T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

GPRS İLE UZAKTAN SAYAÇ OKUMA UYGULAMASI

YÜKSEK LİSANS TEZİ

Bilgisayar Müh. Mehmet GÖÇER

Enstitü Anabilim Dalı	:	BİLGİSAYAR VE BİLİŞİM MÜH.
Tez Danışmanı	:	Yrd. Doç. Dr. Hayrettin EVİRGEN

Haziran 2005

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

GPRS İLE UZAKTAN SAYAÇ OKUMA UYGULAMASI

YÜKSEK LİSANS TEZİ

Bilgisayar Müh. Mehmet GÖÇER

Enstitü Anabilim Dalı : BİLGİSAYAR VE BİLİŞİM MÜH.

Bu tez 22/06/2005 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.

Yrd.Doç.Dr.Hayrettin EVİRGEN	Prof.Dr.Hüseyin EKİZ	Yrd.Doç.Dr. İbrahim Özçelik
Jüri Başkanı	**Üye**	**Üye**

TEŞEKKÜR

Yüksek lisans tezimin hazırlık aşamasında bana en büyük desteği ve yardımı sağlayan danışman hocam Yrd. Doç. Dr. Hayrettin EVİRGEN'e en içten teşekkürlerimi sunarım.

Bu çalışmada, çalışmam süresince beni teşvik eden, destekleyen, maddi manevi her türlü yardımı sağlayan eşim Gülsüm GÖÇER'e teşekkür ederim.

Tüm eğitim hayatım boyunca beni teşvik eden, destekleyen, maddi ve manevi her türlü yardımı sağlayan aileme teşekkür ederim.

Bu seviyeye gelmemde benden maddi manevi yardımlarını esirgemeyen tüm arkadaşlarıma teşekkür ederim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

GPRS : General packet radio service / paket anahtarlamalı radyo hizmetleri

USO : Uzaktan sayaç okuma

AMR : Automatic meter reading

RF : Radio frequency / radyo frekansı

PLC : Power line communication / güç hattından haberleşme

UART : Universal asynchronous receiver transmistter / genel asenkron alıcı gönderici

API : Application programming interface / uygulama programı arabirimi

FSK : Frequency shift key / frekans kaydırmalı anahtar

ASK : Amplitute shift key / genlik kaydırmalı anahtar

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar Kelimeler: GPRS, USO, DES, Sunucu, İstemci

Sürekli gelişen teknolojiyle birlikte evde ve işyerlerinde farklı amaçlar için kullanılan sayaçlar da gelişmiştir. Artık mekanik sayaçların yerini hızla elektronik sayaçlar almaktadır. Sayaçların dijital dünyaya girmeleriyle birlikte fonksiyonları artmış ve bu fonksiyonların arasına haberleşme özelliği de eklenmiştir. Bu gelişme bu araçların kullanıcılarına bir çok avantaj sağlamaktadır.

Dünya, her elektronik aygıtın birbirleriyle haberleştiği bir otomasyon sistemine doğru gitmektedir. Bunların başında ev otomasyonları gelmektedir. Ev otomasyonu uygulamalarına sayaçlar da dahil edilebilir. Sayaçların böyle bir sisteme dahil edilebilmesini sağlayacak sistemler USO sistemleridir. USO sistemleri bu otomasyonun başlangıç seviyesidir. Bu sistemler sayesinde belki ilerde, kredisi biten sayaç otomatik olarak kullanıcının banka hesabı aracılığı ile kredi satın alabilecektir.

Bu tez çalışmasında USO uygulamalarının gelişmekte olan bir çeşidi olan "GPRS üzerinden USO" sistemiyle bir uygulama yapılmıştır. Aynı zamanda diğer USO sistemleri hakkında da bilgi verilmiştir.

AUTOMATIC METER READING OVER GPRS

SUMMARY

Keywords: GPRS, AMR, DES, Server, Client

The meters which are used at home and workplaces and used for different purposes are improved with the growing technology. Nowadays, electronic meters are taking place of mechanical meters. After meters entered the digital world, the numbers of their functions has increased and communication property has been added to these functions. This improvement provides lots of advantages for the users of these tools.

The world is going to an automation system that every electronic device communicates with each other. Home automations have the most importance. Meters can be considered as a part of home automation applications. Meters become a part of home automations with AMR systems. AMR systems are the beginning level of this automation. Maybe in the future, meters which are equipped with these systems will be able to buy credit via user's bank account when they are out of credits.

In this study, AMR

In this study, AMR systems are studied and an application using "AMR over GPRS", which is a kind of AMR systems, has been developed.

BÖLÜM 1. GİRİŞ

Bu tez çalışmasında, USO (Uzaktan sayaç okuma) sistemleri incelenmiş ve yaygın olarak kullanılan USO çeşitleri anlatılmıştır. Ayrıca bir USO çeşidi olan "GPRS ile USO sistemi" uygulaması gerçekleştirilmiştir.

Bu çalışma altı ana bölümden oluşmaktadır.

Birinci bölüm giriş bölümü olup bu çalışmada incelene konular ve geliştirilen uygulamalar hakkında genel bir bilgi verir.

İkinci bölüm USO hakkında detaylı bilgi verir. Bu bölümde USO sistemleri anlatılmakta ve bu sistemlere duyulan ihtiyaçlar ve sistemin getirdiği yararlardan söz edilmektedir. Bu bölümde ayrıca dünya üzerinde kullanılan USO sistemleri hakkında bilgi verilmektedir.

Üçüncü bölüm uygulamada kullanılan GPRS teknolojisi hakkında bilgi vermekte ve GPRS modüller anlatılmaktadır. Aynı zamanda GPRS modüllerin kullanım alanlarında ve avantajlarında bahsetmektedir.

Dördüncü bölüm "GPRS ile USO sistemi" incelenmiş ve "GPRS ile USO sistemi" ile ilgili bir uygulama geliştirilmiştir. Geliştirilen bu uygulama ayrıntılı bir şekilde bu bölümde incelenmiştir.

Beşinci bölümde DES(Data Encryption Standard) algoritması anlatılmış ve geliştirilen "GPRS ile USO sistemi" uygulamasında nasıl kullanıldığı anlatılmıştır.

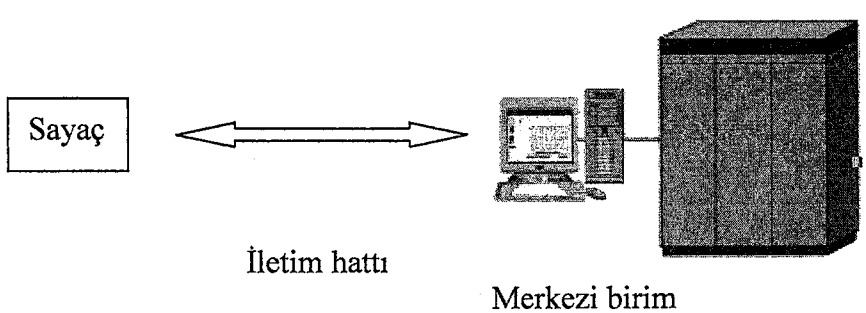
Altıncı ve son bölüm, sonuç ve öneriler bölümüdür. Bu bölümde, yapılan çalışma sonunda elde edilen sonuçlar ve tez konusu ile ilgili ileride yapılabilecek çalışmalara yönelik öneriler yer almaktadır.

BÖLÜM 2. USO

2.1. USO Nedir

USO (Uzaktan Sayaç Okuma), PLC (Power Line carier), SMS (Short Message Service), RF (Radio Frequency) , telefon hattı gibi haberleşme birimleri kullanılarak uzaktan sayaçlardaki verileri okuma sistemidir. Bunu sadece okuma sistemi olarak değerlendirmemek gerekmektedir. Sayaçlar bu sistemler ile kendi durumlarını, müdahaleye uğrayıp uğramadıklarını, ön ödemeli sistemlerde sayaçlara internet üzerinden veya merkezi birimden kredi yüklemek gibi bir çok şeyi kapsamaktadır. USO su, gaz ve elektrik sayacı servisi sağlayan şirketlerin verimliliğini artırır, müşteriye sunulan hizmetleri genişletir, sayaç okuma maliyetini düşürür, kritik bilgilerin anında merkeze bildirilmesini sağlar [7] .

Temel olarak USO üç kısımdan oluşur. Bu birimler şunlardır: Sayaç, Haberleşme Birimi ve Merkezi Sistem Birimidir.



Şekil 2.1. USO sistemi

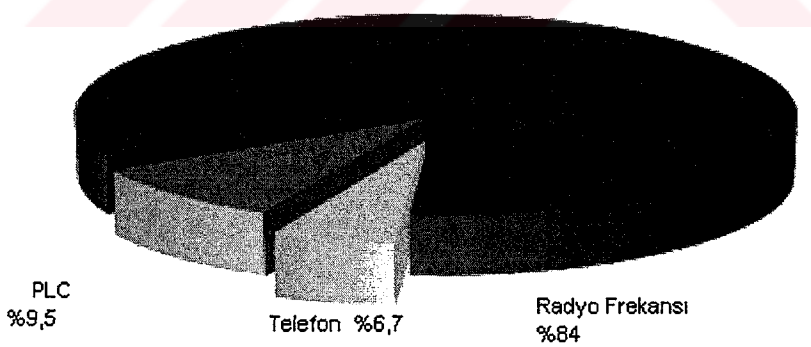
2.2. USO Çeşitleri

USO uygulamaları kullanılan haberleşme birimlerine göre çeşitlilik göstermektedir. Haberleşme birimleri USO uygulamalarının en önemli birimleridir. Bu birimin ne kadar sağlıklı ve başarılı olur ise USO uygulaması da o derece başarılı ve sağlıklı olur. Aynı zamanda haberleşme birimleri USO uygulamalarının maliyetini belirlemektedir [7].

USO uygulamalarında en çok kullanılan haberleş birimleri şunlardır.

- Telefon Hattı
- PLC
- RF
- SMS
- GPRS

Aşağıdaki grafikte Dünya çapında USO uygulamalarında kullanılan haberleşme birimlerinin kullanım yüzdeleri bulunmaktadır.

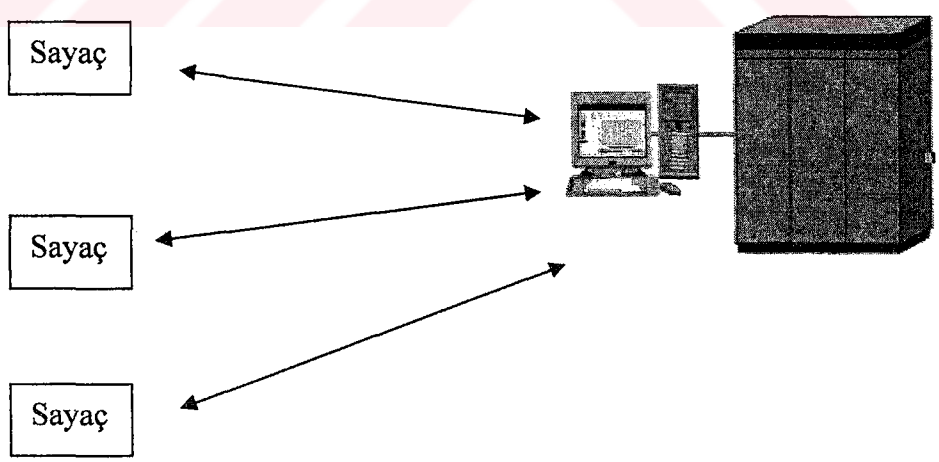


Şekil 2.2. Kullanım yüzdesi

GPRS ve SMS teknolojileri USO uygulamalarında yeni yeni kullanılmaya başlanmıştır. Bu yüzden grafikte gösterilmemektedir.

2.1.1. Telefon hattı

Telefon hattı USO uygulamalarında modemler ile kullanılmaktadır. Veriler önce telefon hattında gidebilecek şekilde modüle edilirler. Karşı tarafta ise alınan veriler demodülasyon ile tekrar elde edilir. Burada merkezi birim erişmek istediği sayacın numarasını çevirerek arar ve data alışverişinde bulunur. Bu işlemi her bir sayaç için sıra ile yapar. Aynı şekilde sayaç kritik bir veriyi aktarmak istediğinde merkezi birimi arar ve verilerini aktarır. Telefon hattının avantajı her evde bir telefonun olmasıdır. Telefon hattında maksimum 56KBps hızında veri aktarılabilir. Aslında bu hız USO uygulaması için yeterlidir. Aynı evde hem su, hem elektrik ve hem de gaz sayacı var ise bu durumda bu üç sayacıda USO uygulamasına bağlamak sorun oluşturmaktadır. Ya her bir sayaç için ayrı hat çekilmeli veya sayaçların önüne bir tane yönetici birim koyulmalıdır. Bu yönetici birim merkezi birimin oradaki muhatabıdır. Merkezi birim yönetici birimle bağlantı kurar ve oradaki hangi sayaç ile bağlantı kurmak istediğini bildirir. Yönetici birim ona göre işlem yaparak merkezi birimin istediği sayaç ile haberleşmesini sağlar [7].



Şekil 2.3. Telefon hattı ile USO

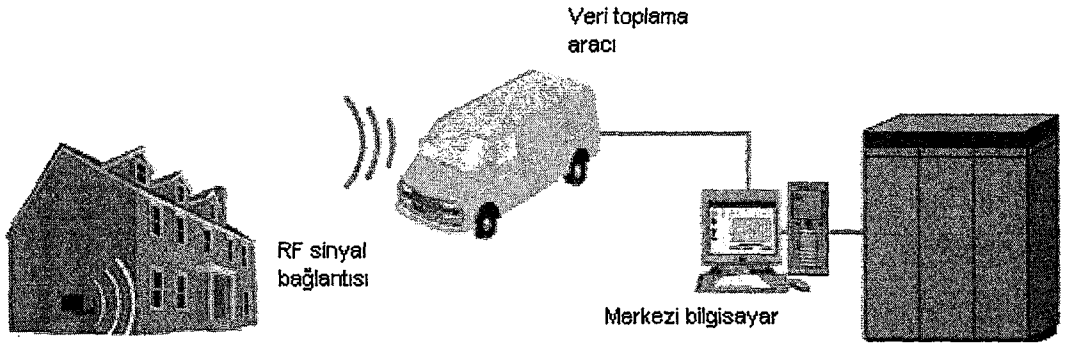
2.2.2. PLC (Power Line Carier)

PLC, mevcut elektrik hatları üzerinden veri haberleşmesini sağlayan bir teknolojidir. Özel bir şekilde modüle edilen veriler mevcut elektrik hattına aktarılmaktadır. Alınan verilerde aynı şekilde demodüle edilerek elde edilmektedir. Elektrik hattının en büyük dezavantajı gürültünün çok olmasıdır. Elektriğe bağlı olarak çalışan her aygıt, elektrik hattında gürültü oluşturmaktadır. Bu gürültülerde aktarılan verilerin bozulmasına sebep olmaktadır. Veri aktarımının başarısını yükseltmek için Dual Narrow Band (çift ince kuşak) ve DSP (Digital Signal Processor, Sayısal Sinyal İşlemcisi) kullanılmaktadır. PLC haberleşmesi trafo geçişlerine kadar olmaktadır. Veriler trafo geçişine kadar elektrik hattında gider, daha sonra başka bir şekilde o verilerin merkezi sisteme aktarılması gerekmektedir. Bu yüzden sadece PLC kullanılarak USO uygulaması yapılamamaktadır. Trafodan sonra verileri aktarmak için telefon hattı ve GPRS kullanılabilir. Her bir trafoya bir arabirim koymak gerekmektedir. Bu arabirim, trafoya gelen verileri merkezi birime aktarmak ile görevlidir [5].

2.2.3. RF (Radio Frequency)

RF, USO uygulamalarında en çok kullanılan haberleşme çeşididir. En önemli özelliği kablolara olan ihtiyacı ortadan kaldırmasıdır. USO uygulamalarında genellikle düşük güçlü RF modüller kullanılır. Bu modüller FSK (Frequency Shift Key), GFSK (Gaussian Frequency Shift Key), ASK (Amplitute Shift Key) gibi modülasyon çeşitlerini kullanırlar. Bu modüller ISM bandındaki frekanslarda çalışırlar. En çok kullanılan bandlar 433, 868, 915Mhz'dir. Şu andaki mevcut rf uygulamalarında genelde 433 Mhz bandı kullanılmaktadır. Bu da Rf kirliliğinin oluşmasına sebep vermektedir, ve data aktarımlarında hata oranlarını artırmaktadır. Bu hata oranlarını düşürmek için çeşitli yöntemler kullanılmaktadır. Bunlardan bir tanesi çalışma esnasında yoğun olan frekanstan başka bir frekansa geçmektir. Bir diğeri ise her bir biti bir bit dizesi şeklinde göndermektir. Örneğin '1' yerine 0110001010101101, '0' yerine ise 1001110101010010 ('1' değerine karşılık gelen dizelerin 'not' işlemine tabi tutulmuş hali) bit dizelerini göndermektir. Bu dizelerden iki veya 3 tane bit bozulsa bile hangi bit değerine karşılık geldiği anlaşılmaktadır. Bu yöntemin

dezavantajı iletim hızını düşürmesidir. USO uygulamalarında düşük güçlü RF modüller kullanıldığı için iletim mesafeleri de kısadır. Yaklaşık olarak 100m civarındadır. Genelde RF'li USO uygulamalarında gezici bir birim vardır. Bu gezici birim araba ile olabileceği gibi bir bisiklet veya motosiklet ile de olabilir. Bu birim ana sokaklarda gezerek verileri otomatik olarak sayaçlardan okumaktadır.



Şekil 2.4. RF ile USO

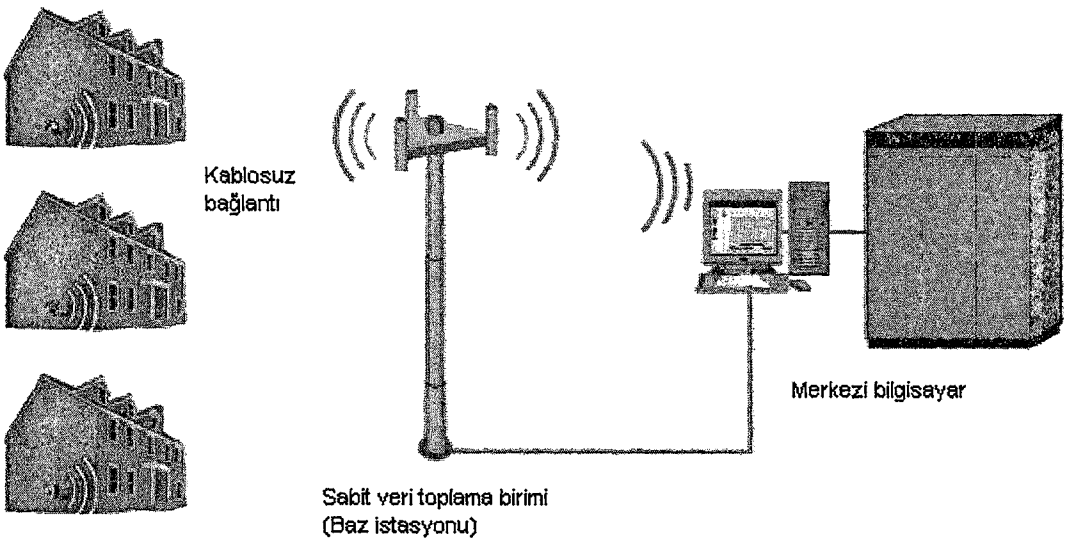
2.2.4. SMS (Short Message Service)

SMS, USO uygulamalarında yaygın olarak kullanılmaz. Bunun nedenleri pahalı olmasıdır. Sistemin yoğun olduğu durumlarda da mesajların anında gitmemesi söz konusudur. SMS mesajlarda Latin alfabesi kullanıldığında maksimum karakter sayısı 160, Latin olmayan alfabeler kullanıldığında ise 70 karakterdir. SMS uygulaması için GPRS/GSM modemler kullanılır.

2.2.5 GPRS (General Packet Radio Service)

GPRS teknolojisi USO uygulamalarında yeni kullanılmaya başlanan bir teknolojidir. USO uygulamalarında bu teknoloji kullanımı hızla artmaktadır. Bunu nedeni kullanım ücretinin az olması ve mevcut GSM ağını kullanmasıdır. Bu teknoloji ile cep telefonlarının çektiği her yerde kablosuz internet hizmetinden faydalanılabilmektedir. USO uygulamaları için her bir sayaca bir adet GPRS modül takılması gerekmektedir. Sayaçlarda bulunan bu modülleri kullanan mikro işlemciler,

gerekli olduğu durumlarda bu modüller ile internete bağlı bulunan merkezi işlem birimine bağlanarak verilerini aktarırlar [1].



Şekil 2.5. GRPS ile USO uygulaması

Şu anki GPRS modül fiyatları oldukça pahalıdır. Modül fiyatlarının düşmesi ile birlikte bu teknolojinin USO uygulamalarındaki yeri çok hızlı bir şekilde artacaktır.

BÖLÜM 3. GPRS MODÜL

3.1. GPRS Nedir

GPRS (General Packet Radio Service/Paket Anahtarlamalı Radyo Hizmetleri), verilerin mevcut GSM şebekeleri üzerinden saniyede 28.8 Kb'den 115 Kb'ye kadar varabilen hızlarda iletilmesine imkan veren, cep telefonu, dizüstü bilgisayar, PDA ve diğer mobil cihaz kullanıcılarına kesintisiz İnternet bağlantısı sunan bir mobil iletişim servisidir [2].

GPRS, mobil iletişim teknolojisinde halen kullanılmakta olan devre anahtarlama (sadece tek bir kullanıcıya tahsis edilen bir hat üzerinden sürekli bağlantı) metodu yerine paket anahtarlama (aynı hattın birden çok kullanıcı tarafından paylaşıldığı ve iletişim hızının 115 Kb'ye kadar çıktığı bir yapı) yöntemini kullanmaktadır [2].

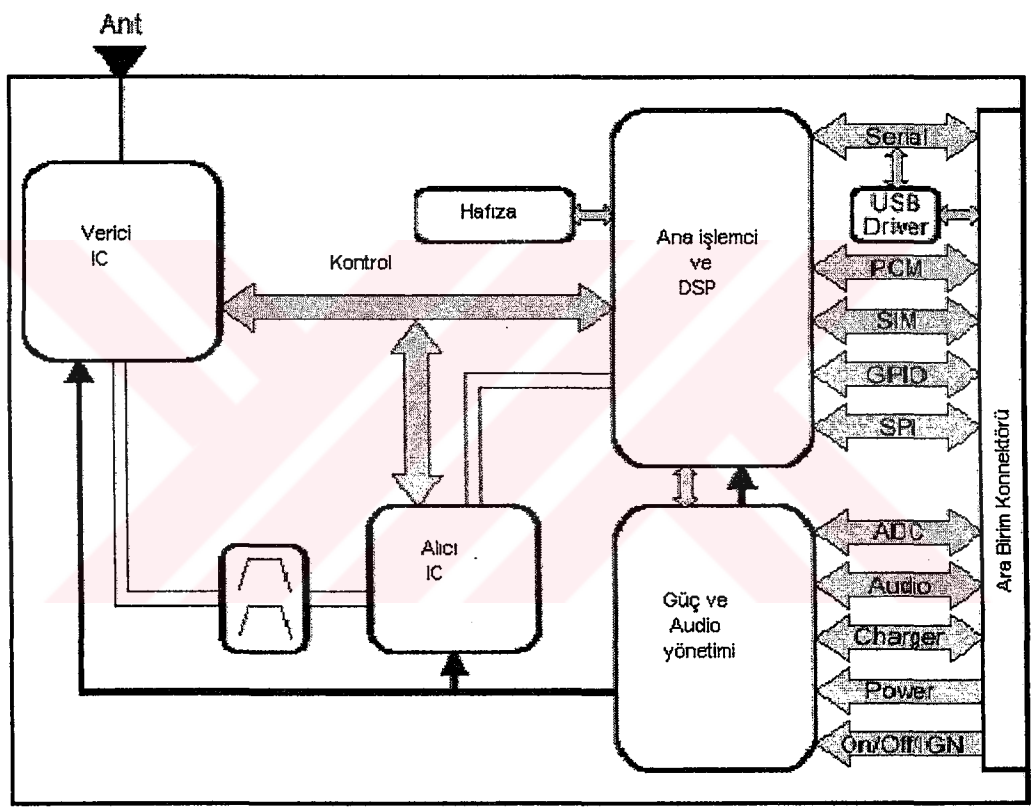
GSM ağlarının normal şartlar altında sunduğu 9.6Kb iletim hızıyla karşılaştırıldığında bu değerler 3 ile 12 kat arasında değişen bir performans artışını ifade etmektedir.

GPRS teknolojisi, kullanıcıya yüksek hızlı bir erişimin yanı sıra, bağlantı süresine göre değil gönderilen ve alınan veri miktarına göre ücretlendirilen ucuz iletişim olanağı da sağlar. Bu sistemde aboneler, internet'e bağlı kaldığı süreye göre değil, yalnızca alıp gönderdikleri veri miktarı kadar ödeme yaparlar.

3.2. GPRS Modül ve Çeşitleri

Şu anda piyasada bir çok farklı özelliklerde GPRS modüller bulunmaktadır. Piyasadaki GPRS modülleri birbirinden ayıran en önemli özellik TCP/IP stack'tir. Bazı modüllerin içerisinde gömülü TCP/IP stack mevcuttur. Bu özellik gömülü

sistemler için bir çok uygulamanın hızlı geliştirilmesine olanak sağlar. Modül içersindeki TCP/IP stack sayesinde çok basit bir şekilde internetteki bir sunucuya bağlantı gerçekleştirilebilir. Bunun için birkaç tane AT komutu yeterlidir. TCP/IP desteği olmayan modüllerde bu desteği vermek için TCP/IP stack uygulamasının yazılması gerekmektedir. Bu ise fazladan yük ve maliyet getirir. Gömülü olarak TCP/IP stack desteği olanların ise birkaç farklı temel özellikleri mevcuttur. Bu özellikler, sunucu portu açıp açamaması, birden fazla portu aynı anda kullanabilmesi gibi [1].



Şekil 3.1. GPRS modül iç blokları

Yukarıda genel bir GPRS/GSM modülünün blok şekilleri görülmektedir.

- Ana işlemci ve DSP : Bu blok tüm ünitelerin görevlerini yerine getirmek ve yönetmek ile ilgilenir. Bu birimde aşağıdaki bileşenler bulunur.
- Ana işlemci
  - Konuşma seçenekleri için DSP işlemci
  - UART
  - USB

- Dijital audio sürücüsü
- SIM kart
- İki tane SPI veri yolu, biri içerde diğeri dışarıda
- Ana osilatör (26MHz)
- Adres/veri yolu
- RF PLL
- Modülün kalbini oluşturan RF işlemcilerin kontrolü

- Alıcı Blok (Receiver Blok) : Bütün alıcı kanallarını içerisinde bulunduran RF blok. Bu blokta aşağıdaki bileşenler bulunur.
- Ön filtre
- LNA'lar
- Mixer
- VCO'ler
- I/Q çıkışlar
- Kontrol sinyalleri

- Verici Blok (Transmitter Blok): Bütün verici kanalları içerisinde bulunduran RF blok. Bu blok aşağıdaki bileşenleri bulundurur.
- Güç yükselteçleri
- Güç kontrol döngüleri
- Anten anahtarlama
- Harmonik filtre
- Giriş tamponu
- Kontrol sinyalleri
- Anten bağlantısı

GPRS modüller ile haberleşme genelde RS232 hattı üzerinden geçekleştirilir. Haberleşmede AT modem komutları kullanılır. Bu komutlara ek olarak genelde modüle bağlı olan özel komutlarda mevcuttur.

Örnek:

Pin numarasını girmek için,

AT+CPIN=1234

Gelen çağrıya cevap vermek için,

ATA

DTMF tonu göndermek için,

AT+VTS=5 5 numaralı tuşun DTMF kodunu yollar

En son aranan numarayı tekrar aramak için

ATDL

GSM ağına bağlantı için (Network Registration)

AT+CREG? Hangilerini desteklediğini görmek için

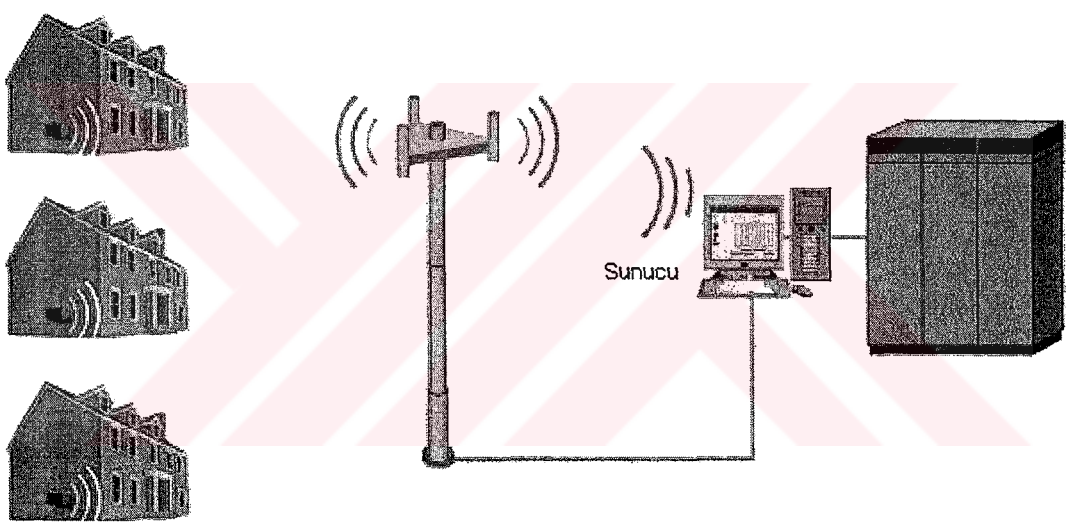
AT+CREG=1 bağlanmak için

3.3 GPRS Modül Uygulamaları

GPRS modül, internet bağlantısına ihtiyacı olan her taşınabilir cihazda çok rahat bir şekilde kullanılabilir. GPRS modüller, ev otomasyonu, taşınabilir pos cihazları, telefon santralleri, güvenlik sistemleri ve USO uygulamaları gibi bir çok uygulamalarda kullanılmaktadır. GPRS modülün kullanım alanları her geçen gün artış göstermektedir.

BÖLÜM 4. GPRS MODÜL İLE USO UYGULAMASI

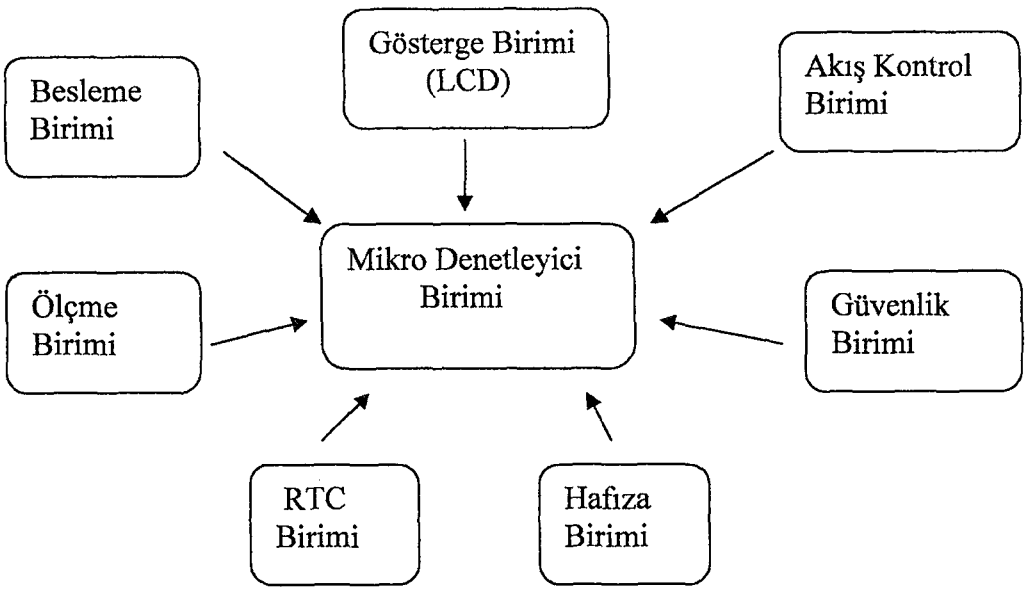
Bu bölümde GPRS ile USO uygulamasının mimari yapısı anlatılmaktadır. GPRS ile USO uygulaması üç temel birimden oluşmaktadır. Bu birimler, Veri Aktarım Birimi(GPRS kısmı), Sunucu Birimi ve İstemci Birimi'dir. Bu çalışmada özellikle Veri Aktarım Birimi incelenmiştir.



Şekil 4.1. GPRS ile USO

4.1. Basit Elektronik Sayaç Yapısı

Bir sayaç basit şekilde bir kaç ana birimden oluşur. Bu birimler, Besleme Birimi, Gösterge Birimi (LCD), Ölçme Birimi, Hafıza Birimi, Güvenlik Birimi, Akış Kontrol Birimi, RTC (Real Time Clock, Gerçek Zaman Saati) Birimi ve son olarak tüm birimleri kontrol eden ve yöneten Mikro Denetleyici Birimi. Biz bu modüllere ek olarak GPRS modül ekleyeceğiz.



Şekil 4.2 Elektronik sayaç yapısı

Besleme Birimi : Devreye güç sağlayan birimdir. Bu birimin önemi GPRS modül kullanıldığında daha da fazla artmaktadır. Çünkü GPRS modüller anlık 1,5A ile 4A arasında akım çekebilmektedir. Bu değer modülden modüle farklılık göstermektedir. Normal bağlantı esnasında ise 200 - 300 mA akım çekmektedir. Bu birim elektrik sayaçlarında beslemeyi şebekeden sağlanmaktadır. Su ve doğal gaz sayaçlarında ise pil kullanılmaktadır.

Ölçme Birimi : Bu birim elektrik sayaçlarında, su sayaçlarında ve gaz sayaçlarında farklılık göstermektedir. Sayaçlarda kullanılan bir çok ölçme tekniği mevcuttur.

Gösterge Birimi : Bu birim Sayacın ekranını oluşturur. Sayaca ait tüm bilgiler burada gösterilebilir. Bu birim genelde modül LCD'lerden veya cam LCD'lerden oluşmaktadır.

Akış Kontrol Birimi : Akışın kontrolünü sağlayan birimdir. Akış kesme ve açma işlemlerini yerine getirir. Örneğin su sayaçlarında bu işi servo motorlu vanalar yerine getirir.

Güvenlik Birimi : Sayaca dışarıdan müdahaleyi algılayan birimidir. Bu birim birkaç tane anahtardan oluşur.

Hafıza Birimi : Sayaca ait bilgilerin tutulduğu birimdir. Bu birim sayaç ile ilgili her şeyi tutar. Sayacın bozulmasında dahi bu bilgiler sayaç devresinden elde edilebilir. Bu birim EEPROM 'dan oluşmaktadır.

RTC Birimi : Gerçek zaman saati birimidir. Zamana bağlı yapılan standart işlerin kontrol edilmesini sağlar.

Mikro Denetleyici Birimi : Diğer birimleri yöneten ve sayacın tüm işlemlerini denetleyen merkezi bir birimdir. Bu birim bir adet mikro denetleyiciden oluşmaktadır. Genelde kullanılan mikro işlemci 8 bitlik, flash rom ve ram'i içerisinde olan ve bir çok çevresel birimi (UART, SPI, I2C, timer, ADC....) içerisinde gömülü olan mikro denetleyicilerdir. Bu birim aynı zamanda GPRS modülü kontrol edecek yazılımı da içerisinde barındıracaktır.

4.2. Veri Aktarım Birimi

Bu birim, sayaçtaki verinin internet üzerinden sunucu birimine başarılı bir şekilde aktarılmasından sorumludur. Bu birim, belirli aralıklarla sunucu birimine bağlanır ve veri transferini gerçekleştirir. Bu aralıkların bağlantı kuracak sayaç miktarına göre ayarlanması gerekmektedir. Bu ayarlama işlemi bağlantı yoğunluğunu zamana yayacak şekilde olmalıdır.

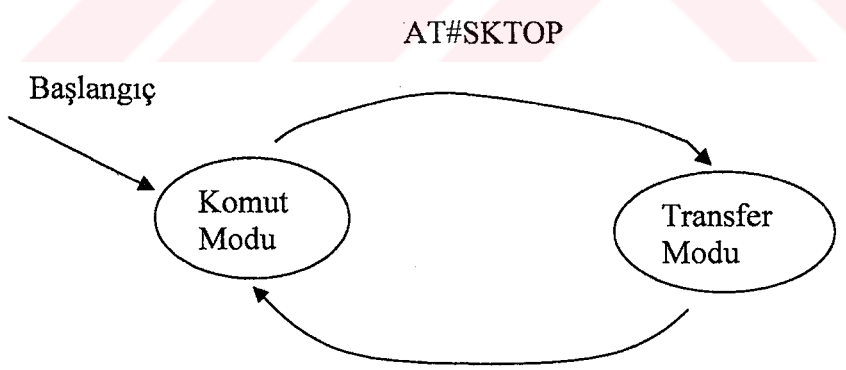
4.2.1. GPRS modül ile internete bağlanma

GPRS ile internete bağlanmak için AT komutlarını UART üzerinden GPRS modüle göndermek gerekmektedir. GPRS ile mikro denetleyici arasındaki haberleşme UART üzerinden gerçekleşir. GPRS modülün ve GSM şebekesinin ayarları bu bağlantı üzerinden aktarılan veriler ile yapılır. GPRS modüller genelde standart olarak 9600

bps hızında çalışmaya başlarlar. İlk başlangıçtan sonra bu hız AT komutları ile değiştirilebilir.

Uygulamada kullanılan GPRS modül Telit GM862'dir. GM862 içerisinde gömülü TCP/IP stack olan bir modüldür. GM862 iki modda çalışır. İlk mod komut modudur. Bu modda UART üzerinden gelen komutlara göre işlem yapar. İkinci modu transfer modudur. Bu modda modül sadece UART veri transferi yapar. Bu modda iken hiçbir komut kabul edilmez. UART üzerinden gelen verileri paketler ve bağlı olduğu adrese yollar. Adresten gelen verileri ise UART üzerinden mikro denetleyiciye gönderir. Komut modundan transfer moduna bağlantı kurulduğu anda geçer (AT#SKTOP komutu ile). Transfer modundan komut moduna ise bağlantı koptuğunda veya "+++" karakterleri gönderildiğinde geçer. Bu karakter dizesi aynı zamanda veri transferinde de gönderilebilir. Veri transferi esnasında gönderilen karakterler arasında bu dizeler olduğunda bağlantının kesilmemesi gerekir. Bunu sağlamak için bu karakter dizesini göndermeden önce gönderdikten sonra bir miktar bekleme süresi vardır. Bu bekleme süresi ATS12 komutu ile belirlenir. Bu değer default olarak 50 (1 saniye)'dir. Komutun değer aralığı ise 20-255'dir.

ATS12 = 100



Şekil 4.3. GM862 durum makinesi

Şebeke ayarları şebekeden şebekeye değişiklik göstermektedir. Aşağıda şu an faaliyette olan üç şebekenin Telit GM862 GPRS modüle göre bağlantı ayarları verilmiştir.

GM862 için bağlantı adımları,

- GPRS giriş ayarlarını yap
- Gömülü olan TCP/IP stack ayarlarını yap
- Bağlantı kurulacak noktayı tanımla
- GPRS ve soket bağlantı isteği yap
- Veri transferini gerçekleştir
- Bağlantıyı kapat

Komutlar,

- AT E0 : yollanılan komutları yankılandırmaması için

- AT V0 : komutların sonuçlarını rakam olarak yollaması için

- AT + CGATT : bu komut ile GPRS bağlantısı kurulur veya bağlantı kesilir.

Örnek,

AT + CGATT = 1	bağlantıyı kurmak için
AT + CGATT = 0	bağlantıyı kesmek için
AT + CGATT ?	bağlantı durumunu görmek için

- AT + CGDCONT : bu komut ile GPRS bağlantı ayarları yapılır. Şebekeden şebekeye farklılık gösteren komut sadece budur.

AT + CGDCONT = 1, "IP", "internet"	Turkcell ve Avea için
AT + CGDCONT = 1, "IP", "telsim"	Telsim için

- AT # USERID : bu komut ile kullanıcı adı girilir.

AT # USERID = "avea"

- AT # PASSW : bu komut ile şifre girişi yapılır.

AT # PASSW = "gprs"

- AT # PKTSZ : gönderilecek paketteki veri miktarını belirler. Modüle gönderilen verilerin sayısı burada belirtilen değere ulaşana kadar modül verileri yollanmaz. Bu değere ulaştıktan sonra yollar. Bu değer maksimum 512'dir. Bu modül ile tek pakette maksimum 512 byte yollanabilir.

AT # PKTSZ = 6

- AT # DSTO : veri yollama esnasındaki zaman aşımı değerini belirleme komutudur. 0 (sıfır) değeri zaman kontrolü yok demek. Aldığı değerler 0-255 arası sayıdır. Her bir artış 100ms karşılık gelir.

AT # DSTO = 0

- AT # SKTTO : burada belirtilen süre kadar veri transferi yapılmaz ise soket bağlantısı kesilir. 0 (sıfır) değeri zaman aşımı yok demektir. Aldığı değerler 0-65535 arasındadır. Değerler saniye cinsindendir.

AT # DSTO = 0

- AT # SKTSET : bu komut soket parametrelerini belirler. İlk parametre soket tipi, ikincisi bağlantı kurulacak port numarası, üçüncüsü bağlantı kurulacak adresi belirler.

Soket tipi,
0 : TCP
1 : UDP

AT # SKTSET = 0, 80, "212.174.163.2"

- AT & K0 : bu komut ile UART haberleşmesindeki RTS/CTS kontrolünün kullanılmayacağı belirtilir.

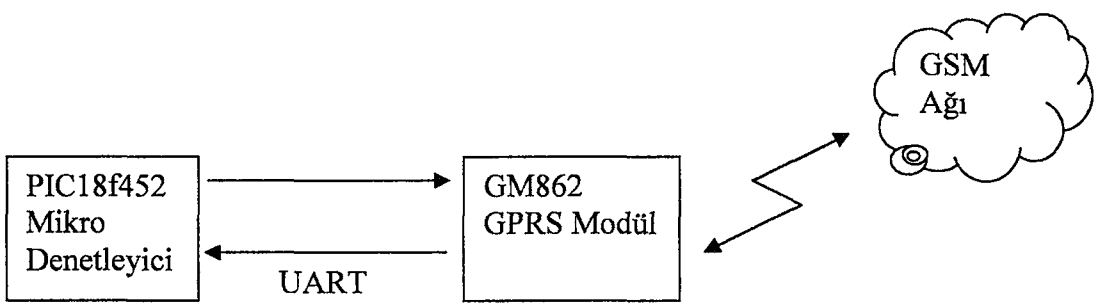
AT&K0

- AT # SKTOP : ayarlar yapıldıktan sonra bağlantı bu komut ile kurulur.

4.2.2. GPRS modül sürücüsü (driver)

Bu sürücü, sayaç programlarında çok fazla değişiklik yapmadan GPRS modülü kullanmayı sağlar. Modül PIC18F452 mikro denetleyicisi için c dili kullanılarak

geliştirildi. C derleyicisi olarak Microchip firmasına ait C18 derleyicisi kullanıldı. Bu sürüsü programı ile çok fazla GPRS modül bilgisi gerekmeksizin mikro denetleyici ile GPRS modül kullanılarak internete bağlanılabilir. GM862 deki UART ile bağlantıda 232 gibi sinyal dönüştürücülerine gerek yoktur. Direk olarak 5V da çalışan mikro denetleyici pinlerine bağlanabilir. Sinyal seviyesi '1' için 5V, '0' için ise 0V.



Şekil 4.4. GPRS ve mikro denetleyici

Sürücü programda kullanılan API'ler aşağıda ayrıntılı bir şekilde anlatılmıştır.

InitModule : Her hangi bir parametre almaz ve parametre geriye döndürmez. Bu API sürücü programını başlatmak için kullanılır.

```
InitModule();
```

SendDataModule : Bu API OutBuff dizisinde bulunan OutLen uzunluğundaki veriyi GPRS modüle yollar. Örneğin,

```
OutBuff[0] = 'A';
OutBuff[1] = 'B';
OutBuff[2] = 'C';
OutLen = 3;
SendDataModule();
```

ConnectInternet : Bu API, GPRS modülü internete bağlar. Unsigned char tipinde bir değeri parametre olarak alır. Bu alınan parametre hem şebekeden hem de pil ile çalışan sayaçlar için kullanılır. Bu parametre 1 ise ve şebeke elektriği kesik ise

bağlantıyı gerçekleştirmez. Bu parametre 0 ise ve elektrik yok ise GPRS bağlantısı pil kullanılarak gerçekleştirilir. Bu özellik şebekede elektrik olmaması durumunda normal veri gönderimini engellemek içindir. Sadece acil durumlarda (sayaca müdahale gibi) pil kullanılarak bağlantı kurulmasını sağlar. Bu API internet bağlantısı başarılı bir şekilde kurulmuş ise 1 değerini geriye döndürür, hata durumunda 0 değerini geriye döndürür.

```
rt =  ConnectInternet(1);
if ( rt == 1)
        // bağlantı gerçekleşti
else
        // bağlantı başarısız
```

CloseConnection : İnternet bağlantısını keser ve GPRS modülü kapatır.

```
CloseConnection();
```

InitGPRSModule : GPRS modül ayarlarını yapar ve internet bağlantısını kurar. Bu API modül bağlantı kuramadığı takdirde TRY ile tanımlanmış sayı kadar deneme işlemi yapar. Bu API ConnectInternet tarafından kullanılır. Bağlantı kurması durumunda geriye 1 döndürür, kuramaması durumunda 0 döndürür.

```
InitGPRSModule();
```

SetModule : Bu API, GPRS modüle internete bağlanması için gerekli AT komutlarını sıra ile yollar. InitGPRSModul tarafından kullanılır.

Örnek,

```
unsigned char rt;
rt  = ConnectInternet(1);
if ( rt == 1)
{
        OutBuff[0] = 'S';
        OutBuff[1] = 'A';
        OutBuff[2] = 'Ü';
        OutLen = 3;
```

```
        SendDataModule();
        CloseConnection();
    }
```

Gelen veri InBuff dizisinde tutulur. Gelen veri uzunluğu InLen değişkeninde tutulmaktadır.

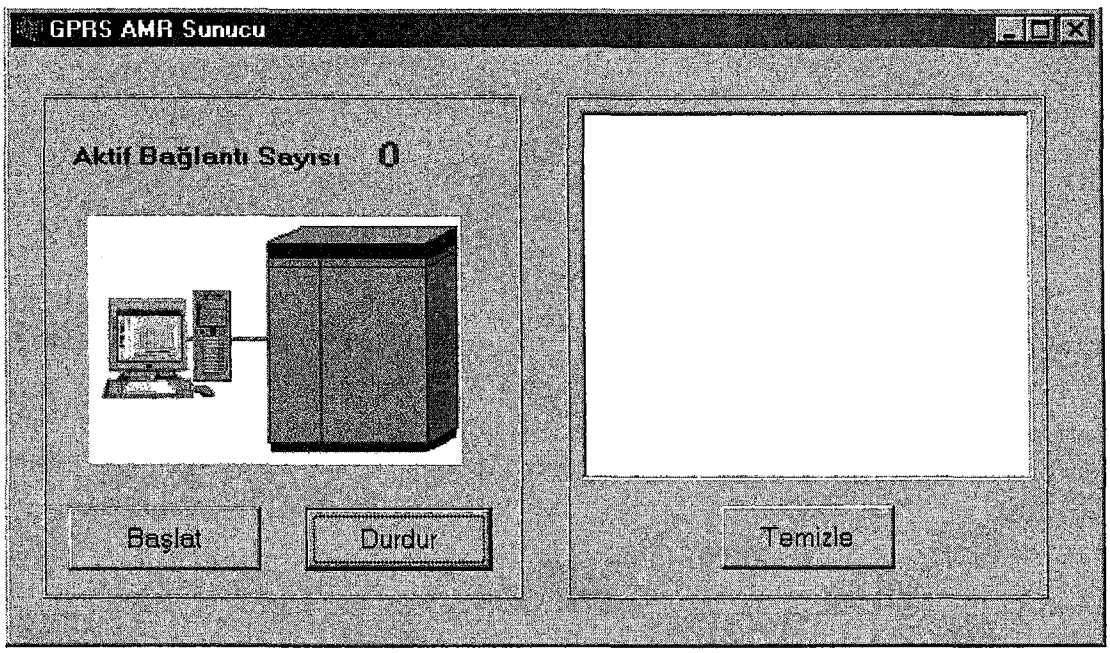
4.3. Sunucu Birimi

Bu birim sayaçlardan gelen verileri ve sayaçlara aktarılacak olan verileri veri tabanında tutan birimdir. Bu birim iki kısımdan oluşmaktadır. Birinci kısım ara yüz programı, ikinci kısım veri tabanı kısmıdır.

4.3.1. Ara yüz programı

Bu program sadece GPRS ile USO uygulamasında test amaçlı geliştirilmiştir. Bu çalışmanın amacı böyle bir program geliştirmek değildir. Bu yüzden program oldukça basittir. Program bir sunucu portu açar. Bu port 5007 numaralı porttur. Sayaçlar veri aktarmak istediklerinde bu porta bağlanırlar. Bir sayaç sunucu programa bağlandığında ilk olarak sunucu programa seri numarasını ve ne amaçla bağlandığını gönderir. Eğer sayaç genel kontrol için bağlanmışsa, sunucu program veri tabanına bu sayaç ile ilgili yapılması gerekli bir iş var mı diye bakar. Var ise bu işleri yerine getirir. Örneğin, son endeks değerini isteyebilir, sayaç ön ödemeli bir sayaç ise ve kredi yüklenecekse kredi yükler, sayaç kullanıma kapatılacaksa sayacı kapatır. Eğer sayaç genel kontrol haricinde bağlanmış ise, sunucu program önce sayacın yolladığı verileri alır. Bu veriler genelde sıra dışı bir durumun olduğunu gösterir. Örneğin, sayaca müdahale edilmesi gibi. Sunucu program bu verileri alır ve veri tabanına kayıt eder.

Aşağıda sunucu programın ekran görüntüsü bulunmaktadır.



Şekil 4.5. Sunucu programın ekran görüntüsü

Sunucu programı oldukça basit bir programdır.

Aktif Bağlantı Sayısı: O an sunucu programına bağlı olan sayaç sayısını göstermektedir.

Başlat butonu : Bu buton 5007 numaralı sunucu portunu açar ve sunucu programını başlatır.

Durdur butonu : Bu buton 5007 numaralı sunucu portunu kapatır. Aktif olan bağlantıların hepsinin bağlantısı kesilir.

Temizle butonu : Hataların, cezaların ve bağlanan sayaçların seri numaralarının yazıldığı yeri temizlemektedir.

4.3.2. Veri tabanı yapısı

Sunucu programın ve istemci programın bağlanarak gerekli işlemleri yaptığı birimdir. Basit bir veri tabanı kullanıldı. Bu işlem için Paradox 7 kullanıldı. Veri tabanı 4 tane tablodan oluşmaktadır. Bunlar,

- Ceza Tablosu
- Son Endeks Tablosu
- Yüklenecek Kredi Tablosu (Ön ödemeli sayaçlar için)

- Yüklenen Kredi Tablosu (Ön ödemeli sayaçlar için)

Ceza Tablosu: Bu tabloda, müdahale edilen sayacın seri numarası, müdahale türü ve müdahale tarihi tutulur. Buradaki müdahale tarihi sayacın kendi içerisinde tutuğu tarihtir. Müdahale türünü sayaç üzerindeki anahtarlar belirler. Bunlar, ön kapak açıldı, Rakorlara müdahale var veya pil kapağı açıldı gibi olabilir.

Tablo 4.1. Ceza Tablosu

Sayaç Seri No	Müdahale Türü	Müdahale Tarihi
123456	Ön kapak açıldı	24.03.2005 14:37
.....	.....	.....
.....	.....	.....

Son Endeks Tablosu: Bu tabloda, sayaçlara ait son endeks bilgileri tutulur. Bu bilgiler ön ödemeli olmayan sayaçlara aittir. Bu tabloda iki tane tarih bilgisi tutulmaktadır. Tarihlerden biri son endeks tarihini tutmaktadır. Diğeri ise bir önceki endeks tarihi tutmaktadır. Bu tabloda son endeks değeri ve bir önceki endeks değeri bilgileri de tutulur. Her son endeksin okunması durumunda okunan bu değer tablodaki son endeks hanesine yazılmadan önce orda bulunan değer önceki endeks hanesine geçirilir. Daha sonrada son endeks hanesine, okunan son endeks değeri kayıt edilir. Aynı şey tarih bilgileri içinde geçerlidir.

Önceki Endeks = Tablodaki son endeks

Tablodaki son endeks = USO ile okunan son endeks

Tablo 4.2. Endeks tablosu

Seri No	Son Endeks	Önceki Endeks	Son Endeks Tarihi	Önceki Endeks Tarihi
12345	100	59	12.06.2004	10.05.2004
.....	.....	.....	.....	.....

Yüklenecek Kredi Tablosu : Bu tabloda ön ödemeli sayaçlara yüklenecek kredi miktarı tutulur. Tablodaki kredi değeri sıfır ise kredi yükleme işlemi yok demektir. Sayaç sunucu programına bağlandığında sunucu program sayaç seri numarasına göre bu tabloda arama işlemi yapar ve bulduğu satırdaki kredi değerini kontrol eder. Eğer yüklenecek kredi var ise kredi yükleme işlemini yerine getirir. Elektrik sayaçları dışındaki sayaçlar pil ile çalıştıklarından sunucuya sürekli bağlanma veya sunucu ile çok sık bağlantı kurma durumları yoktur. Bu sebepten dolayı belirli zaman aralıkları ile bağlanır. Kredi yükleme işlemi de bu bağlantı esnasında geçekleştirilir. Bu sebepten dolayı kullanıcı krediyi aldığı anda alınan kredi sayaca anında yüklenemez. Tabloda ayrıca iki tarih bilgisi de tutulmaktadır. Tarihlerden biri kullanıcının krediyi satın aldığı tarih, diğeri ise kredinin sayaca yüklendiği tarihtir. Bu tarihler bir çok amaç için kullanılabilir. Kredi sayaca yüklendiği anda tablodaki kredi değeri sıfırlanır. Şu anda ön ödemeli sayaçlara kredi yüklemek için smart kartlar veya daha az özelliğe sahip olan memo kartlar kullanılmaktadır. Bu kartlar ile kullanıcılar satış yerlerine giderler ve kartlara kredi yükletirler. Sonrada kartı sayaca takarak karta yüklenen krediyi sayaca yüklenir. USO uygulaması olduğunda bu işlemlere gerek kalmadan uzaktan sayaca kredi yüklenebilecek. USO uygulaması ile internetten dahi sayaçlara kredi yükleme işlemi gerçekleştirilebilir. İnternetten kredi yükleme işleminde bankaların web ara yüzleri kullanılabilir.

Tablo 4.3. Yüklenecek kredi tablosu

Sayaç Seri No	Yüklenecek Kredi	Satın Alınma Tarihi	Yüklenme Tarihi
12345	150	10.06.2005	11.06.2005
3465	315	11.06.2005	
.....	.....	.....	.....
.....	.....	.....	.....

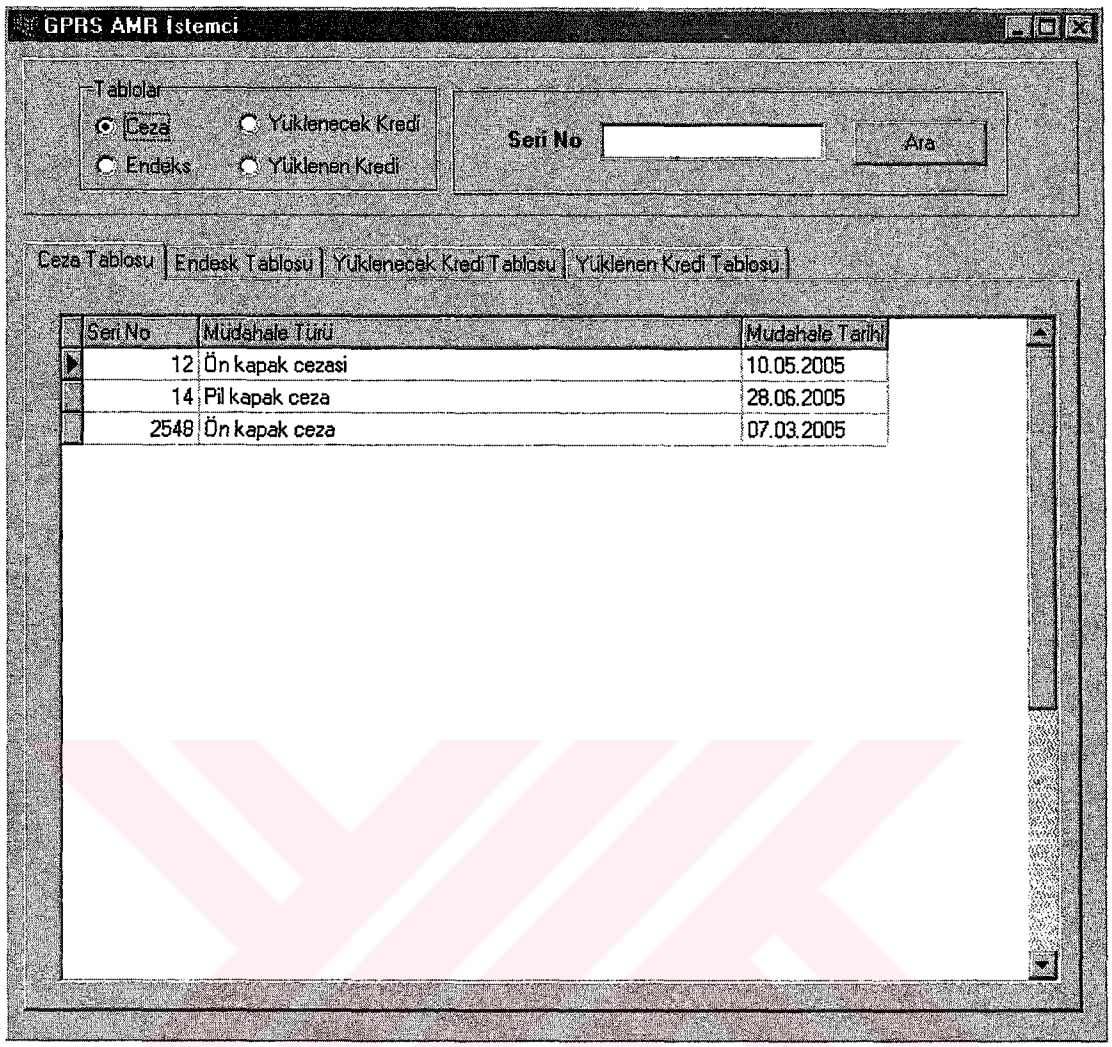
Yüklenen Kredi Tablosu : Bu tabloda yine ön ödemeli sayaçlar için kullanılmaktadır. Bu tablo her kredi satışında büyüyen bir tablodur. Sayaçlara yüklenen kredileri tutmaktadır. Üç sütunu vardır. Birincisi sayaç seri no, ikincisi yüklenen kredi miktarı, üçüncüsü de kredi yüklenme tarihidir.

Tablo 4.4. Yüklenen Kredi Tablosu

Sayaç Seri No	Yüklenen Kredi	Yüklenme Tarihi
12345	90	24.06.2005
4567	240	24.06.2005
.....	.....	.....

4.4. İstemci Birimi

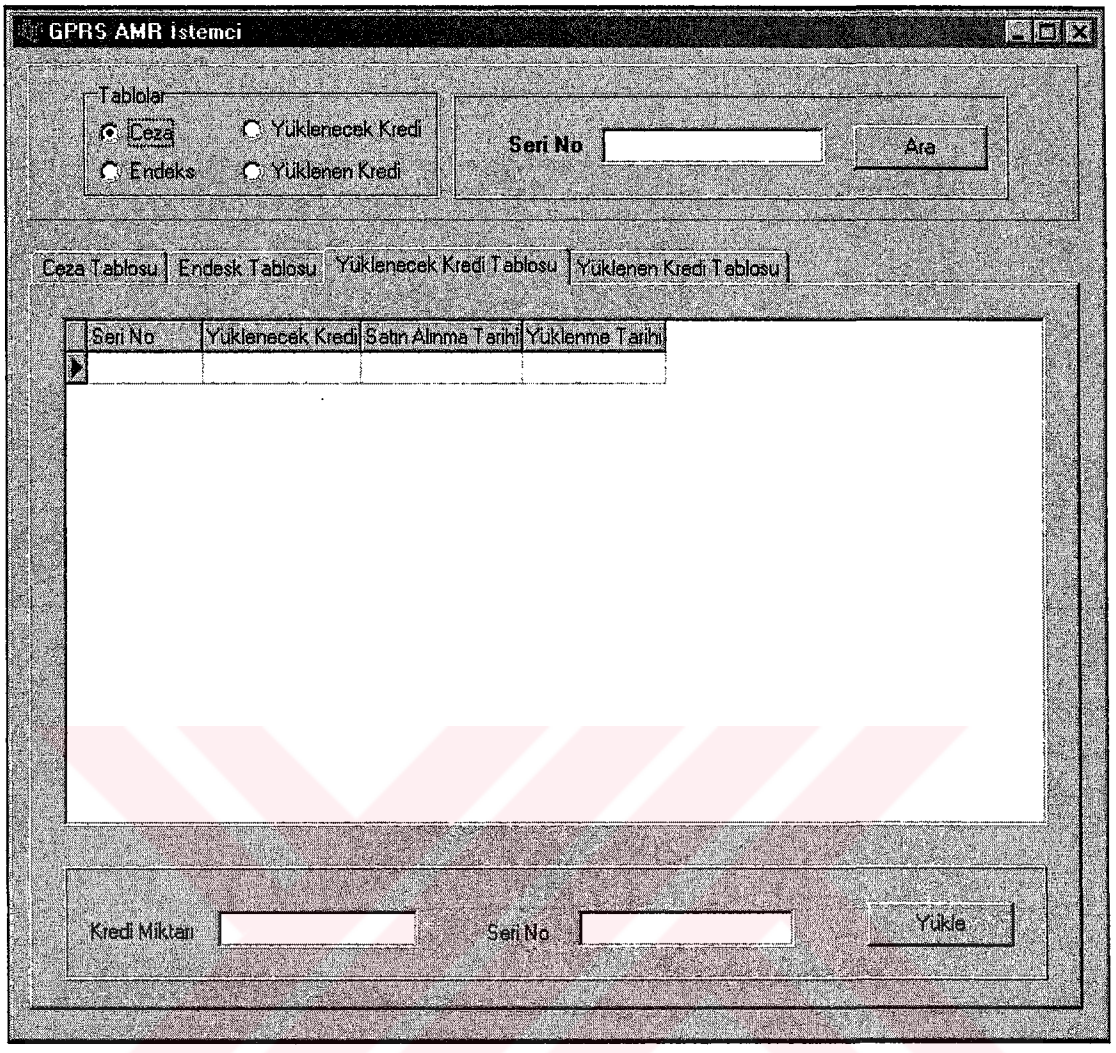
İstemci birimi, sunucu biriminin veri tabanına yazmış olduğu verileri görebilen, veriler üzerinde arama işlemi yapabilen ve sunucunun sayaçlara göndereceği verileri veri tabana yazan programdır. Ön ödemeli sayaçlara kredi yükleme işlemi de bu program ile yapılır.



Şekil 4.6. İstemci programı ekran görüntüsü

İstemci programın üst kısmında bulunan bölüm arama işlemleri içindir. Buradaki "Tablolar" kısmı arama yapılacak tabloyu seçmekte kullanılır. Arama işlemi sadece sayaç seri numarasına göre yapılmaktadır. Seri no kısmına hiç veri yazılmaz ise seçilen tablodaki verilen hepsi alttaki kısımda görüntülenir.

Programın alttaki kısmında ise her tabloya ait bilgilerin görüntülenmesi sağlanır. Buradaki tablolardan veriler incelenebilir.



Şekil 4.7. İstemci programı kredi yükleme yeri

Kredi yükleme işlemi "Yüklenecek Kredi Tablosu" bölümünden yapılmaktadır. Yüklenecek kredi miktarı ve sayaç seri numarası girilir ve kredi yükleme butonuna basılır. Bu işlemden sonra istemci programı bu değerleri "Yüklenecek Kredi" tablosuna kayıt eder. O seri numaralı sayaç sunucuya bağlandığı anda sunucu veri tabanındaki kredi miktarını sayaca yükler ve yükleme tarihini kayıt eder. Aynı zamanda bu verileri "Yüklenen Kredi" tablosuna da ekler.

4.5. Haberleşme Protokolü

Haberleşme protokolü GPRS modül ile sunucu arasındaki veri transferinde kullanılır. Bu protokolde yapılacak olan tüm işlemler tanımlanmıştır. Bu işlemler, kredi

yükleme işlemi, genel kontrol bağlantısı, ceza veya arıza durumu bildirim bağlantısı gibi sayaç ile sunucu arasındaki veri transferini belirler. Veri transferinde esnek bir mesaj yapısı kullanılmıştır. Bu yapıya eklemeler çok kolay bir şekilde yapılabilir. İki mesaj yapısı tanımlanmıştır. Birincisi sunucudan sayaca, diğeri sayaçtan sunucuya. İkisi arasındaki tek fark, sayaçtan sunucuya gönderilen mesajların başında sayaç seri numarası olmasıdır. Sunucudan sayaca giden mesajlarda buna gerek yoktur. Çünkü mesajın geldiği yer belirlidir. Parametreler mesajdan mesaja farklılık göstermektedir. Mesajlar String tipinde olup sonlandırıcı karakter olarak '\0' (ascii sıfır) kullanırlar. Parametreler string'de olabilir, sayıda olabilir.

Tablo 4.5. Sayaçtan sunucuya gelen mesaj formatı

Sayaç seri no	Mesaj	Parametre 1	Parametre 2	.....

Tablo 4.6. Sunucudan sayaca gelen mesaj formatı

Mesaj	Parametre1	Parametre2	.....

Sayaç sunucu programına iki durumdan dolayı bağlanır.

- Genel kontrol bağlantısı
- Ceza veya arıza gibi özel durum bağlantısı

Genel kontrol bağlantısı: Bu bağlantıda sayaçta her hangi normal olmayan bir durum söz konusu değildir. Sayaç sunucuya belirli aralıklarla bağlanır. Bu bağlantıda sunucu gerekli verileri sayaca gönderir veya okuması gereken verileri sayaçtan alır. Genel kontrol bağlantısındaki komutlar, kredi yükleme, endeks okumadır. Her işlemin ardında gönderilen sonuç mesajı vardır. Bu mesajlar "TAMAM" ile "HATA" mesajlarıdır. Bağlantıyı her zaman sunucu tarafı keser. Sunucu bağlantıyı kesmeden önce sayaca "SON" mesajını yollar. Sayaç bu mesajı aldığında bağlantıyı keser. Sayaç her sunucuya bağlandığında ilk önce bağlantı sebebini yollar. Bu mesajlar genel kontrol durumu için "KONTROL", ceza ve arıza gibi mesajlar için ise "ACIL" mesajıdır.

Kredi yükleme mesajı: Sunucudan sayaca gider. Sayaca kredi yüklemek işlemini yerine getiren mesajdır.

"KREDI"yüklenecek_kredi_miktarı

Örnek,

Gelen Mesaj : 2345"KONTROL"

Gönderilen Mesaj : "KREDI"123

Gelen Mesaj : 12346"TAMAM"

Gönderilen Mesaj : "SON"

Endeks gönder mesajı: Sucudan sayaca giden bir mesajdır. Sayaç bu mesajı aldığında endeks değerini sunucuya gönderir.

"ENDEKS"

Örnek,

Gelen Mesaj : 2345"KONTROL"

Gönderilen Mesaj : "ENDEKS"

Gelen Mesaj : 23456"ENDEKS"2345

Gönderilen Mesaj : "TAMAM"

Gönderilen Mesaj : "SON"

Ceza durumu mesajı: Sayaçtan sunucu programa gönderilen mesajdır. Sayaca müdahale durumunda sayaç tarafından sunucu programa gönderilir.

2345"CEZA"ceza_sebebi

Örnek,

Gelen Mesaj : 2345"ACIL"

Gelen Mesaj : 2345"CEZA"2

Gönderilen Mesaj : "TAMAM"

Gönderilen Mesaj : "SON"

Arıza durumu mesajı : sayaçtan sunucu programına gönderilen mesajdır. Sayaçta oluşan arızayı bildirir.

4567"ARIZA"arıza_sebebi

Örnek,

Gelen Mesaj : 2345"ACIL"

Gelen Mesaj : 2345"ARIZA"3

Gönderilen Mesaj : "TAMAM"

Gönderilen Mesaj : "SON"

BÖLÜM 5. GÜVENLİK VE DES

5.1 DES Algoritması

Verilerin yabancı kişiler veya sistemler tarafından okunmasını engellemek amacı ile DES(Data Encryption Standard) kriptolama algoritması kullanılmıştır. Bu algoritma 64 bitlik şifreleme işlemi yapmaktadır. DES algoritması 64 bit uzunluğunda bir mesajı yine 64 bit uzunluğundaki bir şifrele ile şifrelemektedir. Bu algoritma her byte'ın işaret biti olan 8. bitini kullanmamaktadır. Bundan dolayı gerçek şifreleme anahtarı 56 bite inmektedir. Şifreleme işlemi bit düzeyinde yapılmaktadır[8].

Örneğin "8787878787878787" şeklindeki veriyi, "0E329232EA6D0D73" anahtar verisi ile şifrelediğimizde, şifrelenmiş veri "0000000000000000" olmaktadır. Aynı anahtar kelime ile şifreleme işlemini tersine aldığımızda "8787878787878787" bilgisini elde ederiz[8].

DES algoritması 64 bit ve 64 bitin katı olan verileri şifrelemektedir. Ama çoğu veri 64 bitin katı olmayacaktır. Veri 64 bitin katı değilse veriyi 64 bitin katına genişletecek kadar sonuna 0 eklenir. Bu ekleme işleminden sonra veri 64 bitlik anahtar ile şifrelenir[9].

5.2 DES Çalışma Şekli

DES algoritması bloklar üzerinde işlem yapan bir algoritmadır. DES algoritması 8 byte uzunluğundaki veriyi alır şifreler ve tekrar 8 byte uzunluğunda veri oluşturur.

DES algoritması 64 bitlik veriyi iki adet 32 bitlik veri şeklinde böler. Sağ blok (R) ve sol Blok(L).

Örneğin M mesajı söyle olsun:

M = 0123456789ABCDEF , M hex formatında bir veri. M mesajını ikili sistemde yeniden yazdığımızda,

M = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111

elde ederiz.

Bu mesajı sağ ve sol olarak ikiye ayıralım

L = 0000 0001 0010 0011 0100 0101 0110 0111

R = 1000 1001 1010 1011 1100 1101 1110 1111

M mesajının ilk biti '0' en son biti ise '1' dir. Buradaki sıralama soldan sağa şeklindedir.

DES algoritması 64 bitlik veriyi 56 bitlik anahtar ile şifreler. Aslında anahtar kelime 64 bit uzunluğundadır fakat anahtar şifrede 8'in katı olan bitler kullanılmamaktadır (8, 16, 24, 32, 40, 48, 56 ve 64). Bu 8 tane bit alt anahtarlar oluşturulurken yok olmaktadır.

5.2.1 Alt anahtar oluşturma

Örnek olarak aşağıdaki anahtar kelime kullanılacaktır.

K = 133457799BBCDFF1

K = 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001

DES algoritması her biri 48 bit uzunluğunda 16 tane alt anahtar oluşturur. 64 bit uzunluğundaki anahtar kelime Tablo 1 de (PC-1) gösterilen tablo ile işleme tabi tutulur. Bu işlemden sonra 56 bitlik K+ anahtar oluşturulur.

Tablo 5.1. PC-1 tablosu

57	49	41	33	25	17	9
1	58	50	42	34	26	18

10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Tablonun ilk elemanı olan 57, anahtar kelimedeki 57. bit anlamına gelmektedir. Tabloda bulunan her bir değerin karşılığı olan bit yazılır ve tablo soldan sağa, yukarıdan aşağıya dizilir ve 56 bitlik K+ elde edilir.

K = 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001

K+ = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

Elde ettiğimiz K+ anahtarını da iki eşit parçaya ayrılır. Bu parçalar C_0 ve D_0 ile isimlendirilir.

$\mathbf{C_0}$ = 1111000 0110011 0010101 0101111

$\mathbf{D_0}$ = 0101010 1011001 1001111 0001111

Bu değerlerden 16 tane C_n ve D_n elde edilir ($1 \leq n \leq 16$). Her bir C_n ve D_n, C_{n-1} ve D_{n-1} den elde edilir. Bu işlem Tablo2 de verilen her bir iterasyona karşılık gelen sola döndürme işlemi ile yapılır.

Tablo 5.2 İterasyon tablosu

İterasyon sayısı	Öteleme Sayısı
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1

10	2
11	2
12	2
13	2
14	2
15	2
16	1

Örneğin C_3 ve D_3 , C_2 ve D_2 nin iki bit sola döndürülmesi ile elde edilir.

$\mathbf{C_0}$ = 11110000110011001010101111

$\mathbf{D_0}$ = 01010101011001100111100011111

$\mathbf{C_1}$ = 11100001100110010101011111

$\mathbf{D_1}$ = 10101010110011001111000111110

$\mathbf{C_2}$ = 11000011001100101010111111

$\mathbf{D_2}$ = 01010101100110011110001111101

$\mathbf{C_3}$ = 00001100110010101011111111111

$\mathbf{D_3}$ = 01010110011001111000111110101

$\mathbf{C_4}$ = 00110011001010101011111111100

$\mathbf{D_4}$ = 01011001100111100011110101010

$\mathbf{C_5}$ = 11001100101010101111111110000

$\mathbf{D_5}$ = 01100110011110001111010101010

$\mathbf{C_6}$ = 00110010101010111111111000011

$\mathbf{D_6}$ = 10011001111000111101010101010

$\mathbf{C_7}$ = 11001010101011111111100001100

$\mathbf{D_7}$ = 01100111100011110101010110

$\mathbf{C_8}$ = 00101010101111111110000110011

$\mathbf{D_8}$ = 10011110001111010101011001

$\mathbf{C_9}$ = 01010101011111111100001100110

$\mathbf{D_9}$ = 00111100011110101010110011

$\mathbf{C_{10}}$ = 01010101111111110000110011001

$\mathbf{D_{10}}$ = 11110001111010101011001100

$\mathbf{C_{11}}$ = 010101111111100001100110 0101

$\mathbf{D_{11}}$ = 110001111010101010110011 0011

$\mathbf{C_{12}}$ = 010111111110000110011001 0101

$\mathbf{D_{12}}$ = 000111101010101011001100 1111

$\mathbf{C_{13}}$ = 011111111000011001100101 0101

$\mathbf{D_{13}}$ = 011110101010110011001111 00

$\mathbf{C_{14}}$ = 111111100001100110010101 0101

$\mathbf{D_{14}}$ = 111010101010110011001111 0001

$\mathbf{C_{15}}$ = 111110000110011001010101 0111

$\mathbf{D_{15}}$ = 101010101011001100111100 0111

$\mathbf{C_{16}}$ = 111100001100110010101010 1111

$\mathbf{D_{16}}$ = 010101010110011001111000 1111

Elde edilen bu 16 C_nD_n çifti Tablo 3 de gösterilen tablo ile işleme tabi tutulur ve 48 bit uzunluğunda 16 tane alt anahtar elde edilir. Normalde elde edilen C_nD_n çiftleri 56 bit uzunluğundadır. Tablo işleminden sonra bunlar 48 bite inmektedir.

Tablo 5.3. PC –2 tablosu

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Tablo işleminden sonra elde edilen 16 anahtar.

$\mathbf{K_1}$ = 000110 110000 001011 101111 111111 000111 000001 110010

$\mathbf{K_2}$ = 011110 011010 111011 011001 110110 111100 100111 100101

$\mathbf{K_3}$ = 010101 011111 110010 001010 010000 101100 111110 011001

$\mathbf{K_4}$ = 011100 101010 110111 010110 110110 110011 010100 011101

$\mathbf{K_5}$ = 011111 001110 110000 000111 111010 110101 001110 101000

$\mathbf{K_6}$ = 011000 111010 010100 111110 010100 000111 101100 101111

$\mathbf{K_7}$ = 111011 001000 010010 110111 111101 100001 100010 111100

$\mathbf{K_8}$ = 111101 111000 101000 111010 110000 010011 101111 111011

$\mathbf{K_9}$ = 111000 001101 101111 101011 111011 011110 011110 000001

$\mathbf{K_{10}}$ = 101100 011111 001101 000111 101110 100100 011001 001111

$\mathbf{K_{11}}$ = 001000 010101 111111 010011 110111 101101 001110 000110

$\mathbf{K_{12}}$ = 011101 010111 000111 110101 100101 000110 011111 101001

$\mathbf{K_{13}}$ = 100101 111100 010111 010001 111110 101011 101001 000001

$\mathbf{K_{14}}$ = 010111 110100 001110 110111 111100 101110 011100 111010

$\mathbf{K_{15}}$ = 101111 111001 000110 001101 001111 010011 111100 001010

$\mathbf{K_{16}}$ = 110010 110011 110110 001011 000011 100001 011111 110101

5.3. 64 Bitlik Verinin Şifrelenmesi

M mesajı şifrelenmeden önce IP tablosu ile yeniden sıralanır. Sıralamadan sonra 58. bit ilk bit olur, 7. bit ise en sonuncu bit olur.

Tablo 5.4. IP tablosu

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

M mesajı yeniden sıralanmış hali:

M = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111

IP = 1100 1100 0000 0000 1100 1100 1111 1111 1111 0000 1010 1010 1111 0000 1010 1010

Tablo işleminden sonra mesajdan elde edilen IP 32 bitlik iki parçaya ayrılır, bunlar L_0, R_0.

$\mathbf{L_0}$ = 1100 1100 0000 0000 1100 1100 1111 1111

$\mathbf{R_0}$ = 1111 0000 1010 1010 1111 0000 1010 1010

For i = 1 to 16

Begin

$L_n = R_{n-1}$

$R_n = L_{n-1}$ XOR $f(R_{n-1}, K_n)$

End

Yukarıdaki döngü sonunda yukarıdaki işlem sonuncunda $L_{16}R_{16}$ elde edilir. Örneğin,

K_1 = 000110 110000 001011 101111 111111 000111 000001 110010

$L_1 = R_0$ = 1111 0000 1010 1010 1111 0000 1010 1010

$R_1 = L_0 + f(R_0,K_1)$

Buradaki f fonksiyonu 32 ve 48 bit uzunluğunda iki tane parametre almaktadır. F fonksiyonu hesaplama yapmak için her bir R_{n-1} değerini 32 bitten 48 bite çıkarır. Bu işlemi yaparken seçim tablosunu kullanır. Bu tablada bazı R_{n-1} değerleri iki defa kullanılmıştır. Seçim tablosu E fonksiyonu ile ifade edilir. $E(R_{n-1})$ fonksiyonu 32 bit veri alır ve 48 bit veri geri döndürür.

Tablo 5.5. E fonksiyonu bit seçim tablosu

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Örneğin R_0 değerinin E fonksiyonundan sonraki değeri,

R_0 = 1111 0000 1010 1010 1111 0000 1010 1010

$E(R_0)$ = 011110 100001 010101 010101 011110 100001 010101 010101

K_n XOR $E(R_{n-1})$

K_1 = 000110 110000 001011 101111 111111 000111 000001 110010

$E(R_0)$ = 011110 100001 010101 010101 011110 100001 010101 010101

K_1 XOR $E(R_0)$ = 011000 010001 011110 111010 100001 100110 010100 100111.

Bu noktaya kadar, R_{n-1} E seçim tablosu kullanılarak 32 bitten 48 bite genişletildi ve K_n değeri ile XOR işlemine tabi tutuldu. Şu an 48 bit uzunluğunda yani 8 tane 6 bitlik veri mevcut. Bu her bir 6 biti farklı bir işleme tabi tutulacak. Bu işlemin adı S kutuları(S Boxes). Her bir 6 bit farklı bir S kutusunun adresini verir. Her bir 6 bitin gösterdiği adreste 4 bit vardır. Bu 4 bit orijinal 6 bit ile yer değiştirir.

Önceki sonuc çöyle yazılır,

$K_n + E(R_{n-1}) = B_1B_2B_3B_4B_5B_6B_7B_8$, buradaki her bir B değeri 6 bit uzunluğundadır. $S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$ değeri hesaplanır. Toplam 8 tane ayrı S tablosu vardır.

Tablo 5.6. S kutusu 1

	Sütun No															
Satır No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

$S_1(B)$ işlemi şu şekilde yapılır:

B nin ilk ve son iki alınarak 0 ile 3 aralığında 2 bitlik bir sayı elde edilir. Bu sayı satır numarasıdır. Ortadaki 4 bitten de 0-15 arası sayı elde edilir. Bu sayıda sütun numarasıdır. S tablosundan bu satır ve sütun numaraları kullanılarak 4 bitlik sayı elde edilir. Örneğin, B = 011011, budan ilk ve son bitler 01'dir. Bu sayıda 1. satır manasına gelir. ortadaki 4 bit 1101'dir. Bu sayıda 13. sütunu gösterir. 1.satır 13.sütundaki değer 5'dir. $S_1(011011) = 0101$ elde edilir. S tabloları aşağıda verilmiştir

Tablo 5.7. S tabloları

S1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

Tablo 5.7. (Devam) S tabloları

S4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

Tablo 5.7. (Devam) S tabloları

S8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

İlk döngü sonucunda aşağıdakiler elde edilir.

$K_1 + E(R_0) = 011000\ 010001\ 011110\ 111010\ 100001\ 100110\ 010100\ 100111.$

$S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8) = 0101\ 1100\ 1000\ 0010\ 1011\ 0101\ 1001\ 0111$

F fonksiyonu:

$$\mathbf{f = P(S_1(B_1)S_2(B_2)...S_8(B_8))}$$

P permutasyon tablosu Tablo 8 de verilmiştir. Bu tablo 32 bit giriş alır ve 32 bit çıkış verir.

Tablo 5.8. P permutasyon tablosu

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Örnek,

$S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$ = 0101 1100 1000 0010 1011 0101 1001 0111

f = 0010 0011 0100 1010 1010 1001 1011 1011

$R_1 = L_0 + f(R_0 , K_1)$

= 1100 1100 0000 0000 1100 1100 1111 1111
+ 0010 0011 0100 1010 1010 1001 1011 1011
= 1110 1111 0100 1010 0110 0101 0100 0100

Bir sonraki adımda $L_2 = R_1$ olacak, $R_2 = L_1 + f(R_1, K_2)$ değeri hesaplanır. 16 iterasyon sonunda L_{16} ve R_{16} değeri hesaplanır. L_{16} ve R_{16} değeri yer değiştirerek $R_{16}L_{16}$ elde edilir. Bu elde edilen değer IP^{-1} permutasyon tablosuna göre tekrar sıralanır.

Tablo 5.9. IP^{-1} permutasyon tablosu

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

En son elde edilen değer,

L_{16} = 0100 0011 0100 0010 0011 0010 0011 0100

R_{16} = 0000 1010 0100 1100 1101 1001 1001 0101

Bu değerler ters çevrildiğinde,

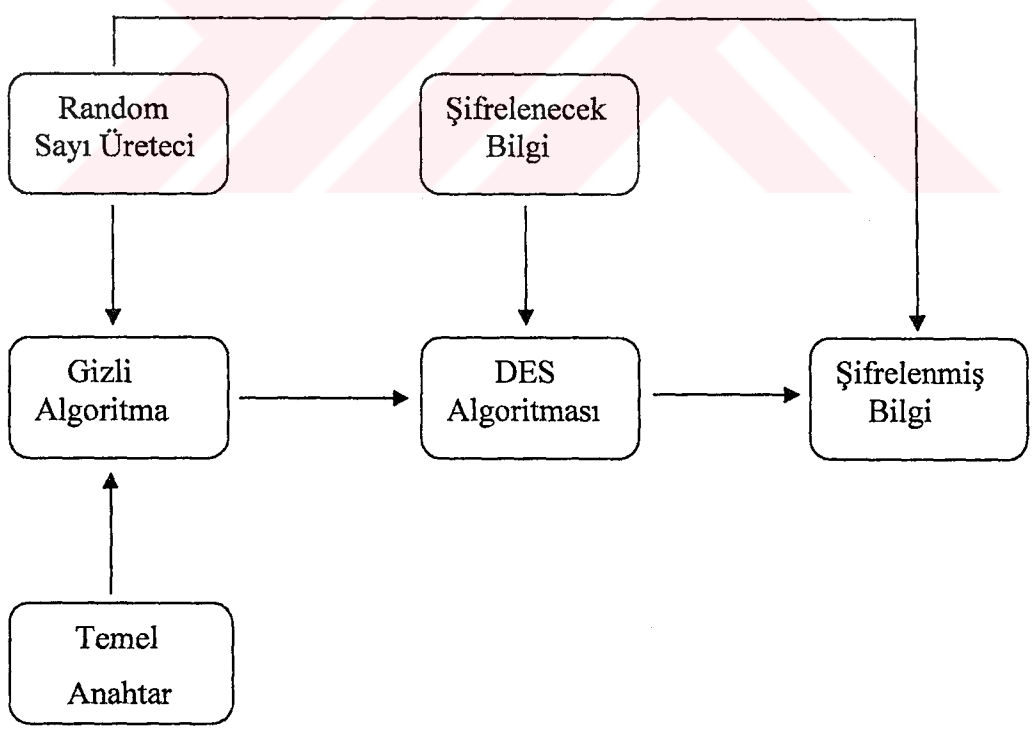
$R_{16}L_{16}$ = 00001010 01001100 11011001 10010101 01000011 01000010 00110010 00110100

IP^{-1} = 10000101 11101000 00010011 01010100 00001111 00001010 10110100 00000101

M = 0123456789ABCDEF mesajının **K** = 133457799BBCDFF1 anahtar ile şifrelenmesi sonuncunda **C** = 85E813540F0AB405 şifrelenmiş veri elde edilir.

5.4. DES 'in Uygulamada Kullanımı

DES algoritması bu işlem için yeterince güvenli bir algoritmadır. Ama yinede anahtar kelimenin bir şekilde öğrenilmesi durumunda hiçbir güvenliği kalmamaktadır. Bu durumu zorlaştırmak için anahtar kelimeyi her veri paketinde değiştirmek yeterli olacaktır. Normalde elimizde bir tane temel anahtar olacaktır. Her pakette değişen şifreler bu temel anahtardan elde edilir. Bu işlem için basit bir tane kapalı algoritma kullanılır. Kapalı algoritmadan kasıt algoritmanın gizli olmasıdır. Bu gizli algoritma, üretilen random şifre ile temel anahtarı kullanarak paket için özel anahtar oluşturur. Paket içerisinde, üretilen random sayıda gizlidir. Bu paketin tekrar çözülmesi için lazımdır.



Şekil 5.1. Şifreleme işlemi

BÖLÜM 6. SONUÇLAR VE ÖNERİLER

Bu çalışma sonunda, GPRS teknolojisi kullanılarak USO (uzaktan sayaç okuma) uygulaması ve bu uygulamaya ek olarak sunucu ve istemci programları geliştirilmiştir.

Bu uygulamadaki sunucu ve istemci programlarının saha uygulamaları için geliştirilmeleri gerekmektedir. Bu programları sahada kullanmak için öncelikle güçlü bir veri tabanı sunucusu gerekmektedir. Bu veri tabanı sunucusuna istemci programları güvenli hatlardan erişebilmesi gerekmektedir. Bu şekilde veri tabanı sunucusu ile istemci programları ayrı yerlerde olabilirler.

Şu anki GPRS modül fiyatları yüksek olduğu için her sayaca bir adet GPRS modül takmak yerine evlerde veya iş yerlerinde kullanılan su, elektrik ve doğal gaz sayaçlarını RF modüller veya RS485 bağlantısı ile birbirlerine bağlayarak maliyette düşüş sağlanabilir. Aynı şekilde apartmandaki tüm sayaçları RF veya RS485 hattı ile GPRS modül bağlantısını kurup oradan veri iletimi sağlanabilir.

Bu çalışma GPRS ile USO sistemleri geliştirilmesinde bir referans olmaktadır. GPRS ile USO Türkiye şartlarında uygulanabilecek bir USO sistemidir. İkinci bir alternatif olan PLC ile USO sitemini Türkiye şartlarında uygulamak ve hayata geçirmek için bir takım zorluklar bulunmaktadır. Bu zorlukların başında güç hatlarındaki problemler gelmektedir. Bu problemler güç hatlarının eski olması ve bu hatların havada olmasıdır. Hatların dışarıda olması hatlarda daha fazla gürültü oluşmasına sebep olur. Güç hatlarındaki gürültüler PLC haberleşmesini olumsuz yönde etkilemektedir.

Dünya, her elektronik aygıtın birbirleriyle haberleştiği bir otomasyon sistemine doğru gitmektedir. Bunların başında ev otomasyonları gelmektedir. Bu ev

otomasyonuna sayaçlarda dahil edilebilir. Sayaçların böyle bir sisteme dahil edilebilmesini sağlayacak sistemler USO sistemleridir. USO sistemleri bu otomasyonun başlangıç seviyesidir. Bu sistemler sayesinde belki ilerde, kredisi biten sayaç otomatik olarak kendine kullanıcının banka hesap numarasını kullanarak kredi satın alabilecektir veya kredisi azaldığında SMS veya mail ile kullanıcıya bildirecektir.

Bu çalışmadaki GPRS modül uygulaması referans alınarak farklı uygulamalar gerçekleştirilebilir.

KAYNAKLAR

[1] Regis J. Bates , GPRS: General Packet Radio Service, McGraw-Hill Professional

[2] Gunnar Heine, GPRS from A-Z, Artech House

[3] Alan Kavanagh, John Beckmeyer , GPRS Networks, Osborne Publishing

[4] Heinrich- Karl Potszeck, Springer-Verlag; 4th rev. ed edition

[5] Dan Ziegler, Home automation: Applying power line carrier technology, Purdue University Calumet

[6] Donald L. Schleger, Frank, Iii Gradilone, Automatic Meter Reading for the Water Industry United Water Resources, Amer Water Works Assn

[7] Alan Rothschild, Automatic remote meter reading: putting your water meter on-line, Hagedorn Publication; ISBN: B00098BQMY

[8] Douglas R. Stinson, Cryptography: Theory and Practice, CRC Press, Boca Raton, 1995

[9] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997

[10] Dorthy Elizabeth Robling Denning, Cryptography and Data Security, Addison-Wesley Publishing Company, Reading, Massachusetts, 1982

[11] Data Encryption Standard, Federal Information Processing Standard (FIPS) Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington D.C. (January 1977).

EKLER

Tez çalışmasında hazırlanan programların tüm kaynak kodları ve çalıştırılabilir dosyaları, CD ortamında ek olarak verilmiştir. Programlar Borland C++ Builder 6 programlama dili kullanılarak yazılmıştır. Ekte verilen programların çalıştırılabilir dosyaları, tüm bilgisayarlarda ek program veya modüllere ihtiyaç duymadan çalıştırılabilir.

ÖZGEÇMİŞ

Mehmet GÖÇER, 1978 yılında İslahiye'de doğdu. İlk öğrenimini İskenderun 50. Yıl İlköğretim Okulunda, orta öğrenimini İskenderun İmam-Hatip Lisesinde, lise öğrenimini İskenderun Endüstri Meslek Lisesi Bilgisayar Donanım Bölümünde tamamladı. 2002 yılında Sakarya Üniversitesi Bilgisayar Mühendisliği Bölümünden mezun olarak Bilgisayar Mühendisi ünvanını aldı.