



CEP TELEFONU (GSM) SİSTEMİ -2

Fikret OTTEKİN
Elektronik Yüksek Mühendisi

Geçen sayımızda Türkiye'de "Cep Telefonu" olarak tanınan GSM (Global System for Mobile Communication) sisteminin genel bir tanımını yapmış, sistemin içerdiği pek çok işlevsel ve teknik özelliği konu etmiştik. GSM sistemi kablosuz iletişim teknolojisinin geldiği en son noktayı yansıtmaktadır. Bu sistemin standartlarının ufak tefek değişikliklerle, GSM'in ikinci nesil temsilcisi olan DCS (Digital Communication System) standartlarına dönüşeceği ve bu sistemlerin çok uzun yıllar güncelliğini koruyacağı düşünülürse GSM standartlarının önemi ortaya çıkar.

Cep telefonu sisteminin standardizasyonu sırasında sistemin güvenliğini ve performansını artırma amacıyla çeşitli yöntemler geliştirilmiştir. Bu yazımızda GSM sisteminin içerisinde yer alan bu ilginç özelliklerden birkaçını sizlere tanıtmaya çalışacağız.

DOĞRULAMA

Bilindiği gibi, kullanıcıların sistemden hizmet alabilmeleri için sistem işleticisi tarafından kendilerine verilen SIM kartlarını kullanmaları gerekmektedir. Terminal açıldığında kullanıcının telefon numarası SIM'den okunup sisteme bildirilir ve yapılan konuşmaların ücretleri ilgili telefon numarasının hesabına kaydedilir.

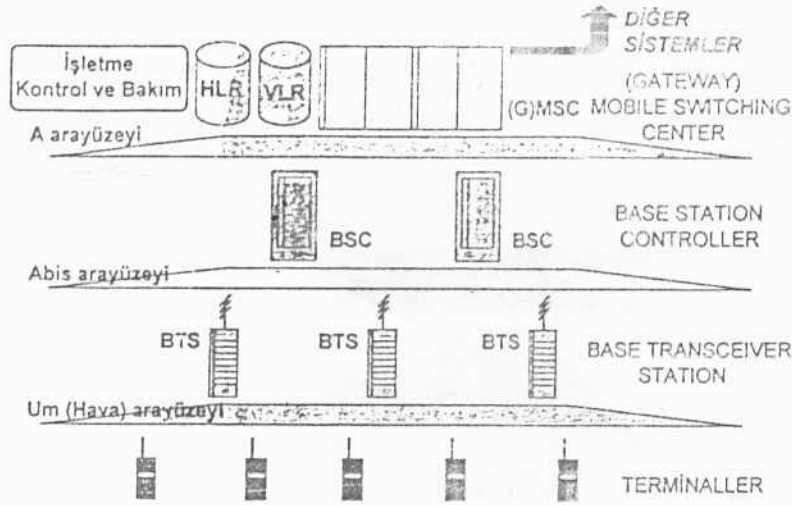
Sistem tarafından tanınan numaraları taşıyan kartların korsan olarak üretilip kullanılma olasılığı, numaranın gerçek sahibini ve sistemin güvenliğini korumak için önlem almayı zorunlu hale getirmektedir.

Sistem işleticisi tarafından her abonenin SIM kartına Ki adı verilen bir kullanıcı anahtarı yerleştirilmiştir. Bu anahtarla ilgili işlemlerin tümü SIM'in üstünde gerçekleştirilir ve böylece Ki'nin hiçbir zaman kartın dışına çıkmaması sağlanmış olur. Sistem tarafından her abone için ayrı ayrı belirlenip saklanan Ki anahtarı, ilgili abone kayıtlanma isteğinde bulunduğu SIM'in geçerliliğini sinama amacıyla kullanılmaktadır. Doğrulama (authentication) olarak adlandırılan bu işlemde başarılı olmayan terminaller sisteme kayıtlanmaz ve acil yardım çağrısı dışında hiçbir isteklerine cevap vermez.

Doğrulama işlemi aşağıdaki aşamalardan oluşur:

- 1) Sistem terminala "RAND" adı verilen 16 byte'lık bir veri gönderir (Şekil 1).
- 2) Terminal RAND'ı SIM'e gönderir ve SIM A3 algoritmasını kullanarak RAND ve Ki'den SRES adı verilen yeni bir parametre üretir. $SRES = f(A3)[Ki, RAND]$
- 3) Terminal SRES'i sisteme geri gönderir.
- 4) Sistem bu arada SRES'i kendi sakladığı Ki'yi kullanarak hesaplar.
- 5) Sistem terminalin hesapladığı SRES ile kendi hesapladığı SRES'i karşılaştırır.

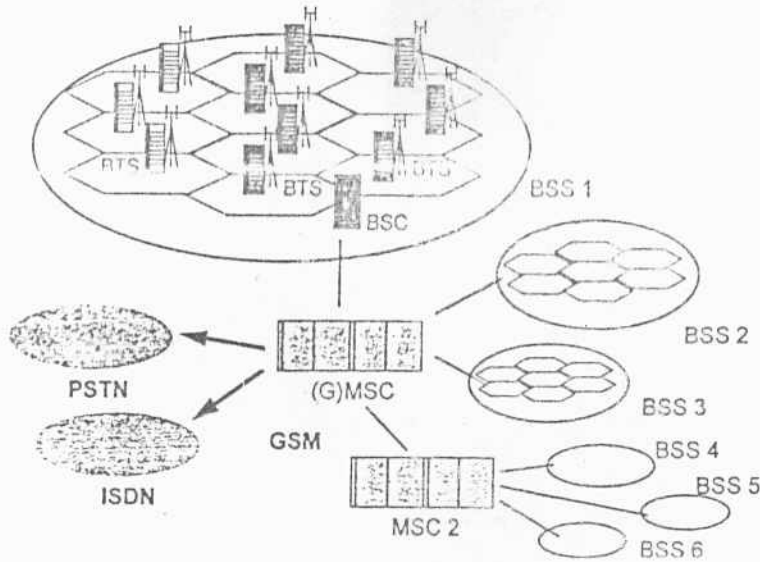
Bu parametreler birbirine eşitse SIM'in geçerli olduğuna karar verilir.



Şekil 4. Sistem Mimarisi

vb. terminallerle BTS'ler arasındaki Um arayüzünde geçerli parametrelerdi). BTS'ler terminallerle ilgili gerekli sinyallerin alınma ve gönderilmesinden sorumlular ve bunun dışında fazlaca bir fonksiyonları yok.

3) Mobile Switching Center (MSC) birimleri birkaç BSC birimini denetliyor ve GSM içi ya da sistemlerarası görüşmelerin kurulma ve sonlandırılmasından sorumlu. Dolayısıyla MSC birimleri diğer sistemlerle (PSTN, ISDN, vb.) bağlantı kurmak için gerekli fonksiyonları (Interworking Functions; IWF) gerçekleştiriyor. Ayrıca sistem operatörleri de alt yapıyı MSC seviyesinden kontrol etmekte.



Şekil 5. GSM Alt Yapısı

2) BTS'lerin bağlı olduğu Base Station Controller (BSC) birimleri trafik yoğunluğuna göre 20, 30 ya da daha fazla BTS'yi kontrol ediyor. Hangi terminalin hangi kanal üzerinden konuşacağına ve gerekirse çağrı sırasında herhangi bir terminalin kanal ya da BTS değiştirmesine (Handover) BSC birimleri karar vermekte. Bir BSC ve kontrol ettiği BTS'lerin oluşturduğu gruba BSS (Base Station Subsystem) adı veriliyor (Şekil 5).

Sistemin MSC seviyesinde bir ya da daha çok MSC'yi destekleyen iki veri tabanı görmekteyiz. Bunlar ziyaretçi veri tabanı (VLR; Visitors Location Register) ve asıl veri tabanı (HLR; Home Location Register) birimleri. Her HLR biriminde sisteme kayıtlı terminallerin belli bir bölümü ile ilgili bilgiler (ek servislerden hangilerine kayıtlanmış olduğu vb.) yer al-

uğu
ller
yo-
ya
S'yi
ngi
nal
şına
nda
alin
ştir-
BSC
kte.
tiği
u-
non
iyor

leri
i ya
ve
ıyla
DN,
için
(In-
ons;
Ay-
i de
sin-

C'yi
anı
iya-
LR;
ter)
LR;
ter)
iri-
ter-
ümü
vis-
yıl-
al-

makta. VLR biriminde ise kendi HLR sahasının dışında dolaşmakta olan terminallerin hangi HLR'ye kayıtlı olduğu bilgisi geçici olarak tutulmakta. VLR ve HLR birimlerinin yüzbinlerce aboneyle ilgili bilgiyi saklayacak ve çağrının kurulmasını yavaşlatmadan gerekli bilgiye ulaşabilecek kapasitede olmaları gerekiyor.

SİSTEM / FREKANS PLANLAMASI

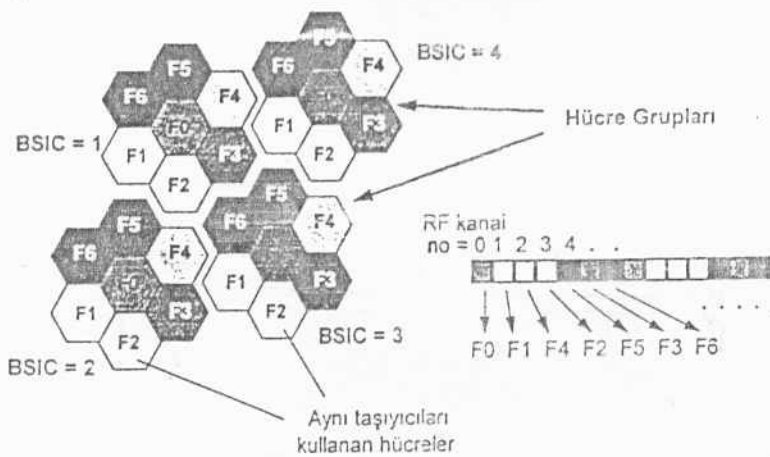
GSM sisteminin toplam 124 taşıyıcıya sahip olduğunu daha önce belirtmiştik. Sistem maliyeti açısından bir değerlendirme yapıldığında en kazançlı yöntemin şehrin ortasına güçlü bir BTS kurmak ve eldeki tüm taşıyıcıları bu BTS'ye yüklemek olacağı şeklinde bir sonuç ortaya çıkıyor. Ancak böyle bir yöntem kullanmak olası değil, çünkü 124 taşıyıcı bir milyon kişilik (ya da çok daha kalabalık) bir şehrin konuşma talebini karşılayamıyor. Bu noktada frekans tekrar kullanımı (Frequency reuse) zorunlu olarak devreye girmekte. Elde sonsuz genişlikte bir frekans bandı olsa da, şehir merkezlerinde yüksek binalar şiddetli yansıma ve kırılmalara neden olduğundan tek hücreyle etkili bir kaplama alanı oluşturulamıyor.

Yoğun trafik ve kaliteli kaplama alanı oluşturma

zorunluluğu şehir merkezlerinde çok küçük hücreler (microcell) kullanma gereğini gündeme getirmekte. BTS'lere kanal tahsisı yapılırken frekans bandında ardışık olarak yer alan taşıyıcıların fiziksel olarak birbirinden olabildiğince uzak hücrelere atanması gerekiyor (Şekil 6). Aksi halde daha önce de belirttiğimiz gibi ara kanal karışımları sistemin performansını önemli ölçüde düşürüyor.

Pasif durumdaki terminallerin aynı frekanstan kontrol kanalı yayını yapan BTS'leri birbirine karıştırmamaları için de bir önlem düşünülmüş. Her BTS bağlı olduğu hücre grubunun kimlik numarasını (BSIC; Base Station Identity Code) yayınlıyor. Böylece pasif durumdaki bir terminal yer değiştirirken dinlemekte olduğu kanaldaki BSIC'in değiştiğini görürse başka bir BTS'yi dinlemeye başladığını fark ediyor.

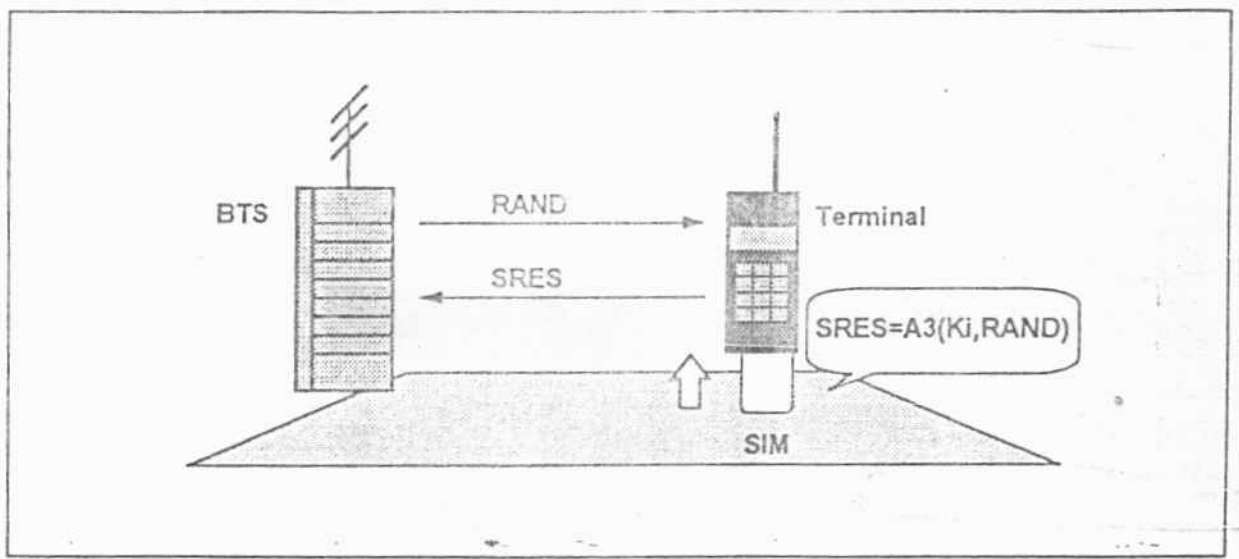
Bu yazımızda GSM sisteminin işlevsel özelliklerini tanıtmış ve bazı teknik özelliklerini incelemiş olduk. Gelecek yazımızda da sistemde kullanılan şifreleme, aralıklı alma / gönderme, aktarma (handover), frekans atlama gibi pek çok ilginç özelliği tanıtmaya çalışacağız.



Şekil 6. Frekans Planlaması

BİYOGRAFİ

1968 yılında Bursa'da doğan Fikret Ottekin, 1990 yılında ODTÜ Elektrik Elektronik Mühendisliği Bölümü'nden mezun oldu. 1990-1992 yılları arasında aynı bölümde Araştırma Görevlisi olarak bulundu. 1992 yılında Telekomünikasyon dalında yaptığı Yüksek Lisans çalışmasını tamamlayarak ASELSAN'da görev ve başladı. Halen HC Sivil Habereleşme Müdürlüğü GSM Proje Grubunda görev yapmaktadır.



Şekil 1. Doğrulama

KRİPTOLAMA

Analog sistemlerde uygulanması hayli zor olan ve çok da iyi sonuç vermeyen kriptolama işlemleri sayısal sistemlerde kolayca uygulanabilmekte ve oldukça başarılı sonuçlar alınmaktadır. Cep telefonu sisteminde kriptolama işlemleri 1996 başlarında ikinci evre çerçevesinde devreye girecek ve tüm ses ve veri iletişimlerine uygulanacaktır. GSM'de kriptolama işleminin temelinde doğrulama amacıyla da kullanılan Ki anahtarı yer almaktadır. Kriptolama işlemi şu şekilde gerçekleştirilir:

- 1) Sistem terminale "RAND" adı verilen 16 byte'lık bir sayı gönderir.
- 2) Terminal RAND'ı SIM'e gönderir ve SIM, "Açık anahtar algoritması" (public key) adıyla ABD'de standartlaşmakta olan A8 algoritmasını kullanarak RAND ve Ki'den Kc adı verilen oturum anahtarını (session key) üretir.
 $Kc = f(A8) [Ki, RAND]$
- 3) Terminal Kc'yi ve sistemin yayınladığı FN (Frame number) parametresini kullanarak A5 algoritmasıyla her çerçeve için iki ayrı şifreleme ve şifre çözme dizisi (S1, S2) üretir.
 $(S1, S2) = f(A5) [Kc, FN]$
- 4) Bu iki dizinin terminalde alınan ve yollanan dizilerle Modulo 2 aritmetiği ile toplanmasıyla

la kriptolama ve kript çözme işlemi gerçekleştirilir.

Mod 2 toplama işlemi çok basit bir işlem olduğundan görüşme sırasında terminalin işlemcisinin çok az vaktini alır. Kriptolamanın başında kullanılan A8 algoritması ise ideal bir kriptolama algoritması özelliklerini taşımaktadır. Şöyle ki algoritmayı çalıştırarak Ki ve RAND'dan Kc'yi elde etmek kolay olduğu halde Kc'den Ki'yi hesaplamamanın neredeyse imkansız olduğunu söyleyebiliriz. Böylece A8 algoritmasıyla Mod2 toplama işleminin aralarda kullanılmasıyla hem çok güvenli hem de çok hızlı bir kriptolama yöntemi oluşturulmuştur.

AKALIKLI ALMA

Terminallerin açık ve sisteme kayıtlı olduğu, fakat herhangi bir görüşmenin olmadığı durumlarda, kontrol kanalını dinleyerek sistemden kendilerine herhangi bir çağrı gelip gelmediğini izlemeleri gerekir. Bu bilgi Genel Kontrol Kanalı'nın (broadcast control channel) Çağırma Kanalı (paging channel) bölümünde yayınlanır.

Terminaller sistemin yayınladığı parametreler uyarınca gruplara ayrılırlar ve her terminal kendisine ait Çağırma Kanalı grup numarasını hesaplar. Daha sonra terminaller Çağırma Kanalı'nın sadece kendi gruplarına ayrılmış bölümünü dinlemekle yükümlü olurlar. Bu durumda terminaler (sistem operatörünün seçeceği paramet-

reye göre) 0.47 saniye ile 2.12 saniye arasında değişebilen bir periyot içerisinde sadece 18.4 milisaniyelik bir süre boyunca alma yaparlar (Şekil 2). Terminaller böylece toplam zamanlarının %0.87 si ile %3.92 si arasında bir bölümünü Çağırma Kanalı'nı dinleyerek geçirmiş olurlar. Bu uygulamaya Aralıklı Alma (Discontinuous Reception) adı verilmiştir.

Aralıklı Alma uygulaması çağrılarının kurulmasında 0.5 - 2.0 saniyelik gecikmeye yol açmasına rağmen batarya tüketimini önemli ölçüde azalttığı için yararlı olmaktadır.

ARALIKLI GÖNDERME

Herhangi bir telefon görüşmesinde tarafların toplam konuşma süresinin yaklaşık yarısında konuştuğunu, kalan sürede ise dinleme durumunda kaldıklarını varsayabiliriz. Dinleme durumundaki kullanıcının terminali bu sırada ortamda var olan gürültüyü işleyip yayınlamak istenmeyen iki sonucun ortaya çıkmasına neden olur.

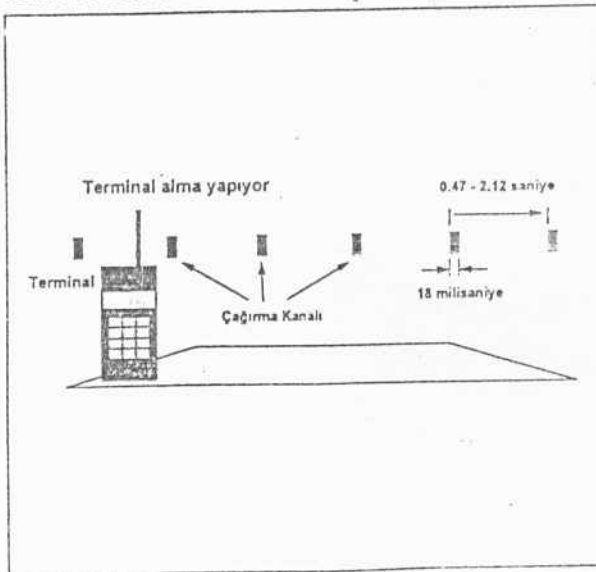
Öncelikle gereksiz bilginin işlenmesi ve yayınlanması cep telefonu tasarımının kritik parametrelerinden batarya tüketimini artırarak daha büyük ve ağır batarya kullanımını zorunlu hale getirir. Batarya tüketiminin yanı sıra GSM bandına sıkışık bir biçimde yerleşmiş RF kanallarında gereksiz yayın yapılması boş yere ara kanal karışımına neden olarak sistemin performansını düşü-

rür.

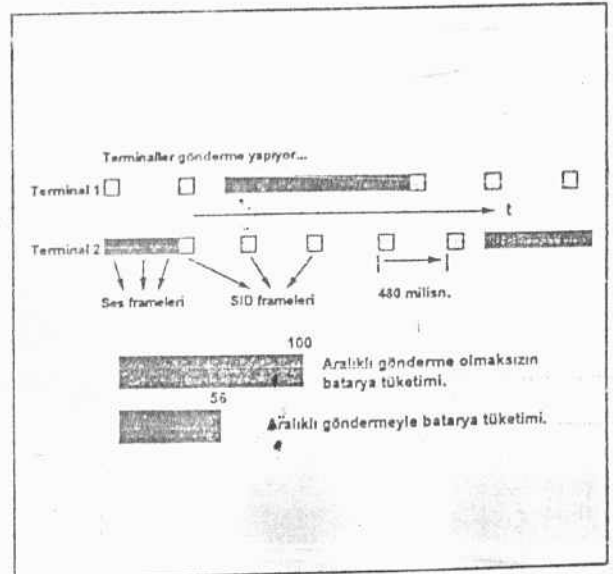
Bu sakıncaları ortadan kaldırmak amacıyla, GSM standardizasyonu sırasında encoder çıkışındaki diziyi inceleyerek kullanıcının konuşup konuşmadığına karar verecek bir algoritma geliştirilmiştir. Voice Activity Detection olarak adlandırılan bu algoritma özetle insan sesini geri plandaki gürültüden ayırıp ortalama gücünü hesaplar. Hesaplanan parametre belirli bir değerin altına düştüğünde algoritma kullanıcının konuşmadığına karar verir.

Konuşmanın olmadığı zaman aralıklarında terminaller ses bilgisi yerine geri plandaki gürültüyü işlerler ve 480 milisaniyede bir çerçeve (frame) üretip yayınlamak normal iletişim hızının yaklaşık 1/24'üne düşerler (Şekil 3). Geri plandaki gürültüyle ilgili bilgiler içeren bu çerçevelere Silence Descriptor (SID) adı verilir. SID çerçeveleri diğer terminalde comfort noise denilen suni bir ses oluşturulması amacıyla kullanılır. Böylece diğer terminaldeki kullanıcının bağlantının koptuğunu sanması engellenmiş olur.

Yukarıda tanımlanan işlemlere özetle Aralıklı Gönderme (Discontinuous Transmission) denilmektedir. Bir terminalin yarım saatlik bir konuşmada 100 birim güç harcadığını varsayarsak aralıklı gönderme özelliği eklendiğinde aynı terminalin harcadığı gücün 56 birime düştüğünü görürüz.



Şekil 2. Aralıklı Alma



Şekil 3. Aralıklı Gönderme

JSM
daki
nuş-
tırıl-
ındı-
olan-
sap-
altı-
şma-

t
ültu-
(fra-
zının
nda-
elere
çeve-
suni
ylece
kop-

alıklı
enil-
nuş-
ara-
ermi-
görü-

DİNAMİK YAYIN GÜCÜ KONTROLU

Cep telefonunun en ilginç özelliklerinden biri de terminallerin yayın gücünün sistem tarafından denetlenmesidir. Terminaller herhangi bir konuşmaya maksimum güçle yayın yaparak başlarlar. Ancak daha sonra yayın güçlerini sistemden saniyede iki kez gelmekte olan Tx-Power parametresine göre ayarlarlar. Bu ayarlamayı yaparken de yayın gücü, ara kanal karışımına neden olmamak için, 2 dB'lik adımlar halinde her adımda 60 milisaniye beklenerek değiştirilir.

Sistem terminallerden yayın güçlerini 13 dBm'e kadar düşürmelerini ya da 43 dBm'e kadar artırmalarını isteyebilir. Bu uygulama sayesinde BTS'lere yakın olan terminallerin yayın yapmak için gerekenin üstünde güç harcamaları önlenmiş, ara kanal karışımı da en alt düzeyde tutulmuş olur.

FREKANS ATLAMASI

Çağrının kurulması aşamasında sistem terminale en az bir, en çok 64 taşıyıcıdan oluşan bir set (Mobile Allocation) gönderir. Terminal, çağrı boyunca belli bir düzene göre bu taşıyıcıların üzerinde dolaşır ve her aralığı değişik bir taşıyıcıda alır / gönderir. Taşıyıcı dizisinin (Hopping Sequence) eldeki taşıyıcı setinden nasıl oluşturulacağı GSM spesifikasyonlarında tanımlanmıştır. Bu tanıma göre taşıyıcı setinin yanı sıra sistem terminale iki parametre daha gönderir (Mobile Allocation Index Offset ve Hopping Sequence Number). Bu parametreler aracılığıyla n taşıyıcıdan oluşan bir taşıyıcı setinden 64 n değişik taşıyıcı dizisi türetilmektedir. Örneğin (6=16 için) 16 taşıyıcıdan oluşan bir setten 1024 değişik dizi

üretilebilir. Ancak bu 16 taşıyıcıdan oluşan bir alanın aynı anda 1024 terminal tarafından kullanılabileceği anlamına gelmez. Frekans bandında belli bir alan birkaç terminal tarafından kullanılacağına, bu terminallerin frekans boyutunda çakışmalarını istenirse 16 taşıyıcıdan oluşan bir bölgede en fazla 16 terminal verilebilir.

Herhangi bir çağrıda frekans atlama kullanılıp kullanılmayacağı sistemden gelen parametreler uyarınca çağrı kurulurken belirlenir. Frekans atlama da kriptolama gibi ikinci evre çerçevesinde devreye girecektir.

Frekans atlama özelliği cep telefonu sistemine iki büyük avantaj getirmektedir. Konuşma sırasında değişik frekansların taranması terminallerin "fading" dediğimiz fiziksel olaydan fazla etkilenmesini sağlar. Bu kavrama Frequency Diversity denilmektedir. Frekans atlama ayrıca sistemi kullanan tüm abonelerin hemen hemen aynı miktarda ara kanal karışımına maruz kalmasını sağlar. Bu kavrama da Interferer Diversity denilmektedir.

EL DEĞİŞTİRME

Kablosuz iletişim sistemlerinde terminaller her an hareket halinde olabildiği için görüşme sürerken içinde bulunulan iletişim ortamı çağrı kurulurkenki durumundan çok daha farklı bir duruma gelebilir. Örneğin terminallerden birinin konuşma sırasında hizmet aldığı hücrenin kaplama alanının dışına çıkması ya da ara kanal karışımından çok daha fazla etkilenen bir bölgeye gelmesi olasıdır. Bu gibi durumlarda görüşmeyi sonlandırmadan çağrının yeni hücre üstünden ya

Gelen Sinyal Şiddeti	Alma Seviyesi
> -48 dBm	63
(-49 dBm, -48 dBm)	62
:	:
(-110 dBm, -109 dBm)	1
< -110 dBm	0

Tablo 1. Gelen sinyal şiddetinden Alma Seviyesi'nin çıkarılması

Bit Hata Oranı	Alma Kalitesi
< 0.2 %	0
(0.2 %, 0.4 %)	1
:	:
(6.4 %, 12.8 %)	7
> 12.8 %	8

Tablo 2. Bit hata oranından Alma Kalitesi'nin çıkarılması

da yeni kanallardan tekrar kurulması işlemine El değiştirme (handover) adı veriliyor.

GSM'de handover işlemi sistem tarafından; ancak terminallerin yardımıyla gerçekleştirilir. Görüşme yapmakta olan tüm terminaller hizmet aldıkları ve alabilecekleri en yakın altı BTS'i (Base Transceiver Station) dinler ve yaptıkları ölçümlerin sonuçlarını sisteme bildirirler. Hizmet alınan BTS'le ilgili olarak Alma Seviyesi (receive level) ve Alma Kalitesi (receive quality) parametreleri, komşu BTS'lerle ilgili olarak ise sadece Alma Seviyesi parametresi hesaplanarak saniyede bir ya da iki kez sisteme iletilir (Tablo 1,2).

Bu parametreler sistem tarafından değerlendirilir (Tablo 3) ve gerekirse el değiştirme işleminin yapılmasına karar verilir.

Tabloda gösterilen ikinci durumda terminal ara kanal karışımından daha az etkilenen bir taşıyıcıya aktarılır. Bu işleme Hücre İçi Aktarma (intra cell handover) adı verilmektedir. Son durumda ise terminal daha iyi hizmet almak için Hücreler Arası Aktarmaya (inter cell handover) gereksinim duyar.

Yukarıda incelediğimiz işlemleri özetlememiz gerekirse (Tablo 4) doğrulama ve şifreleme işlemlerinin sistem güvenliğine, el değiştirme ve Frekans Atlama özelliklerinin sistem performansına, Aralıklı Alma özelliğinin ise batarya tasarrufu açısından terminallere katkı sağladığını söyleyebiliriz. Aralıklı Gönderme işlemiyle Dinamik Yayın Kontrolü özelliği ise hem güvenlik hem de batarya tasarrufu açısından yararlıdır.

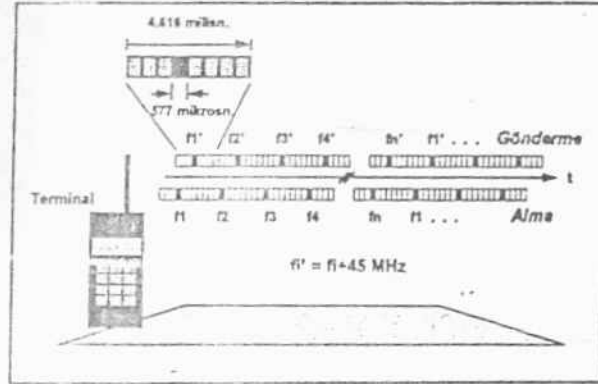
Alma Seviyesi	Alma Kalitesi	Durum
İyi	İyi	Normal
İyi	Kötü	Terminalin konumu iyi ancak ara kanal karışımından etkileniyor.
Kötü	Kötü	Terminal kullanmakta olduğu hücrenin sınırında ya da dışına çıkıyor.

Tablo 3. El değiştirme parametrelerinin değerlendirilmesi

Katı İşlem	Sistem Güvenliği	Batarya Tasarrufu	Sistem Performansı
Authentication	■		
Şifreleme	■		
Aralıklı Alma		■	
Aralıklı Gönderme		■	■
Dinamik Yayın...		■	■
Frekans Atlaması			■
Handover			■

Tablo 4. İncelenen işlemlerin sisteme katkısı

Sistemin sayısal olması başta şifreleme olmak üzere tüm bu işlemlerin etkili bir biçimde gerçekleştirilebilmesine olanak sağlamaktadır.



Şekil 4. Frekans Atlaması

BİYOGRAFİ

1968 yılında Bursa'da doğan Fikret Ottekin, 1990 yılında ODTÜ Elektrik Elektronik Mühendisliği Bölümü'nden mezun oldu. 1990-1992 yılları arasında aynı bölümde Araştırma Görevlisi olarak bulundu. 1992 yılında Kurumlar Bakanlığı'nda yaptığı Yüksek Lisans çalışmasını tamamlayarak ASELSAN'da göreve başladı. Halen HC Sivil Haberleşme Müdürlüğü GSM Proje Grubunda görev yapmaktadır.