 Serbest Hareketlilik Fonksiyonları

Serbest hareketlilik fonksiyonları bir mobil istasyonun PLMN içindeki mevcut yerini izleme amacı ile kullanılmaktadır.

### 4.7.4 Mantıksal Bağlantı Yönetim Fonksiyonları

Mantıksal bağlantı yönetim fonksiyonları mobil istasyon ve PLMN radyo arayüzü arasındaki haberleşme kanalının yönetimi ile ilgilidir. Bu fonksiyonlar mantıksal bağlantı üzerinden akan veri trafiğinin denetimini yapan bağlantının koordinasyonunu sağlamaktadır. Bu fonksiyonlar GPRS şebekesinde SGSN tarafından işletilmektedir.

#### 4.7.4.1 Mantıksal Bağlantı Kurma Fonksiyonu

Mobil istasyonun GPRS servisine erişimi aşamasında mantıksal bağlantı kurulmaktadır. Bu bağlantıyı kuran fonksiyon mantıksal bağlantı kurma fonksiyonudur.

#### 4.7.4.2 Mantıksal Bağlantı Bakım Fonksiyonu

Mantıksal bağlantı bakım fonksiyonu mantıksal bağlantının durumunu ve kontrol bağlantısının durum değişimlerini denetleyen fonksiyondur.

#### 4.7.4.3 Mantıksal Bağlantı Bırakma Fonksiyonu

Mobil istasyonun ilgili GPRS servisine erişim ihtiyacı kalmadığında (oturum kapandığında) mantıksal bağlantı sonlandırılmaktadır. Bu işlemi mantıksal bağlantı bırakma fonksiyonu yerine getirmektedir.

### 4.7.5 Radyo Kaynakları Yönetim Fonksiyonları

Radyo kaynakları yönetim fonksiyonları gerekli radyo haberleşme yollarının ayrımı ve yönetimi ile ilgilidir. GSM radyo kanalları devre anahtarlamalı servisler (ses, veri) ve GPRS arasında paylaşılmaktadır. Bu fonksiyonlar paket kontrol birimi (PCU) tarafından yerine getirilmektedir.

#### 4.7.5.1 Um Yönetim Fonksiyonu

Bu fonksiyon her bir hücre içinde kullanılan fiziksel kanalların yönetimini yapmakta ve GPRS servisi için ayrılacak radyo kanallarının miktarını belirlemektedir. GPRS kullanımı için ayrılan radyo kaynaklarının miktarı yerel kullanıcıların istekleri ve PLMN operatörünün politikasına göre hücreden hücreye değişebilmektedir.

#### 4.7.5.2 Hücre Seçimi Fonksiyonu

Bu fonksiyon bir mobil istasyonun PLMN operatörü ile arasında kurulacak haberleşme bağlantısı için en uygun hücre seçimini gerçekleştirmektedir. Bu işlem yakındaki hücrelerden gelen sinyallerin kalitesini ölçme ve değerlendirmeyi gerektirmektedir. Aynı zamanda aday hücreler içindeki trafik nedeni ile oluşan tıkanıklıkta bir parametre olarak alınmaktadır.

#### 4.7.5.3 Um Veri Transfer Fonksiyonu

Bu fonksiyon mobil istasyon ve BSS arasında kurulan radyo arayüzü üzerinden veri transferi olanağı sağlamaktadır. Aşağıda bu fonksiyonun içerdiği özellikler verilmektedir;

- Radyo kanalı üzerinden erişim sağlama

- Ortak fiziksel radyo kanalları üzerinden paket çoğullaması
- Mobil istasyon içinde paket ayrımının yapılması
- Hata tespiti ve düzeltme
- Akış kontrol prosedürleri

#### 4.7.5.4 Yol Yönetim Fonksiyonu

Bu fonksiyon BSS ve GPRS hizmeti veren düğümler (SGSN ve GGSN) arasındaki haberleşme yolunu yönetmektedir. Bu yolların kurulması ve bırakılması veri trafiğinin miktarına göre dinamik veya her bir hücre içerisinde beklenen maksimum yüke göre statik olabilmektedir.

# 5. KORUNMAYA İHTİYACI OLAN BİLGİLER

**Abone Verisi:** Abonelerin GPRS şebekesi üzerinden transfer ettiği verinin gizliliği, şifreleme gibi teknikler kullanılarak korunmalıdır. Verinin korunma sorumluluğu GPRS operatörününündür ve operatör hem kendi aboneleri hem de başka operatörlerden kendisine gelen ziyaretçi aboneler için gerekli güvenlik tedbirlerini almalıdır. Abone verisine örnek olarak mobil istasyondan kurumsal ağa doğru olan IP paketleri veya aboneye ait kısa mesajlar verilebilir.

**Ücretlendirme Bilgisi:** Ücretlendirme genelde transfer edilen veri üzerinden yapılmaktadır. Bu nedenle kullanıcı tarafından talep edilmemiş verinin mobil istasyona gelmesi engellenmelidir. Ücretlendirme verisinin gizliliği ve bütünlüğü çok önemlidir.

**Sinyalleşme Bilgisi:** GPRS bileşenleri SGSN ve GGSN, GSM sisteminin bileşenleri ile sinyalleşme arayüzleri üzerinden haberleşmektedir. Bunlara ek olarak abone ile dış veri şebekesi arasında veri transferi başlaması için gerekli sinyalleşe aşamalarının başarı ile tamamlanması gereklidir. Bu sebeple GPRS şebekesinin işleyişini temin eden sinyalleşme bilgilerinin korunması gereklidir.

**Abone Bilgisi:** GPRS operatörü hem kendi abonelerinin hem de dolaşım halinde olan başka GPRS operatörlerinin bilgilerini gizli tutmalıdır. Abonenin SIM kartında bulunan anahtarların bir kopyası doğrulama merkezinde (AuC), diğer bilgileri HLR ve VLR veritabanlarında bulunmaktadır. GPRS operatörü bu bilgileri gizli tutmak üzere gerekli güvenlik önlemlerini almalıdır.

**Mobil İstasyon ve SIM Kart Bilgileri:** SIM kart içerisinde tutulan uluslararası mobil abone numarasının (IMSI), Kişisel Kimlik Anahtarının (Ki), Şifreleme Anahtarının (Kc), ilgili anahtarı üretmek için kullanılan A3 ve A8 algoritmalarının, abone telefon defterinin ve abone kısa mesajlarının korunması gereklidir. SIM kartın korunması için mobil istasyon üzerinde bulunan PIN kodu sorma, telefon kilidi gibi güvenlik fonksiyonlarının etkinleştirilmesi gereklidir.

**GPRS Şebekesinin Teknik Bilgileri:** GPRS şebekesinin yapılandırma ve yönetimine dair bilgilerin saldırganların eline geçmesi durumu, yetkisiz bilgilere erişim, ücretsiz hizmet alma, GPRS şebekesinin çalışmasını durdurma, abone oturumlarını dinleme gibi sonuçlar doğurabilmektedir. Bu tür nedenlerle bileşenlerin yapılandırma bilgileri gibi teknik bilgilerin korunması GPRS şebekesi ve aboneler için önemli bir konudur.

# 6. GPRS SİSTEMİNİN POTANSİYEL SALDIRGANLARI

GPRS sisteminin potansiyel saldırganlarını, kötü niyetli internet kullanıcıları, aboneler, altyükleniciler, internet hizmet sağlayıcıları ve iç kullanıcılar olarak sınıflandırmak mümkündür. Aşağıda potansiyel saldırganlar ile ayrıntılar verilmiştir;

- **Kötü niyetli internet kullanıcıları (Hackers/Crackers)**

Bilgi hırsızlığı, kendi kabiliyetlerini gösterme veya GPRS sistemine zarar vermek için çalışan kişilerce yapılır. GPRS şebekesinin doğrudan internet bağlantısı olması nedeni ile internet için var olan tehditler GPRS şebekesi için de tehdit unsurudur. Internet üzerinden gerçekleştirilen saldırırılar doğrudan GPRS kullanıcılarını, GPRS hizmetini kullanan kurumları veya GPRS operatörünü etkilemektedir.

- **Aboneler**

GPRS sisteminin aboneleri şebekenin bir parçasıdır. Aboneler kendilerine tanınan haklardan yaralanarak GPRS şebekesine veya diğer abonelere zarar verebilir. Abonelerden gelebilecek muhtemel saldırılardan korunmak için, GPRS operatörleri abonelerin sadece belirli servis ve cihazlara erişimine izin vermelidir.

**Altyükleniciler**

GPRS operatörü, şebeke içerisinde kullanılan yazılımların güncellenmesi, cihazların bakımı gibi bazı işleri altyüklenicilere yaptırabilirler. Bu tür durumlarda altyüklenici firma çalışanları genellikle farkında olmadan GPRS sistemine zarar verirler. Dikkatsiz yazılım güncellemeleri ve izin alınmadan yapılan cihaz bakımları zarar vermesi muhtemel iki örnektir.

- **Internet hizmet sağlayıcıları**

GPRS operatörleri, abonelerine internet bağlantısı sağlayabilmek için internet hizmet sağlayıcılarından yararlanırlar. Internet hizmet sağlayıcılarının iç ağları, doğrudan GPRS sistemine bağlıdır. Bu nedenle GPRS operatörleri, saldırı riskini mümkün olan en az seviyeye çekmek üzere güvenlik duvarı, erişim kontrol listeleri gibi gerekli önlemleri almalıdır.

- **İç kullanıcılar**

Sistemlerin çalışamaz duruma gelme nedeni yüksek oranda iç kullanıcılardan kaynaklanmaktadır. Çalışanlara güvenilmeli fakat cihaz ve uygulamalara hak verilirken dikkatli olunmalıdır. Sosyal mühendislik tekniği büyük organizasyonlar için ciddi bir tehdittir.

# 7. GPRS GÜVENLİK PROSEDÜRLERİ

## 7.1 Temel Bilgiler ve Algoritmalar

### 7.1.1 Abone Kimlik Modülü (SIM) ve Doğrulama Merkezinde (AuC) Kayıtlı Bilgiler

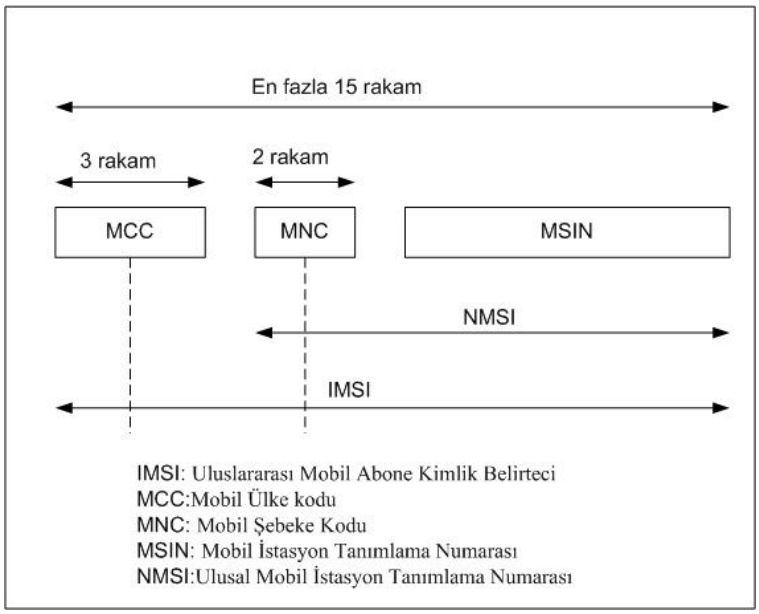
Abonenin SIM kartı ve şebekenin doğrulama merkezi, güvenlik fonksiyonları için önemli bilgiler tutmaktadır. Bu bilgiler aşağıda verilmiştir;

- Abone için parola olarak hizmet veren 128 bit uzunluğunda kişisel kimlik anahtarı (Ki). Bu anahtar, sayısal imza üretme algoritması (A3) ve şifreleme anahtarı üretme algoritmasının (A8) girdilerinden birisidir (Peng,2000).
- Her bir oturum için yeniden üretilen 64 bit uzunluğunda şifreleme anahtarı (GPRS Kc). Bu anahtar şifreleme algoritması ile birlikte kötü niyetli kişilerin oturumun dinlenmesi yolu ile bilgi edinmesini engellemektedir.
- Doğrulama ve şifreleme işlemlerinde ihtiyaç duyulan sayısal imza ve şifreleme anahtarı üretme algoritmaları A3 ve A8.

### 7.1.2 Abone Kimlik Modülü (SIM) ve GPRS Servis Sağlayıcı Düğümünde (SGSN) Kayıtlı Bilgiler

Bu bilgiler dışında iki adet mobil istasyon tanımlayıcısı kullanılmaktadır. Bu bilgiler abonenin SIM kartı ve SGSN cihazında tutulmaktadır.

- **IMSI** (Uluslararası mobil abone numarası): Bir aboneyi şebeke boyunca tanıtmak üzere kullanılan sabit bir kullanıcı adı gibi düşünülebilir. IMSI numarası mobil şebekeye ait ülke kodu (MCC), mobil şebeke kodu (MNC) ve mobil istasyon kimlik numarasından (MSIN) oluşmaktadır. IMSI numarası aynı zamanda HLR ve AuC'de de tutulmaktadır (Sanders,2003).




**Şekil 7-1 IMSI numarası (Kaasin,2001)**

- **P-TMSI** (Mobil abone geçici kimlik paketi): Bir aboneyi şebeke boyunca tanıtmak üzere kullanılan geçici bir kullanıcı numarası gibi düşünülebilir. Bu numara SGSN tarafından tahsis edilmektedir (Sanders,2003).

### 7.1.3 Mobil Ekipman ve Mobil Cihaz Kimlik Tanımı Veritabanında Tutulan Bilgiler

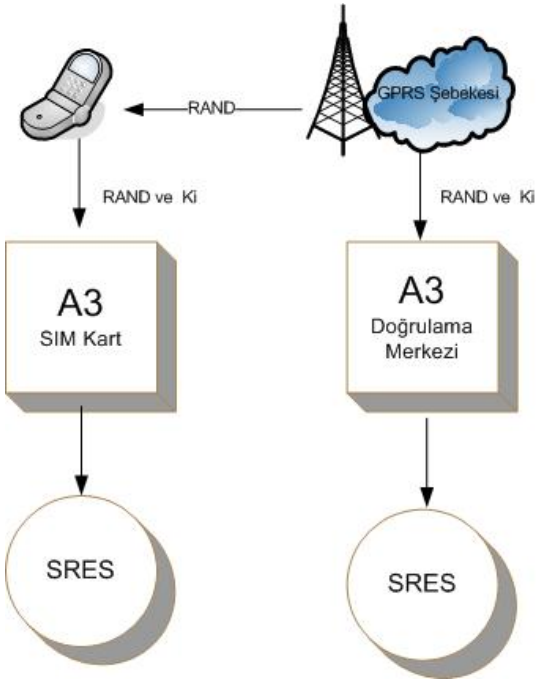
GSM/GPRS şebekelerinde kullanılan her bir mobil ekipmanın kendisine ait bir seri numarası vardır. Bu numara uluslararası mobil cihaz bilgisi (IMEI) numarası olarak adlandırılmaktadır ve üretilmiş her bir mobil ekipman için dünya üzerinde tek olmalıdır. IMEI numarası 14 rakamdan oluşan ondalık bir sayıdır ve aşağıdaki bilgileri içerir (Kaasin,2001).

- 6 rakamlık tür onay kodu (TAC)
- 2 rakamlık final birleştirme kodu (FAC)
- 6 rakamlık seri numarası (SNR)

### 7.1.4 A3 Algoritması

Mobil istasyonun sayısal imzası (SRES) A3 algoritması kullanılarak üretilmektedir. Bu değer 32 bit uzunluğundadır ve doğrulama prosedüründe kullanılmaktadır. A3 algoritması mobil istasyonun SIM kartında ve GPRS şebekesinin doğrulama merkezinde çalışmaktadır (Şekil 7-2). Algoritma girdi olarak 128 bit uzunluğundaki kişisel kimlik anahtarı Ki ve ilgili oturum

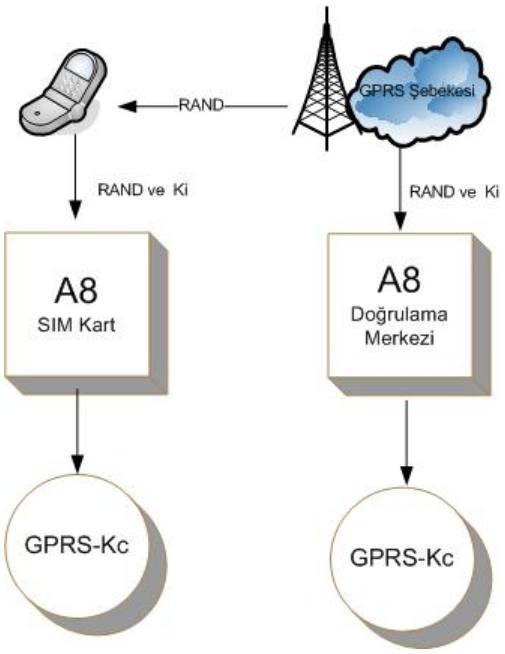
için doğrulama merkezi tarafından üretilmiş 128 bit uzunluğundaki rasgele sayıyı (RAND) almaktadır. Algoritmanın çıktısı 32 bit uzunluğunda bir değerdir ve bu değer mobil istasyonun sayısal imzası olarak adlandırılır (ETSI GSM 03.20).




**Şekil 7-2 A3 algoritması**

### 7.1.5 A8 Algoritması

Veri şifrelemesi sırasında kullanılacak GPRS-Kc anahtarı A8 algoritması kullanılarak üretilmektedir. Bu anahtar 64 bit uzunluğundadır ve şifreleme prosedüründe kullanılmaktadır. A8 algoritması mobil istasyonun SIM kartında ve GPRS şebekesinin doğrulama merkezinde çalışmaktadır (Şekil 7-3). Algoritma girdi olarak 128 bit uzunluğundaki kişisel kimlik anahtarı Ki ve ilgili oturum için doğrulama merkezi tarafından üretilmiş 128 bit uzunluğundaki rasgele sayıyı almaktadır. Algoritmanın çıktısı 64 bit uzunluğunda bir değerdir ve bu değer GPRS-A5 algoritması tarafından veri şifreleme sırasında kullanılmaktadır (ETSI GSM 01.61).




**Şekil 7-3 A8 algoritması**

### 7.1.6 GPRS-A5 Algoritması

GPRS-A5 algoritması mobil istasyon ve SGSN cihazlarında gerçeklenen bir şifreleme ve çözme algoritmasıdır. Şifreleme işlemi verinin modülasyonundan önce, çözme işlemi ise demodüle edilmesinden sonra gerçekleştirilmektedir.

GPRS-A5 algoritması, bir çerçeve süresince (4.615 msn) 114 bit uzunluğunda 2 adet şifreleme/çözme bit dizisi oluşturmaktadır. Bu bit dizilerine BLOK denilmektedir. GPRS-A5 algoritması tarafından üretilen ilk 114 bit BLOK1 olarak, ikinci 114 bit BLOK2 olarak ifade edilmekte ve BLOK1 şifreleme, BLOK2 ise çözme için kullanılmaktadır. GPRS-A5 algoritmasındaki senkronizasyon LLC çerçeve numarasına bağlı olan GİRDİ değeri ile yapılmaktadır. Özetle üretilen bloklar GPRS-Kc şifreleme anahtarına ve GİRDİ zaman değişkenine bağlıdır. Aşağıda GPRS-A5 algoritmasının girdi ve çıktıları görülmektedir;

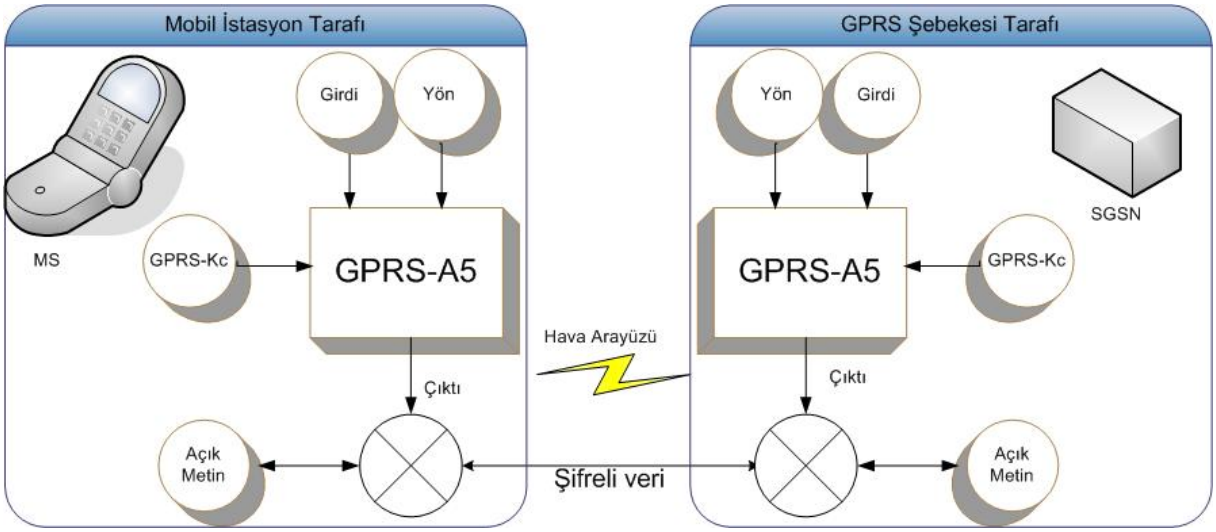
GPRS-A5 algoritmasının girdileri;

- GPRS-Kc: 64 bit uzunluğunda şifreleme anahtarı
- GİRDİ: 22 bit uzunluğunda zaman parametresi. TDMA çerçeve numarası.

GPRS-A5 algoritmasının çıktıları;

- 114 bit uzunluğunda bit dizisi: BLOK1
- 114 bit uzunluğunda bit dizisi: BLOK1

GPRS-Kc anahtarı GPRS-A5 algoritmasının girdilerinden sadece bir tanesidir. Bu algoritma her bir oturum için şifreleme bit dizisi oluşturmaktadır. Her oturum için tekliği sağlamak üzere bit dizisinin oluşturulmasında LLC çerçeve numarası da girdi olarak alınmaktadır. Bu sayede her bir LLC çerçevesi farklı bir bit dizisi ile şifrelenmektedir. Senkronizasyonu sağlamak üzere SGSN düzenli olarak LLC çerçeve numaralarını mobil istasyona göndermektedir (Şekil 7-4) (ETSI GSM 01.61).




**Şekil 7-4 GPRS A5 algoritması**

Bugüne kadar 7 adet GPRS-A5 algoritması tanımlanmıştır. Bunlardan ilk ikisi ve en çok kullanılanları GEA1 ve GEA2'dir. Bu algoritmalar ETSI SAGE tarafından tanımlanmıştır. Bir mobil istasyon şebekeye bağlantı kurmak istediğinde hangi GPRS-A5 algoritmalarını desteklediğini belirtmek zorundadır. Hangi GPRS-A5 algoritmasının kullanılacağına doğrulama prosedürü sırasında karar verilmektedir.

### 7.1.7 Üçüzler

Üçüzler SGSN'in isteği ile doğrulama merkezi tarafından oluşturulur ve SGSN'e gönderilir. Bir üçüz içerisinde RAND, SRES ve GPRS-Kc anahtarı bulunmaktadır (Kaasin,2001).

- RAND: Üçüzlerin hiçbir zaman aynı olmaması için kullanılan, doğrulama merkezi tarafından üretilmiş 128 bit uzunluğundaki rasgele sayıdır.
- SRES: A3 algoritması kullanılarak üretilmiş mobil istasyonun imzası olarak düşünülen 32 bitlik bir sayıdır.
- GPRS-Kc: A8 algoritması kullanılarak üretilmiş mobil istasyon ve SGSN arasında veri şifrelemesi sırasında kullanılacak 64 bit uzunluğunda olan anahtardır.

### 7.2 Doğrulama Prosedürü

Bir mobil istasyon, GPRS şebekesine erişim izni verilmeden önce doğrulanmalıdır. Doğrulama işleminin başlaması için örnek senaryolar aşağıda verilmiştir;

- Yönlendirme alanı güncellenmesinden önce
- GPRS bağlanma ve kopma prosedürlerinden önce
- GPRS şebekesinden veri transferi yapılmadan önce

Doğrulama prosedürünün amacı şebekeye ulaşmaya çalışan abonenin gerçek bir SIM kart ve doğru bir kişisel kimlik anahtarına (Ki) sahip olup olmadığının kontrol edilmesidir. Bu işlem Ki anahtarı hava arayüzüne çıkartılmadan yapılmaktadır. Doğrulama prosedürü SGSN tarafından başlatılmakta ve kontrol edilmektedir (Dinçkan,2005).

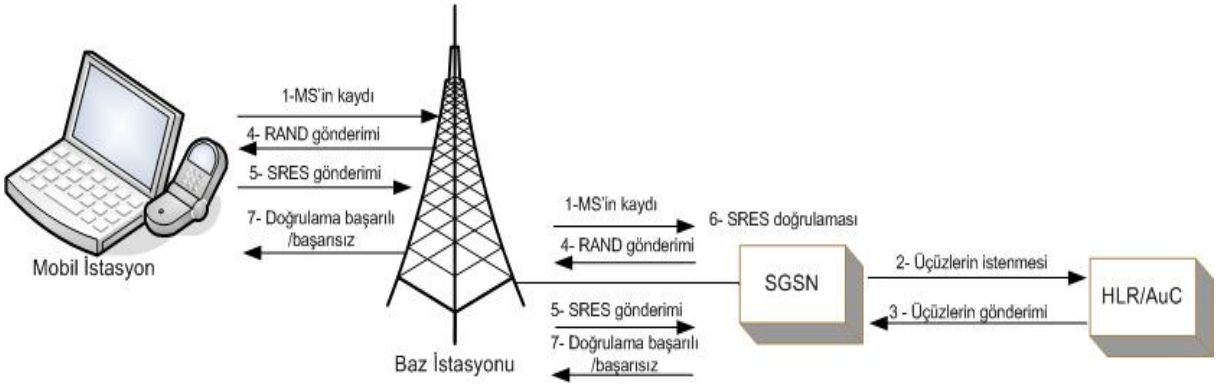
Mobil istasyon, şebeke üzerinden veri aktarmaya başlamadan önce SGSN doğrulama prosedürünü başlatır. SGSN ilk olarak ilgili aboneye ait IMSI numarasının da bulunduğu mesajı doğrulama merkezine gönderir ve üçüzleri ister. Doğrulama merkezi IMSI numarasını kullanarak aboneye ait Ki numarasını bulur ve üçüzleri oluşturur.

Mobil istasyonun sayısal imzası A3 algoritması ile, şifreleme anahtarı ise A8 algoritması ile üretilmektedir. Her iki algoritmada aynı girdileri kullanarak işlem yapmaktadır. Bu girdilerden ilki hem şebeke hem de mobil istasyon tarafından bilinen ve her zaman sabit olan Ki numarası, diğeri ise her doğrulamada değişen RAND sayısıdır.

Bir aboneyi doğrulamak için gerekli aşamalar aşağıda verilmiştir (Şekil 7-5).

1. Doğrulama isteği gerektiren herhangi bir durumun gerçekleşmesi.
2. Doğrulama başlatılır ve SGSN abonenin IMSI numarasının da bulunduğu bir mesajı doğrulama merkezine göndererek üçüzleri ister.
3. Doğrulama merkezi IMSI numarasını kullanarak ilgili aboneye ait Ki anahtarını bulur. Bu anahtarı ve kendisinin oluşturduğu rasgele sayıyı kullanarak üçüzleri oluşturur. Daha sonra bu üçüzleri SGSN'ye gönderir.
4. SGSN üçüzler içerisinden RAND sayısını mobil istasyona gönderir.
5. Mobil istasyonun SIM kartı A3 algoritmasını çalıştırır ve Ki ile RAND sayılarını kullanarak sayısal imzayı oluşturur.

6. Mobil istasyon sayısal imza değerini SGSN'ye gönderir.
7. SGSN mobil istasyondan gelen sayısal imza değeri ile doğrulama merkezi tarafından üçüzler içerisinde kendisine ulaştırılan sayısal imza değerlerini karşılaştırır.
8. Eğer imzalar aynı ise abone doğrulanmış olur. Aboneye "Doğrulama başarılı" mesajı gönderilir. Eğer imzalar farklı ise aboneye "Doğrulama başarısız" mesajı gönderilir.

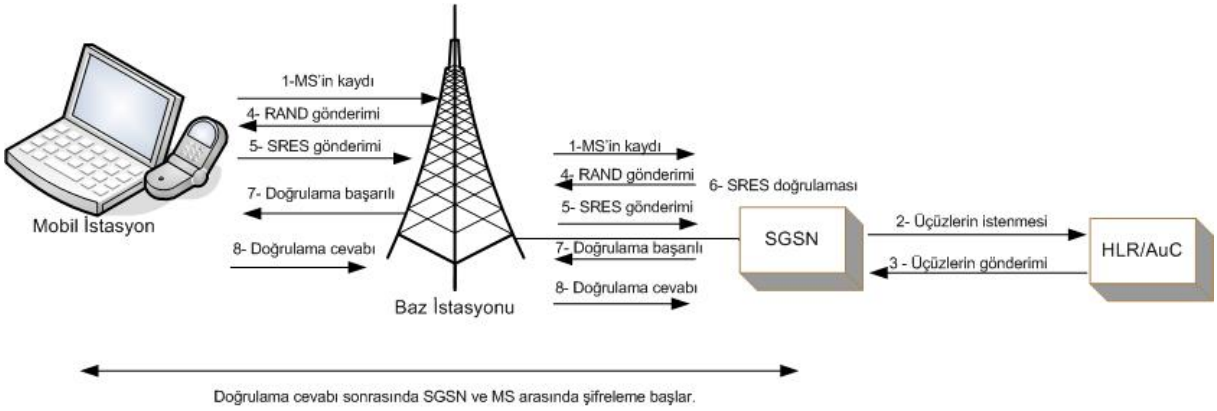



**Şekil 7-5 Doğrulama prosedürü**

Doğrulama prosedürünün tek amacı mobil istasyonun SIM kartının dolayısı ile Ki anahtarının doğrulanmasıdır. Bu işlemler sırasında Ki anahtarı hava arayüzünde hiçbir zaman bulunmamaktadır. Yine de bir sorun vardır. Bu işlemler gerçekleşirken hava arayüzünü dinleyen bir saldırgan sayısal imza ve RAND değerlerine ulaşabilmektedir. Bu değerler ile A3 algoritması kullanılarak Ki değerini yeniden hesaplamak mümkündür. Gerçekte GSM altyapısında kullanılan algoritmalar Ki değerinin sayısal imza kullanarak hesaplanmasını çok zor duruma getirecek biçimde tasarlanmıştır. Böyle bir ters işlemi gerçekleştirmek eskiden işlem gücü yetersizliği nedeni ile mümkün olmamasına rağmen artık mümkündür (Dinçkan,2005).

### 7.3 Şifreleme Prosedürü

GPRS şebekesi üzerinden akacak verinin gizliliğini sağlamak üzere mobil istasyon ve SGSN arasında şifreleme yapılmaktadır. Eğer doğrulama prosedüründe son olarak "Doğrulama başarılı" mesajı gönderildi ise mobil istasyon SGSN'e doğrulama cevabını gönderir ve bu mesajı takiben artık şifreleme başlar.




**Şekil 7-6 Şifreleme prosedürü**

Şifreleme işlemi GPRS-A5 algoritması tarafından GPRS-Kc anahtarı kullanılarak yapılmaktadır. SGSN cihazı GPRS-Kc anahtarını üçüzün bir parçası olarak almaktadır. Mobil istasyon ise RAND sayısını kullanarak A8 algoritması ile GPRS-Kc anahtarını hesap etmektedir.

GSM ve GPRS sisteminde kullanılan şifrelemede belirgin bir fark vardır. GSM şebekesinde şifreleme BTS ve mobil istasyon arasında yapılmakta iken GPRS şebekesinde mobil istasyon ve SGSN arasında yapılmaktadır. GSM şebekesinde A5 algoritmasının üç versiyonundan biri (A5-0, A5-1 veya A5-2) kullanılmakta iken GPRS şebekesinde paket haberleşmesi için geliştirilen yeni sürüm A5 algoritması kullanılmaktadır (Dinçkan,2005).

### 7.4 P-TMSI Yeniden Atama Prosedürü

P-TMSI bir aboneyi şebeke boyunca tanıtmak üzere kullanılan geçici bir kullanıcı numarasıdır. Bu numara SGSN tarafından geçici olarak tahsis edilmekte ve IMSI numarası yerine kullanılmaktadır. Herhangi bir prosedürün başlatılma aşamasında mobil istasyon bu numarayı SGSN'e göndermektedir. Fakat öyle bir durum oluşabilir ki mobil istasyon hiç P-TMSI numarasına sahip olmayabilir veya geçerli bir P-TMSI numarası yoktur. Böyle bir durumda mobil istasyonun IMSI numarasını SGSN'e göndermekten başka seçeneği yoktur. IMSI numarasının hava arayüzüne çıkması istenmeyen bir durumdur.

Her bir doğrulama sonrasında mobil istasyon yeni bir P-TMSI numarası almaktadır. Ayrıca mobil istasyon yeni bir SGSN alanına geçtiğinde yeni SGSN, mobil istasyon için yeni bir P-TMSI numarası gönderir. Mobil istasyonun ilk SGSN alanı içinde kullandığı P-TMSI numarası başka mobil istasyonlar tarafından kullanılmak üzere boşa çıkar. Her bir SGSN, P-

TMSI numaralarından oluşan bir havuza sahiptir. Eğer bir mobil istasyon çok uzun süre aynı SGSN alanı içerisinde kalırsa SGSN bu istasyona yeni bir P-TMSI numarası atayabilir (Sanders,2003).

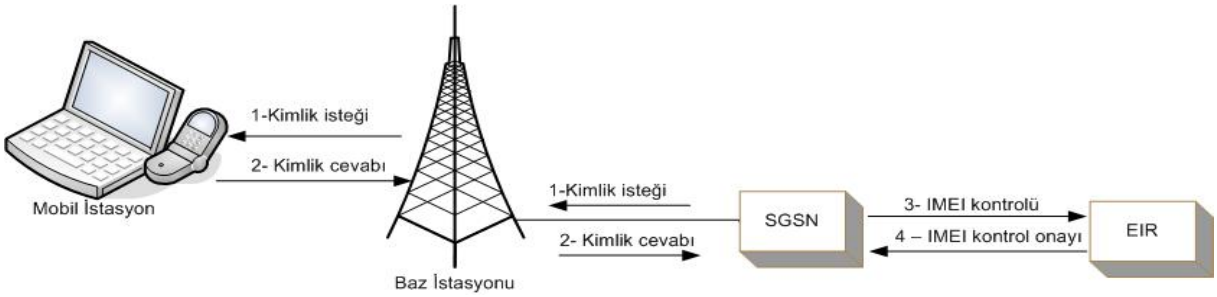
### 7.5 Kimlik kontrol Prosedürü

Eğer istenirse mobil operatör, mobil telefonların çalıntı olup olmadığının veya GPRS şebekesine girme hakkı olup olmadığının kontrolünü yapabilir. Bunun için EIR veritabanı tutulmalı ve şebekede çalışacak mobil telefonların IMEI numaraları bu veritabanında bulunmalıdır. Bu veritabanında üç tür liste vardır;

- **Beyaz liste:** Şebekeye girme izni olan IMEI numaralarının listesidir.
- **Gri liste:** Olası problemlerden dolayı araştırma yapılan IMEI numaralarının listesidir.
- **Siyah liste:** Şebekeye girme izni olmayan IMEI numaralarının listesidir.

Kimlik kontrol prosedürü doğrulama prosedürü işletildikten ve şifreleme işlemi başladıktan sonra yapılmaktadır (Sanders,2003). Prosedürün çalışması aşağıda açıklanmıştır (Şekil 7-7).

1. Doğrulama işlemi tamamlanıp şifreleme işlemine geçtikten sonra SGSN mobil telefona kimlik isteği gönderir.
2. Mobil telefon IMEI numarasının içinde bulunduğu kimlik bilgilerini SGSN'ye gönderir.
3. SGSN aldığı IMEI numarasını kontrol etmesi amacı ile EIR'ye gönderir.
4. EIR, IMEI numarasını kontrol ettikten sonra SGSN'ye onay mesajı gönderir.




**Şekil 7-7 kimlik doğrulama prosedürü**

### 7.6 Kullanıcı Kimliği Gizliliği

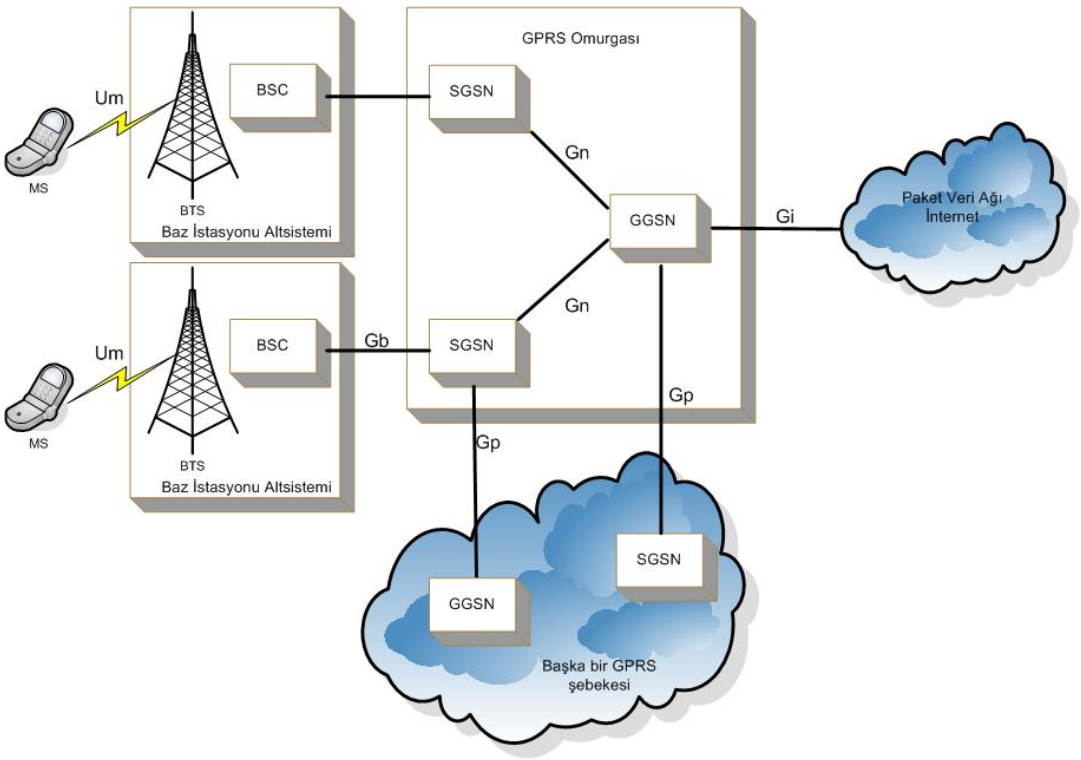
GPRS şebekesinde kullanıcı kimliğini gizlemek için abonenin SIM kartı içerisinde yazılı bulunan uluslararası mobil abone numarasının (IMSI) gizlenmesi gereklidir. GPRS şebekesine bağlantı kurulması esnasında IMSI numarasının gizliliği mobil abone geçici kimlik paketi (P-TMSI) numarası kullanılarak sağlanmaktadır. GPRS şebekesine bağlantı kurulduktan sonra kimliğin gizliliği için Geçici Mantıksal Bağlantı Belirteci (TLLI) numarası kullanılmaktadır. Bu numara mobil istasyon tarafından P-TMSI numarası kullanılarak üretilmektedir. Mobil istasyonun ilk defa çalıştırılması durumu haricinde IMSI numarası SIM kart içerisinden çıkmamaktadır. Geçici mantıksal bağlantı belirteci mobil istasyon ve SGSN arasında kullanılmakta ve IMSI ile olan ilişkisi sadece bu cihazlar tarafından bilinmektedir. Bir yönlendirme alanı içerisinde TLLI ve IMSI arasında birebir eşleşme söz konusudur. Eğer TLLI numarasının hangi yönlendirme alanına ait olduğu belirli değilse TLLI numarası Yönlendirme Alanı Kimliği (RAI) ile birlikte kullanılmaktadır (Peng,2000).

# 8. GPRS OMURGA GÜVENLİĞİ

GPRS mimarisinin ana parçası, GPRS destek düğümlerinin (SGSN ve GGSN) birbirine bağlanmasını sağlayan omurgadır. Omurga üzerinden verinin aktarımı 3GPP tarafından TS 29.060 kodu ile tanımlanmış GTP protokolü tarafından gerçekleştirilir. Bu protokol sinyalleşmenin ve veri aktarımının nasıl yapılacağını belirlemektedir. GPRS omurgası üzerinden haberleşme GTP protokolünün IP ve UDP protokollerini kullanarak tünel oluşturması ile sağlanmaktadır. Tünel kurma ve GPRS omurgası üzerinden veri taşıma işlemleri, GTP protokolünün kendi bünyesinde bir şifreleme mekanizması içermemesi nedeni ile açık metin olarak yapılmaktadır. Bu problemin önüne geçebilmek için günümüz IP ağlarında kullanılan güvenlik mekanizmaları (örneğin IP güvenliği protokolü – IPSec) GPRS omurgasında kullanılabilmektedir. Bu tercih GPRS şebekesini işleten servis sağlayıcıya bağlıdır.

## 8.1 GPRS Tünel Protokolü (GTP)

GTP protokolü hem Gp hem Gn arayüzlerinde kullanılmaktadır. Bu arayüzler SGSN ile GGSN arasında bulunmaktadır. Aynı şebeke içerisinde olduğunda Gn, farklı şebekeler arasında olduğunda Gp arayüzü olarak isimlendirilir (Şekil 8-1).




**Şekil 8-1 GTP mantıksal mimarisinin arayüzler ile gösterilmesi**

GTP protokolü sadece GPRS destek düğümleri olan SGSN ve GGSN üzerinde gerçeklenmektedir. Bir mobil istasyon GPRS hizmeti almak için ilgili SGSN'ye bağlanırken GTP protokolünden haberdar değildir. GTP protokolü sayesinde kendisine ait paketler doğrudan GGSN Gi arayüzüne taşınmaktadır. Omurga üzerinde kullanılan IP adresleri abone IP adreslerinden tamamen bağımsızdır. GPRS omurgası tamamen bir taşıyıcı görevi görmektedir.

SGSN'ler ve GGSN'ler arasında çok noktadan çok noktaya bir ilişki bulunduğu düşünülmelidir. Bir SGSN birçok GGSN'ye hizmet sağlayabilmektedir. Bir GGSN coğrafi olarak dağılmış olan çok sayıda mobil istasyona SGSN'ler üzerinden hizmet verebilmektedir (Şekil 8-1).

### 8.1.1 GTP Sürümleri

GTP protokolü 0 ve 1 olmak üzere iki sürüme sahiptir. GTP'nin ilk sürümü (GTPv0) ETSI tarafından GSM 09.60 numaralı standart ile tanımlanmıştır. GTP protokolünün ikinci sürümü (GTPv1) ise 3GPP tarafında 29.060 kodlu standart ile tanımlanmıştır.

İlk çıkan sürüm (GTPv0) ile bugün kullanılan GTPv1 arasında aşağıda sayılan farklar vardır.

- GTP'nin ilk sürümünde tünel belirteci (TID) rastgele değildir,
- GTP'nin ilk sürümü X25 protokolünün aktarımına olanak sağlamaktadır,
- GTP'nin ilk sürümünde bütün haberleşme için sabit port numarası (3386) kullanılmaktadır,
- GTP'nin ilk sürümü TCP protokolünün kullanımına izin vermektedir,
- GTP'nin ilk sürümünde hizmet kalitesine (QoS) dair seçenekler sınırlıdır.

## 8.2 Örnek GTP Mesajı

GTP protokolünün çalışma prensiplerini açıklayabilmek için Şekil 8-2'de örnek bir GTP içerik oluşturma isteği mesajı verilmiştir. Şekilde görülen numaraların açıklamaları aşağıda sıralanmıştır;

**(1)** GTP paketi GPRS destek düğümleri arasında IP protokolü ile taşınmaktadır. IP protokolü bir alt katmanda (OSI referans modeli ikinci katmanında) Ethernet protokolü üzerinde taşınmaktadır. Bu alan Ethernet protokolüne ait kaynak ve hedef

adreslerini belirtmektedir.

**(2)** Aralarında GTP tüneli kurulan SGSN ve GGSN IP adreslerini göstermektedir. Örnekte GPRS hizmet düğümü adresleri 192.168.10.2 ve 192.168.20.2 olarak görülmektedir.

**(3)** GTP protokolünün haberleştiği uçlar arasında kullanılan UDP portunu tanımlamaktadır. Haberleşme sırasında 2123 numaralı UDP portu kullanılmaktadır.

**(4)** IP paketinin içerisinde taşınan GTP bilgilerinin bulunduğu alandır. Bu aşamadan sonra sıralanacak bilgiler bu alanın içerisinde bulunmaktadır.

**(5)** Kullanılan GTP protokolünün sürüm bilgisini vermektedir. Örnekte GTP sürüm 1 kullanılmaktadır.

**(6)** GTP mesajının türünün GTP içerik oluşturma isteği olduğunu belirten alandır.

**(7)** GPRS hizmet düğümleri arasında kurulan tünele ait tünel belirteci numarasıdır.

**(8)** Abonenin IMSI numarasını gösteren alandır. Örnekte IMSI numarası 240010123456789 olarak görülmektedir.

**(9)** Abonenin bağlantı sırasında bildirdiği erişim noktası adıdır (APN). Örnekte APN internet olarak görülmektedir.

**(10)** GTP protokolü içerisinde tanımlanan GPRS hizmet düğümü IP adresi alanıdır. Örnekte hizmet düğümünün IP adresi 192.168.10.2 görülmektedir. Dikkat edilirse 2 numaralı alanda bulunan kaynak IP adresi ile aynıdır.

**(11)** Aboneye ait MSISDN numarasıdır. Örnekte +46702123456 olarak görülmektedir.


**Şekil 8-2 Örnek GTP mesajı**

## 8.3 GPRS Omurgası Haberleşme Güvenliği

Günümüz GPRS şebekelerinde omurga üzerinden haberleşme IP protokolü sürüm 4 ile yapılmaktadır. IP sürüm 4 kendi bünyesinde herhangi bir güvenlik mekanizması bulundurmamaktadır. IP sürüm 6 ise gizlilik ve kimlik doğrulama konusunda çeşitli kabiliyetlere sahiptir (Piot,1998). Bu kabiliyetler IPSec protokolü gibi yöntemler kullanılarak IP sürüm 4'e de kazandırılabilmektedir. Kazandırılan yetenekler aşağıda sıralanmıştır;

- **Kimlik Doğrulama:** Haberleşen GPRS hizmet düğümlerinin kimlik doğrulamasının yapılması,
- **Gizlilik:** Abone veya sistem bilgilerinin yetkisiz ellere geçmesinin engellenmesi,
- **Bütünlük:** Abone veya sistem bilgilerinin yetkisiz kişiler tarafından değiştirilememesi.

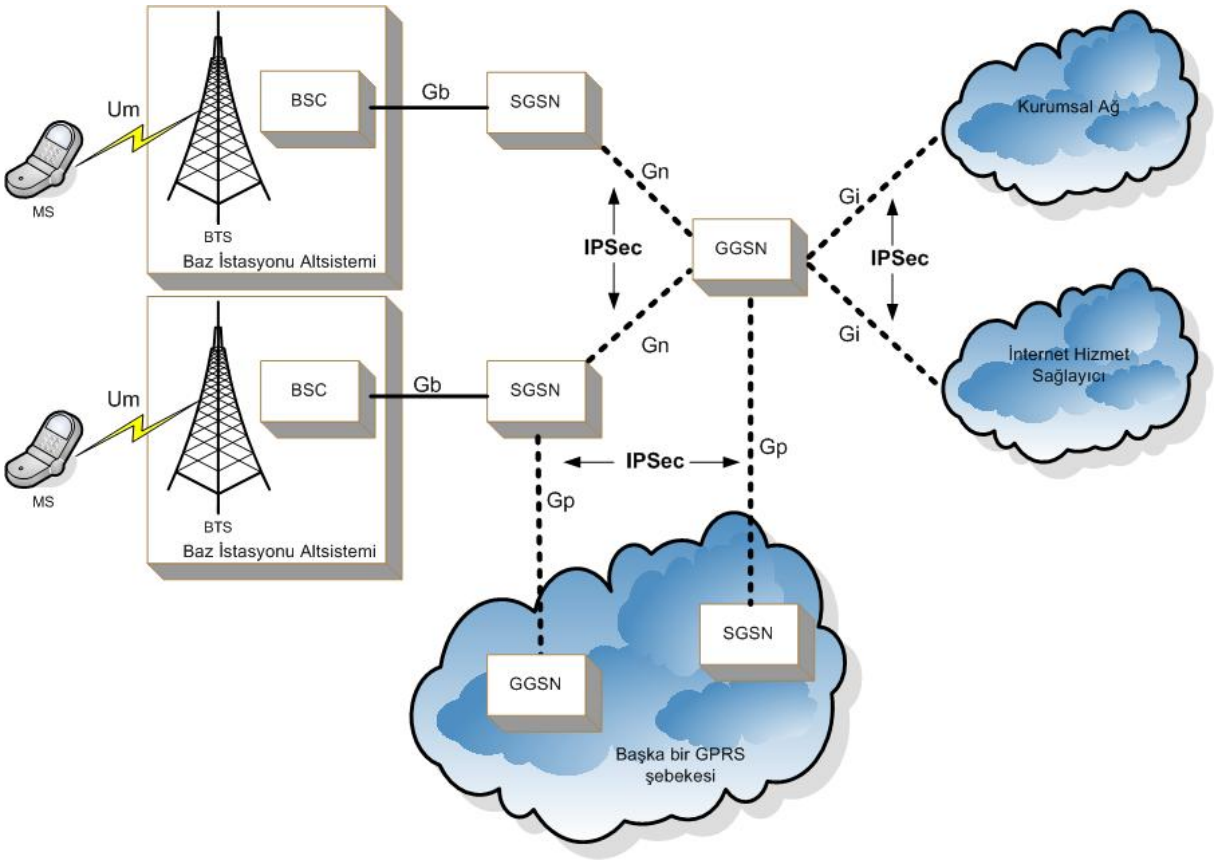
### 8.3.1 IPSec Protokolüne Kısa Bakış

IP protokolünde güvenlik sağlanabilmesi için iki adet başlık kullanılmaktadır. Bu başlıklar IP doğrulama başlığı (AH) ve IP güvenli veri kapsülleme başlığıdır (ESP). Bu bölümde AH ve ESP başlıklarının pratikte en çok kullanılanları incelenecektir.

IP doğrulama başlığı bütünlük ve doğrulama sağlamak amacı ile tasarlanmıştır. IP paketlerinin gizliliği için AH çözüm getirmemektedir. İki veya daha fazla bilgisayar, iki veya daha fazla ağ geçit cihazı veya bilgisayarlar ve ağ geçit cihazlarından oluşan şebekelerde AH kullanılarak güvenlik sağlanabilmektedir. Gönderilen verinin değişmemesi ve gönderen düğümün doğruluğu AH protokolü kullanılarak temin edilir (Piot,1998).

IP ESP protokolü ise AH protokolüne ek olarak gizlilik hizmeti de sağlamaktadır. AH ile aynı senaryolarda kullanılabilmektedir. Hiçbir güvenlik geçidinin bulunmadığı durumlarda dahi iki uç sistem ESP protokolü kullanarak veri şifrelemesi yapabilmektedir. ESP protokolü esnek bir protokoldür ve kullanıcıya arzu edilen gizlilik, kimlik doğrulama ve bütünlük hizmetlerinden birini veya birkaçını birlikte verebilmektedir.

IP tabanlı GPRS omurgası üzerinde SGSN ve GGSN düğümleri arasında IPSec protokolü kullanımı ile omurga üzerinde sinyalleşme ve veri haberleşmesine dair trafiğin gizliliği, bütünlüğü ve sadece izin verilen düğümler arasında haberleşme yapılması sağlanabilmektedir (Şekil 8-3).




**Şekil 8-3 GPRS şebekesinde IPSec kullanımı**

### 8.3.2 Diğer IP Güvenlik Protokolleri

Veri haberleşme protokollerinin yapı ve işlevlerini tanımlamak için 1979 yılında ISO tarafından geliştirilen mimari model kullanılmaktadır. OSI referans modeli, 7 katmanlı yapı yardımı ile haberleşme protokollerinin fonksiyonlarını tanımlamaktadır. IP protokolü OSI referans modelinde üçüncü katman, yani ağ katmanında bulunmaktadır. Bu katmanın görevi veri paketini çeşitli düğümler üzerinden yönlendirerek bir uçtan diğer uca ulaştırmaktır (Dinçkan,2001). Ağ katmanı aynı zamanda internet katmanı olarak da anılmaktadır. Mimari model ilk çıktığında IP paketlerinin güvenliğine dair herhangi bir önlem yoktu. Günümüzde IP paketlerinin güvenliği için en çok kullanılan protokol IPSec protokolüdür. Ancak bu katmanda standart bir güvenlik protokolü fikri IETF IPSec çalışma grubundan önce de gündeme gelmiştir. Bunlar arasında aşağıdaki protokoller önemli olanlarıdır:

- **Güvenlik Protokolü 3 (SP 3) :** ABD Ulusal Güvenlik Ajansı (NSA) ve Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından üretilen bir ağ katmanı güvenlik protokolüdür. Bağlantısız çalışan SP3, Xerox gibi endüstriden pek çok tekel firmanın da arasında bulunduğu taraflarca halen kullanılmakta olan bir güvenlik sistemi olan güvenli veri ağ sistemi (SDNS)'nin bir parçası olarak tasarlanmıştır. Sistemin bütünü

OSI mimarisine uygun biçimde tasarlandığından Ağ katmanı güvenlik protokolü de bir üst katmandan gelen paketleri güvenli biçimde işleyerek alt katmanlara gönderir. Projenin ilk sürümü 1989'da ABD hükümetine sunulmuştur.

- **Ağ Katmanı Güvenlik Protokolü (Network Layer Security Protocol-NLSP):** Uluslararası Standartlar Organizasyonu (ISO) tarafından bağlantısız ağ protokolü güvenliği için tasarlanmıştır. SP 3'ten yola çıkılarak tasarlanmış olup, 1995'te standart olarak yayınlanmıştır.

- **Tümleşik NLSP (Integrated-NLSP) :** NIST tarafından IPv4 güvenlik servisleri sağlamak amacıyla geliştirilmiştir. SP3 ile aynı mantığa dayanmaktadır, sadece küçük detaylarda ayrılır. Güvenli etiket işleme bu özelliklerden biri olup uzun süre önce kullanımdan çıkmıştır.

- **swIPe :** Bir başka deneysel internet katmanı güvenlik protokolüdür. İki yazılımcı tarafından UNIX sistemi için tasarlanmış olup internette açık versiyonu bulunmaktadır.

Burada sayılan güvenlik protokollerinin ayırt edilir farklılıkları bulunmamaktadır. Tamamında aşağıda sayılan ortak özellikler temelinde güvenlik sağlanır (Şekil 8-4).

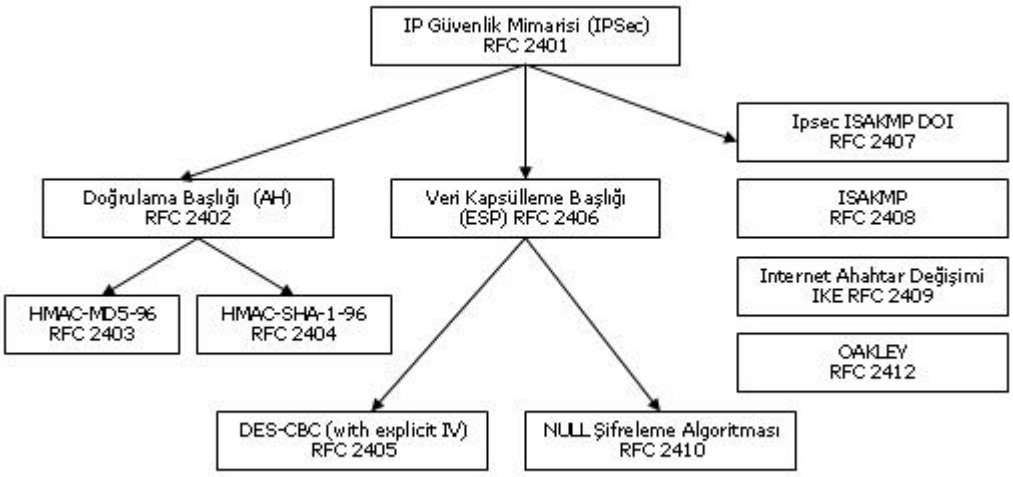
- IP kapsülleme işlemi ile doğrulama ve şifreleme işlemi paralel yürütülür.
- Var olan IP kapsülleme aynen geçerlidir.
- IP paket başlığı da kapsüllenmekte ve şifrelenmektedir.
- Güvenlik protokolü ayrı bir başlık ekler.


**Şekil 8-4 Güvenli IP paketi**

1994'te IP sürüm 6'nın geliştirilmesiyle birlikte internet protokolü için güçlü bir güvenlik mekanizmasının da içine katılması gündeme gelmiştir. Algoritmadan bağımsız, güvenlik kullanmayan taraflarla haberleşmede uyumsuzluk yaratmayacak bir protokol tasarlanması üzerinde bir çalışma başlatılmıştır. IETF tarafından IPsec çalışma grubu (IPsec WG) hem IP Güvenlik Protokolü (IP-Security Protocol-IPSP) hem de internet anahtar yönetim protokolü

(Internet Key Management Protocol-IKMP) tasarımı amacıyla kurulmuştur. Bu iki mekanizmanın birlikte çalışması iki adımda özetlenebilmektedir.

- IKMP taraflar arasında bir Güvenlik Birliği (Security Association-SA) kurar ve Güvenlik Parametre İndekslerini (Secure Parameter Index-SPI) başlatır.
- IPSec , IKMP tarafından belirlenen SA ve SPI' ları kullanarak IP paketlerini şifreli gönderir, doğrulama işlemini yerine getirir.




**Şekil 8-5 IP güvenlik mimarisi standartları**

Şekil 8-5'de IP güvenlik mimarisi konusunda yapılan çalışmalara dair standartlar ve bunların bağlılıkları gösterilmiştir. Daha ileri incelemeler için ilgili standartlara başvurulmalıdır.

### 8.3.3 IP Güvenlik Protokolü (IP Security Protocol - IPSec)

IPv6'nın Güvenlik Mimarisi doğrulama ve şifreleme mekanizmasını birlikte içerir; bu iki mekanizma IPSP'yi oluşturur. Bunlardan kaynak doğrulama ve veri bütünlüğünün sağlanması için Doğrulama Başlığı (Authentication Header-AH); veri güvenliğinin sağlanması için ise Güvenli Veri Kapsülleme (Encapsulating Security Payload-ESP) servisleri kullanılmaktadır (RFC 2411).

Bu iki mekanizmanın birlikte mi yoksa yalnızca birisinin mi kullanılacağı konusuna karar vermek üzere güvenlik birliği (Security Association-SA) devreye girer. Güvenlik Birliği, haberleşen taraflar arasında hangi güvenlik servislerini kullanacakları ve bu servisleri nasıl sağlayacakları hakkında varılan bir anlaşmadır. Güvenlik Birliği aşağıdaki başlıklarda

tarafların uzlaşmasını sağlar:

- Doğrulama algoritmasının tipi, çalışma modu ve kullanılacak anahtarlar,
- Şifreleme algoritması tipi, çalışma modu ve kullanılacak anahtarlar,
- Şifreleme algoritması senkronizasyonu için Başlangıç Vektörü (IV) uzunluğu,
- Anahtarlar ve Güvenlik Birliğinin ömrü,
- Güvenlik Birliğinin kaynak adresi, ( ağ ya da alt ağ adresi de olabilir)

Bir IP paketi alındığında alıcı, paketin güvenlik parametre indeksi (Secure Parameter Index-SPI) üzerinden ilgili güvenlik birliğinin (SA) içeriğine ulaşır ve paketi nasıl çözmesi gerektiği konusunda bilgi edinir. Eğer alıcı IP paketini herhangi bir Güvenlik Birliği içeriği ile ilişkilendiremezse veya yanlış bir anlaşma üzerinden paketi açmaya çalışırsa paketi çözümleyemez (RFC 2401).

Anahtarlama yaklaşımları üçe ayrılabilir:

1. Her bilgisayara farklı anahtar: (IPsec protokolünü çalıştırma yeteneği olan herhangi bir cihazda olabilir)

   Bir bilgisayardaki tüm kullanıcılar, diğer bir bilgisayarda sonlanan trafik için birbirleriyle aynı oturum anahtarını kullanırlar.

2. Her kullanıcıya farklı anahtar:

   Kullanıcı merkezli anahtarlamada, bir bilgisayardaki her kullanıcı diğer bir bilgisayarda sonlanan trafik için farklı anahtar kullanmaktadır.

3. Her oturuma farklı anahtar:

   Oturum merkezli anahtarlama, IP adresi, üst katman protokolü ve port numarası bilgileri üçlüsü için tekil bir anahtar atanmasıdır. Örneğin bir kullanıcı açtığı FTP oturumu ile açtığı Telnet oturumu için ayrı anahtarlar kullanır.

Bir kullanıcının diğer kullanıcının veri trafiğine karşı yapabileceği saldırılara karşı 2 ve 3, 1'e göre daha dayanıklıdır.

### 8.3.4 Doğrulama Başlığı

IP Güvenlik Protokolünde Doğrulama Başlığı (Authentication Header-AH) IP paketleri için veri kaynağının doğrulanması ve bağlantısız veri bütünlüğünün sağlanması amacıyla

kullanılır. Kullanılan şifreleme algoritmasının türüne bağlı olarak kaynağın inkar edilememesini de sağlar. IP paketlerine doğrulama verisi eklenir. Doğrulama bir doğrulama algoritması ve ilgili anahtarın kullanımıyla sağlanır (RFC 2402).

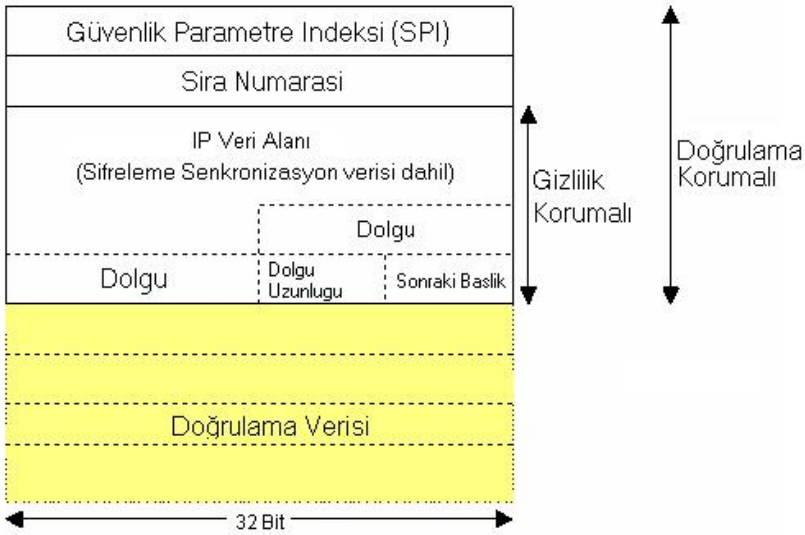
Gönderici IP paketini göndermeden önce doğrulama başlığını hesaplar, alıcı ise güvenlik parametre indeksi ile ilgili güvenlik birliği içeriğine bakarak hangi doğrulama algoritmasının ve anahtarlama yönteminin kullandığını bulur ve göndericiyi doğrular.

IP paket başlığının bazı bölümleri yol boyunca değişikliğe uğrayabilir. Başlıkta değişikliğe uğrayan bilgiler doğrulama başlığında doğrulama verisi hesaplanırken veya değerlendirilirken sabit alınır veya dikkate alınmaz. Gönderici şifrelemeden önce IP paketinin geçici bir versiyonunu hazırlar. Bu versiyon yol boyunca meydana gelecek değişikliklerden etkilenmez.


**Şekil 8-6 Doğrulama başlığı formatı**

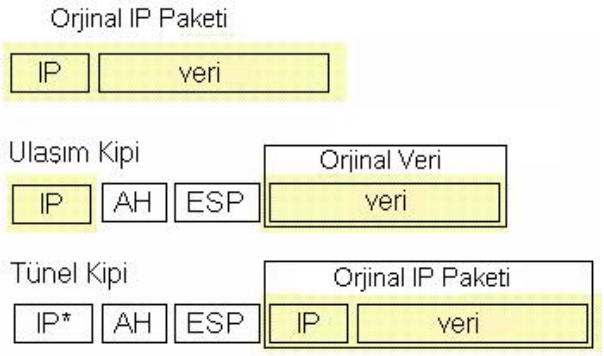
### 8.3.5 Güvenli Veri Kapsülleme (ESP)

IP paketinde verinin bulunduğu alan (yük alanı) doğrulama sırasında açıktır. Verinin gizliliği için şifrelenmesi gerekir. ESP bu amaçla geliştirilmiştir. ESP paketinin biçimi Şekil 8-7'de görüldüğü gibidir. ESP, paketi korumak için IP kapsülleme işlemini kullanır. Gönderici IPSec modülü IP paketini kapsüllerken, alıcı IPsec modülü kapsülü açar. ESP formatı, RFC 2406 standardında belirtilmiştir. Şifrelemede DES, 3DES veya AES gibi standart algoritmalardan birisi seçilebilmektedir (RFC 2406).




**Şekil 8-7 ESP biçimi**

### 8.3.6 IPSec İletişim Kipleri




**Şekil 8-8 Ulaşım ve tünel kipi paket formatı**

IP Güvenlik Protokolünde ulaşım ve tünel olmak üzere iki iletişim kipi bulunmaktadır. IPSec göndericinin (veya onun yerine görev yapan vekil cihazın) her IP paketinin kimlik denetimi yapmasını, şifrelemesini veya her iki fonksiyonu birden pakete uygulamasını sağlar. Bu iki fonksiyonu birbirinden ayırmak ve IPSec kullanmak için kip denilen iki metodun gelişmesine neden olmuştur. Ulaşım kipinde, IP paketinin sadece aktarım katmanı (transport layer – OSI referans modelinde 4. katman) bölümünün kimlik denetimi yapılır veya şifrelenir. IP paketinin tamamına kimlik denetimi veya şifreleme yapan öteki yaklaşıma ise tünel kipi denir. IPSec ulaşım kipi pek çok alanda faydalı olurken, tünel kipi belirli saldırılara karşı çok daha iyi koruma sağlar. GPRS sisteminde güvenlik duvarları ve ağ geçit cihazları arasında tünel kipinde IPSec çalıştırılarak bütün IP paketinin koruma altına alınması önerilir. Tünel kipi IPSec çalışmasında IP paketleri yeni IP paketlerinin içerisinde taşınarak iletişim sağlanmaktadır (Şekil 8-8) (RFC2401).

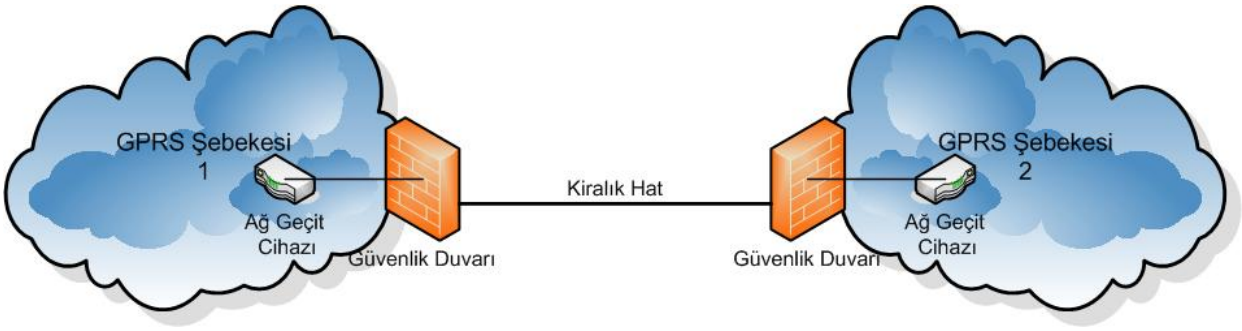
# 9. GPRS OMURGALARININ BAĞLANMASI

Dolaşım halinde olan aboneler hizmet aldıkları GPRS operatörünün anlaşmalı olduğu bir başka operatör üzerinden hizmet alabilirler. GPRS aboneleri eğer kendi operatörünün GGSN düğümünü kullanıyorsa şebekeler arasında sinyalleşme mesajları akmaktadır. Bu sebeple GPRS şebekeleri arasında güvenli bir bağlantı kurulmalıdır. Güvensiz bir ara bağlantı önemli bir açıklıktır (Piot,1998).

GPRS şebekelerinin bağlantısı doğrudan bağlantı, ortak bir omurga ile bağlantı ve PDN şebekesi üzerinden bağlantı olmak üzere üç farklı şekilde yapılabilmektedir.

## 9.1 Doğrudan Bağlantı

İki GPRS şebekesi kiralık hat üzerinden birbirlerine bağlanmıştır (Şekil 9-1). Şebekeler arasındaki güvenlik işlemleri ağ geçit cihazları ve güvenlik duvarları ile sağlanmaktadır.




**Şekil 9-1 Doğrudan bağlantı**

### 9.1.1 Ağ Geçit Cihazı

Ağ geçit cihazı iki şebeke arasında güvenliği sağlamak için kullanılmaktadır. Bu cihazlar belirli yönlendirme algoritmaları kullanan yönlendiriciler gibidir. Aynı zamanda IPSec protokolü kullanılarak güvenlik servisleri verirler (Piot,1998).

Ağ geçit cihazı GPRS şebekesinde bulunan abonelerin harici ve güvensiz sistemler ile olan haberleşmelerinin güvenliğinden sorumludur.

Ağ geçit cihazı GPRS şebekesinden dış şebeke ile haberleşecek abone adına IPSec güvenlik birliği kurmaktadır. Haberleşme güvenliği için AH ve ESP protokollerini kullanarak gizlilik, bütünlük ve doğrulama güvenlik hizmetleri vermektedir.

Ağ geçit cihazı, kendi bağlı bulunduğu GPRS şebekesi içinde bulunan bir aboneden hassasiyet seviyesi tanımlı IP paketlerini alır ve bu paketlerin kendisi ile harici şebeke

arasında aktarımı için kullanılacak güvenlik birliğini oluştururken veya seçerken hassasiyet seviyesini dikkate alır. AH ve ESP protokolleri gereği yapılması gereken işlemler (ör.şifreleme) gerçekleştirilerek paket dış ağa gönderilir. Dış ağdan gelen paketler ise tersi bir işlemden geçirilerek GPRS şebekesinde bulunan aboneye ulaştırılır.

### 9.1.2 Güvenlik Duvarı

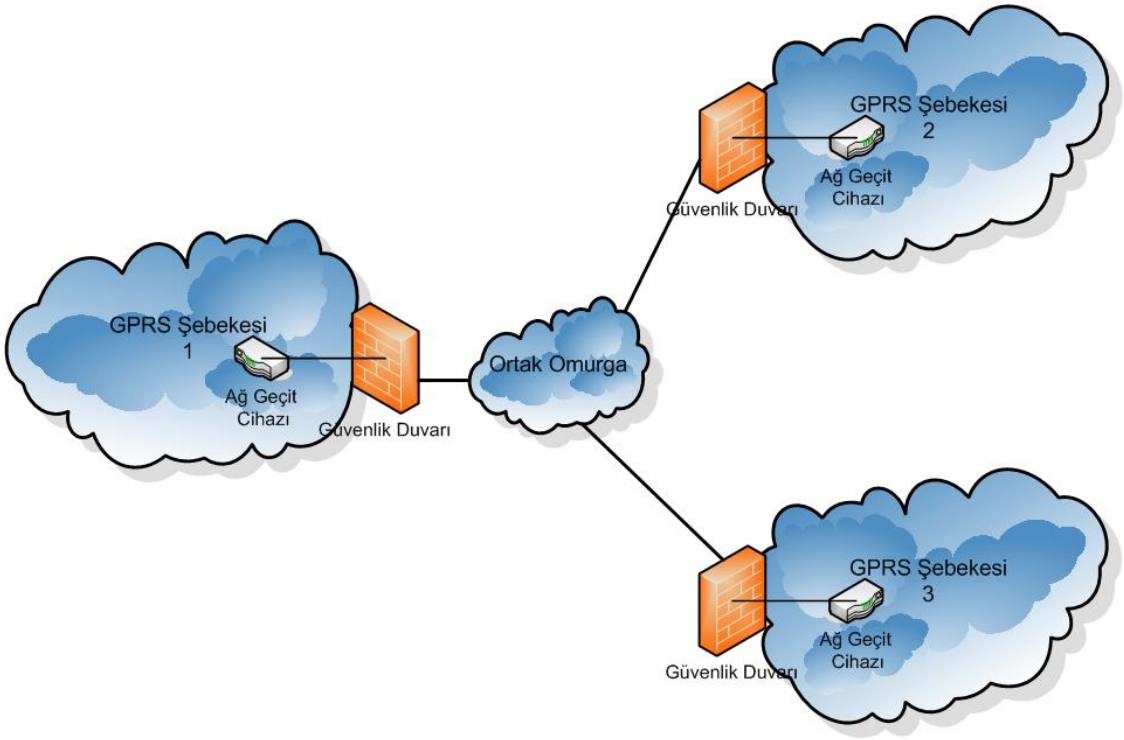
Genel olarak iki şebekeyi birbirinden ayıran cihaz veya uygulama yazılımı olarak tanımlanabilir. GPRS şebekesinin başka bir GPRS şebekesine veya dış bir ağa bağlantısında kullanılmalıdır. Güvenlik duvarı kural setleri ile çalışmaktadır, tanımlanan kural setlerine göre hangi IP adreslerinin hangi IP adresleri ile haberleşeceğine ve hangi servislerin kullanılacağına karar verilir. Bu yöntem ile GPRS şebekesinin veya en genel anlamda iç ağın saldırılardan korunması sağlanır (Piot,1998).

Güvenlik duvarının birinci amacı dış ağlarda bulunanların izin verilen adresler haricindeki adreslere erişimini engellemektir. Bu işlem için kullanılan yöntemler aşağıda verilmiştir.

- **Paket filtreleme:** Bazı özel adreslere dış ağlardan erişim engellenmek istenebilir. Bu durumda ilgili IP adreslere gelen paketler filtrelenir.
- **İstemci erişim listeleri:** Şebeke içerisinde belirli bazı adresler ile haberleşecek olan istemciler belirlenir ve güvenlik duvarına işlenir. Bu sayede istemciler ile iletişim kurulacak olan adresler arasındaki haberleşmeye izin verilmiş olunur.
- **Sunucu erişim listeleri:** Dış ağdan erişilecek olan sunucuların IP adresleri ve hizmet verilecek servis (port numarası, http için 80 vb) güvenlik duvarına işlenir. Bu sayede dışarıya hizmet veren sunucular ile hizmet alan kullanıcılar arasındaki haberleşmeye izin verilmiş olunur.
- **Kullanıcı doğrulama:** Güvenlik duvarı dış ağ üzerinden GPRS şebekesine erişmeye çalışan kullanıcılar için kullanıcı adı ve parola sorabilir. Kullanıcıların girdikleri parolalara göre ilgili servise erişim izni verilir veya istek reddedilir.
- **Adres şaşırtmaca:** Bu yöntemde güvenlik duvarı iç ağa ait IP adresini işaretler ve dış ağda farklı bir IP adresi olarak görüntülenmesini sağlar. Gerçek IP adresinin bilinememesi nedeni ile bu yöntem bilgisayar korsanlarının işini zorlaştırır.

## 9.2 Ortak Bir Omurga İle Bağlantı

Birçok GPRS şebekesi ortak bir omurga üzerinden birbirine bağlanmıştır (Şekil 9-2). Bağlantı için kullanılan ortak omurga genellikle IP tabanlı bir şebekedir.

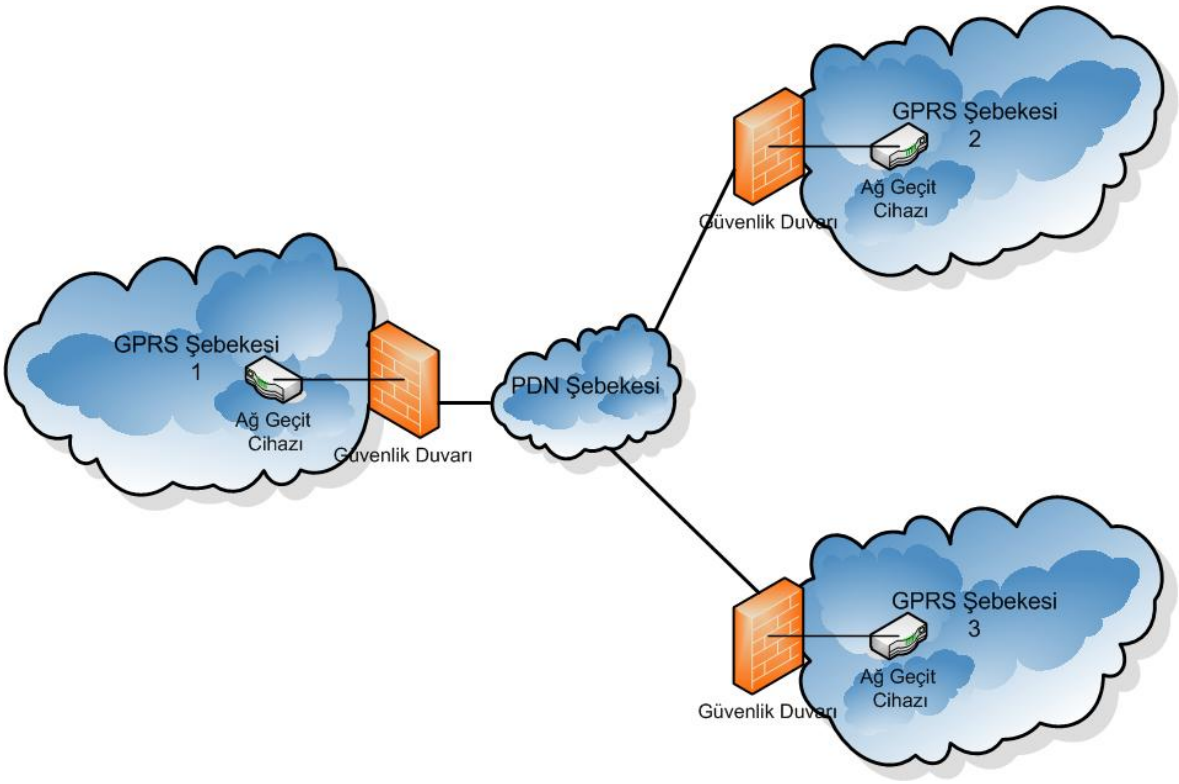



**Şekil 9-2 Ortak bir omurga üzerinden bağlantı**

Doğrudan bağlantıda olduğu gibi güvenlik hizmetleri ağ geçit cihazı ve güvenlik duvarı üzerinden verilmektedir. Ortak omurga üzerinde yönlendirme bilgilerinin değişimi BGP (Sınır ağ geçidi protokolü) ile yapılmaktadır.

## 9.3 PDN Şebekesi Üzerinden Bağlantı

Daha önce aktarılan iki yöntemde Gp arayüzü kullanılmaktadır. PDN şebekesi üzerinde erişimde ise Gi arayüzü üzerinden bağlantı kurulmaktadır. Gi arayüzü GPRS omurgası ile PDN şebekeleri arasındaki bağlantıyı tanımlamaktadır. İki GPRS şebekesinin PDN şebekesi üzerinden bağlanması şebekelerin her birinin PDN şebekesine bağlanması ile oluşmaktadır (Şekil 9-3) (Piot,1998).




**Şekil 9-3 PDN şebekesi üzerinden**

# 10. GPRS ŞEBEKESİ GÜVENLİK TEHDİTLERİ VE ÖNERİLERİ

Bu bölümde GPRS şebekesinde bulunan güvenlik tehditleri incelenecektir. İncelenen tehditlerin tamamı bilgi veya servis ile ilgili erişebilirlik, gizlilik ve bütünlük ile ilgilidir. Aşağıda bu kavramların açıklamaları verilmiştir.

- **Erişilebilirlik:** Servisin istenilen anda erişilebilir ve kullanılabilir olmasıdır.
- **Kimlik Doğrulama:** Haberleşen tarafların kimlik doğrulamasının yapılmasıdır.
- **Yetkilendirme:** Haberleşen tarafların yetki belirlemesinin yapılmasıdır.
- **Gizlilik:** Abone veya sistem bilgilerinin yetkisiz ellere geçmemesidir.
- **Bütünlük:** Abone veya sistem bilgilerinin yetkisiz kişiler tarafından değiştirilememesidir.

## 10.1 Terminal Veya SIM Karta Dair Tehditler ve Öneriler

### 10.1.1 Veri bütünlüğü

GPRS şebekesine bağlı bir mobil istasyon haberleşme için IP protokolünü kullanmaktadır. Bu nedenle ağa bağlı normal bir bilgisayarı etkileyen zararlı kod (virüsler, solucanlar ve Truva atları) tehditleri ile karşı karşıyadır (Kaasin,2001). Günümüzde kullanılan mobil telefonların bazı modelleri üzerinde akıllı işletim sistemleri koşmakta ve üzerine program yüklenip çalıştırılabilmektedir. Yeni yazılan zararlı kodlar artık mobil telefonları da hedef almaktadır. Zararlı kodlardan korunmak amacı ile mobil istasyonlar üzerine (eğer destekliyorsa) anti virüs yazılımı kurulmalı ve güncel tutulmalıdır.

### 10.1.2 Çalınmış mobil telefon veya SIM kart

Mobil telefonların bilgisayardan daha hafif ve küçük olması nedeni ile çalınması daha kolaydır (Kaasin,2001). Çalınmış bir mobil istasyon için iki farklı senaryo vardır. Birincisi SIM kart takılı bir mobil istasyonun çalınması diğeri SIM kart takılı olmayan bir mobil istasyonun çalınmasıdır. SIM kart takılı olmayan bir mobil istasyonun çalınmasının maddi zararı telefonun maliyeti kadardır. Ücretlendirme için kullanılan bilgiler SIM kart üzerindedir. Olası diğer kayıplar SMS mesajlarının ve telefon üzerinde kayıtlı numaralarının kaybıdır. Üzerinde SIM kart takılı bir mobil telefonun çalınması daha ciddi bir sorundur. SIM kart üzerinde kayıtlı bilgilerin kaybına ek olarak çalan kişinin hat iptal ettirilene kadar operatör üzerinden verilen hizmetlerden faydalanması söz konusudur. Çalınma durumu fark edildiği anda GPRS hizmeti alınan operatör ile irtibata geçilerek SIM kartın iptali istenmelidir. Bu tür

durumları engellemek için mobil telefon ve SIM kart güvenliği ile ilgili güvenlik ayarları etkinleştirilmelidir. Çalınan mobil telefonda PIN numarası (SIM karta erişim için gerekli olan parola), telefon kilidi (telefon açıldıktan sonra arama, kısa mesaj gönderme gibi özelikleri kullanmadan önce sorulan parola), güvenlik kodu (telefon üzerinde takılı SIM kartın değiştirilmesi durumunda sorulan parola) gibi bilgilerin bilinmemesi nedeni ile çalan kimse telefonu ve SIM kartı kullanamaz duruma getirilebilir. Telefon kullanımı ile ilgili alınacak önlemler geçici önlemlerdir. Telefonun yazılım güncellemesi yapılarak veya özel bazı yazılımlar kullanarak şifrelerin kırılması mümkündür. SIM karta erişim için verilen PIN kodu tahmin edilemez bir kod olmalıdır. PIN kodu olarak hat sahibinin doğum tarihi, evlilik tarihi gibi önemli tarihler veya bütün kodun aynı rakamdan oluşması (örnek: 1111) gibi PIN kodları kesinlikle kullanılmamalıdır. Aksi durumda SIM kartın başka bir telefona takılması yolu ile hattın kullanılması söz konusudur.

Ülkemizde çalıntı, kaçak veya klonlanmış mobil haberleşme cihazlarının ticaretinden kaynaklı suçların önlenmesine yönelik olarak 5392 numaralı kanunda 2 Temmuz 2005 tarihinde değişiklik yapılmıştır. Kanuna göre Telekomünikasyon Kurumu çalıntı ya da kayıp GSM telefon cihazlarının IMEI numaralarına ait veri tabanı (Kara Liste) oluşturmak ve GSM telefon cihazlarının bloke edilebilmesi için Bilgi ve İhbar Merkezi kurmak ile görevlendirilmiştir. Konu ile ilgili 30 Eylül 2005 tarihinde, İzmir Ticaret Odasında Telekomünikasyon Kurumu Kurul Başkanı, Teknik Düzenleme ve Standardizasyon Dairesi Başkanı ve İzmir Bölge Müdürünün katılımı ile yapılan "2813 Sayılı Telsiz Kanununda Değişiklik Yapılması İle İlgili 5392 Sayılı Kanunun Uygulama Ve Yaptırımları" konulu toplantıda kanunda söz edilen işlere dair çalışmaların devam ettiği, çalışmaların tamamlanmasının ardından GSM işletmecilerinin sistemlerindeki merkezi veri tabanı ile bağlantıların kurulacağı ve sadece yasal GSM telefon cihazlarına hizmet verileceği belirtilmiştir[1].

### 10.1.3 Ödünç alınmış mobil telefon veya SIM kart

Bir diğer tehdit ödünç alınmış telefon veya SIM karttır. GPRS sisteminde ücretlendirme transfer edilen veri miktarına göre yapılmaktadır. Ödünç verilen kimse kendisine verilen bu hakkı kullanım limitlerini aşmak suretiyle kötüye kullanabilir (Kaasin,2001). Buna ek olarak ödünç verilen kimse telefon sahibine ait SMS, telefon numaraları gibi bilgileri edinebilir. Bu tür sebeplerle mobil telefon veya SIM kart tanınmayan kişilere ödünç olarak verilmemelidir.

---

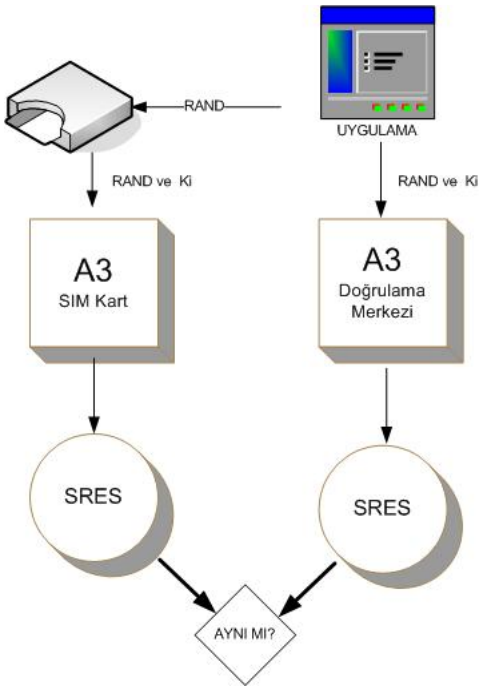
[1] http://www.tk.gov.tr/Etkinlikler/Ulusal_Etkinlikler/Toplantilar/3g.htm

### 10.1.4 Kullanıcı verisi veya doğrulama verisinin gizliliği

Mobil istasyonun çalınması, kaybedilmesi veya ödünç alınması gibi durumlarda eğer PIN kodu, telefon kilidi, güvenlik kodu gibi önlemler alınmamışsa aboneye ait kısa mesajlara veya telefon numaralarına erişmek oldukça kolaydır. Saldırganlar bir sonraki adım olarak SIM kartı bir kart okuyucuya takmak ve SIM kartın içinde saklanan bilgilere ulaşmak için bir yazılım çalıştırmak suretiyle Ki kişisel kimlik anahtarı gibi servis sağlayıcı tarafından verilmiş ve gizli kalması gereken bilgilere erişmeye çalışacaktır.

### 10.1.5 Kopyalanmış SIM kart

SIM kart kopyalamak için gerekli olan bilgiler IMSI numarası ve Ki kişisel kimlik anahtarıdır. Bu işlemin yapılması için en hızlı yöntem SIM karta fiziksel olarak sahip olmaktır. SIM kart içerisindeki Ki kişisel kimlik anahtarının elde edilmesi şu şekilde gerçekleşmektedir; SIM kart üzerinde koşan A3 algoritması girdi olarak şebeke tarafından gönderilen RAND rasgele sayısını ve Ki anahtarını alarak telefona ait sayısal imza (SRES) değerini oluşturmaktadır. SIM kart bir kart okuyucuya yerleştirilerek program çalıştırıldığında, program SIM karta bir RAND sayısı gönderir ve dönen SRES yanıtını alır. Bu andan itibaren kendi içerisinde gömülü A3 algoritmasını çalıştırarak değişen Ki girdilerine karşılık oluşan SRES değerlerini orijinal SRES ile karşılaştırır. Doğru Ki anahtarına ulaşıldığında SRES değerleri birbirine eşittir (Şekil 10-1). Ki anahtarının 128 bit olduğu düşünülürse bu hesaplama günümüz bilgisayarları ile kısa süre içerisinde kırılmaktadır. Tez kapsamında PII 450MHz hızında işlemci ve 256 MB RAM donanıma sahip bir bilgisayar ile yapılan testte 1 saat sonunda Ki kişisel kimlik anahtarına ulaşılmıştır. Kopyalanmış SIM karta sahip olan bir saldırgan gerçek bir abone gibi sistemden hizmet alabilmektedir. SIM kartın kopyalanmaması için mobil telefonun kamuya açık alanlarda ortada bırakılmaması ve kopyalanma riskine karşı ödünç olarak verilmemesi gereklidir.




**Şekil 10-1 SIM kart kopyalama**

### 10.1.6 Onaylanmamış mobil telefon veya donanım kullanımı

Onaylanmamış mobil telefon veya donanım kullanımı şebeke performansını veya diğer abonelere sunulan hizmetin kalitesini olumsuz etkileyebilmektedir (Kaasin,2001). Bu sebeple şebekeye bağlantı sırasında onaylanmış mobil telefon kullanımı tercih edilmelidir.

Ülkemizde, Telekomünikasyon Kurumu'nun 26.01.2005 tarih ve 2005/37 sayılı kararı doğrultusunda GSM telefon cihazlarının piyasaya arzına dair teknik düzenlemeler yapılmıştır. Bu düzenlemeye göre GSM şebekesinde kullanılacak her bir telefon modelinin ETSI TS 100-508 standardına göre IMEI numarasının değiştirilemez olduğunun ispatı istenmektedir. IMEI kara listelerinin kurum bünyesinde bulunan bir veritabanında tutulması ve GSM operatörlerinin bu veritabanı ile bağlantılı çalışması neticesinde onaysız telefon kullanımının önüne geçilmiş olunacaktır.

## 10.2 Gp Arayüzüne Dair güvenlik Tehditleri ve Önerileri

### 10.2.1 Ağ geçit cihazının bant genişliğini doldurma

GPRS servis sağlayıcılarının birbirleri ile olan bağlantılarının ortak bir şebeke üzerinden yapılması durumunda, ortak şebekeye bağlı herhangi bir GPRS servis sağlayıcı, hizmet dışı bırakılmak istenen GPRS hizmet sağlayıcısının ağ geçit cihazına fazla sayıda IP paketleri göndererek Gp arayüzü bant genişliğini doldurabilir. Böyle bir durumda Gp bant genişliği

doldurulan operatörün, diğer operatörlerde bulunan aboneleri hizmet alamaz duruma gelmektedir (Bavosa,2004). Bu tür bir saldırıdan korunmak için Gp arayüzüne konumlandırılacak ağ geçit cihazında paket filtrelemesi yapılmalı ve ortak çalışılan operatörlerin haberleşilecek noktalarının IP adresleri girilmelidir. Operatörler arasında sadece GTP, BGP ve DNS protokollerine ait IP paketlerine izin verilmelidir. Ek önlem olarak ortak şebeke kullanımına dair bir politika hazırlanmalı ve operatörlerin birbirlerine zarar verici hareketlerinin tespiti durumunda kullanılacak yaptırımlar belirtilmelidir.

### 10.2.2 DNS seli saldırısı

GPRS aboneleri isim ve IP adres dönüşümü için DNS sunucularını kullanmaktadır. DNS hizmetinin verilemediği IP şebekeleri dış şebekeler ile olan bağlantısını mantıksal olarak kaybetmektedir. Eğer GPRS servis sağlayıcısının DNS sunucusuna, fazla sayıda doğru veya yanlış alan ismi sorgusu yapılırsa sunucu hizmet veremez duruma gelebilmektedir (Bavosa,2004). Bu tür bir saldırıdan korunmak için DNS sunucuya sorgu gönderebilecek IP adresleri tanımlanmalı ve dışarıdan gelen DNS sorguları güvenlik duvarları veya yönlendiricilerde filtrelenmelidir. Saldırının sorgu yapmaya yetkisiz ağdan gelmesi durumunu tespit edebilmek ve önlemek amacı ile sunucu üzerine veya sunucunun bulunduğu ağa saldırı önleme sistemi (IPS) kurulmalıdır. Sunucunun saldırı olmaksızın devre dışı kalabileceği düşünülerek yedek DNS sunucusu kullanıma hazır olmalıdır.

### 10.2.3 GTP seli saldırısı

GGSN veya SGSN düğümleri yetkisiz GTP trafiği ile meşgul edilerek hizmet veremez duruma getirilebilmektedir. Bu durum aboneleri serbest dolaşım imkanından, Gi arayüzü üzerinden dış şebekelere bağlantı kurmadan veya GPRS şebekesine bağlanmadan yoksun bırakabilmektedir (Bavosa,2004).

Bir abone için veri transferi başlamadan önce içerik etkinleştirilmesi prosedürü çalıştırılmaktadır. Abonenin PDP içerik etkinleştirmesi isteği SGSN tarafından GTP kontrol mesajı kullanılarak GGSN'e iletilmekte ve GGSN içeriğin etkinleştirildiğine veya etkinleştirilmediğine dair GTP kontrol mesajı dönmektedir. İçerik etkinleştirme isteklerinin sayısının çok fazla olması GPRS destek düğümlerinin devre dışı kalmasına neden olabilmektedir. GPRS destek düğümlerinin üzerinde bir saniyede yanıt verilecek GTP kontrol mesajlarının sayısını sınırlandırarak GTP seli saldırısından korunmak mümkündür.

### 10.2.4 Taklit GTP PDP içerik silme mesajı gönderme

Abonenin PDP içeriğine dair tünel belirteci (TID) numarasına sahip olan bir saldırgan, SGSN ve GGSN düğümleri arasında bir aboneye hizmet vermek için kurulmuş bulunan bir tüneli GTP PDP İçerik Silme mesajı göndererek sonlandırabilmektedir (Bavosa,2004). Eğer saldırgan için kimin trafiğini kestiğinin bir önemi yoksa eline geçen her tünel belirteci için içerik silme mesajı göndererek haberleşmeyi sekteye uğratabilir. Bu sebeple saldırganların tünel belirtecini öğrenemeyeceği bir yöntem kullanılmalıdır. Diğer operatörlerin GGSN ve SGSN düğümleri ile IPSec protokolü kullanarak şifreli haberleşme bu yöntemlerden birisidir.

### 10.2.5 Yanlış yönlendirme bilgisi

Serbest dolaşım (roaming) hizmetinin verilmesinde ortak bir şebeke kullanıldığında, şebekeler arasında BGP protokolü ile yönlendirme bilgisi değişimi yapılmaktadır. Saldırganın BGP protokolü çalıştıran yönlendiricilerden birisinin üzerinde kontrol hakkının olması ve bu haktan yararlanarak yanlış yönlendirme kaydı girmesi ortak omurga üzerinde yönlendirme problemlerine yol açacaktır. Böyle bir durum ortak şebekeye bağlı GPRS hizmet sağlayıcılarının serbest dolaşım hizmeti verememesine neden olabilmektedir.

Saldırganların yönlendiriciler üzerinde hak sahibi olmaması için yönlendiriciler üzerinde güvenli parolalar tanımlamak (operatörün parola politikasına uygun olarak), yönetim için erişilecek IP bloğu tanımlamak, son yazılım güncellemelerini yüklemek ve takip etmek gibi güvenlik sıkılaştırmaları yapılmalıdır. Bu tür bir saldırı yönlendiriciler üzerinde yönetim hakkına sahip kullanıcıların parolalarını çaldırması durumunda da söz konusudur. Bu sebeple ortak omurga hizmetini veren kurumda güvenlik araştırması yapılmış personel çalıştırılmalı ve personel için güvenlik bilinçlendirme eğitimleri planlanmalıdır.

### 10.2.6 DNS ön bellek zehirleme

DNS ön bellek zehirlemesi saldırı yöntemi ile GPRS hizmeti alan abonelerin DNS sorgularına yanlış IP adresleri döndürülebilmektedir. Bu durum abonelerin istedikleri şebekeye erişmesini engellemektedir. Bu tür bir saldırıyı engellemek için DNS uygulamasının yapılandırmasında açıklık oluşturabilecek parametreler uygun olarak ayarlanmalıdır. Bu parametreler uygulamadan uygulamaya değişebilmektedir. Örneğin Windows 2000 SP3 ve altı işletim sistemlerinde "Secure cache against pollution" seçeneği ilk kurulumda etkin değildir. El ile etkinleştirilmesi gereklidir. Windows 2000 SP3 ve üzeri işletim sitemlerinde ilk kurulumda etkin olarak gelmektedir. Bu ayarlamalara ek olarak kullanılan DNS sunucusunun işletim sistemi ve DNS uygulamasının son yamaları yapılmış olmalıdır.

### 10.2.7 Taklit PDP içerik isteği oluşturulması

GTP protokolü içerisinde SGSN ve GGSN düğümleri için herhangi bir doğrulama mekanizması bulundurmamaktadır. Uygun bilgilere (PDP tipi, APN adresi, TID, IMSI ve NSAPI numaraları) sahip olan bir saldırgan SGSN düğümünü taklit ederek GGSN ile arasında GTP tüneli kurabilmektedir (Bavosa,2004). Saldırgan bu yol ile GPRS şebekesi içerisinde aboneyi taklit edebilmekte ve abonenin erişim hakkı olan yerlere (örneğin şirket ağına veya internete) erişebilmektedir. Bu tür bir saldırıdan korunmak için GGSN düğümleri üzerinde erişim kontrol listeleri tanımlanarak haberleşilecek düğümler belirtilmelidir. Ek olarak ağ geçit cihazları üzerinde operatörlerde bulunan GPRS destek düğümlerinin IP adresleri tanımlanmalı ve sadece izin verilen düğümler arasında iletişime izin verilmelidir.

### 10.2.8 Taklit PDP içerik güncelleme isteği mesajı

Bir saldırgan kendisine ait bir SGSN düğümü oluşturarak GTP tünellerini işleyen bir GGSN'e taklit PDP içerik güncelleme mesajı göndererek kendisini GTP oturumuna dahil edebilmektedir. Taklit PDP içerik güncellemesi için oturuma dair TID numarasının bilinmesi gereklidir. Bu yöntem ile saldırgan abonenin veri bağlantısını çalabilmekte ve gerçek abone gibi haberleşebilmektedir. Taklit PDP içerik güncelleme isteği saldırısından korunmak için GGSN üzerinde haberleşilecek SGSN düğümleri belirtilmeli ve ağ geçit cihazları üzerinde sadece izin verilen düğümler arasında iletişime izin verilmelidir.

### 10.2.9 Fazla ücretlendirme saldırısı

Böyle bir saldırı, kötü niyetli bir saldırganın başka bir mobil istasyona ait IP adresini öğrenmesi ile başlamaktadır. Saldırgan hedef aboneye fazla ücretlendirme saldırısı yapmak amacı ile bir web sitesi üzerinden dosya indirme işlemi başlatmakta ve oturumdan çıkmaktadır. Bu durumda indirilen bilgiler doğrudan saldırı altında olan mobil istasyona gelmektedir. Ücretlendirmenin toplam veri transferi üzerinden olması nedeni ile saldırı altında olan mobil istasyona fazladan ücretlendirme yapılmaktadır. Aynı yöntem ICMP mesajlarına yanıt veren bir sunucuya mobil istasyon adına kaynak IP adresi değiştirilmiş ICMP paketleri göndermek yolu ile de yapılabilmektedir. Bu saldırı sadece Gp arayüzü için değil Gi ve Gn arayüzleri içinde geçerlidir. Fazla ücretlendirme saldırılarını engellemek için arayüzler üzerinde duruma göre (stateful) paket filtrelemesi yapan güvenlik duvarları kullanılmalıdır. Bu tür güvenlik duvarları kullanılarak abonenin başlatmadığı trafik engellenmektedir. Ayrıca mobil istasyonun şebekeden kopması (pilinin bitmesi veya kapsama alanı dışına çıkması) sonucunda aktif haberleşme olmayan oturumlar GGSN tarafından sonlandırılmalıdır.

### 10.2.10 Abone bilgilerinin ele geçirilmesi, değiştirilmesi

SGSN ve GGSN arasında akan trafiğin şifrelenmemesi nedeni ile düğümler arasındaki trafiği dinleyebilen bir saldırgan abone oturumunu çalmak için gerekli bilgileri (PDP tipi, APN adresi, TID, IMSI ve NSAPI numaraları gibi) edinebilir. Ayrıca açık metin (şifresiz) haberleşme nedeni ile abone verisi okunabilir veya değiştirilebilir (Peng,2000). Bu tür bilgilerin açığa çıkmaması, abone bilgilerinin gizliliği ve bütünlüğü için GPRS düğümleri veya düğümler arasında haberleşmeyi sağlayan ağ geçit cihazları arasında IPSec veya benzer bir şifreleme protokolü ile şifreleme yapılması gereklidir.

## 10.3 Gi Arayüzüne Dair Güvenlik Tehditleri ve Önerileri

Gi arayüzü GPRS şebekesinin internete, kurumsal şebekelere veya diğer ağ hizmet sağlayıcılarına olan arayüzüdür. Abone uygulamasının herhangi bir uygulama olabilmesi nedeni ile Gi arayüzü üzerinden akan trafik ile internet üzerinden akan trafik arasında herhangi bir fark yoktur. Bu sebeple bugün internete bağlı bir bilgisayarın sahip olduğu her türlü problem mobil istasyon içinde geçerlidir. Bu problemlerin başlıcaları virüsler, solucanlar, Truva atları, hizmet dışı bırakma saldırılarıdır.

### 10.3.1 Gi bant genişliğinin doldurulması

Bir GPRS şebekesi, Gi bant genişliğinin doldurulması durumunda dış ağlara olan bağlantısını kaybetmektedir (Bavosa,2004). Bir saldırgan hizmet dışı bırakma (DoS) veya dağıtık hizmet dışı bırakma(DDoS) saldırıları gibi çeşitli yöntemler kullanarak GPRS şebekesinin Gi bant genişliğini doldurabilir. Birçok saldırganın bulunması nedeni ile özellikle dağıtık hizmet dışı bırakma saldırılarından korunmak oldukça zordur. Karşı önlem olarak Gi arayüzününden akacak trafiğin birden fazla hat ile desteklenmesi ve saldırı durumunda trafiğin aktığı yolun değiştirilerek saldırganların devre dışı bırakılması sağlanabilmektedir. En etkili yöntem internet hizmet sağlayıcısında bulunan güvenlik duvarında filtreleme işlemi yaptırtılarak saldırıyı engellemektir.

### 10.3.2 Mobil istasyona doğru aşırı trafik oluşturulması

Mobil istasyonun sahip olduğu IP adresine doğru trafik oluşturulması durumunda, hava arayüzünün bant genişliğinin düşük olması nedeni ile mobil istasyon hizmet alamaz duruma gelebilmektedir. Bu sebeple abone tarafından başlatılmayan bir haberleşmeye dair trafik mobil istasyona gelmemelidir. GPRS operatörünün kullandığı güvenlik duvarlarının duruma göre (stateful) filtreleme özelliği olmalıdır. Bu özellik aynı zamanda fazla ücretlendirme

saldırılarından da korunmayı sağlayacaktır.

### 10.3.3 Doğrulama ve Yetkilendirme İle İlgili Tehditler

GGSN ile bağlı bulunan kurumsal ağlar arasında gizliliği ve bütünlüğü sağlamak için IPSec protokolü ile tünel oluşturularak haberleşildiğinde bile, bir mobil istasyon başka bir mobil istasyonun IP adresini kullanarak erişememesi gereken kurumsal ağa erişebilmektedir. Bu tür bir saldırıdan korunmak üzere kurumsal ağlara erişim için uçtan uca sanal özel ağlar (VPN) kullanılmalıdır. Bu sayede hem erişim kısıtlanmış hem de arada GPRS şebekesi üzerinden akan trafiğin gizliliği sağlanmış olmaktadır.

### 10.3.4 Gizlilik ve Bütünlük İle İlgili Tehditler

IPSec veya uygulama katmanı gibi güvenlik mekanizmaları kullanılmadığı sürece mobil istasyondan kurumsal ağa veya internete giden bilgilere dair hiç bir koruma yoktur. Abone bilgisi hakkı olmayan kişiler tarafından görülebilir ve yetkisiz olarak değiştirilebilir. Bu problemin giderilmesi için kurumsal ağa erişimlerde sanal özel ağlar kullanılmalıdır. Internet erişimi için bu problemin çözümü güvenli http (secure http – https) gibi uygulama katmanı protokolleri kullanarak iletişimde bulunmaktır.

## 10.4 Gn Arayüzüne Dair Güvenlik Tehditleri ve Önerileri

GPRS hizmet sağlayıcıları sadece dış ağlardan gelen saldırılara odaklanmamalı, iç ağdan (abonelerden veya çalışanlardan) gelebilecek saldırılara karşı da hazırlıklı olmalıdır.

### 10.4.1 SGSN ve GGSN düğümleri arasına girme

Saldırgan kendisini GPRS şebekesinin bir paçasıymış gibi göstererek SGSN veya GGSN düğümlerinin arasına (man in the middle) girebilmektedir. Bu andan itibaren saldırgan abonelere ait trafiği dinleyebilmekte ve IP paketlerini değiştirebilmektedir. Kurum içinde bu tip bir saldırının olmasını engellemek için SGSN ve GGSN düğümleri arasında GTP protokolüne ek olarak IPSec protokolü ile tünel tanımlanmalıdır. IPsec kullanımı saldırganın araya girmesini engellememekte, fakat gördüğü IP paketlerin şifreli olmasını sağlamaktadır. Şifreleme için kullanılan anahtarların saldırgan tarafından bilinmemesi nedeni ile haberleşme gizli kalmaktadır. IPSec protokolünde bütünlük hizmetinin de verilmesi nedeni ile paketler üzerinde herhangi bir değişime izin verilmemektedir. Saldırganın pakette değişiklik yapması durumunda paket alıcı tarafta bozuk olarak algılanıp çöpe atılmaktadır.

### 10.4.2 Bir aboneden başka abonelere saldırı

Mantıksal olarak aynı GGSN'e bağlı bütün aboneler aynı ağın bir parçasıdır ve birlerine olan iletişimi filtrelenmemektedir. Saldırıların büyük kısmının iç ağdan geldiği düşünülürse abonelerin birbirleri ile olan iletişiminin mutlaka bir güvenlik duvarı ile filtrelenmesi gereği ortaya çıkar. Trafiğin filtrelenmemesi durumunda, abonelerin başka abonelerin mobil istasyonlarının açıklıklarından faydalanarak yazılım kurması ve hedef mobil istasyon üzerinden veri transferi başlatması mümkündür. Abonenin diğer abonelerin saldırılarından etkilenmemeleri için antivirüs yazılımı, kişisel güvenlik duvarı gibi güvenlik ürünlerini kullanması gereklidir.

### 10.4.3 Taklit GTP PDP içerik silme mesajı

Gn arayüzünü dinleyebilen bir saldırgan abonenin PDP içeriğine dair tünel belirteci (TID) numarasını öğrenebilmektedir. Bu bilgi kullanılarak SGSN ve GGSN düğümleri arasında kurulmuş bir tüneli GTP PDP içerik silme mesajı göndererek silebilmektedir. Eğer saldırgan için kimin trafiğini kestiğinin bir önemi yoksa eline geçen her tünel belirteci için içerik silme mesajı göndererek haberleşmeyi kesintiye uğratabilmektedir. Bu saldırıdan korunmak için saldırganın Gn arayüzünü dinlemesini engelleyecek veya dinlese bile TID numarasını öğrenmesini imkansız kılacak bir yöntem kullanılmalıdır. SGSN ve GGSN cihazlarının güvenli bölgelerde bulunması ve haberleşme için kullanılan Ethernet anahtarlarına erişim kısıtlaması uygulanabilecek yöntemlerdendir. Diğer bir yöntem GGSN ve SGSN düğümleri arasında IPSec protokolü kullanarak şifreleme yapmaktır.

### 10.4.4 Dinleme Yolu İle Bilgi Edinme

SGSN ve GGSN arasında bulunan haberleşme GTP protokolü üzerinden ve açık metin olarak yapılmaktadır. Gn arayüzüne erişebilen bir saldırgan trafiği dinlemek yolu ile ihtiyaç duyduğu bilgileri (PDP tipi, APN adresi, TID, IMSI ve NSAPI numaraları gibi) ele geçirerek başka saldırılar (örnek: taklit GTP PDP içerik silme) gerçekleştirebilir. Ek olarak, şifresiz haberleşme nedeni ile akan trafik içerisindeki abone verisi dinleyen saldırgan tarafından ele geçirilebilir veya değiştirilebilir. Gn arayüzü üzerinden şifreli haberleşerek, GPRS düğümlerinin haberleşmesini sağlayan Ethernet anahtarları üzerinde erişim kısıtlaması yaparak, Gn arayüzü üzerinde saldırıları tespit etmesi ve önlemesi için saldırı önleme sistemi (IPS) kullanarak saldırganların dinleme yolu ile bilgi edinmesi engellenmelidir.

## 10.5 Genel Güvenlik Önerileri

### 10.5.1 Risk Yönetimi Süreci

GPRS şebekesinin kendi risklerini belirleyerek karşı önlemlerini alabilmesi için bir risk yönetimi süreci olmalıdır. Risk yönetimi süreci risk analizi, risk değerlendirmesi ve risk tedavisi olmak üzere üçe ayrılabilir. Risk analizi sürecinde tehdit altında bulunan kritik bilgi varlıklarının neler olduğu çıkarılmalı, varlıklara önem derecesine göre (çok kritik, kritik, orta kritik, az kritik) değerler verilmelidir. Bir sonraki adım olarak varlıklarda bulunan açıklıklar ve bu açıklığı kullanarak varlığa zarar verebilecek tehditler ortaya konulmalıdır. Tehdidin gerçekleşmesi durumunda kurumun göreceği zararın boyutu (etkisi) ön görülmelidir. Bir tehdit ile ilişkili risk değeri, basit olarak tehdidin gerçekleşmesi durumunda vereceği zarar ve gerçekleşme ihtimalinin çarpımı olarak hesap edilebilir. Risk analizi çalışması tamamlandığında operatörün taşıdığı riskler ve bu risklerin seviyeleri (çok yüksek risk, yüksek risk, orta risk, az risk) belirlenmiş olmalıdır. Bir sonraki aşamada (risk değerlendirilmesi) bu risklerin bütçe, maliyet ve kullanılabilirlik gibi kriterler doğrultusunda değerlendirilmesi gereklidir. Uygulanacak karşı önlem riski ortadan kaldırmak olabileceği gibi risk seviyesini düşürmek veya riski kabul etmekte olabilir. Risk tedavisi kısmında ise karşılanması ön görülen riskler ile ilgili karşı önlemlerin uygulama planı çıkartılmalı ve plana uygun olarak riskler kapatılmalıdır.

GPRS operatörünün bu süreci bir yaşam döngüsüne oturtması ve risklerini sürekli kontrol altına alması önerilmektedir. Teknolojinin sürekli değişmesi ve her gün yeni saldırı tekniklerinin ortaya çıkması risk yönetim sürecinin yapılmasını adeta zorunlu kılmaktadır.

### 10.5.2 GPRS Şebekesi Güvenlik Politikası

Gerek operatörün gerek kendisinin gerek abonelerinin mağdur durumda kalmaması için GPRS şebekesine ait bir güvenlik politikası dokümanı bulunmalı ve işletilmelidir. Politika dokümanında aşağıda belirtilen konuların açık olarak belirtilmesi gereklidir.

1. Korunması gereken varlıkların neler olduğu
2. Kimlerden korunması gerektiği
3. Varlıkların hangi yöntemler kullanılarak korunacağı
4. Güvenlik ile ilgili sorumluların kimler olduğu
5. Güvenlik kayıtlarının nasıl ve kimler tarafından inceleneceği

6. Acil durumlarda nasıl hareket edileceği
7. Güvenlik olayları sonucunda nasıl değerlendirme yapılacağı
8. Politikanın sahibinin kim olduğu
9. Dolaşım anlaşması yapılan operatörler ile yapılan sözleşmenin içeriğinde dikkat edilmesi gereken hususların neler olduğu

### 10.5.3 GPRS Şebekesi Konfigürasyon ve Çalışma Esasları

GPRS şebekesinin işletilebilmesi ve görev değişiklikleri nedeni ile sistemin kesintiye uğramaması amacı ile GPRS şebekesinin çalışmasına dair esasların belirtildiği bir doküman bulunmalıdır. Bu dokümanın en az aşağıdaki bilgileri içermesi beklenmektedir.

1. Şebeke içerindeki trafiğin akışı
2. Bileşenlerden sorumlu personelin görevleri ve sorumlulukları
3. Güvenlik duvarı, ağ geçit cihazı gibi güvenlik bileşenlerinin konfigürasyon bilgileri
4. GPRS omurgasının IP adres dağılımı
5. Abonelere verilen IP adreslerinin dağılımı
6. Sistemin işletimine dair kayıtların izlenme yöntemi
7. Yeni bileşen ekleme ve çıkarmanın hangi kurallara göre yapılacağı
8. Konfigürasyon ve çalışma esasları dokümanının güncellenmesine dair hususlar

### 10.5.4 Sistemlere Erişim Kontrolü

Operatör personeli sistemlere belirli kurallar çerçevesinde erişmelidir. Bu kuralları düzenleyen bir erişim kontrol politikası bulunmalı ve personelin politikaya uyması sağlanmalıdır.

GPRS şebekesi erişim kontrol politikasında aşağıdaki maddeler göz önünde bulundurulmalıdır:

1. Şebekenin kritik cihazlarına erişim yetkilendirmesi
2. Şebekenin kritik bilgilerinin saklanma ve erişim yöntemleri
3. Erişim için kullanılacak kullanıcı adı ve parolalarının standardı

4. Özel güvenlik gerektiren odalara giriş için kullanılacak teknikler ve uygulaması
5. Ortak yapılan işler için standart kullanıcı erişim tanımları (örneğin SGSN işletmeni erişim hakları)
6. Cihazlara ve güvenli alanlara erişim ile ilgili kayıtların tutulması

### 10.5.5 Üçüncü Taraflar İle Yapılan Sözleşmeler

İnternet servis sağlayıcı, altyüklenici ve bağlı bulunan GPRS operatörleri ile güvenlik konularının içerisinde bulunduğu sözleşmeler yapılmalıdır. Sözleşmelerde karşılıklı sorumluluklar, kurumsal varlıkların korunma biçimleri, operatör şebekesine yapılan erişimin ne şekilde yapılacağı, sözleşmeye uyulmaması durumunda uygulanacak yaptırımlar gibi konular bulunmalıdır. Üçüncü tarafların GPRS şebekesine erişen personeli için güvenlik bilinçlendirme eğitimleri hazırlanmalıdır.

### 10.5.6 Eğitimler

Operatör personelin teknik yetkinliğini arttırmak için senelik olarak eğitim planlaması yapılmalıdır. Ek olarak GPRS hizmeti vermek için kullanılan sistemlere erişim izni olan her personel için güvenlik politikaları ve prosedürleri konusunda gerekli eğitimler hazırlanmalı ve personelin bu eğitimlere katılımı zorunlu tutulmalıdır.

# 11. GPRS ŞEBEKESİ GÜVENLİK TEST TALİMATI

Bu bölümde GPRS şebekeleri için kullanılabilecek örnek test adımları belirlenmiştir. Belirlenen testler Ericsson Mobility World GPRS şebekesinde uygulanmış ve sonuçları EK 1'de verilmiştir.

## 11.1 GPRS Şebekesi Güvenlik Politikası Dokümanı Testi

Güvenlik gereksinimi olan sistemlerde güvenlik politikası dokümanı bulunmalı ve işletilmelidir. Politika dokümanında aşağıda belirtilen konuların açık olarak belirtilmesi gereklidir.

1. Korunması gereken varlıkların neler olduğu
2. Kimlerden korunması gerektiği
3. Varlıkların hangi yöntemler kullanılarak korunacağı
4. Güvenlik ile ilgili sorumluların kimler olduğu
5. Güvenlik kayıtlarının nasıl ve kimler tarafından inceleneceği
6. Acil durumlarda nasıl hareket edileceği
7. Güvenlik olayları sonucunda nasıl değerlendirme yapılacağı
8. Politikanın sahibinin kim olduğu
9. Dolaşım anlaşması yapılan operatörler ile yapılan sözleşmenin içeriğinde dikkat edilmesi gereken hususların neler olduğu

### 11.1.1 Test Yöntemi

GPRS şebekesinin güvenlik politikası olup olmadığına, eğer varsa yukarıda belirtilen hususların belirtilip belirtilmediğine bakılacaktır.

### 11.1.2 Beklenen Sonuç

GPRS şebekesinin bir güvenlik politikası olmalı ve işletilmelidir. İçeriğinde yukarıda belirtilen hususların bulunması gereklidir.

## 11.2 GPRS Şebekesi Konfigürasyonu ve Çalışma Esasları Dokümanı Testi

GPRS şebekesinin düzgün işletilebilmesi ve görev değişikliklerinden sistemin etkilenmemesi

amacı ile GPRS şebekesinin çalışmasına dair esasların belirtildiği bir doküman bulunmalıdır. Bu dokümanın en az aşağıdaki bilgileri içermesi beklenmelidir.

1. Şebeke içerisindeki trafiğin akışı
2. Bileşenlerden sorumlu personelin görevleri ve sorumlulukları
3. Güvenlik duvarı, ağ geçit cihazı gibi güvenlik bileşenlerinin konfigürasyon bilgileri
4. GPRS omurgasının IP adres dağılımı
5. Abonelere verilen IP adreslerinin dağılımı
6. Sistemin işletimine dair kayıtların izlenme yöntemi
7. Yeni bileşen ekleme ve çıkarmanın hangi kurallara göre yapılacağı
8. Konfigürasyon ve çalışma esasları dokümanının güncellenmesine dair hususlar

### 11.2.1 Test Yöntemi

GPRS şebekesinin konfigürasyon ve çalışma esasları dokümanı olup olmadığına, eğer varsa yukarıda belirtilen hususların belirtilip belirtilmediğine bakılacaktır.

### 11.2.2 Beklenen Sonuç

GPRS şebekesinin yapılandırma ve çalışma esasları dokümanı olmalı ve işletilmelidir. İçeriğinde yukarıda belirtilen hususların bulunması gereklidir.

## 11.3 Gi Bant Genişliği Testi

Şebekenin Gi bant genişliğinin doldurulması durumunda şebeke kullanıcılarına hizmet veremez duruma gelebilmektedir. Bu tür saldırılar genelde servis dışı bırakma saldırıları olarak bilinmektedir ve engellenmeleri oldukça zordur. Karşı önlem olarak, şebekenin internet bağlantısının çoklu yoldan olması tercih edilmelidir.

### 11.3.1 Test Yöntemi

Gi arayüzünden akacak trafiğin birden fazla hat ile desteklenip desteklenmediği sorgulanacaktır. Saldırı durumunda trafiğin aktığı yolların ne şekilde değiştirildiği incelenecektir. GPRS operatörü izin veriyorsa Gi arayüzü IP adresleri öğrenilecek ve Gi arayüzüne doğru trafik oluşturarak bant genişliği doldurulacaktır. Bu esnada şebekenin yanıtı incelenecektir.

### 11.3.2 Beklenen Sonuç

Gi arayüzü bağlantıları çoklu olmalı ve geçiş otomatik olarak yapılmalıdır.

## 11.4 Gizlilik ve Bütünlük Test Adımı

GPRS şebekesi içerisinde abone verisinin gizlilik ve bütünlüğünün korunması amacı ile herhangi bir koruma yoktur. Abone verisi GPRS omurgasına erişebilen kişiler tarafından görüntülenebilmekte ve istenirse bütünlüğü bozulabilmektedir. Abone verisinin GPRS omurgası boyunca şifreli olarak gönderilmesi tercih edilmelidir.

### 11.4.1 Test Yöntemi

SGSN ve GGSN düğümleri arasında herhangi bir şifreleme tekniği kullanılıp kullanılmadığı incelenecektir. Eğer karşı operatör de destekliyorsa gezgin aboneler içinde şifreleme mümkün olmalıdır.

### 11.4.2 Beklenen Sonuç

SGSN ve GGSN düğümleri arasında şifreli haberleşme olmalıdır.

## 11.5 Aboneler Arası Saldırı Testi

GPRS şebekesine bağlı olan abonelerin tamamı şebekenin bir parçasıdır ve birbirlerine saldırıda bulunabilir. Abonelerin başka abonelerin mobil istasyonlarının açıklıklarından faydalanarak cihaza girmesi, gizli bilgileri ele geçirmesi, program kurması veya internet üzerinden bir indirme işlemi başlatması mümkündür.

### 11.5.1 Test Yöntemi

İki ayrı mobil istasyondan GPRS şebekesine erişilecektir. Bir mobil istasyondan karşı mobil istasyona erişim testi yapılacaktır. Bu testlerden bazıları şunlardır.

1. Karşı mobil istasyona ping komutu ile ICMP paketleri göndermek.
2. Karşı mobil istasyon için açıklık taraması yapmak.
3. Karşı mobil istasyonun açık TCP portlarını taramak.

### 11.5.2 Beklenen Sonuç

Ne tür bir erişim testi yapılırsa yapılsın bir mobil istasyondan diğer mobil istasyonlara erişilememelidir.

## 11.6 Internet Üzerinden Saldırı Testi

GPRS aboneleri şebekeye bağlandıkları anda bir IP adresi almaktadır. Abonelere ait bu IP adreslerine bazı özel uygulamaların getirdiği zorunluluklar haricinde ulaşılamamalıdır. GPRS sisteminde ücretlendirmenin transfer edilen veri miktarı üzerinden olması nedeni ile operatörlerin abonelerini korumak üzere gerekli önlemleri (güvenlik duvarları, erişim kontrol listeleri, geçit cihazları) almış olmalıdır.

### 11.6.1 Test Yöntemi

GPRS abonesi olarak şebekeye bağlanılacaktır. Internet üzerinden GPRS şebekesinin aboneye vermiş olduğu IP adresine doğru trafik oluşturulacaktır. Abone mobil istasyonu üzerinde çalıştırılacak bir paket dinleme uygulaması ile internet üzerinden oluşturulan trafiğin aboneye ulaşıp ulaşmadığı kontrol edilecektir.

### 11.6.2 Beklenen Sonuç

Aboneye kendisinin oluşturduğu bağlantılar haricinde hiçbir suretle trafik akmamalıdır.

## 11.7 GPRS Omurgası Bileşenleri Açıklıkları Testi

GPRS omurgasını oluşturan bileşenler (özellikle SGSN ve GGSN) işletim sistemi olan cihazlardır. Bu cihazların kullandıkları işletim sistemlerinden ve ilgili yamaların kurulmamış olmasından kaynaklanan açıklıklar olabilmektedir. Bir saldırgan işletim sistemi açıklıklarından faydalanarak sistemlere girebilir, abone verisini kesme, dinleme, yönlendirme ve bozma gibi faaliyetlerde bulunabilir.

### 11.7.1 Test Yöntemi

En son açıklıklarında yüklü olduğu bir açıklık tarayıcısı kullanılarak sistemler taranacak ve mevcut risk durumu ortaya konacaktır.

### 11.7.2 Beklenen Sonuç

Hiçbir açıklık bulunamaması veya bulunan açıklıkların risk derecelerinin düşük olması istenen durumdur.

## 11.8 Abone IP Adreslerinin Dağıtımı (NAT kullanımı) Testi

GPRS şebekelerine dağıtılan IP adreslerini internetten izole etmek amacı ile özel kullanım için ayrılmış 192.168.0.0, 172.16.0.0 veya 10.0.0.0 adreslerinden dağıtım yapılması

uygundur. Bu adresler internet üzerinde kullanılmayan adreslerdir ve internet bağlantısı için bir adres çevrimi gerektirir. Bu adres çevrimi ağ adresi çevrimi (NAT) olarak adlandırılmaktadır. NAT tekniğinde bire bir eşleme mantığı kullanılmamalı özel IP ye sahip aboneler bir veya birkaç IP üzerinden internete çıkarılmalıdır.

### 11.8.1 Test Yöntemi

GPRS şebekesine bağlanılacak ve tahsis edilen IP adresinin yukarıda belirtilen adres gruplarından olup olmadığı kontrol edilecektir.

### 11.8.2 Beklenen Sonuç

GPRS şebekesine bağlanıldığında tahsis edilen IP adresi özel kullanım için ayrılmış IP adreslerinden olmalıdır.

## 11.9 Güvenlik Duvarı ve Ağ Geçit Cihazları Testi

Aboneler arası trafiği, aboneler tarafından başlatılmamış (Internet üzerinden veya diğer operatörlerin şebekelerinden gelen) trafiği filtreleyen bileşenler GPRS şebekesine eklenmiş olmalıdır.

### 11.9.1 Test Yöntemi

GPRS şebekesinin internet ve diğer GPRS şebekelerine olan bağlantı uçlarında trafik filtreleme amacı ile güvenlik duvarı bulunup bulunmadığına bakılacaktır. Ayrıca GPRS şebekeleri arasında ağ geçit cihazı kullanıp kullanılmadığı, eğer kullanılıyorsa şifreleme yapılıp yapılmadığı incelenecektir.

### 11.9.2 Beklenen Sonuç

Internet trafiğini filtreleyen güvenlik duvarı, diğer GPRS şebekeleri ile iletişimi düzenleyen ve şifreleyen ağ geçit cihazı bulunmalıdır.

## 11.10 Aboneye IP adreslerinden SGSN ve GGSN Sistemlerine Erişim Testi

Abonelere tahsis edilen IP adresleri ile GPRS omurgasında kullanılan IP adresleri farklı IP adres uzaylarında olmalı ve bu uzaylar arasında iletişim bulunmamalıdır.

### 11.10.1Test Yöntemi

GPRS şebekesine bağlanılacak ve aboneye tahsis edilen IP adresinde SGSN ve GGSN cihazlarına ulaşılmaya çalışılacaktır. En basit anlamda ping, telnet ve ssh komutları ile erişim

olup olmadığı test edilecektir.

#### 11.10.2Beklenen Sonuç

Abone IP adreslerinden GPRS omurgasında bulunan cihazlara erişim bulunmamalıdır.

### 11.11 SGSN ve GGSN Düğümleri Erişim Kontrol Listeleri Testi

Saldırganlar tarafından GPRS şebekesine taklit SGSN ve GGSN düğümleri eklenerek ücretsiz internet bağlantısı sağlamak mümkündür. Bu sebeple SGSN ve GGSN düğümleri üzerinde haberleşecekleri düğümlere ait adres bilgilerinden oluşan erişim kontrol listeleri bulunmalıdır. Bu sayede GPRS omurgasını oluşturan düğümler birbirleri ile haberleşecek fakat saldırganlar tarafından sisteme eklenebilecek Taklit SGSN ve GGSN düğümleri asıl düğümler ile haberleşemeyecektir.

#### 11.11.1Test Yöntemi

SGSN ve GGSN düğümleri üzerinde erişim kontrol listesi bulunup bulunmadığına, eğer varsa düğümlere ait IP adreslerin işlenip işlenmediğine bakılacaktır.

#### 11.11.2Beklenen Sonuç

SGSN ve GGSN düğümleri üzerinde erişim kontrol listeleri bulunmalı ve ilgili IP adresleri işlenmiş olmalıdır.

### 11.12 GTP PDP İçerik Silme, İçerik Güncelleme ve İçerik Oluşturma Test Adımı

SGSN ve GGSN düğümleri arasında GTP protokolü kullanılarak haberleşme sağlanmaktadır. Her bir abone oturumu için bir PDP içerik etkinleştirmesi yapılarak tünel kurulmaktadır. Bir saldırgan GTP PDP içerik silme mesajı göndererek abone oturumunu kesebilmekte veya içerik güncelleme mesajı göndererek abone oturumunu çalabilmektedir. Bu problem GTP protokolünün doğasından kaynaklanmaktadır. Bu sayılanlara ek olarak arada akan trafiğin yeniden gönderilmesi sureti ile yeni PDP içeriği oluşturulabilmektedir. Önlem olarak düğümler arasında IPSec protokolü kullanılarak PDP mesajları şifrelenmeli, şifresiz mesajlar kabul edilmemelidir. Düğümler arasında IPSec protokolü ile şifreleme yapılması aynı zamanda abone verisinin gizlilik ve bütünlüğünü de koruyacaktır.

### 11.12.1Test Yöntemi

SGSN ve GGSN düğümleri arasında IPSec protokolü ile şifreleme yapılıp yapılmadığı incelenecektir.

### 11.12.2Beklenen Sonuç

SGSN ve GGSN düğümleri arasında IPSec protokolü ile şifreleme olmalıdır.

# 12. ÖRNEK GPRS SİSTEMİ KURULMASI VE TEST EDİLMESİ

GPRS sistemi güvenlik testlerini yapabilmek için tez kapsamında örnek bir GPRS şebekesi kurulmuştur. GPRS şebekesini oluşturmak için OpenGGSN isimli açık kaynak kod çalışma grubunun GGSN ve SGSNEMU yazılımları kullanılmıştır[1].

## 12.1 OpenGGSN Projesi

### 12.1.1 Giriş

GPRS şebekelerinde kullanılan SGSN ve GGSN düğümleri genelde UNIX işletim sistemi üzerinde koşan bir uygulama olarak gerçeklenmektedir. OpenGGSN açık kaynak kod geliştirme grubu GGSN düğümü, LINUX işletim sistemleri üzerinde genel kamu lisansı (GPL) ile ücretsiz olarak kullanılmak için geliştirilmiştir. Bu proje aynı zamanda GGSN testini yapmak amacı ile SGSN emulatörü geliştirmiştir. Proje grubu tarafından üretilen GGSN ve SGSN yazılımları üçüncü nesil ortaklık projesi (3GPP) tarafından standartlaştırılan protokollere uyumludur.

### 12.1.2 OpenGGSN Projesini Kullanım Nedenleri

OpenGGSN projesi genel olarak yeni sistem veya ekipmanların geliştirilmesi ya da test edilmesi amacı ile kullanılmaktadır. Yazılımın açık kaynak kodlu oluşu geliştirme ve test etme gibi işlemler için uygun bir ortam hazırlamaktadır. Aşağıda OpenGGSN projesinin tipik kullanıcıları bulunmaktadır.

- Mobil operatörler ve
- Altyapı ve test ekipmanı üreticileri
- Danışmanlık ve sistem bütünleştiricileri (entegratörleri)
- Üniversiteler

### 12.1.3 OpenGGSN Düğümü Hakkında Bilgi

Gn arayüzü, GGSN cihazı ile SGSN düğümleri arasında haberleşmek amacı ile kullanılmaktadır. Gn arayüzü GTP protokolünü kullanır ve kullanıcı veri paketleri (genellikle IP paketi) bu protokol ile tünellenir. Tünelleme işleminde 3.katman[2] protokolü olarak IP ve 4. katman[3] protokolü olarak UDP kullanılır.

---

[1] www.openggsn.org

[2,3] OSI referans modeli katmanları

Gi arayüzü, GGSN cihazının dış veri ağları ile haberleşmek için kullandığı arayüzdür. Pratikte Gi arayüzü internet arayüzü olmaktadır.

Tipik olarak GGSN cihazı iki adet Ethernet kartı[1] kullanır. Bu kartlardan bir tanesi Gn arayüzü, diğeri Gi arayüzü içindir. Gi ve Gn arayüzlerini ayırmak amacı ile politika tabanlı (policy based) yönlendirme ve güvenlik duvarı yapılandırması yapılmalıdır.

GGSN, mobil istasyonlardan SGSN yolu ile gelen bağlantı isteklerini işlemektedir. GGSN bir bağlantı isteği aldığında istekte bulunan mobil istasyon için dinamik olarak bir IP adresi ayırmaktadır. Mobil istasyon bu IP adresini kullanarak Gi arayüzüne erişecektir. Bağlantılar mobil istasyon veya SGSN tarafından sonlandırılabilmektedir.

### 12.1.4 SGSN Emulatörü Hakkında Bilgi

SGSN emulatörü Gn arayüzünü gerçeklemektedir. Bu emulatör GGSN testi veya GPRS omurga testi için kullanılabilmektedir. SGSN emulatörü ihtiyaç durumunda gerçek bir SGSN gibi GGSN'e doğru birçok PDP içeriği kuracaktır. Bu aşamada isteğe bağlı olarak MSISDN, IMSI, APN ve QoS gibi birçok parametre belirtilebilir.

SGSN emulatörünün kendi içerisinde bir Ping[1] özelliği bulunmaktadır. SGSN ve GGSN arasında kurulan bağlantı üzerinden paket göndererek iletişimin sağlanıp sağlanmadığının testini yapar. Eğer bu özellik kullanılmak istenmezse yerel bir arayüz oluşturularak bu arayüze gelen trafik Gi arayüzüne doğru yönlendirilebilir.

SGSN emulatörü oluşturulan paketlerin incelenmesi amacı ile ağ analizörü ile birlikte kullanılmalıdır. Ağ analizörü ilgili arayüz üzerinden akan IP paketlerini yakalayıp trafik analizi yapılması amacı ile kullanılır.

### 12.1.5 OpenGGSN Mimarisi

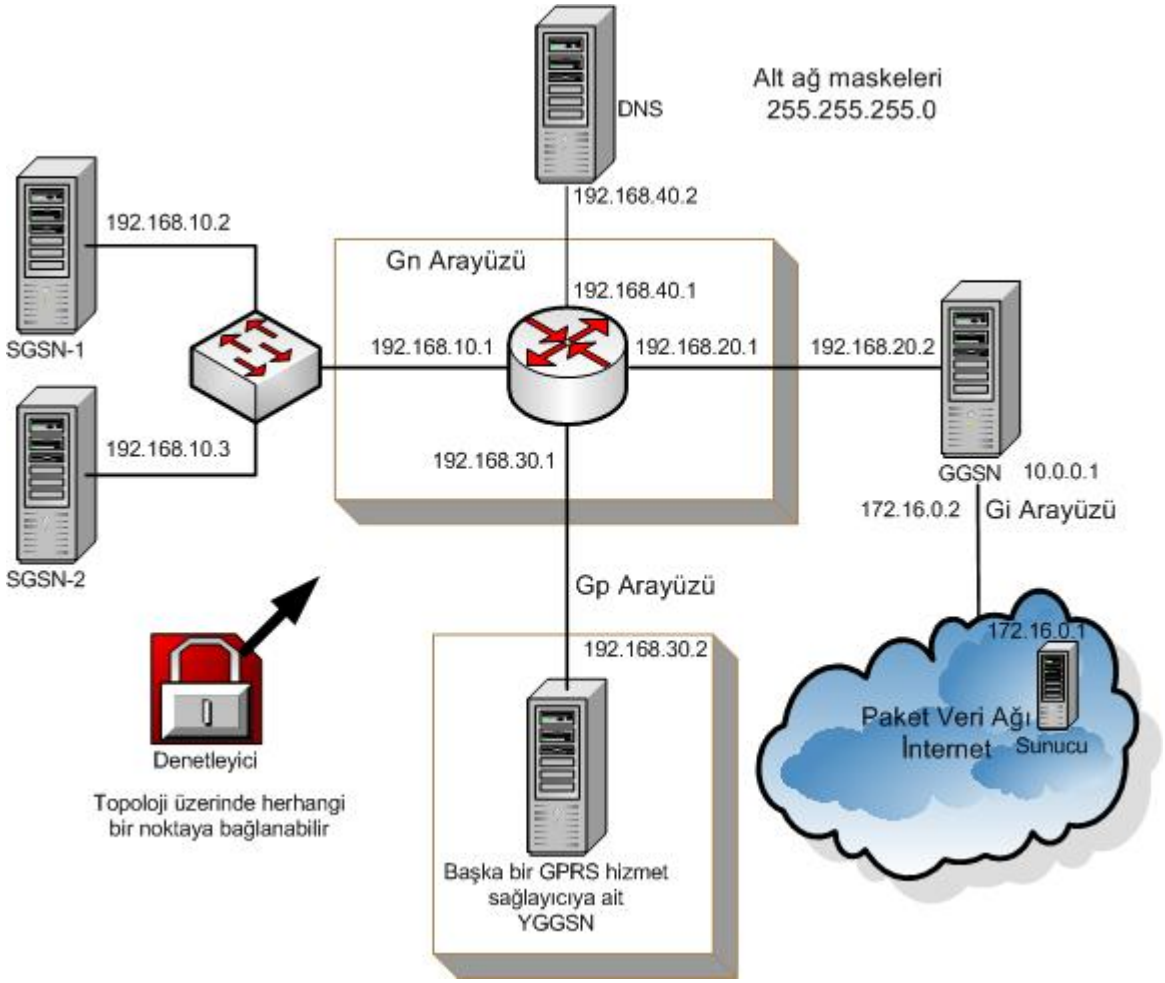
OpenGGSN için birincil işletim sistemi LINUX işletim sistemidir. Buna ek olarak FreeBSD, Solaris ve MAC OS X işletim sistemleri üzerinde de koşabilmektedir. OpenGGSN'in ana tasarım amacı kararlı, başka işletim sistemlerine kolay geçirilebilir ve ölçeklenebilir bir GGSN yazılımı oluşturmaktır. Program (ANSI) C programlama dilinde yazılmış olup başka işletim sistemlerine kolayca geçirilebilmektedir.

[1] Bir bilgisayarın TCP/IP şebekesine bağlantısı amacı ile kullanılmaktadır.

OpenGGSN projesinde üç adet bileşen mevcuttur;

- GTPLIB: SGSN ve SGSNEMU yazılımlarının temelinde kullanılan ve GTP protokolüne ait fonksiyonları içerisinde barındıran yazılım kütüphanesidir. GPL lisansı altında kendi GGSN'ini geliştirmek isteyenler bu kütüphaneyi kullanabilirler. Bu kütüphane GTPv0(GSM 09.60) ve GTPv1(3GPP 29.060) protokollerini desteklemektedir.
- GGSN: Projenin, ağ geçidi GPRS destek düğümü olarak görev yapan parçasıdır. 3GPP standartları ile bire bir uyumludur.
- SGSNEMU: Projenin GPRS servis sağlayıcı düğümü olarak görev yapan emulatörüdür. GPRS omurgasının testi için kullanılmaktadır.

## 12.2 GPRS Şebekesi Topolojisi




**Şekil 12-1 Örnek GPRS sistemi**

## 12.3 Topoloji Açıklamaları

Şekil 12-1'de görülen topoloji bir ana sunucu üzerinde gerçeklenmiştir. Yazılımsal olarak yönlendirici, anahtar ve Ethernet kart gibi cihazları oluşturmak mümkündür. Bütün sunucuları birbirlerinden farklı bir ağda tutmak için alt ağ maskesi 24 bit (255.255.255.0) olarak kullanılmıştır. Farklı ağlarda bulunan sunucuların iletişim ihtiyaçlarını gidermek için bir adet yönlendirici ilave edilmiştir.

## 12.4 GPRS Sistemi Konfigürasyonu

Örnek GPRS şebekesi oluşturmak için kullanılan yazılımlar ve donanımlar aşağıda listelenmiştir. İşletim sistemlerinde kullanılan IP adresleri Şekil 12-1'de verilmiştir.

### 12.4.1 Test Ortamında Kullanılan Yazılımlar

Test ortamında kullanılan yazılımların listesi Çizelge 12-1'de verilmiştir. Örnek GPRS şebekesinin oluşturulmasında bir ana sunucu üzerinde koşturulan işletim sistemleri kullanılmıştır. Bu işlem için kullanılan VMware[1] yazılımı bu tür bir yapı kurmaya izin vermektedir.

**Çizelge 12-1 Test ortamında kullanılan yazılımlar**

| Yazılım Adı | Kullanım Amacı | Sunucular |
|---|---|---|
| Microsoft ® Windows® XP | İşletim Sistemi, yönlendirici, DNS | Ana sunucu, DNS sunucusu |
| RedHat 9.0 | İşletim Sistemi | SGSN ve GGSN sunucuları |
| SGSNEMUv0.84 | GPRS Destek Düğümü | SGSN sunucuları |
| OpenGGSN v0.84 | Ağ geçidi GPRS destek düğümü | GGSN sunucuları |
| Ethereal 0.10.12 | Paket yakalayıcı (Dinleyici) | Denetleyici sunucusu |
| Shomiti Surveyor v3.1 | IP paket üretici | Denetleyici sunucusu |
| Nessus Security Scanner | Açıklık Tarayıcı | Denetleyici sunucusu |
| VMware V4.5.2 | Sanal olarak işletim sistemleri koşturmak | Ana sunucu |

[1] www.vmware.com

### 12.4.2 Test Ortamında Kullanılan Donanımlar

Test ortamında ana sunucu üzerinde gerçeklenen sunuculara ait donanım özellikleri Çizelge 12-2'de verilmiştir.

**Çizelge 12-2 Test ortamında kullanılan donanımlar**

| Sunucu Adı | Donanım Özellikleri | IP Adresi |
|---|---|---|
| Ana Sunucu | Intel P IV 2.26 GHz işlemci, 1024 MB RAM, 80GB Disk | 192.168.10.1 / 192.168.20.1 / 192.168.30.1 / 192.168.40.1 |
| SGSN1 | 64MB RAM, 2GB Disk, 1 Ethernet kartı | 192.168.10.2 / 24 |
| SGSN2 | 64MB RAM, 2GB Disk, 1 Ethernet kartı | 192.168.10.3 / 24 |
| GGSN | 64MB RAM, 2GB Disk, 1 Ethernet kartı | 192.168.20.2 / 24, 172.16.20.2 /24 |
| YGGSN | 64MB RAM, 2GB Disk, 1 Ethernet kartı | 192.168.30.2 / 24 |
| DNS | 128MB RAM, 2GB Disk, 1 Ethernet kartı | 192.168.40.2 / 24 |
| Denetleyici | 128MB RAM, 2GB Disk, 1 Ethernet kartı | Bağlandığı ağa göre değişen IP adresleri |
| Yönlendirici | 64MB RAM, 2GB Disk, 1 Ethernet kartı | 192.168.10.1 / 24<br>192.168.20.1 / 24<br>192.168.30.1 / 24<br>192.168.40.1 / 24 |

### 12.4.3 GGSN Düğümü Konfigürasyonu

Aşağıda üzerinde RedHat 9.0 işletim sistemi ve OpenGGSN yazılımı koşan GGSN düğümünün /etc/ggsn.conf dosyasının içeriği verilmiştir.

```
##############################################################################
###
#
# Örnek GGSN Konfigürasyon Dosyası
#
##############################################################################
###

# TAG: fg
# GGSN prosesi ön planda çalıştırılmak istenirse kullanılacak bayrak
#
#fg

# TAG: debug
```

```
# Yazılımın çalışması sırasında haberleşme izlemek istendiğinde
kullanılacak bayrak
debug



# TAG: conf
# Kullanılacak konfigürasyon dosyasına ait bayrak. Bu dosya konfigürasyon
#dosyasıdır. Konfigürasyon dosyasına dair  bir parametrenin burada
#değiştirilmesinin anlamı yoktur. Komut satırından #ggsn komutu
#çalıştırılırken bu bayrak kullanılabilir.

# TAG: pidfile
# Yazılımın Proses ID si ile ilgili bilgilerin saklandığı dosya
# Yazılımın aşağıda yazılı dosya/klasör için yazma hakkı olmalıdır.
#pidfile /var/run/ggsn.pid

# TAG: statedir
# Değişmez depolama (nonvolatile storage) için kullanılacak klasör
# Yazılımın aşağıda yazılı klasöre yazma hakkı olmalıdır
#statedir /var/lib/ggsn/


# TAG: listen
# Bağlantı istekleri için dinlenecek IP adresi
listen 192.168.20.2

# TAG: net
# Dış paket veri ağı için IP ağı adresi
# Ağ arayüzlerini kurmak için kullanılacaktır. Sgsnemu ile bağlanan
kullanıcılara tahsis edilecek IP adres bloğudur.
net 10.0.0.0/24

# TAG: ipup
# Ağ arayüzünün çalışır hale gelmesini takiben çalıştırılacak betik
(Script)
# Betik şu parametreler ile çalıştırılmalıdır: <devicename> <ip address>
#ipup /etc/ggsn/ip-up

# TAG: ipdown
#Ağ arayüzünün kapatılmasını takiben çalıştırılacak betik (Script)
# Betik şu parametreler ile çalıştırılmalıdır: <devicename> <ip address>
#ipdown /etc/ggsn/ip-down

# TAG: dynip
# Dinamik IP adresi havuzu
# IP adresinin HLR tarafından verilmemesi durumunda kullanılacak IP adres
bloğunun tanımı
# Eğer bu seçenek aktif değilse net seçeneğinde verilen bilgi kullanılır
#dynip 192.168.0.0/24

# TAG: pcodns1
# Birinci DNS (Domain Name System) sunucusu için konfigürasyon parametresi
pcodns1 192.168.20.1

# TAG: pcodns2
# İkinci DNS (Domain Name System) sunucusu için konfigürasyon parametresi
pcodns2 192.168.10.1

# TAG: timelimit
# Bağlantı için zaman aşımı süresi tanımlama
```

```
# Zaman aşımı süresinin sıfır olarak ayarlanması programın hiç bir zaman
durmayacağı anlamına gelir
#timelimit 0

# TAG: apn
# Bu başlık DENEY amaçlı olarak kullanılmaktadır
# Yazılımın istemci (sgsnemu) olarak çalıştırılması durumunda bağlantı
kurulacak erişim noktası adı (Access point name-APN)
#apn internet

# TAG: qos
# Bu başlık DENEY amaçlı olarak kullanılmaktadır
#Yazılımın istemci (sgsnemu) olarak çalıştırılması durumunda talep edilen
servis kalitesi (QoS) için kullanılır
#qos 0x0b921f
```

## 12.5 Örnek GPRS Sisteminin İşler Duruma Getirilmesi ve Test Edilmesi

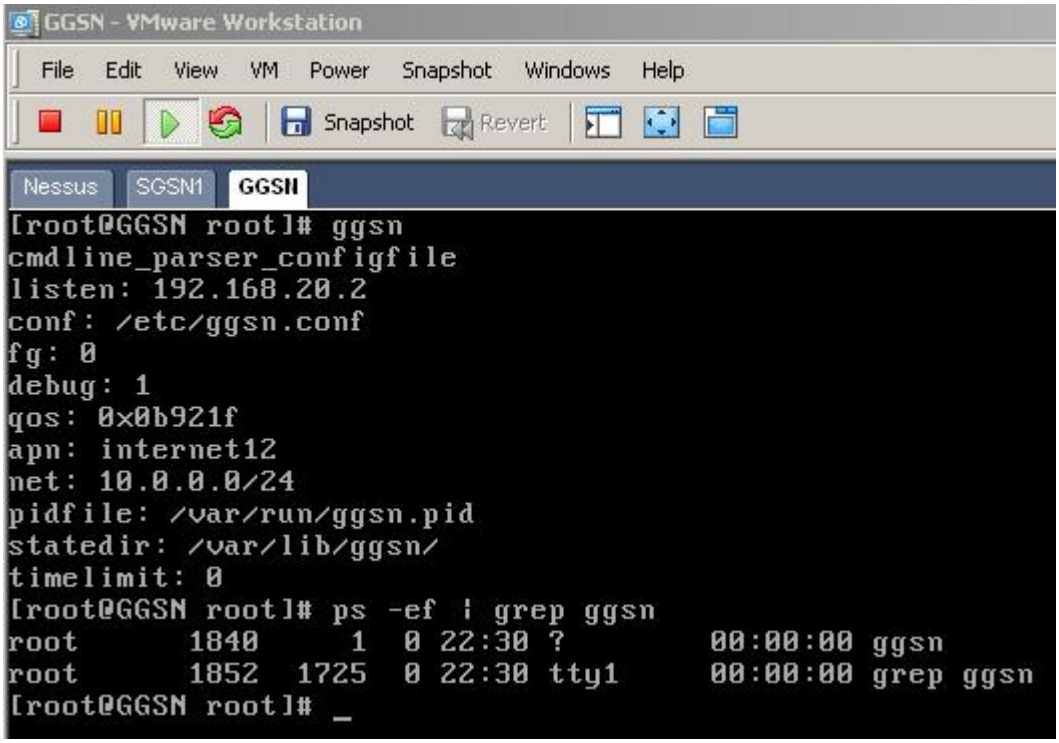
### 12.5.1 OpenGGSN Yazılımının Çalıştırılması (Şekil 12-2)

1. **adım:** GGSN düğümü üzerinde ggsn yazılımını çalıştırmak için ***ggsn*** komutu işletilir.

2. **adım:** OpenGGSN yazılımının çalışması durumunda GGSN düğümü işlem listesinde ggsn yazılımı görünmelidir.

   a. GGSN düğümü üzerinde ***ps –ef | grep ggsn*** komutu çalıştırılır

   b. Komut çıktısında ggsn görünmelidir.




**Şekil 12-2 OpenGGSN yazılımının çalıştırılması**

### 12.5.2 SGSN1 ve GGSN Arasında Tünel Kurulması ve Test Edilmesi

1. **adım:** Denetleyici sunucusu 192.168.20.0 ağına bağlanır.

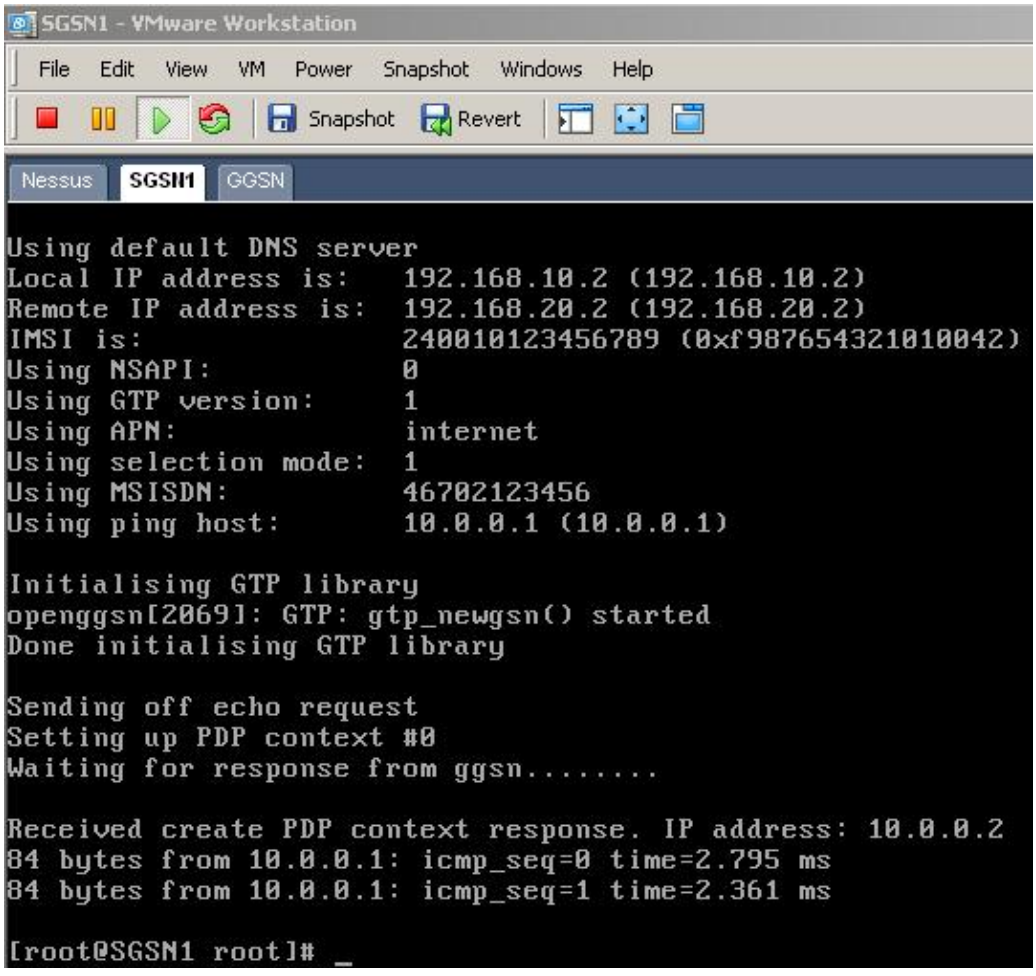
2. **adım:** Denetleyici sunucusu üzerinde Ethereal paket yakalayıcı yazılımı çalıştırılır.

3. **adım:** SGSN düğümü üzerinde "*sgsnemu –listen 192.168.10.2 –remote 192.168.20.2 –pinghost 10.0.0.1"* komutu çalıştırılır.

    a. –listen parametresi ile SGSN in GTP tünelinde kullanılacak arayüz IP adresi belirtilmiştir (yerel arayüz IP adresi)

    b. –remote parametresi ile GGSN in GTP tünelinde kullanılacak IP adresi belirtilmiştir. (Uzak uç IP adresi)

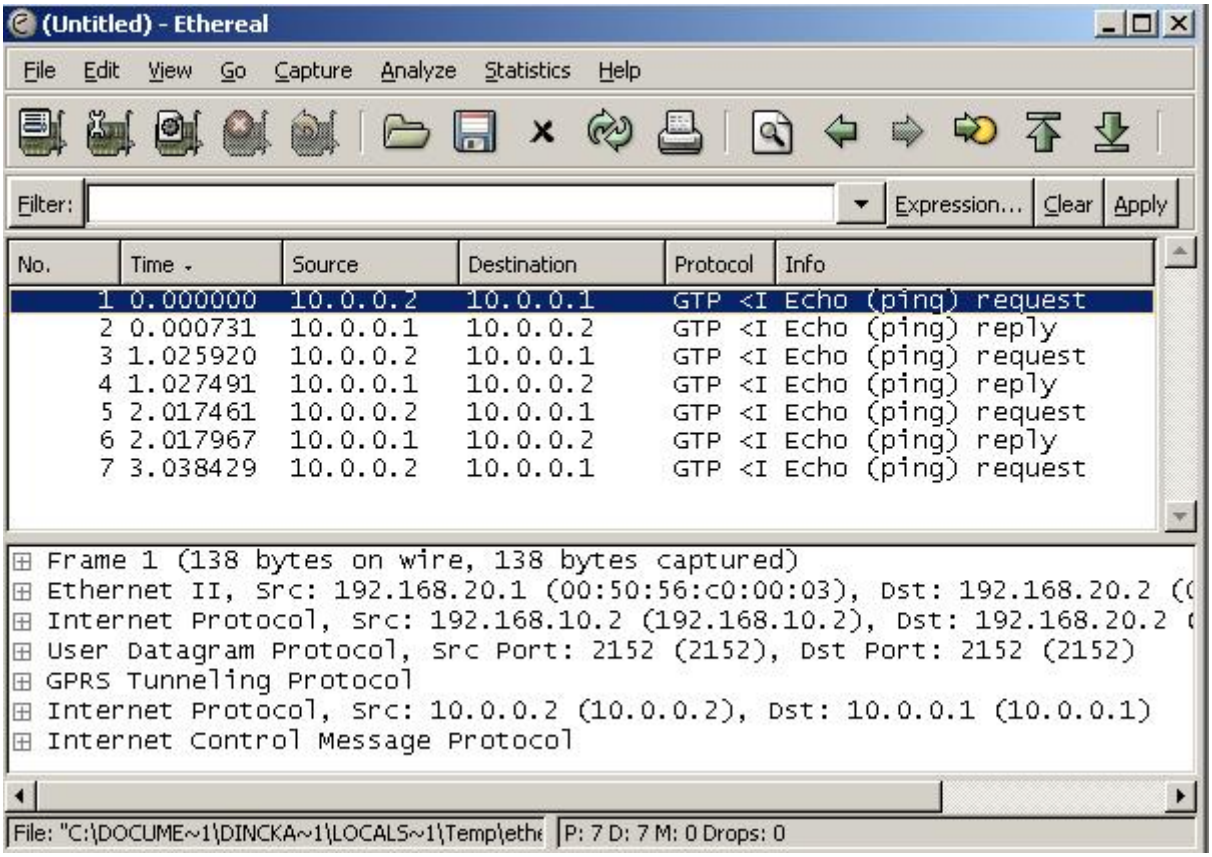
    c. –pinghost parametresi ile kurulacak GTP tüneli üzerinden gönderilecek IP paketleri belirtilmiştir. Test sırasında kurulan tünel üzerinden GGSN Gi arayüzü IP adresi olan 10.0.0.1 adresine ICMP paketleri gönderilmiştir.




**Şekil 12-3 SGSN ve GGSN arasında tünel kurulması ve test edilmesi**

4. **adım:** Şekil 12-3'ten görüldüğü üzere SGSN düğümü üzerinden gönderilen ICMP paketlerine yanıt alınmıştır. GGSN tarafından GTP tünelinin kurulumu sırasında 10.0.0.2 IP adresi tahsis edilmiştir. Kurulan bağlantıya ait GTP versiyonu, APN adresi, MSISDN numarası bilgileri yine Şekil 12-3'te görülmektedir.

5. **adım:** Denetleyici sunucusu üzerinde çalışan Ethereal paket dinleyici, SGSN ve GGSN arasında akan ICMP IP paketlerine dair GTP paketlerini yakalamıştır (Şekil 12-4). Yakalanan paketlerin ayrıntılarına bakılırsa IP paketinin kaynak ve hedef adresleri 192.168.10.2 ve 192.168.20.2'dir. Diğer taraftan kapsüllenmiş olan trafik 10.0.0.1 ve 10.0.0.2 arasındadır. Bütün bu sonuçlardan SGSN ve GGSN arasında GTP tünelinin başarı ile kurulduğu anlaşılmaktadır.




**Şekil 12-4 GTP tüneli kurulması**

### 12.5.3 GPRS Omurgasına Yeni Bir SGSN Eklenmesi

Örnek GPRS omurgası üzerinde mevcut durumda bir adet GGSN ve bir adet SGSN cihazı çalışmaktadır. GGSN düğümü birden fazla SGSN düğümüne hizmet verebilmelidir. Bu adımda yeni bir SGSN düğümü eklenerek GGSN ile haberleşmenin testi yapılmıştır.

1. **adım:** Yeni SGSN düğümü üzerinde "*gsnemu –listen 192.168.10.3 –remote*

*192.168.20.2 –pinghost 10.0.0.1”* komutu çalıştırılır.

a. –listen 192.168.10.3 parametresi ile GTP tüneli için kullanılacak SGSN IP adresi belirtilmiştir.

b. –remote 192.168.20.2 parametresi ile GTP tüneli için kullanılacak GGSN IP adresi belirtilmiştir.

c. –pinghost *10.0.0.1* parametresi ile kurulacak GTP tüneli üzerinden haberleşilecek karşı uç IP adresi verilmiştir. Bu adres GGSN Gi arayüzü IP adresidir.

**2. adım:** 1. adımda işletilen komut sonucunda yeni SGSN ekranında görünen bilgiler yorumlanır. (Şekil 12-5)

a. GTP bağlantısının 192.168.10.3 (Yeni SGSN Gn arayüzü) ve 192.168.20.2 (GGSN Gn arayüzü) IP adresleri arasında gerçekleştiği görülmektedir.

b. GTP bağlantısı sırasında GTP V1 kullanılmıştır.

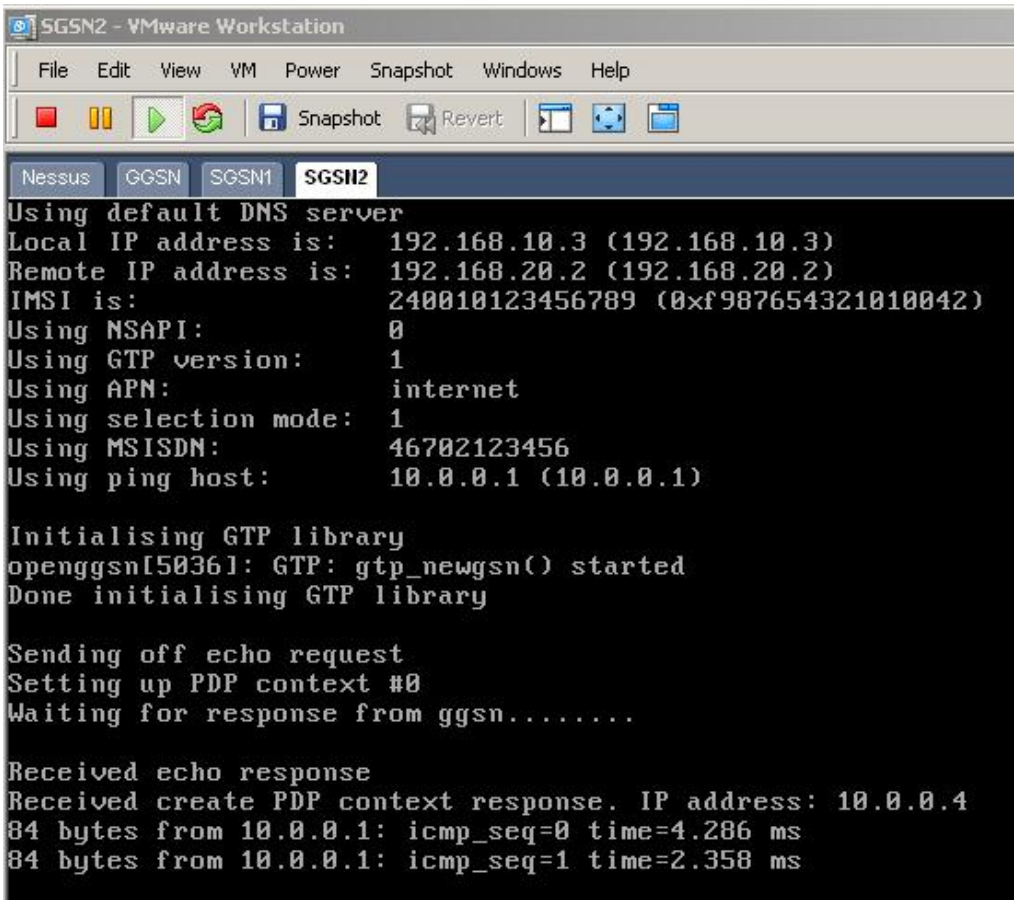
c. Bağlantının APN adresi internet olarak görülmektedir.

d. Bağlantı için kullanılan MSISDN numarası 46702123456’tür.

e. Karşı uçta paket gönderilen IP adresi GGSN Gi arayüzü (10.0.0.1) adresidir.

f. SGSN üzerinden kurulan bağlantıya GGSN tarafından 10.0.0.4 IP adresi atanmıştır.

g. Gönderilen ICMP paketlerine yanıt gelmiştir. Bu adım sonucunda yeni SGSN’in omurga üzerinde başarı ile çalıştığı anlaşılmıştır.




**Şekil 12-5 Yeni bir SGSN'in örnek GPRS şebekesine eklenmesi**

# 13. ÖRNEK GPRS ŞEBEKESİ GÜVENLİK POLİTİKASI

## 13.1 Giriş

GPRS şebekesi güvenlik politikası şebeke operatörü tarafından uygulanan bilgi güvenliği ilkelerini belirlemektedir. Güvenlik politikası, şebekede bilginin ve işlenme yöntemlerinin güvenli olarak gerçekleştirilmesi amacıyla düzenlemeler yapmaktadır.

## 13.2 Bilgi Güvenliğinin Tanımı

Bilgi güvenliği gizlilik, bütünlük ve süreklilik olmak üzere üç ana unsurdan oluşmaktadır. Şebeke üzerinde bulunan cihazların ve bilgilerin güvenlik ile ilgili konuları bu kapsamda değerlendirilecektir.

a. **Gizlilik (Confidentiality):**
   i. Yetkisiz kişilerin bilgiye erişiminin engellenmesi;
   ii. Bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesi.
b. **Bütünlük (Integrity):**
   i. Bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesinin engellenmesi;
   ii. Bilginin kasıtlı ya da kazayla bozulmasının engellenmesi.
c. **Süreklilik (Availability):**
   i. Bilginin her zaman kullanıma hazır durumda olması;
   ii. Herhangi bir sorun ya da problem çıksa bile sistemin hizmet vermeye devam etmesi;

## 13.3 Güvenlik Politikasının Amaçları

Güvenlik Politikası aşağıdaki amaçlara hizmet etmek için oluşturulmuştur:

- GPRS operatörünün sahip olduğu bilgilerin ihtiyaç duyulan seviyede gizliliğinin, bütünlüğünün ve sürekliliğin korunması için genel bakış açısının tanımlanması,
- Korunması gereken varlıkların tanımlanması,
- Varlıkların korunma biçiminin belirlenmesi,
- Güvenlik sorumlularının kimler olduğu,
- Güvenlik kayıtlarının ne şekilde inceleneceği,

- Acil durumlarda nasıl hareket edileceği,
- Diğer operatörler ile yapılan anlaşmalarda dikkat edilecek hususların neler olduğu.

### 13.4 Güvenlik Politikasının Sahibi

GPRS Güvenlik Politikasının sahibi örnek GPRS operatörünün en üst düzey yöneticisidir.

### 13.5 Güvenlik Politikasının Gözden Geçirilmesi ve Güncellenmesi

GPRS Güvenlik Politikası, periyodik olarak 6 ayda bir veya gerekli görüldüğü hallerde örnek GPRS şebekesi güvenlik yöneticisi tarafından gözden geçirilir ve gözden geçirme sonuçları yönetime sunulur. Örnek GPRS şebekesi Güvenlik Yöneticisi politikanın gözden geçirilmesi sırasında operatör personeli veya uzmanlarının görüşüne başvurabilir. Güvenlik yöneticisi yönetimden gelen değişiklik onayına göre gerekiyorsa politikayı günceller ve sürüm numarasını bir arttırır. Değişiklik yapılmış güvenlik politikası yönetimce imzalanır ve uygulamaya girer. Güvenlik Yöneticisi yeni politika gereğince şebekenin işleyişi ile ilgili yapılması gerekenleri planlamak ve yerine getirmekten sorumludur.

Aşağıda sıralanan durumlarda güvenlik politikasının güncellemesi mutlaka yapılmalıdır.

- Sistem bileşenlerinde değişiklik olması
- Yeni tipte güvenlik açıklıklarının çıkması
- GPRS şebekesi işletim talimatlarında değişiklik olması
- Güvenlik gereksinimlerinde değişiklik olması
- Güvenlik ihlallerinin belirlenmesi

Güvenlik Politikası gözden geçirilirken aşağıda listelenen hususlar özellikle göz önünde bulundurulmalıdır;

- Mevcut politikanın etkinliği ve yeterliliği
- Tercih edilen güvenlik önlemlerinin ve korunan varlıkların değerleri
- Teknolojideki değişiklikler

### 13.6 Güvenlik Sorumlulukları

Çalışan personel ile ilgili güvenlik sorumlulukları ve uygulanan kurallar aşağıda verilmiştir;

- GPRS şebekesinin işletiminde bulunacak personelin iş tanımlarında güvenlik sorumluluğu yazılır. Personelin tespit edilen güvenlik ihlallerinde kullanılmak üzere iş tanımı imzalatılır.
- GPRS hizmeti vermek için kullanılan sistemlerin yönetimini yapacak personelin sistemleri yanlış kullanımın engellenebilmesi amacıyla mümkün olduğunca görevlerin ayrımı ilkesi uygulanır.
- Güvenlik politikasının sahibi GPRS şebekesinin güvenliğinden en üst düzeyde sorumludur.
- Güvenlik yöneticisi şebekenin güvenliğinin tahsis edilmesinden sorumludur. Güvenlik olaylarını, politika değişikliklerini ve tespit ettiği açıklıkları güvenlik politikası sahibine bildirmekle yükümlüdür.
- Güvenlik yöneticisi personelin güvenlik bilincinin geliştirilmesi için çalışmalar yapmaktan sorumludur. Periyodik bilinçlendirme eğitimleri yapmaktan ve işe yeni başlayan personele güvenlik politikasının tanıtımından sorumludur.

### 13.7 GPRS Şebekesinde Korunan Varlıklar

Örnek GPRS şebekesinde korunması gereken varlıklar aşağıda listelenmiştir.

- **Abone Verisi:** Abonelerin GPRS şebekesi üzerinden transfer ettiği verinin gizliliği ve bütünlüğü SGSN ve GGSN cihazları arasında şifreleme yaparak korunur. Aboneye uçtan uca bir şifreleme güvenliği verilmez. Abone uçtan uca şifreleme istiyorsa kendisi gerçekleştirmelidir.

- **Ücretlendirme Bilgisi:** Müşteri mağduriyetine sebep olmamak için ücretlendirme bilgisinin gizliliği ve bütünlüğü korunur.

- **Sinyalleşme Bilgisi:** GPRS bileşenleri SGSN ve GGSN, GSM sisteminin bileşenleri ile sinyalleşme arayüzleri üzerinden haberleşmektedir. Güvenli bir haberleşme için GPRS şebekesinin işleyişini temin eden sinyalleşme bilgileri korunur.

- **Abone Bilgisi:** Örnek GPRS operatörü hem kendi abonelerinin hem de dolaşım halinde olan başka GPRS operatörlerinin bilgilerini gizli tutar. Abonelere ait olan ve şebekenin Doğrulama Merkezi (AuC), HLR ve VLR veritabanlarında bulunan veriler korunur.

- **GPRS Şebekesinin Teknik Bilgileri:** GPRS şebekesi bileşenlerinin yapılandırma bilgileri gibi teknik bilgileri korunmaktadır.
- **Şebeke cihazları:** Şebekede kullanılan SGSN, GGSN, DNS, anahtarlama ve yönlendirme cihazları gibi GPRS hizmeti için kullanılan cihazların tümü korunur. GPRS şebekesinin ihtiyaç duyduğu GSM şebekesi bileşenlerinin koruması yapılır veya yaptırılır.
- **Personel:** GPRS şebekesinin işleyişi ve güvenliği için en önemli bileşen çalışan personeldir. Personelin yeterli bilgi düzeyinde olması ve güvenlik konusunda bilinçli davranması için gereken önlemler alınır.

### 13.8 Potansiyel Tehdit Unsurları

Kötü niyetli internet kullanıcıları, aboneler, çalışan personel ve altyüklenici firma çalışanları şebeke için potansiyel tehdit unsurları olarak görülerek gerekli güvenlik önlemleri alınır.

### 13.9 Fiziksel güvenlik

GPRS şebekesinin ihtiyaç duyduğu GSM şebekesi bileşenlerinin koruması GSM operatörünün sorumluluğundadır. Aynı kurum olması nedeni ile GSM bölümü ile kurum içi hizmet sözleşmesi yapılmıştır.

### 13.10 Personel Güvenliği

Tüm çalışanlar, operatörün bilgi güvenliği politikalarına uymakla yükümlüdürler. Personel, politikalara uygun olmayan davranışları sonucu meydana gelebilecek güvenlik olaylarından sorumlu olacaklardır.

### 13.11 Güvenlik Eğitimi

Alt yükleniciler de dahil olmak üzere, operatör sistemlerini kullanması gereken her personel için güvenlik politikaları ve prosedürleri konusunda gerekli eğitimler hazırlanır ve personelin bu eğitimlere katılımı sağlanır.

### 13.12 Fiziki ve Çevresel Güvenlik

#### 13.12.1Güvenli Bölgelerde Çalışma

Kritik cihazlar (SGSN, GGSN vb) kart kontrollü girişlerle korunan, fiziksel erişim kontrolü

gerektiren alanlarda bulunur, gerekiyorsa kamera kontrolü de kullanılarak girişler kayıt altına alınır. Sözü edilen kayıtlar en az 1 yıl süreyle saklanır.

### 13.12.2Cihaz Güvenliği

Personel, önemli cihazların bulunduğu güvenli alanlarda sigara içmez, yiyecek ve içecekle güvenli alanlara girmez.

Cihazların herhangi bir elektrik kesintisinde çalışmalarına devam etmeleri için kullanılan UPS, jeneratör gibi güç kaynakları 12 ayda bir periyodik olarak üreticinin talimatlarına uygun biçimde kontrol edilir. Tüm cihazların, sürekliliği ve güvenilirliğini garanti etmek amacıyla üretici firmanın talimatlarına uygun olarak, yetkili kişilerce düzenli periyotlarla bakımları yapılır. Bakımlar kayıt altına alınır ve ilgili kayıtlar en az 2 sene saklanır.

## 13.13 İşletim Güvenliği

### 13.13.1 İşletim Prosedürleri ve Sorumluluklar

Şebekenin işletimi için gerekli prosedürler dokümante edilir ve bu prosedürlerin sürekliliği sağlanır. İşletim prosedürleri resmi dokümanlar olarak ele alınır ve gereken değişiklikler ancak yönetimden izin alındıktan sonra yapılır.

### 13.13.2 İşlemsel Değişikliklerin Kontrol Edilmesi

GPRS hizmeti vermek için kullanılan sistemlerde yapılan değişiklikler kontrol edilir. Özel olarak aşağıdaki kontrol mekanizmaları göz önüne alınır:

a. Önemli değişikliklerin belirlenmesi ve kaydedilmesi,

b. Önemli değişikliklerin sistem üzerinde olabilecek potansiyel etkisinin değerlendirmeye tabi tutulması,

c. Yapılması düşünülen değişiklikler için resmi izin alınması,

d. İlgili kişilerin değişikliklerle ilgili detaylar hakkında bilgilendirilmesi,

e. Başarısızlıkla sonuçlanan değişikliklerin geri alınması ya da iptal edilmesi için gereken sorumlulukları belirten prosedürlerin tanımlanması.

### 13.14 Güvenlik Olaylarının Yönetimi

Güvenlikle ilgili gelişen olaylara daha çabuk, daha etkin ve düzgün bir şekilde karşılık verebilmek için bu olayların yönetimine ilişkin sorumluluklar ve prosedürler tanımlanır. Yönetim sürecinde aşağıdaki kontrol mekanizmaları göz önüne alınır:

1. Belirlenecek prosedürler, aşağıdaki olaylar da dahil olmak üzere bütün olası olay tiplerini kapsar:
   - Sistem arızaları ve servis kayıpları,
   - Servis dışı kalma,
   - Eksik ve geçersiz iş verisinden kaynaklanan hatalar,
   - Gizlilik prensibinin ihlal edilmesi.
2. Prosedürler, ek olarak aşağıdaki hususları da kapsar;
   - Olayın nedeninin belirlenmesi ve analiz edilmesi,
   - Eğer gerekirse, olayların tekrar olmasını engellemek için çıkar yolların planlanması ve gerçeklenmesi,
   - Olaylarla ilgili kayıtların ve benzer kanıtların toplanması,
   - Gelişen bir olayla ilgili olarak kurtarmaya katılan ya da bu kurtarmadan etkilenen kişilerle haberleşme,
   - Yapılanların yönetime raporlanması.
3. Güvenlikle ilgili sorunların ortadan kaldırılması ve sistem hatalarının düzeltilmesi için yapılanlar dikkatlice ve resmi bir şekilde kontrol edilir. Prosedürler aşağıdakileri garanti eder:
   - Sadece net bir şekilde tanımlı ve yetkili bir kadronun canlı sisteme ve veriye erişimine izin verilir,
   - Acil olarak yapılan bütün faaliyetler detaylı olarak dokümante edilir,
   - Acil olarak yapılan faaliyetler yönetime raporlanır ve düzgün bir şekilde gözden geçirilir,
   - İş sistemlerinin ve kontrol mekanizmalarının bütünlüğü en az gecikmeyle onaylanır.

### 13.15 Görevlerin Ayrı Tutulması

Görevlerin ayrı tutulması, Sistemin kasıtlı ya da kasıtsız olarak kötüye kullanılmasından kaynaklanan risklerin azaltılması için kullanılan bir metottur. Yetkisiz erişime veya servislerin kötüye kullanılmasına olanak tanıyan olayların azaltılması için belirli işlerin veya sorumluluk alanlarının yönetilmesi ya da yürütülmesine ilişkin ayrım yapılır.

### 13.16 Güvenlik Kayıtları

Hizmet vermek için kullanılan cihazlara ve odalara erişimin takip edilmesi için kayıtlar tutulur. Bu kayıtların tutulmasının sağlanması ve kontrol edilmesi güvenlik yöneticisinin sorumluluğundadır. Güvenlik kayıtları güvenlik ihlali durumunda kanıt olarak kullanılır.

### 13.17 İşletmen Kayıtları

Sistemin işlemesiyle ilgilenen personel, yaptıkları işlerin kaydını tutar. Bu kayıtlar aşağıdakileri içerir:

- Sistemin çalıştırılmaya başlanma ve çalışmasının sonlandırılma zamanları;
- Sistem hataları ve yapılan düzeltici hareketler;
- Yapılan işlemlerin onayı;
- Kaydı tutan personelin bilgileri.

Operatör kayıtları, işletim prosedürlerine karşı düzenli ve bağımsız incelemelere tabi tutulur.

### 13.18 Arızaların Kaydının Tutulması

Sistemde gerçekleşen arızalar raporlanır ve gereken düzeltici önlemler alınır. Kurum personelinin veya abonelerin ilgili sorunlarına ilişkin raporladıkları arızaların kaydı tutulur. Raporlanmış arızaların işlem görmesi için açık kurallar oluşturulur. Arızaların tatmin edici bir şekilde giderildiğinden emin olmak için arıza kayıtlarının yeniden gözden geçirilmesi yapılır. Kontrol mekanizmalarının tehditlere karşı korunmasız kalmadığından ve hareketlerin tamamen yetkili olarak yapıldığından emin olunması bakımından düzeltici ölçütlerin yeniden gözden geçirilmesi yapılır.

### 13.19 Sistem Dokümantasyonunun Güvenliği

GPRS şebekesinin yapılandırma ve yönetimine dair bilgilerin saldırganların eline geçmesi durumu yetkisiz bilgilere erişim, ücretsiz hizmet alma, GPRS şebekesinin çalışmasını durdurma, abone oturumlarını dinleme gibi sonuçlar doğurabilir. Bu tür nedenlerle

bileşenlerin yapılandırma bilgileri gibi teknik bilgiler korunur.

Koruma için aşağıdaki kontrol mekanizmaları ele alınır:

- Sistem dokümantasyonu güvenli bir şekilde saklanır,
- Sistem dokümantasyonuna ilişkin erişim listesi minimum düzeyde tutulur ve güvenlik yöneticisi tarafından yetkilendirilir,
- Tüm personelin erişimi olan sistem dokümantasyonunun uygun bir şekilde korunması için kontroller geliştirilir.

### 13.20 Erişim Kontrolü

Erişim kontrolü için iş gereksinimleri tanımlanır ve raporlanır. Bütün personel için erişim kontrolü kuralları ve hakları, erişim politikası ile açık olarak belirtilir. Personelin ve alt yüklenicilerin karşılaması gereken iş gereksinimleri, erişim kontrolleri politikasında açıkça anlatılır.

Erişim kontrol politikasında aşağıdaki maddeler göz önünde bulundurulur:

- Şebekenin kritik cihazlarına erişim yetkilendirmesi,
- Şebekenin kritik bilgilerinin saklanma ve erişim yöntemleri,
- Erişim için kullanılacak kullanıcı adı ve parolalarının standardı,
- Özel güvenlik gerektiren odalara giriş için kullanılacak teknikler ve uygulaması,
- Ortak yapılan işler için standart kullanıcı erişim tanımları (örneğin SGSN işletmeni erişim hakları),
- Cihazlara ve güvenli alanlara erişim ile ilgili kayıtların tutulması.

### 13.21 Yasal Gereksinimlerle Uyumluluk

Kurum ülke içerisinde uymak zorunda olduğu mevzuata uygun hareket etmekten sorumludur. Mevzuat gereği yapılması gereken işlemler planlanır ve uygulanır.

### 13.22 Üçüncü Taraflar İçin Erişim Riskleri

İş gereği üçüncü partinin kurumdaki kaynaklara erişimi söz konusu olduğunda, bu işlem için gerekli kontrol mekanizmaları belirlenir ve ortaya çıkabilecek güvenlik sorunlarıyla ilgili olarak risk değerlendirmesi yapılır. Belirlenen kontrol mekanizmaları üzerinde üçüncü partilerle anlaşmaya varılır ve bu hususlar yapılan sözleşmelerde belirtilir. Alt yükleniciler ve dolaşım anlaşması yapılan GPRS operatörleri bu sınıfa girmektedir.

### 13.22.1Erişim Türleri

Üçüncü partilere, operatör kaynaklarından yararlanmaları için verilen erişimin niteliği büyük önem taşır. Örneğin, GPRS hizmet düğümleri ağlarına olan erişimden kaynaklanan riskler, fiziksel erişimden kaynaklanan risklerden farklı özelliktedir. Ele alınması gereken erişim türleri aşağıdaki gibidir:

- Fiziksel erişim, örneğin ofislere, sistem odalarına erişim,
- Mantıksal erişim, örneğin kurumun veritabanlarına, bilgi sistemlerine veya GPRS hizmet düğümlerine olan erişim.

### 13.22.2Sözleşmelerde Geçen Güvenlik Gereksinimleri

Üçüncü partilerin kurumsal bilgi ve bilgi işleme mekanizmalarına olan erişimleri ile ilgili olarak resmi sözleşme yapılır. Bu sözleşme, ilgili kurum ve üçüncü parti arasında hiçbir anlaşmazlık olmadığını garanti etmektedir. Sözleşmede aşağıdaki hususlar yer alır:

1. Bilgi güvenliği ile ilgili genel politika
2. Kurumsal varlıkların korunması
   - Kuruma ait bütün varlıkların korunması için gerekli prosedürler,
   - Varlıklara zarar verici olayların (örneğin bilginin tahrip edilmesi ya da değiştirilmesi) belirlenmesi için gerekli prosedürler,
   - Sözleşmenin sonunda ya da sözleşmede belirtilen herhangi bir zaman diliminde işi biten bilginin ya da varlığın geri iade edilmesi ya da imhası ile ilgili kontrol mekanizmaları,
   - Bütünlük ve sürekliliğin sağlanması,
   - Bilginin kopyalanmasına ya da kullanımına sınırlamalar getirilmesi.
3. Sağlanacak her türlü hizmetin tanımının yapılması
4. Hedeflenen hizmet seviyesinin ve kabul edilemez hizmet seviyelerinin saptanması
5. İlgili çalışanların başka bir bölüme nakledilmeleri ile ilgili maddeler
6. Sözleşmede adı geçen partilerin karşılıklı sorumlulukları
7. Yasal hükümlerin getirdiği sorumluluklar; (örneğin bilginin korunması ile ilgili yasada geçen maddeler) eğer başka ülkelerdeki kurumlarla işbirliği yapılıyorsa bu ülkelere ait yasalar da göz önüne alınır
8. Kullanılan ürün ve yazılımlarla ilgili telif hakları ve birlikte yürütülen işlerin koruma altına alınması
9. Erişim kontrolü ile ilgili anlaşmaya varılan konular

- İzin verilen erişim yöntemleri ve kullanıcı ismi ve parolası (şifresi) gibi kimlik belirteçlerinin kullanımının denetlenmesi,
- Kullanıcı erişim hakları ve ayrıcalıklarının belirlenmesi,
- Sağlanan hizmetleri kullanmaya yetkili kullanıcıları içeren bir listenin hazırlanması ve bununla ilgili hak ve ayrıcalıkların tespit edilmesi.

10. Etkinliği ölçülebilir ve doğrulanabilir performans kıstaslarının sistem içinde tanımlanması ve bununla ilgili denetleme ve raporlama işlemlerinin yapılması
11. Kullanıcı aktivitelerinin gözlenebilmesi ve kullanıcı haklarının iptal edilebilmesi hakkı
12. Sözleşmede belirlenen sorumlulukların kurum ya da üçüncü partiler tarafından denetlenebilmesi hakkı
13. Yazılım ve donanım kurulum ve bakımıyla ilgili sorumluluklar
14. Açık ve net bir raporlama mekanizmasının oluşturulması ve belirli raporlama biçimlerinde anlaşmaya varılması
15. Sistemde meydana gelen ya da gerçekleştirilen değişikliklerle ilgili yapılması gerekenlerin açıkça belirtilmesi
16. Fiziksel korunmanın sağlanabilmesi için ihtiyaç duyulan kontrol mekanizmalarının gerçeklenmesi ve bu mekanizmaların uygulanıp uygulanmadığının denetlenmesi;
17. Güvenlik prensip ve prosedürlerini uygulamak üzere kullanıcıların ve sistem yöneticilerinin eğitilmesi
18. Zararlı yazılımlara karşı korunmak için gereken kontrol mekanizmaları
19. Güvenlik sorunlarının ve güvenlikle ilgili olarak gelişen olayların araştırılması, belirlenmesi ve raporlanması için gerekli hazırlıkların yapılması

# 14. ÖRNEK GPRS ŞEBEKESİ GÜVENLİK TESTİ

Örnek GPRS şebekesinin güvenlik testi sırasında 11. Bölümde verilen test talimatı kullanılmıştır.

## 14.1 Test Adımları Özet Tablosu

**Çizelge 14-1 Örnek GPRS şebekesi test adımları özet tablosu**

| Test Numarası | Test Adımı | Test Sonucu |
|---|---|---|
| 1 | | GEÇTİ |
| 2 | GPRS Şebekesi Konfigürasyonu ve Çalışma Esasları Dokümanı Testi | KALDI |
| 3 | Gi Bant Genişliği Testi | KALDI |
| 4 | Gizlilik ve Bütünlük Test Adımı | KALDI |
| 5 | Aboneler Arası Saldırı Testi | GEÇTİ |
| 6 | İnternet Üzerinden Saldırı Testi | GEÇTİ |
| 7 | GPRS Omurgası Bileşenleri Açıklıkları Testi | KALDI |
| 8 | Abone IP Adreslerinin Dağıtımı (NAT kullanımı) Testi | GEÇTİ |
| 9 | | GEÇTİ |
| 10 | Abone IP adreslerinden SGSN ve GGSN Sistemlerine Erişim Testi | KALDI |
| 11 | SGSN ve GGSN Düğümleri Erişim Kontrol Listeleri Testi | KALDI |
| 12 | GTP PDP İçerik Silme ve İçerik Güncelleme Engelleme Test Adımı | KALDI |

## 14.2 Test Adımları

### 14.2.1 GPRS Şebekesi Güvenlik Politikası Dokümanı Testi

#### 14.2.1.1 Test Adımının Uygulanması

Yapılan inceleme sonucunda GPRS şebekesinin işletimine dair bir güvenlik politikasının bulunduğu görülmüştür. Politika içerisinde korunması gereken varlıkların neler olduğu, kimlerden korunması gerektiği, güvenlik ile ilgili sorumlulukların neler olduğu, acil durumlarda nasıl hareket edileceği, üçüncü taraflar ile yapılan anlaşmalarda yer alan maddeler gibi konuların bulunduğu görülmüştür.

#### 14.2.1.2 Karar

Güvenlik politikasının bulunması ve içeriğinin istenilen konuları kapsamanı nedeni ile GPRS şebekesi test adımından **GEÇTİ**.

### 14.2.2 GPRS Şebekesi Konfigürasyonu ve Çalışma Esasları Dokümanı Testi

#### 14.2.2.1 Test Adımının Uygulanması

Kurum personeli ile yapılan görüşmede GPRS şebekesinin konfigürasyon ve çalışma esaslarının bulunduğu dokümanların mevcut olmadığı anlaşılmıştır. İşlemler yazılı prosedürler olmadan yürütülmektedir.

#### 14.2.2.2 Karar

Konfigürasyon ve çalışma esasları dokümanının bulunmaması nedeni ile GPRS şebekesi test adımından **KALDI.**

### 14.2.3 Gi Bant Genişliği Testi

#### 14.2.3.1 Test Adımının Uygulanması

GPRS şebekesinin ağ topolojisinden ve kurum çalışanları ile görüşmelerden Gi arayüzünden akacak trafiğin birden fazla hat ile desteklenmediği öğrenilmiştir.

#### 14.2.3.2 Karar

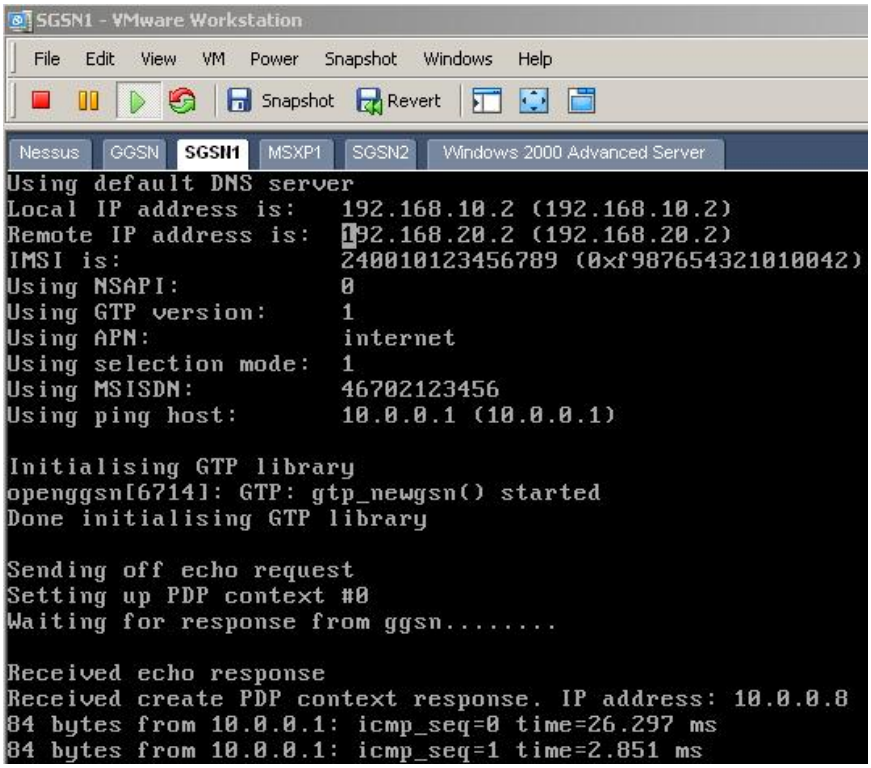
GPRS şebekesinin Gi arayüzünün tek bir hat ile paket veri ağına bağlanmış olması nedeni ile test adımından **KALDI.**

### 14.2.4 Gizlilik ve Bütünlük Test Adımı

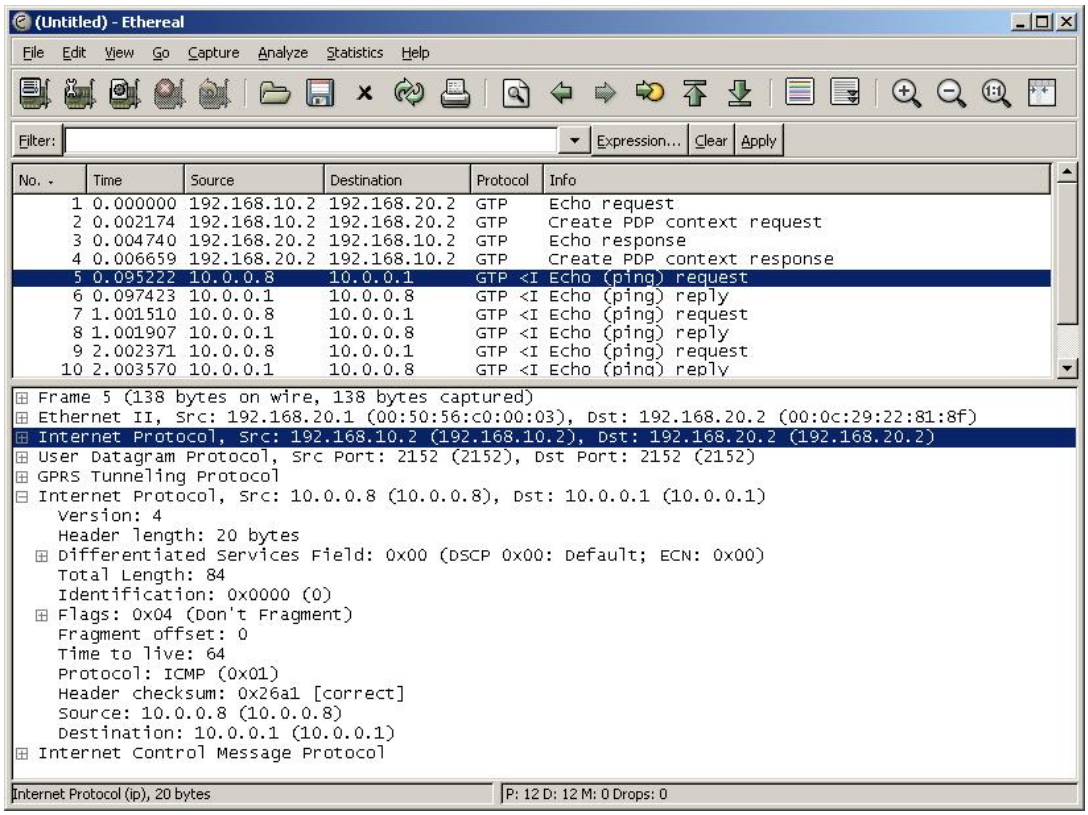
#### 14.2.4.1 Test Adımının Uygulanması

SGSN ile GGSN düğümü arasında ağ dinleyici çalıştırılarak düğümler arasında akan IP paketleri yakalanmaya başlanmıştır. Daha sonra SGSN düğümü üzerinde "s*gsnemu –listen 192.168.10.2 –remote 192.168.20.2 –pinghost 10.0.0.1*" komutu çalıştırılarak SGSN-GGSN düğümleri arasında GTP tüneli kurulması sağlanmıştır. Tünel kurulum aşamasında abone için GGSN tarafından 10.0.0.8 IP adresi tahsis edilmiştir. Komutun çalıştırılması ile SGSN düğümü üzerinde görünen bilgi mesajları Şekil 14-1'de verilmiştir. Komut içerisinde verilen *pinghost* parametresi ile GGSN üzerinde Gi arayüzü IP adresi olan 10.0.0.1 adresine sürekli olarak ICMP mesajları gönderilmiştir.

Şekil 14-2'de SGSN ve GGSN arasında kurulan tünele ait IP paketleri görülmektedir. Protokol kısmında GTP görünmesi nedeni ile haberleşmenin açık metin (clear text) olarak yapıldığına karar verilmiştir. IPSec gibi bir şifreleme yöntemi kullanılmış olsaydı IP paketi içerisinde bulunan bilgiler şifreli olarak gönderilmiş olacaktı. Şekil 14-2'de IP paketi içerisinde bulunan paketin bilgileri (IP paketi içindeki IP paketi) açık olarak görülmektedir.




**Şekil 14-1 SGSN düğümü üzerinde SGSNEMU komut çıktısı**




**Şekil 14-2 SGSN ve GGSN arasındaki trafiğin analizi**

#### 14.2.4.2 Karar

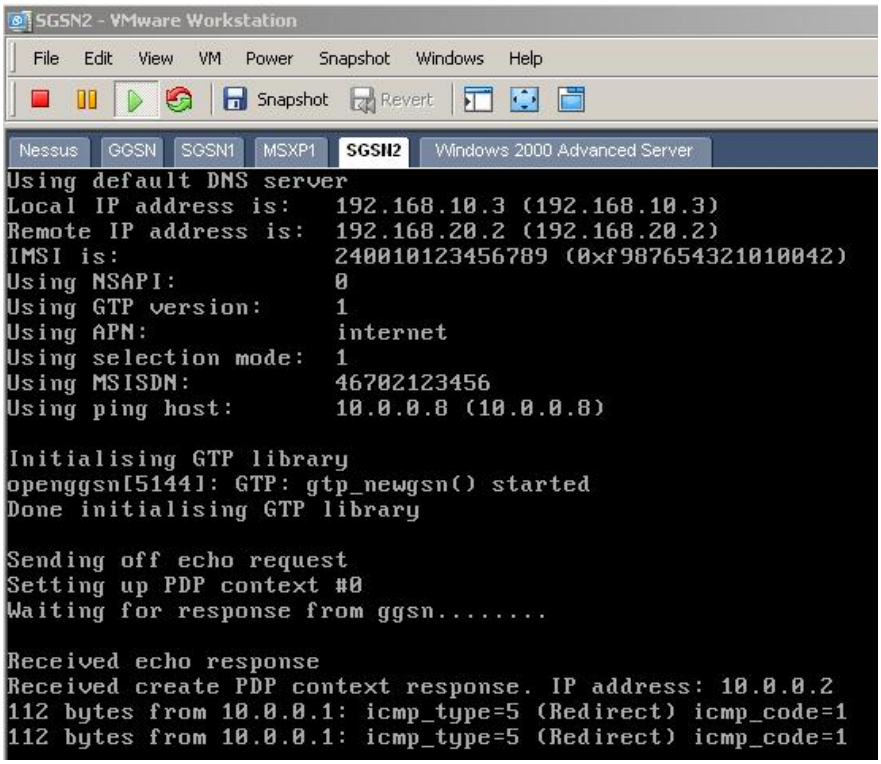
SGSN ve GGSN düğümleri arasında şifreleme yapılmaması nedeni ile GPRS şebekesi test adımından **KALDI.**

### 14.2.5 Aboneler Arası Saldırı Testi

#### 14.2.5.1 Test Adımının Uygulanması

Dört numaralı adımda aboneye GGSN tarafından 10.0.0.8 IP adresi tahsis edilmiştir. Uygulamakta olduğumuz test adımında ikinci bir SGSN (SGSN-2) üzerinde "s*gsnemu –listen 192.168.10.3 –remote 192.168.20.2 –pinghost 10.0.0.8*" komutu çalıştırılarak aboneler arası iletişim testi yapılmıştır. Test sırasında GGSN tarafından tahsis edilen IP adresi 10.0.0.2'dir (Şekil 14-3)

10.0.0.2 IP adresine sahip aboneden 10.0.0.8 IP adresine sahip aboneye ICMP paketleri gönderildiğinde 10.0.0.1 IP adresinden (GGSN IP adresi) ICMP mesaj türü olarak 5, kodu olarak 1 olan bilgi mesajları geri dönmüştür. Bu mesajın anlamı hedeflenen IP adresine (10.0.0.8) ulaşılamayacağıdır. Sonuç olarak örnek GPRS şebekesi üzerinde aboneler arası iletişimin engellendiği anlaşılmaktadır.




**Şekil 14-3 Aboneler arası saldırı testi**

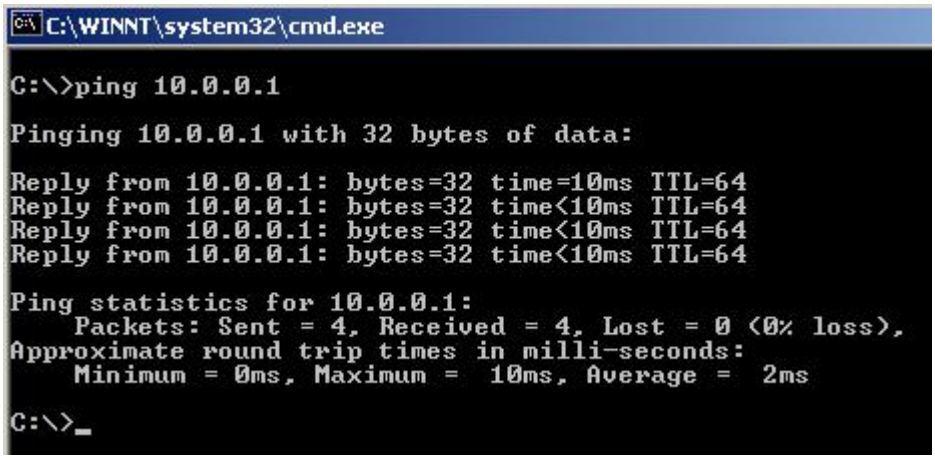
#### 14.2.5.2 Karar

GPRS şebekesine bağlı aboneler arasındaki trafiğin filtrelenmesi nedeni ile GRPS şebekesi test adımından **GEÇTİ.**

### 14.2.6 İnternet Üzerinden Saldırı Testi

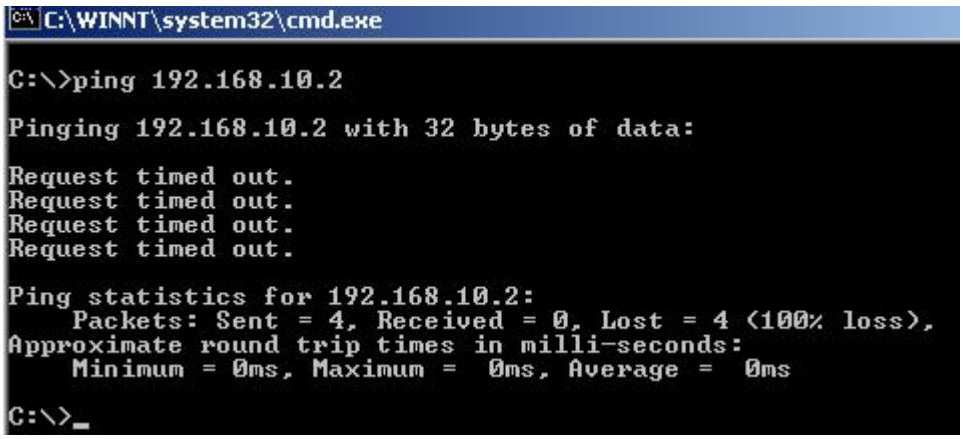
#### 14.2.6.1 Test Adımının Uygulanması

Denetçi sunucusu GPRS şebekesinin bağlı bulunduğu paket veri ağına bağlanmış ve 172.16.0.1 IP adresi verilmiştir. Bu bilgisayar üzerinden 10.0.0.1 IP adresine (GGSN Gi arayüzü IP adresi) ICMP paketleri gönderilerek erişim testi yapılmıştır (Şekil 14-4).



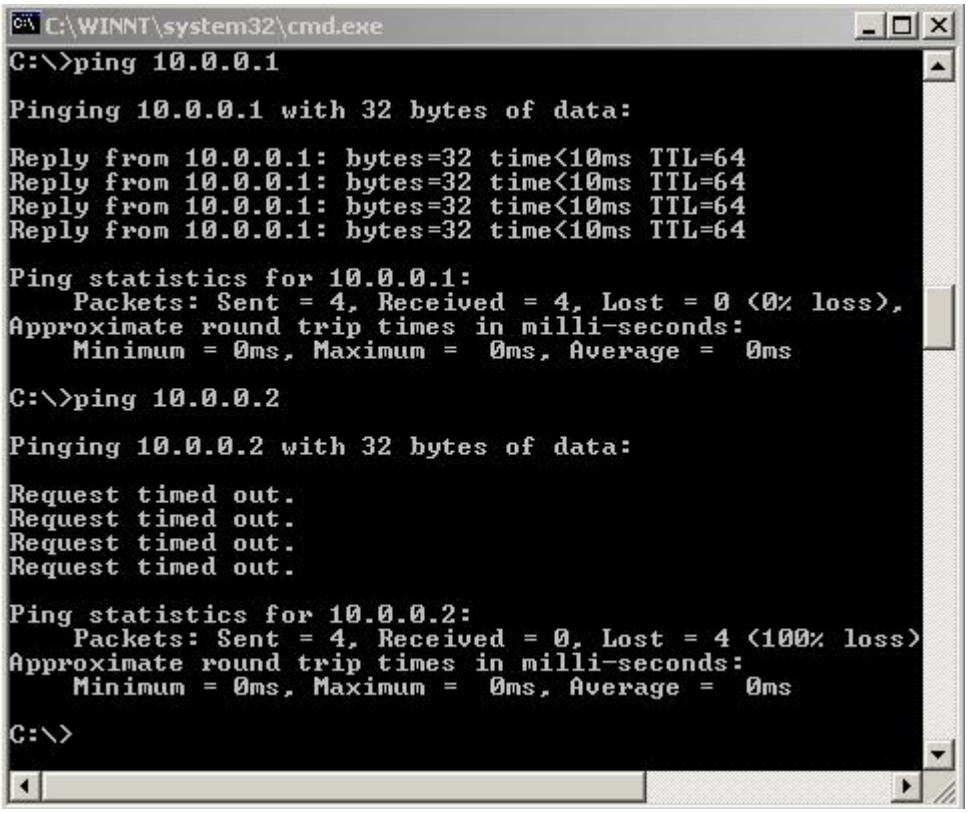

**Şekil 14-4 Paket veri ağından Gi arayüzüne erişim testi**

Paket veri ağında bulunan denetçi sunucusu GPRS omurgasında bulunan IP adreslerine ( Örneğin SGSN Gn arayüzü IP adresine – 192.168.10.2) erişememelidir. Denetçi sunucusu üzerinde *"ping 192.168.10.2"* komutu ile paket veri ağında bulunan bir bilgisayarın GPRS omurgasına ulaşma testi yapılmıştır. Sonuç olarak ulaşılamadığı görülmüştür (Şekil 14-5).




**Şekil 14-5 Paket veri ağından Gi arayüzüne erişimi**

Bir sonraki adımda SGSN düğümü üzerinde "s*gsnemu –listen 192.168.10.2 –remote 192.168.20.2 –pinghost 10.0.0.1*" komutu çalıştırılarak SGSN-GGSN düğümleri arasında GTP tüneli kurulması sağlanmıştır. Tünel kurulum aşamasında abone için GGSN tarafından 10.0.0.2 IP adresi tahsis edilmiştir. Daha sonra denetçi sunucusu üzerinde *"ping 10.0.0.2"* komutu çalıştırılarak aboneye erişilmeye çalışılmıştır. Sonuçta aboneye erişilemediği görülmüştür (Şekil 14-6).




**Şekil 14-6 Paket veri ağından aboneye erişim**

### 14.2.6.2 Karar

Paket veri ağı üzerinden abone IP adreslerine erişimin engellenmiş olması nedeni ile GPRS şebekesi test adımından **GEÇTİ.**

### 14.2.7 GPRS Omurgası Bileşenleri Açıklıkları Testi

#### 14.2.7.1 Test Adımının Uygulanması

En son açıklıkların yüklü olduğu *Nessus Security Scanner* yazılımı ile güvenlik taraması yapılmıştır.

Tarama yapılan IP adresleri aşağıdaki gibidir;

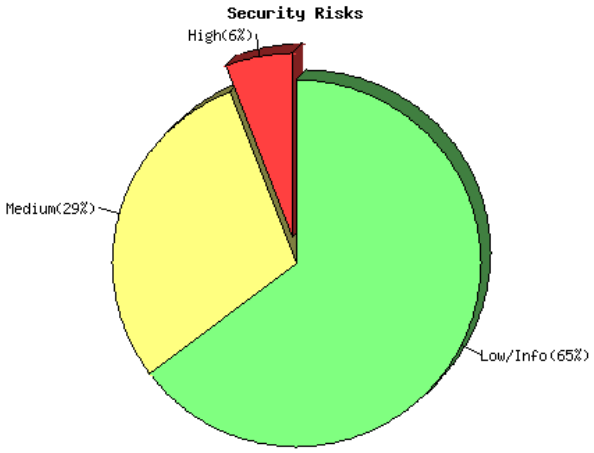
SGSN Gn arayüzü IP adresi 192.168.10.2

GGSN Gn arayüzü IP adresi 192.168.20.2

GPRS şebekesinin kurulumu sırasında RedHat 9.0 Linux işletim sistemi kullanılması nedeni ile tarama sonucunda her iki düğüm içinde aynı bulgular elde edilmiştir. Tarama sonuçlarına göre 1 adet güvenlik açığı, 5 adet güvenlik uyarısı ve 11 adet güvenlik notu bulunmuştur.

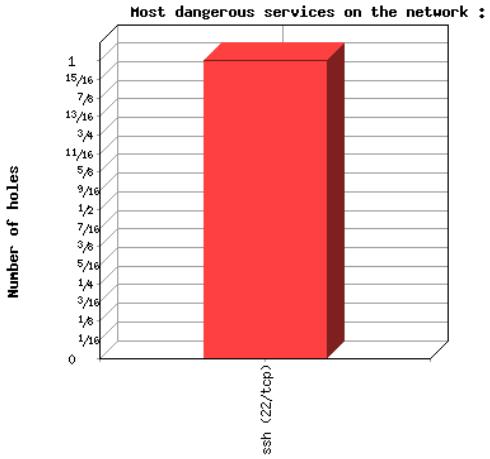
##### 14.2.7.1.1 Tarama Sonuçları (Grafik)

SGSN ve GGSN düğümleri tarama sonuçlarında tespit edilen güvenlik risklerine ait dağılım Şekil 14-7'te görülmektedir. Dağılıma göre tespit edilen risklerin %6'sı yüksek, %29'u orta ve %65'i düşük risk grubundadır.




**Şekil 14-7 Tarama sonuçları güvenlik riski dağılımı**

Düğümler üzerinde yapılan tarama sonucunda bulunan en tehlikeli servis ***ssh (22/TCP)*** servisidir.




**Şekil 14-8 Tarama sonucunda tespit edilen en tehlikeli servis**

### 14.2.7.1.2 Tarama Sonuçları (Yazılı)

Güvenlik tarayıcısı tarafından bulunan açık portlar aşağıda listelenmiştir:

| **Port numarası** | **Tarama sonucu** |
|---|---|
| ssh (22/tcp) | Güvenlik açığı bulundu |
| sunrpc (111/tcp) | Güvenlik notu bulundu |
| kdm (1024/tcp) | Güvenlik notu bulundu |
| sunrpc (111/udp) | Güvenlik notu bulundu |
| unknown (1024/udp) | Güvenlik uyarısı bulundu |
| general/udp | Güvenlik notu bulundu |
| general/tcp | Güvenlik uyarısı bulundu |
| general/icmp | Güvenlik uyarısı bulundu |

**1 numaralı güvenlik açığı - ssh (22/tcp)**

Ssh protokolü linux sunuculara uzaktan erişerek yönetim yapmak amacı ile kullanılmaktadır. Tarama sonucunda sunucu üzerinde 3.7.1'den daha eski sürüm OpenSSH koştuğu tespit edilmiştir. 3.7.1'den daha eski OpenSSH sürümleri tampon bellek yönetim fonksiyonlarında açıklık içermektedir.

**Uyarı:** Saldırganlar bu açıklığı istismar ederek rastgele komutlar çalıştırabilirler.

**Çözüm:** OpenSSH sürümü 3.7.1'e çıkartılmalıdır.

**Risk faktörü:** Yüksek

**1 numaralı güvenlik uyarısı - ssh (22/tcp)**

Sunucu üzerinde koşan ssh servisi, 1.33 veya 1.5 ssh sürümlerini kullanarak bağlanmaya çalışan bilgisayarlara izin vermektedir.

**Uyarı:** ssh sürüm 1.33 ve 1.5 ile haberleşme güvenli olarak şifrelenememektedir.

**Çözüm:** OpenSSH servisinin konfigürasyonunda "protocol" parametresi "2" olarak değiştirilmelidir.

**Risk faktörü:** Düşük

**2 numaralı güvenlik uyarısı - ssh (22/tcp)**

Tarama sonucunda sunucu üzerinde 3.6.1'den daha eski sürüm OpenSSH koştuğu tespit edilmiştir. 3.6.1'den daha eski OpenSSH sürümleri sunucu üzerinde tanımlanmış erişim kontrol listelerinin atlatılmasına yönelik açıklık içermektedir.

**Uyarı:** Bir saldırgan bu açıklığı kullanarak sunucu üzerinde tanımlanmış erişim kontrol listelerini atlatıp başka sunucuculara erişebilir.

**Çözüm:** OpenSSH sürümü en az 3.6.1'e çıkartılmalıdır.

**Risk faktörü:** Düşük

**3 numaralı güvenlik uyarısı – 1024 numaralı UDP portu**

Tarama sonucunda sunucu üzerinde 1024 portunda çalışan RPC servisi tespit edilmiştir. Günümüzde çıkan açıklıkların bir çoğu RPC servisini etkilemektedir.

**Uyarı:** 1024 numaralı portta çalışan RPC servisine dair bir güvenlik açığı henüz tespit edilmemiştir. Bu ifade açıklık olmayacağı anlamına gelmemektedir.

**Çözüm:** Servisin çalışması gerekmiyorsa durdurulması tavsiye edilir.

**Risk faktörü:** Yüksek

**4 numaralı güvenlik uyarısı - General/tcp**

Tarama sırasında gönderilen FIN bayrağı kurulmuş TCP SYN paketlerinin düğümler tarafından işlendiği görülmüştür (paketler çöpe atılmamıştır).

Daha ayrıntılı bilgi için aşağıdaki internet adresleri kullanılmalıdır.

http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html
http://www.kb.cert.org/vuls/id/464113

**Uyarı:** Saldırgan kullanılan güvenlik duvarının türüne bağlı olarak güvenlik kurallarını atlatabilir.

**Çözüm:** Bu açıklık için yama çıkarılıp çıkarılmadığı kontrol edilmeli, çıkarılmadıysa üretici firmadan talep edilmelidir.

**Risk Faktörü:** Orta

**4 numaralı güvenlik uyarısı - General/icmp**

Test edilen sistem ICMP zaman damgası isteklerine yanıt vermiştir. Bu durum bir saldırganın test edilen sistemin saat bilgisini öğrenebileceği anlamına gelmektedir.

**Uyarı:** Saldırgan zaman bilgisini kullanarak doğrulama protokollerinin çalışmasını sekteye uğratacak eylemlerde bulunabilir.

**Çözüm:** ICMP zaman damgası istekleri (port numarası 13) ve ICMP zaman damgası yanıtları (port numarası 14) kısıtlanmalıdır. Ayrıntılı bilgi için RFC 867'e başvurulabilir.

**Risk Faktörü:** Düşük

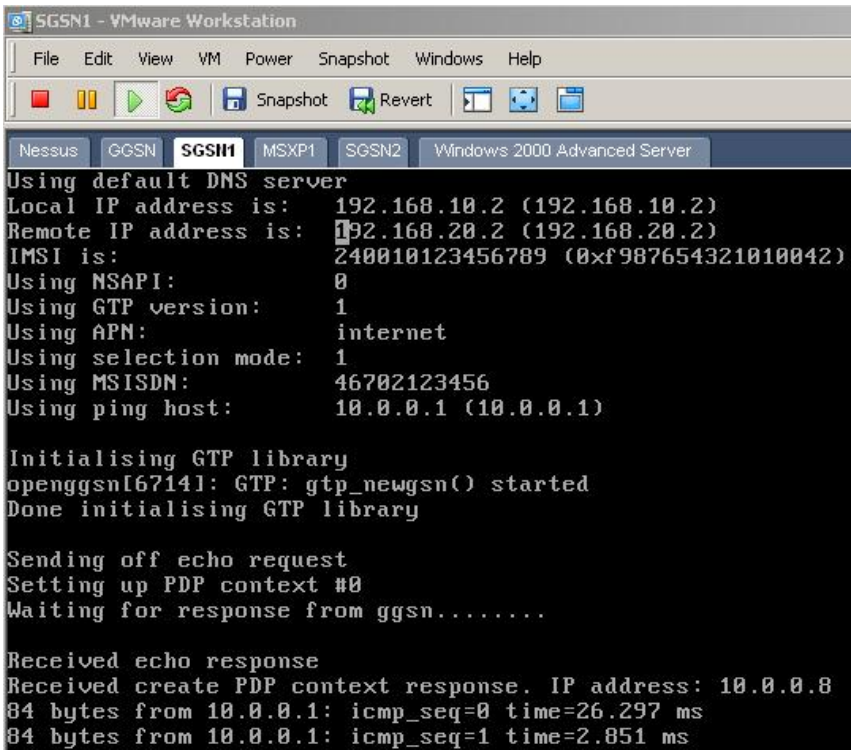
#### 14.2.7.2 Karar

SGSN ve GGSN düğümlerinde güvenlik açıklıkları bulunması nedeni ile GPRS şebekesi test adımından **KALDI.**

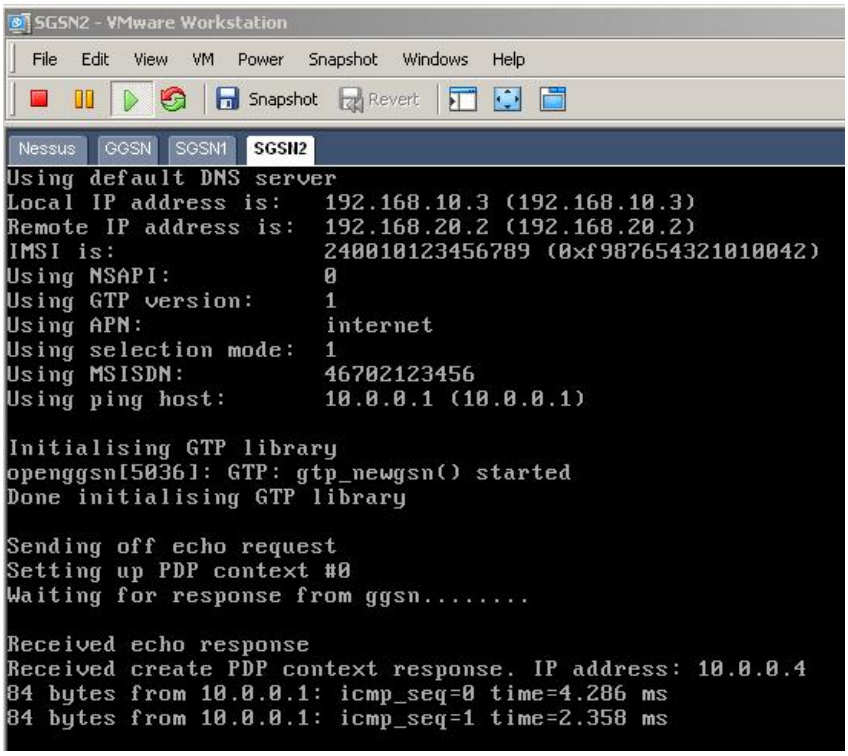
### 14.2.8 Abone IP Adreslerinin Dağıtımı (NAT kullanımı) Testi

#### 14.2.8.1 Test Adımının Uygulanması

SGSN1 sunucusu üzerinde "s*gsnemu –listen 192.168.10.2 –remote 192.168.20.2 –pinghost 10.0.0.1*" komutu, SGSN2 sunucusu üzerinde "s*gsnemu –listen 192.168.10.3 –remote 192.168.20.2 –pinghost 10.0.0.1*" komutu çalıştırılmıştır. Çalıştırılan komutlar sonucunda GGSN düğümüne bağlantı kurulmuş ve SGSG1 sunucusuna 10.0.0.8 (Şekil 14-9), SGSN2 sunucusuna 10.0.0.4 (Şekil 14-10) IP adresi atandığı görünmüştür. Buradan abonelere 10.0.0.0 ağında IP adresi verildiği anlaşılmaktadır. GPRS omurgasında bulunan SGSN düğümleri için 192.168.10.0 IP adres bloğu, GGSN için ise 192.168.20.0 IP adres bloğunun kullanıldığı görülmüştür.




**Şekil 14-9 Birinci abone IP adresi**




**Şekil 14-10 İkinci abone IP adresi**

### 14.2.8.2 Karar

GPRS şebekesi üzerinde kullanılan ve abonelere dağıtılan IP adreslerinin internet üzerinde

kullanılan IP adreslerinden izole edilmiş olması nedeni ile GPRS şebekesi test adımından **GEÇTİ.**

### 14.2.9 Güvenlik Duvarı ve Geçit Cihazları Testi

#### 14.2.9.1 Test Adımının Uygulanması

GPRS şebekesinin başka GPRS şebekesine ara yüzü bulunmamaktadır. Bu sebeple Gp arayüzüne dair ağ geçit cihazı, güvenlik duvarı gibi kontrollerin yapılmasına gerek yoktur.

İnternet bağlantısını sağlayan GGSN düğümü üzerinde güvenlik duvarı hizmetlerini vermek üzere "IPTables" yazılımı koşmaktadır. Aboneler arası saldırı testi adımında abonelerin birbirleri ile iletişimi olmadığını ve internet üzerinden saldırı test adımında internet üzerinden abonelere doğru gönderilen trafiğin filtrelendiği görülmüştür.

#### 14.2.9.2 Karar

Şebeke üzerinde ihtiyaç duyulan güvenlik duvarı bulunması nedeni ile GPRS şebekesi test adımından **GEÇTİ.**

### 14.2.10 Abone IP adreslerinden SGSN ve GGSN Sistemlerine Erişim Testi

#### 14.2.10.1 Test Adımının Uygulanması

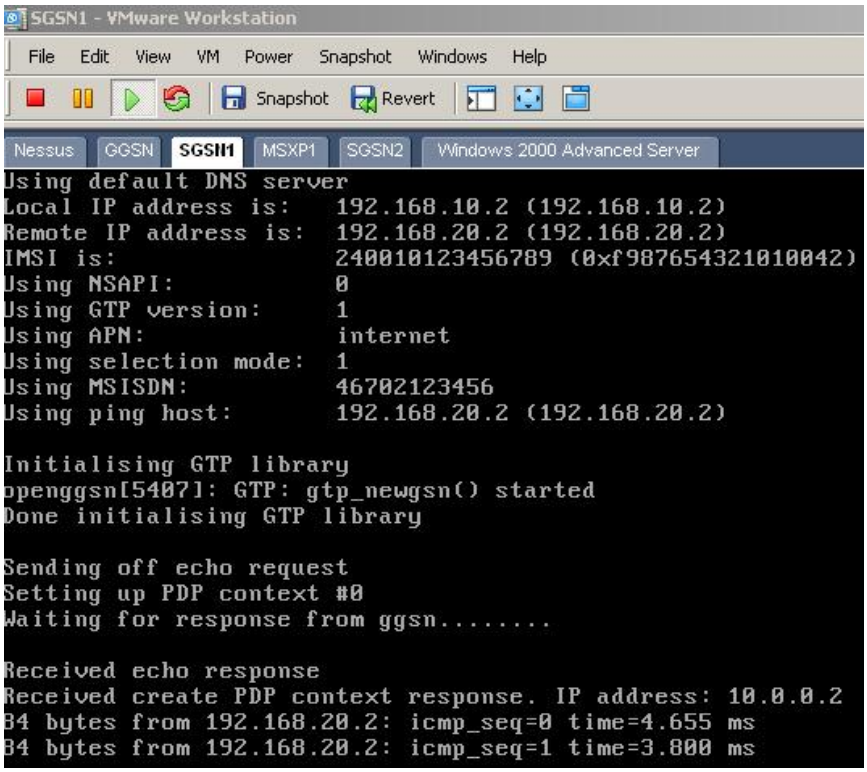
Abonelere tahsis edilen IP adresleri (10.0.0.0) ile GPRS omurgasında kullanılan IP adreslerinin (192.168.10.0 ve 192.168.20.0) farklı IP adres uzaylarından olduğu görülmüştür. Buna karşın 10.0.0.0 abone IP adresleri ağından 192.168.10.0 ve 192.168.20.0 GPRS destek düğümleri ağlarına erişilebildiği tespit edilmiştir.

İlk olarak SGSN1 düğümü üzerinde "s*gsnemu –listen 192.168.10.2 –remote 192.168.20.2 –pinghost 192.168.20.2*" komutu çalıştırılmıştır. Bu komut sonucunda 10.0.0.2 abone IP adresinden 192.168.20.2 GGSN IP adresine erişilmiştir (Şekil 14-11).

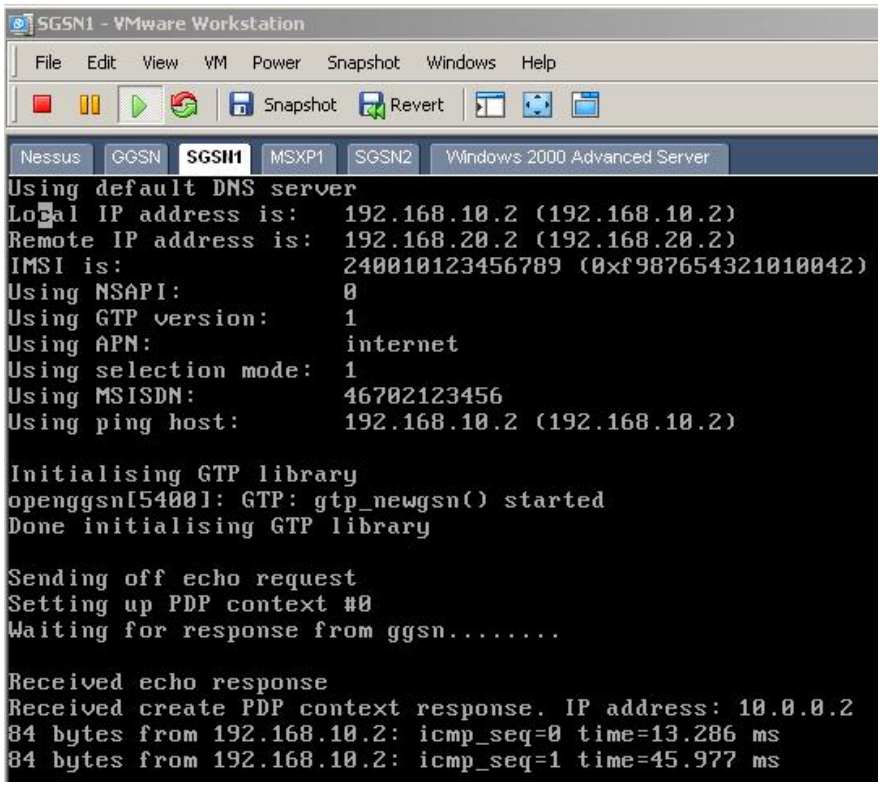
Daha sonra yine SGSN1 düğümü üzerinde "s*gsnemu –listen 192.168.10.2 –remote 192.168.20.2 –pinghost 192.168.10.2*" komutu çalıştırılmıştır. Bu komut sonucunda 10.0.0.2 abone IP adresinden 192.168.20.2 GGSN IP adresine erişilmiştir (Şekil 14-11).

Bu işlemler sırasında GGSN düğümü üzerinde "*tcpdump*" komutu çalıştırılarak IP paketleri yakalanmıştır. Yakalanan IP paketlerinden ping komutu ile gönderilen ICMP paketlerinin 192.168.10.2 (SGSN) adresinden 192.168.20.2 (GGSN) adresine GTP protokolü ile taşındığı ve bu adresten sonra 192.168.10.2 adresine yönlendirildiği görülmüştür. 192.168.20.2 IP

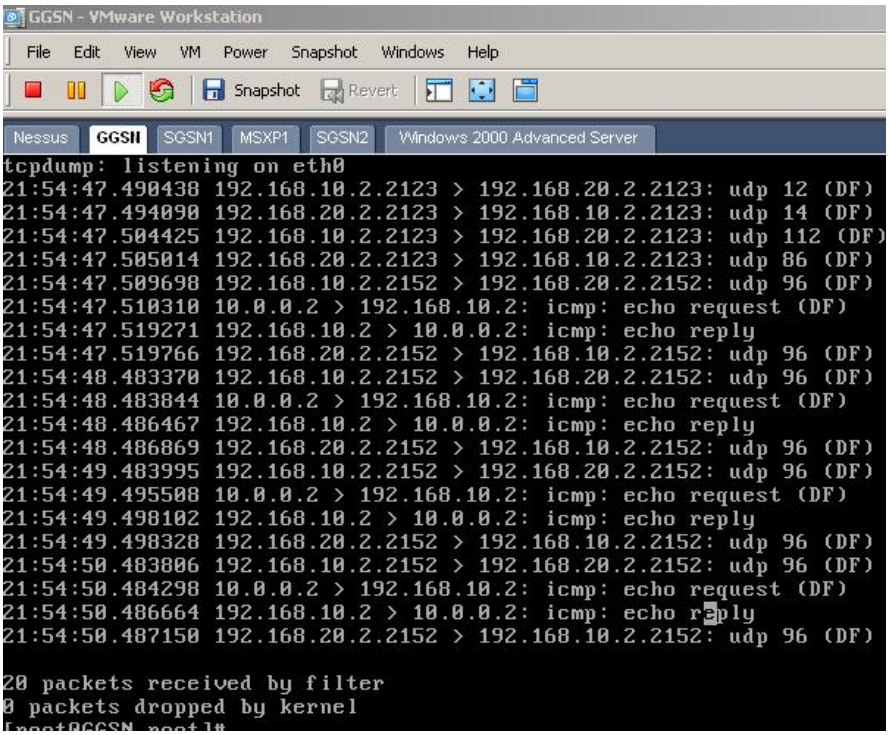
adresinden gelen yanıtların GGSN düğümüne geldiği ve buradan tünel ile SGSN'e gönderildiği görülmüştür (Şekil 14-13).




**Şekil 14-11 Abone IP adresinden GGSN IP adresine erişim**




**Şekil 14-12 Abone IP adresinden SGSN IP adresine erişim**




**Şekil 14-13 GGSN düğümü üzerinde yapılan dinleme**

#### 14.2.10.2 Karar

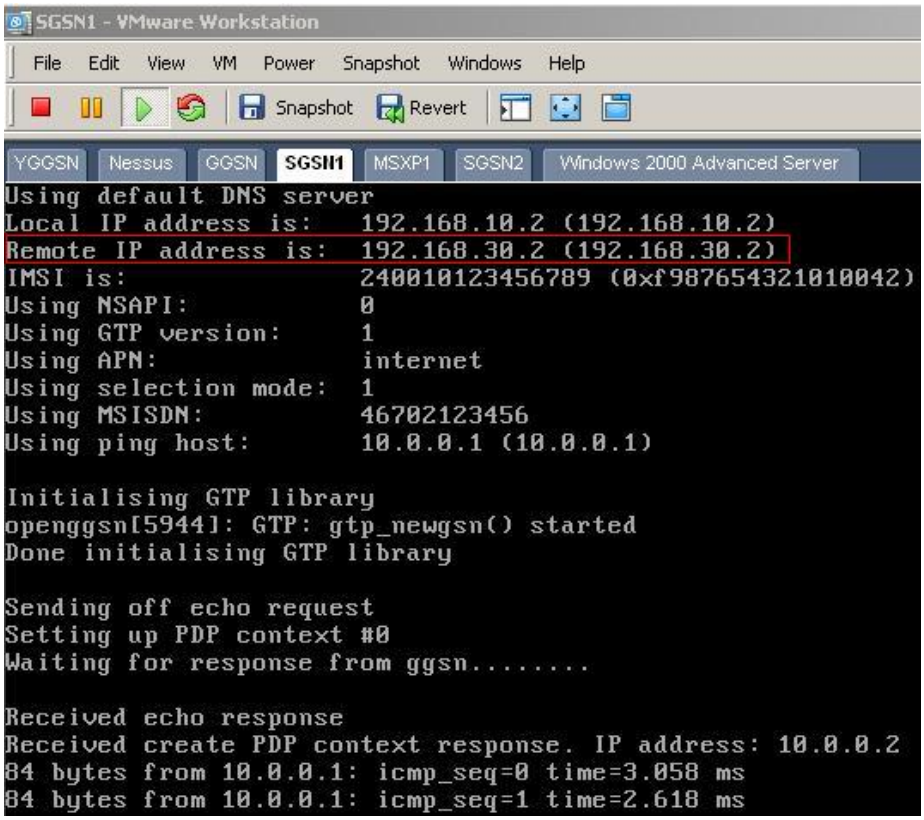
Abone IP adreslerinden SGSN ve GGSN düğümlerinin IP adreslerine erişilebilmesi nedeni ile GPRS şebekesi test adımından **KALDI.**

### 14.2.11 SGSN ve GGSN Düğümleri Erişim Kontrol Listeleri Testi

#### 14.2.11.1 Test Adımının Uygulanması

Yapılan inceleme sonucunda SGSN ve GGSN düğümleri üzerinde haberleşecekleri düğümlere ait adres bilgilerinden oluşan erişim kontrol listeleri bulunmadığı görülmüştür. Mevcut sistem üzerinde taklit SGSN ve GGSN düğümleri oluşturularak gerçek düğümler ile haberleşilmesi mümkündür.

İnceleme sonuçlarının doğruluğu için sisteme yeni GGSN eklenerek SGSN1 üzerinden bağlantının testi yapılmıştır. Yeni GGSN IP adresi 192.168.30.2 olarak ayarlanmıştır (Şekil 14-14). SGSN1 düğümü üzerinde "s*gsnemu –listen 192.168.10.2 –remote 192.168.30.2 –pinghost 10.0.0.1*" komutu çalıştırılmıştır. Komut sonucunda GTP tünelinin kurulduğu görülmüştür.




**Şekil 14-14 Taklit GGSN düğümü ekleme**

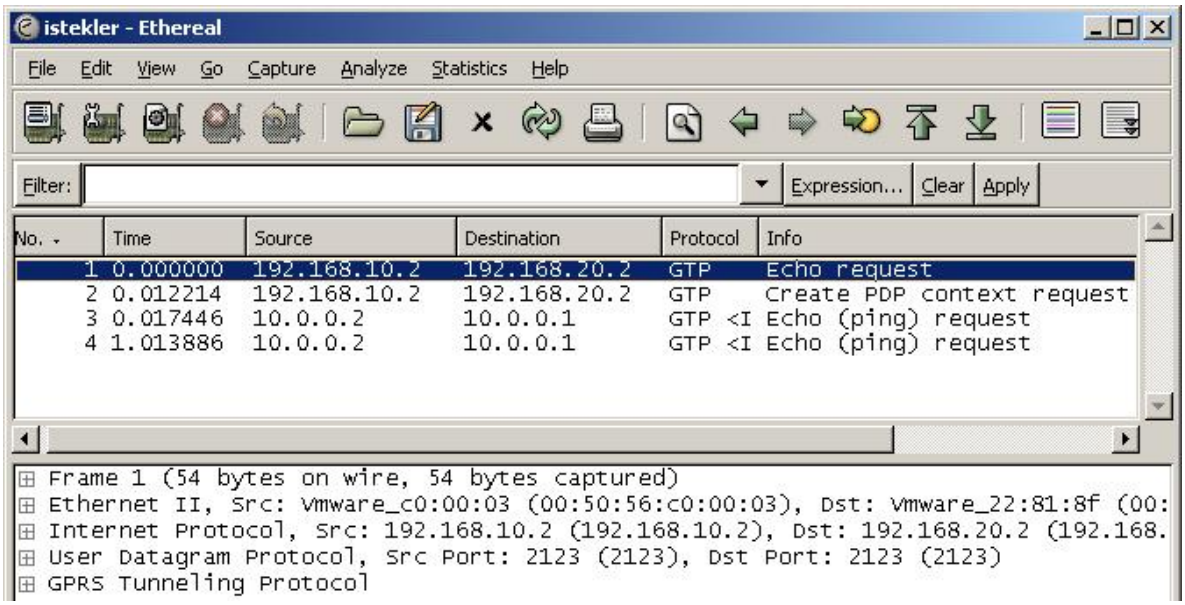
#### 14.2.11.2 Karar

SGSN ve GGSN düğümleri üzerinde erişim kontrol listelerinin tanımlanmamış olması nedeni ile GPRS şebekesi test adımından **KALDI.**

### 14.2.12GTP PDP İçerik Silme, İçerik Güncelleme ve İçerik Oluşturma Test Adımı

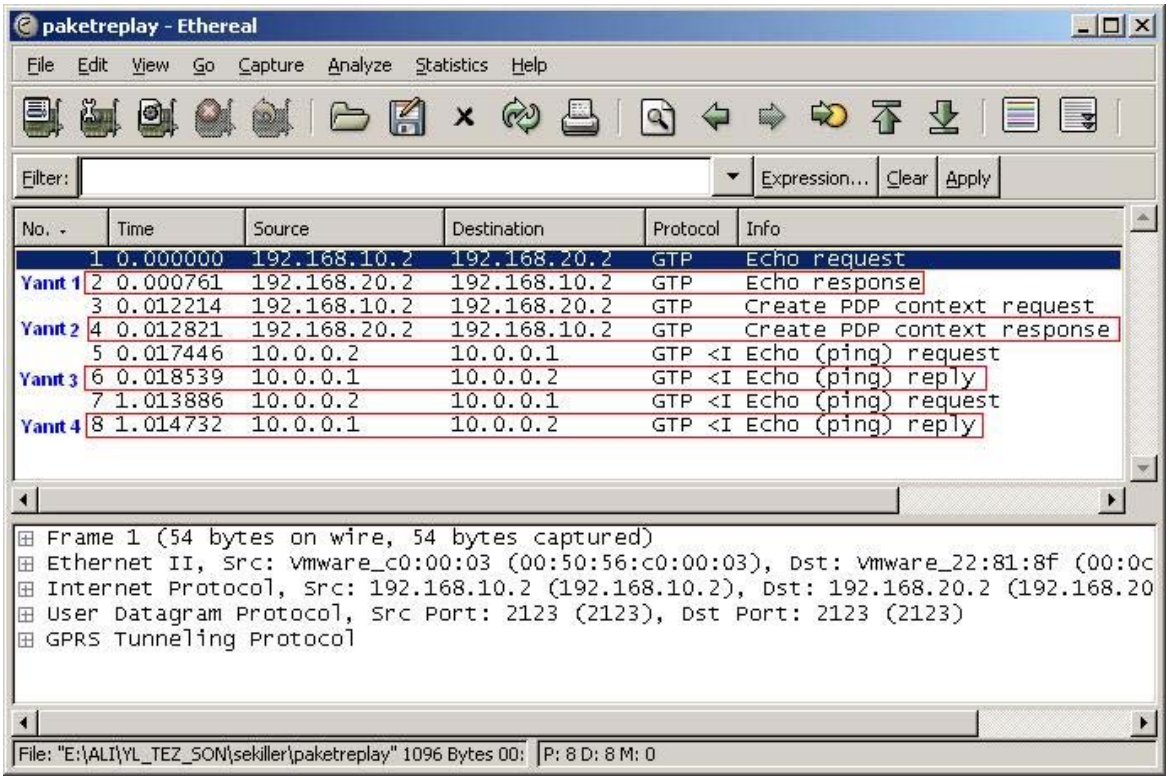
#### 14.2.12.1 Test Adımının Uygulanması

İlk olarak Denetçi sunucusu 192.168.20.0 ağına bağlanmış ve Shomiti yazılımı paket yakalama modunda çalıştırılmıştır. Aynı anda yönlendirici üzerinde etherel paket yakalayıcı başlatılmıştır. Daha sonra SGSN1 üzerinde "s*gsnemu –listen 192.168.10.2 –remote 192.168.20.2 –pinghost 10.0.0.1*" komutu çalıştırılmıştır. Bu komut sayesinde PDP içerik etkinleştirmesine dair IP paketleri yakalanmıştır (Şekil 14-15).




**Şekil 14-15 PDP içerik etkinleştirmesine ait GTP paketleri**

İkinci adım olarak denetçi sunucusu üzerinde yakalanan paketler yeniden ağa verilmiştir. Gönderilen paketlere (Şekil 14-15) GGSN düğümünün yanıt verdiği görülmüştür (Şekil 14-16).




**Şekil 14-16 GGSN düğümünün taklit GTP paketlerine yanıtı**

PDP içerik silme ve güncelleme, SGSN ile GGSN arasındaki trafiğin dinlenerek tünel belirteçlerinin öğrenilmesinin ardından rahatlıkla yapılabilir. Bu problemlerin çözümü için

SGSN ve GGSN düğümleri arasında IPSec protokolü ile şifreleme yapılmalıdır.

#### 14.2.12.2 Karar

SGSN ve GGSN düğümleri arasında IPSec protokolü ile şifreleme yapılmaması nedeni ile GPRS şebekesi test adımından **KALDI.**

# 15. SONUÇLAR

Geçtiğimiz 10 yıl zarfında mobil cihazlar büyük bir değişime uğramıştır. Önceleri ses haberleşmesi yapmaktan öteye gitmeyen cihazları bugün adeta küçük bir bilgisayar olarak ceplerimizde taşımaktayız. Mobil cihazların gelişmesi ve kullanım alanlarının çeşitlenerek yaygınlaşması, özellikle kurumların veri güvenliği için ciddi bir tehdit oluşturmuştur. Güvenlik konusunda zincirdeki en zayıf halka ilkesi geçerlidir. Bu nedenle mobil cihazlar ile alınan hizmetler için uçtan uca güvenlik sağlanması önemlidir. Kurumlar güvenlik gerektiren uygulamalarında GPRS üzerinden sanal özel ağ (VPN) teknolojisini kullanmalıdır.

GPRS şebekesinde korunması gereken bilgilerin neler olduğu ve kimlerden korunması gerektiği bilinmeden olası tehditleri ortaya koymak mümkün değildir. Tez kapsamında GPRS şebekelerinde korunması gereken bilgiler ve bu bilgilerin kimlerden korunması gerektiği verilmiştir. Her GPRS operatörü, kendine ait tehditleri ve bu tehditlerin gerçekleşmesi durumunda oluşabilecek potansiyel zararları belirlemeli, tehditlerin etkisinin azaltılması veya ortadan kaldırılması için gerekli önlemleri planlayarak uygulamalıdır. Bu işlemler risk yönetimi süreci olarak adlandırılmaktadır. Bu süreç GPRS operatörü tarafından bir yaşam döngüsüne oturtulmalı ve riskler sürekli kontrol altında tutulmalıdır.

GPRS şebekesi kendi abonelerini doğrudan paket veri ağlarına (en genel anlamda internet) bağlamaktadır. GPRS şebekesinde ücretlendirmenin transfer edilen veri miktarı üzerinden olduğu düşünülürse, aboneler tarafından başlatılmayan bağlantıların filtrelenmemesi durumunda aboneye yüksek ücretlendirme yapılması söz konusudur. Aynı durum aboneler arası (abone başka bir GPRS operatörünün abonesi de olabilir) trafiğin engellenmemesinde de yaşanabilmektedir. Bu tür problemlerin önüne geçebilmek için şebekenin internet arayüzünde ve diğer şebekeler ile olan arayüzlerinde filtreleme yapılmalıdır.

GPRS şebekesinde şifreleme, abone ile SGSN düğümü arasında yapılmaktadır. Şebekenin geri kalan bölümlerinde herhangi bir doğrulama ve şifreleme mekanizması çalışmamaktadır. Tez kapsamında yapılan çalışmalarda, GPRS omurgasına ulaşabilen bir saldırganın abonelere ait trafiği dinleyebildiği, değiştirebildiği ve eğer haberleşmeyi kesintiye uğratmak istiyorsa PDP içerik silme mesajı göndererek kesebildiği tespit edilmiştir. Bu riski ortadan kaldırmak için SGSN ve GGSN düğümleri arasında IPSec protokolü kullanılarak şifreleme yapılmalıdır. IPSec kullanımı ile hem önceden belirlenmiş SGSN ve GGSN düğümlerinin birbiri ile haberleşmesi, hem de düğümler arasında akan verinin güvenliği sağlanmış olacaktır. Aynı yöntem diğer operatörler ile yapılan bağlantılarda da uygulanmalıdır.

GPRS operatörünün belirlemiş olduğu risklere karşı alacağı önlemlerin tamamı teknik önlemler olmamalıdır. Şebekenin işletimine ve güvenliğine dair kuralların belirlenmesi, bu kuralların personelin tamamı tarafından bilinerek uygulanması gereklidir. Oluşturulması gereken dokümanlardan ilki güvenlik politikasıdır. Bu politika, GPRS operatörü tarafından uygulanacak güvenlik ilkelerinin tamamını içermelidir. Politikanın kullanımı ile GPRS operatörünün sahip olduğu bilgilere dair gizliliğin, bütünlüğün ve sürekliliğin ihtiyaç duyulan seviyede korunması amaçlanmalıdır. Tez içerisinde GPRS operatörleri için örnek teşkil edecek bir güvenlik politikası verilmiştir. İkinci kritik doküman şebekenin düzgün işletilebilmesi ve görev değişikliklerinden etkilenmemesi için hazırlanması gereken konfigürasyon ve çalışma esasları dokumanıdır. Bu doküman içerisinde en az, GPRS şebekesini oluşturan cihazlar ile ilgili konfigürasyon bilgileri, omurganın IP adres dağılımı, sistemin işletimine dair kayıtların izleme yöntemi ve şebeke bileşenlerinden sorumlu personelin görevleri bulunmalıdır.

Tez kapsamında geliştirilen güvenlik talimatı, ilk olarak Ericsson Mobility World GPRS şebekesi üzerinde uygulanmış ve beş adet kritik eksiklik tespit edilmiştir. Bu eksikliklerden ilki GPRS şebekesine dair bir güvenlik politikasının bulunmayışıdır. Her GPRS operatöründe yönetimin bakış açısını ve desteğini içeren bir güvenlik politikası bulunmalı, aksi durumda güvenlik bilinci olmadığı kabul edilmelidir. Tespit edilen diğer önemli açıklıklar GPRS omurgasında şifreleme yapılmaması, aboneler arasındaki trafiğin şifrelenmemesi ve GPRS hizmet düğümleri üzerinde erişim kontrol listelerinin tanımlanmamış olmasıdır. Bu üç açıklık saldırganlar için açık kapı niteliğindedir ve GPRS şebekesi için ciddi bir risk oluşturmaktadır. Son olarak tespit edilen açıklık GPRS hizmet düğümlerinin işletim sistemi yamalarının yapılmamış olmasıdır. Test talimatının ikinci uygulaması, kurulan örnek GPRS şebekesi üzerinde yapılmıştır. Test sonucunda GPRS şebekesinin yedi test adımından kaldığı tespit edilmiştir. Test şebekesindeki en önemli iki açıklık abonelerden GPRS destek düğümlerine erişilebilmesi ve düğümler arasında şifreleme yapılmıyor olmasıdır. Yapılan güvenlik testleri incelendiğinde ek güvenlik tedbirleri almayan GPRS şebekelerinin çok yüksek riskler içerdiği, bu nedenle güvensiz olduğu sonucuna varılmıştır. Bu tez kapsamında GPRS operatörlerinin alması gereken güvenlik tedbirleri detaylı olarak açıklanmıştır.

**KAYNAKLAR**

3GPP TR 21.905, "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications (Release 1999)".

3GPP TS 21.133, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Threats and Requirements (3G TS 21.133 version 3.1.0)"

3GPP TS 23.121, "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Architecture Requirements for Release 99".

3GPP TS 29.060," 3rd Generation Partnership Project (3GPP); General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface",(Release 6)

3GPP TS 33.105, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Cryptographic Algorithm Requirements (Release 1999)"

3GPP TS 33.120, "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".

AT&T Wireless Developer Program, (2003), "Secure Application Deployment with GPRS/EDGE", DevCentral White Paper

Bavosa, A., (2004),"GPRS Security Threats and Solution Recommendations", Juniper Networks, Inc.

Bettstetter, C., Vögel, H.J., Eberspächer, J., (1999),"GSM Phase 2+ General Packet Radio Service GPRS: Architecture, Protocols, and Air Interface". Technische Universität München (TUM). (IEEE Communications Surveys, Third Quarter 1999, vol. 2 no. 3)

Blyth, K. J., Cook, A., (2001), "Designing a GPRS Roaming Exchange Service", 3G Mobile Communication Technologies, Conference Publication No.477

Brookson, C., (2001), "GPRS Security", Charles Brookson

Brookson, C., "Adopting A Proactive Approach To GPRS Security", GSM Association Security Group, London, England

Candan, M.M., (2002), "Üçüncü Nesil Mobil Haberleşme Sistemleri İçin Türkiye'de Uygulanacak Frekans Bandı, Lisans, Servisler, Uygulamalar ve Ülkemizdeki Durumu" Uzmanlık Tezi, Telekomünikasyon Kurumu

Candolin, C., Lundberg, J.,(2001) "Attacks on GPRS", Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology, Finland

Check Point Software Technologies, (2004), "Achieving Vital Business Objectives While Securing Your GPRS/UMTS Network", Check Point Software Technologies Ltd.

Dinçkan, A., Kavas, A.,(2005), "Authentication and Ciphering In GPRS Network", ELECO Conference, Bursa

Dinçkan,A.,(2001), "TCP/IP Protocol Suit",Undergraduate Thesis, Istanbul Technical University, Elecktronics and Communication Engineering Department

Ericsson Radio System AB, (2000), “GPRS Support Node (GSN) Configuration”, Student Text LZU 108 3945

Ericsson Radio Systems AB, (2000), “GPRS System Survey”, Training Document, Student Text, Course Number LZU 108 876

Ericsson Radio Systems AB, (2000), “Administration and use of Network Configuration Data in SGSN; Function Description”

ETSI 3GPP TS 08.18, ”Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Base Station System (BSS) – Serving GPRS Support Node (SGSN) interface; BSS GPRS Protocol (BSSGP) (3GPP TS 08.18 version 8.6.0 Release 1999)”

ETSI GSM 01.04, ”Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms (GSM 01.04 version 8.0.0 Release 1999)”

ETSI GSM 01.61. “Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS);GPRS ciphering algorithm requirements, Vers,on 6.0.1”

ETSI GSM 03.03, ”Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification (GSM 03.03 version 7.5.0 Release 1998)”

ETSI GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

ETSI GSM 03.60, ”Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2 (GSM 03.60 version 7.4.1 Release 1998)”

ETSI GSM 04.01, ”Digital cellular telecommunications system (Phase 2+); Mobile Station – Base Station System (MS - BSS) interface; General aspects and principles (GSM 04.01 version 8.0.0 Release 1999)”

ETSI GSM 08.14, ”Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Base Station System (BSS) – Serving GPRS Support Node (SGSN) interface; Gb interface Layer 1 (GSM 08.14 version 8.0.0 Release 1999)”

ETSI GSM 08.16, ”Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Base Station System (BSS) – Serving GPRS Support Node (SGSN) interface; Network Service (GSM 08.16 version 8.0.0 Release 1999)”

ETSI GSM 08.18:”Digital cellular telecommunications system (Phase2+); General Packet Radio Service (GPRS); Base Station System (BSS)-Serving GPRS Support Node (SGSN); BSS GPRS Protocol (BSSGP)”

ETSI GSM 09.60, ”Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface (GSM 09.60 version 7.5.1 Release 1998)”

ETSI TS 121 133, “Universal Mobile Telecommunication System (UMTS); 3G Security; Security Threads and Requirements” V3.1.0

Grecas, C. F., Maniatis, S.I., Venieris, I.S., (2001), “Towards the Introduction of the Asymmetric Cryptography in GSM, GPRS, and UMTS Networks”, Electrical and Computer Engineering Dept., National Technical University of Athens

Hannikainen, M., Hamalainen, D., Niemi, M., Saarinen, J., (2002), "Trends in personel wireless data communications", Computer Communications, 25, s84.

Hannu, K., (2002), "GPRS Security Issues", Lecture notes

Heine, G., Sagkob, H., (2003), "GPRS: Gateway to Third Generation Mobile Networks", Artech House

Kaasin, E., Bjåen, G.S (2001), "Security in GPRS", Agder University College, Grimstat.

Kalden, R., Meirick, I., Meyer, M., (2000), "Wireless Internet Access Based on GPRS", Ericsson Research, Ericsson Eurolab, Deutschland

Kitsos, P.,Sklavos, N., Koufopavlou, O., (2004), "An End-to-End Hardware Approach Security for the GPRS", IEEE Mediterranean Electrotechnical Conference

Larsen, E., (2001), "GPRS for GSM Upgrade Strategies using Network Redundancy", Masters Thesis, Information and Communication Technology, Grimstad, Norway

Özdemir,E., (2001), "3. Nesil Mobil Haberleşme Sistemlerine Geçiş ve UMTS", KOU Bitirme Tezi, Kocaeli

Peng, C., (2000),"GSM and GPRS Security", Tik-110.501 Seminar on Network Security

Pesonen, L. ,(1999) "GSM Interception" , Helsinki Univerity of Technology

Piot, S.,(1998), "Security Over GPRS", Master of Science in Telecommunication, University College London

Rautpalo, J., (2000), "GPRS Security - Secure Remote Connections over GPRS", Tik-110.501 Seminar on Network Security

RFC 1825,(1995), "Security Architecture for the Internet Protocol", Naval Research Laboratory

RFC 1826,( 1995), "IP Authentication Header", Naval Research Laboratory

RFC 1827, (1995), "IP Encapsulating Security Payload" , Naval Research Laboratory

RFC 2401,(1998),"Security Architecture for the Internet Protocol"

RFC 2402,(1998),"IP Authentication Header (AH)"

RFC 2406,(1998),"IP Encapsulating Security Payload (ESP)"

RFC 2411,(1998), "IP Security Document Roadmap"

Ricky Ng, Trajkovic, L., (2002) "Simulation of General Packet Radio Service Network", School of Engineering Science, Simon Fraser University, Canada

Salberg, B.,(2001), "WLAN – GPRS Interworking", Graduate Thesis, Information and Communication Technology, Grimstad – Norway

Sanders, G, Thorens, L., Reisky, M., Rulik, O. , Deylitz, S. (2003), "GPRS Networks", John Wiley & Sons, 17-40, 87-106

Schafer,G., (2000), "Placement of Intelligence Within Networks to Provide Corporate VPN Services", Elsevier, Information Security Technical Report, vol 6, No 1

Schneier, B.,( 1994), “Applied Cryptography”, John Wiley & Sons, Section 8.6, New York, NY,

Seurre, E., Savelli, P., Pietri, J.P.,(2003), “GPRS for Mobile Internet”, Artech House

Shneyderman, A.,(2000), “Mobile VPNs for Next Generation GPRS and UMTS Networks”, Lucent Technologies White Paper

Sicher, A, (2002), “GPRS Technology Overview”, Dell Computer Corporation

Spirent Communications, (2004), “Three Hidden Dangers of GPRS Deployment and How to Avoid Them”, Spirent Communications, Inc., Calabasas, USA

Steele, R., Gould, P., (2001) “GSM, cdmaOne and 3G Systems”, John Wiley & Sons Ltd

UMTS Forum (1997), “A Regulatory Framework For UMTS”, Report No:1, s12.

Walker, M., (2000), “On the Security of 3GPP Networks”, Vadafone Air Touch & Royal Holloway, University of London

Weber, M., Redl, S., Oliphant,M., (1998),“GSM and Personal Communications Handbook”, Artech House

Whitehouse, O., (2002), “GPRS Wireless Security: Not Ready For Prime Time” Atstake Inc., Research Report

Whitehouse, O., Murphy, G., (2004), “Attacks and Counter Measures in 2.5G and 3G Cellular IP Networks” Atstake Inc., Research Report

Xenakis, C., Gazis, E., Merakos, L.,(2001), “Secure VPN Deployment in GPRS Mobile Networks” Communication Networks Laboratory, Department of Informatics & Telecommunications, University of Athens

Xenakis, C., Merakos,L.,(2002), “On Demand Network-wide VPN Deployment in GPRS”, University of Athens

Yi-Bing Lin, Herman C., Rao, H., Imrich C., (2001), “Wireless and Mobile Network Architectures”, John Wiley and Sons

Yousef, P., (2004), “GSM-Security: a Survey and Evaluation of the Current Situation”, Master’s thesis, Linköping Institute of Technology

**INTERNET KAYNAKLARI**

**[1]**GSM Association, “What is General Packet Radio Service”, http://www.gsmworld.com/technology/gprs/intro.shtml

**[2]**GSM Supplier Association, GSM/3G statistics, http://www.gsacom.com/news/statistics.php4

**[3]** GSM siteminin gelişimi, http://www.symbiandev.net/node/3

**[4]**OpenGGSN, SGSNEMU, http://www.openggsn.org

**[5]**Stallings, W., “IPV6 : the new Internet Protocol” http://www.cs-ipv6.lancs.ac.uk/ipv6/documents/papers/stallings/

**[6]**Telekomunikasyon Kurumu, "Türkiye İçin Genişbantta Yeni Teknolojiler (3G)", http://www.tk.gov.tr/Etkinlikler/Ulusal_Etkinlikler/Toplantilar/3g.htm

## EK 1 ERICSSON GPRS ŞEBEKESİ TEST RAPORU

Bu bölümde Ericsson Mobility World GPRS şebekesinde uygulanmış olan test adımları ve sonuçları verilmiştir.

İÇİNDEKİLER Sayfa

## ŞEKİLLER

## 16. Test Adımları Özet Tablosu

| Test Numarası | Test Adımı | Test Sonucu |
|---|---|---|
| 1 | GPRS Şebekesi Güvenlik Politikası Dokümanı Testi | **KALDI** |
| 2 | GPRS Şebekesi Konfigürasyonu ve Çalışma Esasları Dokümanı Testi | GEÇTİ |
| 3 | Gi Bant Genişliği Testi | N/A |
| 4 | Gizlilik ve Bütünlük Test Adımı | **KALDI** |
| 5 | Aboneler Arası Saldırı Testi | **KALDI** |
| 6 | İnternet Üzerinden Saldırı Testi | GEÇTİ |
| 7 | GPRS Omurgası Bileşenleri Açıklıkları Testi | **KALDI** |
| 8 | Abone IP Adreslerinin Dağıtımı (NAT kullanımı) Testi | GEÇTİ |
| 9 | Güvenlik Duvarı ve Geçit Cihazları Testi | GEÇTİ |
| 10 | Abone IP adreslerinden SGSN ve GGSN Sistemlerine Erişim Testi | GEÇTİ |
| 11 | SGSN ve GGSN Düğümleri Erişim Kontrol Listeleri Testi | **KALDI** |
| 12 | GTP PDP İçerik Silme ve İçerik Güncelleme Engelleme Test Adımı | N/A |

N/A: Test adımının uygulanabilir olmadığını göstermektedir.

# 17. GPRS Şebekesi Güvenlik Testleri

## 17.1 GPRS Şebekesi Güvenlik Politikası Dokümanı Testi

Güvenlik gereksinimi olan sistemlerde güvenlik politikası dokümanı bulunmalı ve işletilmelidir. Politikada aşağıda belirtilen konular açık olarak belirtilmelidir.

10. Korunması gereken varlıkların neler olduğu,
11. Kimlerden korunması gerektiği,
12. Varlıkların hangi yöntemler kullanılarak korunacağı,
13. Güvenlik ile ilgili sorumluların kimler olduğu,
14. Güvenlik kayıtlarının nasıl ve kimler tarafından inceleneceği,
15. Acil durumlarda nasıl hareket edileceği,
16. Güvenlik olayları sonucunda nasıl değerlendirme yapılacağı,
17. Politikanın sahibinin kim olduğu.
18. Roaming anlaşması yapılan operatörler ile yapılan sözleşmenin içeriğinde dikkat edilmesi gereken hususların neler olduğu

### 17.1.1 Test Yöntemi

GPRS şebekesinin güvenlik politikası olup olmadığına, eğer varsa yukarıda belirtilen hususların belirtilip belirtilmediğine bakılacaktır.

### 17.1.2 Beklenen Sonuç

GPRS şebekesinin bir güvenlik politikası olmalı ve işletilmelidir. İçeriğinde yukarıda belirtilen hususların bulunması gereklidir.

### 17.1.3 Alınan Sonuç

GPRS şebekesinin yetkilileri ile yapılan görüşmeler sonucunda şebekenin işletimine dair bir güvenlik politikası bulunmadığı saptanmıştır.

### 17.1.4 Karar

GPRS güvenlik politikasının bulunmaması nedeni ile GPRS şebekesi test adımından **KALDI**.

## 17.2 GPRS Şebekesi Konfigürasyonu ve Çalışma Esasları Dokümanı Testi

GPRS şebekesinin düzgün işletilebilmesi ve görev değişikliklerinden sistemin etkilenmemesi amacı ile GPRS şebekesinin çalışmasına dair esasların belirtildiği bir doküman bulunmalıdır. Bu dokümanın en az aşağıdaki bilgileri içermesi beklenmelidir.

9. Şebeke içerisindeki trafiğin akışı,
10. Bileşenlerden sorumlu personelin görevleri ve sorumlulukları,
11. Güvenlik duvarı, geçit cihazı gibi güvenlik bileşenlerinin konfigürasyon bilgileri,
12. GPRS omurgasının IP adres dağılımı,
13. Abonelere verilen IP adreslerinin dağılımı,
14. Sistemin işletimine dair kayıtların izlenme yöntemi,
15. Yeni bileşen ekleme ve çıkarmanın hangi kurallara göre yapılacağı,
16. Konfigürasyon ve çalışma esasları dokümanının güncellenmesine dair hususlar.

### 17.2.1 Test Yöntemi

GPRS şebekesinin konfigürasyon ve çalışma esasları dokümanı olup olmadığına, eğer varsa yukarıda belirtilen hususların belirtilip belirtilmediğine bakılacaktır.

### 17.2.2 Beklenen Sonuç

GPRS şebekesinin konfigürasyon ve çalışma esasları dokümanı olmalı ve işletilmelidir. İçeriğinde yukarıda belirtilen hususların bulunması gereklidir.

### 17.2.3 Alınan Sonuç

GPRS operatörünün yetkilileri ile yapılan görüşmeler sonucunda konfigürasyon ve çalışma esasları dokümanının mevcut olduğu görülmüştür. Doküman içerisinde olması gereken tüm bilgilerin mevcut olduğu tespit edilmiştir.

### 17.2.4 Karar

Şebekenin söz konusu dokümanının bulunması ve doküman içerisinde test adımında belirtilen maddelerin yer alması nedeni ile GPRS şebekesi test adımından **GEÇTİ.**

## 17.3 Gi Bant Genişliği Testi

Şebekenin Gi bant genişliğinin doldurulması durumunda şebeke kullanıcılarına hizmet veremez duruma gelebilmektedir. Bu tür saldırılar genelde servis dışı bırakma saldırıları olarak bilinmektedir ve engellenmeleri oldukça zordur. Karşı önlem olarak, şebekenin internet bağlantısının çoklu yoldan olması tercih edilmelidir.

### 17.3.1 Test Yöntemi

Gi arayüzünden akacak trafiğin birden fazla hat ile desteklenip desteklenmediği sorgulanacaktır. Saldırı durumunda trafiğin aktığı yolların ne şekilde değiştirildiği incelenecektir. GPRS operatörü izin veriyorsa Gi arayüzü IP adresleri öğrenilecek ve Gi arayüzüne doğru trafik oluşturarak bant genişliği doldurulacaktır. Bu esnada şebekenin yanıtı incelenecektir.

### 17.3.2 Beklenen Sonuç

Gi arayüzü bağlantıları çoklu olmalı ve geçiş otomatik olarak yapılmalıdır.

### 17.3.3 Alınan Sonuç

GPRS şebekesinin test amacı ile kullanılması nedeni ile çoklu çıkışa ihtiyaç yoktur. Gi bant genişliğinin doldurulması herhangi bir probleme neden olmamaktadır. Test adımının uygulanmasına gerek yoktur.

### 17.3.4 Karar

Test adımının uygulanmamasına karar verilmiştir.

## 17.4 Gizlilik ve Bütünlük Test Adımı

GPRS şebekesi içerisinde abone verisinin gizlilik ve bütünlüğünün korunması amacı ile herhangi bir koruma yoktur. Abone verisi GPRS omurgasına erişebilen kişiler tarafından görüntülenebilmekte ve istenirse bütünlüğü bozulabilmektedir. Abone verisinin GPRS omurgası boyunca şifreli olarak gönderilmesi tercih edilmelidir.

### 17.4.1 Test Yöntemi

SGSN ve GGSN düğümleri arasında herhangi bir şifreleme tekniği kullanılıp kullanılmadığı incelenecektir. Eğer karşı operatör de destekliyorsa gezgin aboneler içinde şifreleme mümkün olmalıdır.

### 17.4.2 Beklenen Sonuç

SGSN ve GGSN düğümleri arasında şifreli haberleşme olmalıdır.

### 17.4.3 Alınan Sonuç

Ericsson Mobility World GPRS şebekesinin diğer operatörlere doğru Gp arayüzü yoktur (GPRS roaming yapılmamaktadır). Bu sebeple Gp arayüzü şifreleme işlemi kontrol edilmemiştir.

SGSN ve GGSN arasında bulunan Gn arayüzünde yapılan incelemeler sonucunda ise şifreleme yapılmadığı tespit edilmiştir.

### 17.4.4 Karar

SGSN ve GGSN arasında şifreleme yapılmaması nedeni ile test adımından **KALDI.**

## 17.5 Aboneler Arası Saldırı Testi

GPRS şebekesine bağlı olan abonelerin tamamı şebekenin bir parçasıdır ve birbirlerine saldırıda bulunabilir. Abonelerin başka abonelerin mobil istasyonlarının açıklıklarından faydalanarak cihaza girmesi, gizli bilgileri ele geçirmesi, program kurması veya İnternet üzerinden bir indirme işlemi başlatması mümkündür.

### 17.5.1 Test Yöntemi

İki ayrı mobil istasyondan GPRS şebekesine erişilecektir. Bir mobil istasyondan karşı mobil istasyona erişim testi yapılacaktır. Bu testlerden bazıları şunlardır.

4. Karşı mobil istasyona ping konumutu ile ICMP paketleri göndermek.
5. Karşı mobil istasyon için açıklık taraması yapmak.
6. Karşı mobil istasyonun açık TCP port'larını taramak.

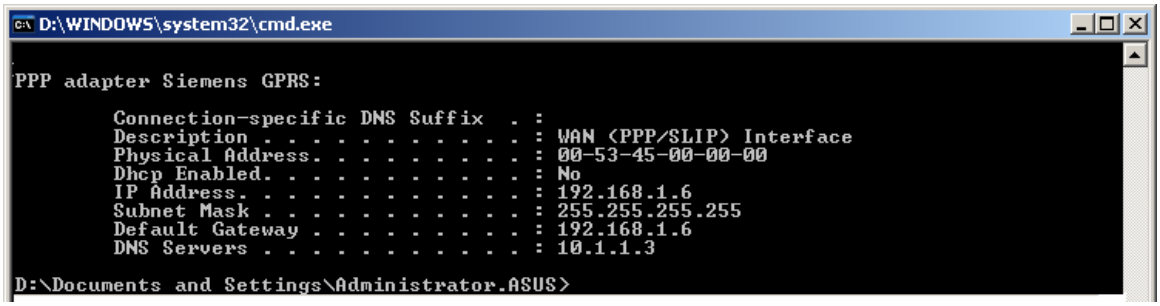
### 17.5.2 Beklenen Sonuç

Ne tür bir erişim testi yapılırsa yapılsın bir mobil istasyondan diğer mobil istasyonlara erişilememelidir.

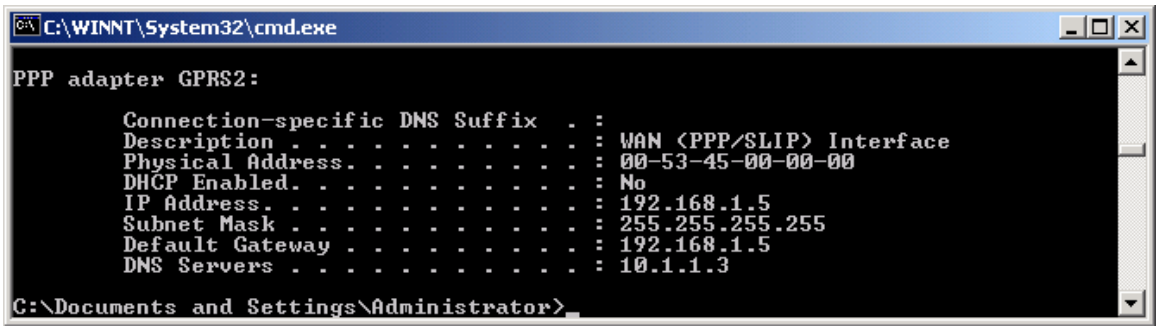
### 17.5.3 Alınan Sonuç

İki adet mobil istasyon kullanılarak GPRS şebekesine erişilmiştir. Şebekeye bağlanan abonelere ait IP adresleri 192.168.1.6 ve 192.168.1.5 olarak tespit edilmiştir (Şekil 17-1)

(Şekil 17-2).

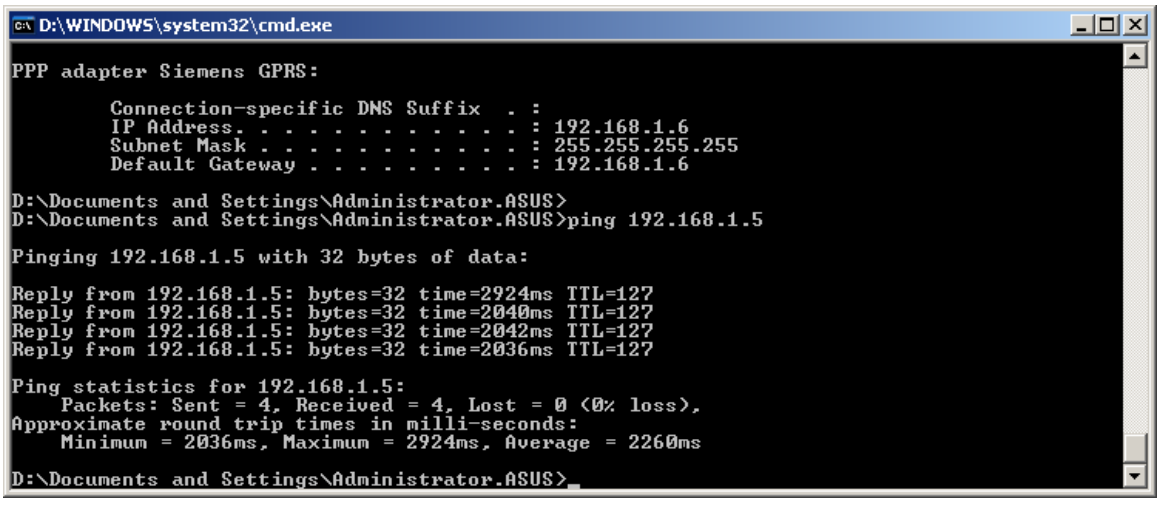



**Şekil 17-1 İlk abonenin IP adresi**




**Şekil 17-2 İkinci abonenin IP adresi**

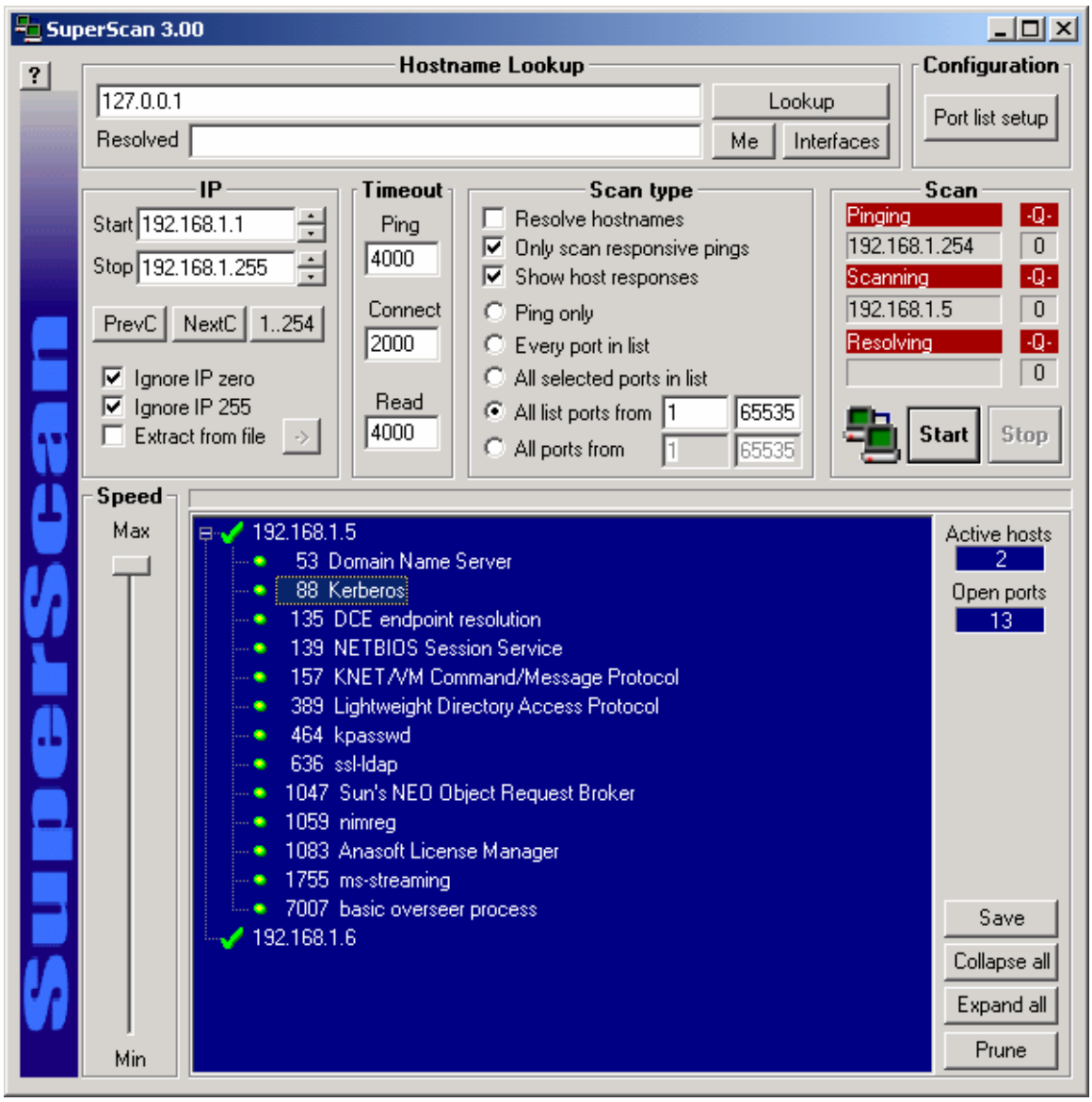
Bir numaralı aboneden (192.168.1.6) iki numaralı abonenin IP adresine (192.168.1.6) ping komutu kullanılarak gönderilen ICMP paketlerine yanıt döndüğü görülmüştür. Bu durum aboneler arası iletişimin engellenmediğini göstermektedir (Şekil 17-3).




**Şekil 17-3 Bir numaralı aboneden iki numaralı aboneye erişim**

ICMP paketleri ile iletişim testi yapıldıktan sonra bir numaralı abone üzerinden SuperScan yazılımı kullanılarak port taraması başlatılmıştır. Tarama sonucunda tarama anında sadece test abonelerinin bulunduğu ve bu abonelerin açık olan portlarının belirlenebildiği görülmüştür

(Şekil 17-4).




**Şekil 17-4 SuperScan tarama sonucu**

Sonuç olarak GPRS şebekesine bağlanan bir abonenin komşu abonelere doğru trafik oluşturarak fazla ücretlendirme saldırısı yapabildiği, port ve açıklık taraması yaparak sistemin açıklıklarını tespit edebildiği tespit edilmiştir.

### 17.5.4 Karar

GPRS şebekesi abonelerinin birbirleri ile arasında iletişim bulunduğu tespit edildiğinden şebeke test adımından **KALDI.**

## 17.6 İnternet Üzerinden Saldırı Testi

GPRS aboneleri şebekeye bağlandıkları anda bir IP adresi almaktadır. Abonelere ait bu IP adreslerine bazı özel uygulamaların getirdiği zorunluluklar haricinde ulaşılamamalıdır. GPRS sisteminde ücretlendirmenin transfer edilen veri miktarı üzerinden olması nedeni ile operatörlerin abonelerini korumak üzere gerekli önlemleri (güvenlik duvarları, erişim kontrol listeleri, geçit cihazları) almış olmalıdır.

### 17.6.1 Test Yöntemi

GPRS abonesi olarak şebekeye bağlanılacaktır. İnternet üzerinden GPRS şebekesinin aboneye vermiş olduğu IP adresine doğru trafik oluşturulacaktır. Abone mobil istasyonu üzerinde çalıştırılacak bir paket dinleme uygulaması ile İnternet üzerinden oluşturulan trafiğin aboneye ulaşıp ulaşmadığı kontrol edilecektir.

### 17.6.2 Beklenen Sonuç

Aboneye kendisinin oluşturduğu bağlantılar haricinde hiçbir suretle trafik akmamalıdır.

### 17.6.3 Alınan Sonuç

GPRS şebekesine iki adet bağlantı kurulmuştur. GPRS şebekesi tarafından tahsis edilen IP adresleri 192.168.1.0 ağından olmuştur. İnternet üzerinde http://www.lawrencegoetz.com/programs/ipinfo/ adresi ziyaret edilerek İnternet tarafından görünen IP adresi tespit edilmiştir. Her iki bağlantı için 213.74.28.139 numaralı IP adresi ile bağlantı kurulduğu gözlenmiştir. İnternet üzerinde http://www.web-geek.com/utils/ping.html sayfasından 213.74.28.139 numaralı IP adresine ICMP paketleri gönderilmiştir ve abonelerin mobil istasyonları üzerinde ağ dinlemesi yapılmıştır. Sonuç olarak İnternet üzerinden gelen trafiğin abonelere ulaşmadığı görülmüştür.

### 17.6.4 Karar

İnternet üzerinden mobil istasyonlara doğru oluşturulan trafiğin mobil istasyonlara ulaşmaması nedeni ile şebeke test adımından **GEÇTİ.**

## 17.7 GPRS Omurgası Bileşenleri Açıklıkları Testi

GPRS omurgasını oluşturan bileşenler (özellikle SGSN ve GGSN) işletim sistemi olan cihazlardır. Bu cihazların kullanmış oldukları işletim sistemlerinden ve ilgili yamaların kurulmamış olmasından kaynaklanan açıklıklar olabilmektedir. Bir saldırgan işletim sistemi açıklıklarından faydalanarak sistemlere girebilir, abone verisini kesme, dinleme, yönlendirme ve bozma gibi faaliyetlerde bulunabilir.

### 17.7.1 Test Yöntemi

En son açıklıklarında yüklü olduğu bir açıklık tarayıcısı kullanılarak sistemler taranacak ve mevcut risk durumu ortaya konacaktır.

Tarama yapılacak IP adresleri aşağıdaki gibidir;

SGSN Gn arayüzü IP adresi 192.168.186.18

GGSN Gn arayüzü IP adresi 192.168.186.19

GGSN Gi arayüzü IP adresi 192.168.186.112

### 17.7.2 Beklenen Sonuç

Hiçbir açıklık bulunamaması veya bulunan açıklıkların risk derecelerinin düşük olması istenen durumdur.

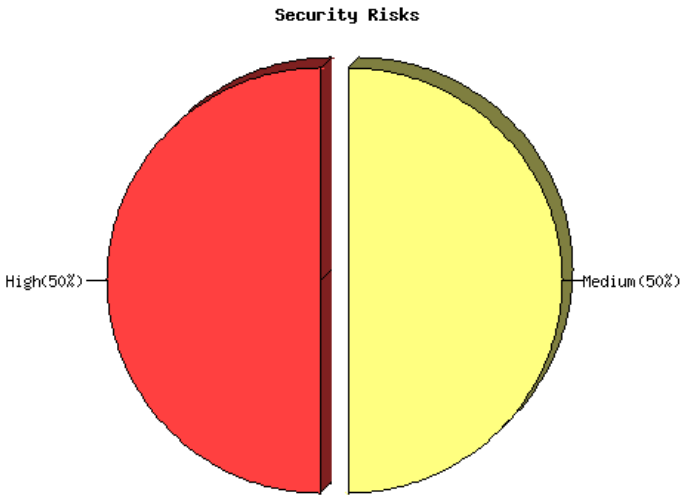
### 17.7.3 Alınan Sonuç

SGSN ve GGSN Gn arayüzlerine aboneye tahsis edilen IP adresleri üzerinden erişilememiştir. Bu arayüzler abone tarafından erişilebildikleri takdirde risk taşımaktadır.

GGSN Gi arayüzüne erişim sağlanmış ve *Nessus Security Scanner* ile güvenlik taraması yapılmıştır. Tarama sonuçlarına göre bir adet güvenlik açığı ve bir adet güvenlik uyarısı tespit edilmiştir.

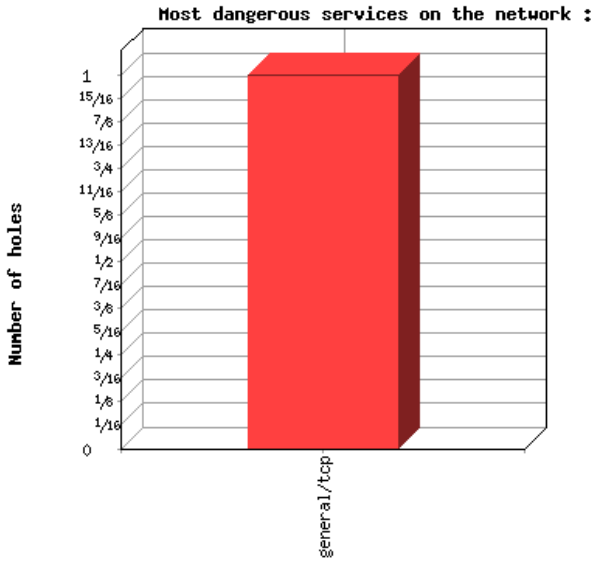
### 17.7.3.1 Nessus Güvenlik Tarayıcısı Sonuçları (Grafik)

Şekil 14-7'te görüldüğü üzere GGSN Gi arayüzü üzerinde bulunan risklerin yarısı yüksek yarısı orta derecede önemlidir.



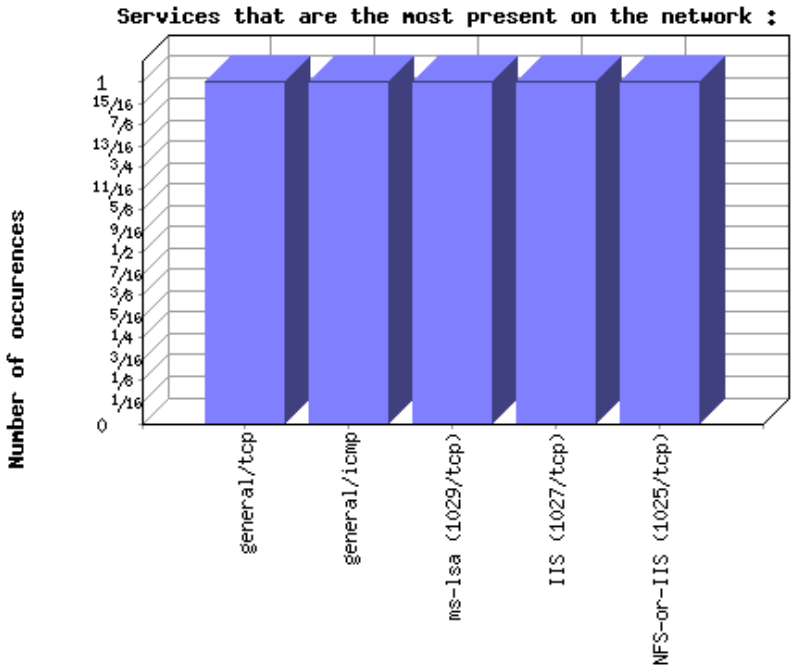

**Şekil 17-5 GGSN Gi arayüzü güvenlik riski**

Arayüz üzerinde bulunan en tehlikeli servis *General/TCP* servisidir.




**Şekil 17-6 GGSN Gi arayüzü üzerinde bulunan en tehlikeli servis**

GGSN Gi arayüzü üzerinde çalışan servisler Şekil 17-7'de görünmektedir.




**Şekil 17-7 GGSN Gi arayüzü üzerinde bulunan servisler**

### 17.7.3.2 Nessus Güvenlik Tarayıcısı Sonuçları (Yazılı)

Tarayıcı tarafından bulunan açık portlar:

- NFS-or-IIS (1025/tcp)
- IIS (1027/tcp)
- ms-lsa (1029/tcp)
- general/icmp (Güvenlik uyarısı bulundu)
- general/tcp (Güvenlik açığı bulundu)

**General/icmp için bulunan güvenlik uyarısı**

Test edilen sistem ICMP zaman damgası isteklerine yanıt vermiştir. Bu durum bir saldırganın test edilen sistemin saat bilgisini öğrenebileceği anlamına gelmektedir.

**Uyarı:** Saldırgan zaman bilgisini kullanarak doğrulama protokollerinin çalışmasını sekteye uğratacak hareketlerde bulunabilir.

**Çözüm:** ICMP zaman damgası istekleri (port numarası 13) ve ICMP zaman damgası yanıtları (port numarası 14) kısıtlanmalıdır. Ayrıntılı bilgi için RFC 867'e başvurulabilir.

**Risk Faktörü:** Düşük

**General/tcp için bulunan güvenlik açığı**

Test edilen sistem tahmin edilebilir TCP sıra numaraları kullanmaktadır.

**Uyarı:** Saldırgan bu açıklığı kullanarak taklit TCP (spoofed TCP) bağlantısı kurabilir.

**Çözüm:** Test edilen sistemin üreticisi tarafından güvenlik yamasının çıkarılıp çıkarılmadığı kontrol edilmeli, eğer çıkarıldıysa sistemin üzerine uygulanmalıdır.

**Risk Faktörü:** Yüksek

### 17.7.4 Karar

GGSN düğümü üzerinde yüksek risk taşıyan bir açıklık bulunması nedeni ile GPRS şebekesi test adımından **KALDI.**

## 17.8 Abone IP Adreslerinin Dağıtımı (NAT kullanımı) Testi

GPRS şebekelerine dağıtılan IP adreslerini İnternet'ten izole etmek amacı ile özel kullanım için ayrılmış 192.168.0.0, 172.16.0.0 veya 10.0.0.0 adreslerinden dağıtım yapılması uygundur. Bu adresler internet üzerinde kullanılmayan adreslerdir ve İnternet bağlantısı için bir adres çevrimi gerektirir. Bu adres çevrimi ağ adresi çevrimi (NAT) olarak adlandırılmaktadır. NAT tekniğinde bire bir eşleme mantığı kullanılmamalı özel IP ye sahip aboneler bir veya birkaç IP üzerinden internete çıkarılmalıdır.

### 17.8.1 Test Yöntemi

GPRS şebekesine bağlanılacak ve tahsis edilen IP adresinin yukarıda belirtilen adres gruplarından olup olmadığı kontrol edilecektir.

### 17.8.2 Beklenen Sonuç

GPRS şebekesine bağlanıldığında tahsis edilen IP adresi özel kullanım için ayrılmış IP adreslerinden olmalıdır.

### 17.8.3 Alınan Sonuç

İki adet mobil istasyon ile GPRS şebekesine bağlantı kurulmuştur. Tahsis edilen IP adreslerinin 192.168.1.0 ağından olduğu görülmüştür. GPRS omurgası için kullanılan IP adres bloğu ise 192.168.186.0 ağındandır.

### 17.8.4 Karar

GPRS şebekesinde kullanılan IP adreslerinin ve abonelere dağıtılan IP adreslerin özel

kullanım için ayrılmış gruptan olması nedeni ile test adımından **GEÇTİ.**

## 17.9 Güvenlik Duvarı ve Geçit Cihazları Testi

Aboneler arası trafiği, aboneler tarafından başlatılmamış (İnternet üzerinden veya diğer operatörlerin şebekelerinden gelen) trafiği filtreleyen bileşenler GPRS şebekesine eklenmiş olmalıdır.

### 17.9.1 Test Yöntemi

GPRS şebekesinin İnternet ve diğer GPRS şebekelerine olan bağlantı uçlarında trafik filtreleme amacı ile güvenlik duvarı bulunup bulunmadığına bakılacaktır. Ayrıca GPRS şebekeleri arasında geçit cihazı kullanıp kullanılmadığı, eğer kullanılıyorsa şifreleme yapılıp yapılmadığı incelenecektir.

### 17.9.2 Beklenen Sonuç

İnternet trafiğini filtreleyen güvenlik duvarı, diğer GPRS şebekeleri ile iletişimi düzenleyen ve şifreleyen geçit cihazı bulunmalıdır.

### 17.9.3 Alınan Sonuç

GPRS şebekesinin Gp arayüzü bulunmaması nedeni ile diğer operatörlere gelen giden trafiği düzenleyen bir güvenlik duvarına ihtiyaç yoktur. GPRS şebekesinin internet bağlantısını düzenleyen bir güvenlik duvarı bulunmaktadır.

### 17.9.4 Karar

Uygun olan noktalarda güvenlik duvarlarının bulunduğu tespit edildiğinden test adımından **GEÇTİ.**

## 17.10 Abone IP adreslerinden SGSN ve GGSN Sistemlerine Erişim Testi

Abonelere tahsis edilen IP adresleri ile GPRS omurgasında kullanılan IP adresleri farklı IP adres uzaylarında olmalı ve bu uzaylar arasında iletişim bulunmamalıdır.

### 17.10.1Test Yöntemi

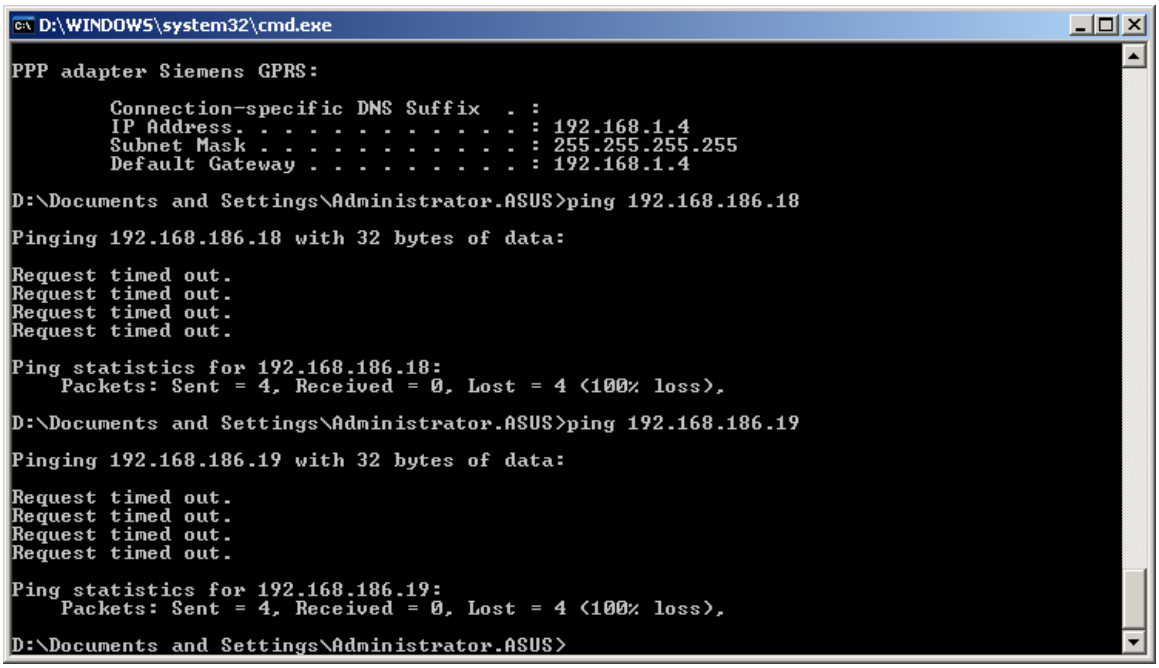
GPRS şebekesine bağlanılacak ve aboneye tahsis edilen IP adresinde SGSN ve GGSN cihazlarına ulaşılmaya çalışılacaktır. En basit anlamda ping, telnet ve ssh komutları ile erişim olup olmadığı test edilecektir.

### 17.10.2Beklenen Sonuç

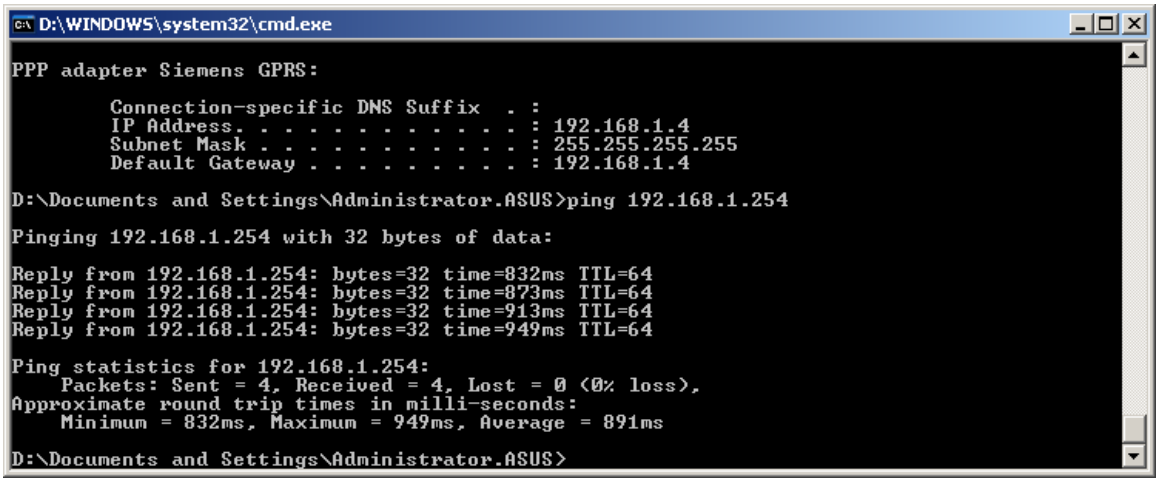
Abone IP adreslerinden GPRS omurgasında bulunan cihazlara erişim bulunmamalıdır.

### 17.10.3Alınan Sonuç

Abone IP adreslerinden (192.168.1.0) SGSN ve GGSN düğümlerine (192.168.186.18-19) erişilemediği görülmüştür (Şekil 17-8). Aynı anda GGSN Gi arayüzüne erişilebilmiştir (Şekil 17-9). Bu sebeple 192.168.1.0 ağı ile 192.168.186.0 ağı arasında yönlendirme bulunmamaktadır.




**Şekil 17-8 SGSN ve GGSN düğümlerinin Gn ara yüzlerine erişim**




**Şekil 17-9 GGSN Gi arayüzü erişimi**

#### 17.10.4Karar

Abone IP adreslerinden GPRS şebekesinin omurgasında bulunan düğümlere erişimin bulunmadığı tespit edildiğinden test adımından **GEÇTİ.**

### 17.11 SGSN ve GGSN Düğümleri Erişim Kontrol Listeleri Testi

Saldırganlar tarafından GPRS şebekesine taklit SGSN ve GGSN düğümleri eklenerek ücretsiz internet bağlantısı sağlamak mümkündür. Bu sebeple SGSN ve GGSN düğümleri üzerinde haberleşecekleri düğümlere ait adres bilgilerinden oluşan erişim kontrol listeleri bulunmalıdır. Bu sayede GPRS omurgasını oluşturan düğümler birbirleri ile haberleşecek fakat saldırganlar tarafından sisteme eklenebilecek taklit SGSN ve GGSN düğümleri asıl düğümler ile haberleşemeyecektir.

#### 17.11.1Test Yöntemi

SGSN ve GGSN düğümleri üzerinde erişim kontrol listesi bulunup bulunmadığına, eğer varsa düğümlere ait IP adreslerin işlenip işlenmediğine bakılacaktır.

#### 17.11.2Beklenen Sonuç

SGSN ve GGSN düğümleri üzerinde erişim kontrol listeleri bulunmalı ve ilgili IP adresleri işlenmiş olmalıdır.

#### 17.11.3Alınan Sonuç

Yapılan incelemeler sonucunda SGSN ve GGSN düğümleri üzerinde erişim kontrol listesi bulunmadığı tespit edilmiştir.

#### 17.11.4Karar

SGSN ve GGSN düğümleri üzerinde erişim kontrol listesi bulunmaması nedeni ile test adımından **KALDI.**

### 17.12 GTP PDP İçerik Silme ve İçerik Güncelleme Engelleme Test Adımı

SGSN ve GGSN düğümleri arasında GTP protokolü kullanılarak haberleşme sağlanmaktadır. Her bir abone oturumu için bir PDP içerik etkinleştirmesi yapılarak tünel kurulmaktadır. Bir saldırgan GTP PDP içerik silme mesajı göndererek abone oturumunu kesebilmekte veya içerik güncelleme mesajı göndererek abone oturumunu çalabilmektedir. Bu problem GTP protokolünün doğasından kaynaklanmaktadır. Önlem olarak düğümler arasında IPSec

protokolü tünel modunda kullanılarak PDP mesajları şifrelenmeli, şifresiz mesajlar kabul edilmemelidir. Düğümler arasında IPSec protokolü ile şifreleme yapılması aynı zamanda abone verisinin gizlilik ve bütünlüğünü de koruyacaktır.

### 17.12.1Test Yöntemi

SGSN ve GGSN düğümleri arasında IPSec protokolü ile şifreleme yapılıp yapılmadığı incelenecektir.

### 17.12.2Beklenen Sonuç

SGSN ve GGSN düğümleri arasında IPSec protokolü ile şifreleme olmalıdır.

### 17.12.3Alınan Sonuç

SGSN ve GGSN düğümlerinin tek bir düğümde toplanması nedeni ile Gn arayüzüne erişmek ve IP paketleri göndermek mümkün değildir. Bu sebeple arada akan trafiğin şifreli olup olmamasının bu test adımı için bir önemi yoktur.

### 17.12.4Karar

Hizmet düğümlerinin tek bir cihazda toplanması nedeni ile test adımı uygulanmamıştır.

## ÖZGEÇMİŞ

| | | |
|---|---|---|
| Doğum tarihi | 04.03.1979 | |
| Doğum yeri | Tekirdağ | |
| Lise | 1991-1996 | Tuzla Teknik Lisesi – Elektronik Bölümü |
| Lisans | 1996-2001 | İstanbul Teknik Üniversitesi<br>Elektrik ve Elektronik Fakültesi<br>Elektronik ve Haberleşme Mühendisliği Bölümü |

**Çalıştığı kurum(lar)**

| | |
|---|---|
| 2001-2003 | SPD İletişim Sistemleri A.Ş. – Teknik Danışman |
| 2003-Devam ediyor | Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Araştırmacı |