

MOBİL TELEKOM SEKTÖRÜNDE GÜVENLİK ÇÖZÜMLERİ

Adem Karahoca¹, Talat Fırlar²

¹Bahçeşehir Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü 34538 Bahçeşehir-İstanbul

²İstanbul Üniversitesi Teknik Bilimler M.Y.O. Avcılar –İstanbul

ABSTRACT

Mobile telecommunication industry is in a radical development process in today's world. In this process, an increase in the services which are based on data for mobile users are more anticipated than the voice communication systems. Effective security solutions must be provided as soon as possible to continue the success of this industry. A secure environment should be obtained for the mobile network systems, application providers and subscriptions in order to allow them to perform operations.

According to the Nokia, there are approximately 300 third-generation mobile networks and each of them has at least 1000 access nodes with one billion subscribers in the mobile telecommunication industry. These wide area networks are going to be IP based systems so secure environments must be established which includes the functions of verification, warning and tracing.

In this article, security solutions of second and third generation mobile technologies are generally explained for mobile groups. Also the writer deals with the security problems and solutions in the parallel of the great experiences which were gained while working in a GSM operator in Turkey.

Key Words - GSM, Security

ÖNSÖZ

Mobil telekomünikasyon endüstrisi, radikal dönüşüm sürecindedir. Bu süreçte, ses iletişiminden çok, mobil kullanıcılar için veriye dayalı servislerin artırılması öngörülmektedir. Endüstrinin başarısının devamı için, etkili güvenlik çözümlerine ihtiyaç vardır. Mobil ağların, uygulama sağlayıcıların ve abonelerin güvenli bir biçimde işlemlerini yapabilmelerini sağlamak için güvenilir ortamlar oluşturmak gerekmektedir.

Mobil telekom endüstrisinde, 300 tane üçüncü-kuşak mobil ağdan, her birinde en az 1000 erişim düğümünden ve 1 milyar aboneden bahsedilmektedir. (kaynak: Nokia) bu çok geniş ağlar, IP tabanlı olacak ve bu yüzden doğrulama, uyarı, izleme ve takip etme fonksiyonlarının içerileceği güvenlik ortamlarının kurulması gerekmektedir.

Bu makalede, mobil topluluklar için, ikinci, 2 ½. ve üçüncü kuşak mobil teknolojilerin güvenlik çözümleri üzerinde durulmaktadır. Yazarlar, Türkiye'deki bir GSM operatöründeki deneyimlerinden yol çıkarak güvenlik açıkları ve çözümlerini ele almaktadırlar.

Anahtar Kelimeler- GSM, Security

1. GİRİŞ

Mobil telekom sektörü, ikinci kuşak teknolojiye, IP tabanlı üçüncü kuşak teknolojilere geçiş aşamasındadır. Üçüncü kuşak ağların en önemli özellikleri [1];

- IP tabanlı ağlar sayesinde, hem ses hem de veri iletişimi ile daha çok sayıda ve çeşitte İnternet tabanlı hizmetlere, mobil ortamda olanak sağlayacaklar.
- Çok geniş olacaklar ve bu sayede binlerce ağ, büyük miktarlardaki mobil abonelere hizmet verecektir.

Bugünlerde, 2. kuşak teknolojilerinden WAP(Wireless Application Protocol-Mobil uygulamalar protokolü) ve SMS(short message service-kısa mesaj servisi) teknolojilerinin hayata geçirilmesine rağmen, interaktif İnternet hizmetlerinin birçoğu mobil aboneler tarafından kullanılmamaktadır. Wap ve SMS'teki güvenlik açıkları hala tam olarak çözülemediğinden dolayı, özellikle bankacılık uygulamalarında, bu tür mobil çözümler kısıtlı olarak kullanılabilir. 2 ½. ve 3. kuşak teknolojilerin uygulamaya geçirilmesi ile, birçok yeni servis devreye alınacaktır. Dolayısı ile, daha etkin güvenlik çözümlerine ihtiyaç vardır[2].

Mobil ağ operatörlerinin güvenliği, mobil kullanıcının cihazından, operatörün ağına kadar olan kısmı kapsamaktadır. Uygulamadaki çözümlerde, iletişim havada şifrelenir, fakat, operatörün ağına iletişim şifreli değildir.

Tablo 1. Mobil Teknoloji Kuşakları

<i>Kuşak</i>	<i>Teknoloji</i>	<i>Uygulama Zamanı</i>
2.	GSM,CDMA,TDMA	Sms ve WAP hizmetleri hayatta
2 ½.	GPRS	2001 ilk çeyreğinde uygulandı
3.	UMTS	1. Asya/Pasifik – 2002 1. Çeyreğinde uygulandı
		2. Avrupa – 2004 1. Çeyreğinde uygulanacak
		3. ABD – 2006 1. Çeyrekte uygulanacak

Veri iletişimde güvenlik, sadece ağ operatörü ve aboneyi değil, aynı zamanda, uygulama sağlayıcıyı da kapsamaktadır.

2. İKİNCİ KUŞAK AĞLAR

İkinci kuşak ağlarda, aboneler, internet erişimlerini, aynı zamanda internet sağlayıcı konumundaki mobil servis sağlayıcılardan, yani gsm operatörlerinden sağlamaktadırlar. İnternet'e bağlandıktan sonra aboneler, kurumsal veya ticari WAP servislerinden hizmet alabilirler. SMS, mobil ağ operatöründen doğrudan kullanılabilir bir hizmettir. İkinci kuşak ağlardaki güvenlik konuları şunlardır:

- Kurumdan, operatöre bağlanmak için kullanılan hattın güvenliği,
- WAP ve SMS için, güvenilir erişim ve kısıtlanmış erişim.

WAP, genellikle IP üzerinden uygulanır; fakat, SMS bir IP servisi değildir. Standart, VPN(virtual private Networks-sanal özel ağ)/Firewall(Ateş duvarı) çözümleri kurumdan operatöre giden hatlarda güvenilir veri aktarımı için uygulanabilir. Hem kurumsal hem de ticari WAP servis sağlayıcıları, aşağıdaki şartları sağlamalıdır.

1. Servisin sadece yetkilendirilmiş kullanıcılar tarafından kullanılmasını sağlamak,
2. Kullanıcıların veriye erişimlerini kısıtlamak.

2.1. Mobil Uygulama Protokolü(WAP)

Mobil uygulama protokolü, mobil cihazlarda, mobil bilginin sunulması ve teslim edilmesi için kullanılan standarttır[3]. WAP genellikle, IP servisi olarak uygulanır ve mobil cihazlar için web gezgini aracılığı ile bilgi edinimini mümkün kılar. WAP kullanıcıları, İnternet'e bağlı olmalıdırlar ve bu yüzden hem internette hem de abonelerden gelecek tehditlere açık durumdadırlar.

Şekil 1, kurumsal bilginin bir WAP hattı boyunca, güvenilir bir biçimde, nasıl taşınacağını göstermektedir.

- (1) VPN/ Firewall'da kullanıcı bilgisi, VPN/Firewall Modülünden alınır ve web sunucusu kullanılabilir hale getirilir.
- (2) VPN/ Firewall'da ise, WAP geçidi korunmaktadır. Burada ateş duvarı uygulanmazsa, WAP geçidi ile kurumsal geçit SSL kullanılarak şifrelenebilir. WAP geçidi bir VPN/Firewall modülü ile korunursa;
 - a. Mobil kullanıcıya abonenin giriş bilgisi, HTTP'den açılarak, ya da kullanıcıdan erişim bilgileri tekrar istenerek, güvenilir giriş sağlanabilir.
 - b. Bağlantıyı özelleştirmek için, WAP geçidi ve kurumsal geçit arasında bir VPN kurulur.

2.1.1. Güvenilir SMS Veri Akışı

Şekil 2’de, kurumsal verinin güvenilir bir biçimde, bir mobil cihaza iletilebilmesi gösterilmektedir. Kurumsal web sunucusu ile uygulama sağlayıcı arasında bir sanal özel ağ yapılandırılmalıdır. Bir uygulama, (SMS-C’nin yanındaki uygulama sunucuda, kurumsal ağ dışındaki) IP Protokolüne (HTTP veya SMTP) gömülmüş SMS mesajı VPN aracılığı ile güvenilir hale getirilir.

3. 2 ½. KUŞAK YÜKSEK HIZLI VERİ AĞLARI

2 ½. kuşak, 3. kuşak ağların evrimine bir geçiş oluşturmaktadır. 2 ½. kuşakta, 2. kuşak alt yapısından ses iletimi aynı kalmaktadır ve IP tabanlı veri ağı, 2. kuşak ağ içerisinde uygulanmaktadır. Mobil ağ, Internet servis sağlayıcı konumuna gelmektedir ve 2 ½. kuşak GPRS(General Packet Radio Service-Genel Paketlemeli Radyo Servisi) servisi “her zaman bağlı kal” ortamını GPRS’i destekleyen GSM telefonları için sağlamaktadır. GPRS European Telecommunication Standards Institute(ETSI) tarafından geliştirilmiştir. Standartlaştırma çalışmaları 1993’de başlamış ve spesifikasyon faz 1 için tamamlanmıştır, fakat, birçok küçük değişiklik beklenmektedir. GPRS, veri transferini ileriye götürmek ve büyük miktarlardaki veriyi iletmek için tasarlanmış bir teknolojidir. GPRS, bir GSM hizmeti olarak ele alınmaktadır ve kendine has bir öz ağı olmasına rağmen, radyo ağı GPRS ve GSM öz ağları arasında paylaşılmaktadır. Ek olarak, GSM, GPRS öz ağından faydalanarak daha iyi performans ile birlikte veriye bağlı GSM hizmetleri vermek için uygundur. Ancak, herhangi bir GSM ağında bağlamaksızın bir GPRS ağı oluşturmak mümkündür. Bu durumda GPRS ağı kendi radyo ağına sahip olmalıdır.

Şekil 3’deki ağ konfigürasyonunda, mobil cihazdan Internet’e bağlantı kurulmaktadır[4].

1. Bir abone SGSN’e bağlanır,
2. SGSN bir GTP(GPRS Tünel Protokolü) açar GGSN’e bağlanır,
3. Mobil cihaz için bir IP adresini GGSN tahsis eder,
4. Bağlantı, GTP tüneli üzerinden kurulur.

3.1. Güvenlik Konuları

1. Mobil operatörün ağını, Internetten ve diğer mobil operatörlerden korumak,
2. Bir abone tabanlı politika sağlamak,
3. Farklı ara yüzlerden(Gn,Gi) veri bağlantısını korumak,
4. GGSN’ler ve kurumsal geçitler arasında VPN’ler oluşturmak.

3.1.1. IP Adresi Yönetimi

IP Adresi Yönetimi, GPRS ağlarında ilave bir konudur:

1. IP adreslerinin sınırlı sayıda olmasından dolayı, IP adresi tahsis mekanizmasının bir havuz kullanılarak sağlanması gerekmektedir,
2. Dolaşım – Mobil telefonlar bir hücreden diğerine veya bir mobil operatörün ağından diğerine geçerlerken, yeni bir IP adresine ihtiyaç duyarlar (mikro mobiliti ve makro mobiliti)

3.2. Güvenlik Çözümleri**3.2.1. Mobil Ağ Korumak**

Mobil veri ağı IP tabanlıdır ve internetten gelebilecek tüm saldırılara ve herhangi bir kurumsal ağdan gelecek tehditlere de açıktır. Mobil ağ, her erişim düğümünde (GSNler) korunmalıdır.

1. Abonenin GSM telefonuna bağlantıları,
2. Diğer mobil ağların bağlantıları,
3. Internet

Geleneksel mobil ağlar, çok büyük olduklarından, büyük operatörlerde binlerce SGSN oluşturmak zorundadırlar

3.2.2. Abone Tabanlı Güvenlik Politikası

VPN ve Firewall, ağ operatörlerinin abone tabanlı bir Güvenlik Politikasını, erişim düğümlerinde (GGSN’lerde) uygulamaya olanak sağlamaktadır. Abonenin erişimi, mobil ağın güvenlik politikasında bir konudur ve aboneler, mesela mobil virüs saldırılarından korunmaktadır.

3.2.3. Veri Bağlantısının Korunması

Sadece ağı değil, fakat; aynı zamanda veri iletişimi de korunmalıdır. VPN teknolojisi, iletişimin kişiye özel olmasını, erişimini ve güvenliğini mobil ağ boyunca korumaktadır.

Hava bağlantısı, mobil ağ teknolojisi standartları ile şifrelenir ve iletişim, baz istasyonunda şifre açılarak tamamlanır. VPN/Firewall ikilisi ilk olarak GSN’den başlanarak güvenliği sağlar. Bu, VPN, GSN ve kurumsal geçit arasındadır. Verinin şifrelenmesinin gerektiği bölgeler;

1. Mobil operatörün ağında (SGSN-GGSN)
2. Internet’te (GGSN-Internet)
3. Mobil operatör ağları arasında (BG-BG)

3.3. Uygulama Senaryoları

Bu bölüm aşağıdaki uygulama senaryolarının örneklerini sunmaktadır:

1. Saydam Internet Erişimi,
2. Kurumsal VPN,
3. Dolaşım VPN’leri,
4. Abone tabanlı izleme,

3.3.1. Saydam İnternet Erişimi

Şekil 4’de, abonelerin internet erişiminin, hem GPRS’den hem de İnternet abonelerinin saldırılarından korunmasını sağlayan bir konfigürasyonu göstermektedir. VPN/Firewall modülleri, GPRS ağındaki her GSN’ye yüklenir.

Bu konfigürasyonda, İnternet ve diğer GPRS ağları (GGSN-BG) arasında VPN’e ihtiyaç vardır. SGSN-GGSN hattında (GPRS ağındadır), VPN seçimlidir ve özelleştirmenin yanı sıra, servis kalitesini de sağlamaktadır.

3.3.2. Kurumsal VPN

Şekil 5’de, kurumsal veri (kurumsal VPN ve Firewall modülüyle şifrelenir) internette şifrelenmiş olarak iletilir. VPRN, SGSN-GGSN hattında VPN seçimlidir.

3.3.3. Dolaşım VPN’leri

Şekil 6’daki konfigürasyonda, mobil cihaz dolaşımında olsa bile, VPN’lerin mobil cihaza sağlanan kurumsal verinin güvenliğini sağladığı görülmektedir[5].

Şekil 6’daki konfigürasyonda çok sayıda ekstranetin yönetimini sağlayacak bir çözüme ihtiyaç vardır.

3.3.4. Abone Tabanlı Engelleme

Şekil 7’deki konfigürasyonda, abonenin erişimi, her bir aboneye dayandırılarak kontrol edilmektedir. Web içeriği, ağ operatörlerinin web sunucularına gönderilmekte ve içeriğe erişim, bireysel abonelere hizmet, abone oldukları servisler göre sağlanmaktadır.

GPRS abonesi, bireysel olarak GPRS IP ağına uzaktan doğrulamalı, kullanıcı servisi (RADIUS) aracılığı ile bağlanarak IP havuzundan bir IP alır ve ağa bağlanır. GPRS destek düğümüne eriştikten ve ateş duvarını aştıktan sonra uygulama web sunucularına erişebilir[6].

4. 3. KUŞAK MOBİL AĞLAR

3. Kuşak Mobil ağlarda, hem ses hem de veri IP tabanlı olabilecektir. Korkunç sayıda mobil telefon sayısından dolayı, her cihazın bir IP adresine ihtiyaç duyulacaktır. Bundan dolayı da, 3. kuşak ağlarda hem IPv6 hem de geleneksel IPv4 adresleme kullanılacaktır[6,7,8].

3. kuşaktaki bazı güvenlik konuları, 2 ½. Kuşaktakiler ile benzerlik göstermektedir:

- Mobil operatörün ağının İnternette ve de diğer mobil ağlardan korunması,
- Abone tabanlı bir politikanın uygulanabilmesi,
- Farklı ara yüzler(Gn,Gi,v.s.) üzerinde veri iletişiminin korunması,
- VPNlerin yaratılması

2 ½. Kuşak güvenlik konularına ek olarak, aşağıdaki güvenlik konuları 3. kuşak ağlardaki konuları daha uygun bir biçimde tanımlamaktadır:

- Üçüncü partilerin güvenilirliği,
 - Katma değerli servislerin daha çok ortaya çıkması ile, 3. partilerden alınacak içeriklerin ve servislerin abonelere sağlanması esnasında, 3. partiler ile abone arasında taşıyıcı rolündeki mobil operatörün çift taraflı güvenlik mekanizmasını devreye sokması gerekmektedir.
- Faturalamada kötüye kullanım,
 - Hem tüketiciler, hem de servis sağlayıcılar dürüst bir şekilde güvenilir bir fiyatlandırma ve ödeme sürecine ihtiyaç duymaktadır.

4.1. Güvenlik Çözümleri

Mobil ağdaki güvenlik sağlanırken, her erişim düğümü (GSNler) korunmalıdır.

- Abonenin cihazına bağlantılar,
- Diğer mobil ağlara bağlantılar,
- İnternet,

5. TEMEL KAVRAMLAR

5.1. Tünel Tabanlı Rota

Mobil operatörler, abonelerine veri servisleri sağlamalarına rağmen, doğrudan bir İnternet bağlantısını sağlamazlar. Bunun iki ana nedeni:

1. İnternet servisi, bir internet servis sağlayıcı tarafından verilmektedir,
2. Abone bir kurumsal müşteridir ve internette çok, kurumsal bir ağa erişmesi gerekmektedir,

Abone veri oturumunu kurarken, GGSN abonenin profiline bağlı olarak erişim noktasını sağlar ve abonenin verisi bir tünel içerisinden, İpsec, L2TP, GRE, özel hat veya MPLS tabanlı VPN protokollerinden birinin yardımı ile iletilir. Bir çok durumda, RADIUS kullanılarak adres havuzundan bir IP adresi, abone için tahsis edilir.

5.1.1. IP Adresi Tahsis Etme Mekanizması

GGSN tabanlı IP adresi havuzunda, her bir GGSN için bir IP havuzu tanımlanır. Böylece GGSN her bir oturum için bir adres ayırır ve oturum sonlandırıldığında IP adresini havuza geri koyar. Havuzdaki IP adresleri;

- İnternette kullanımda olabilir,
- Geçersiz bir adres olabilir, örneğin; 10.x.y.z

Bu metodun içerdiği dezavantaj;

- Yönetimi – Her GGSN için bir havuz oluşturmada basit bir yol gerekir. Ayrıca, iki GGSN’in aynı geçerli adresi kullanmamaları sağlanmalıdır,
- GGSN içersinde spesifik bir kod yazana kadar, hangi kullanıcının hangi IP’yi kullandığı bilgisine erişilemez,
- Bir GGSN için havuzdaki İplerin tükenmekte olduğunu rapor edecek bir yöntem yoktur,

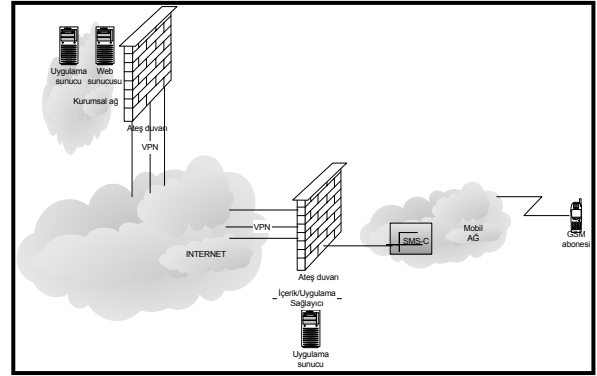
- Yüksek kullanılabilirlik modundaki bir kaç GGSN kullanımı – Bir GGSN devre dışı kaldığında, havuzundaki IP adreslerinin statüsü bilinemez. GGSN kurtarıldığında, bütün kullanıcıların İpleri kaldıkları yerden devam edemezler.

5.1.2. Bir DHCP İstemcisi Olarak GGSN

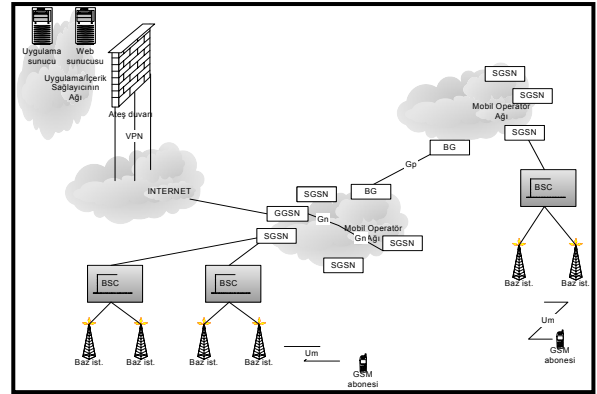
Bu mekanizmada, GGSN (bir DHCP istemcisi veya DHCP Relay gibi) bütün GGSNler için IP adresi havuzunu yöneten bir DHCP sunucusu ile haberleşir. DHCP sunucuları, yukarıda bahsettiğimiz yönetim, GGSN'in devre dışı kalması, IP havuzu yönetimi, DNS üzerinden kullanıcı-IP yayımı gibi konuların çözümleri için kullanılabilir. Adresler tanımlı veya tanımsız olabilir.

6. SONUÇ

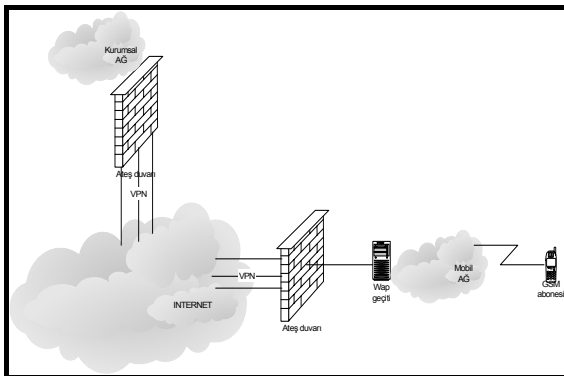
Türkiye'deki bir GSM operatöründe yapmış olduğumuz testlerde, yukarıda belirttiğimiz gibi, çeşitli noktalarda açıklar bulunmaktadır. Özellikle, 2. ve 2½. kuşak ağlardaki alt yapının elverişli olmamasından dolayı, mobil bankacılık uygulamalarında, “parasal işlemlerin yapılması” gerçekleştirilememiştir. Özellikle, mobil-PKI teknolojisinin 3. kuşak ağlarla daha entegre bir şekilde, paketlerin şifrelenerek gönderilebilmesi ve paketlerin mobil operatörün ağında değil, doğrudan mobil telefonda açılabilmesini destekleyen teknolojiler içerebilmesinden dolayı mevcut açıkların kapatılabileceği öngörülmektedir. Havada güvenliğin kısıtlı olması ve Mobil istasyonlardan bant genişliğinin düşük olmasından dolayı GPRS hizmetlerine saldırılar mümkündür. Özellikle, diğer GSM ağlarına bağlanırken kullanılan GTP'den kaynaklanan güvenlik açığı, yukarıda da belirttiğimiz gibi GTP üzerine yerleştirilecek bir ateş duvarı aracılığı ile kontrol edilebilir. Ayrıca, VPN/VLAN tünel bağlantıları kullanarak da haberleşme bilgisinin şifreli iletilmesini sağlayarak güvenlik açıkları en aza indirgenilmektedir.



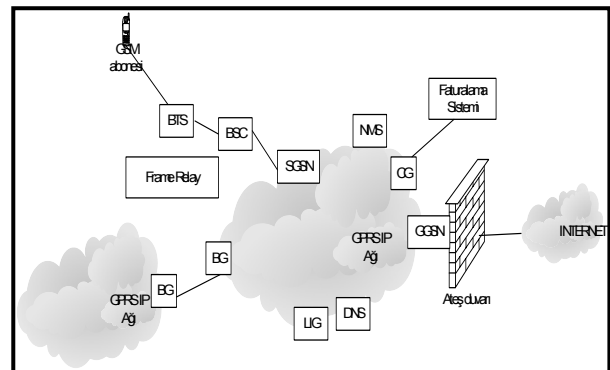
Şekil 2. Güvenilir SMS verisi akışı



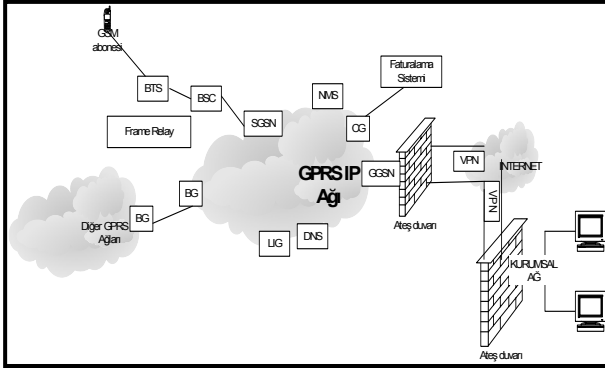
Şekil 3. Tipik Mobil Ağ Konfigurasyonu



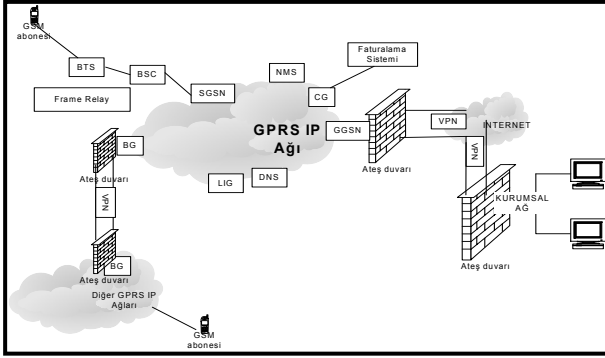
Şekil 1. Mobil Kullanıcılar için WAP'a erişim kontrolü



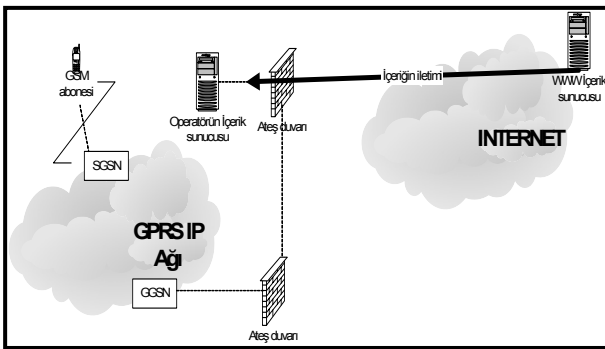
Şekil 4. GPRS ile Saydam İnternet Erişimi



Şekil 5. Kurumsal VPN



Şekil 6. GPRS dolaşım VPN'leri



Şekil 7. GPRS-Abone tabanlı engelleme

EK 1. Mobil ağ teknolojilerinde kullanılmakta olan terimlerin bazıları aşağıdaki gibidir:

Tablo 2. Terimler

AH	Doğrulama başlığı
ANSI	Amerikan Ulusal Standartlar Enstitüsü
APN	Erişim noktası ismi
AuC	Doğrulama merkezi
BG	Sınır geçidi
BLUETOOTH	Kısa mesafeli (10 metre) iletişim standardı
BSC	Baz istasyonu kontrolcüsü
BSS	Baz istasyonu alt sistemi
BTS	Baz iletişim istasyonu
CGSN	Ortak konumlandırılmış GPRS destek düğümü
CIA	Gizlilik, bütünlük ve doğrulama
CKSN	Şifreleme anahtar dizisi sayısı
CS	Devre anahtarlama
DNS	Domain Name System
END-TO-END SECURITY	Şifrelenmiş ve doğrulanmış bir tünel üzerinden haberleşmek. Sadece 3. kuşak IP tabanlı ağlarda olabilmektedir.
ETSI	Avrupalı Telekomünikasyon Standartları Enstitüsü
FR	Çerçeve iletimli
FW	Ateş duvarı
GGSN	GPRS destek düğümü geçidi
GMSC	MSC
GPRS	Global Paketlemeli Radyo Sistemi (veri servisi sağlayan, GSM ve TDMA'ye bağlı bir mobil ağ)
GPRS	General Packet Radio Service
GSM	Mobil Komünikasyon için Global Sistem
GSN	GPRS destek düğümü
GSN	GPRS Support Node
GTP	GPRS Tünel Protokolü
GUI	Grafik kullanıcı ara birimi
HTTP	Hiper Metin Transfer Protokolü
IMEI	Uluslararası Mobil Cihaz Kimliği
IMSI	Uluslararası Mobil Abone Kimliği
IP	İnternet Protokolü
IPSec	IP güvenliği
IPv4	İnternet Protokol sürüm 4
IPv6	İnternet Protokol sürüm 6
ISP	İnternet servis sağlayıcı
LAN	Yerel ağ
LIG	Yasal yolunu kesme geçidi
MCC	Mobil Ülke Kodu

ME	Mobil Cihaz
MM	Mobillığın Yönetimi
MNC	Mobil ağ kodu
MS	Mobil istasyon
MSC	Mobil hizmetleri açma merkezi
MSIN	Mobil abone kimlik no
MT	Mobilde sonlanma
NE	Ağ elemanı
NMSI	Ulusal Mobil İstasyon Kimlik No
O&M	Bakım ve onarım
PDN	Paket veri ağı
PDP	Paket veri protokolü
PIN	Kişisel kimlik no
PS	Paket anahtarlama
PSTN	Genel kullanımlı telefon ağı
QoS	Servis kalitesi
RADIUS	Uzaktan doğrulama, kullanıcı servislerinin aranması
RAI	Rota alanı kimliği
RAND	RANDom sayı
RPC	Uzaktan prosedür çağırma
SGSN	GPRS destek düğümünün sunulması
SIM	Abone kimlik modülü
SMS	Kısa mesaj servisi
SNR	Seri numara
SRES	İmzalanmış yanıt
SS7	İşaretleme sistemi no 7
TA	Terminal Adaptörü
TCP	İletişim kontrol protokolü
TE	Terminal cihazı
UMTS	Evrensel Mobil Telekomünikasyon Sistemleri
VC	Sanal devre
VLR	Konuğun yerinin kaydı
VPN	Sanal özel ağ
WAP	Mobil uygulama protokolü
WIRELESS VIRUS	Mobil cihazlar arasında yayılabilen virüsler

KAYNAKLAR

- [1]. GsmWorld. *What is General Packet Radio Service?*, <http://www.gsmworld.com/technology/gprs/intro.shtml>, (07.02.2005'de kontrol edildi).
- [2]. Christer, E., Per O. (1998). *WAP—The wireless application protocol*, Ericsson Review. 150-153, No.4
- [3]. Peter, A., Johan, H., and Peter, S. (2001). *WAP 2.x architecture—Features, services and functions*, Ericsson Review. 178-183, No.4
- [4]. Jussi R. *GPRS Security - Secure Remote Connections over GPRS*, http://www.hut.fi/~jrautpal/gprs/gprs_sec.html
- [5]. Peter, C., and Bert, W. (1999). *Tigris—A gateway between circuit-switched and IP networks* Ericsson Review. 70-81, No.2
- [6]. ETSI. *GSM0260: Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 1, Version 7.4.0.* (March 2000).
- [7]. ETSI. *GSM0360: Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2, Version 7.3.1.* (July 2000).
- [8]. ETSI. *GSM0161: Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements, Version 6.0.1.* (March 2000).