İSTANBUL TEKNİK ÜNİVERSİTESİ

ELEKTRİK-ELEKTRONİK FAKÜLTESİ

MİKROİŞLEMCİLERİN BLUETOOTH ÜZERİNDEN GÜVENLİ HABERLEŞMESİNİN GERÇEKLENMESİ

BİTİRME ÖDEVİ

OĞULCAN BAL

040090404

Bölümü: Elektronik ve Haberleşme Mühendisliği Bölümü

Programı: Elektronik Mühendisliği

Danışmanı: Doç. Dr. Sıddıka Berna ÖRS YALÇIN

MAYIS 2015

ÖNSÖZ

Öncelikle üniversitedeki lisans dönemim boyunca verdikleri eğitimle beni her açıdan geliştiren tüm öğretim üyelerine ve özellikle bitirme projem süresince beni yönlendiren, önerileri ve bilgileriyle her zaman beni destekleyen saygıdeğer hocam Doç. Dr. Sıddıka Berna ÖRS YALÇIN'a sonsuz teşekkürlerimi sunmayı bir borç bilirim.

Üniversite hayatım boyunca, beni sportif bir takım ruhuyla disipline ederek daha iyi ve başarılı bir birey olmamı sağlayan itükış, fakülte ve üniversite futbol takımıma, aynı zamanda getirdiği sorumluluklar ve etkinlikler ile beni sosyal olarak geliştiren başta ESN ITU olmak üzere, yerel, ulusal ve uluslararası seviyedeki tüm ESN (Erasmus Student Network) üyelerine ve hayatımın iyi kötü tüm anlarında yanımda bulunan bütün arkadaşlarıma defalarca teşekkür ederim.

Son olarak, hayatım boyunca her zaman yanımda olan, beni maddi ve manevi olarak destekleyen, sevgiyle büyüterek bugünlere getiren başta annem ve babam olmak üzere tüm aileme minnet dolu teşekkürlerimi sunarım.

Mayıs 2015 Oğulcan BAL

İÇİNDEKİLER

KISALTMALAR

WLAN: Wireless Local Area Network

WMN: Wireless Mesh Network

TEA: Tiny Encryption Algorithm

ISM: Industrial Scientific Medical

AFH: Adaptive Frequency Hopping

BR: Basic Rate

LE: Low Energy

EDR: Enhanced Data Rate

AMP: Alternate MAC/PHY

RF: Radio Frequency

UART: Universal Asynchronous Receiver Transmitter

RISC: Reduced Instruction Set Computing

CCS: Code Composer Studio

LPM: Low Power Mode

SSH: Secure Shell

ASCII: American Standard Code for Information Interchange

DCO: Digitally Controlled Oscillator

SMCLK: Sub-Main Clock

USCI: Universal Serial Communication Interface

XOR: Exclusive Or

ŞEKİL LİSTESİ

MİKROİŞLEMCİLERİN BLUETOOTH ÜZERİNDEN GÜVENLİ HABERLEŞMESİNİN GERÇEKLENMESİ

ÖZET

Günümüz teknolojisinde Bluetooth ile kablosuz haberleşen cihazlar günlük hayatımızın önemli bir kısmını oluşturmaya başlamıştır. Teknolojinin ilerlemesiyle birlikte, bu tarz taşınabilir ve giyilebilir cihazların kullanımı da gittikçe yaygınlaşmaktadır. Bu noktada cihazların düşük güç tüketimi, hızlı ve güvenli bir şekilde haberleşmesi önem kazanmaktadır. Farklı çalışma modlarıyla farklı miktarda güç tüketimi sağlayan mikroişlemciler ile bu sistemlerin tasarlanması mümkündür. Bu mikroişlemciler kullanılarak Bluetooth üzerinden taşınan verilerdeki bilgilerin güvenliği için gönderilmeden, mikroişlemci üzerinde şifrelenmesi ve veri alındığında veri işlenmeden önce, yine mikroişlemci üzerinde şifresinin çözülmesi gerekmektedir.

Bu bitirme tezinde farklı Bluetooth teknolojileri araştırılarak çalışma yapıları incelenmiştir. Tasarlanan sistemin gerçeklenmesi sırasında kullanılacak cihazların ayrıntılarından ve bu cihazları kontrol etmek için kullanılacak programların çalışmasından bahsedilmiştir. Mikroişlemciler ve Bluetooth cihazları, Evrensel Eşzamansız Alıcı-Verici (Universal Asynchronous Receiver Transmitter – UART) üzerinden bilgisayara bağlanarak yapılandırılmıştır. Mikroişlemcilerin Bluetooth cihazları aracılığıyla haberleşmesi sırasında yapılacak şifreleme ve şifre çözme işlemleri için Küçük Şifreleme Algoritması (Tiny Encryption Algorithm - TEA) kullanılmıştır. Böylece hızlı ve güvenli bir haberleşme amaçlanmıştır.

TEA, MSP430G2553 mikroişlemcisi üzerinde C programlama dili kullanılarak gerçeklenmiştir. Mikroişlemciler arasındaki kablosuz haberleşme HC-05 ve HC-06 Bluetooth modülleri ile sağlanmıştır. Şifreleme ve şifre çözme yazılımlarının mikroişlemci üzerinde düzgün çalışıp çalışmadığı farklı veriler gönderilerek denenmiştir. Algoritma, mikroişlemcinin göndereceği veriyi şifrelemesi, aldığı verinin de şifresini çözmesi için ilgili işkesme rutinleri içinde tanımlanmıştır.

IMPLEMENTATION OF A SECURE BLUETOOTH COMMUNICATION ON MICROPROCESSORS

SUMMARY

Devices that are communicating wireless with Bluetooth have been an important part of our daily lives in present technology. These types of portable and wearable devices are becoming widespread with the improvements in technology. Low power consumption, fast and secure communication of these devices is becoming more important. It is possible to design such systems with microprocessors that consume different amount of power with different operational modes. The data that is going to be transmitted with microprocessors over Bluetooth has to be encrypted on the microprocessor before sending and decrypted before processing on the microprocessor for the security of the information.

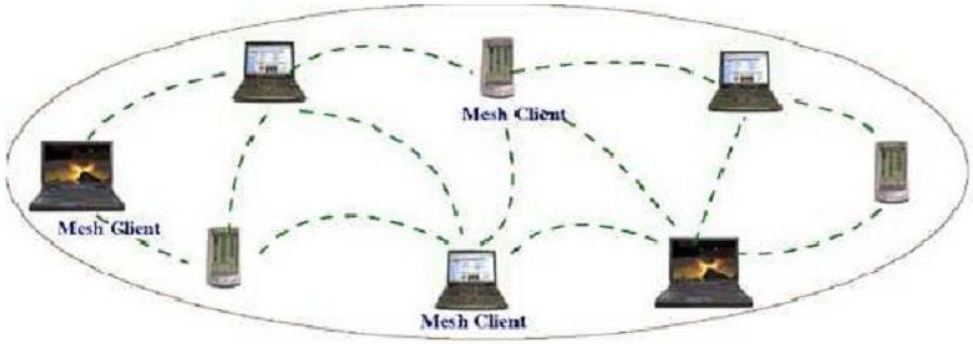
In this thesis, different Bluetooth technologies have been investigated and their operation configurations have been researched. Details of the devices and operation of the software programs that are going to be used during the implementation of the designed system have been mentioned. Microprocessors and Bluetooth devices have been configured by connecting them to the computer over Universal Asynchronous Receiver Transmitter. Tiny Encryption Algorithm has been used for the encryption and decryption processes during the communication of the microprocessors over Bluetooth. Thus, fast and secure communication is intended.

TEA has been implemented on MSP430G2553 microprocessor using the C programming language. Wireless communication between microprocessors is established with HC-05 and HC-06 Bluetooth modules. Different data combinations have been transmitted to check whether the encryption and decryption software on the microprocessor is functioning properly or not. Algorithm has been defined inside the corresponding interrupt routines for the microprocessor to encrypt the data which is supposed to be sent and decrypt the data which is received.

1. GİRİŞ

Kablosuz haberleşme teknolojilerinin gelişimiyle birlikte sayısal sistemlerde kullanımı artmış ve hayatımızın vazgeçilmez bir parçası olmuşlardır [1]. Bu bağlamda IEEE 802.11 haberleşme protokolü yıllardır geliştirilerek kullanılmaktadır. Telsiz Yerel Ağ (Wireless Local Area Network – WLAN) standardını temsil eden bu protokol kullanılırken cihazlar arası iletişimin daha hızlı olması için Telsiz Göz Ağ (Wireless Mesh Network – WMN) tipindeki birden çok atlama yapabilen ağlar kullanılmalıdır.

WMN ağlarının alıcılar ve yönelticiler olmak üzere iki farklı üyesi vardır [2]. Geleneksel yönelticilerin sahip olduğu tüm özelliklere sahip olan bu yönelticiler ekstra olarak birden çok kablosuz ara yüze sahiptir. Buna rağmen geleneksel yönelticilere karşı en büyük avantajları, birden çok atlamalı iletişim kullanarak çok daha düşük güç tüketimi sağlamalarıdır. WMN ağlarındaki alıcılar ise sadece tek bir kablosuz ara yüze sahip olduklarından ağ geçidi ve köprü oluşturma özellikleri yoktur. Bu nedenle alıcılar yönelticilere göre daha basit ve daha yaygın cihazlardır. Ancak alıcılar da yönelticiler gibi atlamalı iletişim özelliğine sahiptirler. Böylece Şekil 1.1'deki gibi sadece alıcılardan oluşan yöneltici içermeyen bir WMN oluşturmak mümkündür. Bu ağdaki iletişimde gerekli yapılandırma ve yönlendirme gibi işlevler ve son kullanıcılara iletim, alıcılar tarafından yapılabildiğinden yönelticilere ihtiyaç yoktur.



Şekil 1.1: Alıcı Telsiz Göz Ağı örneği [2].

Bu bitirme tezinde gerçeklenecek sistemin taşınabilir olması için minimum güç harcaması ve boyutunun uygun olması gerekmektedir. Aynı zamanda aktarılan

bilginin ve iletişimin hızlı olması gerekmektedir. Gerekli haberleşme mesafesinin uzaklığı da düşünülünce sistemin Bluetooth ile haberleşmesi tasarlanmıştır.

Kablosuz iletişim ağlarında bilgiler iletilirken bilginin gizliliği açısından güvenlik önlemleri alınması da şart olmuştur. Bu nedenle kablosuz iletişim kanallarında alınan ve gönderilen bilginin şifreli olması güvenlik açısından şarttır. Bunun için gönderilen bilginin şifrelendiği gibi alınan bilginin de aynı şekilde şifresinin çözülmesi gerekir. Bu şifreleme ve şifre çözme yapısı için, kullanım kolaylığı ve hızı düşünülerek Küçük Şifreleme Algoritması (Tiny Encryption Algorithm - TEA) kullanılmıştır [21]. Tüm bu donanımların oluşturduğu sistem ise MSP430 LaunchPad geliştirme aracı ve içindeki MSP430G2553 mikroişlemcisi ile kontrol edilmiştir.

Bitirme tezinin ikinci bölümünde Bluetooth ile kablosuz haberleşmenin nasıl yapıldığından bahsedilmiştir. Üçüncü bölümde ise sistemin tasarımı sırasında kullanılan cihazlar ve bu cihazları kontrol eden programların nasıl kullanıldığı anlatılmıştır. Sonrasında da bu donanım ve yazılımların hangi algoritmalarla nasıl gerçeklendiği açıklanmıştır.

2. BLUETOOTH İLE KABLOSUZ HABERLEŞME

Bluetooth teknolojisi 1994'te Ericsson tarafından RS-232 veri kablolarına kablosuz bir alternatif olarak yakın mesafeler için geliştirilmiş olup günümüzde çok geniş bir kullanım alanına sahiptir [9].

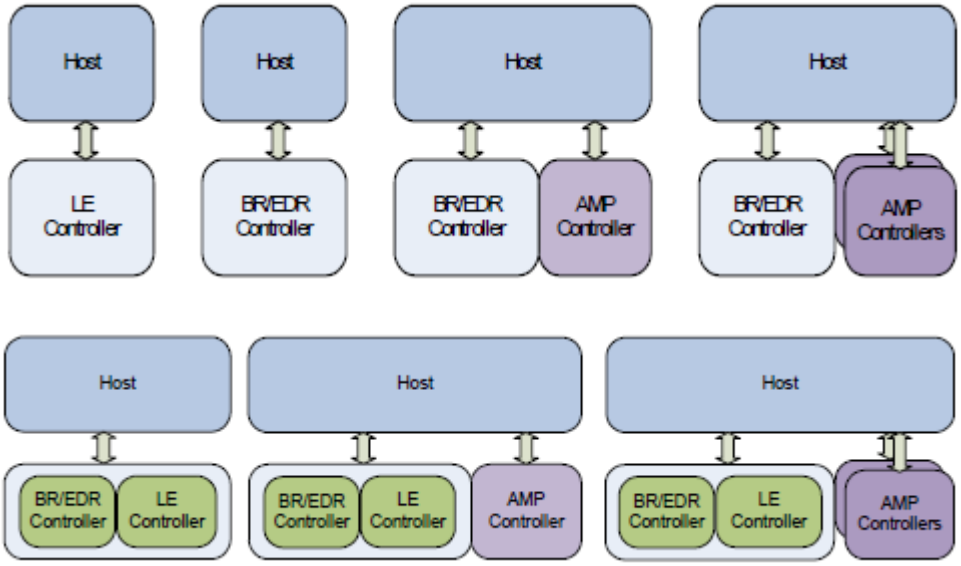
Bluetooth cihazları 2,4 GHz ile 2,485 GHz arasındaki Sınai, Bilimsel ve Tıbbi Cihaz (Industrial Scientific Medical – ISM) bandında çalıştığından tüm dünya çapında çoğu ülkede lisanssız olarak kullanılabilirler [5]. Aynı bandı kullanan çok sayıda cihaz olduğundan iletişim müdahaleye açıktır ancak bu durumu engellemek için cihazın kolayca frekans atlamasını sağlayan Uyarlanır Frekans (Sıklık) Hoplaması (Adaptive Frequency Hopping – AFH) özelliği geliştirilmiştir. Bu özelliğin temeli yakın çevrede kullanılan frekansları tespit ederek bu frekansları kullanmaktan kaçınmaktır. Frekans atlama özelliği ile uzaklık ve bozucu gibi problemler maksimum seviyede çözülerek aynı zamanda alıcı-verici için minimum fiyat sağlanmış olur. Tüm bunların yanı sıra Bluetooth çift yönlü iletişim sağlaması nedeniyle de avantajlıdır. Düşük enerji kullanımı ve ucuz olması da kullanıcıların daha çok tercih etmelerine sebep olmaktadır. Bu bitirme tezinde Bluetooth ile haberleşmenin kullanılmasının sebepleri de bunlardır.

Bluetooth kablosuz teknolojisinin tarihine genel olarak bakmak gerekirse; kısa mesafede kablosuz haberleşme sağlayan dünya çapında ve lisanssız bir standart üretmek için Ericsson, IBM, Intel, Nokia ve Toshiba firmaları tarafından, 1998 yılında Bluetooth Special Interest Group (SIG) kurulmuştur [6]. Bu teknolojinin herkes tarafından kabul edilmesi ve rahatça kullanılabilmesi için SIG bütün bilgi ağını halka açmaya karar vermiştir. 1999 yılında Bluetooth teknik özellikleri versiyon 1.0A çıkarıldıktan sonra 3Com, Lucent, Microsoft ve Motorola firmaları da eklenerek bu teknolojiyi geliştirmeye devam etmişlerdir. Günümüzde son versiyon olarak Bluetooth 4.2 çıkarılmış olup haberleşme hızı, haberleşme mesafesi ve harcanan güç miktarı gibi özellikleri yüksek oranda geliştirilmiştir.

Birçok elektronik aletin yanı sıra, akıllı evlerdeki donanımlarda kullanılan Bluetooth ile hastaların sağlık durumunu gösteren biyolojik sinyallerin takibi uzaktan kolaylıkla yapılabilir [3]. Daha da önemlisi riskli durumdaki hastalarda hayati tehlike önceden belirlenebilir.

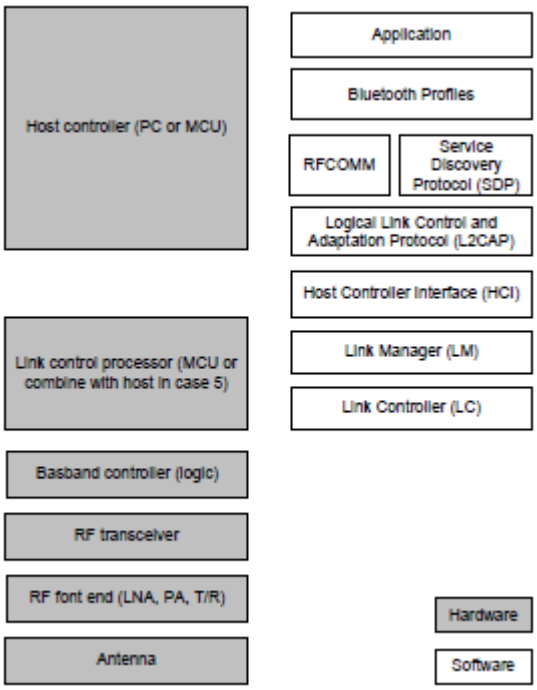
2.1. Bluetooth Cihazının Yapısı

Günümüz teknolojisinde Bluetooth cihazlarının Temel Hız (Basic Rate - BR) ve Düşük Enerji (Low Energy - LE) olmak üzere iki farklı formu vardır. Her iki sistem de cihaz bulma ve bağlantı oluşturma gibi temel özelliklere sahiptirler. Geliştirilmiş Veri Hızı (Enhanced Data Rate – EDR) özelliğine sahip BR sistemleri senkronize ve asenkronize olmak üzere Değişik MAC/PHY (Alternate MAC/PHY – AMP) özelliği ile birlikte 54 Mb/s hızına kadar çıkabilirler [8]. LE sistemleri ise daha düşük akım çeken, daha ucuz ve daha basit uygulamalar için geliştirilmiştir. Kullanım alanlarına göre biri diğerine göre daha uygun olabilir. Bir cihaz sadece BR veya sadece LE sistemine sahip olabileceği gibi her iki sisteme de aynı anda sahip olabilir. Bu durumda iletişim kanalları sadece cihazın aynı formda olup birbirini tanıyan sistemleri arasında gerçekleştirilebilir. Bluetooth cihazının çekirdek sistemini oluşturan ana işlemci ve kontrolör sistemlerinin çeşitli kombinasyonları Şekil 2.1'de görüldüğü gibi örneklenebilir.



Şekil 2.1: Bluetooth çekirdek yapısı [8].

Bir Bluetooth cihazının BR formunun donanımsal kısmı Şekil 2.2'de de görüldüğü gibi; ana kodları çalıştıran bir bilgisayar, basit kodları çalıştıran bir mikro kontrolör, alıcı-verici kısmını kontrol eden lojik bir blok, Yüksek Frekans (Radio Frequency – RF) alıcı-verici, band geçirici filtreyi içeren RF ucu ve antenden oluşmaktadır [4].



Şekil 2.2: Temel Hız formundaki Bluetooth cihazının yapısı [4].

Sadece iki cihaz arasındaki (point to point) iletişimin sağlanmasında basit bir seri bağlantı yeterli olurken birkaç cihaz arasında (point to multipoint) iletişimin sağlanması için cihazın üstünde gömülü olarak işletim sistemi içeren bir mikro işlemci bulunması gerekir [4].

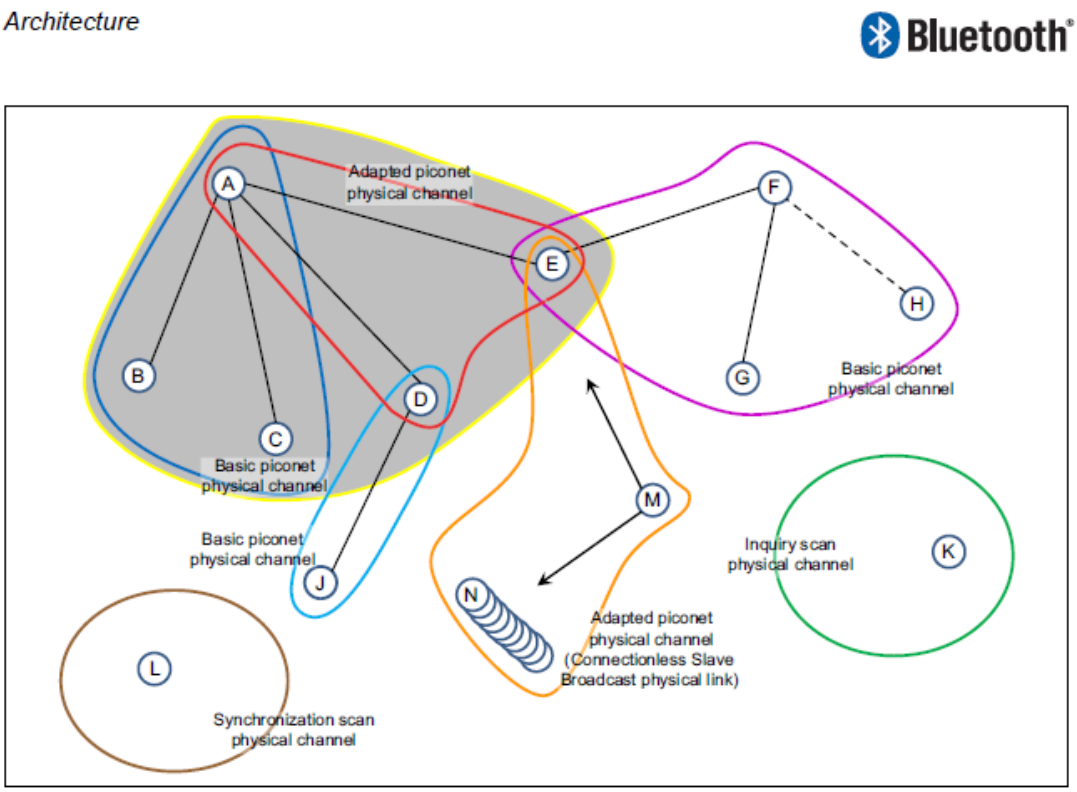
2.2. Bluetooth İletişim Topolojisi

Bu bölümde Bluetooth teknolojisinin farklı uygulamaları için geliştirilen BR ve LE sistemlerinin iletişim kanallarını nasıl oluşturduklarından ve nasıl veri alışverişi yaptıklarından bahsedilecektir.

2.2.1. Bluetooth Temel Hız Topolojisi

Bluetooth teknolojisini kullanan cihazlardan iki veya daha fazlası birbirleriyle iletişime geçtiklerinde oluşan ağa Piconet adı verilir [8]. Piconet içindeki tüm cihazlar aynı saat işareti ve frekans ile haberleşirler. Bir Piconet ağı en az bir ana cihaz ve en çok yedi bağımlı cihazdan oluşur [6]. Tüm Piconet ağının saat işareti ve frekans atlama düzeni ana cihazın saat işareti ve cihaz adresinden türetilerek belirlenir [8]. Bu ağa bağlanan diğer tüm cihazlar bağımlı cihaz olarak nitelendirilir. Yakın mesafe içinde birbirinden bağımsız farklı Piconet ağları bulunabilir ancak her ağın kendine özgü bir fiziksel iletişim kanalı vardır. Bu kanal her ağın ana cihazı

tarafından sahip oldukları farklı saat işareti ve frekans atlama düzeni ile oluşturulur. Bir Bluetooth cihazı bağımlı olarak birden çok ayrı Piconet ağında bulunabilir ancak ana cihaz olarak sadece bir Piconet ağını oluşturabilir. Birden çok Piconet ağına bağlı olan bağımlı cihazların oluşturduğu ağa da Scatternet adı verilir. Ancak aynı Scatternet ağı içindeki farklı Piconet ağlarını birbirinden ayırt edebilmek için bir ana cihaz sadece bir Piconet ağına ana cihaz olabilir [6]. BR sisteminde çalışan Bluetooth cihazlarının oluşturabileceği Piconet ağı örnekleri Şekil 2.3'te gösterilmiştir.



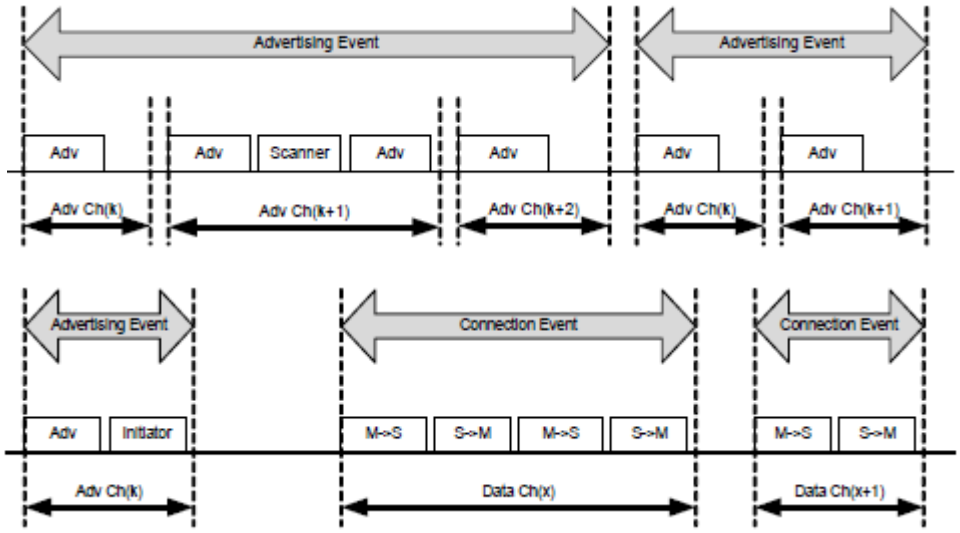
Şekil 2.3: Bluetooth Temel Hız topolojisi örneği [8].

Piconet içindeki her bir bağımlı cihazı tespit etmek için ana cihaz tarafından her birine aktif üye adresi atanır [6]. Bu adresler yerel olarak eşsizdir ve hangi cihazın ne zaman veri ileteceğini ana cihaz kontrol eder.

Ana cihaz tarafından belirlenen frekans atlama düzeni ISM bandı içindeki 79 frekansın 1er MHz atlanması şeklinde gerçekleşir. Başka cihazlar tarafından kullanılan frekanslardan kaçınılarak frekans atlama düzeni uyarlanabilir [8]. Fiziksel iletişim kanalı oluşturulduktan sonra çift yönlü veri transferi için ana ve bağımlı cihazlar arasında fiziksel bir bağlantı oluşturulur. Her ana cihaz ile bağımlı cihaz arasında bu bağlantı vardır ancak Piconet içerisindeki bağımlı cihazlar arasında hiçbir zaman fiziksel bir bağlantı yoktur.

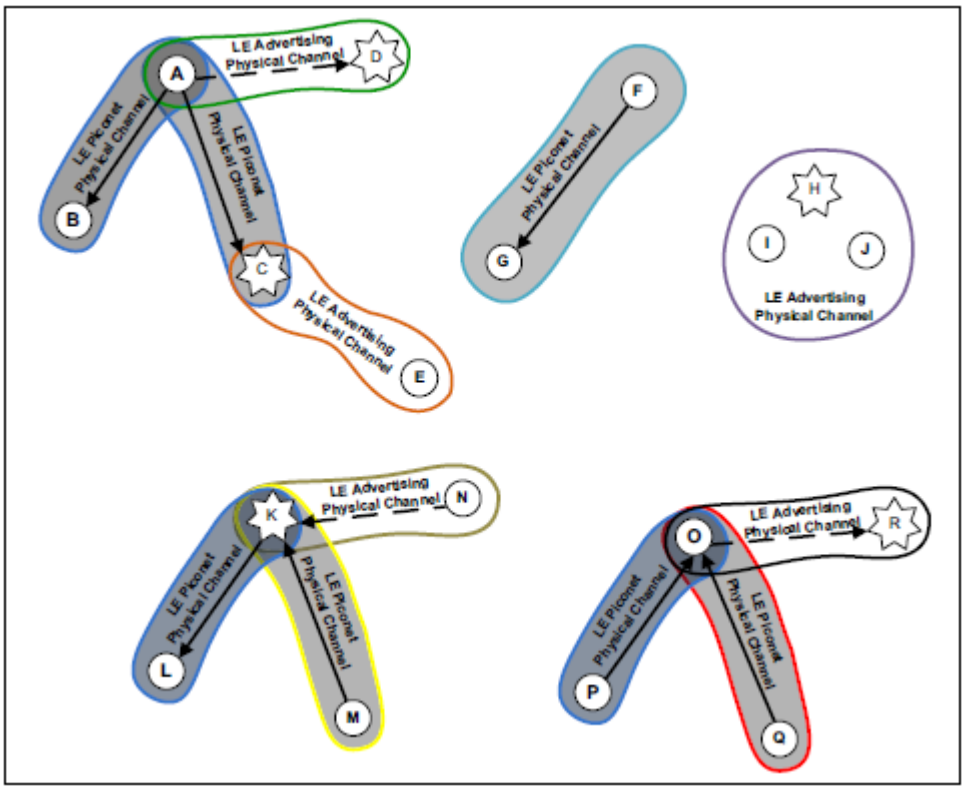
2.2.2. Bluetooth Düşük Enerji Topolojisi

Bluetooth LE sistemi de Bluetooth BR sistemi gibi ISM bandında çalışır [8]. Ancak bu sistemde farklı olarak 2 MHz aralıklarla oluşturulan 3 tanıtım kanalı ve 37 veri kanalı olmak üzere 40 adet fiziksel iletişim kanalı bulunur. Herhangi bir bağlantı oluşturulmadan önce ortamda tanıtım kanalı oluşturan tanıtıcılar, bağlanma amacı olmadan ortamdaki kanalları tarayan tarayıcılar ve bağlantı yapmak için ortamı dinleyen başlatıcılar bulunur. Bir başlatıcı tanıtıcıya bağlantı isteği yollar ve tanıtıcı da bunu kabul ederse bağlantı oluşturulmuş olur. Bu durumda başlatıcı oluşturulan Piconet ağının ana cihazı, tanıtıcı ise bağımlı cihazı haline gelir. Bu olaylar, tanıtım ve veri kanallarının değişimi Şekil 2.4'teki gibi gösterilmiştir.



Şekil 2.4: Bluetooth Düşük Enerji tanıtım ve bağlantı olayları [8].

Fiziksel iletişim kanalı oluşturulduktan sonra BR sisteminde olduğu gibi bağlantıyı ana cihaz kontrol eder. Bu kanal içindeki her bağımlı cihaz ile ana cihaz arasında farklı fiziksel bağlantılar oluşturulur. Bağımlı cihazların birbirleri arasında bağlantı oluşturması mümkün değildir. LE sisteminde çalışan Bluetooth cihazlarının oluşturabileceği Piconet ağı örnekleri Şekil 2.5'te gösterilmiştir.



Şekil 2.5: Bluetooth Düşük Enerji topolojisi örneği [8].

3. KULLANILAN CİHAZLAR VE PROGRAMLAR

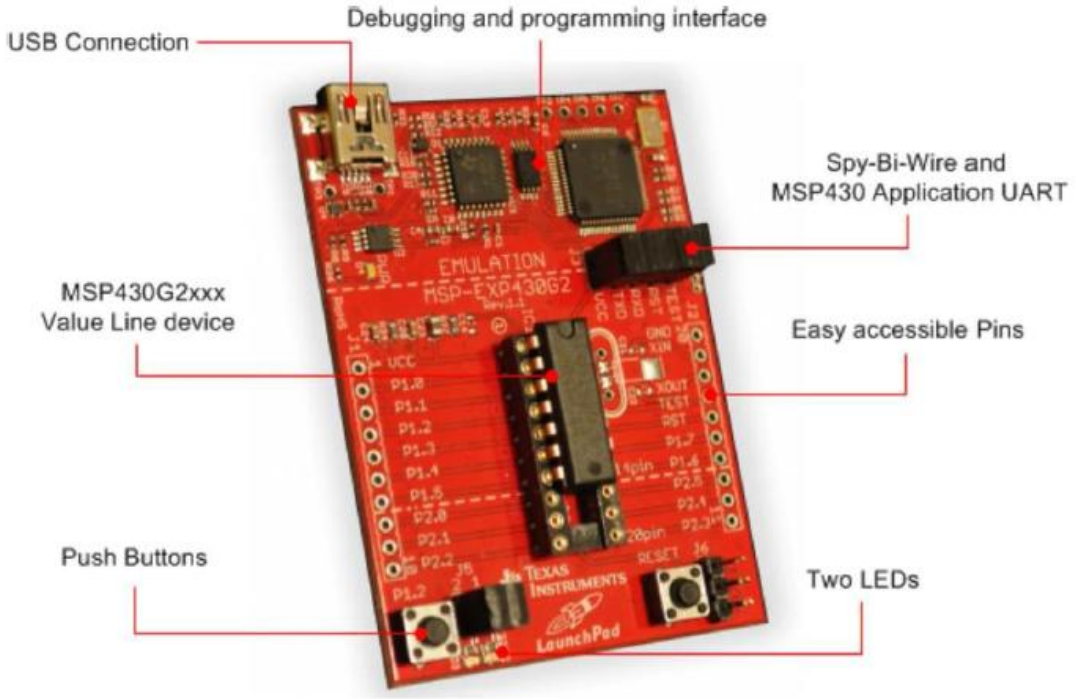
Bitirme tezinin bu kısmında tasarım sırasında kullanılan cihazların özelliklerinden ve bu cihazları kontrol eden programların nasıl çalıştıklarından bahsedilmiştir.

3.1. Kullanılan Cihazlar

Bu bitirme tezinde Bluetooth ile kablosuz haberleşen ve bu haberleşmeyi şifreli olarak gerçekleştiren iki taşınabilir cihazın tasarımı yapılmıştır. Bu tasarımda MSP430 Launchpad [10] geliştirme aracı üzerindeki MSP430G2553 mikroişlemcisi, HC05 ve HC06 Bluetooth modülleri kullanılmıştır.

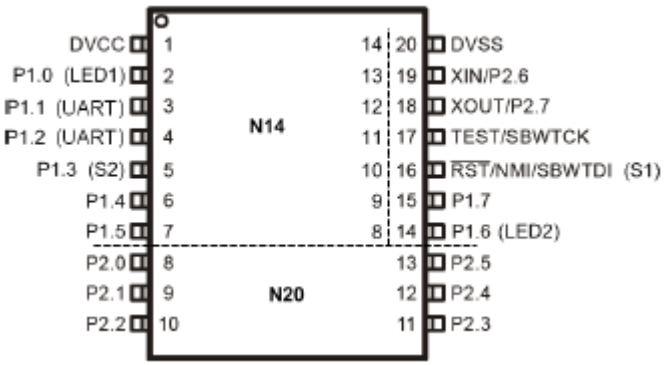
3.1.1. MSP430 Launchpad Geliştirme Aracı

Texas Instruments firmasının geliştirdiği MSP430 Launchpad, basit ve ucuz olmasının yanı sıra, üzerindeki butonlar, LED ışıklar, programlama ve hata ayıklama bölümleri ile kullanıcılarına MSP430G2xx serisi mikroişlemcileri kullanmalarında kolaylık sağlar [10]. USB üzerinden hata ayıklama ve programlama imkanı sunan cihaz Şekil 3.1'de gösterilmiştir.



Şekil 3.1: MSP430 Launchpad Geliştirme Aracı [10].

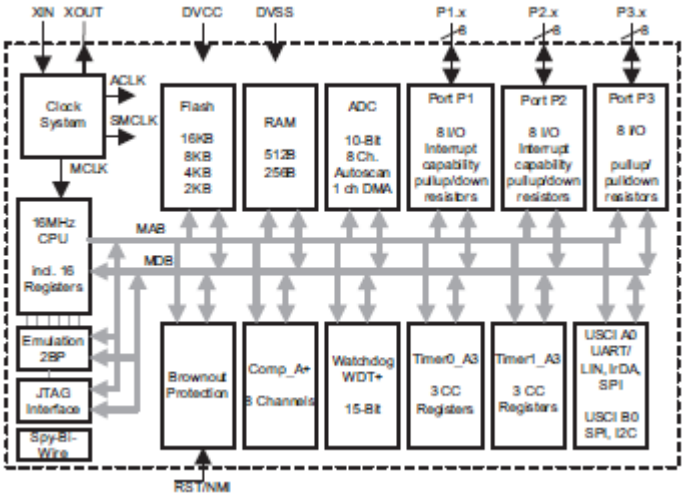
MSP430 ailesi, ücretsiz yazılım sağlaması, ucuz mikroişlemci ve düşük güç harcaması gibi sebeplerden proje geliştirmek için ideal bir cihazdır [7]. Birçok 16 bitlik MSP430 mikroişlemcisiyle uyumlu olan bu cihaz 9600 baud hızına kadar Evrensel Eşzamansız Alıcı-Verici (Universal Asynchronous Receiver Transmitter – UART) seri iletişim sağlar [10]. Hem 14 bacaklı hem de 20 bacaklı mikroişlemciler kullanılarak uygulama geliştirilebilir. Cihazın bacak dağılımı Şekil 3.2'de görüldüğü gibidir.



Şekil 3.2: MSP430 Launchpad bacak dağılımı [10].

3.1.1.1. MSP430G2553 Mikroişlemcisi

MSP430 Launchpad geliştirme aracı ile beraber gelen MSP430G2553 mikroişlemcisi 16 bitlik ve 20 bacaklı bir yapıda olup düşük besleme gerilimi aralığı ile beş farklı düşük güç tüketim modu içerir [12]. Bu modlar sayesinde uzun batarya ömrü amaçlanan taşınabilir uygulamalar için idealdir. Sahip olduğu 16 bitlik İndirgenmiş Komut Takımıyla Hesaplama (Reduced Instruction Set Computing – RISC) bilgisayarı, 16 bitlik saklayıcıları ve sabit katsayı üreticileri ile maksimum kod verimliliği sağlarlar. Mikroişlemcinin mimari yapısı Şekil 3.3'teki gibidir.

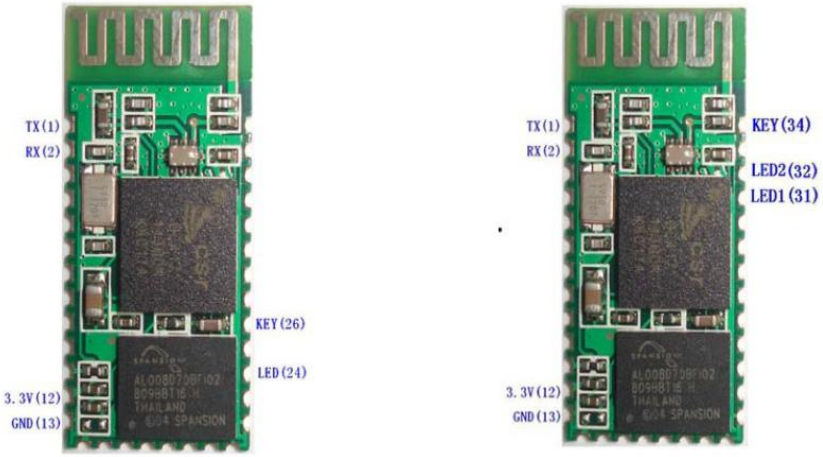


Şekil 3.3: MSP430G2553 Mimari Yapısı [12].

Cihaz içinde yerleşik olarak 16 bitlik sayıcılar, 24 genel amaçlı girdi çıktı bacağı, çok yönlü analog karşılaştırıcı ve 10 bitlik analog sayısal çevirici bulunur [12]. En sık kullanıldığı uygulamalar, ucuz algılayıcılarla analog sinyallerin yakalanıp sayısal değerlere çevrilerek, elde edilen verinin bir ekranda gösterilmesi veya başka bir sisteme gönderilmesi şeklindedir.

3.1.2. HC-05 ve HC-06 Bluetooth Modülleri

HC serisi Bluetooth modülleri Bluetooth seri haberleşme birimi ve Bluetooth uyarlayıcısından oluşur [13]. Çift rakamlarla adlandırılan cihazlar fabrikada ana veya bağımlı cihaz olarak tanımlanır ve sonradan değiştirilemez. Tek rakamlarla adlandırılan cihazlar ise ana veya bağımlı cihaz olarak AT komut modunda değiştirilebilir. İki cihazın birbiriyle haberleşebilmesi için Bluetooth modüllerinden birinin ana diğerinin bağımlı cihaz olması, şifrenin doğru olması ve seri bağlantı kapısı parametrelerinin aynı olması gerekir [14]. Bu Bluetooth modülleri için varsayılan bağlantı kapısı parametreleri; baud hızı 9600 bit/s, 1 durma biti ve eşlik biti yok olarak tanımlanmıştır. Şekil 3.4'te solda HC-06, sağda HC-05 olmak üzere Bluetooth cihazları ve kullanılan bacakları gösterilmiştir.



Şekil 3.4: HC-06 ve HC-05 Bluetooth Modülleri [13].

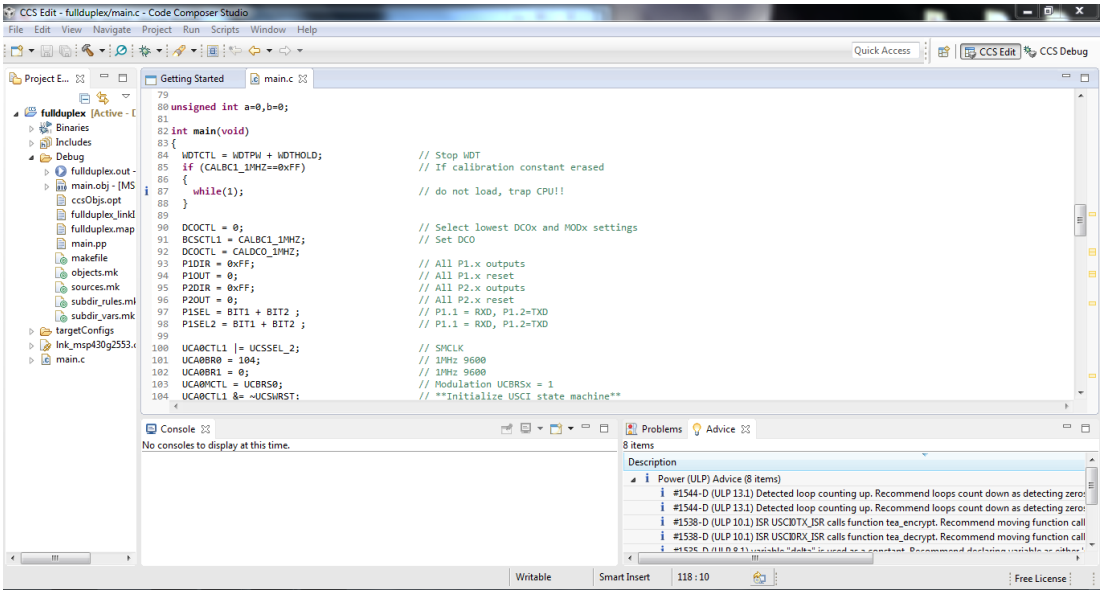
HC serisi Bluetooth modülleri üzerindeki LED ışıkların yanıp sönme frekansları ile hangi çalışma durumunda oldukları anlaşılabilir[13]. Her iki modülde de besleme gerilimi olarak sadece 3.3 (V) veya 5 (V) kullanılabilir.

3.2. Kullanılan Programlar

Bitirme tezinin bu kısmında tasarımdaki cihazları programlamak, kontrol etmek ve görüntülemek için kullanılan programlardan bahsedilecektir.

3.2.1. Kod Tertipleyen Stüdyo(CCS) Programı

MSP430G2553 mikroişlemcisi programlanırken, Texas Instruments firmasının kendi ürünleri için geliştirdiği Kod Tertipleyen Stüdyo (Code Composer Studio - CCS) Programı kullanılmıştır [15]. Bu program ile MSP430 mikroişlemcilerinde program geliştirme, hata ayıklama ve enerji tüketimini görüntüleme gibi işlemler yapılabilir. Kolay ve anlaşılır ara yüzü kullanıcılara büyük kolaylık sağlamaktadır. Programlama yapıldıktan sonra cihaza yüklemeden önce yapılan hatalar, yazılımla ilgili uyarılar ve öneriler ayrı ayrı gösterilerek kullanıcının mikroişlemciyi en verimli şekilde kullanması sağlanmıştır. Programın bilgisayar ekranındaki görüntüsü Şekil 3.5'teki gibi gösterilmiştir.



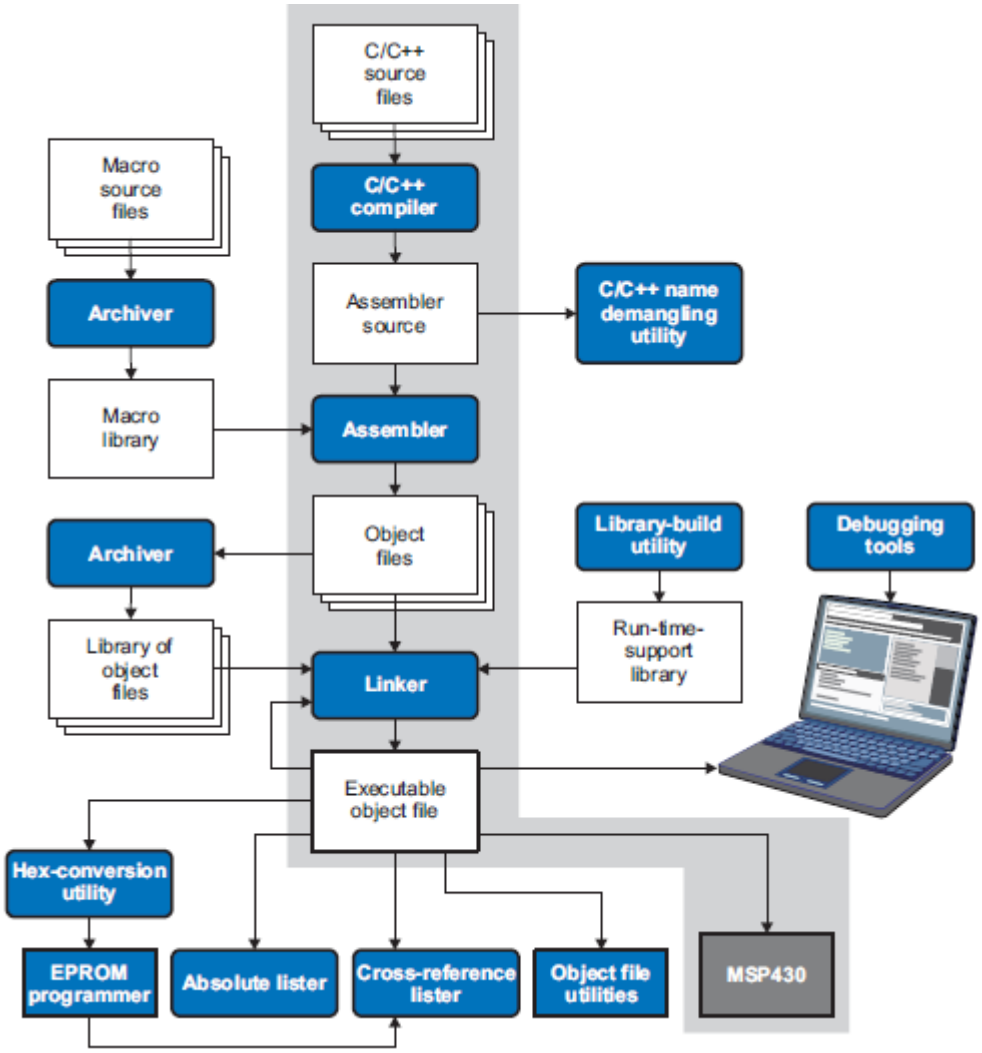
Şekil 3.5: CCS Programının Görüntüsü.

MSP430 projelerinde genel olarak yapılan hatalardan biri güvenlik zamanlayıcısını etkisiz hale getirmemektir [15]. Güvenlik zamanlayıcısı varsayılan olarak aktif haldedir. Etkisiz hale getirilmediği takdirde cihazı ilk duruma getirir, kaynak kodu ekranı beyaz hale gelir ve hata ayıklayıcı sorunu bulamaz. Hata ayıklayıcı CCS programının bir parçasıdır ve bağımsız bir uygulama olarak kullanılabilir. Aynı zamanda işkesme ve Düşük Güç Kullanımı Modu (Low Power Mode – LPM) uygulamalarında da kullanılabilir. Cihaz çalışırken hata ayıklayıcının cihaz

saklayıcılarına ve hafızaya erişmesi mümkün değildir. Bunun için cihazın durdurulması gerekir.

3.2.1.1. C Programlama Dili

CCS Programı hem çevirici (assembly) dilinde hem de C programlama dilinde programlama olanağı sunmaktadır. Ancak hem kolaylığı hem de daha modern olması açısından bu bitirme tezinde C programlama dili tercih edilmiştir. CCS içinde bulunan derleyici C kodunu derleyerek çeviriciye gönderir [16]. Çevirici tarafından makine koduna çevrilen yazılım bağ düzenleyicisi aracılığıyla MSP430 üzerine yüklenir. CCS programı içindeki derleyici araçları, yürütme hızını arttırmak, C kodunun boyutunu azaltıp basitleştirmek, komutları ve deyimleri yeniden düzenlemek ve değişkenleri saklayıcılara atamak gibi işlemleri gerçekleştirerek mikroişlemciye yüklenecek yazılımın en iyi duruma gelmesini sağlarlar. Bu yazılım geliştirme akışı Şekil 3.6'daki gibi gösterilmiştir.

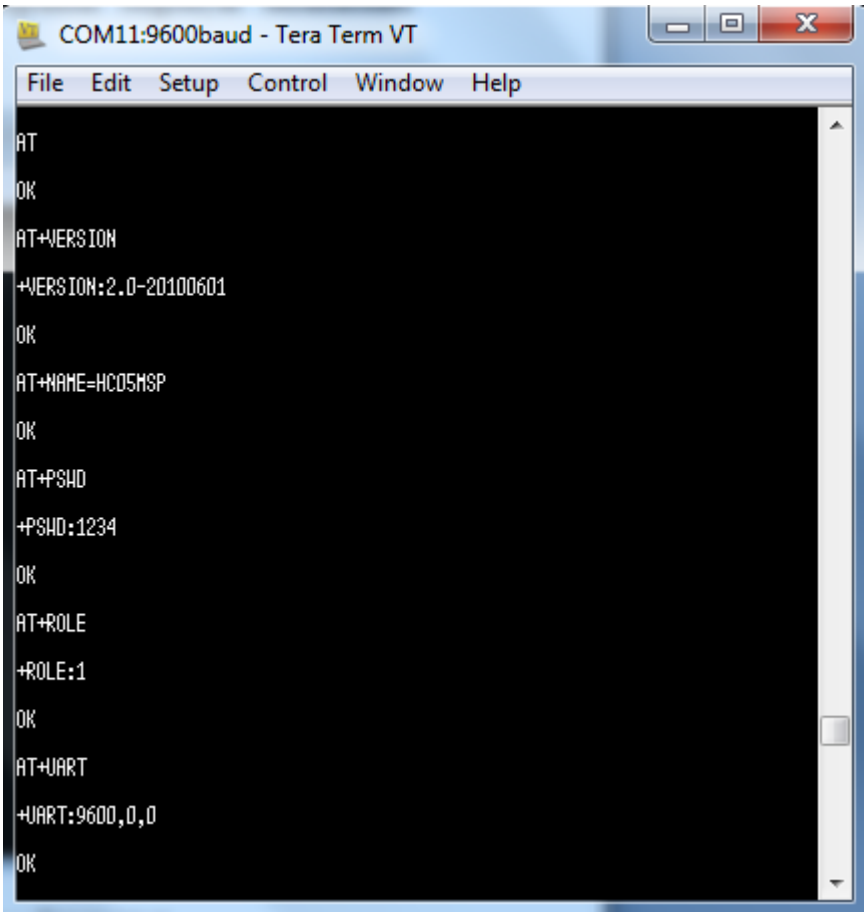


Şekil 3.6: CCS Yazılım Geliştirme Akışı [16].

3.2.2. Tera Term Terminali

Tera Term Microsoft Windows için tasarlanmış, dizisel kapı, telnet ve Güvenli Kabuk (Secure Shell - SSH) bağlantılarını destekleyen bir bağlantı öykünücüdür [17]. Genelde bilgisayar tarafından başlatılan uzaktan bağlantı ile ilgili görevleri otomatikleştirmek için kullanılır.

Bu bitirme tezinde Tera Term programı Bluetooth cihazlarıyla seri iletişim kurularak komutlarla yapılandırılmaları sırasında kullanılmıştır. İnternet üzerinde herkese açık bir kaynak olması nedeniyle tercih edilmiştir. Programın bilgisayar ekranındaki görüntüsü Şekil 3.7'de görüldüğü gibidir.

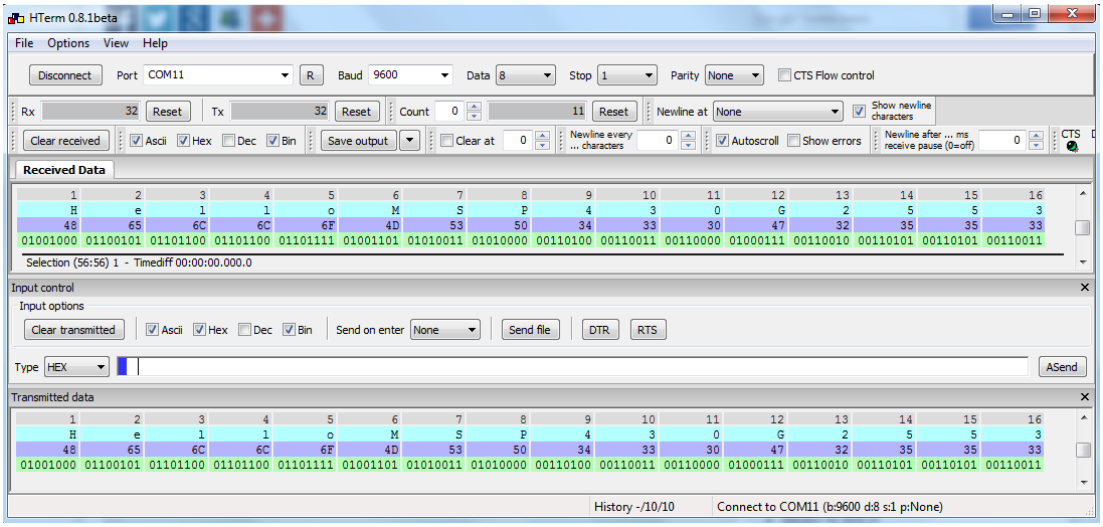


Şekil 3.7: Tera Term Terminali Ekran Görüntüsü.

3.2.3. HTerm Terminali

HTerm terminali seri bağlantı kapısı aracılığıyla iletişim kurmayı sağlayan bir programdır. Kullanıcı istediği seri bağlantı kapısı parametrelerini seçerek cihazla bağlantı kurar [18]. Alınan ve gönderilen karakter miktarını sayma, ikili, ondalık, onaltılık sayı dizgesi, Bilgi Değişimi İçin Amerikan Standart Kodlama Sistemi

(American Standard Code for Information Interchange – ASCII) ile veri girişi girebilme ve veri çıkışı alabilme gibi özellikleriyle kullanıcıya kolaylık sağlar. İnternet üzerinde herkese açık bir kaynak olması nedeniyle de bu bitirme tezinde kullanılması tercih edilmiştir. Programın bilgisayar ekranındaki görüntüsü Şekil 3.8'de görüldüğü gibidir.



Şekil 3.8: HTerm Terminali Ekran Görüntüsü.

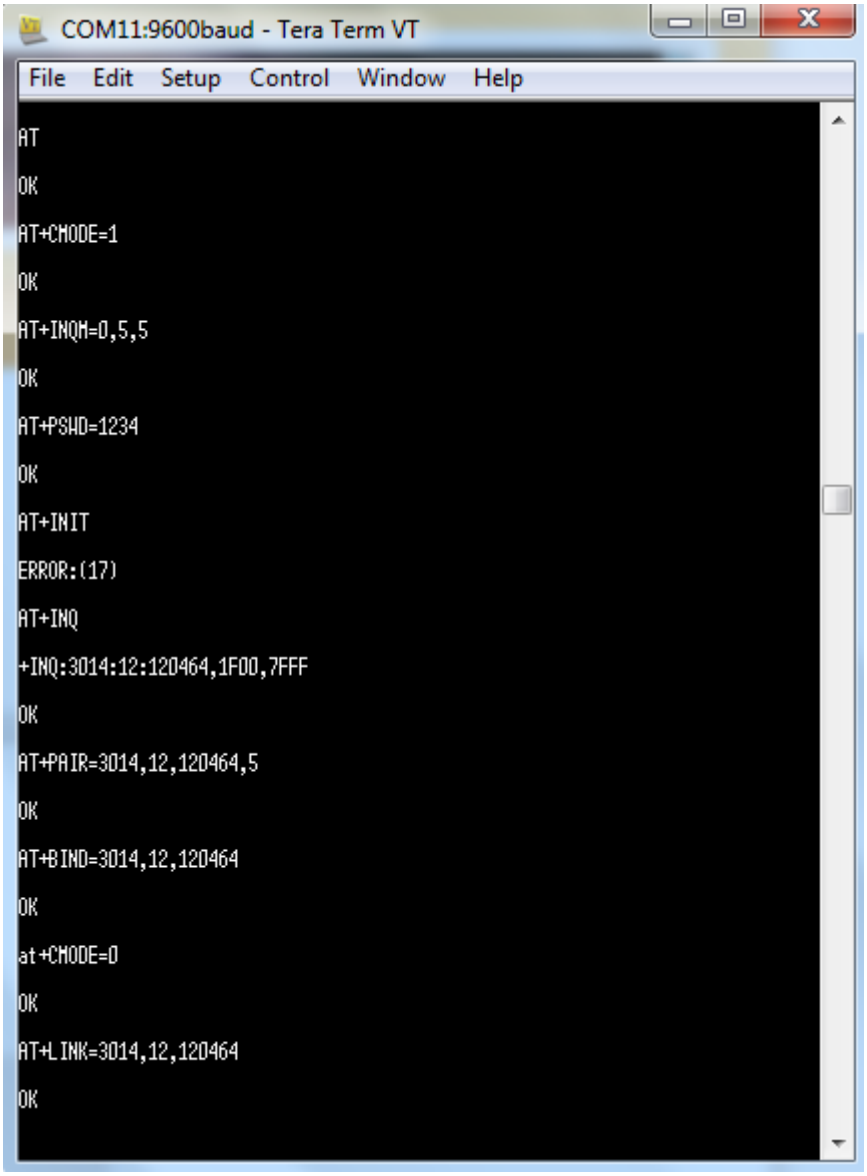
4. DONANIM VE YAZILIM GERÇEKLEMESİ

Yapılan araştırmalar sonunda, tasarım ölçütlerini karşılayan donanım ve yazılım ihtiyaçları belirlenip karşılandıktan sonra istenilen haberleşme protokolünün gerçeklenmesi yapılmıştır. Bu bölümde bitirme tezinde gerçeklenen haberleşme protokolünün ve algoritmaların nasıl gerçeklendiği adım adım anlatılmıştır. İlk adımda MSP430G2553 mikroişlemcilerinin Bluetooth ile haberleşmelerini sağlamak için kullanılacak Bluetooth cihazlarının ana ve bağımlı olmak üzere yapılandırmaları yapılmıştır. Daha sonra mikroişlemcinin UART üzerinden Bluetooth cihazına yolladığı verilerin diğer mikroişlemci tarafından veri kaybı olmadan alması sağlanmıştır. Son adım olarak gönderilen verinin gönderilmeden önce mikroişlemci üzerinde TEA algoritması ile şifrelenip diğer mikroişlemciye aktarıldıktan sonra şifresinin çözülmesi gerçeklenmiştir.

4.1. Bluetooth Cihazlarının Yapılandırılması

Mikroişlemciler arasında tam çift yönlü bir haberleşme sağlamak amacıyla her mikroişlemci için alıcı kısmına bağımlı cihaz, verici kısmına ana cihaz olmak üzere toplamda 4 adet Bluetooth cihazı yapılandırılmıştır. Öncelikle tüm bu yapılandırmaların yapılabilmesi için cihazların TX verici bacakları USB-TTL seri kablosunun RX alıcı bacağına, cihazların RX alıcı bacakları da USB-TTL seri kablosunun TX verici bacağına olmak üzere karşılıklı olarak kablo bağlantısı yapılmıştır. Tera Term programı kullanılarak UART üzerinden cihazlar AT komut kipine sokulup, cihazların seri bağlantı kapısı parametreleri kontrol edilerek aynı baud hızında haberleşmeleri sağlanmıştır. Aynı zamanda cihaz isimleri, şifreleri, ana/bağımlı cihaz rolleri, Bluetooth adresleri sorgulanarak gerekli tanımlamalar yapılmıştır. Eşleştirme işlemi için sadece eşleştirilmek istenen ana ve bağımlı cihazlara enerji verildikten sonra bir mikroişlemcinin verici kısmındaki ana cihaz AT komut kipine sokulmuştur. Ana cihaz üzerinden çekim alanındaki Bluetooth cihazları aranarak diğer mikroişlemcinin alıcı kısmındaki bağımlı cihazın Bluetooth adresi öğrenilmiştir. Bu adres kullanılarak ana ve bağımlı cihaz komut kipinde eşleştirilmiştir. Bağımlı cihazların, ana cihazın çekim alanına girdikleri anda Piconet ağının otomatik olarak oluşturulması ve iletişim kanalının yaratılması için gerekli

yapılandırmalar ayarlanmıştır. Tüm bu yapılandırma ve eşleştirmelerin örnek ekran görüntüsü Şekil 4.1'deki gibidir.



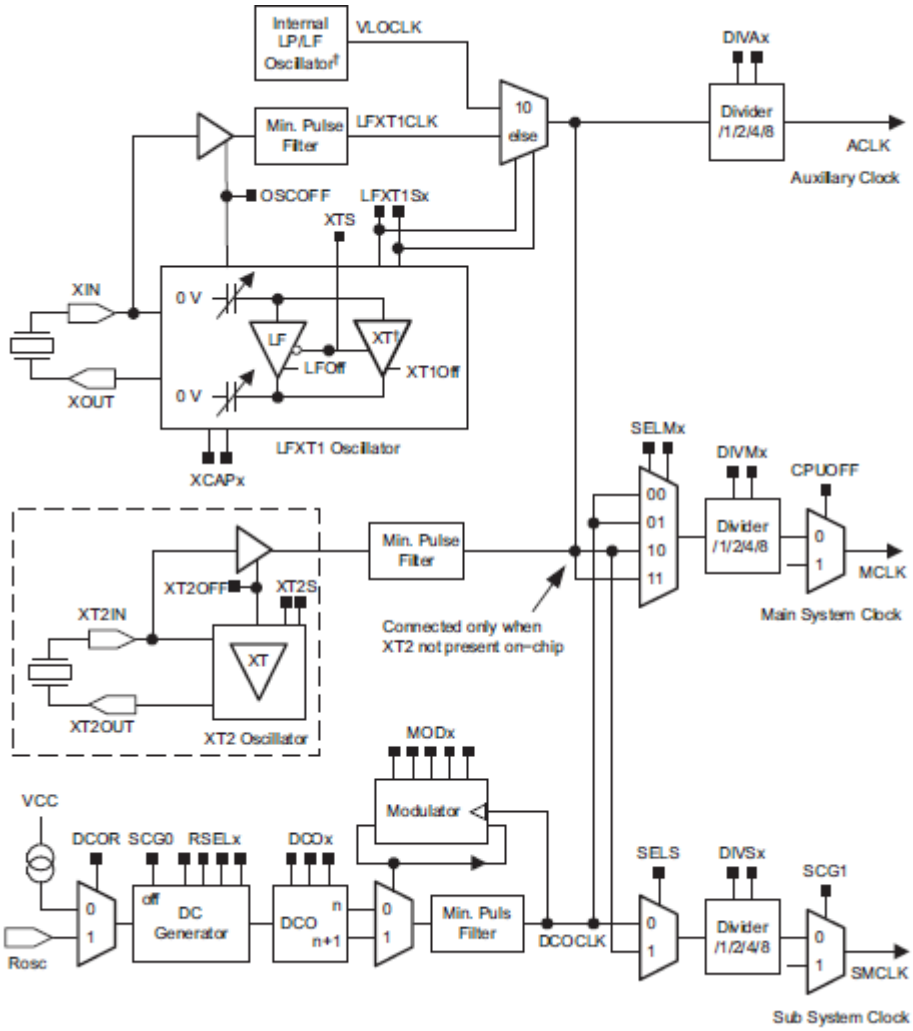
Şekil 4.1: Bluetooth Cihazlarının Yapılandırılması ve Eşlenmesi.

Aynı işlem diğer ana ve bağımlı cihazlar için de tekrarlanarak Bluetooth cihazlarının yapılandırılması ve eşleştirilmesi tamamlanmıştır.

4.2. Mikroişlemcilerin Yapılandırılması

MSP430G2553 mikroişlemcisi ile Bluetooth cihazı arasındaki iletişimin ve doğal olarak iki mikroişlemci arasındaki iletişimin sağlıklı ve düzgün bir şekilde sağlanması için aynı seri bağlantı kapısı parametreleri ile haberleşmeleri gerekmektedir. Bunun için mikroişlemcilerin saat işaretinin Bluetooth cihazlarının

baud hızı ile aynı seçilmesi gerekir. MSP430 ailesinin çok sayıda saat kaynağı ve bu kaynaklardan elde edilen saat işareti seçeneği vardır [11]. Farklı çalışma gereklilikleri için tanımlanan bu seçenekler farklı miktarda güç tüketimine neden olurlar. Bu bitirme tezinde yüksek frekanslarda çalışmaya ihtiyaç olmadığından Sayısal Denetlenen Salıngaç (Digitally Controlled Oscillator – DCO) 1MHz frekansına ayarlanmıştır. MSP430G2553 mikroişlemcisi için saat işaretlerinin üretilme yapısı Şekil 4.2'de gösterilmiştir.



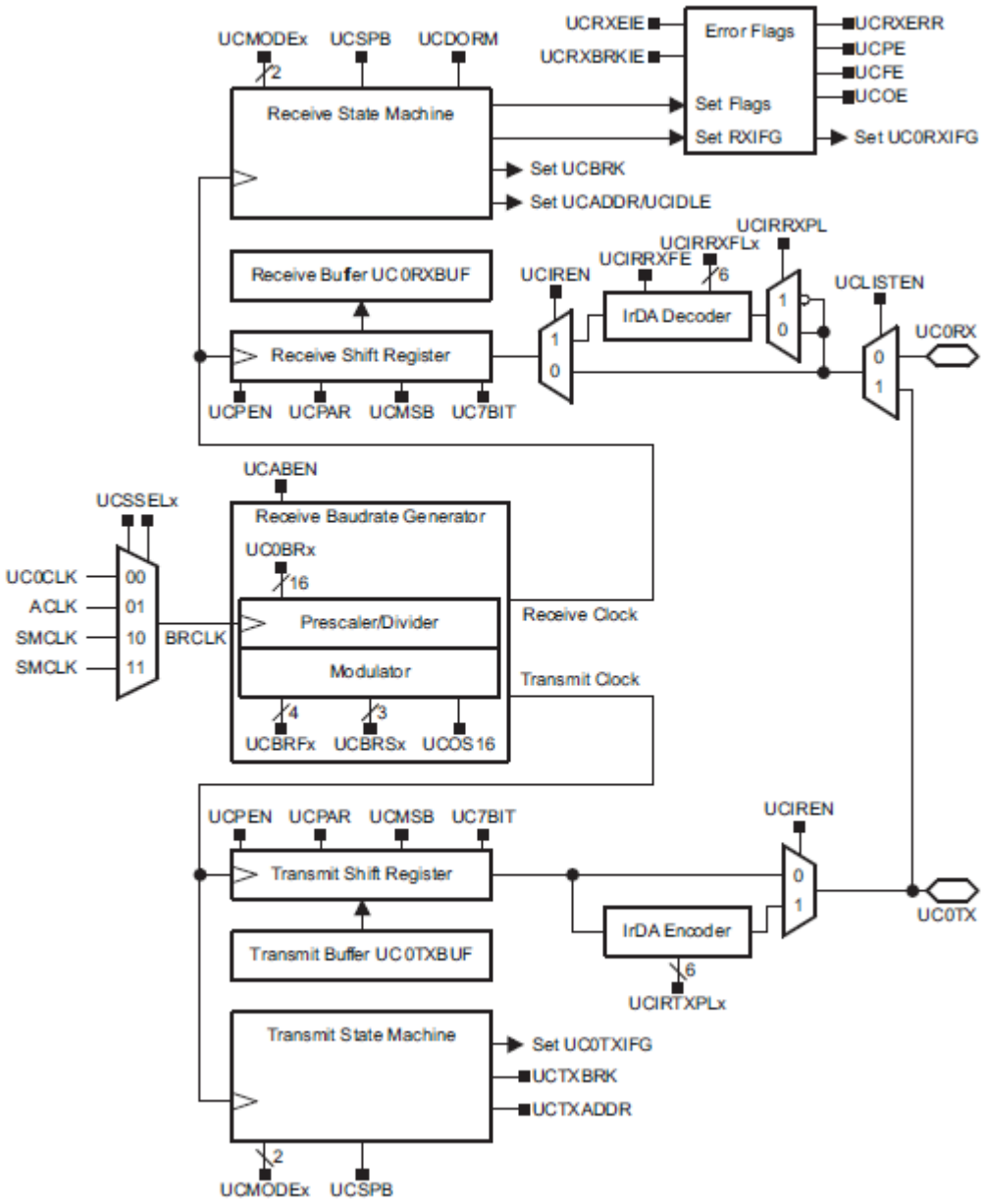
Şekil 4.2: Saat işaretlerinin üretilme yapısı [11].

Tablo 4.1: Baud Hızı ve Hata Ayarları [11].

BRCLK Frequency [Hz]	Baud Rate [Baud]	UCBRx	UCBRSx	UCBRFx	Maximum TX Error [%]		Maximum RX Error [%]	
1,000,000	9600	104	1	0	-0.5	0.6	-0.9	1.2
1,000,000	19200	52	0	0	-1.8	0	-2.6	0.9
1,000,000	38400	26	0	0	-1.8	0	-3.6	1.8
1,000,000	56000	17	7	0	-4.8	0.8	-8.0	3.2
1,000,000	115200	8	6	0	-7.8	6.4	-9.7	16.1
1,000,000	128000	7	7	0	-10.4	6.4	-18.0	11.6
1,000,000	256000	3	7	0	-29.6	0	-43.6	5.2

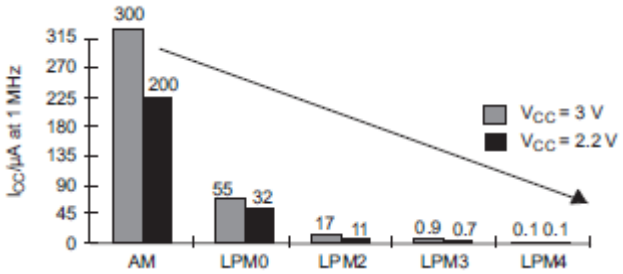
Aynı zamanda minimum güç tüketimi amaçlandığından Alt-Ana Saat İşareti (Sub-Main Clock – SMCLK) kullanılması tercih edilmiştir. Tablo 4.1'deki verilere göre ayarlanan değişkenlerle 9600 baud hızı düşük RX ve TX hata miktarıyla seçilmiştir.

Mikroişlemci içinde bulunan Evrensel Seri Haberleşme Ara Yüzü (Universal Serial Communication Interface – USCI) birçok seri haberleşme yöntemini destekler [11]. UART modunda eşzamansız olarak çalışan RX ve TX bacakları vardır. Veriler mikroişlemciden UART donanımı kullanılarak gönderileceğinden RX ve TX bacaklarının tanımlamasının yapılması gerekmektedir. USCI birimi UART çalışma yapısı Şekil 4.3'teki gibi gösterilmiştir.



Şekil 4.3: Alıcı Verici Çalışma Yapısı [11].

Tüm bu tanımlamalardan sonra mikroişlemcide son olarak LPM ayarlarının yapılması gerekmektedir. Amaç mikroişlemcinin aktif halde değilken minimum güç tüketimi yapmasını sağlamaktır. MSP430G2553 5 farklı LPM uygulamasına sahiptir [12]. Gerek ve yeterli olan minimum güç tüketimi için LPM3 seçilmiştir [11]. Ayrıca USCI alıcı ve verici işkesme rutinleri çalışır hale getirilerek gereksiz yere ana işlem biriminin çalışması önlenmiştir. Yapılacak bütün işlemlerin işkesmeler içinde yapılması sağlanmıştır. Böylece cihaz veri alıp veri göndermediği sürece gereksiz enerji sarf etmeyecek ve düşük güç tüketimi modunda çalışacaktır. USCI birimi bu sırada SMCLK aktif olmamasına rağmen gerektiğinde kontrol biti ayarlarına bakmadan otomatik olarak SMCLK saat işaretini aktif hale getirebildiğinden büyük avantaj sağlar. USCI birimi işkesmeleri etkin olmayan duruma geldiklerinde saat kaynağı kontrol bitlerindeki ayarlara geri döner. Tüm bu işler minimum güç tüketimi için yapılır. Farklı durumlardaki güç tüketim miktarları Şekil 4.4'te gösterilmiştir.



Şekil 4.4: MSP430G2553 Güç Tüketimi [11].

4.3. Küçük Şifreleme Algoritması

Bilgisayar sistemleri yaygınlaştıkça ve karmaşıklaştıkça veri güvenliği de gittikçe önem kazanmıştır [19]. Kriptolama algoritmaları ve protokolleri, sistemlerin ağ iletimi ve veri saklama gibi temel bileşenlerini korurlar. Böyle sistemlerin güvenliği büyük oranda anahtarların oluşturulması, yönetilmesi ve dağıtılması sırasında kullanılan şifreleme teknikleriyle alakalıdır. Anahtar temelli şifreleme algoritmalarının, simetrik ve asimetrik olmak üzere iki farklı çeşidi vardır. Simetrik algoritmalar şifreleme ve şifre çözme için aynı anahtarı kullanırken, asimetrik algoritmalar farklı anahtarlar kullanırlar. İdeal durumlar için şifre çözme anahtarını şifreleme anahtarından hesaplamak mümkün değildir. Simetrik algoritmalar akım halinde şifreleme ve blok halinde şifreleme olarak ikiye ayrılabilir. Akım halinde

şifreleme her bir biti ayrı ayrı şifrelerken, blok halinde şifreleme bir grup biti aynı anda tek bir bitmiş gibi şifreler.

Güvenli bir haberleşme için verinin göndermeden şifrelenmesi, alındıktan sonra da şifresinin çözülmesi gerekir [20]. TEA, mikroişlemciler üzerinde bu işlemlerin yapılması için tasarlanmıştır. Garaj kapısı, araba kilidi, araba marşı ve konut girişi gibi kablosuz anahtarlar için şifreleme gereklidir. Yeterli bilgi işleme gücü ile çok yüksek seviyede güvenli şifreleme algoritmalarını gerçekleştirmek mümkündür.

TEA, 1994 yılında Wheeler ve Needham tarafından şifreleme sırasında bellek kullanımını azaltmak ve hızı arttırmak amacıyla tasarlanmıştır [19]. Feistel çevrimleri ile çift taraflı kaydırma sayesinde verinin ve anahtarların bütün bitleri sürekli olarak karıştırılır. Sonuç olarak TEA ile girişte verilen veride bir bit değişikliği, çıkışta şifrelenen veride 32 bit değişikliğe neden olur. TEA, şifreleme için çok karmaşık işlemler kullanmak yerine basit bir formül ile çok fazla özyineleme yapar [20].

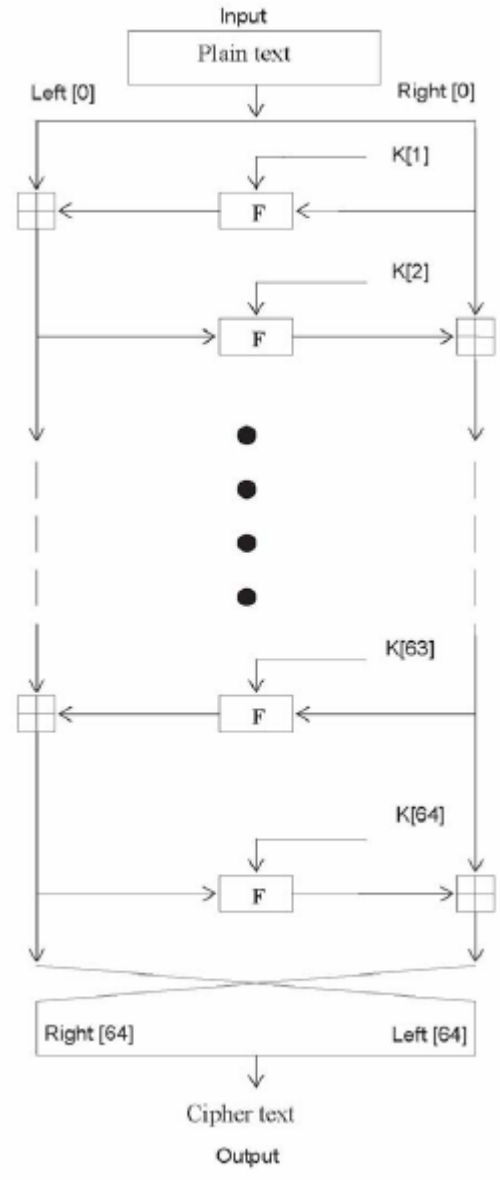
4.3.1. Şifreleme Döngüsü

TEA, blok halinde şifreleme yapan bir algoritma olduğu için her blokta şifrelenecek verinin 64 bit olması gerekir. Şifrelenecek veri sağ ve sol olmak üzere 32 bitlik iki değişkene bölünür [19]. Her bir değişken diğer değişkeni 64 çevrim boyunca şifrelemek için kullanılır. Şifreleme sırasında kullanılacak anahtar 128 bit seçilerek basit arama tekniklerinin başarısız olması amaçlanmıştır [21]. Bu anahtar 32 bitlik dört farklı anahtara bölünerek her çevrimde farklı anahtar kullanılır. Delta sabiti ise altın orandan türetilir ve Denklem 4.1'den hesaplanarak elde edilir. Her döngüde delta sabitinin farklı bir katı kullanılarak her bitin sürekli olarak değişmesi sağlanmıştır.

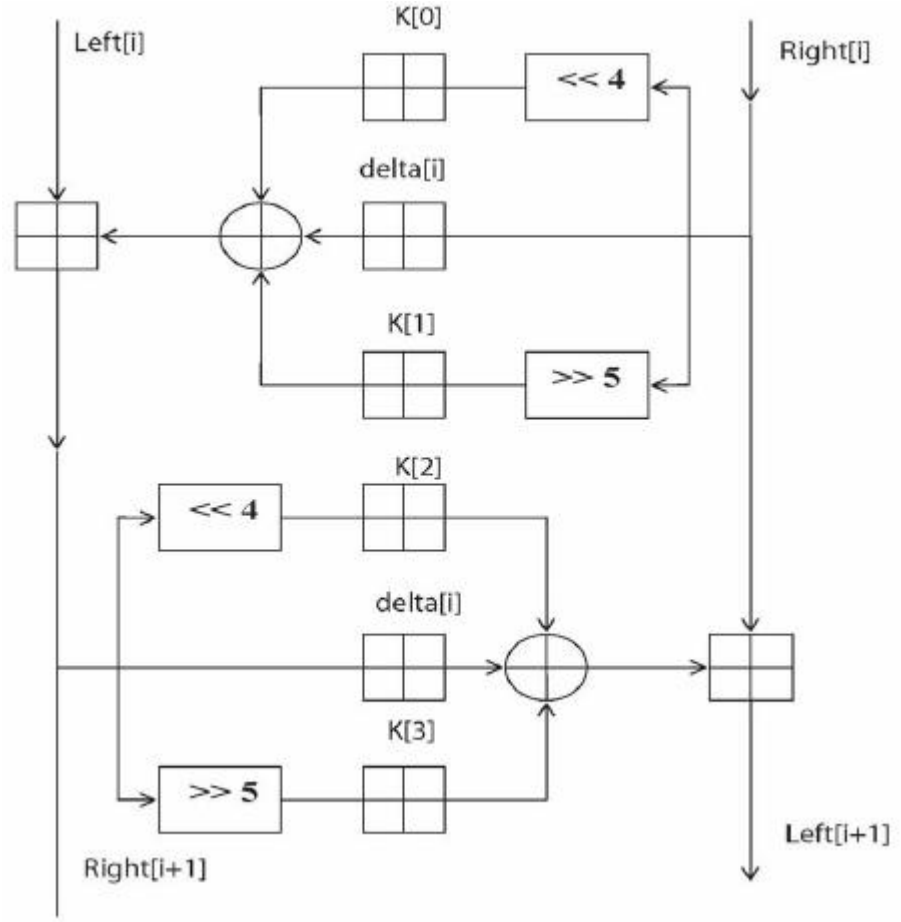
$$delta = \left(\sqrt{5} - 1\right) * 2^{31} = 9E3779B9_h \quad (4.1)$$

Şifrelenecek 64 bitlik veri Sol[0] ve Sağ[0] olmak üzere 32 bitlik verilere ayrılır [19]. Önce Sağ[0], anahtar ve delta sabiti ile şifrelenerek Sol[0] ile toplanır ve Sol[1] elde edilir. Daha sonra Sol[1], anahtar ve delta sabiti ile şifrelenerek Sağ[0] ile toplanır ve Sağ[1] elde edilir. Bu işlem 32 sefer tekrarlanarak sonuçta TEA ile şifrelenmiş çıkış alınır. Bu 64 çevrimden oluşan şifreleme döngüsü Şekil 4.5'te gösterilmiştir.

Verilerin şifrelenmesi sırasında yapılanlar ise anahtar ekleme, bit bit özel veya (Exclusive Or – XOR) ve bit kaydırma işlemlerinden oluşur [19]. 128 bitlik anahtar K[0], K[1], K[2] ve K[3] olmak üzere 32 bitlik 4 farklı anahtara ayrılmıştır. Sağ[0] girişi 4 bit sola kaydırılıp K[0] anahtarı ile toplanır. Ayrıca 5 bit sağa kaydırılıp K[1] anahtarı ile toplanır. Bu iki değer delta sabitiyle özel veya işlemine sokularak sonuç Sol[0] girişi ile toplanır ve Sol[1] değerine atanır. Elde edilen Sol[1] değeri yine 4 bit sola kaydırılıp K[2] anahtarı ile toplanır. Ayrıca 5 bit sağa kaydırılıp K[3] anahtarı ile toplanır. Bu iki değer yine delta sabitiyle özel veya işlemine sokularak sonuç Sağ[0] girişi ile toplanır ve Sağ[1] değerine atanır. Şekil 4.6'da şifreleme sırasında yapılan işlemler gösterilmiştir.



Şekil 4.5: TEA Şifreleme Döngüsü [19].



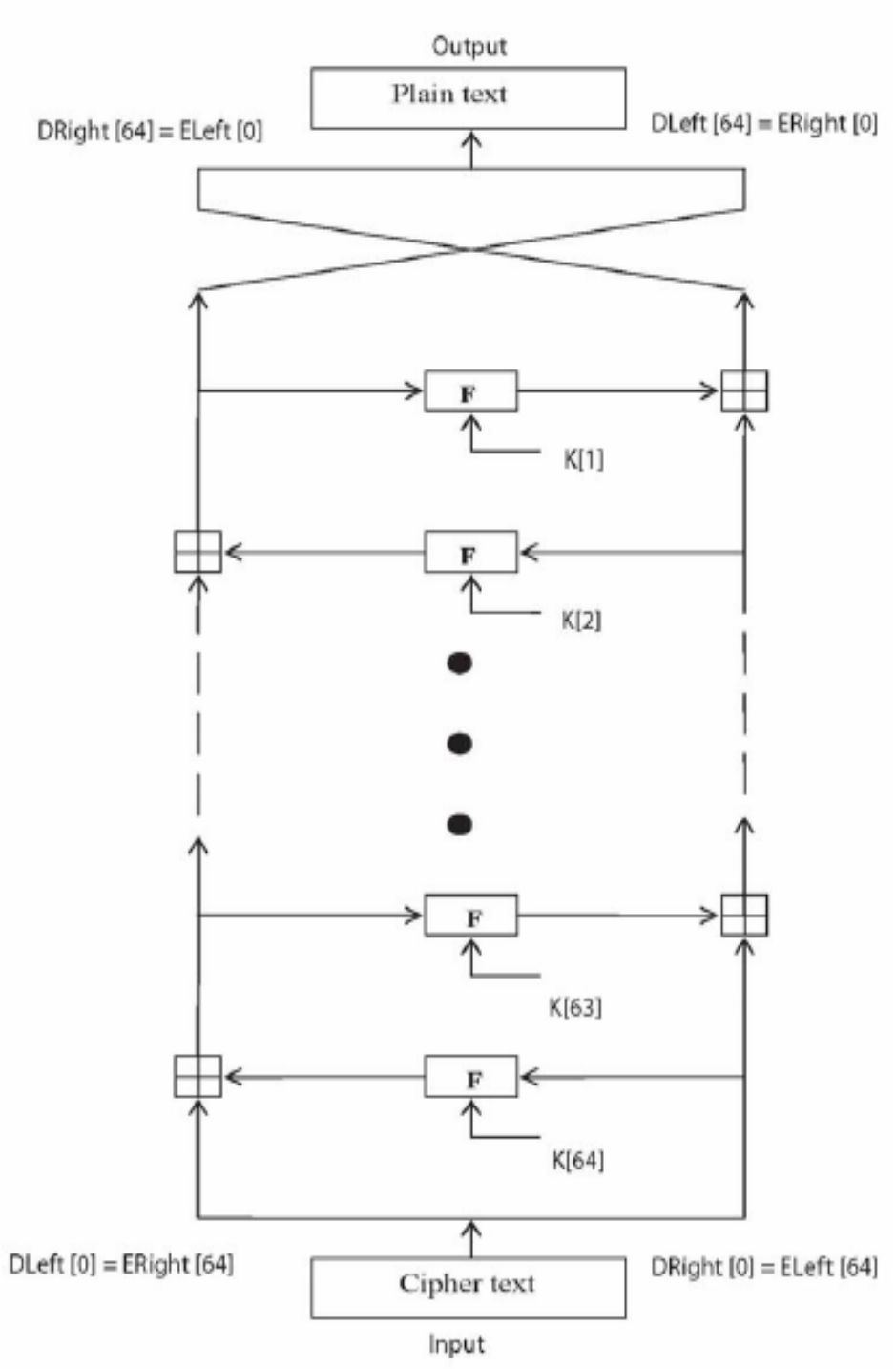
Şekil 4.6: TEA Şifreleme İşlemleri [19].

4.3.2. Şifre Çözme Döngüsü

Şifre çözülürken yapılan işlemler şifrelemeyle neredeyse aynıdır [19]. Şifre çözme döngüsünde şifreli veri giriş olarak alınır ancak şifre çözmek için kullanılacak anahtarlar ters sırada kullanılır. Şifresi çözülecek 64 bitlik veri DSol[0] ve DSağ[0] olmak üzere 32 bitlik verilere ayrılır. Bu ayırmada da yönler şifrelemedekinin tersi olarak kullanılır. Önce DSağ[0], anahtar ve delta sabiti ile şifresi çözülerek DSol[0] değerinden çıkartılır ve DSol[1] elde edilir. Daha sonra DSol[1], anahtar ve delta sabiti ile şifresi çözülerek DSağ[0] değerinden çıkartılır ve DSağ[1] elde edilir. Bu işlem 32 sefer tekrarlanarak sonuçta TEA ile şifresi çözülmüş çıkış alınır. Bu 64 çevrimden oluşan şifre çözme döngüsü Şekil 4.7'de gösterilmiştir.

Verilerin şifresinin çözülmesi sırasında ise önce DSağ[0] girişi 4 bit sola kaydırılıp K[2] anahtarı ile toplanır. Ayrıca 5 bit sağa kaydırılıp K[3] anahtarı ile toplanır. Bu iki değer delta sabitiyle özel veya işlemine sokularak sonuç DSol[0] değerinden çıkartılır ve DSol[1] değerine atanır. Elde edilen DSol[1] değeri yine 4 bit sola

kaydırılıp K[0] anahtarı ile toplanır. Ayrıca 5 bit sağa kaydırılıp K[1] anahtarı ile toplanır. Bu iki değer yine delta sabitiyle özel veya işlemine sokularak sonuç Sağ[0] değerinden çıkartılır ve Sağ[1] değerine atanır.

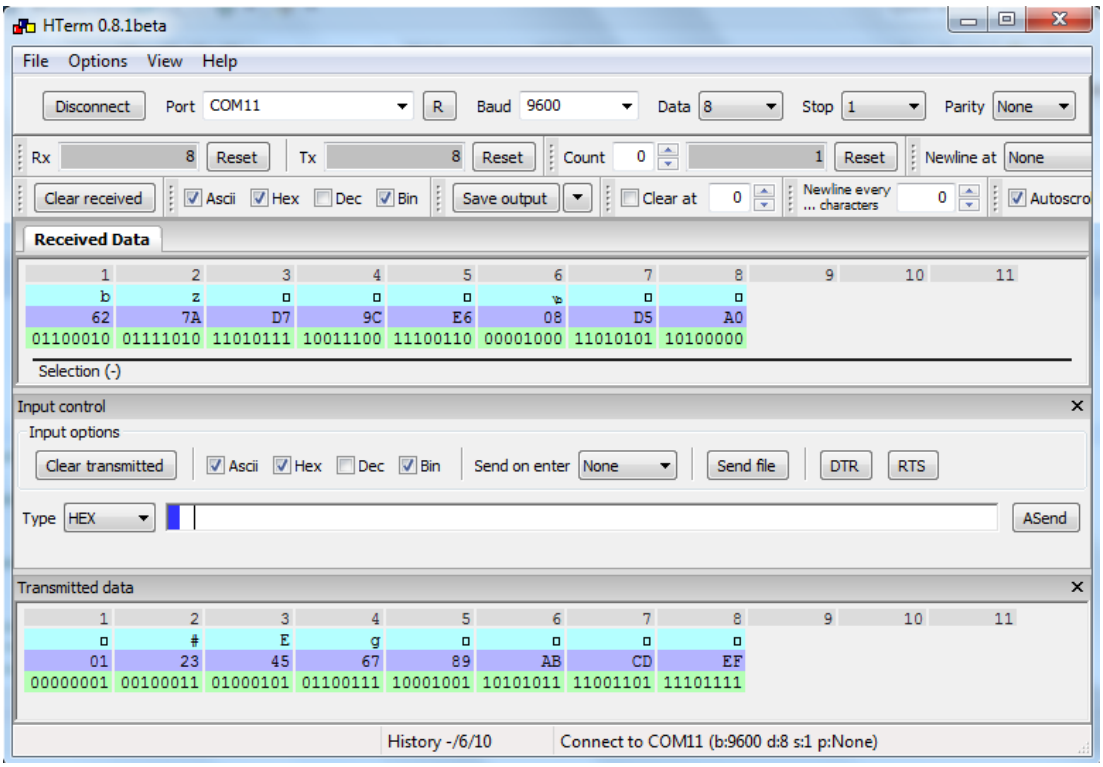


Şekil 4.7: Şifre Çözme Döngüsü [19].

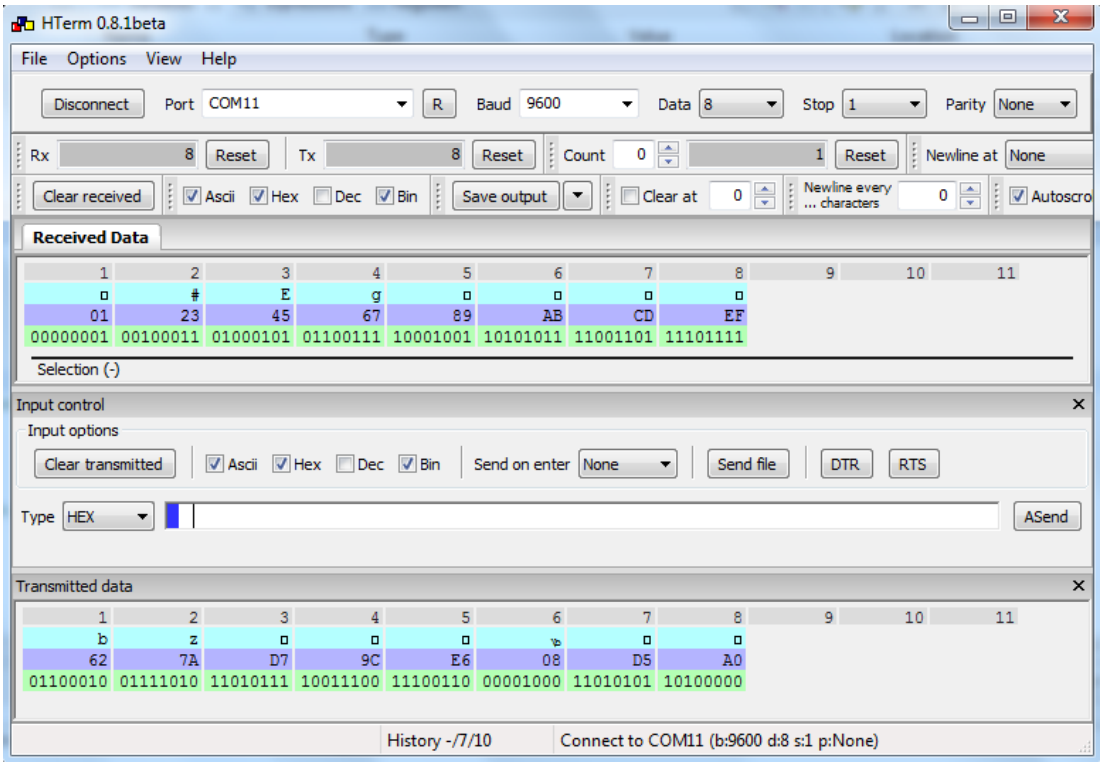
4.4. Güvenli Haberleşmenin Gerçeklenmesi

UART üzerinden gönderilen ve alınan verilerin, şifrelenmesi ve şifresinin çözülmesi için TEA, MSP430G2553 mikroişlemcisi üzerinde gerçeklenmiştir. Bunun için mikroişlemci, UART birimi üzerinden bilgisayara bağlanarak veri alış verişi takip edilmiştir. UART üzerinden gönderilen veriler her işkesme rutini için 8 bitlik gruplar halinde yollanır. Bu nedenle şifrelenmek istenen 64 bitlik veriler önce 8 bitlik dizilere kaydedilmiştir. Dizinin her bir elemanı 32 bitlik değişkenlere atandıktan sonra gerekli bit kaydırma ve XOR işlemlerinden sonra şifrelenmek istenen veri sol ve sağ olmak üzere 2 adet 32 bitlik dizi halinde elde edilir. 128 bitlik şifreleme anahtarı da mikroişlemci üzerinde tanımlanarak 4 adet 32 bitlik anahtar dizisi halinde elde edilir. Son olarak elimizdeki veri anahtarlar ile şifreleme işlemine sokulur.

Şifreleme algoritmasının doğru bir şekilde çalıştığını görmek için deneme amaçlı anahtarlar K[0]= 0x0123ABCD, K[1] = 0x89EF4567, K[2] = 0x16011914 ve K[3] = 0x14071991 olarak tanımlanmıştır. Şifreleme için gönderilen 0x012345678ABCDEF 64 bitlik verinin şifreli hali Şekil 4.8'de görüldüğü gibi 0x627AD79CE608D5A0 olarak elde edilmiştir. Aynı veri şifre çözme için gönderilmiş ve Şekil 4.9'da görüldüğü gibi 0x012345678ABCDEF elde edilmiştir.

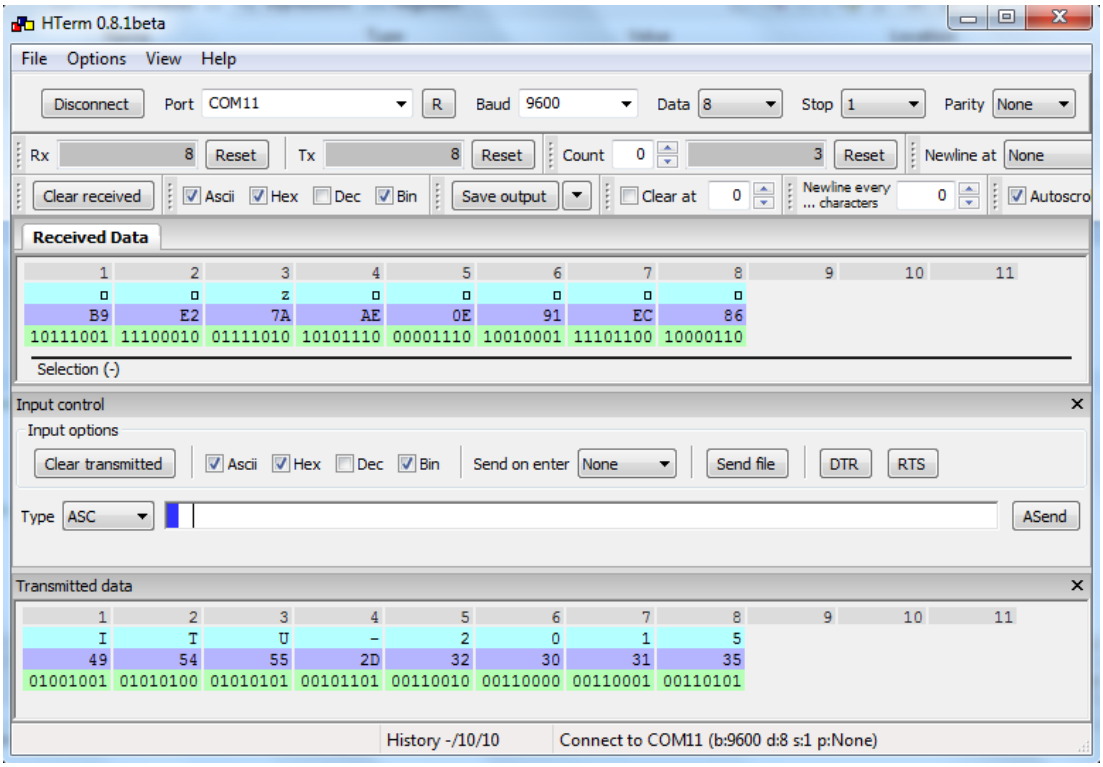


Şekil 4.8: Şifreleme Sonucu.



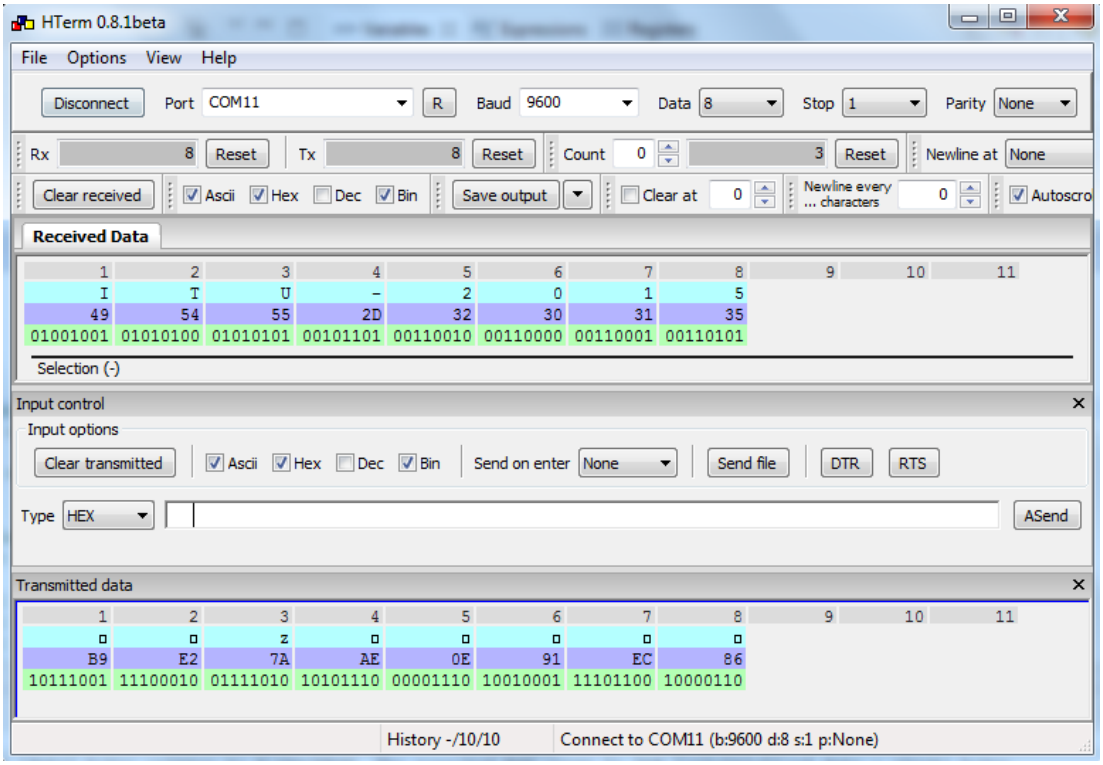
Şekil 4.9: Şifre Çözme Sonucu.

Aynı işlemler, aynı anahtarlarla metin dizgisi şifrelemek için denenmiştir. 64 bitlik veri olarak "ITU-2015" dizgisi şifrelenmiş ve şifreli hali Şekil 4.10'da görüldüğü gibi 0xB9E27AAE0E91EC86 olarak elde edilmiştir.

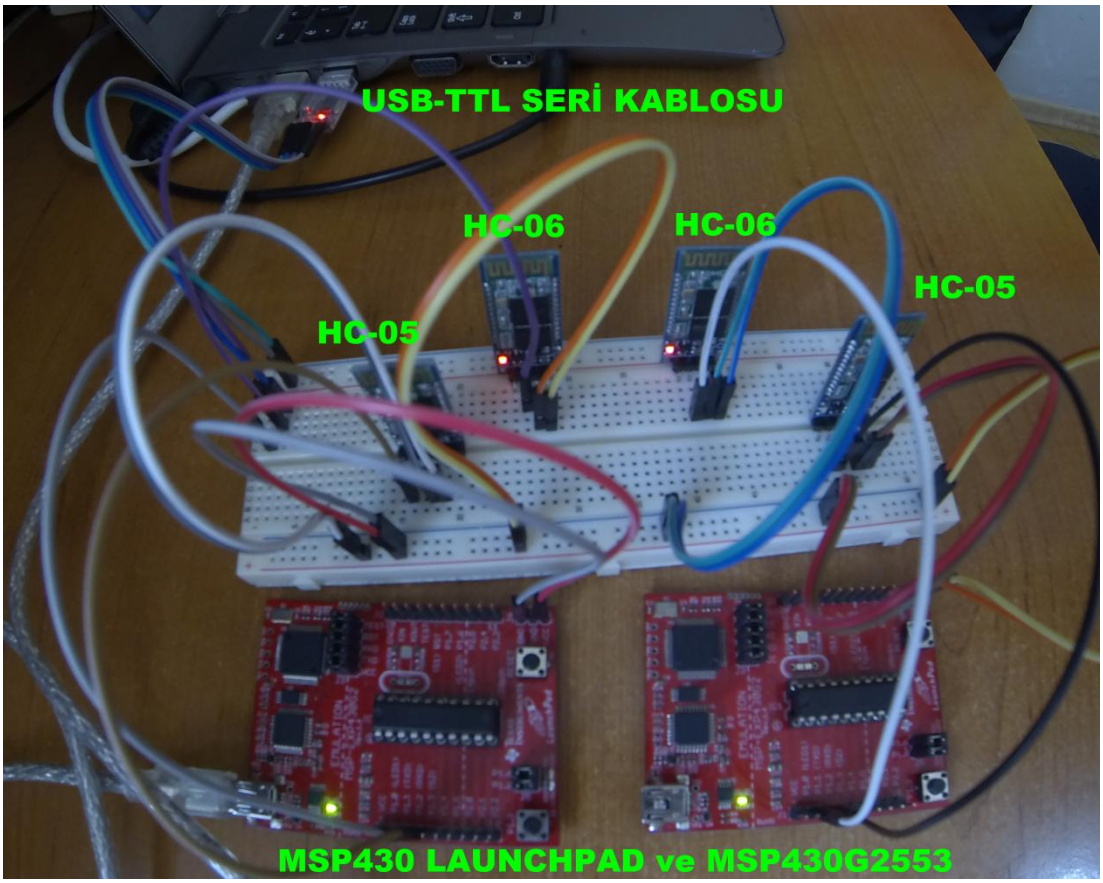


Şekil 4.10: Metin Dizgisi Şifreleme.

Şifrelenmiş verinin şifresi çözüldüğünde de Şekil 4.11'de görüldüğü gibi 64 bitlik "ITU-2015" metin dizgisi elde edilmiştir. Gerçekleme sırasında mikroişlemciler ile Bluetooth cihazları arasında ve bilgisayar ile sistem arasında yapılan bağlantılar Şekil 4.12'de gösterilmiştir.



Şekil 4.11: Metin Dizgisi Şifre Çözme.



Şekil 4.12: Gerçeklenen Sistem.

5. SONUÇLAR VE TARTIŞMA

Bu bitirme tezinde Bluetooth ile haberleşerek güvenli veri alışverişi yapabilen bir sistem tasarlanmıştır. Tasarım yapılırken WMN tipindeki ağlar temel alınmıştır. Tasarlanan sistem MSP430G2553 mikroişlemcisi, HC-05 ve HC-06 Bluetooth modülleri kullanılarak gerçeklenmiştir. Kablosuz olarak gönderilen verinin TEA şifreleme algoritması ile şifrelenmesi sağlanmış, alınan verinin de şifresinin çözülmesi sağlanmıştır. Cihazların yapılandırılması ve tasarlanan sistemin doğru bir şekilde çalışıp çalışmadığı, cihazlar UART üzerinden bilgisayara bağlanarak kontrol edilmiştir.

MSP430 ailesi mikroişlemcilerin sahip olduğu düşük güç kullanımı, işkesme rutinleri ve USCI birimi UART modu tasarımın gerçeklenmesini kolaylaştırmıştır. Tasarımda seçilen HC-05 ve HC-06 Bluetooth modülleri Bluetooth 2.0 BR+EDR teknolojisine aittir. Bu da cihazların ana cihaz durumu ile bağımlı cihaz durumu arasında geçiş yapması sırasında, değişen baud hızı, geç alınan cevapların getirdiği hatalar nedeniyle zorluklar çıkarmıştır. Bu nedenle 2 ana, 2 bağımlı olmak üzere 4 adet Bluetooth cihazı kullanılarak tam çift yönlü haberleşme sağlanmıştır. İleride bu geçişi daha kolay ve hatasız sağlayan Bluetooth 4.0 ve üzeri teknolojilere ait modüller kullanılarak yarı çift yönlü haberleşme sağlanabilir. Bu cihazlar aynı zamanda LE sisteminde çalışacağından daha da az güç tüketen daha gelişmiş bir sistem tasarlanabilir.

KAYNAKLAR

[1] **Wang, X. and Lim, A.O.**, 2007. IEEE 802.11s wireless mesh networks: Framework and challenges, Ad Hoc Networks, 6, pp. 970-984

[2] **Akyildiz, I.F., Wang, X. and Wang, W.,** 2005. Wireless mesh networks: a survey, Computer Networks, vol. 47, pp. 445-487

[3] **Kubes, J., Parak, J., Pokorny, M., and Havlik, J.,** IMPLEMENTATION OF THE BLUETOOTH WIRELESS COMMUNICATION USING THE FINITE STATE MACHINE. situations, 6, 7.

[4] **Johnson, D.,** (2004, September). Hardware and software implications of creating Bluetooth Scatternet devices. In AFRICON, 2004. 7th AFRICON Conference in Africa (Vol. 1, pp. 211-215). IEEE.

[5] **Haartsen, J. C., and Mattisson, S.,** (2000). Bluetooth-a new low-power radio interface providing short-range connectivity. Proceedings of the IEEE, 88(10), 1651-1661.

[6] **Bisdikian, C.,** (2001). An overview of the Bluetooth wireless technology. IEEE Commun Mag, 39(12), 86-94.

[7] **Sainz, B., Antolín, J., López-Coronado, M., and Castro, C. D.,** (2013). A novel low-cost sensor prototype for monitoring temperature during wine fermentation in tanks. Sensors, 13(3), 2848-2861.

[8] **SIG**, (2014). Bluetooth Specification Version 4.2 – Architecture & Terminology Overview, Vol. 1, 02 December 2014.

[9] **SIG,** [Alıntı Tarihi: 3 Mayıs 2015], http://www.bluetooth.com

[10] **Texas Instruments,** 2015. MSP-EXP430G2 LaunchPad Evaluation Kit User's Guide (Rev. F)

[11] **Texas Instruments,** 2013. MSP430G2xxx Family User's Guide (Rev. J)

[12] **Texas Instruments,** 2013. MSP430G2x53-mixed signal microcontroller (Rev.J)

[13] **Guangzhou HC Information Technology,** HC Serial Bluetooth Products User Instructional Manual, [Alıntı Tarihi: 5 Mayıs 2015], http://abc-rc.pl/templates/images/files/995/1425483439-hc-06-datasheet.pdf

[14] **Guangzhou HC Information Technology,** HC-03/05 Embedded Bluetooth Serial Communication Module AT command set, [Alıntı Tarihi: 5 Mayıs 2015], http://www.linotux.ch/arduino/HC-0305_serial_module_AT_commamd_set_201104_revised.pdf

[15] **Texas Instruments,** 2015. Code Composer Studio™ v6.1 for MSP430™

User's Guide (Rev. AH)

[16] **Texas Instruments,** 2014. MSP430 Optimizing C/C++ Compiler v 4.4 User's Guide (Rev. J)

[17] **TeraTerm,** Tera Term Help Index, [Alıntı Tarihi: 7 Mayıs 2015], http://ttssh2.sourceforge.jp/manual/en/

[18] **Hammer, T.,** HTerm, [Alıntı Tarihi: 7 Mayıs 2015], http://www.der-hammer.info

[19] **Andem, V.R.,** 2003. A Cryptanalysis of the Tiny Encryption Algorithm, MSc. Thesis, The University of Alabama, ALABAMA.

[20] **Texas Instruments,** 2005. TEA Encryption and Decryption With the MSP430 (Rev. A)

[21] **Wheeler, D. J., and Needham, R. M.,** (1995, January). TEA, a tiny encryption algorithm. In Fast Software Encryption (pp. 363-366). Springer Berlin Heidelberg.

ÖZGEÇMİŞ

Adı Soyadı: Oğulcan BAL

Doğum Yeri ve Tarihi: İzmir, 1991

Lise: Bornova Anadolu Lisesi; 2005-2009

Lisans: İstanbul Teknik Üniversitesi, Elektronik Mühendisliği; 2009-2015