GPS DONANIMLI TELEFONLARA YÖNELİK KONUMLANDIRMA SİSTEMİ

POSITIONING SYSTEM FOR GPS-ENABLED MOBILE PHONES

HASAN TAHSİN BİLGİÇ

Hacettepe Üniversitesi

Lisansüstü Eğitim – Öğretim ve Sınav Yönetmeliğinin

ELEKTRİK ve ELEKTRONİK Mühendisliği Anabilim Dalı İçin Öngördüğü

YÜKSEK LİSANS TEZİ

olarak hazırlanmıştır.

2011

Fen Bilimleri Enstitüsü Müdürlüğü'ne,

Bu çalışma jürimiz tarafından **ELEKTRİK ve ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI 'nda YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Başkan	:….. Prof. Dr. Selçuk GEÇİM
Üye (Danışman)	:….. Doç. Dr. Ali Ziya ALKAR
Üye	:….. Yrd. Doç. Dr. Harun ARTUNER
Üye	:….. Yrd. Doç. Dr. Mehmet DEMİRER
Üye	:….. Yrd. Doç. Dr. Umut Sezen

ONAY

Bu tez Hacettepe Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliği'nin ilgili maddeleri uyarınca yukarıdaki jüri üyeleri tarafından ...../...../..... tarihinde uygun görülmüş ve Enstitü Yönetim Kurulunca ...../...../..... tarihinde kabul edilmiştir.

Prof.Dr. ……..
Fen Bilimleri Enstitüsü Müdürü

GPS DONANIMLI TELEFONLARA YÖNELİK KONUMLANDIRMA SİSTEMİ

Hasan Tahsin Bilgiç

ÖZ

Bu tez çalışmasında gerçek zamanlı ya da önceden alınmış verilerle harita üzerinde çalışan güvenli uzaktan mobil telefon takibi uygulaması gerçekleştirilmiştir. GPS özellikli cep telefonları üzerinde çalışmakta olan yazılım, GPRS veya 3G gibi bir internet bağlantısı üzerinden, internette çalışmakta olan sunucuya coğrafi konum bilgilerini göndermektedir.

Alınan konum bilgileri sunucuda veritabanına aktarılmakta ve orada saklanmaktadır. Kullanıcılar ise web arayüzüne bağlanarak, burada, veri gönderen ya da veri göndermiş kullanıcıların konum izlerini harita üzerinde görebilmektedirler.

Harita üzerinde, kullanıcılar tarafından diğer kullanıcılar için coğrafi çerçeveleme yapılabilmektedir. Kullanıcılar çerçeve sınırları dışına çıktığında çerçeveyi belirleyen kullanıcı e-posta yoluyla bilgilendirilmektedir.

Konum bilgileri, güvenliği sağlamak amacıyla cep telefonu yazılımında AES şifreleme algoritması kullanılarak şifrelenmektedir. Şifre olarak her telefonda bulunan ve telefona özel olan seri numarası kullanılmaktadır. Bu sayı, gerekli şifre formatına çevrilmektedir. Sunucu tarafında ise gelen şifrelenmiş veri çözülerek veritabanına yazılmaktadır.

Cep telefonu yazılımının gerçekleştirilmesinde hemen her akıllı telefonda koşabilen JAVA ME kullanılmıştır. Geliştirme NetBeans üzerinde yapılmıştır. Sunucu ve web arayüzü kısmında MySQL, PHP ve HTML kullanılmıştır. Takibin yapılmasında görsellik sağlayan haritalar ise Google Maps kullanılarak gerçekleştirilmiştir.

Anahtar Kelimeler: GPS, GPRS, Google Maps, JAVA ME, MySQL, PHP, Mobil Cihaz Takibi, Coğrafi Çerçeveleme, AES.

Danışman: Doç. Dr. Ali Ziya ALKAR, Hacettepe Üniversitesi, Elektrik ve Elektronik Mühendisliği Anabilim Dalı

POSITIONING SYSTEM FOR GPS-ENABLED MOBILE PHONES

Hasan Tahsin Bilgiç

ABSTRACT

GPS-enabled phones are becoming more and more popular and common. In recent years, tracking of objects using GPS data on maps has become a popular topic. In this work, we propose a secure real-time tracking system for GPS-enabled phones based on dynamically updated maps.

In the cell phone, we have built a software to send GPS data to a main server using GPRS. In the server, the data is saved into a database. Any time, a user can go on the web interface and track senders' GPS data on the map.

Users can apply geo fencing for other tracked users. Whenever a tracked user goes off the boundaries set by the geo fencing application, an e-mail is sent to inform the person who set the fencing.

The GPS data is encoded with AES algorithm to preserve authenticity and for security purposes by the software on cell phone. The data is then decoded on the server. For the encryption key, a unique serial number that comes with every cell phone has been used. This number is transformed into the needed format before being used as an encryption key.

The software on the cell phone is built by JAVA ME, which is found in almost every smart phone today. The development environment is NetBeans. The server and the web interface use MySQL, PHP and HTML. The visual tracking on the map is made possible by using Google Maps.

Keywords: GPS, GPRS, Google Maps, JAVA ME, MySQL, PHP, Mobile Phone Tracking, Geo Fencing, AES.

Advisor: Assoc. Prof. Ali Ziya ALKAR, Hacettepe University, Electrical and Electronics Enginering Department

TEŞEKKÜR

Yazar, bu çalışmanın gerçekleşmesinde katkılarından dolayı aşağıda adı geçen kişi ve kuruluşlara içtenlikle teşekkür eder.

Tez danışmanım olan Sayın Doç. Dr. Ali Ziya ALKAR, çalışmanın sonuca ulaştırılmasında ve karşılaşılan güçlüklerin aşılmasında yön gösterici olmuştur.

TÜBİTAK UEKAE İLTAREN ailesi tez süresince maddi ve manevi desteklerini esirgememiştir.

Ailem, gerek tez öncesindeki öğrenim hayatımda, gerekse tez çalışmalarım sırasında ilgi ve desteklerini eksik etmemişlerdir.

İÇİNDEKİLER DİZİNİ

Sayfa

ŞEKİL DİZİNİ

Sayfa

ÇİZELGE DİZİNİ

Sayfa

SİMGELER VE KISALTMALAR DİZİNİ

A-GPS	**A**ssisted **GPS** (Yardımcı GPS)
AES	**A**dvanced **E**ncryption **S**tandard (Gelişmiş Şifreleme Standartı)
AJAX	**A**synchronous **J**avascript **a**nd **X**ML (Zamanuyumsuz Javascript ve XML)
API	**A**pplication **P**rogramming **I**nterface (Uygulama Programlama Arayüzü)
ASCII	**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange (Bilgi Değiştokuşu için Amerikan Standart Kodu)
CBC	**C**ipher **B**lock **C**haining (Şifre Blok Zincirlemesi)
CDC	**C**onnected **D**evice **C**onfiguration (Bağlı Cihaz Konfigürasyonu)
CDMA	**C**ode **D**ivision **M**ultiple **A**ccess (Kod Bölmeli Çoklu Erişim)
CERN	European Organization for Nuclear Research (Avrupa Nükleer Araştırma Organizasyonu)
CFB	**C**ipher **F**eed**b**ack (Şifre Geri Beslemesi)
CLDC	**C**onnected **L**imited **D**evice **C**onfiguration (Bağlanmış Sınırlı Cihaz Konfigürasyonu)
CSS	**C**ascading **S**tyle **S**heets (Basamaklı Stil Şablonları)
C/A	**C**ourse **A**cquisition (Rota Tayini)
DES	**D**ata **E**ncryption **S**tandard (Veri Şifreleme Standartı)
ECB	**E**lectronic **C**ode**b**ook (Elektronik Kodkitabı)
FCC	**F**ederal **C**ommunications **C**ommission (Federal Haberleşme Komisyonu)
GGSN	**G**ateway **G**PRS **S**upport **N**ode (Ağ Geçidi GPRS Destek Düğümü)
GPRS	**G**eneral **P**acket **R**adio **S**ervice (Genel Paket Radyo Servisi)
GPS	**G**lobal **P**ositioning **S**ystem (Küresel Konumlandırma Sistemi)
GSM	**G**lobal **S**ystem for **M**obile Communications (Mobil Haberleşme için Küresel Sistem)
GTP	**G**PRS **T**unneling **P**rotocol (GPRS Tünel Protokolü)

HTML	**H**yper**t**ext **M**arkup **L**anguage (Hipermetin Biçimleme Dili)
IBM	**I**nternational **B**usiness **M**achines (Uluslararası İş Makineleri)
IMEI	**I**nternational **M**obile **E**quipment **I**dentity (Uluslararası Mobil Cihaz Kimliği)
IP	**I**nternet **P**rotocol (İnternet Protokolü)
Java ME	Java **M**icro **E**dition (Java Mikro Basımı)
JCP	**J**ava **C**ommunity **P**rocess (Java Topluluğu Süreci)
JDK	**J**ava **D**evelopment **K**it (Java Geliştirme Teçhizatı)
JRE	**J**ava **R**untime **E**nvironment (Java İşleyiş Süresi Ortamı)
JSR	**J**ava **S**pecifications **R**equests (Java Şartname Talepleri)
KML	**K**eyhole **M**arkup **L**anguage (Keyhole Biçimleme Dili)
KNC	**K**işisel **N**avigasyon **C**ihazları
MySQL	**My S**tructured **Q**uery **L**anguage (My Yapılı Sorgulama Dili)
NGA	**N**ational **G**eospatial-Intelligence **A**gency
NIST	**N**ational **I**nstitute of **S**tandards and **T**echnology (Ulusal Standartlar ve Teknoloji Enstitüsü)
PHP	**P**HP: **H**ypertext **P**reprocessor (PHP: Hipermetin Önişlemcisi)
PND	**P**ersonal **N**avigation **D**evices (Kişisel Navigasyon Cihazları)
PPS	**P**recise **P**ositioning **S**ervice (Kesin Konumlandırma Sistemi)
RSA	**R**ivest, **S**hamir, **A**dleman
RUIM	**R**emovable **U**ser **I**dentity **M**odule (Silinebilir Kullanıcı Kimlik Modülü)
SATSA	**S**ecurity **a**nd **T**rust **S**ervices **A**PI (Güvenlik Servisleri API)
SATSA-APDU	SATSA-**A**pplication **P**rotocol **D**ata **U**nit (SATSA-Uygulama Protokolü Veri Ünitesi)
SATSA-JCRMI	SATSA-**J**ava **C**ard **R**emote **M**ethod **I**nvocation (SATSA-Java Kart Uzaktan Metot Yürütmesi)
SATSA-PKI	SATSA-**P**ublic **K**ey **I**nfrastructure (SATSA-Açık Anahtar Altyapısı)
SGSN	**S**erving **G**PRS **S**upport **N**ode (Servis GPRS Destek Düğümü)

SIM	**S**ubscriber **I**dentity **M**odule (Sürdürümcü Kimlik Modülü)
SMS	**S**hort **M**essage **S**ervice (Kısa Mesaj Servisi)
SPS	**S**tandard **P**ositioning **S**ervice (Standart Konumlandırma Servisi)
Symbian OS	Symbian **O**perating **S**ystem (Symbian İşletim Sistemi)
TDMA	**T**ime **D**ivision **M**ultiple **A**ccess (Zaman Bölmeli Çoklı Erişim)
UICC	**U**niversal **I**ntegrated **C**ircuit **C**ard (Evrensel Entegre Devre Kartı)
VPN	**V**irtual **P**rivate **N**etwork (Sanal Özel Ağ)
WGS84	**W**orld **G**eodetic **S**ystem 84 (Dünya Jeodezi Sistemi 84)
XML	E**x**tensible **M**arkup **L**anguage (Uzayabilir Biçimleme Dili)
3DES	Triple DES (Üçlenmiş DES)
3G	**3**rd **G**eneration Mobile Telecomunications (3. Nesil Mobil Uziletişimi)

İNGİLİZCE – TÜRKÇE TERİMLER SÖZLÜĞÜ

Active Object	: Aktif Obje
Allowed	: İzin Verildi
Almanac	: GPS Uydularında Durum Bilgisi
Block Cipher	: Blok Şifreleme
Bug	: Hata
Byte Substitution Layer	: Byte Değiştirme Katmanı
Charging Gateway	: Ücretlendirme Geçidi
Ciphertext	: Şifre Metni
Circle	: Çember
Cleanup Stack	: Ek Bellek Temizleme
Concurrent	: Eşzamanlı
Cookie	: Tanımlama Bilgisi
Datum	: Veri
Decryption	: Şifre Çözme, Deşifreleme
Descriptor	: Tanımlayıcı
Diffusion Layer	: Difüzyon Katmanı
Directions Service	: Yol Tarifi Servisi
Drop-down Menu	: Aşağıya Açılır Liste
Encryption	: Şifreleme
Ephemeris	: Kesin Yörünge Bilgisi
Evaluation	: Değerlendirme
Floating Point	: Kayan Noktalı
Geometry	: Geometri
Geo Fencing	: Coğrafi Çerçeveleme
Google Earth	: Google Dünya
Google Maps	: Google Haritalar
Home Location Register	: Ev Yer Yazmacı
Ignored	: Kabul Edilmedi
Implementation	: Uygulama, Gerçekleştirme
InfoWindow	: Bilgi Penceresi
In Progress	: İlerleme Halinde
Key	: Anahtar
Key Addition Layer	: Anahtar Ekleme Katmanı
Load Testing	: Yükleme Testi

Location	: Mevki, Yer
Look-up Table	: Başvuru Çizelgesi
Low-level	: Düşük Seviye
Map	: Harita
Marker	: İşaretleyici, Belirteç
Medium Earth	: Orta Yörünge
Mix Column Layer	: Sütun Karıştırma Katmanı
Overlay	: Katman
Polygon	: Çokgen
Polyline	: Ard Arda Bağlanmış Doğrular
Plaintext	: Açık Metin
Pop-up Box	: Açılır Pencere
Rectangle	: Dikdörtgen
Satellite	: Uydu
Selective Availability	: Seçici Uygunluk
Session	: Oturum
Shift Rows Layer	: Sıra Değiştirme Katmanı
Stream Cipher	: Akım Şifreleme
Track Map	: İz Haritası
Travel Mode	: Gezi Durumu
User Friendly	: Kullanışlı
Zoom	: Yakınlaştır
Zoom in- Zoom out	: Yakınlaştır-Uzaklaştır

1. GİRİŞ

GPS (Küresel Konumlandırma Sistemi), daha önce sadece ABD askerleri tarafından kullanılmasına rağmen, bir sivil uçağın düşürülmesi sonrasında 1983 yılı itibariyle sivil kullanıma da açılmış küresel konumlama sistemidir[1]. Yıllarca eklenen ve geliştirilen yeni uydular ile doğruluğu arttırılmıştır. Bugün GPS cihazları çok küçük hatalarla dünya üzerindeki bir yerin koordinat tespitini yapabilmektedir.

Özellikle son yıllarda GPS ve navigasyon cihazları yaygın bir şekilde kullanılır hale gelmiştir. Bu cihazların yaygınlığıyla beraber değişik takip ve izleme sistemleri akademik ve ticari anlamda uygulanmakta ve geliştirilmektedir.

GPS cihazları takibi, izlenmesi ve harita üzerinde gösterilmesi alanında son yıllarda akademik anlamda değişik çalışmalar yapılmıştır. Bunların bazılarının amacı daha çok toplumun sosyal yaşantısını incelemeye yönelikken, diğer bazı çalışmaların amacı yürütülmekte olan başka bir bilimsel çalışmanın izlenmesi olmuştur. Bir çoğunun amacıysa takip ve izlemedir.

Bu hedeflerin yerine getirilmesinde GPS cihazları ya da üzerinde GPS yongası bulunan mobil cihazlar kullanılmıştır. Bir kısmında ise yeni bir cihaz tasarlanıp GPS yongası ve veri gönderici ünite aynı cihazda birleştirilmeye çalışılmıştır.

Mesela [1]'de GPS verileri geliştirilmiş cihaz ile bir merkeze yollanmaktadır. Bu verilerin araç kullanım saatlerinin ayarlanmasında kullanılması amaçlanmaktadır. [2]'de GPS ve GSM modüllerini içeren bir cihaz geliştirilmiş ve bununla kullanıcıların takibi amaçlanmıştır. Veriler sunucuya SMS (Kısa Mesaj Servisi) yoluyla gönderilmiştir. [3]'de araştırmacılar yine kendi ürettikleri gömülü sistem ile Google Maps sunucusu ile irtibata geçip konum verilerini harita üzerinde göstermektedirler. Bir öncekinden farklı olarak burada GPRS (Genel Paket Radyo Servisi) kullanılmıştır. Bu çalışmalarda GPS ve GSM modüller birleştirilerek, işlemi gerçekleştirecek cihazlar geliştirilmiştir. Bu çalışmalarda verileri göndermek ve haritada göstermek dışında kullanıcılara interaktif bir özellik sunulmamıştır. Ayrıca çalışmalarda herhangi bir güvenlik kaygısı da bulunmamaktadır.

[1] International Civil Aviation Organization (ICAO), Shooting down of a Korean Airlines Boeing 747 (Flight KE 007) on 31 August 1983, http://www.icao.int/cgi/goto_m.pl?icao/en/trivia/kal_flight_007.htm.

[4]'de VPN (Sanal Özel Ağ) üzerinden kalıcı bağlantı yapılıp veriler bir sunucuya aktarılmakta ve oluşturulan KML (Keyhole Biçimleme Dili) dosyaları Google Earth üzerinde gösterilmektedir. Gösterim en fazla 15 dakika ile sınırlı kalmaktadır. [5]'de GPS kayıtları bir sunucuya kullanıcı tarafından yüklenip, bu sunucuda değerlendirmelere tabi tutulmaktadır. Bu verilerden insanların sık kullandığı yollar ya da gözde mekanlar gibi bilgilerin çıkarımları yapılmaya çalışılmaktadır. Bu çıkarımlar sonucunda kullanıcılar dilediğinde tavsiyeler alabilmektedir. Bu makalede bir öneri olarak GPS donanımlı telefonların da bu işlemde kullanılabileceği belirtilmektedir. [6]'da ise GPS donanımlı telefonlar kullanılmaktadır. Bu çalışmada GPS verileri filtrelenip düzgünleştirilmekte ve başka bir telefona SMS yoluyla gönderilmektedir. Alıcı telefonda alınan konum bilgisi Google Maps yardımıyla harita üzerinde gösterilmesi sağlanmaktadır. [7]'de GPS donanımlı telefonlarla araçların yol durumlarına dair bilgiler edinilmekte ve dinamik bir ulaşım sağlanılmaya çalışılmaktadır. Bu çalışmada da kayıtlar tutulup belli aralıklarla sunucuya yüklenmekte ve değerlendirme yapılmaktadır. Herhangi bir harita söz konusu değildir. [8]'de GPS özellikli mobil telefon kullanıcılara yönelik bir uygulama gerçekleştirilmiştir. Kullanıcıların önceden kaydettikleri otobüs duraklarını kaçırmamaları sağlanmaktadır. Bu bakımdan bir coğrafi çerçeveleme uygulaması olarak da değerlendirilebilmektedir.

Değişik amaçlar güden bu akademik çalışmalar son yıllarda GPS kullanılarak izleme yapılmasının yaygınlaştığının göstergeleridir. Google Maps gibi harita sağlayıcılarının sunduğu yeni özelliklerle ve GPS donanımlı cep telefonlarının da yaygınlaşmasıyla sıradan cep telefonu kullanıcılarının da bu tip sistemlerden yararlanabilecekleri değerlendirilmektedir. Bu kullanıcılara güvenli bir ortam oluşturmak amacıyla bir takım güvenlik algoritmalarıyla da konum verilerinin korunmasının desteklenmesi de sağlanabilecektir.

Akademik çalışmaların yanı sıra GSM operatörlerinin sunduğu telefon yerinin bildirilmesine yönelik servisler bulunmaktadır. Bunlarda noktasal bir konum bilgisi edinme kaygısı bulunmamaktadır. Mesela Turkcell'in sunduğu Neredeyim servisinde şehir içinde 300-500 metreye kadar, şehir dışındaysa 1.5 km'ye kadar bir hassasiyetle telefon konumlarının bildirebileceği belirtilmektedir[2]. Fiyat ve

[2] Turkcell Neredeyim Servisi, http://www.turkcell.com.tr/bireysel/servisler/hayatinizikolaylastirin/turkcellneredeyim.

hassasiyet düşünüldüğünde bu tip sistemleri telefonlarıyla kullanmak isteyen insanlar için bu ve benzeri ticari servislerin hem pahalı hem de yetersiz olduğu görülmektedir.

GPS bilgisinin alınabilmesi için birkaç yıl öncesine kadar GPS cihazları kullanılırken, artık cep telefonları da GPS bilgisini sağlayan gömülü sistemler haline gelmişlerdir. Küresel konum bilgisini öğrenme cep telefonlarıyla beraber sunulan ve şu anki markette çoğu cep telefonunda da bulunan bir özellik haline gelmiştir. İleriki yıllarda, cep telefonlarının sunduğu standart bir özellik haline gelmesi kaçınılmazdır. Bu tez kapsamında da konum takip sistemi geliştirilmesi için, GPS ve navigasyon cihazları yerine GPS donanımlı cep telefonları kullanılmıştır. Böylece, bu tip sistemlerin sıradan cep telefonu kullanıcıları tarafından da kullanılabilmesi hedeflenmiştir. Ayrıca, bu tip bir sistemin daha az maliyetle kurye takip sistemlerine de bir alternatif olabileceği değerlendirilmektedir.

Bu tip sistemler, genel itibariyle, verileri toplayan merkezle irtibatı SMS ya da GPRS yoluyla sağlamaktadır. Bu tez kapsamında veri iletimindeki maddi kaygılar göz önünde bulundurularak GPRS ve 3G kullanılmıştır.

Yine bu tez kapsamında GPS bilgisinin gönderilmesine güvenlik sağlanması amacıyla verinin şifrelenmesi ve şifre çözülmesi gerçekleştirilmiştir. Her kullanıcıya ait farklı bir anahtar kullanılmıştır.

GPS bilgileri, PHP (PHP: Hipermetin Önişlemcisi) özellikli bir sunucu tarafından alınmakta ve bir veritabanına MySQL (My Yapısal Sorgulama Dili) ile işlenmektedir. Veritabanına kullanıcıların kolaylıkla ulaşabilmesi için bir arayüz ihtiyacı doğmuştur ve bir web arayüzü geliştirilmiştir. Web arayüzüne kullanıcılar kendi belirledikleri bir kullanıcı adı ve şifre ile girebilmektedirler. Arayüz üzerinde görmeye yetkili oldukları kullanıcıların şu anki ve önceki konum bilgilerini bir harita üzerinde görebilmektedirler. Harita uygulaması için Google Maps'in parasız sunduğu olanaklardan yararlanılmıştır. Ayrıca harita üzerinde kullanıcıların, diğer kullanıcılara ait konum verileri üzerinde etkisini arttırabilmek amacıyla Google Maps API (Uygulama Programlama Arayüzü)'nin son versiyonu olan Versiyon 3 ve Google Maps tarafından 2011 yılında kullanıma sunulmuş olan kütüphaneler kullanılarak bir takım yeni özellikler ve görsellikler eklenmiştir.

Tez kapsamında hazırlanmış web arayüzünde bu eklenen özelliklerden en dikkat çekeni coğrafi çerçeveleme uygulamasıdır. Bu uygulama ile bir kullanıcı için Google Maps haritası üzerinde, çizerek, sınırlar belirlenmekte ve kullanıcının bu sınırlar dışına çıkıp çıkmadığının takip edilebilmesi amaçlanmaktadır. Kullanıcı bu sınırlar dışına çıktığında bu kullanıcı için sınırlar belirlemiş olan kişiye e-posta yoluyla bilgi mesajı gönderilmektedir. Böyle bir uygulamanın bir konum takip sistemi için ya da kurye şirketleri için gerekli olabileceği düşünülmektedir. Ebeveynler çocukları için ya da kurye şirketleri şehir içinde kuryeleri takip etmek için böyle bir uygulamayı kullanmalarının faydalı olabileceği değerlendirilmektedir.

Bu tez çalışmasının takip eden kısımların düzenlenmesi şu şekildedir: Bölüm 2'de GPS'e değinilmektedir. Bir sonraki bölümde ise iletişimde kullandığımız GPRS yönteminden kısaca bahsedilmektedir. Bölüm 4'te kriptografiye değinilecek ve bu tezde kullanılmış algoritmadan genel hatlarıyla bahsedilmektedir. Bölüm 5'de ise konumlandırmada harita kullanımı üzerine bilgiler yer almaktadır. Bölüm 6'da gerçekleştirilen konumlandırma sisteminden ve yapılan çalışmalardan bahsedilmektedir. Bölüm 7'de sonuç ve değerlendirmeler yer almaktadır. Eklerde ise takip sisteminin tüm kullanımı örneklerle gösterilmektedir.

2. GPS

2.1 Tanımı ve Tarihçesi

GPS, küresel konumlama sistemidir. Dünya üzerindeki bir nesnenin yükseklik, enlem ve boylam cinsinden koordinat bilgilerini sağlamaktadır. Bu sistemin yöneticisi ve sahibi ABD'dir. İlk çıkışı ve kullanılışı askeri amaçlı olmasına rağmen, günümüzde sivil kullanıcılar tarafından da kullanılmaktadır. Ama hassasiyet bakımından sivil kullanıcılar askeri kullanıcılar kadar yüksek hassasiyete sahip değillerdir.

Bir çok teknolojik gelişme gibi GPS'in gelişimi de askeri ihtiyaçlardan doğmuştur. İkinci Dünya Savaşı sırasında kara bazlı radyo navigasyon sistemleri kullanılmıştır. Soğuk savaşla beraber nükleer ve nükleer olmayan silahlanma artmıştır. Özellikle ABD için daha güvenilir bir konumlama sistemi ihtiyacı doğmuştur. O yıllarda ABD'nin sahip olduğu füzelerin büyük kısmı denizaltı ve uçaklarda konuşlandırılmıştır. Hareket halindeki bu platformlardan özellikle de denizaltılardan istenilen hedeflere noktasal atışların yapılması için denizaltıların kendi yerlerini tam doğrulukla bilme ihtiyacı doğmuştur[1]. 1960'lı yıllarda Amerikan Donanması tarafından Transit ve Timation sistemleri geliştirilmiştir. Bu sistemlerin veri sağlama hızlarının ise sınırlı olduğu bilinmektedir. Bu sistemler, Amerikan Hava Kuvvetleri'nin hızlı hareket ihtiyacını karşılayamamıştır. Bunun için de Hava Kuvvetleri tarafından 621B geliştirilmiştir. 1973'te ise bu sistemlerin önemli özelliklerini kendisinde birleştiren Navstar-GPS'in hayata geçirilmesine karar verilmiştir[1]. Böylece GPS doğmuştur.

1983 yılında Kore Hava Yolları'na ait 007 sefer sayılı sivil uçağın SSCB'ye ait yasak hava sahasına girmesi ve sonrasında Sovyet havadan havaya mermileri tarafından düşürülmesi sonucunda 269 sivilin öldüğü talihsiz hava saldırısı meydana gelmiştir[2]. Bunun üzerine ABD Başkanı Ronald Reagan GPS sisteminin sivil kullanıma açılmasına yönelik bir yönerge yayınlamıştır.

---

[1] Aerospace Corporation. Charting a course toward global navigation, http://www.aero.org/publications/crosslink/summer2002/01/html.

[2] Internation Civil Aviation Organization (ICAO), Shooting down of a Korean Airlines Boeing 747 (Flight KE 007) on 31 August 1983, http://www.icao.int/cgi/goto_m.pl?icao/en/trivia/kal_flight_007.htm.

GPS sistemine ait ilk deneysel uydu 1978 yılında, ilk modern uydu ise 1989 yılında fırlatılmıştır. Günümüze kadar fırlatılan uyduların bir kısmı kullanımdan çıkarılmış ve yerlerine daha modern teknolojiye sahip uydular fırlatılmıştır[123]. Çizelge 2.1'de GPS uydularının fırlatılma miktarları ve şu anki durumları gösterilmektedir[123].

Uydu Bloğu	Fırlatılma Periyodu	Uydu Fırlatılışları		
		Başarılı	Başarısız	Yörüngede ve Çalışır Durumda
I	1978-1985	10	1	0
II & IIA	1989-1997	28	0	10
IIR	1997-2009	21	1	20
IIF	2010-2011	1	0	1

Çizelge 2.1 GPS Uydu Fırlatılma Tarihleri ve Şu Anki Durumları.

GPS sisteminde sivil kullanım açısından tarihi bir dönüm noktası da 1 Mayıs 2000 gecesi olmuştur. Dönemin ABD Başkanı Bill Clinton'un direktifleriyle GPS sistemindeki sivil kullanımlara yönelik seçici-uygunluk kaldırılmıştır[4]. Sivil kullanıcıların da yüksek doğrulukla GPS sistemlerinden yararlanmasının önü açılmıştır.

Piyasada Garmin, TomTom ve Magellan gibi markalara ait GPS cihazları bulunmaktadır. Bunlar GPS alıcısı şeklinde de isimlendirilebilmektedirler. Bu cihazlar yüksek doğrulukta sonuçlar vermektedirler ancak bu cihazlardan GPS verisi başka bir yere gönderilmek istendiğinde internet bağlantısı kurabilen başka bir cihaza beslenmesi gerekmektedir. Piyasada son yıllarda içerisinde barındırdığı GPS yongası ile bazı cep telefonları da GPS cihazı olma özelliğine sahip olmuşlardır.

[1] Navstar, http://www.astronautix.com/project/navstar.htm.
[2] GPS Block 2R, http://www.astonautix.com/craft/gpsock2r.htm.
[3] Navstar 65, http://www.nssdc.gsfc.nasa.gov/nmc/spacecraftDisplay.do?=2010-022A.
[4] National Geodetic Survey, GPS&Selective Availability Question&Answer, http://ngs.woc.noaa.gov/FGCS/info/sans_SA/docs/GPS_SA_Event_QAs.pdf.

2.2 Çalışma Prensibi

GPS alıcıları konumlarını GPS uydularından gelen sinyallere göre hesaplamaktadırlar. Bu hesaplamanın doğru yapılabilmesi için sinyallerin ne kadar sürede alındığının yüksek doğrulukla hesaplanabiliyor olması gerekmektedir. Küçük bir zamanlama hatası bile önemli yanlışlara yol açabilmektedir. Mesela 1 mikro saniyelik bir hata gelen sinyallerin hızının, c, yani ışık hızı olduğu düşünüldüğünde (2.1)'deki gibi hesaplanabilmektedir. Bundan dolayı yüksek doğrulukta bir ölçümün yapılıyor olması gerekmektedir.

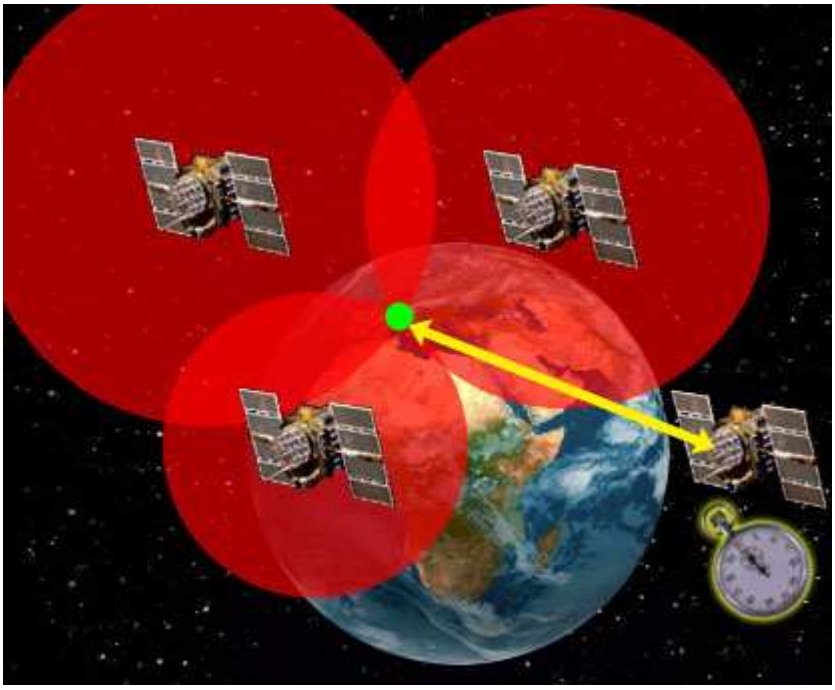
$$hata = c \times 1\mu s = 300m \tag{2.1}$$

GPS alıcıları konumlarını belirlemek için üç uydudan bilgi alıyor olmasının yeterli olabileceği düşünülebilir. Ama bu varsayım, sinyallerin yüksek hızından dolayı hatalı sonuçlar verebilmektedir. Bundan dolayı dört ya da daha fazla sayıda uydudan GPS sinyallerinin alınıyor olması gerekmektedir.

GPS uydusunun gönderdiği sinyalleri kullanarak, GPS alıcısı ona olan uzaklığı hesaplayabilmektedir. Bunun için geçen zaman ve ışık hızının çarpılması yeterli olmaktadır. Bu hesaplamada bulunan uzaklığı, merkezi, GPS uydusu olan bir dairenin yarıçap uzunluğu olarak düşünüp, bir daire oluşturmak mümkündür. Diğer uydulardan gelen sinyaller için de benzer daireler oluşturulabilmektedir. Eğer hiçbir hata yoksa GPS alıcısının bu dairelerin ortak kesişim noktasında olması beklenmektedir. Yüksek kapasiteli GPS alıcılarında, beklenen şekilde konum, dairelerin kesişim noktasında hesaplanmaktadır.

Yalnız, yüksek maliyetlerden dolayı üreticiler GPS alıcılarını bu kadar yüksek hassasiyetli üretmekten kaçınmaktadırlar. Zamandaki yanlış hesaplamanın yüksek hatalara yol açacağı belirtilmiştir. Bu GPS alıcılarının da zamanda oluşan hatayı ortadan kaldırmaları gerekmektedir. Bunun için de kesişime göre hatayı belirleyip bunu hesaplamalara eklemektedirler. Böylece dünya üzerindeki konumlarını da doğru olarak hesaplamaktadırlar.

Şekil 2.1'de GPS uyduları ve dünyanın yer aldığı bir çalışma şeması gösterilmektedir.



Şekil 2.1 GPS Uydularının Çalışması[1].

GPS sisteminde verilerin sağlanmasında iki farklı servis kullanılmaktadır. Bunlar Standart Konumlama Servisi (SPS) ve Yüksek Doğruluklu Konumlama Servisi (PPS)'dir. SPS, tüm kullanıcılara açık olan servistir. PPS ise ABD tarafından yetkilendirilen askeri kullanıcılara açıktır.

GPS verisi üç kısımdan oluşmaktadır. İlk kısımda zaman bilgisi vardır. Bu bilgiyi GPS alıcılar kendi saatlerini ayarlamak için kullanmaktadırlar. İkinci kısım veriyi gönderen uydunun koordinat bilgisidir. Üçüncü kısımda ise uydu durumları ve uyduların birbirine göre durum bilgisi bulunmaktadır. Ayrıca bu son kısımda hata düzeltme bilgisi de yer almaktadır.

GPS sinyalleri değişik bantlara yayılmıştır. Kullanılan temel iki frekans vardır. Bunlar L1 ve L2'dir. L1 herkese açıkken, L2 sadece askeri amaçlı kullanılmaktadır. L2 üzerinde kriptolu veri de gönderilmektedir. L1 1575.42 MHz ve L2 1227.60 MHz'dir. L1 frekansı C/A ve P iken, L2 yalnızca P'dir. Sivil kullanıcı kısmı tek banttan oluşmakta ve askeri kısım iki banda yayılmaktadır. Sivil kullanım için de bir bant daha eklenmesi planlanmaktadır. Bu bandın muhtemelen L5 olacağı ve frekansının 1176.45 MHz olacağı bildirilmektedir[2].

[1] Trilateration-GPS.jpg, http://www.unc.edu/~jdmc79/HowGPSWorks.html.
[2] GNSS Facts, http://www.navtechgps.com/extra/GNSSfacts.asp.

Temel frekans 10.23 MHz olarak alınmak üzere L1, L2 ve L5'e ait hesaplamalar (2.2), (2.3) ve (2.4)'de verilmektedir.

$$f_{L1} = 154 \times 10.23MHz = 1575.42MHz \quad (2.2)$$

$$f_{L2} = 120 \times 10.23MHz = 1227.60MHz \quad (2.3)$$

$$f_{L5} = 115 \times 10.23MHz = 1176.45MHz \quad (2.4)$$

2.3 Yapısı

GPS üç ana bölümden oluşmaktadır. Bunlar uzay bölümü, kontrol bölümü ve kullanıcı bölümüdür.

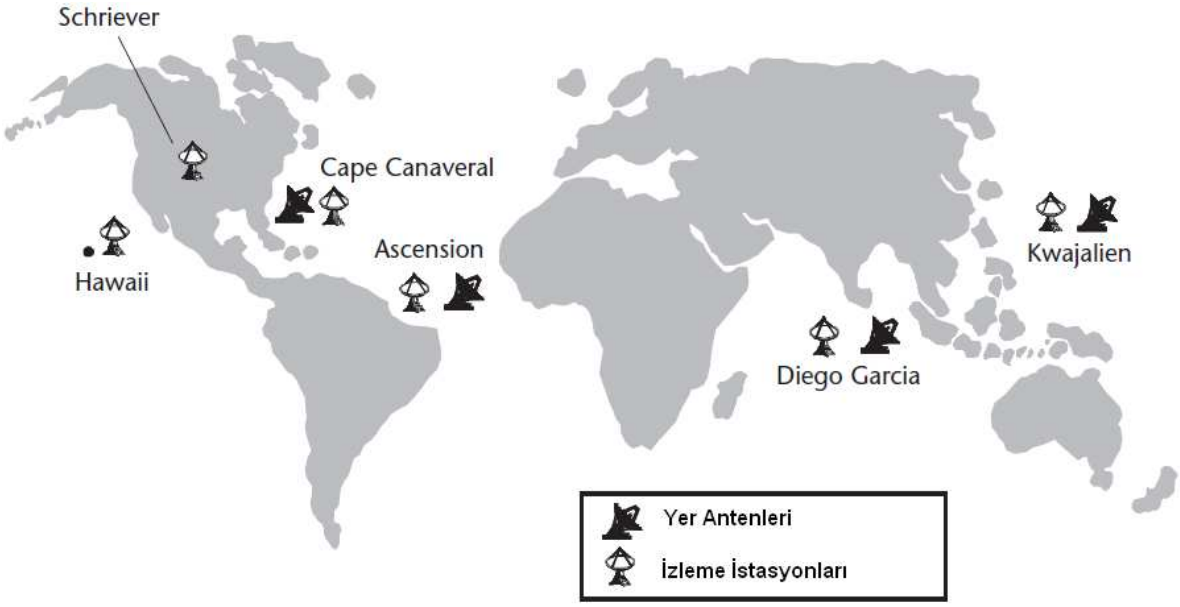
2.3.1 Uzay Bölümü

Uzay bölümü 24 ila 32 uydudan oluşmaktadır. Uydular dünya yörüngesinde bir günde iki tur tamamlamaktadırlar. Yaklaşık 20200 metre yükseklikte bulunmaktadırlar[1]. Böylece, uydular yeterli bir kapsama alanına ulaşmaktadırlar. Bu yörüngeye orta yörünge denilmektedir. Şu anki uydular düşünüldüğünde dünyanın herhangi bir yerinden bir GPS alıcısı en az 6 uydu görebilmektedir. Hesaplamaların da yapılması için en az 4 uydu gerekmektedir.

2.3.2 Kontrol Bölümü

Kontrol bölümü ana kontrol istasyonu ve kontrol merkezlerinden oluşmaktadır. Kontrol bölümünde ana kontrol istasyonu, alternatif ana kontrol istasyonu, yer antenleri ve izleme istasyonları bulunmaktadır. Ana kontrol istasyonu Colorado'da bulunan Schriever Hava Kuvvetleri Üssü'nde bulunmaktadır. İzleme istasyonları ise Colorado, Colorado Springs, Cape Canaveral, Hawaii, Kwajalien, Diego Garcia ve Ascension Adası'nda bulunmaktadır. Antenler ise Cape Canaveral, Kwajalien, Diego Garcia ve Ascension Adası'nda bulunmaktadır [9]. Şekil 2.2'de bu istasyon ve antenlerin bulundukları yerler gösterilmiştir.

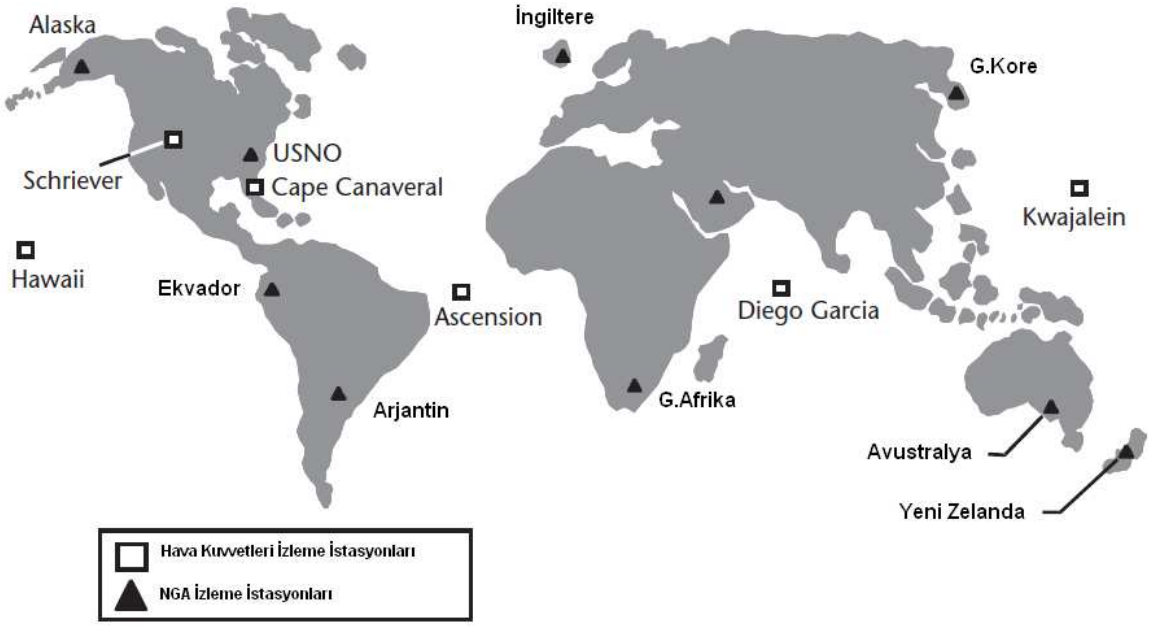
[1] GPS Satellite Constellation, http://www.gmat.unsw.edu.au/snap/gps/gps_survey/chap2/222.sats.htm.



Şekil 2.2 GPS İzleme İstasyonları ve Antenleri [9].

İzleme istasyonları ana kontrol istasyonuna GPS uydularıyla ilgili saat ve kesin yörünge bilgisi (ephemeris) gibi bilgileri sağlamaktadırlar. Ana kontrol istasyonu da gerekli düzeltmeleri yapmak için yer antenleri vasıtasıyla uydulara atomik saatlerini düzeltici bilgi göndermektedir. Böylece nanosaniyelik hassasiyet elde edilmektedir.

Bunlar dışında NGA'ya ait izleme istasyonları da bulunmaktadır [9]. Şekil 2.3'de bunların yerleri verilmektedir.



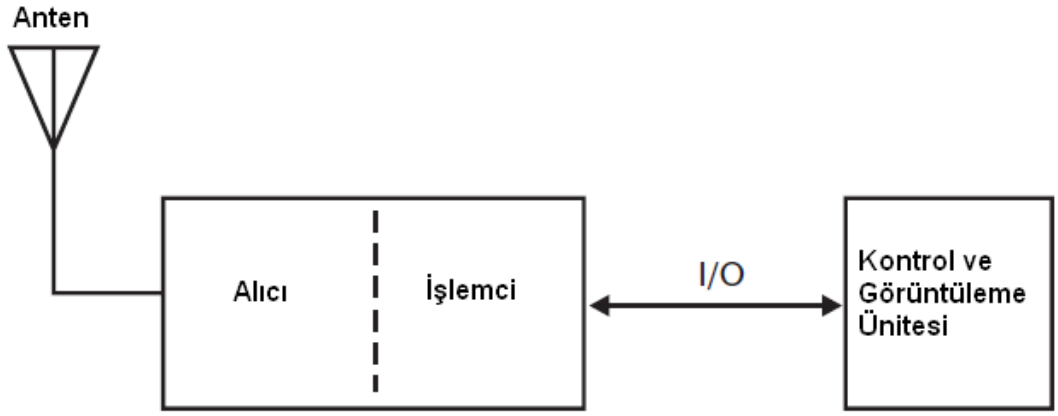
Şekil 2.3 NGA İzleme İstasyonları [9].

2.3.3 Kullanıcı Bölümü

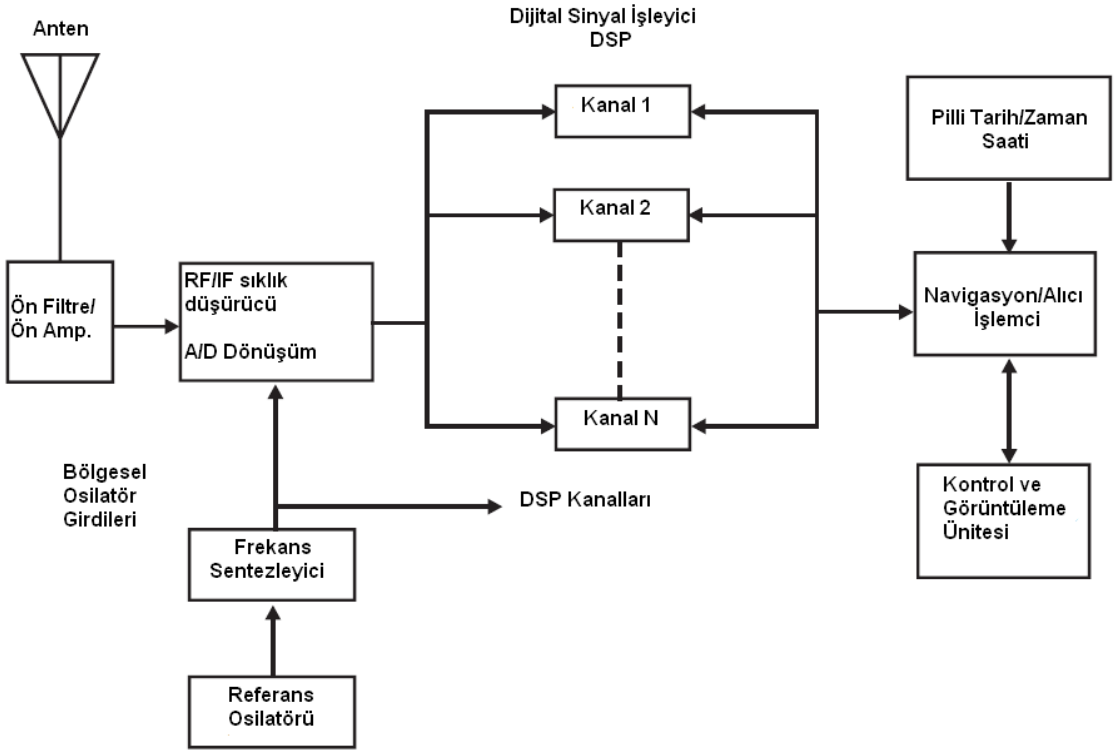
Kullanıcı bölümü ise GPS alıcılarından oluşmaktadır. Bunlar daha önce de değinildiği gibi özel GPS cihazları, GPS donanımlı telefonlar ya da üzerinde GPS yongaları barındıran özel üretim cihazlar olabilmektedir.

GPS alıcılarında L bandındaki sinyali yakalamaya yarayan bir anten bulunmaktadır. GPS donanımlı cep telefonlarında bu antenin bulunduğu yer kullanıcı el kitabında belirtilmektedir.

Şekil 2.4'de genel GPS alıcısı yapısı gösterilmektedir. Şekil 2.5'de ise tüm kullanıcılara açık olan SPS yapısı gösterilmektedir.



Şekil 2.4 Genel GPS Alıcısı Yapısı [9].



Şekil 2.5 SPS Yapısı [9].

2.4 A-GPS

GPS cihazları ilk veriyi alırken zorlanmaktadırlar. Uydulara ait durum ve zaman bilgisinin alınması gerekmektedir. Bu süre uyduların görünmesinin zor olduğu bazı durumlarda dakikalar alabilmektedir. Bu tip durumlarda GPS cihazları özellikle de GPS donanımlı cep telefonları A-GPS denen bir yöntem kullanmaktadırlar.

A-GPS cihaza başlangıç için kolaylaştırıcı veri sağlamaktadır. Mesela hangi uyduların görüldüğü bilgisi ya da zaman bilgisi buna örnektir. Böyle bir bilginin var olması cihaza kolaylıkla gelen zayıf sinyalleri değerlendirme yetisi kazandırmaktadır.

A-GPS cihaza şu bilgileri sağlayarak yardım etmektedir:

- GPS alıcısının uyduları daha hızlı görmesini sağlamak için uydulara ait almanac yani durum bilgisi
- Yüksek doğruluklu zaman bilgisi
- Kendi işlemcilerini kullanarak konum bilgisi

A-GPS bulunan cep telefonlarının birçoğunda GPS de ayrı olarak bulunmaktadır. Telefonda konum bilgisi sorgulandığında ilk önce kendi başına duran GPS aygıtına bağlanılmakta ve konum sorgulanmaktadır. Bu sorgulamanın uzun sürmesi durumunda A-GPS devreye girmektedir. Bu ilk veriyi sağladıktan sonra A-GPS aradan çekilmektedir. A-GPS kullanımı GSM operatörleri tarafından ücretlendirilmektedir. Ücret olarak standart GPRS bağlantısı ücreti alınmaktadır. A-GPS kullanan cep telefonu kullanıcılarının bu ücretlendirmeye dikkat etmeleri gerekmektedir. Çünkü bazı telefonlarda GPS'e geçiş otomatik değildir ve GPS bilgilerini A-GPS sağlamaya devam etmektedir.

3. GPRS VE 3G

3.1 GPRS

GPRS, GSM, CDMA (Kod Bölmeli Çoklu Erişim) ve TDMA (Zaman Bölmeli Çoklu Erişim) gibi ağlar üzerinde bir ağ katmanı olarak bulunan paket tabanlı veri taşıyıcı servistir. GPRS, GSM mobil istasyonları ve harici paket veri ağları arasında verimli veri transferini paket radyo prensipleri uygulayarak sağlamaktadır. Paket değişiminde veri paketlere ayrılarak gönderilmesi birbirlerinden ayrı olarak gerçekleştirilmektedir. Alıcı ucunda ise bu paketler birleştirilerek veri tekrar oluşturulmaktadır. GPRS, dünyadaki önde gelen paket tabanlı internet haberleşme protokolleri olan internet protokol (IP) ve X.25'i desteklemektedir. X.25 yoğunlukla Avrupa'da kullanılan bir protokoldür. GPRS varolan IP ve X.25 uygulamalarının cep telefonlarında çalışmasının önünü açmaktadır.

GPRS internet bağlantısının anında yüklenmesini ve sürekli bağlantı sağlanmasını gerçekleştirmektedir. GPRS kullanıcıları her seferinde bağlantı kurmalarına gerek kalmadan istediklerinde internete ya da ofis ağı gibi ağlara bağlanabilmekte ve sadece gönderdikleri ya da aldıkları veri kadar ücretlendirilmektedirler. Çünkü GPRS iki nokta arasında sürekli bir bağlantı kurmak yerine bant genişliğini sadece veri transferi olduğunda kullanmaktadır. Böylelikle varolan radyo bant genişliğinin verimli kullanılması sağlanmaktadır. Anlaşılacağı üzere GPRS devre anahtarlamalı ağlar gibi sürekli bir fiziksel bağlantı yapmadığı için ve paketler sadece ihtiyaç oldukça gönderildiği için maliyeti daha az olmaktadır.

Paket tabanlı veri transferinin bir diğer avantajı ise bant genişliğini daha az meşgul edilmesinden dolayı hızın artmasıdır. Böylelikle telefonlar için yazılan uygulamaların daha yavaş çalışan ağlara adapte edilmesi derdi ortadan kalkmaktadır.

GPRS veri hızları 14.4 kbit/s ve 115 kbit/s arasında değişmekte ve cep telefonu ve bilgisayar kullanıcıları için sürekli bir bağlantı sağlamaktadır. GPRS veri hızlarının ortalama 56 kbit/s civarında olduğu gözlenmektedir [10]. Daha yüksek hızlara ulaşılabilir ise video ve grafik uygulamalarını da destekleyebileceği düşünülmektedir. GPRS'in 3G yolunda bir aşama olduğu düşünüldüğünde 3G ile bu hız seviyesi de yakalanmıştır.

GPRS GSM'den birtakım farklarla ayrılmaktadır. GPRS, daha yüksek bant genişliği sunmaktadır, böylelikle daha yüksek hızlara çıkabilmektedir. Anında ve sürekli internet bağlantısı sağlamaktadır. Devre anahtarlamalı bir yapı yerine paket tabanlı bir yapı kullanmaktadır. Daha yüksek verimlilik ve daha düşük maliyet sağlamaktadır. GSM'den ücretlendirme yönüyle de ayrılmaktadır. Ücretlendirmelerde bağlı kalınan süre yerine transfer edilen veri miktarı gibi özellikler baz alınmaktadır. Bunun için de ağ kullanımı monitör edilmektedir.

Ticari GPRS uygulamaları 2000'li yıllarla beraber GSM operatörleri tarafından desteklenmeye başlanmıştır. Omnipoint, SmarTone ve BT Cellnet gibi firmalar bu yıllarda GPRS servisini sunacaklarını açıklayan ilk firmalardandır [10].

GPRS teknolojisiyle beraber GSM operatörlerinin de yapması gereken bir takım uygulamalar ve tarifeler; alması gereken de bir takım önlemler olmuştur. Daha gelişmiş planlar sunmak bunların başında gelmektedir. Yeni tarifeler uygulayarak ellerindeki aboneleri tutmak ve yeni aboneler çekmek için maliyet verimliliğini arttırmak da bunlardan sayılabilmektedir. Operatörlerin bant genişliğinin birçok kullanıcı tarafından aynı anda kullanılabiliyor olmasından dolayı aşırı bir önlem almalarına gerek kalmamaktadır.

Kullanıcılar için ise yeni servislerin olması, hızlı bir bağlantı sağlanması, maliyetin verimli olması ve aynı anda konuşma ve veri transferinin sağlanabiliyor olması önem kazanmaktadır.

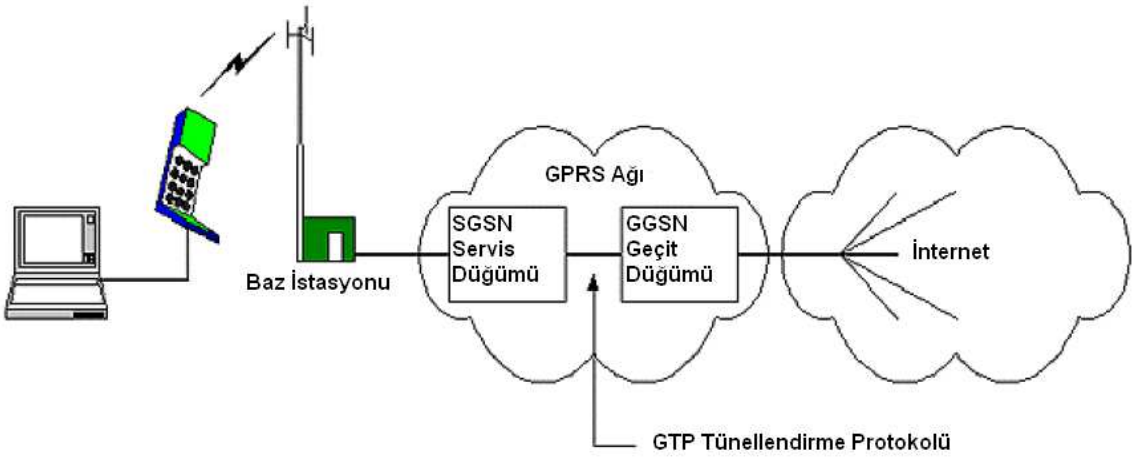
Kullanıcılar GPRS servislerinden yararlanabilmek için bu servisleri destekleyen bir telefona ihtiyaç duymaktadırlar. Ayrıca servis ayarlarının yapılmış olması gerekmektedir.

GPRS servisini sunmak için servis operatörlerinin bir GPRS network katmanını kurmuş olmaları gerekmektedir. Şekil 3.1'de GPRS ağının genel yapısı gösterilmektedir.

SGSN (Servis GPRS Destek Düğümü), GSM içinde veri alışverişini sağlayan ve servis alanı içindeki kullanıcıların bilgisini tutan düğümdür. SGSN, kullanıcıları izlemekte, onları onaylamakta ve onların faturalandırma bilgilerini toplamaktadır.

GGSN (Ağ Geçidi GPRS Destek Düğümü), internet protokolü gibi ağlara olan bağlantı arayüzüdür.

Ücretlendirme Geçidi, ücretlendirme sistemiyle GPRS arasında arayüzdür.

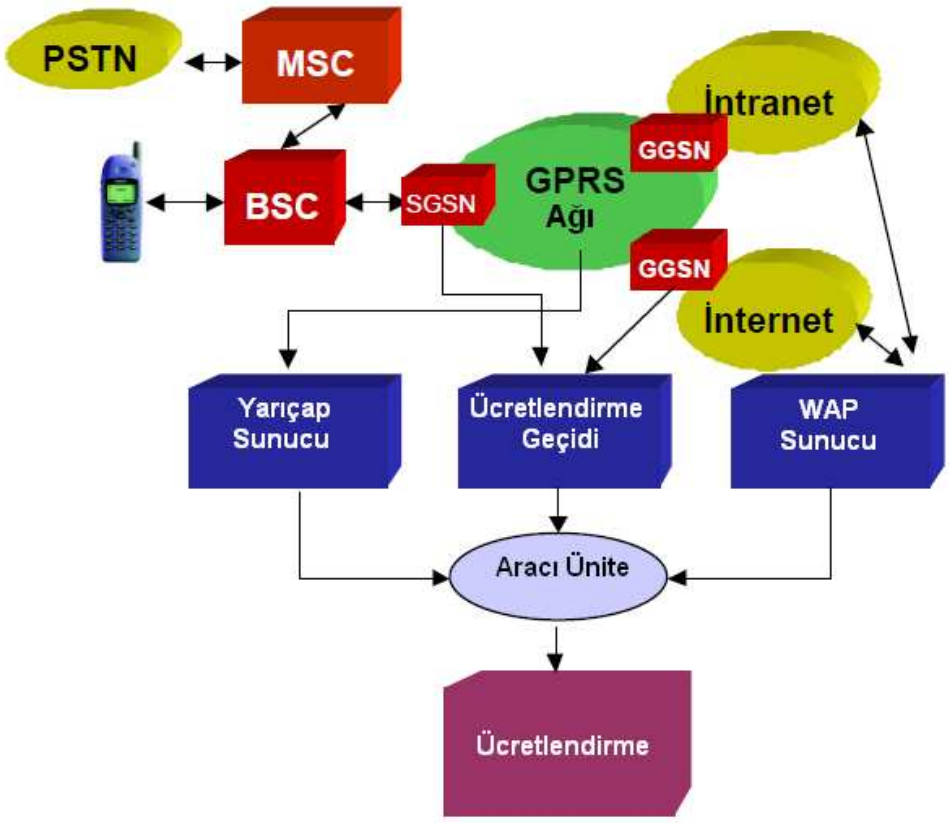


Şekil 3.1 GPRS Network Yapısı [10].

GPRS tünellendirme protokolü (GTP, GPRS Tünel Protokolü), SGSN ve GGSN'yi birbirine bağlamaktadır.

Bunların dışında GPRS ağının çalışması için baz istasyonu sistemi ve ev yer yazmacı kurulu olması gerekmektedir.

GPRS'nin mimari yapısı Şekil 3.2'de verilmektedir.



Şekil 3.2 GPRS'nin Mimari Yapısı [10].

GPRS'nin çalışmasını bir örnekle açıklayabiliriz. Diz üstü bilgisayarına cep telefonu bağlanmış olan bir iş adamını düşünelim. GPRS özellikli cep telefonu baz istasyonuyla irtibata geçer. Baz istasyonu SGSN ile irtibatlıdır. SGSN internet protokolü gibi diğer bağlantılarla haberleşmeyi sağlayan GGSN ile irtibata geçer. Veriler buradan gönderilir ve tekrar alınır. IP paketler alındıktan sonra GGSN tarafından SGSN'ye iletilir. Buradan da mobil cihaza gönderilir. SGSN ve GGSN bu paketleri birbirleri arasında göndermek için özelleşmiş bir protokol olan GTP'yi kullanırlar [10]. Kullanıcı basit bir bağlantı yaptığını düşünürken ağ içinde bağlantılar açılıp kapanmaktadır.

GPRS konuşmanın iletiminin sağlandığı bandı kullanmaktadır. Bu bandın genişliği 200 kHz'dir. Bu kanal 271 kbit/s'dir ve 8 parçaya ayrılmaktadır. Parçaların her biri ortalama 34 kbit/s civarındadır. Veri doğrulama bilgileriyle birlikte her biri 13-14 kbit/s veri taşımaktadır. Geriye kalan kısmı ise GPRS kullanarak 100 kbit/s'ye çıkabilmektedir. Ortalama hız 56 kbit/s'dir [10].

GPRS hakkındaki bu bilgiler düşünüldüğünde tez kapsamında GPRS gibi bir internet bağlantısının kullanılması gerektiği ve verilerin telefondan sunucuya gönderilmesinde yeterli olacağı değerlendirilmiştir. Cep telefonu ile yapılan denemeler sırasında da düzgün çalıştığı gözlenmiştir.

3.2 3G

GPRS'ten başka 3G de yaygınlaşmaya başlamıştır. Henüz GPRS kadar her telefonda yaygın olarak kullanılmamaktadır. 3G'nin tam belli bir tanımı olmamakla beraber GPRS'e göre daha hızlı veri iletişimi sağlayan bir ağ olduğunu söylemek mümkündür. İndirmede 14.4 Mbit/s ve yüklemede 5.8 Mbit/s hızlarına erişebilmektedir[1].

3G ilk defa 2001 yılında Japonya'da kullanılmıştır. Türkiye'de ise 2009 yılından beridir kullanılmaktadır. 3G ile cep telefonlarında mobil tv, görüntülü konuşma gibi uygulamalar da rahatlıkla gerçekleştirilebilmektedir.

[1] 3G-HSPA, UMTS High Speed Packet Access Tutorial, http://www.radio-electronics.com/info/cellulartelecomms/3g-hspa/umts-high-speed-packet-access-tutorial.php.

4. KRİPTOGRAFİ

4.1 Giriş

Gizli yazı anlamına gelen kriptografi bilginin gizlenmesini konu alan bilim dalıdır. Kriptografi matematik, bilgisayar ve elektronik bilimleriyle de içli dışlıdır. Eskiden özellikle diplomasi ve savaşlarda kullanılmasına karşın günümüzde bankalardan günlük bilgisayarlara kadar birçok alanda kullanıma girmiştir.

Bu bilimin temel amacı bir metnin saklanması ve onun sadece yetkili kişiler tarafından okunmasının sağlanmasıdır. Birçok insanın okuma yazma bilmediği eski çağlarda basit yöntemler kullanılmış iken, bugün süper bilgisayarların varlığında kriptografi algoritmaları da olabildiğince kompleks hale gelmiştir.

Teoride bu kompleks algoritmalarla oluşturulmuş şifrelenmiş metinler kırılamaz veya çözülemez değildir, yalnız bu çözme işlemi bilgisayarların varlığında bile algoritmanın zorluğuna dayanarak haftalar ya da yıllar sürebilmektedir. Kırılamaz yapılmaya çalışıldıkça bu algoritmaların da bilgisayarda ya da başka bir cihazda uygulanması da çok zor hale gelmektedir. Bunun için uygulanabilirliği olan ama kırılması çok uzun zaman alabilecek algoritmalar geliştirilmiştir ve geliştirilmektedir.

Kriptografi biliminde şifrelenmemiş, herkes tarafından okunabilir metne açık metin; şifrelenmiş metne ise şifre metni denilmektedir. Açık metinden şifre metnine çevirme işlemine şifreleme, şifre metnini tekrar açık metne çevirme işlemine de şifre çözme denilmektedir. Çoğu kripto algoritmasında şifreleme ve şifre çözme hem şifreleyen hem de çözenin üzerinde önceden anlaştığı ve üçüncü şahıslardan gizli tuttukları bir anahtar ile yapılmaktadır. Esasında şifreleme algoritmaları birçok insan tarafından bilinmekte ve çalışılmaktadır. Şifrelenmiş metnin kırılamaz olmasını ve tekil olmasını sağlayan kullanılan anahtardır. Mesela DES (Veri Şifreleme Standartı) algoritmasıyla şifrelenmiş bir metnin DES ile şifrelendiğini bilen bir saldırganın metni çözmesi algoritmayı bilmesine rağmen anahtarı bilmediği için süper bilgisayarlar ile çok uzun vakit almaktadır.

Kod, kriptografi algoritmalarındaki şifreleme yapısıyla karıştırılmamalıdır. Burada mesela bir askeri birlik tarafından yapılacak saldırı taktiği ve yöntemi bir kod ile

belirlenmekte ve o kod ile emir verilerek söz konusu taktiğin gerçekleştirilmesinin gerekliliği bildirilmektedir.

Kriptografi biliminde çağlar boyu birçok yöntem kullanılmıştır. Bir cümlenin harflerinin yerlerini değiştirme en basit yöntemlerden olmuştur. Sezar'ın komutanlarıyla haberleşmek için kullandığı meşhur Sezar şifrelemesinde metindeki her harf alfabede kendisinden üç sıra sonra gelen harf ile değiştirilmektedir. Mesela "şifre" kelimesi Türkçe alfabede Sezar şifrelemesi ile "ülıth" halini almaktadır. Bu metni alan kişi bunun Sezar şifrelemesiyle şifrelendiğini bilmekte ve açık metni elde edebilmektedir.

Bir diğer yöntem de her bir harfi başka bir harf ile değiştirmek olmuştur. Bu yöntem de Sezar şifrelemesinin değişik bir uygulamasıdır ama harfler arasında belli bir sıra ile değil, karışık bir eşleştirme bulunmaktadır. Bu tip harf değişikliklerine dayalı şifreli metinlerin çözümlenmesinde harflerin kullanım sıklığından yani frekanslarından yararlanılmaktadır. Her dilin kendine göre bir harf frekansı vardır. Buradan yola çıkarak hangi harf daha sıklıkla kullanılmışsa o harf kullanım frekansı yüksek olan harflerden birine denk gelmektedir yorumu çıkartılabilmektedir.

Modern kriptografide iki önemli şifreleme yöntemi bulunmaktadır. Bunlar simetrik anahtarlı ve asimetrik (açık) anahtarlı şifrelemedir.

Tez kapsamında bir simetrik anahtarlı şifreleme yöntemi olan AES (Gelişmiş Şifreleme Standartı) kullanıldığı için ilk önce diğer şifreleme yöntemi olan asimetrik anahtarlı şifrelemeye kısaca değinilecek, daha sonra simetrik anahtarlı şifreleme ve özellikle AES şifreleme algoritması detaylı bir şekilde incelenecektir.

4.2 Asimetrik Anahtarlı Şifreleme

Asimetrik şifreleme algoritmaları anahtar paylaşımının güvenli olmayan kanal üzerinde yapılmasını sağlamak amacıyla doğmuştur. Bu algoritmalara açık anahtarlı şifreleme algoritmaları da denilmektedir.

Bu tip algoritmalarda bir taraf açık bir anahtar üretmektedir. Bu anahtarla ilişkili olan ama başkası tarafından üretilemeyen bir de gizli anahtar üretilmektedir. Açık anahtar ile bu kişiye şifrelenmiş bilgi gönderilebilmektedir. Ama bu bilginin okunması için gizli anahtar gerekmektedir.

Buna benzer bir durum herkes tarafından kullanılan posta kutularında gözlenebilmektedir. ABD'de belli yerlerde herkesin kullanabileceği posta kutuları bulunmaktadır. Buraya herkes postasını atabilmektedir. Bu postayı kutuya atma işleminde herkesin açık bir hakkının olduğu görülmektedir. Kutunun kapağını açma işlemi de açık anahtarlama olarak düşünülebilir. Ama bu postalara, o kutuyu açma yetkisine ya da posta kutusunu açacak anahtara sahip olan görevliden başkası erişememektedir. Burada görevlinin sahip olduğu anahtar gizli anahtardır. Aynı şekilde dilek şikayet kutuları da bu şekilde zihinde canlandırılabilir. Herkes dilek ve şikayetini oraya atabilirken sadece anahtara sahip kişi açıp okuyabilmektedir.

Bu yaklaşım ilk defa 1976'da Whitfield Diffie, Martin Hellman ve Ralph Merkle tarafından ortaya atılmıştır [11]. Daha sonra benzer mantığı kullanan algoritmalar geliştirilmiştir. Şu anda yaygın olarak kullanılan algoritmalar Diffie-Hellman, RSA ve El Gamal'dır.

4.3 Simetrik Anahtarlı Şifreleme

Simetrik şifrelemede şifreleme için alıcı ve verici tarafın ortak olarak bildikleri gizli bir anahtar kullanılmaktadır. Simetrik şifreleme algoritmaları kriptolamanın varlığından itibaren kullanılagelmiştir. Kullanılan algoritmalara DES, 3DES (Üçlenmiş DES) ve AES örnek olarak verilebilir.

Şifreleme algoritmaları simetrik ve asimetrik anahtarlı olarak ayrılabildiği gibi akış ve blok şifrelemeler olarak da ayrılabilmektedir. Akış şifrelemede anahtar uzunluğu şifrelenecek metin kadar uzundur. Bundan dolayı kısa metinler dışında kullanışlı değildir. Akış şifrelemede her bir bit ayrı ayrı şifrelenmektedir. Blok şifrelemede ise AES'te olduğu gibi 128 bitlik bloklar ya da DES'te olduğu gibi 64 bitlik bloklar kullanılmaktadır.

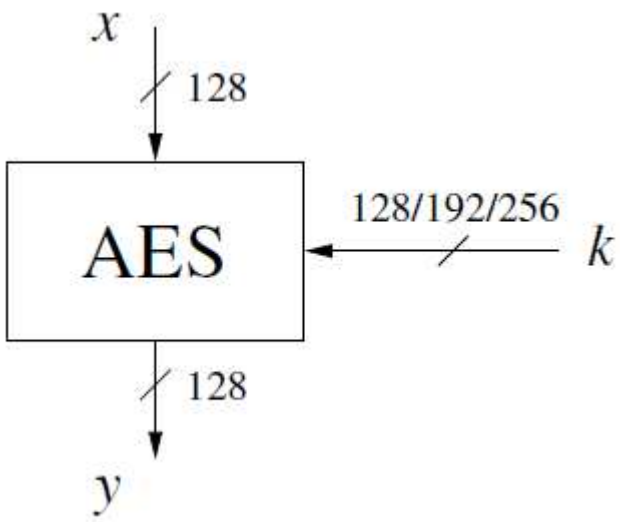
DES simetrik ve blok şifreleme algoritmalarının en önemlilerindendir. Günümüzde bu algoritmanın kırılmasından dolayı geçerliliği kalmamıştır ama yine de kullanılmaktadır. DES için, NIST (Ulusal Standartlar ve Teknoloji Enstitüsü) 1973 ve 1974 yıllarında iki defa böyle bir şifreleme standardının gerekliliğine yönelik talep yapmıştır. DES, IBM (Uluslararası İş Makineleri)'deki bir takım tarafından Lucifer'in üzerine geliştirilmiştir. Takımda Walter Tuchman, Don Coppersmith ve Lucifer'in uygulayıcısı Horst Feistel gibi isimler yer almaktadır [11].

DES'in ardından 3DES, DESX gibi algoritmalar da geliştirilmiştir. 1997 yılında NIST yeni bir standart geliştirilmesi için bir yarışma açmıştır. DES'in kırılmış olması ve 3DES'in güçlü olmasına rağmen bilgisayar uygulamalarının yavaş olması bunda etken olmuştur. Ayrıca bilgisayar teknolojisindeki ilerleme de göz önünde bulundurularak yakın bir gelecekte quantum bilgisayarlarıyla bu algoritmaların kırılabileceği değerlendirilmiştir. Bu gibi nedenlerle yarışma açılmış ve katılan algoritmalar içinden seçilen algoritma 2001 yılında yeni standart olan AES olarak belirlenmiştir [11]. AES hakkında bahsedilen daha güvenli ve daha hızlı olması gibi nedenlerden dolayı bu tez kapsamında GPS verilerinin şifrelenmesi ve çözülmesinde AES algoritmasının kullanılmasına karar verilmiştir.

4.4 AES-Rijndael

Rijndael algoritması iki Belçikalı kriptocu Joan Daemen ve Vincent Rijmen tarafından geliştirilmiştir. 2001 yılında yeni AES standardı haline gelmiş ve AES-Rijndael ya da AES olarak anılmaya başlanmıştır [11].

Blok şifreleme büyüklükleri 128 bittir. Anahtar uzunlukları 128, 192 ya da 256 bit olarak belirlenebilmektedir. Şekil 4.1'de AES'in genel şeması gösterilmektedir.



Şekil 4.1 AES Genel Şeması.

Telefon yazılımı kısmında bahsedileceği gibi 128 bitlik anahtar uzunluğu standart olarak SATSA (Güvenlik Servisleri API) standartına sahip her telefonda

uygulanabilmekteyken diğer anahtar uzunluklarının uygulanması için telefona özel paketlerin yüklenmesi gerekmektedir[1].

Anahtar uzunluğuna göre AES algoritmasının iç döngü miktarı Çizelge 4.1'de gösterilmektedir.

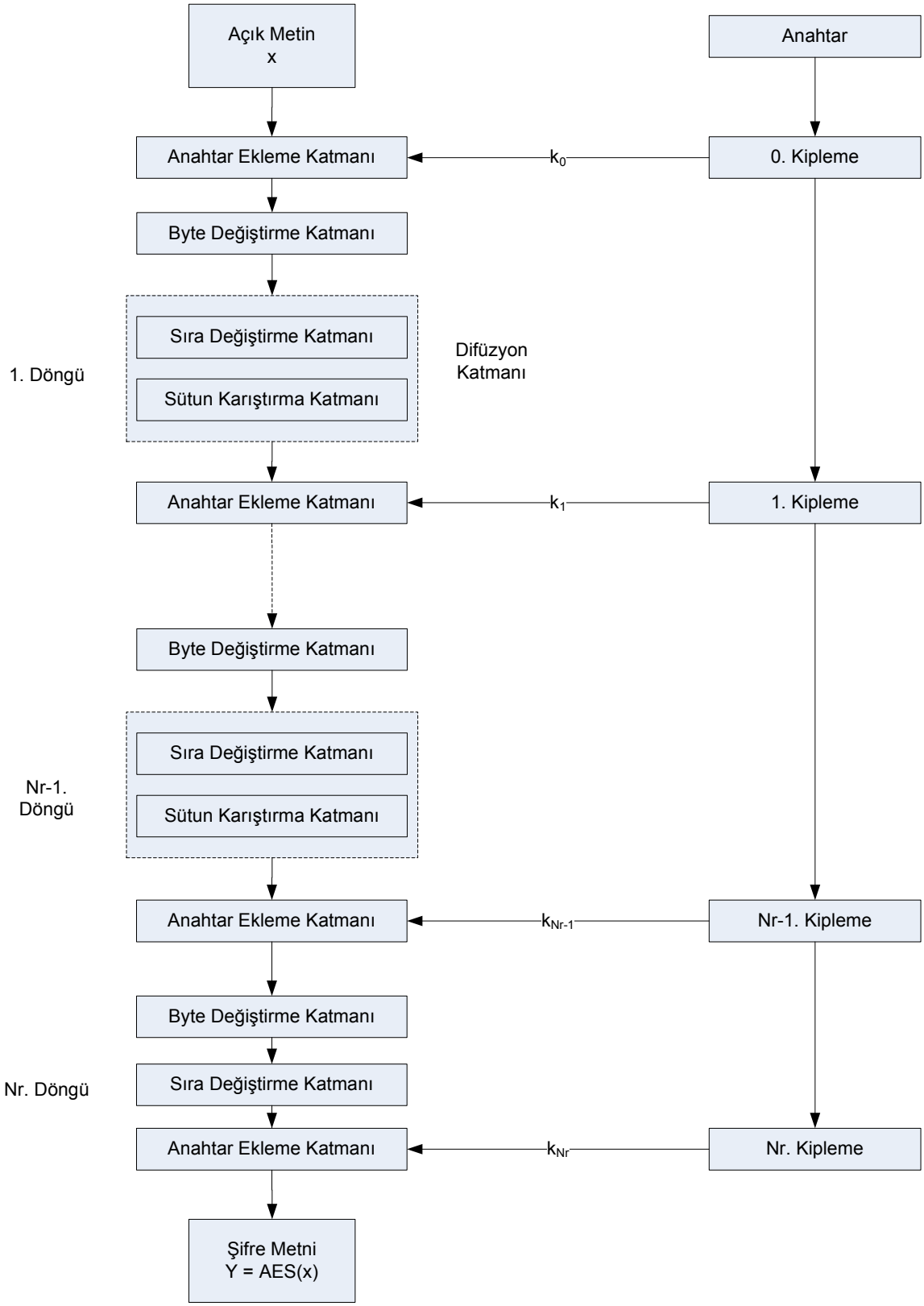
Anahtar Uzunlukları	Döngü Sayısı
128 Bit	10
192 Bit	12
256 Bit	14

Çizelge 4.1 AES İç Döngü Miktarları.

4.4.1 Şifreleme

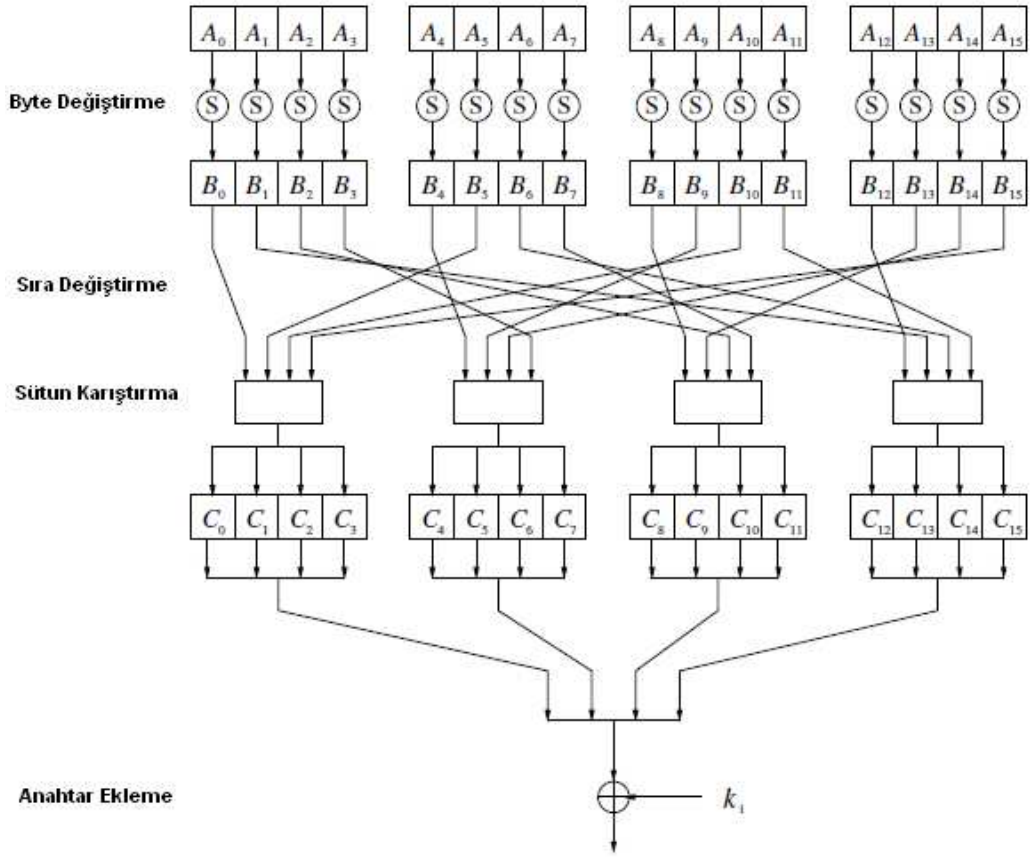
AES şifreleme bloğu diyagramı Şekil 4.2'de verilmektedir. Başlangıçta Anahtar Ekleme Katmanı (Key Addition Layer) bulunmaktadır. Sonrasında birbirinin aynısı olan toplam döngü sayısının 1 eksiği kadar döngü bulunmaktadır. Bunlar Byte Değiştirme Katmanı (Byte Substitution Layer), Sıra Değiştirme Katmanı (Shift Rows Layer) ve Sütun Karıştırma Katmanı'ndan (Mix Column Layer) oluşan Difüzyon Katmanı (Diffusion Layer) ve Anahtar Ekleme Katmanıdır. Şifrelemede en son döngüde Sütun Karıştırma Katmanı bulunmamaktadır.

[1] Using AES with JAVA Technology, http://java.sun.com/developer/technical/Articles/Security/AES/AES_v1.html.



Şekil 4.2 AES Şifreleme Blok Diyagramı.

Her döngünün iç yapısı Şekil 4.3'de verilmektedir. Bu döngünün her bir katmanının yapısı incelenecektir.



Şekil 4.3 AES Döngü Yapısı [11].

4.4.1.1 Byte Değiştirme Katmanı

Byte Değiştirme Katmanında S-Kutusu'nda belirlenmiş olan karşılıklarıyla her bir byte değiştirilmektedir. Bu işlem yazılımlarda Şekil 4.4'deki hazır tablodan yararlanılarak gerçekleştirilirken, donanım tasarlamalarında (4.1)'deki matematiksel formül uygulanmaktadır. Burada B_i' olarak gösterilmiş bitler döngüye giren A_i'nin Galois alanında çarpmaya göre tersidir.

$$\begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \\ B_4 \\ B_5 \\ B_6 \\ B_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} B'_0 \\ B'_1 \\ B'_2 \\ B'_3 \\ B'_4 \\ B'_5 \\ B'_6 \\ B'_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \bmod 2 \qquad \textbf{(4.1)}$$

									y							
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
x 8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Şekil 4.4 S-Kutusu [11].

Mesela B7 baytı değiştirilecek ise S-Kutusundaki karşılığına bakılıp A9 olarak değiştirilir.

4.4.1.2 Difüzyon Katmanı

Difüzyon Katmanı iki alt katmana ayrılmaktadır. Bunlar Sıra Değiştirme Katmanı ve Sütun Karıştırma Katmanıdır. Sıra Değiştirme Katmanında 16 Byte büyüklüğündeki Çizelge 4.2'de verilen blok, birinci sıra aynı bırakılarak, ikinci sıra 1 sola, üçüncü sıra 2 sola ve dördüncü sıra 3 sola kaydırılacak şekilde değiştirilmektedir.

B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

Çizelge 4.2 16 Byte'lık Blok.

Kaydırmalar sonucunda Çizelge 4.3'deki blok elde edilmektedir.

B_0	B_4	B_8	B_{12}
B_5	B_9	B_{13}	B_1
B_{10}	B_{14}	B_2	B_6
B_{15}	B_3	B_7	B_{11}

Çizelge 4.3 Kaydırılmış Blok.

Sütun Karıştırma Katmanında bir matris çarpımı yapılmaktadır. (4.2)'de bu çarpım tek bir sütun için gösterilmektedir.

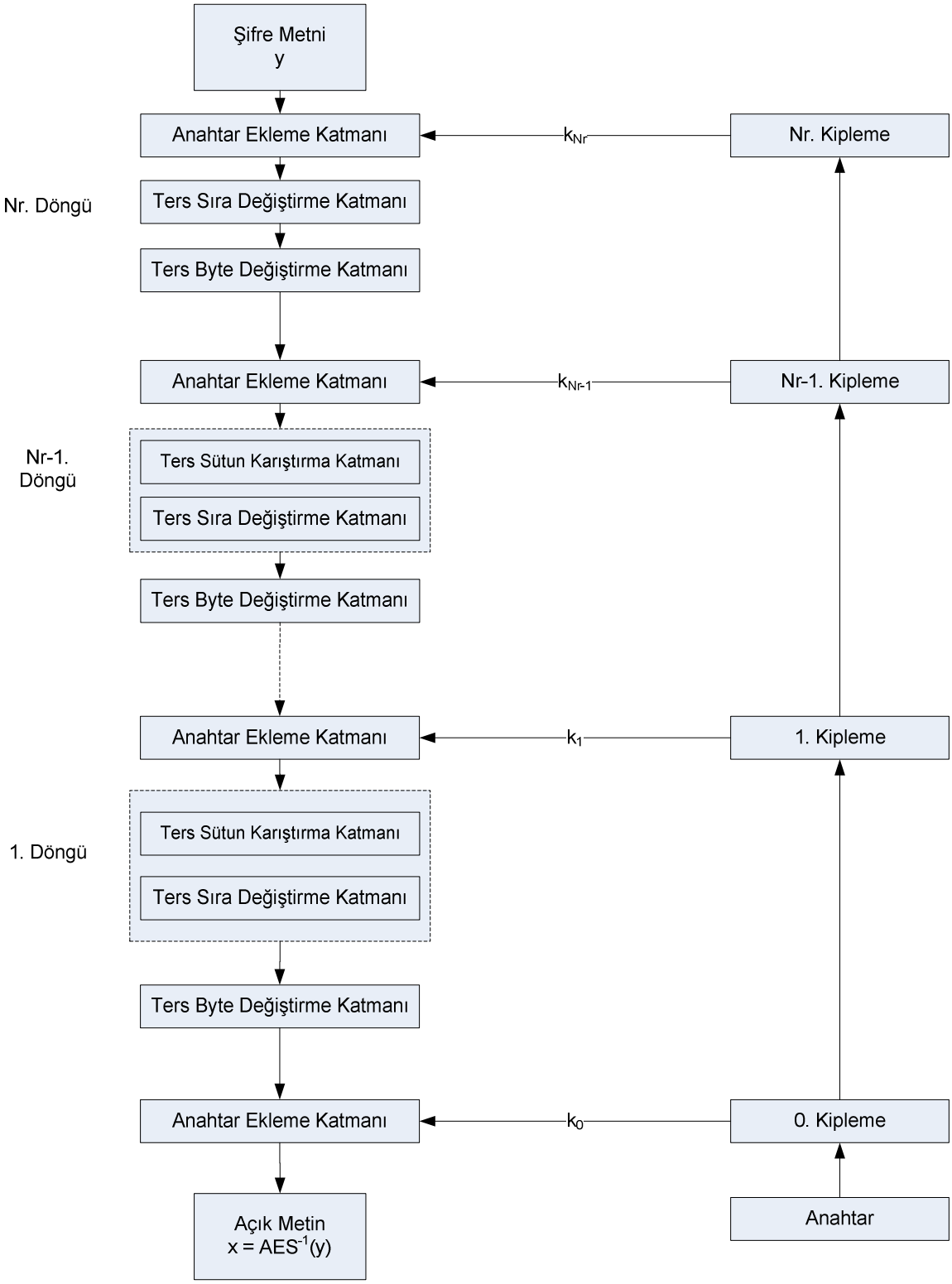
$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix} \quad \textbf{(4.2)}$$

4.4.1.3 Anahtar Ekleme Katmanı

Anahtar Ekleme Katmanı bit-bit XOR işlemidir. Bu katmanda Difüzyon Katmanının sonucu ile anahtar XOR işleminden geçirilmektedir.

4.4.2 Şifre Çözme

Şifre çözme, şifreleme bloğunun tam tersi olduğu için onda da ilk döngüde sütun karıştırma katmanı bulunmamaktadır. Son döngüden sonra ise anahtar ekleme katmanı bulunmaktadır. Kısaca şifre çözmede, ilk döngü hariç, her döngüde anahtar ekleme katmanı, ters sütun karıştırma katmanı, ters sıra değiştirme katmanı ve ters byte değiştirme katmanı yer almaktadır. Şekil 4.5'de şifre çözme bloğu diyagramı verilmektedir.



Şekil 4.5 AES Şifre Çözme Blok Diyagramı.

Anahtar ekleme katmanı, şifrelemede olduğu gibi XOR işleminden oluşmaktadır. Diğer katmanlar ise şifrelemedekilerin tersidir.

4.4.2.1 Ters Sütun Karıştırma Katmanı

Burada sütun karıştırma işleminin tersi alınması için matrisin de tersi kullanılmaktadır. (4.3)'de bu işlem gösterilmiştir.

$$\begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \end{pmatrix} = \begin{pmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix} \begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} \quad \textbf{(4.3)}$$

4.4.2.2 Ters Sıra Değiştirme Katmanı

Burada sıra değiştirme katmanının tam tersi bir işlem uygulanmaktadır. İlk sıra hiç kaydırılmamaktadır. İkinci sıra bir sağa kaydırılmakta, üçüncü sıra iki sağa kaydırılmakta, son sıra ise üç sağa kaydırılmaktadır.

4.4.2.3 Ters Byte Değiştirme Katmanı

Bu katmanda byte değiştirme katmanındaki tablonun tersi uygulanmaktadır. Matematiksel formüller kullanılmak istendiğinde (4.4)'deki formül uygulanıp sonucun Galois alanındaki tersi alınması gerekmektedir.

$$\begin{pmatrix} B'_0 \\ B'_1 \\ B'_2 \\ B'_3 \\ B'_4 \\ B'_5 \\ B'_6 \\ B'_7 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \\ B_4 \\ B_5 \\ B_6 \\ B_7 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \bmod 2 \quad \textbf{(4.4)}$$

4.5 ECB

ECB (Elektronik Kodkitabı), her bloğun aynı anahtar ile şifrelenmesi durumudur. Şifrelenecek bilginin kısa olmasından dolayı büyük metinlerde olabilecek tekrarlamaların meydana gelmeyeceği değerlendirilmektedir. Bundan dolayı da tek bloğun şifrelenmesi durumunda CBC (Şifre Blok Zincirlemesi) gibi diğer bazı yöntemlerle aynı sonucu verecektir.

5. KONUMLANDIRMADA HARİTA KULLANIMI

5.1 Giriş

Koordinatı bilinen bir yerin nerede olduğuna görsellik kazandırılmak istendiğinde haritalar kullanılmaktadır. Günümüzde internette birçok harita uygulaması bulunmaktadır. Bunlar adres öğrenmek, yol tarifi almak gibi amaçlarla kullanılmaktadır.

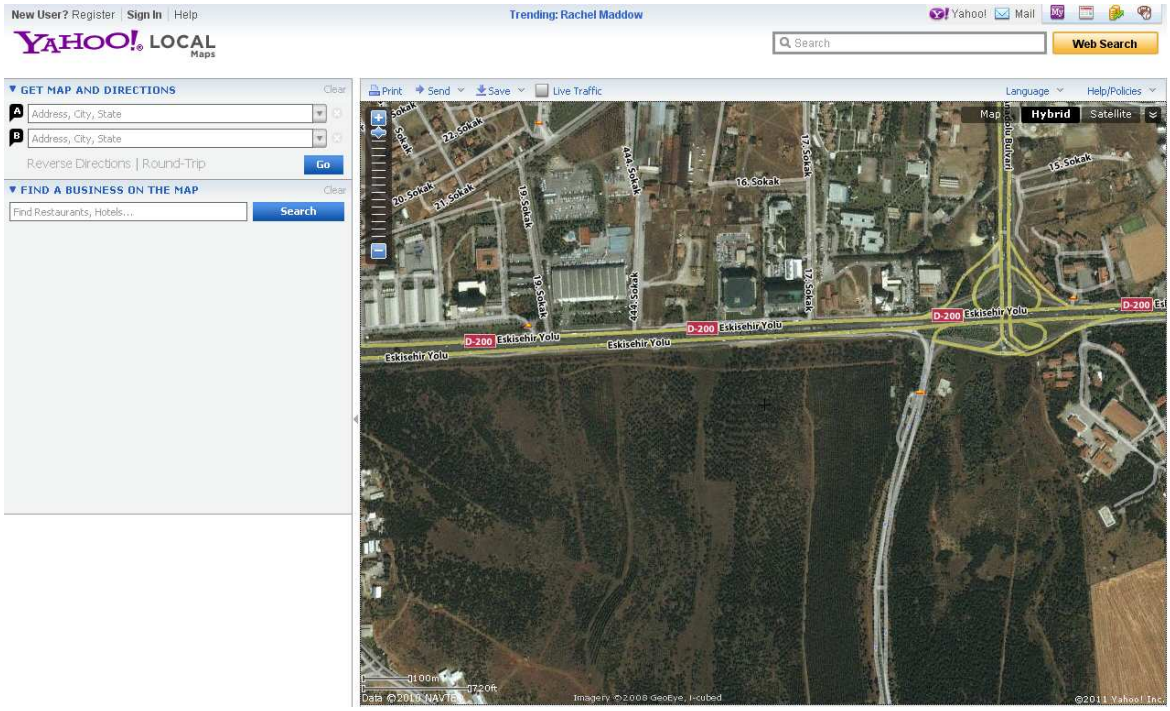
İnternette kullanıcıların ve yazılımcıların kullanımına sunulmuş birçok harita uygulaması bulunmaktadır. Bunların en popüler olanları Google Maps, Yahoo Maps, Bing Maps ve Map Quest'tir. Bunlar parasız kullanılabilen uygulamalardır. Ayrıca Map Xtreme gibi paralı uygulamalar da bulunmaktadır.

Bunların birçoğu üzerinde harita tabanlı uygulamalar geliştirilebilmektedir. Google Maps başta olmak üzere Bing Maps ve Yahoo Maps, haritaların başka bir web sitesine gömülmesine olanak sağlayan API'ler sunmaktadırlar. Bu firmalar, ticari amaç gütmeyen uygulamalar için kullanıcılardan herhangi bir ücret talep etmemektedirler.

Bu tez kapsamında kullanılan harita uygulaması olarak seçilmiş olan Google Maps'e geçmeden önce varolan diğer harita uygulamalarına değinilecektir.

Yahoo, Yahoo Maps uygulamasını 16 Mayıs 2007'de sunmuştur. Bu uygulama, Cartifact isimli bir şirket tarafından üretilmiştir[1]. Yahoo Maps ABD ve Kanada için yol tarifi bilgisi de sağlamaktadır. Bu ülkeler dışındaysa Yahoo Maps'in yetersiz olduğunu söylemek mümkündür. Yol haritaları ve uydu resimleri oldukça eskidir. Mesela Ankara'daki birçok bina, bahçe ve yol bulunmamaktadır. Bu şartlar altında koordinatları verilen bir yer, eski bir harita üzerinde gösterileceği için şu anki durumu da yansıtamayacaktır. Yahoo Maps'e ait bir Ankara haritası Şekil 5.1'de verilmiştir. Bu haritadan bilgilerin güncel olmadığı gözlenebilmektedir.

[1] The Map Room: Yahoo Moves to New Map Platform, http://www.maproomblog.com/2007/05/yahoo_moves_to_new_map_platform.php.

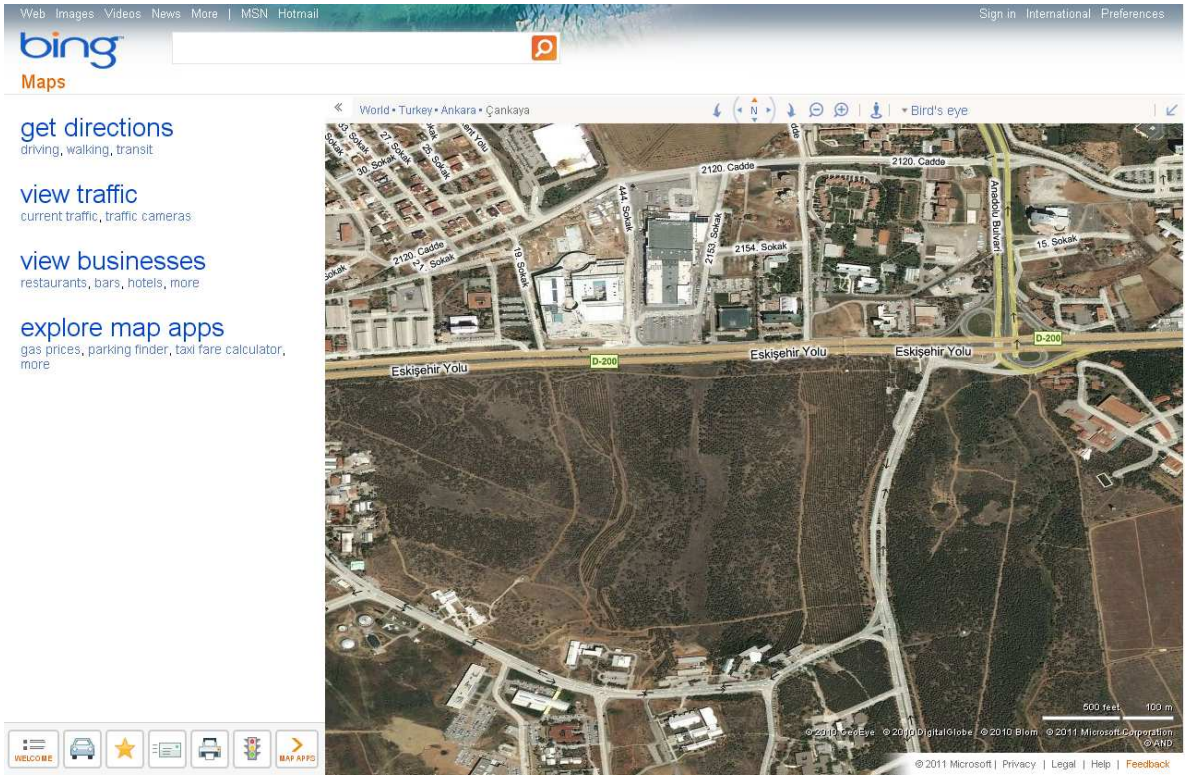


Şekil 5.1 Yahoo Maps'te Ankara'dan Bir Bölgenin Gösterimi.

Yahoo Maps'in dışında popüler bir uygulama olarak Bing Maps bulunmaktadır. Bing Maps Microsoft'a ait bir uygulamadır. Bu harita uygulaması Aralık 2005'te ilk defa Windows Live Local adıyla kullanıma sunulmuştur. 2009 Haziranında ise Bing Maps adını almıştır[1]. Performans olarak Google Maps kadar hızlı değildir ama kullanım bakımından Google Maps'e en yakın uygulamadır. Günlük kullanıma yönelik ABD için bazı şehirlerde trafik yoğunluğu verme gibi güzel uygulamaları vardır. Uygulama geliştirilmesine el veren Bing Maps Platform kararlı sürümünü 2008 sonlarında yayınlamıştır[1]. Ayrıca uygulama geliştirmek için yazılımcıların Bing Maps'e üye olup bir hesap açmaları gerekmektedir. Bu bakımdan Google Maps API'nin en son versiyonundan da ayrılmaktadır. Google Maps API artık eski versiyonlarında olduğu gibi herhangi bir üyelik istememektedir. Ayrıca Bing Maps, Microsoft ürünü olmasından dolayı gelecekte ücretlendirme konusunun nasıl olacağı da kullanıcılarda şüphe uyandırmaktadır. Çünkü Google çıkış ilkesiyle bilginin ücretsiz olması gerektiği görüşünü benimsemiş bir şirkettir ve Google Maps servisini de API'leri ve kütüphaneleri dahil ücretsiz sunmaktadır. Bing Maps'in bir negatif yanı da haritaların Google Maps'in haritaları kadar güncel olmamasıdır. Yahoo Maps gibi bu uygulamada da bir yerin haritada gösterilmesi

[1] Bing Maps 2011, http://bingmaps2011.blog.com.

durumunda Yahoo Maps kadar eski olmasa da Google Maps'e göre eski bir harita kullanılmaktadır. Bing Maps'e ait bir Ankara haritası Şekil 5.2'de verilmektedir. Bu haritanın da güncel olmadığı gözlemlenmektedir. Google Maps'ten bahsedilmeye başlandığında aynı yerin Google Maps ile oluşturulmuş haritası da verilecektir.



Şekil 5.2 Bing Maps'te Ankara'dan Bir Bölgenin Gösterimi.

Ayrıca Bing Maps'te mesela "Hacettepe" kelimesi arandığında hiçbir sonuç döndüremezken Google Maps, Hacettepe Üniversitesi, Hacettepe Hastanesi ve Hacettepe Spor Kulübü gibi birçok alternatifin bulunduğu sonuçları döndürmektedir. Bu özellik de bir kullanıcı açısından önemlidir. Özetle Google Maps diğer uygulamalara göre ABD ve Kanada dışındaki ülkeler için daha güncel haritalar kullanmaktadır. Ayrıca geliştirme için API ve kütüphaneler ile yazılımcılara sunduğu deneyim daha kullanışlıdır.

5.2 Google Maps

Google Maps iki Danimarkalı kardeş Lars ve Jens Rasmussen tarafından geliştirilmiştir. İkisi Sydney'de Where 2 Technologies isminde harita çözümleri üreten bir şirket kurmuşlardır. Ekim 2004'te şirket Google tarafından satın alınmıştır. Daha sonra yine bu iki kardeş Google Maps'i üretmişlerdir [12].

Şubat 2005'te Google Maps bir Google bloğunda duyurulmuştur [12]. O zamana kadar olan harita çözümleri genelde yüksek kapasiteli harita sunucularına ihtiyaç duymaktaydı. Ayrıca harita sürükleme özelliği de ilk defa Google Maps ile eklenmiştir.

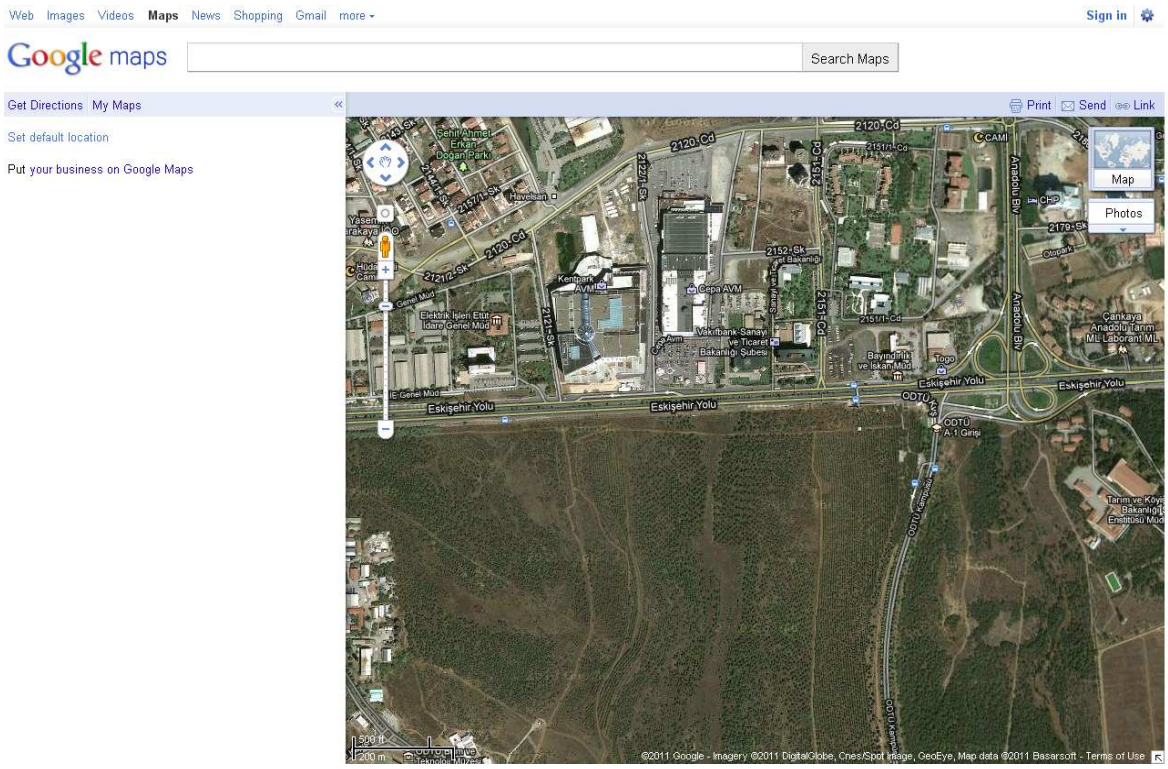
Google Maps javascript, HTML ve CSS'in beraber çalışmasıyla elde edilmektedir. Haritalar ise AJAX ile güncellenmekte ve sayfaya gelmektedir. Bir yer, harita üzerinde işaretlendiğinde ise harita tamamen güncellenmeyip sadece üzerine bir katman daha eklenmektedir.

Google Maps'in kullanımının ücretlendirilmesine yönelik iki farklı uygulama vardır. Google Maps uygulamasını web sitelerinde yer vermek isteyen kullanıcılar sitelerine erişim ücretsiz ise ve site herkese açıksa herhangi bir ücret ödemeleri gerekmemektedir. Ayrıca web sitelerinde kullanıcılarının girmesi için şifre isteyen siteler de bu şifreleri ücretsiz sağlıyorlar ise herhangi bir ücretlendirmeye tabi tutulmadan Google Maps uygulamasını web sitelerinde kullanabilmektedirler. Web sitelerinin kullanımı ücrete tabi tutulan ya da Google Maps uygulamasını kullanarak gelir elde eden kullanıcılar ise Google Maps Premier kullanmak zorundadırlar[1].

Ayrıca uydu fotoğrafı detayları yerleşim yerinin nüfus yoğunluğuna bağlı olarak orantılanmıştır. Hiç kimsenin yaşamadığı yerler daha az detaylıyken metropoller çok detaylıdır.

Google Maps sadece ABD ve Kanada'yı hedef kitlesi olarak kabul etmemiştir. Dünyanın her tarafında olabildiğince güncel veriler sağlamayı hedeflemiştir. Google Maps ile Ankara'daki bir yerin görüntüsü Şekil 5.3'de verilmektedir. Bu harita, söz konusu yerin güncel görüntüsünü de yansıtmaktadır. Buradan Google Maps'in rakip uygulamalara göre ne kadar güncel olduğu da anlaşılabilmektedir.

[1] Google Maps/Google Earth APIs Terms of Service, http://code.google.com/tr-TR/apis/maps/term.html.



Şekil 5.3 Google Maps'te Ankara'dan Bir Bölgenin Gösterimi.

5.3 Google Maps API

Google Maps'in Şubat 2005'te servislerini sunmaya başlamasından sonra bazı web sitesi geliştiricileri Google Maps'i kendi sitelerinde göstermeyi çözmeyi başarmışlardır. Housingmaps sitesi Google Maps'i ve Craiglist ilanlarını kullanmıştır ve Google Maps'i API yayınlanmadan önce kullanarak bunun ilk örneği olmuştur. Bunun üzerine Google kullanıcıların böyle bir ihtiyacı olduğuna karar vermiştir. Haziran 2005'te kullanıcılara Google Maps'i web sitelerinde kullanmalarına yardımcı olacak Google Maps API'nin ilk versiyonu yayınlanmıştır [12].

Google Maps API, internette kullanılan API istatistiklerini tutan ProgrammableWeb'e göre şu anda internette en çok kullanılan API'dir. Kullanım oranı Google Maps için %41 olarak belirtilmişken; Bing Maps'e ait Virtual Earth için %3 olarak belirtilmiştir[1].

Google Maps API ilk oluşturulduğunda şu an mevcut olan birçok kütüphane henüz eklenmemiştir. Google Maps'in bu işleri kendisi halletmesi gerekmiştir. Bundan

[1] API Dashboard, http://www.programmableweb.com/apis.

dolayı şu anda mesela AJAX ile halledilen yakınlaştır-uzaklaştır gibi çağrıları kendisi yapmak zorunda kalmıştır. Ayrıca o dönemde cep telefonu endüstrisi bu kadar ileri olmadığı için Google Maps'in cep telefonlarında gösterilebilme ihtiyacı hesaba katılmamıştır. Yeni kütüphaneler ve yeni ihtiyaçların doğması sonrasında Google Maps yeni ve daha hızlı bir API yapmaya karar vermiştir. Mayıs 2010'da Google Maps API Versiyon 3'ün kararlı sürümü kullanıma sunulmuştur [12]. Bu tarihten itibaren de versiyon 2 kullanılmamaya başlanmıştır.

Versiyon 3, versiyon 2'de olduğu gibi ardışık fonksiyon çağrıları yerine eş zamanlı fonksiyon çağrıları yapmaktadır. Böylece masa üstü ve cep telefonu uygulamalarında ciddi bir hızlanma sağlanmıştır. Yeni API'de harita gösterilmesindeki önemli kodlar ilk önce çalışmakta sonra diğer kodlar çalışmaktadır. Ayrıca Google Maps API bir javascript uygulaması olmasından dolayı versiyon 2'de sayfada bulunan diğer javascript kodlarıyla karışabilmektedir. Bundan dolayı isimlendirme konusunda da yeni API ile düzenlemeye gidilmiştir. Önceki versiyonda Google Maps'e ait objeler ve değişkenler G harfi ile başlatılırken şu anki versiyon ile beraber google.maps. ile başlatılmaktadır. Mesela versiyon 2'de haritada koordinatları belirten obje Gmarker iken, versiyon 3 ile beraber google.maps.Marker olarak değiştirilmiştir. Böylece Google Maps API ile çalışan kullanıcılara büyük bir kolaylık sağlanmıştır. Ayrıca versiyon 3 ile beraber Google Maps API anahtar uygulaması da kaldırılmıştır. Önceki versiyonlarda kullanıcıların bir anahtar alıp bununla Google Maps'i çağırmaları gerekmektedir. Şu anki versiyon ile herhangi bir sayfada anahtar kullanmadan uygulama çağrılabilmektedir.

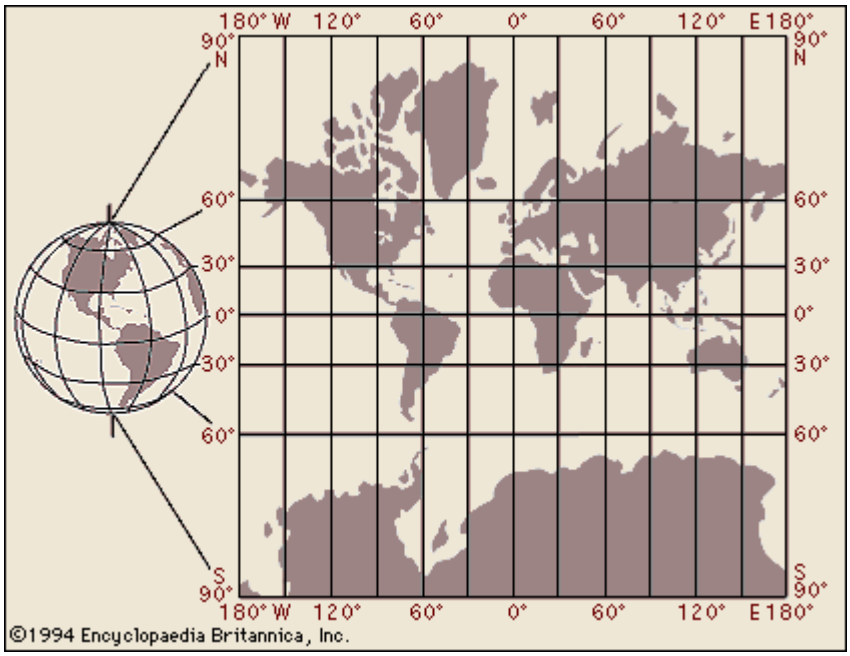
5.4 Harita Bilgisi ve Merkator Haritası

Google Maps'i sitesinde kullanmak isteyen kullanıcıların biraz da olsa harita bilgisine ihtiyaçları olacağı düşünülmektedir. Bir koordinatın dünya üzerindeki gösterimi ve uygulamasını bir yerin harita üzerindeki yerini gösterirken bilmek gerekmektedir. Ayrıca Google Maps merkator harita yaklaşımını uyguladığı için bunu da incelemek yararlı olacaktır.

Koordinat bir yerin dünya üzerindeki konumuna denilmektedir. Koordinatlar enlem ve boylam olarak adlandırılmaktadır ve derece, dakika ve saniye ile ifade edilmektedir. Aynı analitik geometride olduğu gibi Greenwich boylamını ve Ekvator

enlemini y ve x olarak düşünüp dünya üzerinde 4 bölge oluşturulabilmektedir. Burada kuzey yarım kürede kalan enlemler yani y koordinatları “+” ile güneyde kalan enlemler “-“ ile ifade edilmektedir. Boylamlara gelince, onlar da 0 noktası olarak Greenwich boylamını kabul etmişlerdir. 0 boylamının doğusu “+”, solunda yani batısında kalan boylamlar ise “-“ ile ifade edilmektedir.

Koordinat bilgisine değinildikten sonra haritacılığın en zorlu aşaması olan küreye benzeyen şekildeki dünyanın düzlem üzerinde gösterilmesinden bahsedilecektir. Bunun için projeksiyon yöntemleri kullanılmaktadır. En ünlüsü WGS 84 Datum’da da kullanılan Merkator Gösterimidir. Merkator Projeksiyon, Flemenkli Gerardus Mercator tarafından 1569 yılında geliştirilmiştir[1]. Boylamları düzlem üzerinde de dik göstererek kuzeye doğru gösterilen alanların daha büyük gösterilmesiyle elde edilmektedir. Şekil 5.4‘de gösterilmiştir. Kutuplarda sonsuzluk oluştuğu için 85. enlemler sonrası gösterilememektedir. Aynı şekilde Google Maps API Merkator Projeksiyon kullandığı için 85. enlemler sonrası bulunmamaktadır. Ama buralarda herhangi bir yol bulunmadığı için Google Maps kullanıcıları açısından sorun oluşturmamaktadır.



Şekil 5.4 Merkator Projeksiyon[2].

[1] Gerardus Mercator, http://inventors.about.com/library/inventors/blmercator.htm.
[2] Mercator2.gif, http://www.mrkay.org/mrk/images/mercator2.gif.

5.5 Google Maps API Sınıfları ve Kütüphaneleri

Google Maps API kullanıcılara birçok sınıf ve kütüphane sunmaktadır. Gün geçtikçe bunlara yenileri de eklenmektedir. Mesela Ocak 2011'de eklenen Geometry kütüphanesinden sonra AdSense ve en son olarak da Places kütüphaneleri kullanıma sunulmuştur[1].

İlk önce Google Maps API'nin sunduğu sınıflar incelenecektir. API'nin en önemli sınıfı google.maps.Map sınıfıdır. Bu sınıf web sayfasına yeni bir harita yüklenmesini sağlamaktadır. Burada haritanın hangi koordinatlara ait olduğu, yakınlaştırma derecesinin ne olacağı, haritanın uydu mu yoksa yol haritası mı olacağı gibi özellikler belirlenmektedir.

Haritada bir noktayı işaretlemek için google.maps.Marker sınıfı kullanılmaktadır. Bu sınıf kullanılarak bir Marker objesi oluşturulmaktadır. Bu objeyle işaretlenen yerin koordinatı belirlenmektedir. Diğer işaretleme özellikleri için ise başka sınıflar kullanılmaktadır. Mesela imge seçiminde ve imge özellikleri belirlenirken google.maps.MarkerImage, işarete animasyon özellikler eklemek için google.maps.Animation ve işarete bilgi penceresi eklemek için google.maps.InfoWindow kullanılmaktadır.

Harita üzerinde şekiller çizdirmek için Polyline, Polygon, Rectangle ve Circle gibi sınıflar bulunmaktadır.

Bunlar dışında Google Maps API birçok sınıfı kullanıcılara sunmuştur. Google Maps uygulamasındaki yol tarifi gibi uygulamaların yapılmasını sağlayan TravelMode, DirectionsService ve Overlay sınıfları bulunmaktadır.

Google Maps API birçok kütüphane de sunmaktadır. Ocak 2011'de Geometry kütüphanesi yayınlanmıştır[1]. Kütüphanenin en önemli özelliği küresel hesaplamalara olanak sağlamasıdır. Dünya haritalarını düzlem olarak düşünüp haritalar üzerinde öklit geometrisinin uygulanması doğru değildir. İki yer arasındaki en kısa mesafe bir düz çizgi olmayacaktır. Küre üzerindeki iki nokta arasındaki en kısa yol da aslında bir çemberin parçasını oluşturmaktadır. Bundan dolayı da düzlemsel geometri uygulanamamaktadır. Bunun bir uygulaması da uluslararası uçuşlarda görülebilmektedir. Frankfurt ve Los Angeles arasında uçuş yapan bir

[1] Google Geo Developers Blog: A little help with spherical geometry from our first Maps API library, http://googlegeodevelopers.blogspot.com/2011/01/little-help-with-spherical-geometry.html.

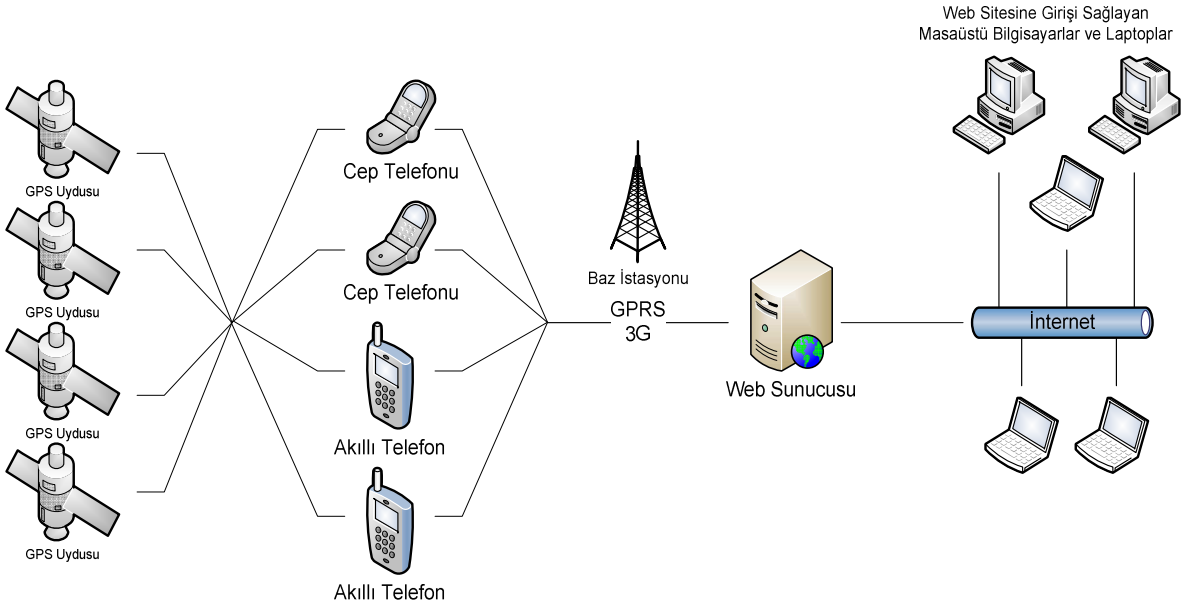
uçak dünya haritasında iki şehir arasında çizilen düz çizgide gitmeyip en kısa mesafeye yakın olan Grönland üzerinden geçmektedir. Ayrıca küre üzerinde çizilen bir üçgenin iç açıları toplamı da 180 dereceden fazladır. Düzlemsel geometrinin uygulanamadığı küre üzerinde Geometry kütüphanesi kullanılarak hesaplamalar yapılmaktadır.

Geometry kütüphanesine ek olarak AdSense kütüphanesi ve en son olarak da Places kütüphanesi çıkarılmıştır. AdSense kütüphanesi ile kullanıcılar haritalarda reklam gösterebilmekte ve tıklamalardan kazanç elde edebilmektedir. Bunun için bir AdSense hesabı gerekmektedir. En son olarak da Places kütüphanesi oluşturulmuştur. Bu kütüphane ile belirlenen bir yer içerisindeki yerler isimleriyle aranabilmektedir.

Bu sınıflar ve kütüphaneler kullanılarak coğrafi çerçeveleme uygulamaları tez kapsamında geliştirilmiştir. Coğrafi hesaplamalar ise buna el veren ileri düzey Geometry kütüphanesi ile yapılabilmiştir. Dünyanın yuvarlaklığından ve düzlemsel haritaların projeksiyon ile yapılıyor olmasından dolayı bu hesaplamaların coğrafi formüller ile yapılması gerekmektedir. Bu hesaplamaların gerekliliği bir örnek ile açıklanabilir. Koordinatları bilinen iki yerin birbirine olan uzaklıklarını bulmak için enlem ve boylam farkını alıp derece cinsinden bir değer elde etmek gerekmektedir. Sonra da bu değer, 1 derecelik uzaklıkla çarpılmaktadır. Ama 1 derecelik uzaklık dünya üzerinde sabit değildir. Boylamlar kutuplara yaklaştıkça aralarındaki uzaklık da azalmaktadır. Bundan dolayı bu uzaklığın hesaplanması için coğrafi formüller gerekmektedir. Burada Merkator Projeksiyonda kullanılan formüller kullanılmaktadır. Bu formüllerin Geometry kütüphanesi üzerinden kullanmak mümkündür.

6. GERÇEKLEŞTİRİLEN KONUMLANDIRMA SİSTEMİ

Bu kısımda tez kapsamında gerçekleştirilmiş olan çalışmalar aktarılmaktadır. Bu çalışmalar telefon yazılımı ve web arayüzü çalışmalarıdır. Şekil 6.1'de sistemin GPS uyduları, mobil telefonlar, web sunucusu ve bilgisayarların bulunduğu genel çalışma şeması gösterilmektedir.



Şekil 6.1 Sistemin Genel Çalışma Şeması.

Bölüm 6.1'de telefon yazılımı başlığı altında mobil telefonların sahip olması gereken özellikler, GPS donanımlı telefonların piyasadaki durumları ve telefon için gerçekleştirilmiş yazılımdan bahsedilmektedir. Bölüm 6.2'de ise kullanıcı arayüzünü sağlamak için geliştirilmiş web arayüzünden bahsedilmektedir.

6.1 TELEFON YAZILIMI

6.1.1 Giriş

Günümüzde hemen herkesin cep telefonu bulunmaktadır. Konuşma ve kısa mesaj atma dışında internet ve fotoğraf makinesi gibi özellikler de cep telefonlarını cazip hale getiren ve kullanışlı kılan özelliklerdir. Herkesin bildiği ve kullandığı bu özelliklerin ve servislerin dışında artık birçok cep telefonunun sunduğu ve acil durumlarda ya da iş hayatında işe çok yarayabilecek GPS özelliği de bulunmaktadır.

GPS özellikli bu telefonlar insanlara birçok açıdan fayda sağlayabilmektedirler. Bir acil durumda yerini konum bilgileriyle yüksek doğrulukta bir merkeze bildirebilmek bunlardan en önemlisi olarak sayılabilmektedir. Bunun dışında ebeveynlerin çocuklarının nerede olduğunu takip edebilmesi istenebilecek özelliklerdendir. Aynı zamanda şirketlerin kurye ve kargo takiplerinde bu tip bir sistemi kullanmak isteyebilecekleri değerlendirilmektedir. Muhakkak büyük şirketlerin ileri özellikli GPS cihazlarını içeren sistemleri bulunmaktadır. Ama herhangi bir GPS takibi kullanmayan şehir içi kurye şirketlerinin çalışanlarının cep telefonlarını kullanarak kuryeleri takip eden bir sistem hayata geçirmeleri hem neredeyse maliyetsiz hem de kendileri için önemli bir sistem olabileceği düşünülmektedir.

Acil durumlarda telefonların yerlerinin öğrenilmesine yönelik önemli bir dönüm noktası ABD'deki Federal Haberleşme Komisyonu'nun (FCC) cep telefonlarına yönelik istediği gereksinimler olmuştur. Birinci aşama olarak cep telefonlarından yapılan, özellikle 911 gibi, acil aramalarda aramayla beraber cep telefonunun bağlandığı baz istasyonu bilgisinin sağlanması istenmektedir. İkinci aşamada ise cep telefonlarının %95'inin konum bilgisi sağlayabilen özellikte olması şart koşulmaktadır. İkinci aşama 31 Aralık 2005 tarihinde gerçekleştirilmiştir. Şu anda ABD'de 911 arandığında kullanılan GSM operatörüne bağlı olarak gerçek konum bilgisine kadar verilebilmektedir. Bazı operatörler baz istasyonlarından konum bilgisi sağlayarak 200-300 metre hatalarla bu bilgiyi sağlarken Verizon Wireless ve T-Mobile gibi ABD'deki önemli operatörler A-GPS kullanarak konum bilgisini sağlamaktadırlar. 2012 yılına kadar ise acil telefon aramalarında her operatörden arama yapan tüm kullanıcıların konum bilgilerini en çok 300 metre içinde vermeleri istenmektedir[1].

6.1.2 Donanım Bilgileri

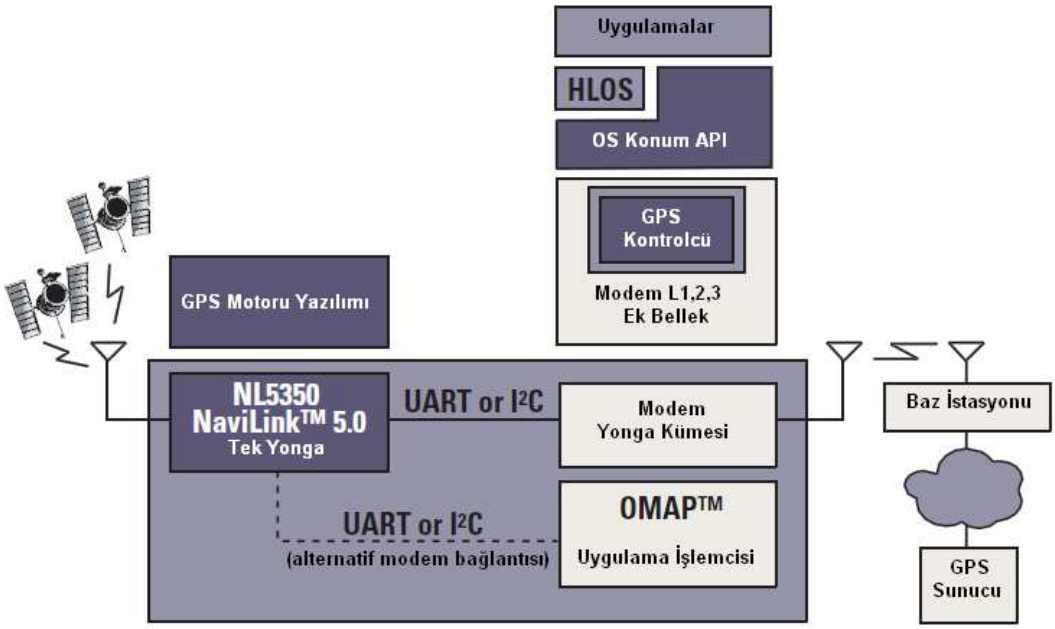
GPS donanımlı cep telefonları, GPS servisini sunabilmeleri için bir takım donanımsal özelliklerle donatılmışlardır. Şu an piyasada bulunan GPS telefonlarının bir kısmında gömülü GPS yongaları bulunmaktayken bir kısmı ise bu servisi A-GPS ile sunmaktadır.

[1] Enhanced 9-1-1. Federal Communications Commission. Public Safety and Homeland Security Bureau, http://transition.fcc.gov/pshs/services/911-services/enhanced911/Welcome.html.

A-GPS bölüm 2.4'de değinildiği gibi GSM operatörlerinin de yardımı alınan yönlendirilmiş GPS sistemleridir. Bunlarda ilk bilgi alınıp sonrasında cep telefonunun özelliğine bağlı olarak kendi GPS yongasından bilgi almaya devam etmekte ya da operatörden bilgi alarak işlemi sürdürmektedir. Bu tip A-GPS kullanımının maliyeti ise çok cüzidir. Özellikle Neredeyim servisi gibi operatörlerin sunduğu servislerle kıyaslandığında hem maliyet bakımından çok ucuz hem de performans ve doğruluk bakımından gerçeğe çok yakın oldukları ve daha hassas oldukları gözlenmektedir.

Cep telefonlarının GPS verisini sağlamasına yardımcı bir diğer unsur da içerisindeki gömülü GPS yongaları olmaktadır. Bazı telefonlarda bu yongaların olduğu bilinmektedir. Bu yongalardan bazı modeller incelenecektir.

Yonga üreticilerinin öncü firmalarından olan Texas Instruments'in ürettiği GPS5300 NaviLink 4.0, NL5350 NaviLink 5.0 ve NL5500 NaviLink 6.0 gibi yongalar bulunmaktadır. Bu yongalar A-GPS özelliği de sunmaktadırlar. Uydularla olan bağlantıyı da sağlamaktadırlar. Bu yongalar bir önceki sürümlerine göre daha az yer kaplamakta, daha ucuz maliyet sağlamakta ve daha az güç harcamaktadırlar. Cep telefonlarında olan böyle bir sistemden de beklenen özellikler bunlardır. Cep telefonları küçük olduklarından ve kısa bir pil ömrüne sahip olduklarından GPS yongalarının da hem çok az yer kaplaması hem de az enerji tüketmeleri istenmektedir. Şekil 6.2'de NL 5350 NaviLink 5.0 GPS yongasına ait bir çalışma diyagramı gösterilmektedir.



Şekil 6.2 GPS Yongası Sistem Blok Diyagramı[1].

GPS donanımının cep telefonlarında nasıl sağlandığından bahsedildikten sonra piyasada GPS özelliğine sahip telefonlardan bahsedilmesi uygun olacaktır.

Şekil 6.3'de GPS donanımlı bir telefonun GPS sorgulama ekranı gösterilmektedir.

Şekil 6.3 GPS Donanımlı Cep Telefonu.

[1] Texas Instruments, GPS NaviLink 5.0 Solution, http://focus.ti.com/pdfs/wtbu/ti_navilink_5.pdf.

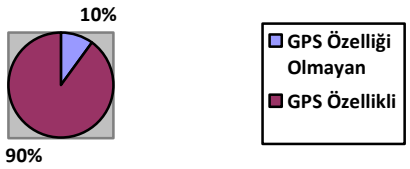
Bugün piyasada Nokia, Samsung, Sony Ericsson, LG ve Blackberry'e ait birçok telefonda GPS özellikleri bulunmaktadır. Çizelge 6.1'de bazı popüler GPS donanımlı cep telefonları verilmektedir.

MARKASI	**MODELİ**
Nokia	5800 Express Music, E52, 6730 Classic, 6710 Navigator, E72, N97, X6-00, C7 vb.
Samsung	B7510, S5670, i9003, S5830, i5510, S5620 vb.
Sony Ericsson	XPERIA X10
LG	P503, GD 880
Blackberry	9780

Çizelge 6.1 GPS Donanımlı Cep Telefonu Modelleri.

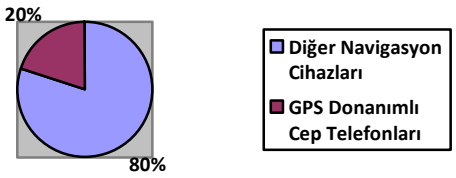
Cep telefonu piyasasında son yıllarda GPS özelliği olan telefonlara talep artmıştır. ABI ismindeki araştırma şirketinin araştırmalarından birisinde 2009 yılında cep telefonu piyasasında %4-5'lik düşüş yaşanmasına rağmen GPS özellikli cep telefonu satışlarında %6.4'lük bir artış olduğu ve toplam satışın 240 milyon üniteye çıktığı belirtilmektedir[1]. Yine aynı araştırmada 2014'e kadar %19'luk bir artış olacağı ve her 10 akıllı telefondan 9'unda GPS donanımı bulunacağı belirtilmektedir[1]. Çizelge 6.2'de 2014 yılına ait akıllı telefonlarda GPS özelliğine sahip olma oranı gösterilmektedir.

[1] ABI Research, GPS-Enabled Handsets Expected to Bypass the Economic Downturn. Press Release, http://www.abiresearch.com/press/1351-GPS-enabled+Handsets+Expected+to+Bypass+the+Economic+Downturn.



Çizelge 6.2 2014'te Akıllı Telefonlarda GPS Özelliğine Sahiplik Oranları.

Uzman analizci George Perros şu anki global ekonomik durumun iç açıcı olmamasına rağmen fiyatların düşmesi ve kullanıcılarda GPS farkındalığı oluşması sonucunda GPS özellikli telefonlara olan talebin artacağını düşünmektedir[1]. Canalys'in bir araştırmasına göre mobil telefon kullanıcılarının %60'ı cep telefonlarının GPS özellikli olmasını arzulamaktadır. Yine aynı şirketin araştırmasında Çizelge 6.3'de verildiği gibi GPS ve navigasyon cihazı piyasası ekonomisinin 2008 sonu itibariyle %20'lik kısmını GPS özellikli telefonların oluşturduğu belirtilmektedir[1].

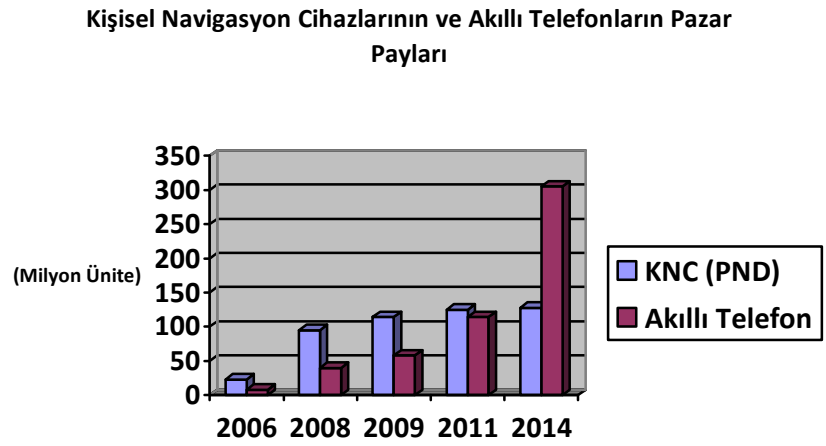


Çizelge 6.3 2008 Sonu GPS Cihaz Oranları.

Çizelge 6.4'de kişisel navigasyon cihazlarının ve navigasyon özelliğine sahip akıllı telefonların tüm dünyadaki kullanım durumları gösterilmektedir. Akıllı telefonların

[1] Demand for GPS-enabled phones seen growing, http://www.asiaone.com/Motoring/Owners/Motor%2BTech/Story/A1Story20080919-99750.htm.

pazar payının arttığı görülmektedir. 2014 yılı için ise akıllı telefonların kişisel navigasyon cihazlarını geçeceği tahmin edilmektedir[1].



Çizelge 6.4 Kişisel Navigasyon Cihazları ve Akıllı Telefon Market Payları[2].

GPS donanımlı telefonlara talep artarken GPS özelliğinin de cep telefonlarının standart bir özelliği haline gelmesi beklenmektedir. Nokia Singapur'un genel yöneticisi Grant McBeath, Nokia'nın ürettiği telefonlarda navigasyon, konum bildirme ve harita gibi konuma dayalı uygulamaların standart bir özellik haline geleceğini ifade etmektedir[3].

GPS donanımının cep telefonlarında daha yaygın hale gelebilmesinde GPS yongası üreticilerinin daha az enerji tüketen ve daha az maliyetli GPS birimleri üretmeleri de etkili olmaktadır. ABI Research'un başka bir raporunda cep telefonlarının içeride veya az sinyal alınması durumunda çalışmasına el verecek GPS yongalarının üretilmesinin amaçlandığı belirtilmektedir[4]. Baş analizci Dominique Bonte'ye göre GPS yongası ve birimleri üreticilerinin, kişisel

[1] Smart Phones to Surpass PNDs in Navigation Market in 2014, http://www.isuppli.com/automotive-infotainment-and-telematics/news/pages/smart-phones-to-surpass-pnds-in-navigation-market-in-2014.aspx.
[2] Smart Phones to Surpass PNDs in Navigation Market in 2014, http://www.isuppli.com/automotive-infotainment-and-telematics/news/pages/smart-phones-to-surpass-pnds-in-navigation-market-in-2014.aspx.
[3] Demand for GPS-enabled phones seen growing, http://www.asiaone.com/Motoring/Owners/Motor%2BTech/Story/A1Story20080919-99750.htm.
[4] ABI Research, More Than 550 Million GPS Enabled Handsets Will Ship by 2012. Press Release, http://www.abiresearch.com/press/1125-More+Than+550+Million+GPS+Enabled+Handsets+Will+Ship+by+2012.

navigasyon cihazlarına ilginin artmasıyla yeni marketler bulmak için cep telefonlarında kullanılabilecek GPS birimlerine yöneldikleri belirtilmektedir[4].

6.1.3 Yazılım Bilgileri

6.1.3.1 Cep Telefonu Özellikleri ve API'leri

Cep telefonunun tez kapsamında hazırlanan yazılımı çalıştırması için bir takım özelliklere sahip olması gerekmektedir. Yazılım cep telefonunun konum verisini alıp şifreleyip bunu bir sunucuya yollamasından dolayı, cep telefonunun konum bilgisini verebilen yani GPS özelliğine sahip bir telefon olması gerekmektedir. Ayrıca söz konusu GPS bilgisine ulaşılmasını sağlayan JSR-179 Konum API'a sahip olması gerekmektedir. Alınan konum verisini şifrelemesi için de cep telefonunun sahip olması gereken bir diğer özellik ise JSR-177 Güvenlik API'dir. Bu bilginin sunucuya gönderilmesi için ise GPRS ya da 3G gibi bir internet bağlantı özelliğine sahip olması gerekmektedir.

JSR (JAVA Şartname Talepleri), Java ortamına eklenmesi önerilen özellik ve teknolojileri tanımlayan resmi dokümanlardır. JSR dokümanlarının son halini almasını kararını ise JCP (Java Topluluğu Süreci) yönetim komitesi vermektedir. Son halini almış JSR dokümanı o teknolojinin uygulanmasını örneklendiren uygulamalar barındırmak zorundadır.

JSR-179, Eylül 2003'te ilk defa yayınlanmış ve Mart 2006'da da versiyon 1.0.1 olarak güncellenmiştir. JSR-179'u oluşturan ve şu anda da bu API'nin sahibi olan Nokia'dır [13].

JSR-179'un bir telefonda kullanılabilmesi için cep telefonunda CLDC v1.1 (J2ME Bağlanmış Sınırlı Cihaz Konfigürasyonu) ya da CDC (Bağlanmış Cihaz Konfigürasyonu) konfigürasyonlarından birisi olmalıdır. Bu API, CLDC v1.0 ile kullanılamamaktadır, çünkü bu konfigürasyon kayan noktalı sayıları desteklememektedir [13].

JSR-179'da konum işlerini yapan paket javax.microedition.location paketidir. Bu paketin içindeki LocationProvider sınıfı konum bilgilerini sağlayan sınıftır. LocationProvider sınıfı ile ölçümlerin alınmasını sağlayan Location cinsinden objeler elde edilebilmektedir. Burada QualifiedCoordinates cinsinden enlem, boylam ve rakım bilgileri tutulmaktadır. Sürekli bir bağlantı söz konusu ise

LocationListener kullanılmalıdır. Cep telefonu konumunda oluşan değişiklikler dinlenip bildirilebilmektedir. Bunlara ek olarak bu bilginin doğruluk derecesi ve kullanılan cihazın hızı ve yönü gibi bilgiler de verebilmektedir. Konum %68 ihtimalle doğru bilgi vermektedir [13].

Konum hesaplamalarında JSR-179'da belirlenmiş olan değişik metotlar kullanılabilmektedir. Bundan dolayı her metodun sağlamak zorunda olduğu bilgiler için bir standart zorunlu kılınmıştır. Her metot konumu ölçülen yerin enlem, boylam ve doğruluk bilgilerini vermek zorundadır. Ayrıca konum alınan anın zaman bilgisi de verilmelidir. Kullanılan metoda bağlı olarak ise rakım, doğruluk-kesinlik, yön ve hız, adres bilgisi ve belirli nokta bilgisi sağlanabilmektedir. Ayrıca kullanılan donanıma bağlı olarak pusula açısı; yükseklik ve döndürme açıları da sağlanabilmektedir.

Ayrıca JSR-179'daki metotlar, eğer API'nin ulaşmaya çalıştığı bilgilere erişim engelleniyorsa güvenlik hatası vermektedir. Cep telefonunda GPS bilgilerine ve eğer varsa pusula gibi bilgilere ulaşılmasına izin veriliyor olması gerekmektedir.

Bu tez kapsamında geliştirilmiş yazılımda LocationProvider, LocationListener, Coordinates, QualifiedCoordinates, Criteria, Location, LocationException gibi sınıflar kullanılmaktadır.

Güvenlik uygulamalarının cep telefonlarında yapılabilmesine el veren JSR-177 ilk defa 2003 yılında tasarlanmıştır. Kullanılan son versiyonu 2004 yılına aittir [14].

Bir cep telefonunda JSR-177, güvenli veri depolanmasını, kişisel bilgilerin güvenli bir şekilde tutulmasını sağlamaktadır. Ücret ödeme protokollerinde veri doğruluğu ve gizliliğini sağlamaktadır. Kullanıcılar bu API'nin sunduklarından faydalanarak bankacılık ve gizlilik gereken uygulamalarını yapabilmektedirler.

Bu API cep telefonunun güvenlik elemanına entegre olarak güvenlik servislerinin çalışabilmesini sağlamaktadır. Güvenlik elemanı cep telefonlarında birkaç şekilde olabilmektedir. GSM cep telefonlarında bu SIM karttadır. Başka çeşit telefonlarda UICC ya da RUIM kartlarında da bulunmaktadır [14]. Mesela GSM ağlarında operatör, kişisel bilgileri SIM kartına yüklemekte ve telefonun ağ tarafından tanınması sağlanmaktadır.

JSR-177 ile birbirinden bağımsız dört paket uygulanabilmektedir. Bunlar SATSA-APDU, SATSA-JCRMI, SATSA-PKI ve SATSA-CRYPTO'dur. SATSA-APDU, akıllı

kartlarla telefonun haberleşmesini sağlayan bir protokol tanımlamaktadır. SATSA-JCRMI, Java kart RMI API'dır. SATSA-PKI, dijital imza ve kimlik uygulamaları içindir. SATSA-CRYPTO, cep telefonlarında kripto algoritmalarının uygulanması, şifreleme ve şifre çözme için kullanılmaktadır [14]. Bu tez kapsamında da SATSA-CRYPTO paketi kullanılmıştır.

SATSA-CRYPTO paketi içerisinde MessageDigest, Signature, Cipher, KeyFactory ve SecretKeySpec gibi sınıflar bulunmaktadır. Bu tez kapsamında geliştirilen yazılımda yoğun bir şekilde bu sınıflardan yararlanılmış ama en öne çıkanı ise Cipher sınıfı olmuştur. Bu sınıf şifreleme ve şifre çözme algoritmalarını destekleyen sınıftır. Anahtarlama işlemlerinde ise SecretKeySpec gibi sınıflar kullanılmaktadır.

6.1.3.2 İşletim Sistemi ve Yazılım Dilleri

Cep telefonlarında yazılım geliştirmek için birçok platform ve dil bulunmaktadır. Bunlardan tez kapsamında çalışma ve inceleme fırsatı bulunulan Symbian C++ ve Java ME detaylandırılacaktır.

Symbian özellikle Nokia telefonlarının birçoğunda bulunan işletim sistemidir. İlk çıkışı Symbian Ltd. İken, şirketin Nokia tarafından satın alınması sonrasında, işletim sistemi Nokia tarafından yürütülmeye başlanmıştır.

Daha önceden Symbian OS ismiyle anılmaktadır. S60 Feature Pack 2 3rd Edition ve S60 5th Edition Symbian OS'ta çalışan yazılım platformudur. İşletim sisteminin şu an çıkan yeni versiyonları Symbian^1, Symbian^2 şeklinde isimlendirilmektedir.

Symbian C++, Symbian işletim sistemlerinde yazılım geliştirme dilidir. Diğer diller kadar ilgi görmediği bir gerçektir. Bu dil ile yazılacak basit programlar bile çok zor hale gelebilmektedir. Yazılım sırasında özel teknikler uygulamak gerekmektedir. Bu dilde hafıza işletimi çok önemlidir. Hafızada açılan herhangi bir değerin devamlı kontrol altında tutulması gerekmektedir. Daha düşük seviyedeki işlemleri yapmak da yazılımcıya bırakıldığı için zorluklar yaşatmaktadır. Bunların yanı sıra descriptor, active object ve cleanup stack gibi tekniklerin sürekli uygulanması gerekmektedir.

Symbian C++'ın bir diğer kötü yanı ise cep telefonu modeline özel olmasıdır. S60 5th Edition için yazılan bir uygulamanın S60 Feature Pack 2 3rd Edition bir

telefonda çalışmasını beklememek gerekmektedir. Bundan dolayı GPS gibi belli bir özelliğe sahip her telefonda çalışması planlanan bir yazılımın Symbian C++ ile yazılmaması gerektiği değerlendirilmiştir.

Java ME cep telefonu gibi gömülü sistemlerde çalışmak için tasarlanmış platforma özel Java dilidir. Java ME, Oracle şirketine bağlı Sun Microsystems tarafından geliştirilmiştir. Bu dilin detayları JSR-68 dokümanında belirlenmiştir [15].

CLDC, Java ME ile uygulama geliştirmek için gerekli minimum kütüphaneleri bulundurmaktadır. Bu kütüphanelere eklemeler de yapılabilmektedir.

Java ME'nin platformlarda çalışması için en az JRE (Java İşleyiş Süresi Ortamı) 1.3'e gereksinim duyulmaktadır. JRE'nin daha yeni versiyonları olmasına rağmen üreticiler için güncelleme sıkıntısı olacağından dolayı 1.5 ya da 1.6 gibi yeni versiyonlara geçilmemektedir.

Java ME'nin Symbian C++'a göre en büyük avantajı birçok platformda yazılımda değişiklik yapılmadan çalışabilmesidir. Ancak iPhone ve Blackberry QNX gibi yeni cep telefonu platformlarının bazılarında Java ME desteklenmemektedir.

Bu tez kapsamında daha çeşitli cep telefonu marka ve modellerinde çalışabilmesinden dolayı Java ME seçilmiştir. Cep telefonu için uygulanmış program Java ME dilinde yazılmıştır.

6.1.3.3 Yazılım Geliştirme Platformları

Cep telefonu yazılımları geliştirmek için bir takım platformlar bulunmaktadır. Ayrıca yazılımları test etmek için de emülatör ve uzaktan bağlanılan cihazlar da mevcuttur.

Cep telefonlarında Java geliştirmek için NetBeans tercih edilen bir platform olmuştur. NetBeans, 1996'da Prag'ta Charles Üniversitesi'nde bir üniversite projesi olarak başlamış, daha sonra 1997'de bir şirket formatını almıştır. 1999'da ise Sun Microsystems tarafından satın alınmıştır[1]. Özellikle Java geliştirme platformudur. Bu platformun bir diğer özelliği tamamen açık kod olması yani herkese tam kullanım hakları verilmiş olmasıdır. Bilindiği gibi Visual Studio gibi platformları kullanmak için lisanslarını satın almak gerekmektedir.

[1] A Brief History of NetBeans, http://netbeans.org/about/history.html.

NetBeans dışında cep telefonu yazılımı geliştirmek için kullanılan ve Nokia sayesinde popülerlik kazanmış Carbide.c++ platformu bulunmaktadır. Bu platform özellikle Symbian işletim sistemi üzerinde çalışabilecek c++ uygulamalar geliştirmeyi hedeflemiştir. Carbide'nin sahibi Nokia ve Symbian kuruluşudur.

Bu tüm platformlarda üretilen yazılımların denenebilmesi ve gerçek bir cihazda çalışırcasına test edilebilmesi için hem Sun Microsystems hem de cep telefonu üreticileri özellikle de Nokia, emulatörler geliştirmişlerdir.

Sun Microsystems tarafından geliştirilen JDK (Java Geliştirme Teçhizatı) en çok kullanılan Java geliştirme emülatörüdür. Seçeneklerde birçok değişik emülatör arayüzü bulunmaktadır. Şekil 6.4'de JDK emülatörü gösterilmektedir.

Şekil 6.4 JDK Emülatörü.

JDK emülatöründen başka yazılımcıların kullanabilecekleri ve Nokia'nın geliştirdiği cep telefonu modellerine özel emülatörler bulunmaktadır. Nokia'nın geliştiriciler

için kurduğu forum sitesinden bu tip ekipmanlar indirilebilmektedir[1]. S60 5th Edition ve diğer S40, S60 3rd Edition Feature Pack 2 gibi modeller için Nokia emülatörler geliştirmiştir. Şekil 6.5'de Nokia S60 5th Edition emülatörü gösterilmektedir.

Şekil 6.5 S60 5th Edition Emülatörü.

Emülatörler ile yazılım geliştirmesi ve denenmesi yapılabildiği gibi gerçek bir telefonda denenmek istendiğinde platformlar yardımıyla çalıştırma dosyaları cep telefonuna aktarılabilmektedir. Eğer yazılımcı bir cep telefonuna sahip değilse ya da yeni çıkan telefonlarda yazılımını denemek isterse Uzaktan Cihaz Erişimi ile cep telefonlarına erişim sağlayabilmektedir. Şekil 6.6'de Nokia 5800 için Uzaktan Cihaz Erişimi ekranı gösterilmektedir.

[1] Nokia Developer, http://www.developer.nokia.com.

Şekil 6.6 Uzaktan Cihaz Erişimi Ekranı.

6.1.4 IMEI

IMEI (Uluslararası Mobil Cihaz Kimliği) her cep telefonunda bulunan ve sadece o cep telefonuna ait özel bir numaradır. Özellikle çalınma gibi durumlarda cep telefonunun kimliklendirilmesi ya da bloke edilmesi için kullanılmaktadır.

IMEI numarası, cep telefonlarında genelde pil altında yazılıdır. Pil kısmının açılmadan öğrenilebilmesi için cep telefonunda *#06# tuşlandığında IMEI numarası ekrana gelmektedir.

IMEI numarası genelde 15 haneden oluşan bir sayıdır. Bunun ilk 14 hanesi IMEI numarası iken son hanesi kontrol hanesidir.

IMEI numarasının alınması işlemi cep telefonu markalarına göre değişmektedir. System.getProperty metodu kullanılarak cep telefonuna ait IMEI numarası

öğrenilebilmektedir. Çizelge 6.5'de System.getProperty içerisine verilen parametreler cep telefonu üreticilerine göre gösterilmiştir.

Telefon Markası	System.getProperty Parametresi
Nokia	com.nokia.mid.imei
Samsung	com.samsung.imei
Sony Ericsson	com.sonyericsson.imei
Motorola	com.motorola.IMEI
Siemens	com.siemens.IMEI

Çizelge 6.5 System.getProperty Parametreleri.

IMEI numarası tez kapsamında AES şifreleme anahtarı olarak kullanılmaktadır. Böylece her kullanıcıya ayrı bir şifreleme anahtarı sağlanmış ve kullanıcının kendi cep telefonuyla sunucuya bağlanması zorunlu kılınmıştır. AES şifrelemede kullanılan anahtar 128 bit olacak şekilde belirlenmiştir. 192 veya 256 bit anahtarlar çok gizli seviyesinde sayılmalarından dolayı bu anahtar boyutlarını kullanmak için cep telefonları kullanıcılarının özel paketler indirmeleri gerekmektedir[1]. Bunun da her kullanıcı için sorun yapacağı ve fazladan iş yükü bindireceği düşünülerek 128 bit anahtar kullanımında karar kılınmıştır. 15 karakterli IMEI numarası ise toplamda 60 bittir. Geri kalan 68 bitin tamamlanması gerekmektedir. Bunun için IMEI numarasına 128 bite tamamlanana kadar 0 eklemek yerine IMEI numarası tekrarlanıp geri kalan kısım geriye sayıp 1'e kadar giden sayılarla doldurulmaktadır. Mesela 60 bitlik IMEI numarası iki defa tekrarlanıp 120 bitlik bir sayı elde edildikten sonra geri kalan 8 bit "21" ile doldurulmaktadır. Eğer IMEI numarası 60 bitten büyük ise ikinci tekrar yazılırken 128 bit olacak kadar kısmı anahtar olarak kabul edilmektedir. Bu işlemin aynısı sunucu tarafında da tekrarlanmakta ve alınan bilginin şifre çözülmesi gerçekleştirilmektedir.

[1] Using AES with JAVA Technology, http://java.sun.com/developer/technical/Articles/Security/AES/AES_v1.html.

6.1.5 Program Arayüzü

Tez kapsamında yazılan cep telefonu programının kullanıcı arayüzü Şekil 6.7'de verilmiştir.

Şekil 6.7 Cep Telefonu Kullanıcı Arayüzü.

Kullanıcı, "Kullanıcı Adı?" kısmına tez kapsamında geliştirilmiş web arayüzünden aldığı kullanıcı adını, ve "Şifre?" kısmına da web arayüzüne bağlanırken kullandığı şifresini girmektedir.

Kripto seçeneğinden GPS verisini kriptolu mu yoksa kriptosuz mu göndermek istediğini seçmektedir. Kriptolu seçeneği işaretlendiğinde Google Map Me programı cep telefonunun IMEI numarasına ulaşmaktadır. Bu numaradan daha

önce de bahsedildiği gibi şifrelemede kullanılacak anahtar üretilmektedir. Kriptolu seçeneğinde, program GPS verilerini şifreleyerek göndermektedir.

Eğer kriptosuz seçeneği seçilirse program, cep telefonunun IMEI numarasına erişmemektedir. Ayrıca GPS verisinde de herhangi bir şifreleme yapılmamaktadır.

Sonrasında kullanıcının kullandığı cep telefonu markasını işaretlemesi gerekmektedir. Daha önce de değinildiği gibi her cep telefonu markasında IMEI numarasına erişilmesi için farklı bir kod gerekmektedir. Bundan dolayı program arayüzünde kullanıcıdan cep telefonu markasını seçmesi istenmiştir. Cep telefonu markası seçeneğinde Nokia, Samsung, Sony Ericsson, Motorola ve Siemens verilmiştir.

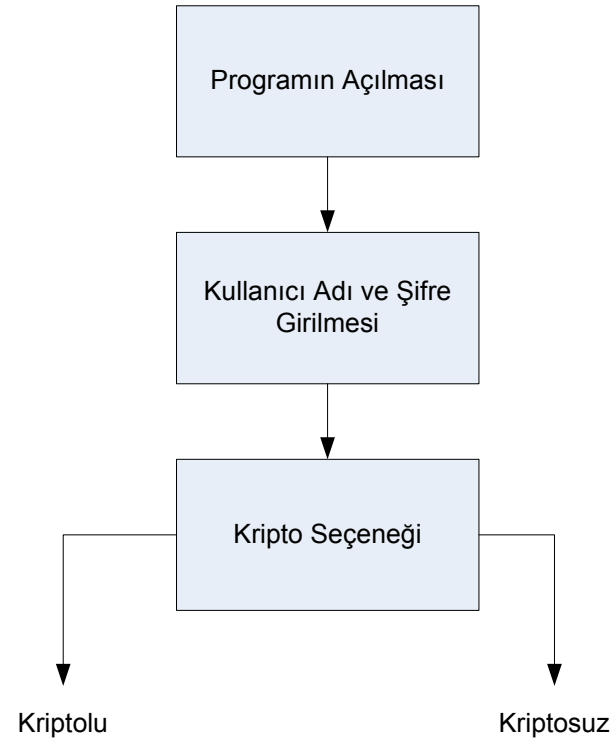
Kullanıcı "Gönderme Aralığı" seçeneğinden sunucuyla bağlantıya geçilecek ve veri gönderilecek zaman aralığını belirlemektedir. Bahsedilen bu aralıkta varsayılan değer 1 ile belirlenmiştir. Eğer kullanıcı bir değişiklik yapmaz ise GPS verilerine her saniyede ulaşılmaya çalışılmakta ve ulaşıldığında veri gönderimi gerçekleştirilmektedir.

Bütün seçenekleri işaretledikten sonra kullanıcı girdiği kullanıcı adı ve şifrenin doğrulanması için "Bağlan" tuşuna basmaktadır. Eğer yanlış veya eksik bilgi girilmiş ise program penceresinde buna dair bir uyarı belirmektedir. Eğer doğrulama başarı ile gerçekleştirilir ise "Bağlan" tuşunun yerine "Başlat" tuşu çıkmaktadır. Kullanıcı "Başlat" tuşuna bastığında bu tuş otomatik olarak "Durdur" tuşuna dönüşmektedir. Ayrıca "Çıkış" tuşu da kaybolmaktadır. Eğer kullanıcı "Durdur" tuşuna basarsa program GPS bağlantısı sağlamayı ve sunucuya veri göndermeyi durdurmaktadır. Bu durumda "Başlat" ve "Çıkış" tuşları tekrar belirmektedir. Eğer kullanıcı programdan çıkmak isterse "Çıkış" tuşuna basması yeterli olmaktadır. Ayrıca bazı cep telefonu modellerinde kırmızı renkli "No" tuşu da çıkış işini gerçekleştirmektedir.

Programın geri planda çalışması için ise beyaz tuşa basılması gerekmektedir. Ya da kırmızı tuş dışında herhangi bir menü tuşuna basılarak da geri planda programın çalışmasına izin verilebilmektedir.

6.1.6 Programın Çalışması

Programın çalışma şeması Çizelge 6.6'da gösterilmektedir. Çizelge 6.6'da da gösterildiği gibi kullanıcının programı açıp kullanıcı adı ve şifresini girmesi gerekmektedir. Kripto seçeneğine bağlı olarak programın çalışma seyri değişmektedir.



Çizelge 6.6 Programın Çalışma Şeması İlk Bölüm.

6.1.6.1 Kriptolu Çalışma Seçeneği

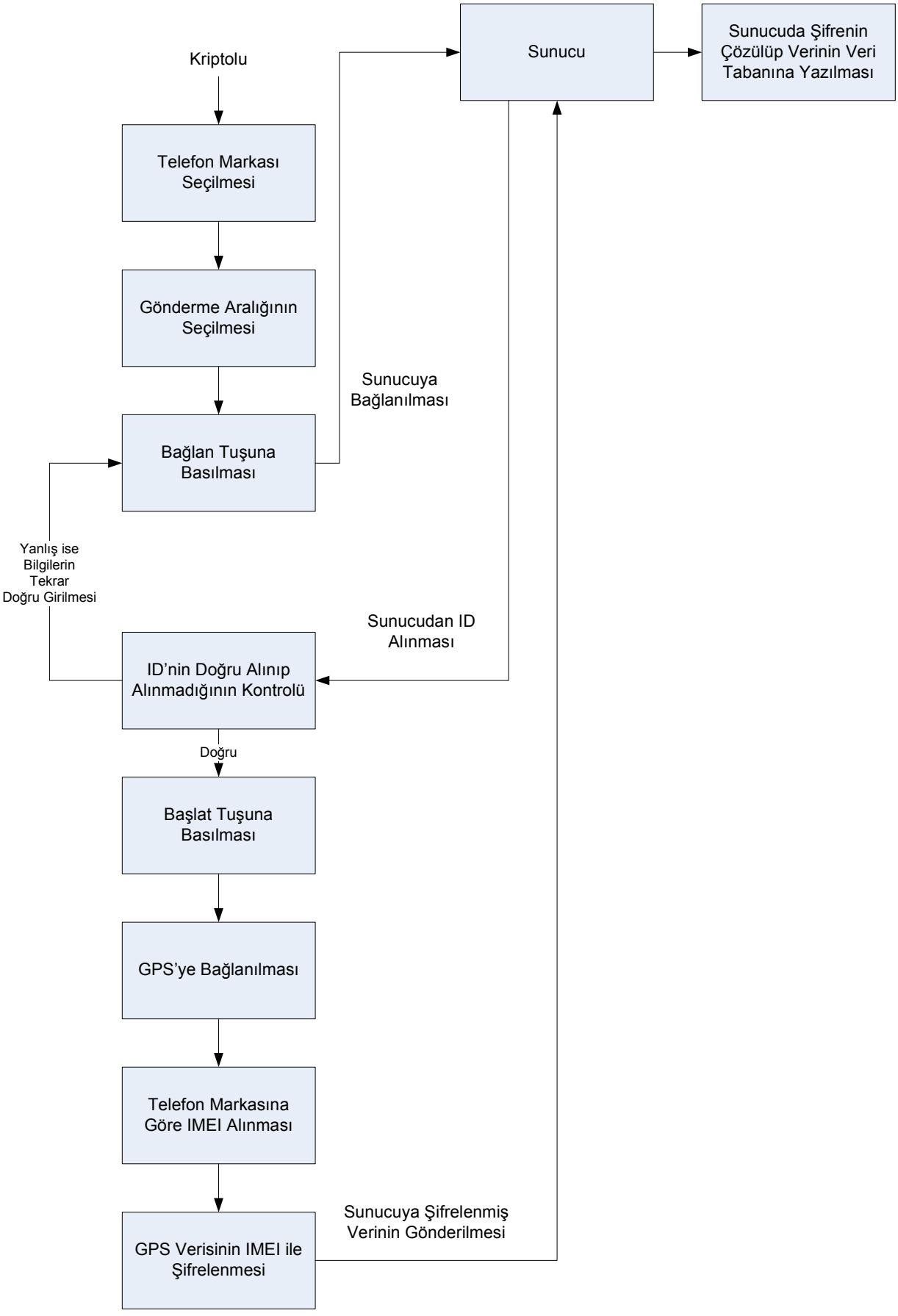
Kriptolu çalışma seçeneği GPS verisinin güvenli bir şekilde sunucuya gönderilebilmesi için yazılıma eklenmiştir.

Bu çalışma seçeneğinin kullanılabilmesi için program arayüzünde bahsi geçmiş olan "Kripto seçeneği"nden "Kriptolu" seçilmesi gerekmektedir. "Telefon markası seçeneği"nden cep telefonu markası seçilmesi gerekmektedir. Sonrasında "Gönderme Aralığı" belirlenmesi gerekmektedir. Bu seçimler yapıldıktan sonra "Bağlan" tuşuna basılarak sunucuyla bağlantı sağlanmaktadır. Bağlantı sağlandı ise, sunucu kullanıcıya özel olan bir ID göndermektedir. ID'nin kontrolü program tarafından gerçekleştirilmektedir. Eğer kullanıcı adı veya şifresi yanlışsa, sunucu cep telefonuna girilen bilgilerin yanlış olduğunu belirten bir ID göndermektedir. Eğer bilgiler doğru ise cep telefonuna kullanıcıya özel ID gönderilmektedir.

Sonrasında program, cep telefonunun GPS yongasıyla bağlantıya geçmekte ve konum verisini almaktadır. Bundan sonraki işlem ise verinin şifrelenmesi işlemidir. Anahtar olarak cep telefonunun IMEI numarası kullanıldığı için ilk önce cep telefonunun IMEI numarası öğrenilmekte ve bu numara 128 bitlik şifreleme anahtarı formatına dönüştürülmektedir. GPS verisi bu anahtar ile şifrelenmekte ve sunucuya gönderilmektedir.

Şifrelenmiş veri, kullanılan standart ASCII (Bilgi Değiştokuşu için Amerikan Standart Kodu) karakterlerine sahip değildir. Şifrelenmiş veride genişletilmiş ASCII tablosundan karakterler bulunmaktadır. Bundan dolayı da bu verinin normal bir bağlantı kurularak gönderilmesi sorun oluşturmaktadır. Şifrelenmiş veri bu sebepten dolayı ASCII tablosundaki indeks numaralarına çevrilmekte ve gönderim sırasında da bu sayıların karakter olduğunun belirtilmesi için her bir indeks numarasının başına “%” işareti eklenmektedir. Sunucu aldığı şifrelenmiş veriyi veritabanında bulunan IMEI bilgisi ile anahtar oluşturarak ve bu anahtarı kullanarak çözmektedir. Sunucu, bu verinin uygun koordinat verisi olup olmadığını kontrol edip veritabanına işlemektedir.

Kriptolu seçeneği seçildikten sonra “Bağlan” tuşuna basıldığında programın nasıl bir çalışma izleyeceği Çizelge 6.7‘de verilmektedir.



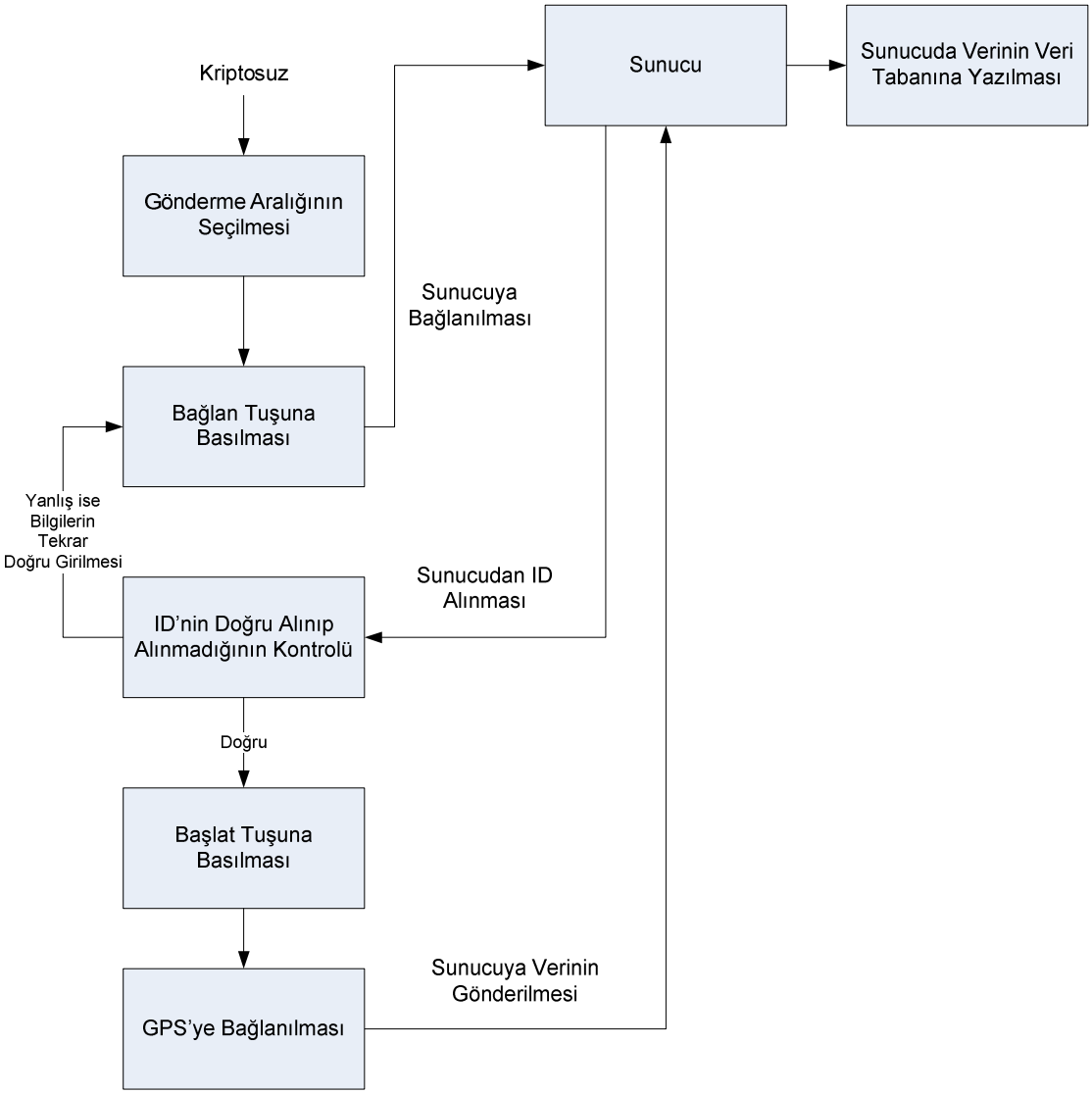
Çizelge 6.7 Kriptolu Seçeneğinde Programın Çalışma Şeması.

6.1.6.2 Kriptosuz Çalışma Seçeneği

Cep telefonu programının kriptosuz çalışmasına dair bir gösterim Çizelge 6.8'da verilmektedir.

Kriptosuz çalışma seçeneği seçildiğinde geriye kalan "Gönderme Aralığı" ve "Telefon Markası" seçeneklerinden "Gönderme Aralığı" seçeneğinin bir önemi kalmaktadır. Telefon markası için hangi seçeneğin belirlendiği bir önem arz etmemektedir çünkü GPS verisi üzerinde herhangi bir şifreleme işlemi yapılmadığı için şifreleme sırasında anahtar oluşturmak için kullanılan IMEI numarasının da alınmasına gerek kalmamaktadır.

Kriptosuz çalışma durumunda da kriptoluda olduğu gibi seçilmiş gönderme aralıklarında GPS verileri alınmakta ve bu veriler sunucuya gönderilmektedir. Yalnız bu çalışma modunda herhangi bir kriptolama uygulanmadığı için GPS verileri enlem ve boylam olarak sayısal halleriyle sunucuya gönderilmektedirler. Sunucuda da herhangi bir şifre çözme işlemi uygulanmamaktadır. Sunucuda sadece gelen verinin mantıklı bir koordinat verisi olup olmadığına bakılmakta ve eğer koordinat verilerinde herhangi bir yanlışlık yoksa veritabanına aktarılmaktadır.



Çizelge 6.8 Kriptosuz Seçeneğinde Programın Çalışma Şeması.

6.2 WEB ARAYÜZÜ

6.2.1 Giriş

Sunucu, veri tabanı ve telefon yazılımından oluşan cep telefonu takip sisteminin kullanıcı arayüzünü oluşturmak için bir web arayüzü tasarlanmıştır. Arayüz PHP, MySQL, Javascript, HTML (Hipermetin Biçimleme Dili) kullanılarak yapılmıştır. Ek C'de bunlar hakkında bilgiler yer almaktadır. Ayrıca harita ile ilgili kullanımlar Google Maps API ile sağlanmıştır.

Web arayüzündeki coğrafi çerçeveleme, şifre çözme ve e-posta gönderme gibi bazı uygulamalar ücretsiz alınan alanlarla sağlanamadığı için tezin belli bir aşamasında ücretli alana geçilmek zorunda kalınmıştır.

Web arayüzünü kullanmak için kullanıcıların üye olması gerekmektedir. Arayüzde kullanıcıların konumları gösterildiği için bir üyelik sistemi getirilmesi zorunlu olmuştur. Ayrıca her kullanıcının her kullanıcıya ait konum bilgilerine erişebilmesini engellemek amacıyla kullanıcıların birbirlerine bu yetkiyi vermeleri gerekmektedir. Bunun için kullanıcıların görmek istedikleri kullanıcıya talep göndermeleri ve kabul edilmeleri gerekmektedir. Kullanıcılar ayrıca ileriki bir zamanda ekledikleri kullanıcıyı silebilmektedirler.

Harita uygulamalarında ise Google Maps API'nin sunduğu birçok özellik web arayüzünde uygulanmıştır. Kullanıcının son bulunduğu konum, ya da belirlenen bir zaman aralığına kadar izlediği yol gösterilebilmektedir. Ayrıca birden fazla kullanıcının konumları da gösterilebilmektedir. Bunun için bir grup gösterimi haritası oluşturulabilmektedir.

Burada kısaca değinilmiş olan web arayüzünün özellikleri detaylı bir şekilde anlatılacaktır.

6.2.2 Web Arayüzünün Yapısı ve Kullanımı

6.2.2.1 Üyelik

Web arayüzünün ve dolayısıyla cep telefonu ile takip sisteminin tümünün kullanılması için kullanıcıların web arayüzüne ücretsiz üye olmaları gerekmektedir. Üyelik işlemlerinin yapılabileceği sayfaya anasayfadaki linkten ulaşılabilmektedir. Şekil 6.8'de yeni üyelik sayfasının görünümü verilmektedir.

Şekil 6.8 Üyelik Sayfası.

Bu sayfanın arka planında JavaScript ile çalışan ve girilen bilgilerin mantıklı olup olmadığını kontrol eden kodlar bulunmaktadır. Böyle bir uygulama mantıklı girdileri almak açısından önemlidir. Ayrıca kullanıcılar farkında olmadan bu tip bilgileri girebilmektedirler.

Kullanıcı adının çok kısa ya da uzun olmasını engellemek amacıyla kullanıcı adının 5 ila 20 karakter arasında olması istenmektedir.

Kullanıcı adı doğru uzunlukta girildikten sonra şifrenin de belli sınırlamalar içerisinde girilmesi istenmektedir. 5 ila 10 karakterin dışındaki şifreler kabul edilmemektedir. Çok kısa şifreler güvenlik açısından iyi değilken çok uzun şifrelerin ise akılda tutulma zorluğundan dolayı kullanıcıya sorun oluşturabileceği değerlendirilmiştir.

Kullanıcı isminin de 5 ila 30 karakter olması istenmektedir. İsimlerin isim ve soy isim ile birlikte toplam olarak ortalama bu uzunluklarda olduğu düşünülmüştür. Belirlenmiş sayıdaki karakteri tutmadığında isimle ilgili uyarı verilmektedir.

E-posta uzunluğunun 10 ila 40 arasında olması beklenmektedir. Ayrıca e-postaların belirli karakter yapıları olmasından dolayı bunlar da kontrol edilmektedir. E-postada uzunluk dışında kontrol edilen hususlar şunlardır:

- E-posta içerisinde “@” karakteri bulunmalıdır.
- “@” işaretinden önce en az bir karakter bulunmalıdır.
- “@” karakterinden ve “.” işaretinden önce en az bir karakter; “.” işaretinden sonra ise iki ya da üç karakter bulunmalıdır.

Cep telefonu numarası 10 ila 15 karakter uzunluğunda olmalıdır.

IMEI numarasının standart uzunluğu 15’tir. Ama bazı telefonlarda bu uzunluğun farklı olabileceği düşünülerek 10 ila 19 arasında bir uzunluk istenmektedir. IMEI numarasının bilinmesi kullanıcı ayırt etmede ve doğrulama sağlanmasında ayrı bir önem arz etmektedir.

Bütün bilgiler uygun girildiğinde “Kaydol!” düğmesine basılmaktadır. Kullanıcı adının daha önce başkası tarafından alınıp alınmadığı kontrol edilmektedir. Bunun için ise kullanıcılara ait bilgilerin bulunduğu veri tabanında bulunan kullanıcı adları kontrol edilmektedir. Eğer kullanıcı adı daha önce başka bir kullanıcı tarafından alınmış ise bir uyarı çıkmaktadır.

Eğer kullanıcı adı başkası tarafından alınmamış ise kayıdın gerçekleştirildiğini belirten sayfaya yönlendirilmektedir. Bu sayfada kullanıcılara ait bilgilerin bulunduğu veritabanına yeni kullanıcı girişi yapılıp bu kullanıcıya özel bir kullanıcı ID numarası tahsis edilmektedir.

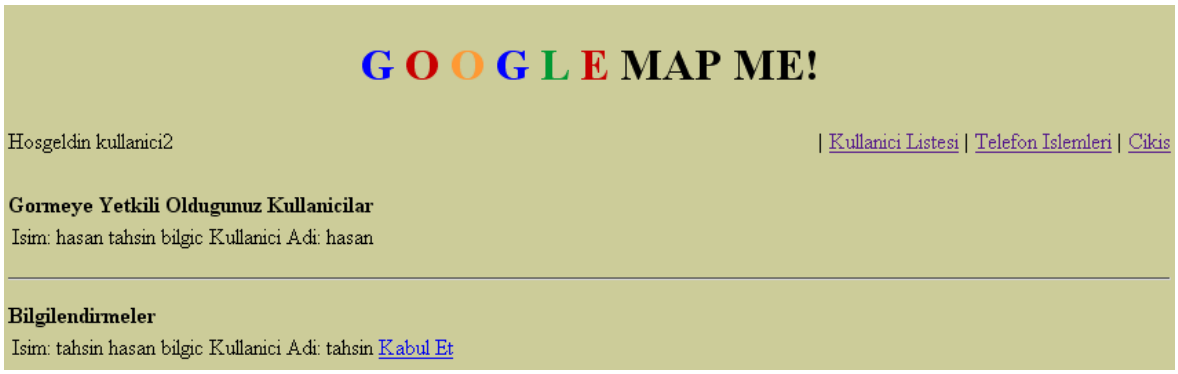
6.2.2.2 Web Arayüzü Girişi ve Anasayfa

Kullanıcı, kullanıcı adı ve şifre ile kaydolduktan sonra Şekil 6.9‘daki web arayüzünün açılış sayfasına giderek yeni alınan kullanıcı adı ve şifre ile giriş yapabilmektedir.

Şekil 6.9 Googlemapme.net Açılış Sayfası.

Girilen bilgiler kullanıcı veritabanındaki bilgiler ile örtüşmezse kullanıcı adı ya da şifrenin yanlış olabileceğine dair bir uyarı ekrana çıkmaktadır.

Eğer giriş başarı ile tamamlanır ise Şekil 6.10'daki anasayfa ekranı açılmaktadır.



Şekil 6.10 Anasayfa.

Anasayfada kullanıcının görmeye yetkili olduğu kullanıcıların listesi ve aynı zamanda kullanıcıya yönelik herhangi bir ekleme talebi gelip gelmediği görülebilmektedir.

6.2.2.3 Kullanıcı Listesi

Kullanıcı listesi sayfasında kullanıcıları ekleme, silme işlemleri yapılabilmektedir. Kullanıcı, önceden kendi yaptığı talepleri iptal edebilmektedir. Aynı zamanda kendine gelen talepleri kabul edebilmektedir. Şekil 6.11'deki kullanıcı listesi sayfasında kullanıcının görmeye yetkili olduğu bir kullanıcı bulunmaktadır. Talep edebileceği de bir kullanıcı listelenmiştir. Ayrıca kendisi bir kullanıcıya talep iletmiş ve kendisine de başka bir kullanıcıdan bir talep gelmiştir. Bu sayfada kullanıcı adıyla kullanıcı da aranıp eklenebilmektedir.

Şekil 6.11 Kullanıcı Listesi Sayfası.

6.2.2.3.1 Kullanıcı Ekleme

Bir kullanıcıyı eklemek için talep yapıldığında kullanıcı durumları veri tabanında iki kullanıcı arasındaki ilişki “ilerleme halinde” olarak değiştirilmektedir.

6.2.2.3.2 Talep Değerlendirme

Kullanıcı kendisine yapılmış talebi kabul ettiğinde durum veri tabanında iki kullanıcı arasındaki ilişki “izin verildi” şeklinde değiştirilmektedir.

Eğer kendisine yapılan talebi kabul etmezse durum veritabanı “kabul edilmedi” şeklinde güncellenmektedir.

6.2.2.3.3 Kullanıcı Silme

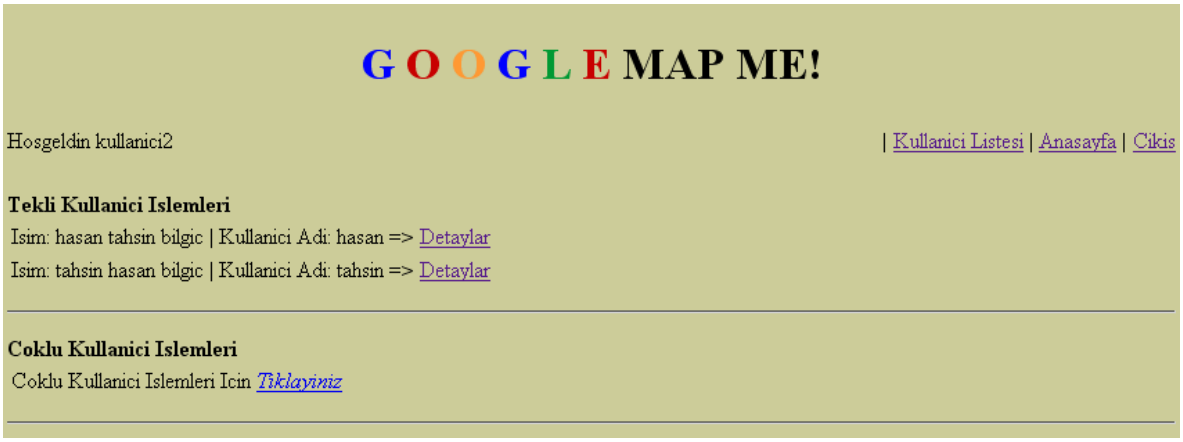
Kullanıcı eğer izin verdiği kişilerden birisini silmek isterse kullanıcı durum veritabanında iki kullanıcı arasındaki ilişki tamamen silinmektedir.

6.2.2.3.4 Talep İptali

Kullanıcı yaptığı talebi iptal etmek istediğinde durum veritabanından ikisi arasındaki ilişki tamamen silinmektedir.

6.2.3 Telefon İşlemleri

Bu sayfada kullanıcılar bilgilerini görmeye yetkili oldukları diğer kullanıcıların tek tek veya grup halinde harita üzerinde konumlarını görebilmektedirler. Telefon işlemleri sayfası Şekil 6.12'de gösterilmektedir.



Şekil 6.12 Telefon İşlemleri Sayfası.

6.2.3.1 Tek Kullanıcı İşlemleri

Tek kullanıcı ile ilgili işlem yapmak ve bilgilerini görebilmek için telefon işlemleri sayfasında tek kullanıcı işlemleri altında sıralanmış görmeye yetkili olunan kullanıcılardan herhangi birinin yanındaki detaylar linkine tıklanması gerekmektedir. Kullanıcı detayları sayfası Şekil 6.13'de verilmektedir.

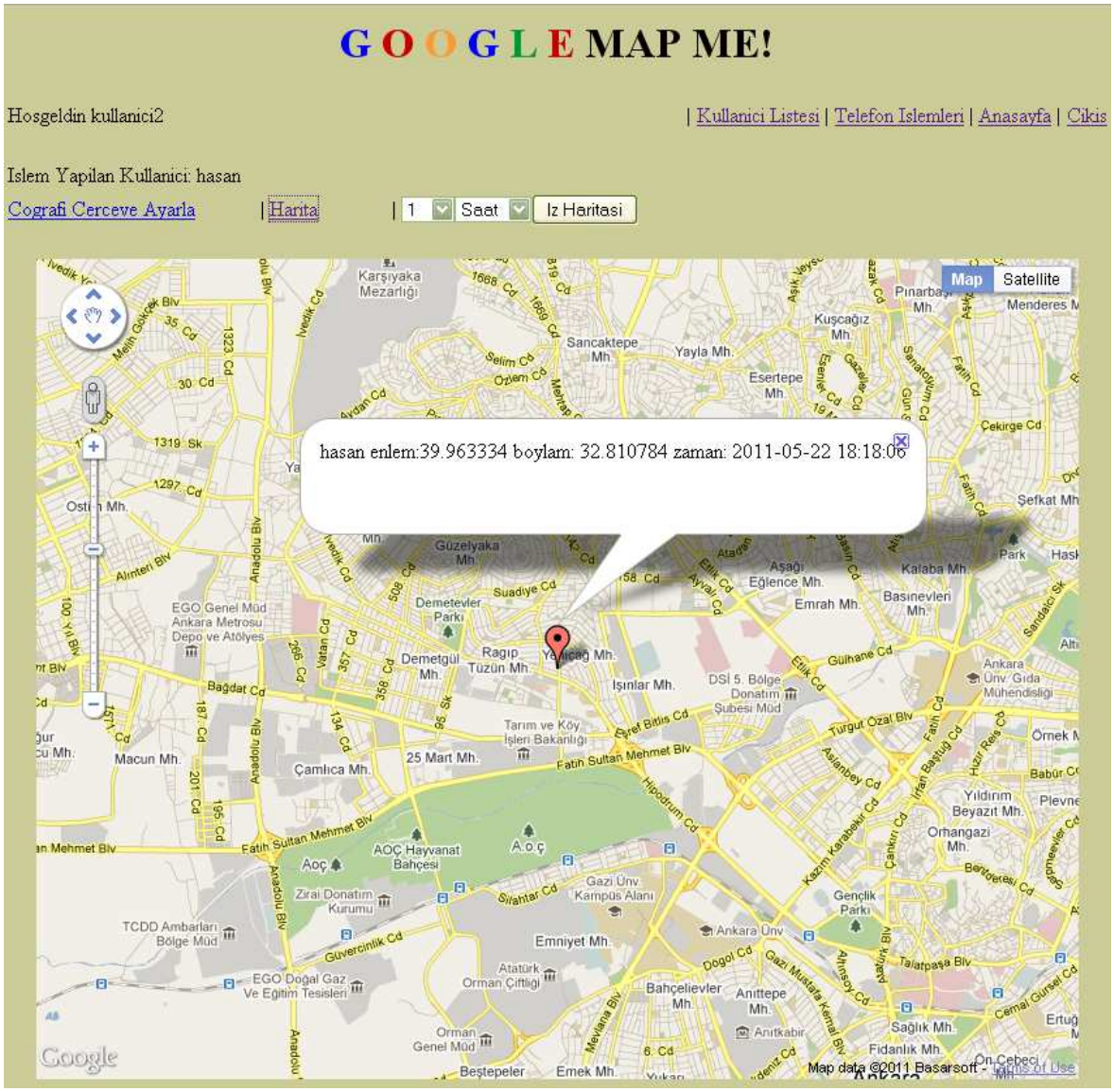
Şekil 6.13 Kullanıcı Detayları Sayfası.

Eğer detayları görülmek istenen kullanıcıya ait herhangi bir koordinat bilgisi yoksa Şekil 6.14'deki gibi koordinat bilgisinin bulunmadığını belirten bir uyarının da yer aldığı bir sayfa görüntülenmektedir.

Şekil 6.14 Koordinat Bilgisi Bulunmayan Kullanıcıya Ait Detaylar Sayfası.

6.2.3.1.1 En Son Konum Haritası

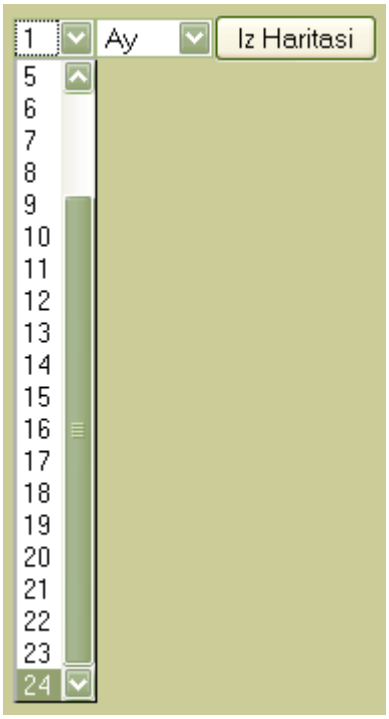
Kullanıcı detayları sayfasında haritaya tıklanarak kullanıcıya ait veritabanına işlenmiş en son konum Google Maps haritası üzerinde görüntülenebilmektedir. Haritadaki konum işaretine tıklandığında o konuma ait zaman ve koordinat bilgileri bir bilgi penceresinde gösterilmektedir. Bahsi geçen harita ekranı Şekil 6.15'de gösterilmiştir.



Şekil 6.15 Kullanıcı Konumun Google Maps Üzerinde Gösterilmesi.

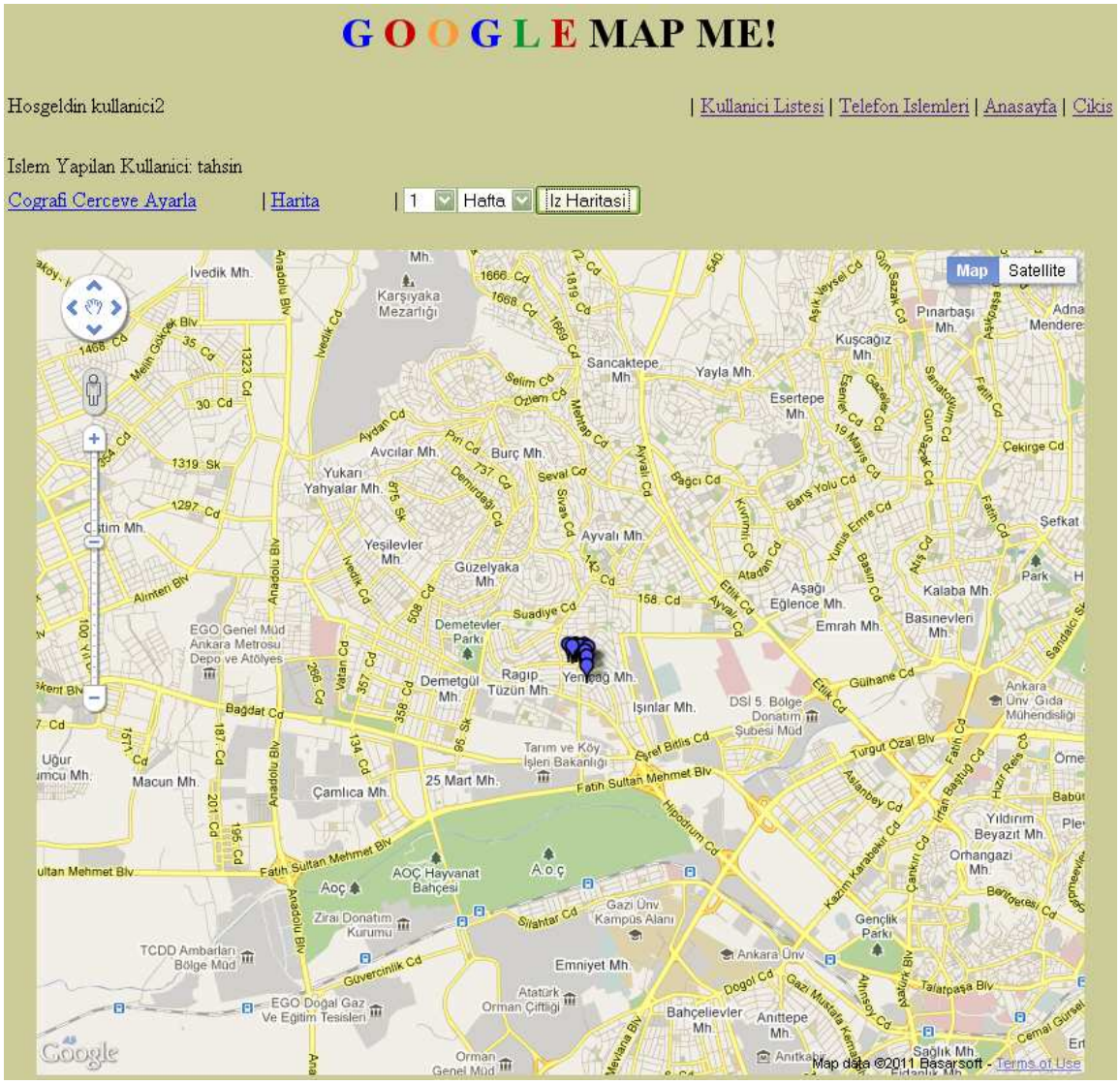
6.2.3.1.2 İz Haritası

İzleme Haritası'nda en son ne kadar süre ile kullanıcıya ait konumlar görüntülenecek ise süre seçilmesi gerekmektedir. 24 aya kadar süre seçme seçeneği vardır. İz Haritası için süre seçimi Şekil 6.16'da gösterilmektedir.



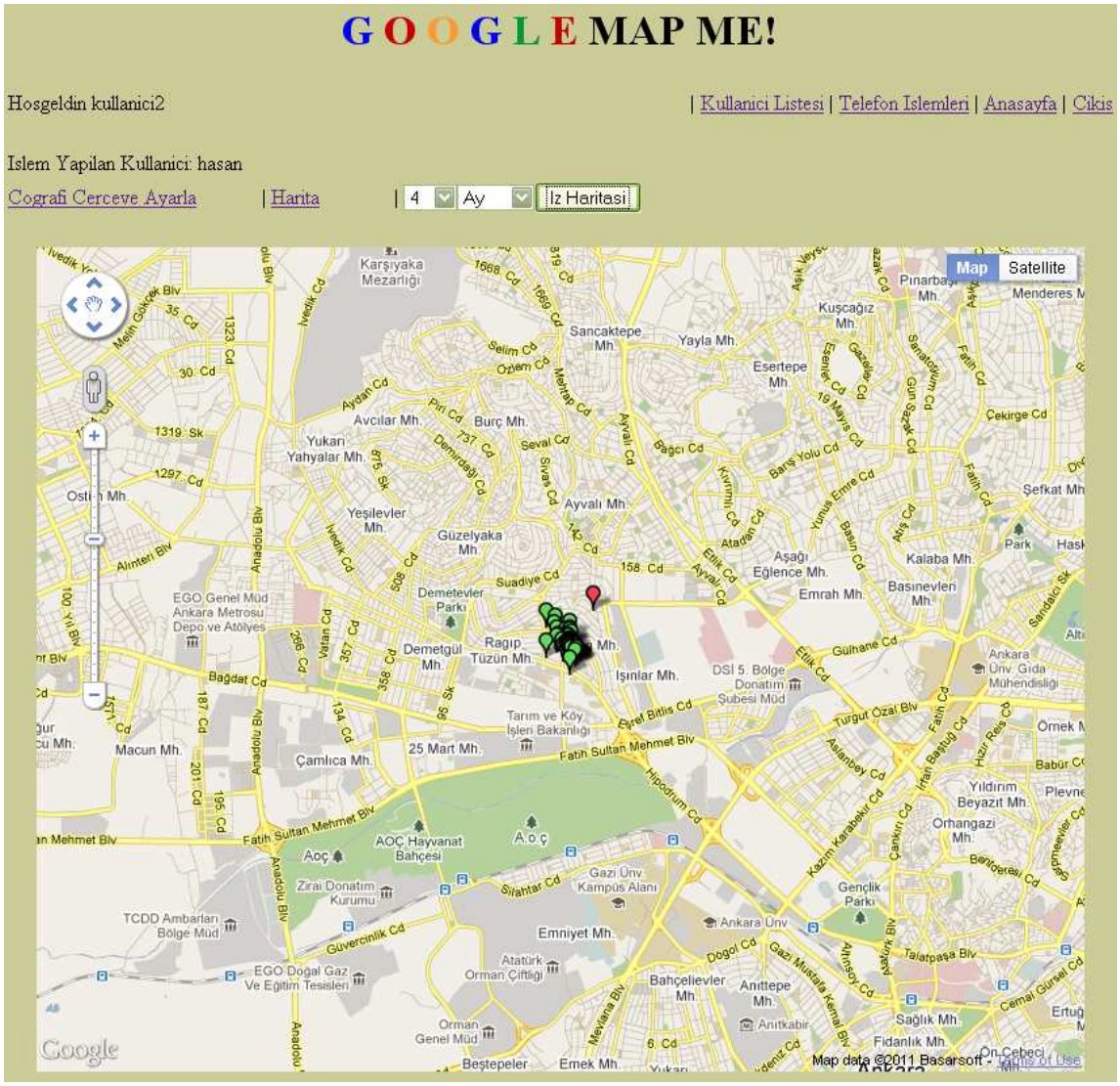
Şekil 6.16 Grup Haritası Süresi Belirlenmesi.

İz haritası düğmesine basıldığında o kullanıcıya ait seçilen süre içerisindeki tüm konum bilgileri ekrana gelmektedir. Ekrana gelen haritada kullanıcıya ait izler mavi renkte ya da yeşil ve kırmızı renklerde olmaktadır. Eğer kullanıcı için herhangi bir coğrafi çerçeveleme ayarlanmamışsa kullanıcı koordinatları haritada mavi işaretler ile gösterilmektedir. Benzer bir harita sayfası Şekil 6.17'de verilmektedir. Burada herhangi bir işaretin üzerine gelindiğinde o işaretin hangi tarih ve saate ait olduğu kullanıcı adıyla beraber gösterilmektedir.



Şekil 6.17 Coğrafi Çerçeveleme Uygulaması Yapılmadan İz Haritası Gösterimi.

Eğer kullanıcı için ayarlanmış koordinat limitleri varsa çerçeve içerisindeki koordinatlar harita üzerinde yeşil işaret ile gösterilirken çerçevenin dışında kalan koordinatlar kırmızı işaret ile gösterilmektedir. Şekil 6.18'de böyle bir harita uygulaması gösterilmektedir.



Şekil 6.18 Coğrafi Çerçeveleme Uygulandığında İz Haritası Gösterimi.

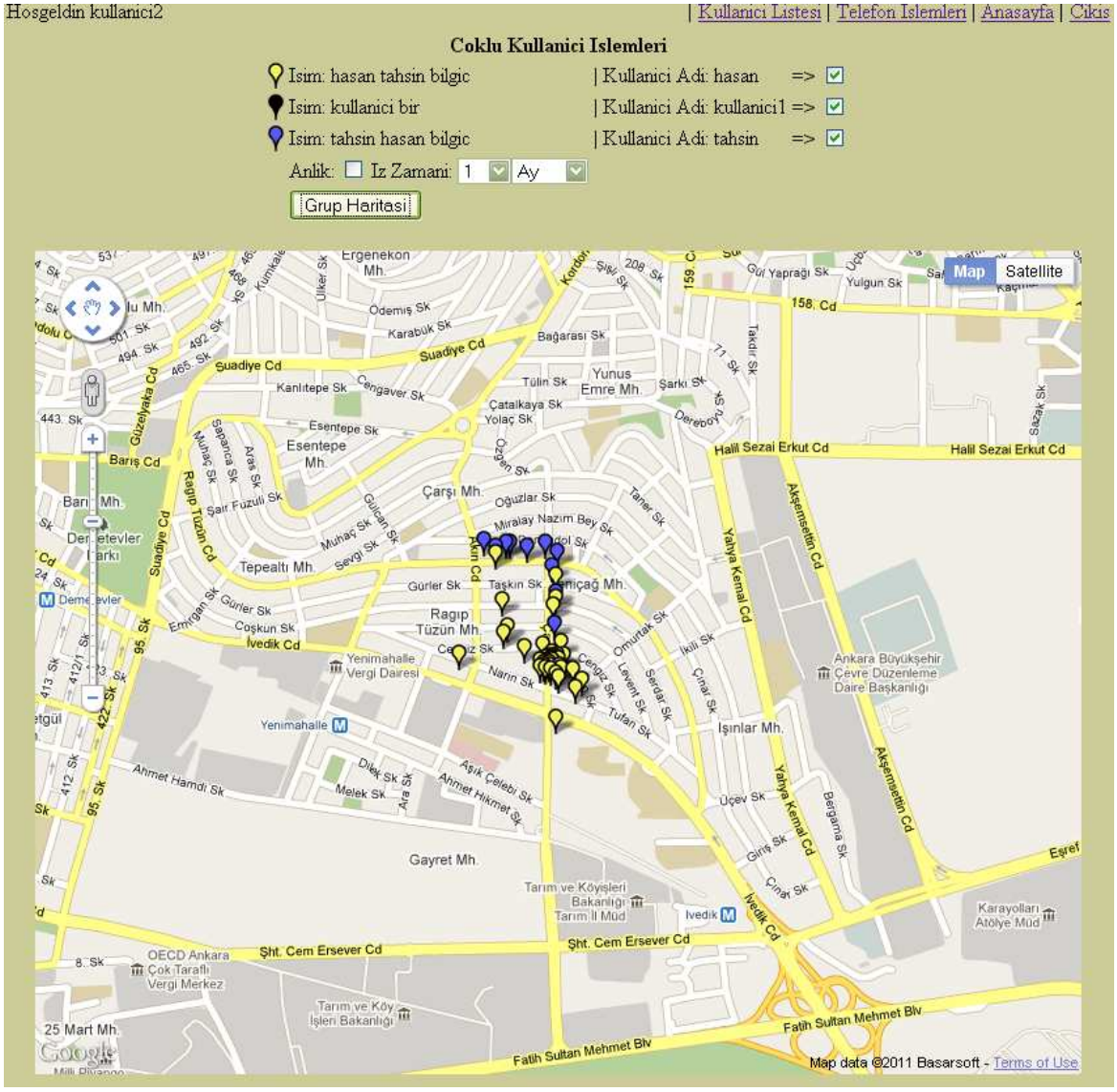
6.2.3.2 Çoklu Kullanıcı İşlemleri

Çoklu kullanıcı işlemlerinin yapılabildiği sayfanın görünüşü Şekil 6.19'da verilmektedir. Bu şekilde birçok kullanıcıya hizmet verilmektedir.

Şekil 6.19 Çoklu Kullanıcı İşlemleri.

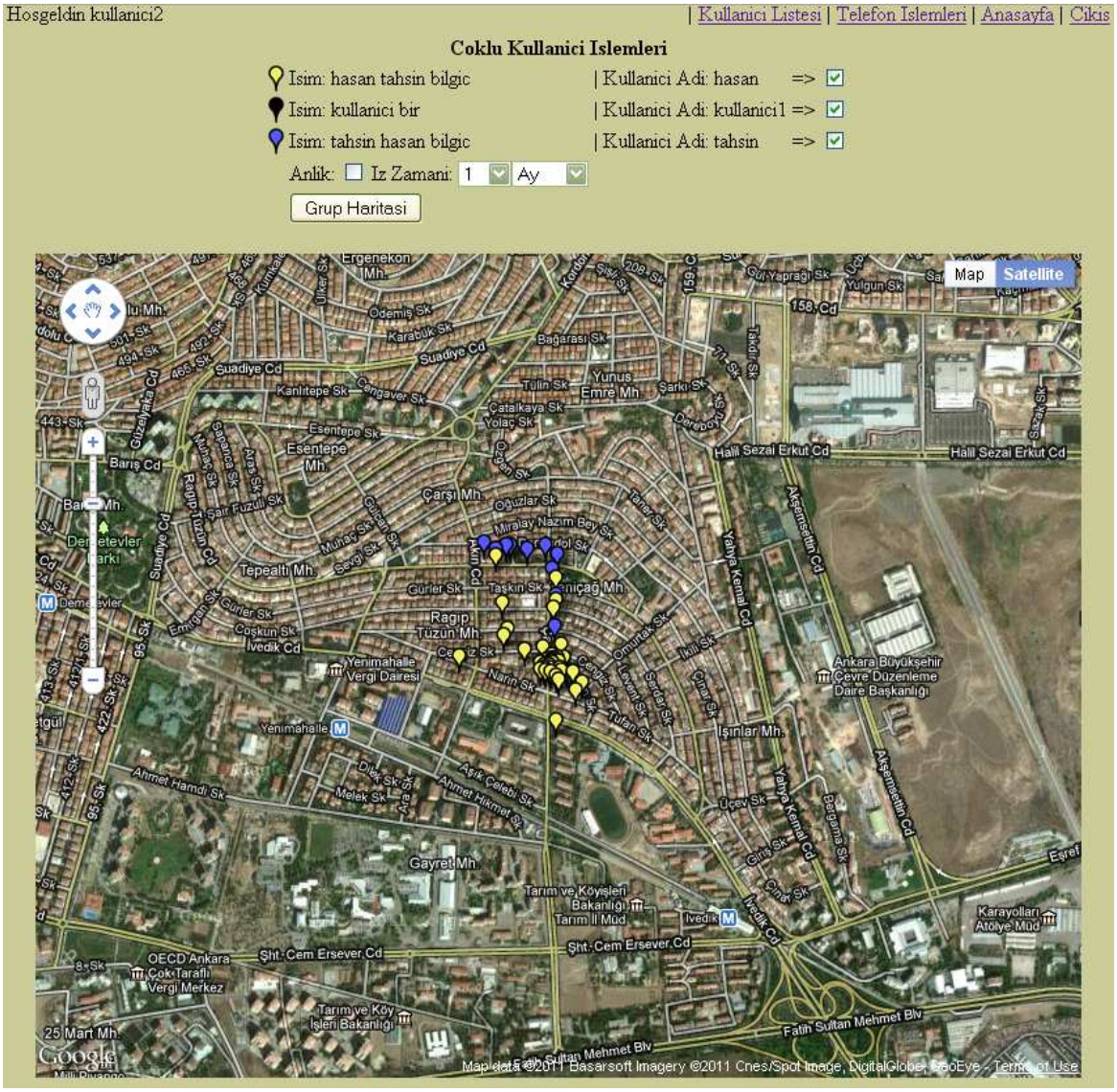
Bu sayfada listelenen kullanıcılar bilgilerini görmeye yetkili olunanlardır. Bu kullanıcıların yanlarındaki işaret kutusuna tıklanarak o kullanıcıya ait bilgilerin de Google Maps haritası üzerinde gösterilmesi sağlanmaktadır. Kullanıcıların isimlerinin önündeki renkli işaretler harita üzerinde hangi işaret ile gösterileceklerini ifade etmektedir. Haritanın süresi için aşağıya açılır liste ile 24 aya kadar seçenekler yerleştirilmiştir. İstenirse anlık seçeneği işaretlenerek kullanıcılara ait alınmış en son konum bilgileri de harita üzerinde gösterilebilmektedir.

Şekil 6.20'de birden fazla kullanıcının bulunduğu bir harita gösterilmektedir. Kullanıcılar farklı renklerle verilmiştir.



Şekil 6.20 Birden Fazla Kullanıcının Harita Üzerinde Gösterilmesi.

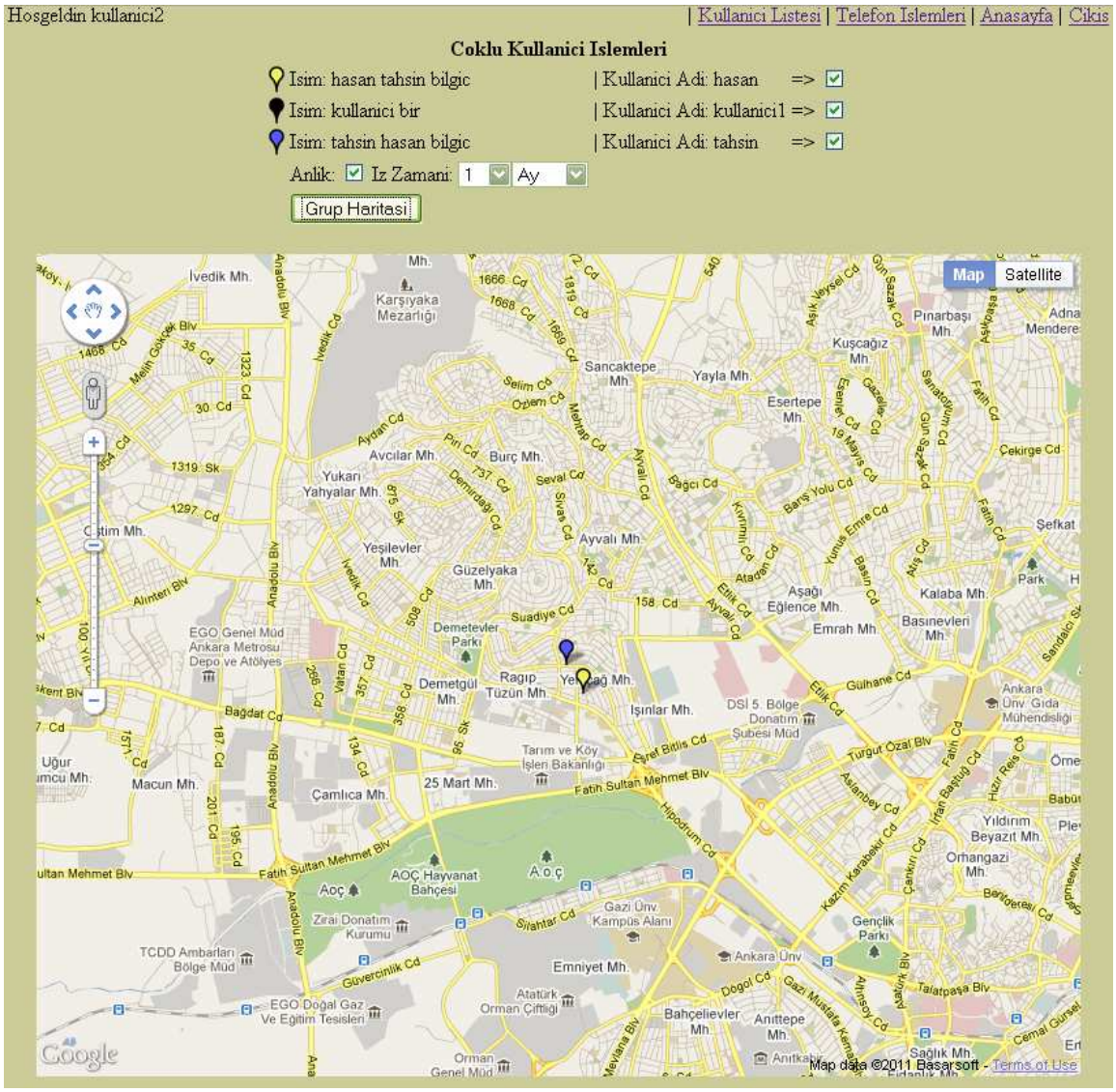
Eğer istenir ise haritalar için uydu haritaları da kullanılabilmektedir. Bunun için haritanın sağ üst köşesindeki Satellite (Uydu) düğmesine tıklanmalıdır. Şekil 6.20'deki haritanın uydu haritası Şekil 6.21'da verilmektedir.



Şekil 6.21 Birden Fazla Kullanıcının Uydu Haritası Üzerinde Gösterilmesi.

Şekil 6.22'de anlık seçeneği seçilerek işaretlenmiş kullanıcılardan alınmış en son konumlar harita üzerinde gösterilmektedir. Anlık seçeneği seçiliyse uygulama zaman aralığına bakmamaktadır.

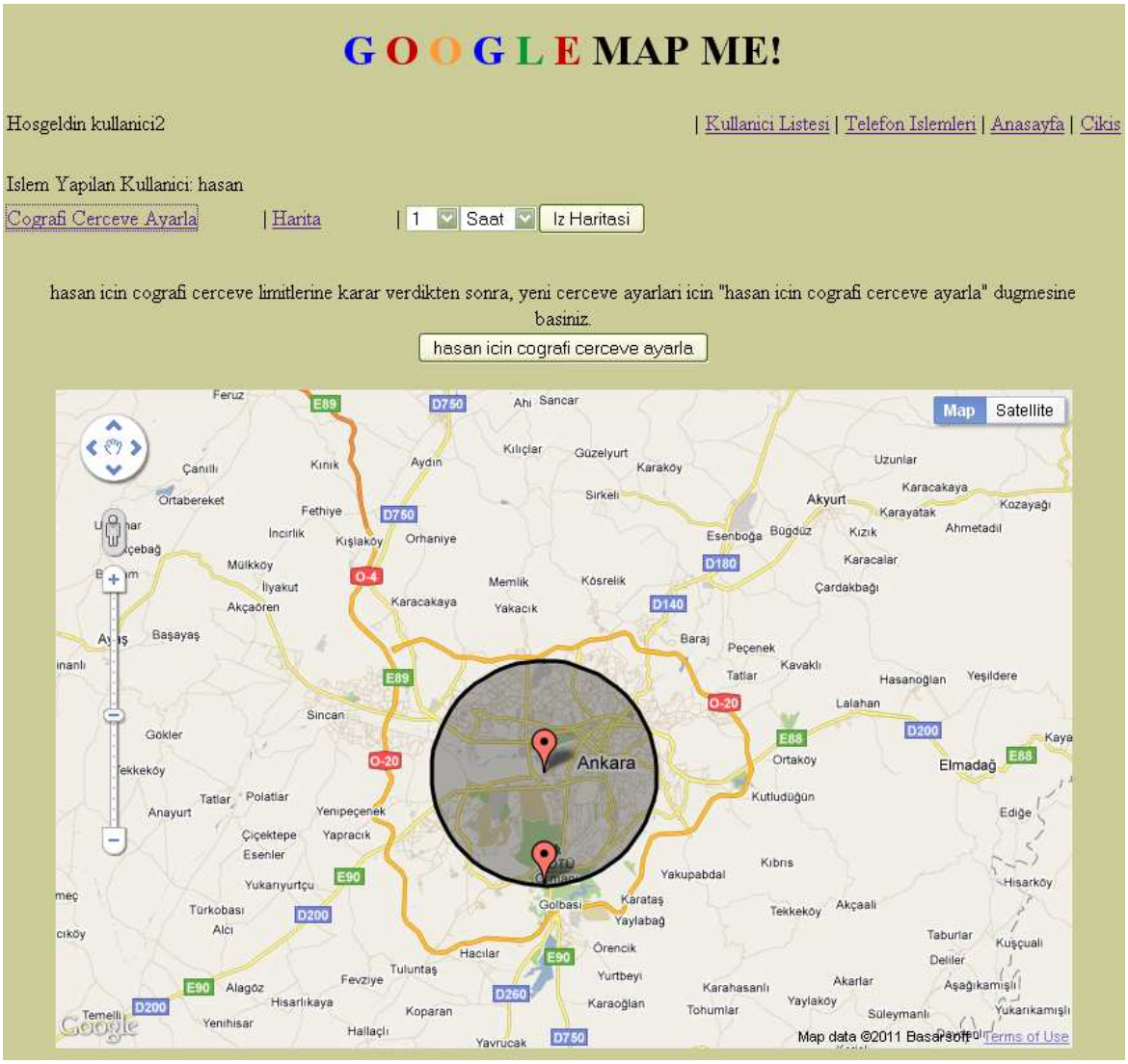
Çoklu kullanıcı uygulamaları ile ilgili verilmiş haritalarda siyah işaretli kullanıcı görünmemektedir. Bunun sebebi bu kullanıcıya ait herhangi bir koordinat bilgisinin veritabanında bulunmamasıdır.



Şekil 6.22 Birden Fazla Kullanıcıya Ait Alınmış En Son Konumların Haritası.

6.2.4 Coğrafi Çerçeve Ayarlama

Kullanıcı detayları sayfasından kullanıcı için bir coğrafi çerçeveleme ayarlanması da mümkündür. Böyle bir çerçevenin ayarlanmasında Google Maps API'de bulunan katman ve çizim sınıfları kullanılmaktadır. Küresel hesaplamalar için ise daha önceden Google Maps API bölümünde bahsedilen Geometry kütüphanesinden yararlanılmaktadır. Bir kullanıcı için böyle bir çerçeve oluşturulduktan sonra "Coğrafi Çerçeve Ayarla" linkine basılarak bu verinin veritabanına girmesi sağlanmaktadır. Bu uygulamanın yapıldığı sayfa Şekil 6.23'de gösterilmektedir.



Şekil 6.23 Bir Kullanıcı için Coğrafi Çerçeve Oluşturulması.

Çerçeve şekli olarak çember seçilmiştir. Bu çerçeve için koordinat ayarlanırken iki parametreyle oynanmaktadır. Bunlar çemberin merkezi ve yarıçapıdır. Yarıçap uzunluğu hesaplanması, iki işaret arasındaki uzaklığın küresel formüller ile hesaplanmasıyla bulunmaktadır. Bu formüllerin uygulanmasında Google Maps API'de yer alan Geometry kütüphanesinden ve Çember sınıfından yararlanılmaktadır.

6.2.5 GPS Verisi Alınması İşlemleri

GPS verisinin alınması cep telefonu takibi sisteminin çok önemli bir parçasını oluşturmaktadır. Cep telefonunda GPS yongasından alınan GPS konum bilgisi

telefonda çalışan yazılımla şifrelenip ID numarası ile birlikte web sunucusuna gönderilmektedir.

Web sunucusunda PHP kodları kullanılarak veri alınmaktadır. Alınan veri şifrelenmiş olmasından dolayı ilk yapılan iş bu verinin çözülmesidir. Şifrelenmiş GPS verisiyle beraber gelen ID numarası kullanılarak kullanıcıya ait IMEI numarası veritabanından alınmaktadır. IMEI numarası 128 bit'e tamamlanarak AES-Rijndael şifre çözme algoritmasında kullanılabilecek hale getirilmektedir.

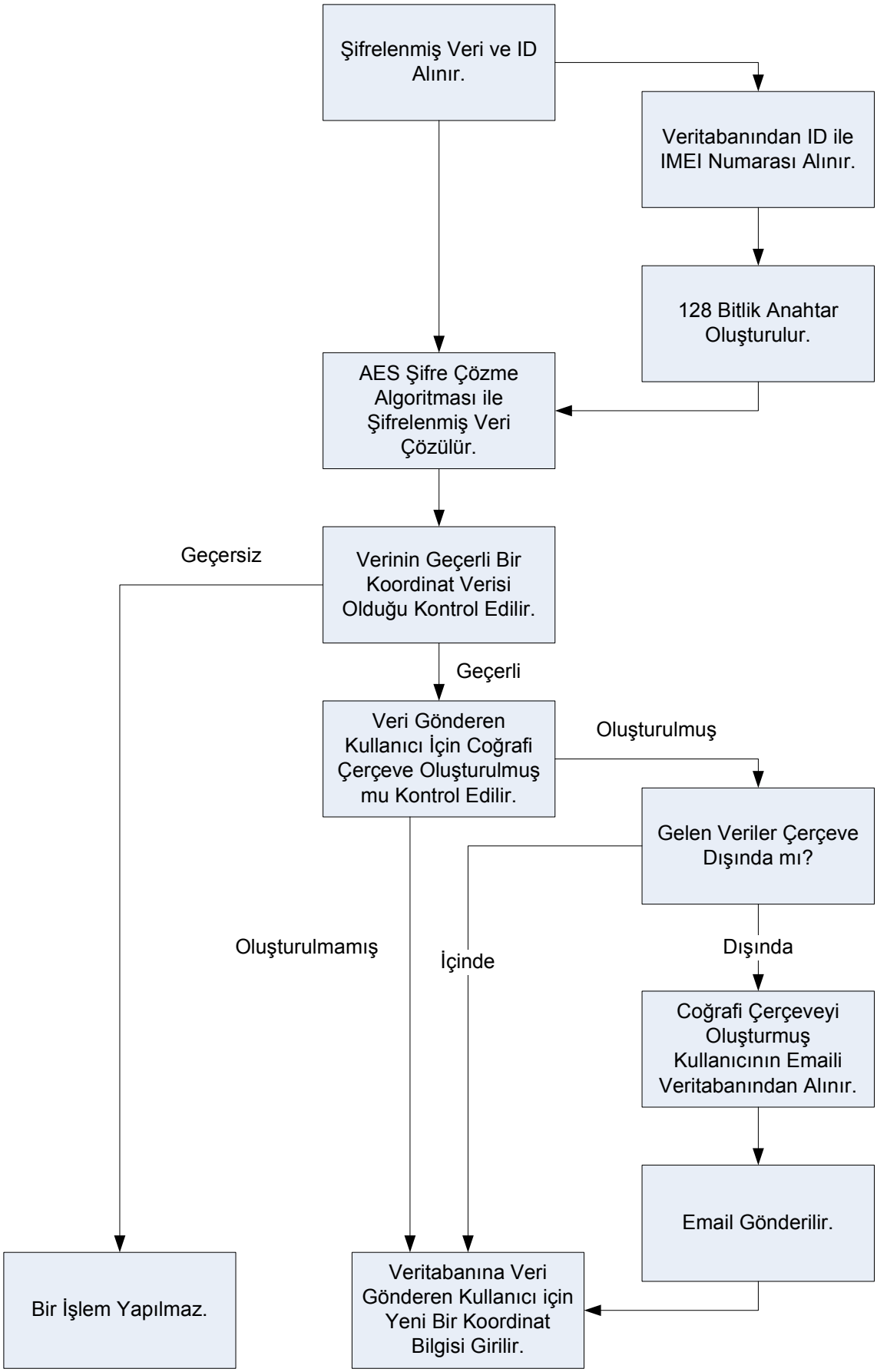
Şifrelenmiş veri oluşturulan anahtar yardımıyla çözülmektedir. Veri parçalanıp enlem ve boylam verileri çıkarılmaktadır. Bu verilerin geçerli veriler olup olmadığına bakılmaktadır. Eğer geçerliyse işlemlere devam edilmektedir. Değilse başka işlem yapılmamaktadır.

Veritabanında veri göndermiş olan kullanıcı için herhangi bir çerçeve belirlenip belirlenmediği kontrol edilmektedir. Eğer herhangi bir çerçeve belirlenmemişse enlem ve boylam sunucu zamanıyla beraber veritabanına işlenmektedir. Eğer bir çerçeve belirlenmişse çözülmüş enlem ve boylam bilgileri çerçeve ile karşılaştırılmaktadır. Çerçevenin içinde olup olmadığına bakılmaktadır. Eğer içindeyse veri tabanına aktarılmaktadır. Eğer koordinat bilgisi çerçevenin içerisinde değilse çerçeveyi oluşturan kullanıcının e-posta adresi veritabanından alınmaktadır. İlgili kullanıcıya çerçeve dışına çıkmış kullanıcının çerçeve dışına çıktığına dair e-posta gönderilmektedir. Sonra da veri göndermiş kullanıcının koordinat bilgileri sunucu zamanıyla beraber veritabanına işlenmektedir.

Çerçeve hesaplamalarında Haversine hesaplamaları kullanılmaktadır. Bölüm 6.2.5.1'de bu hesaplamaların nasıl yapıldığına değinilmektedir.

Şifre çözme işlemlerinde Mcrypt kütüphanesinden yararlanılmıştır. Mcrypt kütüphanesinden bölüm 6.2.5.2'de bahsedilmektedir.

Çizelge 6.9'da GPS alınması işleminin şeması verilmiştir.



Çizelge 6.9 GPS Alınması Şeması.

6.2.5.1 Haversine Hesaplamaları

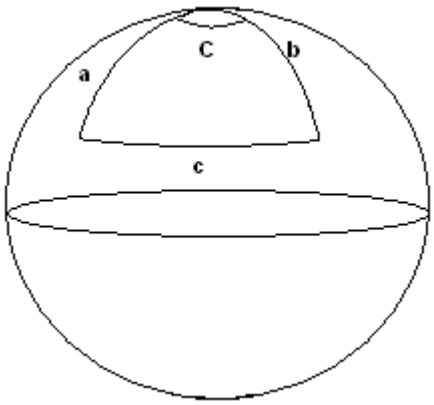
Dünya üzerindeki iki nokta arasındaki uzaklığı düzlemsel geometri ile hesaplamak yanlış sonuçlar vermektedir. Burada küresel dünyanın düzleme aktarılmasının zorluklarını göstermesi bakımından çerçeveleme uygulaması ile çizilen bir çemberin düzlemsel dünya haritası üzerinde oluşturduğu sinüs benzeri şekil gösterilecektir. Şekil 6.24'de bu şekil verilmektedir. Burada aslında ekvatora belli bir açı yapan çember dünyanın tamamını sarmaktadır. Düzlemde bu şekli almaktadır.

Şekil 6.24 Küresel Dünyada Çizilen Çemberin Düzlemsel Dünyaya Aktarılması.

Kürenin düzleme aktarılmasındaki zorluklardan dolayı küre üzerine uygulanmış formüllerin kullanılması gerekmektedir. Bu hesaplamalarda öne çıkan üç hesaplama yöntemi bulunmaktadır. Bunlar: Küresel cosinus kuralı ile hesaplamak, Haversine formülü ile hesaplamak ve Vincencty yöntemi ile hesaplamaktır. Vincenty yöntemi en doğru sonucu vermektedir. Yalnız hesaplamaların karmaşıklığı ve uzunluğu yazılımlara yük olmaktadır. Ayrıca bu yöntem asıl farkını kutuplara yaklaştıkça kanıtlamaktadır. Küresel cosinus kuralı ya da Haversine formüllerinden birisiyle hesaplamak yakın sonuçlar vermektedir. Ama küresel cosinus kuralı uygulandığında uzaklığı hesaplanan noktalar çok yakın olduklarında anlamsız sonuçlar elde edilmektedir. Bunlardan dolayı çerçeve hesaplamalarında

Haversine formülü kullanılmıştır. Aslında Haversine formülü de küresel cosinus kuralının özel bir durumudur.

Şekil 6.25'de dünya yüzeyine çizilmiş bir üçgen üzerinde gerekli hesaplamaları yaparak c kenarı ile gösterilen uzaklığı bulmak mümkündür.



Şekil 6.25 Küresel Üçgen.

Haversine formülüne ulaşmak için ilk önce küresel cosinus kuralını yazmak gerekmektedir.

$$\cos(c) = \cos(a)\cos(b) + \sin(a)\sin(b)\cos(C) \quad \textbf{(6.1)}$$

(6.1)'de verilmekte olan bu formülden

$$haversin(\theta) = sin^2(\theta/2) = (1 - cos(\theta))/2 \quad \textbf{(6.2)}$$

$$\cos(a-b) = \cos(a)\cos(b) + \sin(a)\sin(b) \quad \textbf{(6.3)}$$

(6.2) ve (6.3)'ten de yararlanarak

$$1 - 2haversin(c) = \cos(a-b) - \sin(a)\sin(b) + \sin(a)\sin(b)\left(1 - 2haversin(C)\right) \quad \textbf{(6.4)}$$

(6.4)'e ulaşmak mümkündür.

$$1 - 2haversin(c) = 1 - 2haversin(a-b) - \sin(a)\sin(b) + \sin(a)\sin(b)\left(1 - 2haversin(C)\right) \quad \textbf{(6.5)}$$

(6.5)'ten, (6.6) çıkarılabilmektedir.

$$1-2haversin(c)=1-2haversin(a-b)-\sin(a)\sin(b)+\sin(a)\sin(b)+2\sin(a)\sin(b)haversin(C) \quad \textbf{(6.6)}$$

(6.6) sadeleştirildiğinde (6.7)'ye ulaşılmaktadır.

$$haversin(c)=haversin(a-b)+\sin(a)\sin(b)haversin(C) \quad \textbf{(6.7)}$$

(6.7)'de ulaşılan sonucun dünyaya uygulanabilmesi için a yerine $enlem_1$ ve b yerine $enlem_2$ getirilmesi gerekmektedir. Şekil 6.25'deki küresel üçgende kuzey kutup noktasından başlayan bir üçgen olduğu kabul edilir ise (6.7)'deki formülde a yerine $\frac{\pi}{2}-enlem_1$ ve b yerine $\frac{\pi}{2}-enlem_2$ gelmektedir. Çünkü enlemler 0º-90º arasında değişmektedir.

$$haversin(c)=haversin\left(\frac{\pi}{2}-lat_1-\frac{\pi}{2}+lat_2\right)+\sin(\frac{\pi}{2}-lat_1)\sin(\frac{\pi}{2}-lat_2)haversin(C) \quad \textbf{(6.8)}$$

(6.7), (6.8) halini almaktadır. Trigonometriden $\sin\left(\frac{\pi}{2}-\theta\right)=\cos(\theta)$ olduğu bilinmektedir. (6.8), (6.9) haline gelmektedir.

$$haversin(c)=haversin\left(lat_2-lat_1\right)+\cos(lat_1)\cos(lat_2)haversin(C) \quad \textbf{(6.9)}$$

(6.9)'de C yerine boylam farkı olmasından dolayı $\Delta boylam$ yazmak mümkündür. Birim kürede c radyan cinsinden açı değerine eşit olmaktadır. Bu kenarın uzunluğuna d denirse

$$d=\frac{2\pi R}{360}\frac{c}{180\pi}=Rc \quad \textbf{(6.10)}$$

(6.10) elde edilmektedir. Burada $\frac{c}{180\pi}$, c'nin derece cinsinden değeridir. Buradan c yerine $\frac{d}{R}$ yazılabileceği görülmektedir. Bu bulgular doğrultusunda (6.9),

$$haversin\left(\frac{d}{R}\right)=haversin\left(lat_2-lat_1\right)+\cos(lat_1)\cos(lat_2)haversin(\Delta boylam) \quad \textbf{(6.11)}$$

(6.11) halini almaktadır. Buradan ters haversin ya da arcsin uygulanarak d (6.12)'deki gibi bulunmaktadır.

$$d = Rhaversin^{-1}\left(haversin\left(\frac{d}{R}\right)\right) = 2R\arcsin\left(\sqrt{haversin\left(\frac{d}{R}\right)}\right) \quad \textbf{(6.12)}$$

6.2.5.2 Mcrypt Kütüphanesi

Mcrypt kütüphanesi crypt kütüphanesinin güncellenmiş halidir. Bu kütüphanede DES, AES, Blowfish gibi şifreleme algoritmaları ve ECB, CFB (Şifre Geri Beslemesi) gibi şifreleme kiplerine dair fonksiyonlar bulunmaktadır.

PHP'de şifreleme işlemlerinin yapılması bu kütüphane ile mümkün olmaktadır. İlk önce mcrypt ile rijndael-128 modülü oluşturulmaktadır. Anahtar bu algoritmanın kullanabileceği bir anahtar yapısına mcrypt fonksiyonlarıyla dönüştürülmektedir. Şifre çözme yapılmaktadır.

Mcrypt kütüphanesinin kullanılabilmesi için ya bu modülün yüklenmiş olması ya da web arayüzünün ve sunucusunun yer aldığı alan tarafından sağlanması gerekmektedir.

6.3 Konumlandırma Sistemine Yönelik Performans Değerlendirmeleri

Kullanıcılara yönelik geliştirilmiş sistemlerin performanslarının ölçülmesi için çok sayıda kullanıcı tarafından test edilmesi gerekmektedir. Yüzlerce kullanıcı ile test koşullarının sağlanması ise zor olmaktadır. Bundan dolayı test koşullarının simülasyonu yapılmaktadır ve sistemin oluşturulan test senaryolarında nasıl davranacağı, performansının nasıl olacağı ölçülebilmektedir. Konumlandırma sisteminin birçok kullanıcı tarafından kullanıldığında nasıl bir performans sergileyeceğinin anlaşılması için de testler uygulanmıştır. Bu testlerin gerçekleştirilmesi için iki hususun sağlanması gerekmektedir. Bunlar, sistemin olabildiğince çok kullanıcı ile denenmesi ve bu kullanıcıların aynı anda yani eşzamanlı olarak sistemi kullanmasıdır.

6.3.1 Yükleme Testi

Yükleme testi bir uygulamanın değişik senaryolarda test edilmesi için kullanılan bir yöntemdir. Beklenen olayın modellenmesi ve sonrasında bu modelin eşzamanlı olarak belirlenmiş sayıda kullanıcı tarafından kullanımının simüle edilmesi ile gerçekleştirilmektedir.

Yükleme testlerinde iki önemli kriter ön plana çıkmaktadır. Bunlar, yanıt süresi ve bağlantı oranı olarak verilmektedir [16]. Konumlandırma sistemi için koşulacak senaryolarda da bu kriterler not edilmekte ve değerlendirilmektedir.

Bu testin gerçekleştirilmesinde birçok program kullanılmaktadır. Konumlandırma sisteminin birçok eşzamanlı kullanıcı ile oluşturulan senaryolarda simüle edilmesinde Testing Master[1] programı kullanılmıştır. Buna benzer çoğu ücretli olan birçok program bulunmaktadır. Bu program değerlendirme süresince programın tüm özelliklerinin kullanılmasına izin vermektedir.

Testte senaryo olarak sunucuya GPS verilerinin kriptolu ya da kriptosuz olarak gönderilmesi sağlanmıştır. Senaryo 10 defa tekrarlanmış ve çıktıların ortalaması alınmıştır. Herbir tekrar arasında gecikme uygulanmamaktadır.

[1] Testing Master, http://www.siteloadtesting.com.

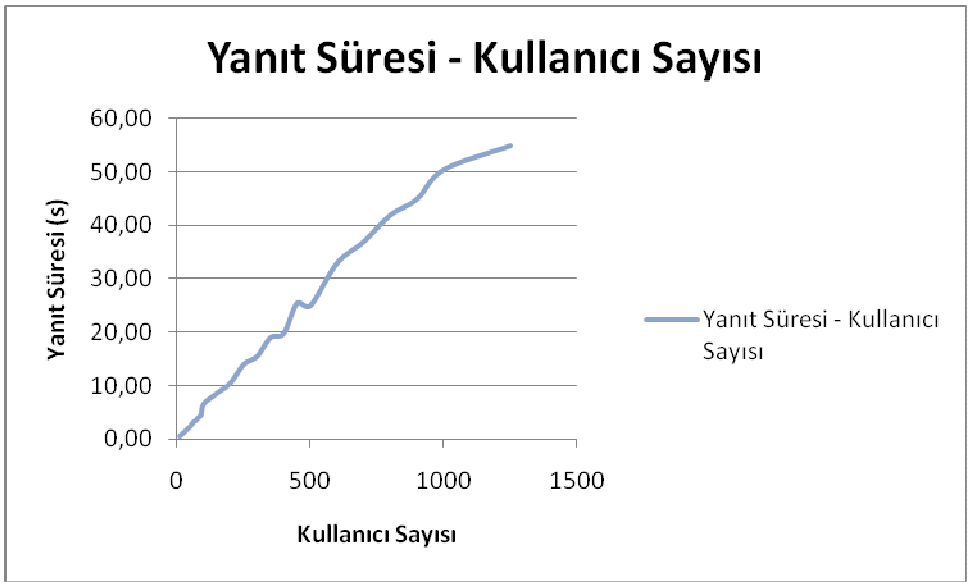
6.3.2 Performans Değerlendirmeleri

Testler sistemin iki farklı kullanıcı seçeneği olan kriptosuz ve kriptolu seçenekleri için ayrı ayrı gerçekleştirilmiştir.

6.3.2.1 Kriptosuz Seçeneğinin Performans Değerlendirmeleri

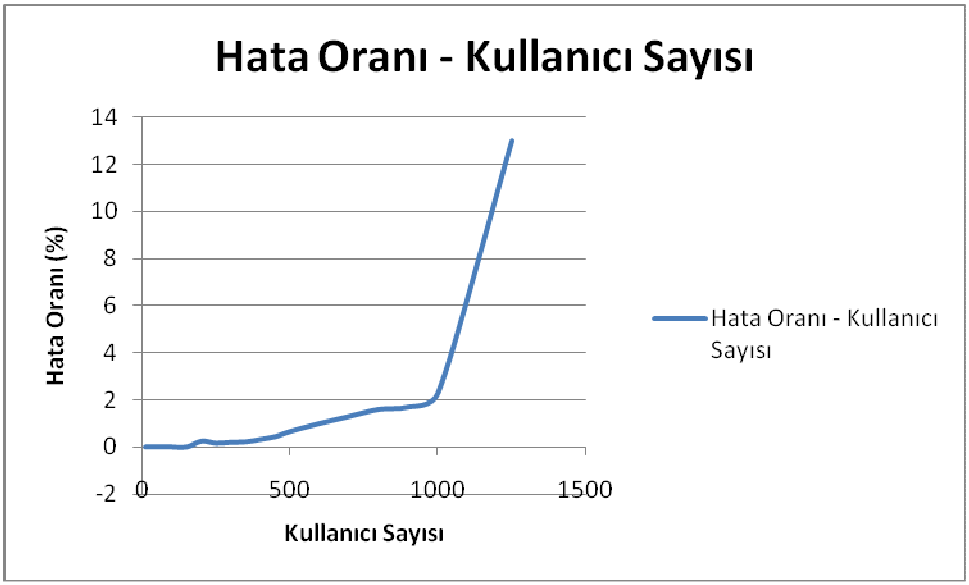
Bu testin gerçekleştirilmesi için sisteme eşzamanlı kullanıcıların herbiri tarafından kriptolanmamış veri gönderilmektedir. Testler kademeli olarak 10 kullanıcıdan başlayarak 1250 kullanıcıya kadar gerçekleştirilmiştir.

Çizelge 6.10'da da gözlenebildiği gibi eşzamanlı kullanıcı sayısı arttırıldığında sunucudan gelen yanıt süresi de artmaktadır. Buradan sunucunun kullanıcılardan yapılan tüm isteklere karşılık verebildiği ama eşzamanlı istek sayısı arttıkça yanıt süresinin de arttığı gözlemlenmektedir.



Çizelge 6.10 Kriptosuz Seçeneğinde Yanıt Süresi – Kullanıcı Sayısı Grafiği.

Çizelge 6.11'de sunucuya yapılan isteklerinden dönen hata oranı verilmektedir. Eğer sunucuya veri ulaştırılmışsa sunucudan başarılı olduğunu gösteren kod dönemktedir, bu da başarılı bir bağlantı gerçekleştirildiğini göstermektedir. Ama sunucudan bağlantı kurulamadığına dair hata kodu döndürüldüğünde bağlantı kurulamadığı anlamına gelmektedir. Az sayıda eşzamanlı kullanıcının sunucuyla bağlantı kurduğu durumda hata oranı %0 civarındadır. Eşzamanlı bağlantı sayısı arttıkça bir kısım kullanıcının sunucuyla bağlantı kuramadığı ve veri gönderimini gerçekleştiremediği gözlemlenmektedir.



Çizelge 6.11 Kriptosuz Seçeneğinde Hata Oranı – Kullanıcı Sayısı Grafiği.

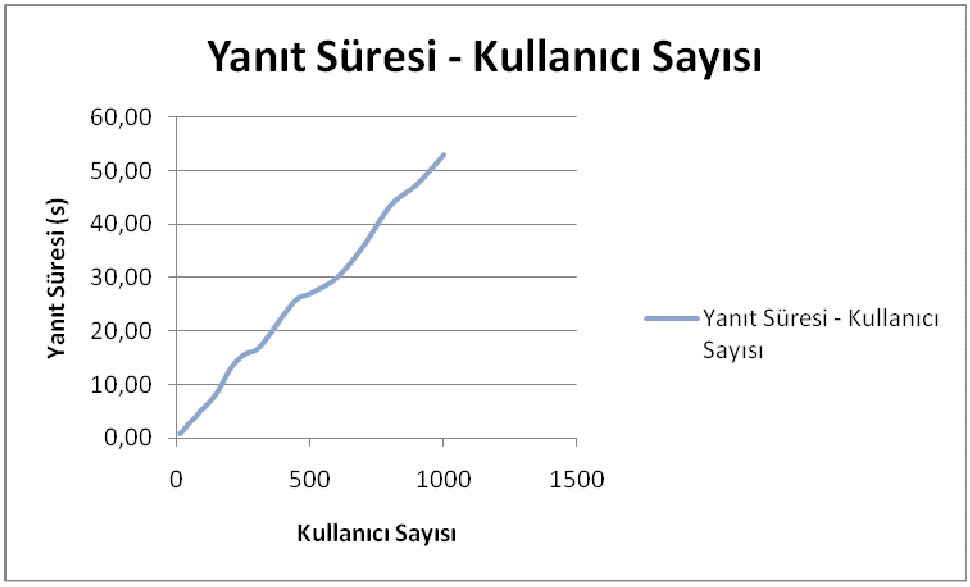
Hata oranını azaltmak için web sunucusunun özelliklerinin arttırılması gerekmektedir. Mesela Google anasayfasına eşzamanlı onbinlerce kullanıcı bağlanmaktadır, ama her kullanıcının başarıyla bağlanması sağlanmaktadır. Google'un bu bağlantı miktarını kaldıracak altyapısı ve sunucu özellikleri bulunmaktadır. Bu tez kapsamında kullanılan web sunucusu ortak bir sunucudur. Sunucular üzerinde Dual Xeon E5620 2.40 GHz Quad Core işlemciler çalışmaktadır. 100 mbps hıza kadar bağlantı hızını desteklemektedir[1]. Aynı şekilde bu sistemin web sunucusunun özellikleri arttırılarak hata oranının düşürülmesi mümkündür.

Bu grafiklerden anlaşılan bir diğer durum ise sistemin bu haliyle binlerce kullanıcının kullanımına cevap verebilecek olmasıdır. 500 eşzamanlı kullanıcıya kadar hata oranı çok düşüktür. 500 eşzamanlı kullanıcının aynı anda bağlanıyor olması ise şehir içi kurye sistemleri ya da bu sistemi kullanmayı düşünebilecek şirketler için karşılaşılması zor bir durumdur.

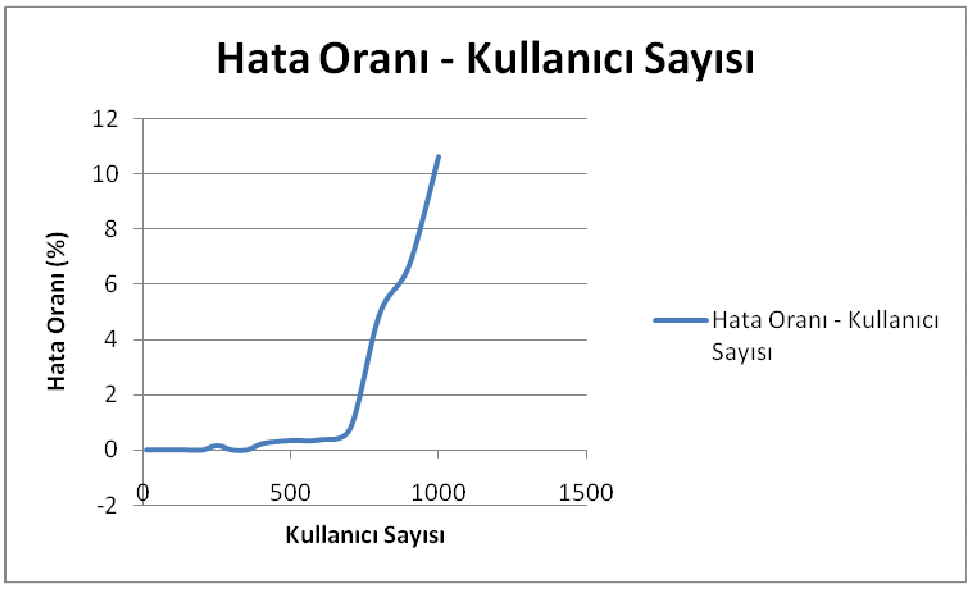
6.3.2.2 Kriptolu Seçeneğinin Performans Değerlendirmeleri

Kriptolu seçeneğinde de kriptosuz seçeneğindekine benzer senaryolar uygulanmıştır. Çizelge 6.12'de yanıt süresi – kullanıcı sayısı grafiği ve Çizelge 6.13'de hata oranı – kullanıcı sayısı grafiği verilmiştir.

[1] Server Specifications, http://support.hostgator.com/articles/hosting-plans/server-specifications-specs.



Çizelge 6.12 Kriptolu Seçeneğinde Yanıt Süresi – Kullanıcı Sayısı Grafiği.



Çizelge 6.13 Kriptolu Seçeneğinde Hata Oranı – Kullanıcı Sayısı Grafiği.

Bu grafiklerden kriptolu seçeneğinde yanıt süresinin kriptosuz seçeneğine göre arttığı gözlemlenmektedir. Bunun da beklenen bir sonuç olduğu değerlendirilmektedir. Yanıt süresinin artmasına kodda yer alan şifre çözmek için konulmuş kısmın neden olduğu düşünülmektedir.

Hata oranı ise hemen hemen kriptosuz seçeneği ile aynıdır. Sunucudan hata dönülmesinde yani sunucu ile bağlantıya geçilememesinde, web sunucusuna ve web sunucusu sağlayıcısına o an için ne kadar yükleme olduğu etkili olmaktadır.

Aynı zamanda web sunucusunun gücü ve özellikleri de hata oranını etkileyen etmenlerdir.

7. SONUÇLAR VE DEĞERLENDİRMELER

Bu tez çalışmasında GPS donanımlı cep telefonlarında çalışabilen bir kullanıcı programı geliştirilerek cep telefonlarının takip edilebilmesi gerçekleştirilmiştir. Cep telefonlarından alınan GPS verisi kullanıcının isteğine göre kriptolu ya da kriptosuz olarak bir sunucuya gönderilmekte ve kontrolü yapılarak sunucudaki veritabanına işlenmektedir. Verileri kullanıcıların görebilmesi ve diğer kullanıcılara ait koordinat verilerini harita üzerinde izleyebilmelerinin sağlanabilmesi için Google Maps'in kullanıldığı bir web arayüzü geliştirilmiştir. Web arayüzü ile kullanıcıların kendi koordinatlarını kimlerin görmelerine izin verebilecekleri bir yapı oluşturulmaya çalışılmıştır.

Web arayüzünde sunulan önemli bir uygulama da coğrafi çerçeveleme uygulamasıdır. Bu uygulama ile kullanıcılar, diğer kullanıcılar için çıkmamalarını istedikleri bir çerçeve belirlemekte ve takipteki kullanıcı çerçeve dışına çıktığında e-posta ile kullanıcının çıktığına dair bilgilendirme almaktadırlar. Böyle bir uygulamanın bu tip sistemler için önemli olabileceği değerlendirilmiştir. E-posta uyarısının sıradan olduğu günümüzde, kullanıcıların devamlı web arayüzüne bağlanıp kontrol etmesine gerek kalmadan herhangi bir uyarı gerektiren durumda, kullanıcılar e-posta ile bilgilendirilebileceklerdir.

Cep telefonunda GPRS gibi bir bağlantı kullanılabildiği gibi kullanıcıların seçeneğine göre 3G'nin de kullanılabilmesi mümkündür. GPRS kullanılarak yapılan testler sonucunda kriptosuz veri gönderim sırasında her göndermede ortalama 0.9 KB civarında bir veri gönderilmektedir. Kriptolu veri gönderiminde ise veri büyüklüğü ortalama 1 KB'nin üzerine çıkmaktadır. Çizelge 7.1 ve Çizelge 7.2'de kriptosuz ve kriptolu veri gönderim seçeneklerine göre tek bir deneme için kullanılan byte miktarları gösterilmektedir.

Veri Niteliği	Veri Adeti	Byte Miktarı
Kriptosuz	1	2115
Kriptosuz	2	2979
Kriptosuz	3	4051
Kriptosuz	4	5077
Kriptosuz	5	5883

Çizelge 7.1 GPRS ile Kriptosuz Veri Gönderiminde Veri Büyüklükleri.

Veri Niteliği	Veri Adeti	Byte Miktarı
Kriptolu	1	2550
Kriptolu	2	4079
Kriptolu	3	5437
Kriptolu	4	6267
Kriptolu	5	7381

Çizelge 7.2 GPRS ile Kriptolu Veri Gönderiminde Veri Büyüklükleri.

Elde edilen bu tablolardan çıkarılan sonuç kriptosuz veri gönderme seçeneğinde kullanılan veri büyüklüğünün daha az miktarda olacağı yönündedir. Bundan dolayı da maliyetinin de daha az olması beklenmektedir.

Harita uygulamalarının oluşturulabilmesi için Google Maps'in seçilmiş olmasının sebebi yaygınlığı ve güncelliğidir. Sunulan servislerin ücret karşılığında olmaması da ayrı bir önem arz etmektedir. Google Maps'in önemli bir özelliği ise API ve kütüphanelerinin kullanışlı oluşudur. Bir web arayüzü tasarlanarak kullanıcılara harita üzerinde görsellik sunulmaya çalışıldığı için Google Maps'in kullanımı web arayüzü açısından önemli olmuştur. Google Maps'in kullanımı, web arayüzüne hem görsellik kazandırmış hem de Google Maps'in rakiplerine göre sahip olduğu güçlü alt yapısıyla coğrafi çerçeveleme gibi uygulamaların web arayüzünde uygulanabilmesine olanak sağlamıştır.

Cep telefonu programının geliştirilmesinde Java ME dili kullanılmıştır. Bu dilin avantajı birçok telefonda desteklenmesi ve çalışabilmesidir. Programın geliştirilmesi Nokia marka bir telefonda gerçekleştirildiği için Nokia'ya özel

Symbian C++ programlama dili ile başlanmış ama sonrasında aynı marka başka bir telefon modelinde bile programın çalışmayacağı düşünülerek Java ME dilinde geliştirme gerçekleştirilmiştir.

Cep telefonunda programın çalışması için cep telefonunun sahip olması gereken Java özellikleri ilgili bölümlerde bahsedilmiştir. Özetle Java programlarını çalıştırabilen ve başta JSR-179 ve JSR-177 gibi özelliklere sahip bir cep telefonu olması gerekmektedir. Cep telefonunun sahip olması gereken en önemli özellik ise GPS'dir. Tez kapsamında incelenen GPS özelliğine sahip olduğu belirtilen bazı cep telefonlarının koordinat verisini veremedikleri gözlemlenmiştir. Bu tip telefonlar internet bağlantısı yardımıyla bulundukları yeri bir harita üzerinde işaretleyip ekranda göstermekte ama koordinatları ekranda gösterememektedirler. Bu cep telefonlarında programın istenilen şekilde çalışması gözlemlenememiştir. Zaten bu telefonlarda koordinat sorgulaması da yapılamamaktadır. Denenen cep telefonlarıyla ilgili elde edilen sonuçlar Çizelge 7.3'de verilmektedir.

Denenen Cep Telefonu	**Başarı Durumu**	**Açıklama**
Nokia 5800	Başarılı	Cep telefonu programı geliştirilmesi bu marka ve model telefon üzerinde gerçekleştirilmiştir.
HTC Wildfire	Başarısız	Cep telefonunda konum sorgulama bulunmamaktadır. Sadece harita üzerinde internet yardımıyla yer gösteren bir uygulama yer almaktadır. GPS özelliğinin aktif edilmesi başarılamamıştır. Ayrıca telefonun Java çalıştırma özelliği olmadığı için Android tarafından okunabilecek bir formata çevrilmiş ama yine de başarı sağlanamamıştır.
Nokia N8	Başarılı	Sorunsuz çalışmıştır.
Samsung S8300	Başarılı	Sorunsuz çalışmıştır.
Samsung Wave II	Başarılı	Sorunsuz çalışmıştır.

Çizelge 7.3 Cep Telefonu Denemeleri.

Telefon denemeleri sırasında bazı cep telefonu modellerinde giderilemeyen hataların olduğu gözlenmiştir. Mesela Nokia 6110 Navigator cep telefonu modelinde GPS yongası bir süre kullanıldıktan sonra kilitlenmektedir[1]. Ayrıca bazı S60 5th Ed. Nokia cep telefonlarında 100 civarında GPS sorgulaması yapıldıktan sonra veri gelmemektedir[2]. Bu problemlerden bazılarının çözümleri üretici firmalar tarafından bulunmuş iken bazılarınınki henüz bulunamamıştır. Bundan dolayı uzaktan güvenli takip sistemi uygulamasının kullanılacağı cep telefonlarında bu tip durumlara dikkat edilmesi gerekmektedir. Cep telefonu kullanıcılarının alabileceği bir diğer önlem de cep telefonlarının güncellemelerini yapmaktır.

Denemelerde ulaşılan bir diğer değerlendirme de cep telefonlarından yapılan GPS sorgulamalarındaki veri kilitlenmesidir. Eğer JSR-179 API'deki GPS verisi dinlemede varsayılan değerler kullanıldığında fonksiyon bir süre sonra çok sıklıkla gelen GPS verilerini idare edememektedir. Böyle bir durumda GPS simgesi ekranda görünmeye devam etmekte, program çalışmakta ama GPS verileri alınamamaktadır. Bundan dolayı geliştirilen yazılımda da varsayılan sorgulamaya izin verilmemiştir.

Denemeler sırasında GPS verisinin ilk alınması gerçekleştirildikten sonra A-GPS'nin kullanılmasına bağlı olarak cep telefonunda GPS sorgulamasının bina içerisine bir miktar daha girebildiği gözlemlenmiştir. Bir diğer gözlem ise dışarıda açık bulutsuz havada yapılan uygulamalarda bile bazen GPS verisinin bir süre alınamadığı ve sonra tekrar alınmaya başlandığıdır. Mesela her saniye yapılan bir sorgulamada 10-15 saniye veri alınamadığı ve sonra tekrar alındığı gözlemlenmiştir. Bunun nedeninin, açık havada bina dışında yapılan bir deney olmasına rağmen, ağaç ve bina yansımaları gibi çevresel etmenlerden kaynaklandığı değerlendirilmektedir. A-GPS'ten bahsedilirken de değinildiği gibi bu tip etmenler GPS sorgulamasını zaman zaman etkileyebilmektedir.

Cep telefonu yazılımıyla yapılan bir diğer deneme de batarya harcamasına yönelik olmuştur. Bu denemeler sonucunda takip sistemi uygulamasının kullanılmasının bataryada ciddi harcamalara neden olduğu gözlemlenmektedir. Bunun nedeni cep

[1] KIJ000996 – Calling getLocation() periodically may result in device lock-ups with Nokia 6110 Navigator, http://www.developer.nokia.com/Community/Wiki/ KIJ000996_-_Calling_getLocation()_ periodically_may_result_in_device_lock-ups_with_Nokia_6110_Navigator.
[2] KIJ001579 – Location MIDlet closed after 110th orientation call in S60 5th Edition, http://www.developer.nokia.com/Community/Wiki/ KIJ001579_-_Location_MIDlet_closed_after_ 110th _orientation_call_in _S60_5th_Edition.

telefonunun sürekli GPS bağlantısı sağlamak zorunda olmasıdır. Batarya süresini üçte bir ila yarı yarıya azalttığı gözlemlenmektedir. Bu sürenin her cep telefonunda farklı olacağı değerlendirilmektedir. Ama batarya süresine GPS kullanımının etkisinin cep telefonu ile konuşmanın etkisinden daha az olduğu gözlemlenmektedir.

Sistemin kullanımının kullanıcılarla performansının ölçülebilmesi için yükleme testleri gerçekleştirilmiştir. Oluşturulan sanal kullanıcılar ile gerçekleştirilen testler sonucunda sistemin 500 eşzamanlı kullanıcıya kadar sorunsuz çalışacağı değerlendirilmektedir.

KAYNAKLAR

[1] Xu Kaihua, Wang Ya, Teng Wei, Liu Yuhua, 2006, Design and Implementation of Intelligent Vehicle Monitoring and Management System Based on the Multi-Net, IEEE Asia-Pacific Conference on Services Computing, 650-653.

[2] Wu Qingfeng, Yang Xianyan, Liu Han, Dong Huailin, 2008, Mobile Guardian: A Novel Positioning and Monitoring System for Outdoor Special Users Based on GPS, IEEE International Symposium on IT in Medicine and Education, 596-600.

[3] Chadil Noppadol, Russameesawang Apirak, Keeratiwintakorn Phongsak, 2008, Real-Time Tracking Management System Using GPS, GPRS, Google Earth, ECTI-CON, 393-396.

[4] Trullols E. et al., 2009, Real-Time Fleet Ship Monitoring System Using Satellite Broadband Communications and Google Earth, First Internatioanl Conference on Advances in Satellite and Space Communications, 146-155.

[5] Zheng Yu, Wang Longhao, Zhang Ruchi, Xie Xing, Ma Wei-Ying, 2008, GeoLife: Managing and Understanding Your Past Life over Maps, The Ninth International Conference on Mobile Data Management, 211-212.

[6] Zahaby Mohammad, Gaonjur Pravesh, Farajian Sahar, 2009, Location Tracking on GPS using Kalman Filter Through SMS, EUROCON, 1707-1711.

[7] Cao Huasong, Hui Ronald, Leung Victor C.M., 2010, Cell Link: Real-Time Data Tracking of Automobiles via Cell Phones, ICCE, 305-306.

[8] Barbeau S.J., Winters P.L., Georggi N.L., Labrador M.A., Perez R., 2010, Travel Assistance Device: Utilising Global Positioning System-Enabled Mobile Phones to Aid Transit Riders with Special Needs, Intelligent Transport Systems, vol.4, no.1, 12-23.

[9] Dorsey A.J. et al., 2006, GPS System Segments, http://acc.igs.org/understanding-GPS_Ch03.pdf.

[10] Usha Communications Technology, 2000, GPRS General Packet Radio Service White Paper by Usha Communications Technology, http://www.mobilein.com/GPRS.pdf.

[11] Paar Christof, Pelzl Jan, 2010, Understanding Cryptography: A Textbook for Students and Practitioners, Springer.

[12] Svennerberg Gabriel, 2010, Beginning Google Maps API 3, Apress.

[13] Loytana Kimmo, Nokia, 2006, JSR 179 Location API for J2ME, http://www.jcp.org/en/jsr/detail?id=179 .

[14] Ahmad Saqib, Zelov Roman, 2007, JSR 177 Security and Trust Services, API for J2ME. http://jcp.org/en/jsr/detail?id=177 .

[15] Riggs Roger, 2002, JSR 68 J2ME Platform Specification, http://www.jcp.org/en/jsr/detail?id=68.

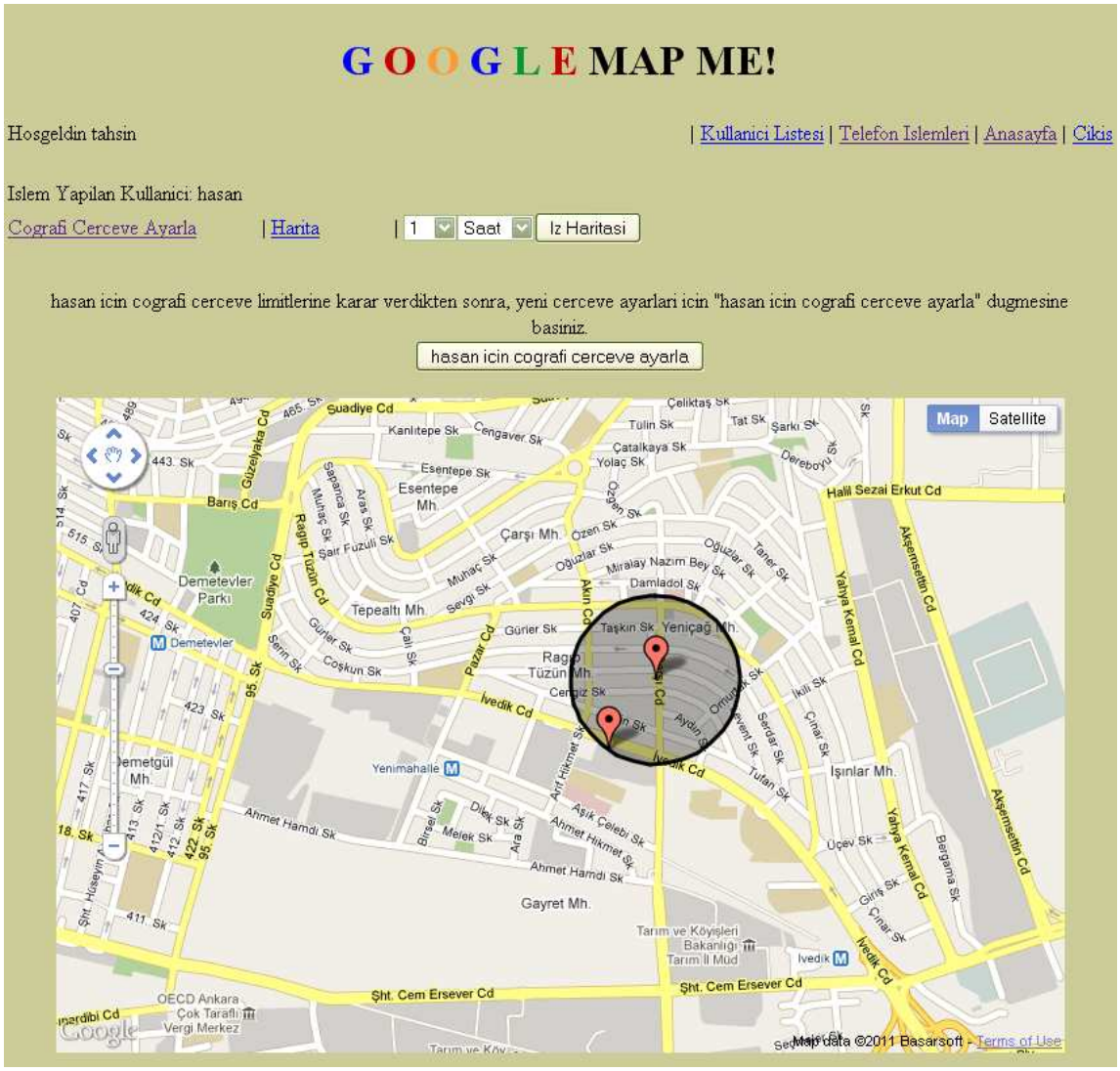
[16] Menasce D.A., 2002, Load Testing of Web Sites, Internet Computing, vol.6, no.4, 70-74.

EKLER DİZİNİ

EK A. TEK KULLANICI TAKİBİ DEMOLARI

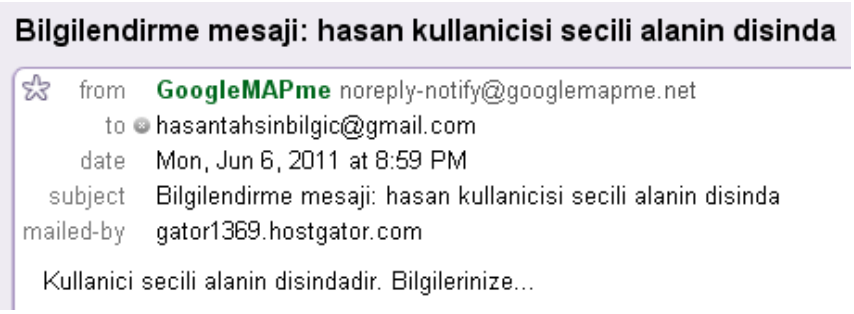
A.1 Tek Kullanıcı Takibi Kullanım Demosu-1

Bu testte tek bir kullanıcının başka bir kullanıcı tarafından takip edilmesi demolandırılmıştır. Takip edilen “hasan” isimli kullanıcı için “tahsin” isimli kullanıcı tarafından Şekil A.1‘deki gibi bir çerçeve belirlenmektedir.



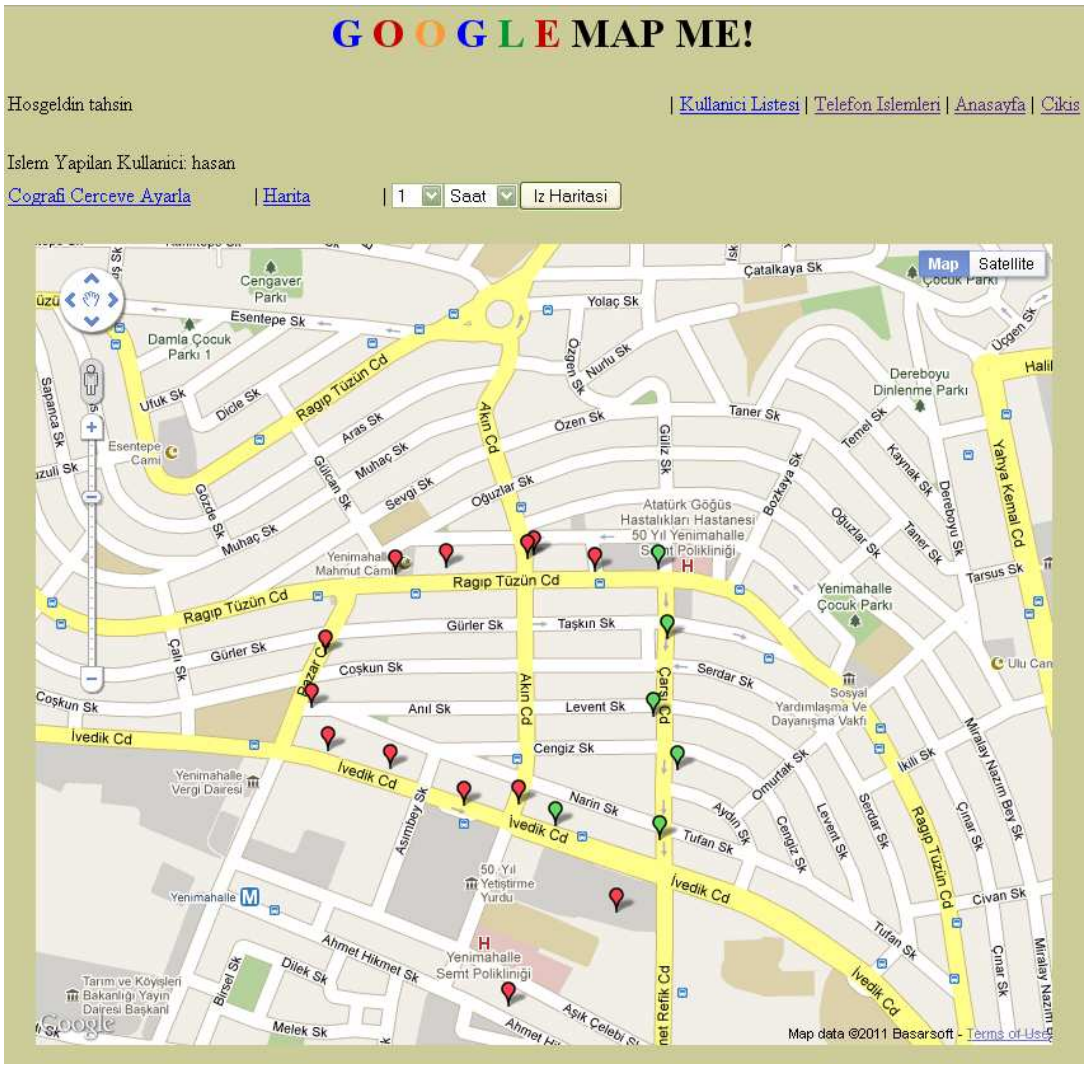
Şekil A.1 Takipteki Kullanıcı için Coğrafi Çerçeve Belirlenmesi.

“hasan” isimli kullanıcı yürümeye bu çerçevenin içinden başlamaktadır. Bu kullanıcı çerçevenin dışına çıktığı andan itibaren “tahsin” isimli kullanıcının e-posta adresine Şekil A.2‘de gösterilmiş olan e-posta gelmektedir. “hasan” isimli kullanıcı çerçevenin içine tekrar girdiğinde e-posta gönderilmesi kesilmiştir.



Şekil A.2 Gönderilen Uyarı E-postası.

"hasan" isimli kullanıcının bu test sırasındaki güzergahının Google Maps üzerinde gösterilmesi Şekil A.3'de verilmektedir. Burada gözlenebileceği gibi "hasan" isimli kullanıcının gönderdiği koordinat noktalarından çerçeve içinde kalanlar harita üzerinde yeşil işaret ile gösterilmiştir. Çerçeve dışında kalan noktalar ise kırmızı işaret ile işaretlenmektedir.

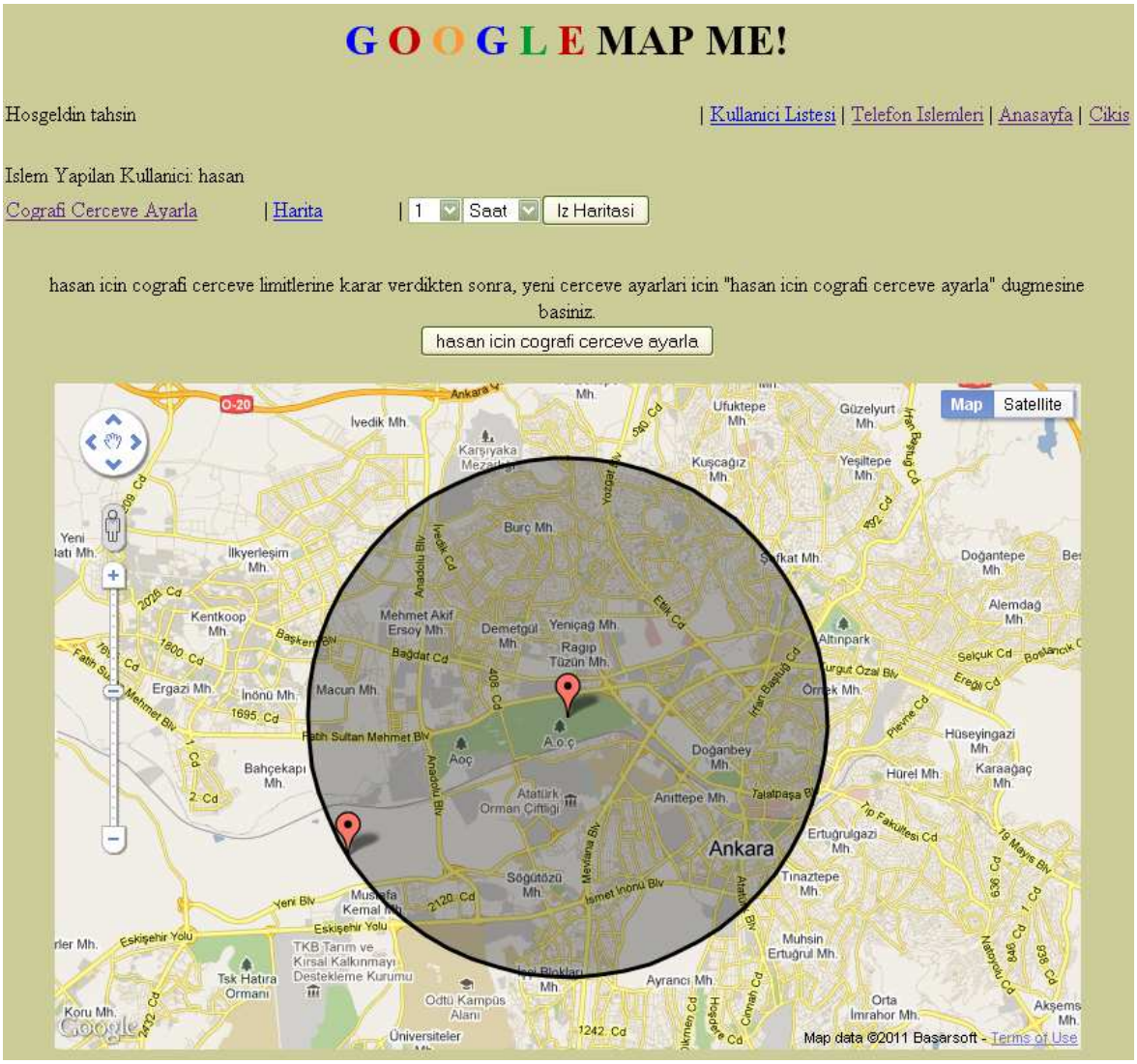


Şekil A.3 Takip Edilen Kullanıcının İz Haritası

A.2 Tek Kullanıcı Takibi Kullanım Demosu-2

Bu testte tek kullanıcının takibi üç ayrı kullanıcı tarafından yapılmaktadır. İlk iki kullanıcı, takip edilen kullanıcı için coğrafi çerçeveleme uygulamasını kullanarak Şekil A.4 ve Şekil A.5'deki gibi farklı çerçeveler belirlemiş iken; son kullanıcı, takip edilen kullanıcı için herhangi bir çerçeve belirlememiştir.

Şekil A.4 "tahsin"in Coğrafi Çerçeve Belirlemesi.



Şekil A.5 "kullanici1"in Coğrafi Çerçeve Belirlemesi.

İlk iki kullanıcıya takip edilen kullanıcı çerçeve dışına çıktığında bilgilendirme için e-posta gelmektedir. Son kullanıcı herhangi bir çerçeve belirlemediği için e-posta da almamaktadır.

Takip edilen kullanıcının coğrafi çerçeveleme uygulamasının da etkisiyle farklı kullanıcılar için oluşturulmuş haritaları Şekil A.6, Şekil A.7 ve Şekil A.8'de verilmektedir.

Şekil A.6 “tahsin” için Oluşturulan Harita.

Şekil A.7 “kullanici1” için Oluşturulan Harita.

Şekil A.8 "kullanici2" için Oluşturulan Harita.

Burada da gözlenebildiği gibi takip edilen kullanıcı için belirlenmiş farklı çerçeveler harita üzerinde de farklı renklendirme sonuçları vermiştir. Takip edilen kullanıcı için herhangi bir çerçeve belirlenmediği durumda ise harita üzerinde koordinat noktaları mavi işaret ile işaretlenmektedir.

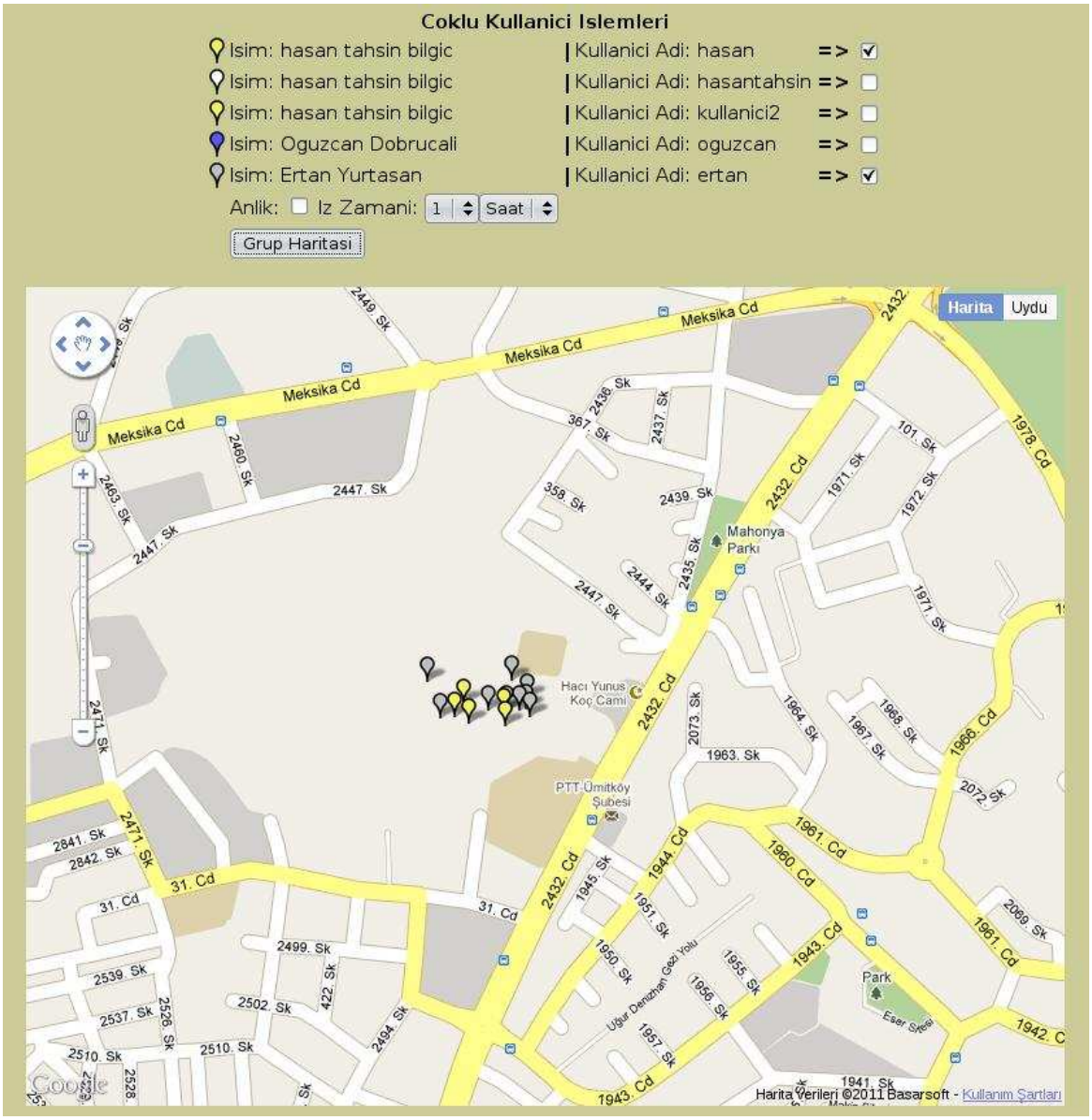
EK B. ÇOKLU KULLANICI TAKİP DEMOLARI

B.1 Çoklu Kullanıcı Testi

Bu testte birden fazla kullanıcı kullanılmıştır. Bu test ile sistemin beklendiği gibi birden fazla kullanıcı ile çalışabildiği gösterilmiştir. Bu testte “ertan” ve “hasan” isminde iki kullanıcı bulunmaktadır. “ertan” isimli kullanıcı IMEI numarasını vermek istemediği için “kriptosuz” olarak bağlantı sağlamıştır. Aynı kullanıcının cep telefonunda A-GPS özelliği de kapalıdır. Bundan dolayı “ertan” isimli kullanıcının cep telefonunun bina içerisinde pencere kenarında GPS verisini alması için bir süre beklenmiştir. Değinildiği gibi A-GPS cep telefonlarında ilk konum verisinin hızlı alınmasını sağlamaktadır. “ertan” isimli kullanıcının cep telefonu da GPS uydularını gördükten sonra iki kullanıcı aynı zamanlarda programı çalıştırmışlardır. “hasan” isimli kullanıcı ise A-GPS kullanmıştır. Aynı kullanıcı, GPS verilerini ise “kriptolu” seçeneği ile göndermiştir.

Bu test, birden fazla kullanıcının aynı anda çalışmasını göstermesi bakımından faydalı olmuştur. Aynı zamanda kullanıcılardan birisi A-GPS’yi hiç kullanmamıştır. GPS uydularını görüp ilk veriyi alabildikten sonra cep telefonunun A-GPS özelliğinin açık ya da kapalı olmasının iki kullanıcının gönderdikleri veri miktarları ve doğruluklarında herhangi bir farklılık oluşturmadığı gözlemlenmiştir.

Şekil B.1‘de bu test sonunda oluşmuş harita görüntüsü gösterilmektedir. Burada “hasan” ve “ertan” kullanıcılarına ait son 1 saat içindeki iz haritası Google Maps üzerinde gösterilmiştir.



Şekil B.1 İki Kullanıcı ile Test Gerçekleştirilmesi.

EK C. HTML, Javascript, PHP ve MySQL

Web arayüzü yapımında HTML, Javascript, PHP ve MySQL kullanılmaktadır.

HTML, web sitelerinin genel formatını, şablonunu belirleyen dildir. Hiper metin biçimleme dilidir. HTML dilinde belli bir yazım formatı belirlenmiştir. Metinler, resimler, videolar HTML tag'leri arasında gösterilmektedir. Tag'ler "<" ve ">" arasında gösterilmektedir. HTML ile oluşturulan sayfanın başlangıç ve bitişinde <html> ve </html> bulunmaktadır. HTML doküman paylaşım yöntemi olarak CERN'de görev yapan fizikçi Tim-Berners Lee tarafından öne sürülmüştür[36]. HTML'nin ilk uygulamasını 80'li yılların sonunda ortaya koyulmuştur. 90'lı yıllarda ise yeni sürümleriyle şekillenmiştir. HTML sayfalarının ifade ettiklerini anlayabilmek için bunları işleyebilen Mozilla Firefox gibi internet tarayıcıları kullanılmaktadır.

Javascript, kısıtlamaları bulunmayan fonksiyonların yazılabildiği dinamik bir script dilidir. Brendan Eich tarafından tasarlanmıştır. Netscape tarayıcısı altında Mocha ve daha sonra LiveScript adını almıştır. Daha sonra Sun Microsystems ile yapılan bir duyuruyla JavaScript adını almıştır[37]. Java'dan türetilmiş bir dil olmamasına rağmen o dönemde popüler bir dil olan Java'nın ününden yararlanılmak istendiği akla gelmektedir. JavaScript kullanıcı tarafında çalışan bir dildir. HTML sayfalarına dinamiklik katmak amacıyla kullanılmaktadır. Mesela, bir kullanıcıya adının ne olduğu bir açılır pencere ile sorulup, verdiği cevaba göre web sayfasında isminin yer aldığı bir karşılama mesajı yazdırılabilmektedir.

PHP web sayfasında dinamizmin temel taşını oluşturmaktadır. Web arayüzündeki kullanıcıların birbirleriyle haberleşmeleri, sunucudan alınan sonuçları görebilmeleri PHP ile mümkün olmaktadır. PHP, 1995'te Rasmus Lerdorf tarafından tasarlanmıştır[38]. Şu anda çalışmalar PHP Grubu tarafından devam ettirilmektedir. PHP ilk kurulduğunda kısaltmanın anlamı Kişisel Ana Sayfa iken zamanla PHP'nin de yapısını daha iyi yansıtan PHP: Hipermetin Önişlemcisi uzatmasını almıştır. PHP'ye ait kodlar HTML sayfası içerisine yazılabilmektedir. İçerisinde PHP kodları bulunan sayfalar .php uzantısını almaktadır. PHP kodlarının bulunduğu kısımlar başına "<?php" ve sonuna "?>" koyularak HTML tag'lerinden ayrılmaktadır. PHP kodları HTML gibi sayfaya bağlanıldığında statik olarak görünmemektedir. İnternet

[36] History of HTML, Tim Berners-Lee, http://inventors.about.com/od/computersoftware/a/html.htm.
[37] Brendan Eich and Javascript, http://inventors.about.com/od/jstartinventions/a/JavaScript.htm.
[38] Rasmus Lerdorf, http://lerdorf.com/bio.php.

tarayıcısı tarafından işlenmekte ve sayfada görünebilecek hali almaktadırlar. Mesela bir kullanıcı sayfaya kullanıcı adı ve şifresiyle girdiğinde kullanıcının adı PHP ile oturum ya da tanımlama bilgisi oluşturularak tutulmakta ve sayfada PHP "echo" ya da "print" kodları ile yazdırılabilmektedir.

MySQL, Michael Widenius tarafından tasarlanmıştır. İsmini Widenius'un kızı My'den almıştır[39]. SQL ise yapılı sorgulama dili anlamındadır. Veritabanlarına erişimi sağlayan kodlar web sitelerinde bu dille yazılmaktadır. PHP kodlarının içine MySQL kodları yazılarak sunucu üzerindeki veritabanlarıyla irtibat kurulup sonuçları PHP ile web sayfalarında gösterilmektedir.

[39] MySQL Reference Manual, History of MySQL, http://dev.mysql.com/doc/refman/4.1/en/history.html.

ÖZGEÇMİŞ

Adı Soyadı :		Hasan Tahsin BİLGİÇ
Doğum Yeri :		Adana
Doğum Yılı :		1984
Medeni Hali :		Bekar

Eğitim ve Akademik Durumu:

Lise	1999 – 2002	: Özgören Lisesi, ADANA
Lisans	2003 - 2007	: Güney Kaliforniya Üniversitesi, Elektrik ve Elektronik Mühendisliği Bölümü, LOS ANGELES, ABD
Yabancı Dil:		İngilizce (İleri Derece)

İş Tecrübesi:

2007 -...	TÜBİTAK/UEKAE/İLTAREN, Araştırmacı