Marmara Fen Bilimleri Dergisi 2016, 3: 100-111
DOI: 10.7240/mufbed.73633

Nesnelerin İnterneti Teknolojisinde Güvenli Veri İletişimi - Programlanabilir Fiziksel Platformlar Arasında WEP Algoritması ile Kriptolu Veri Haberleşmesi Uygulaması

Samet Akkuş

Marmara Üniversitesi, Fen Bilimleri Enstitüsü, Elektrik-Elektronik Mühendisliği Bölümü, İstanbul, Türkiye

ÖZ

Günümüzde geliştirilen yüksek teknolojili cihazlar modern toplumların vazgeçilmez değerleri arasındadır. Günlük ihtiyaçlarımızın birçoğunda kullandığımız bu teknolojiler hayatımızı oldukça kolaylaştırmaktadır. Bu cihazların çoğu birbirinden bağımsız olarak çalışmaktadır. Son yıllarda Nesnelerin İnterneti (Internet of Things - IoT) teknolojisi ile birlikte günlük hayatta kullandığımız tüm cihazların birbiri ile haberleşerek akıllı bir haberleşme ekosistemi oluşturulması amaçlanmaktadır. Bu bağlamda, IoT ekosisteminde bulunan internet üzerinde herhangi iki farklı yerel ağa bağlı, programlanabilir mikrodenetleyiciler arasında kriptolu veri haberleşmesi gerçekleştirilmiştir. Kullanılan bu programlanabilir mikrodenetleyicilere IO(Input-Output) arayüzü üzerinden her türlü cihaz bağlanabilmekte ve kontrol edilebilmektedir. Yerel ağda bulunan cihaz üzerinden uzak ağa veri gönderilmek istenildiğinde, cihaz veriyi şifreler ve internet üzerinden karşıdaki yönlendiriciye gönderir. Yönledirici veriyi kendi ağında bulunan programlanabilir cihaza yönlendirir. Programlanabilir cihaz ise şifreli veriyi çözerek kendi yerel ağında bulunan bilgisayara iletir. Bu işlemin gerçekleşebilmesi için gerekli port yönlendirme ve NAT ayarları hem yönlendiricleri hem de cihazlar üzerinde gerçekleştirilmelidir. Oluşturulan bu sistemin avantajı, cihazın IP filtrelemesi yaparak dışarıdan gelecek saldırılara karşı duyarlı olması ve paket içeriğini şifrelediği için veri bloğu okunsa dahi içerikten bir anlam çıkartılamamasıdır.

Anahtar Kelimeler: Nesnelerin İnterneti, Programlanabilir Fiziksel Platformlar, İletişim Güvenliği, IP Güvenliği

Secure Communication for The Internet of Things - Encrypted Data Communication Between Programmable Physical Platforms With WEP Algorithm

ABSTRACT

In a world where the technology has been developing constantly, the privacy and reliability of information gains importance each day. With the popularization of Internet of Things technology in recent years, all kinds of devices are now connected to internet in addition to computers and servers, and this necessitated designing encryption algorithms, network topologies and firewalls. Within the scope of this study, cryptographic data communication has been carried out between two different devices connected to a local network on the Internet of Things ecosystem. When a data transfer is needed to a remote network through a device located on the local network, one of the devices, assigned a static IP address by the router on the local network, encrypts the data and transfers it to the other device. The device receiving the data decrypts it and transfers it to the computer on the same local network. In order to carry out this process, it is important to perform the required port forwarding and NAT settings on both router and the device. The advantage of this system developed is that the device becomes protected against outside attacks through IP filtering, and even if the package is opened on its path, the encrypted data cannot be read, and a meaningful substance cannot be extracted from the package content.

Keywords: Internet Of Things, IoT Security, Arduino, IP Security

Sorumlu Yazar / Corresponding Author: Samet AKKUŞ, Tel: 0 507 528 0903, e-posta: sametakkus@marun.edu.tr
Gönderilme/Submitted: 07/06/2016, **Kabul/Accepted:** 18/08/2016

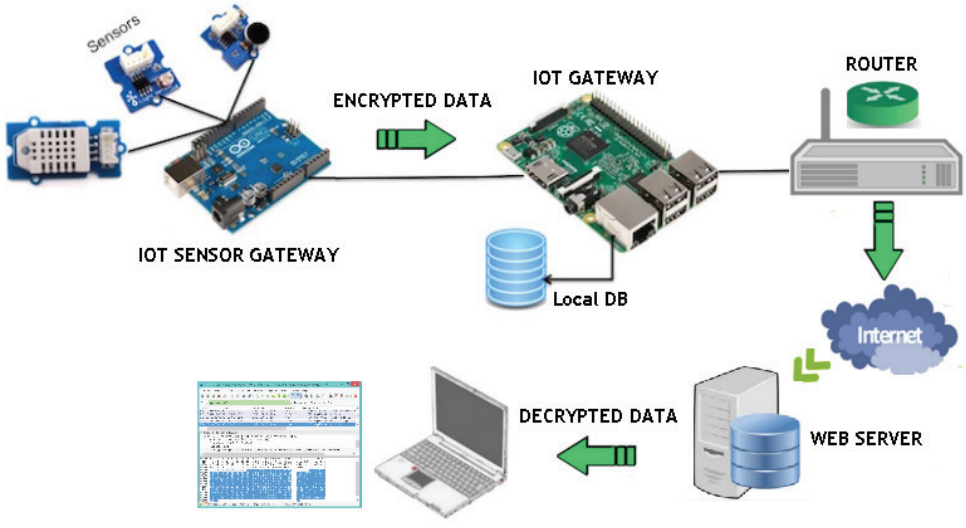
I. GİRİŞ

Teknoloji dünyasında bir bilginin gizliliği, bütünlüğü ve erişilebilirliği önemli konuların başında yer almaktadır. Günümüzde bilgi güvenliği teknolojilerine en fazla ihtiyaç duyan alanlar internet bankacılığı, e-ticaret siteleri, kimlik doğrulama sistemleri, kablosuz cihazlar ve günlük hayatta kullandığımız her türlü cihazın internete bağlanmasına olanak sağlayan Nesnelerin İnterneti teknolojisi olarak sayılabilir. Nesnelerin İnterneti teknolojisi ile birlikte bilgisayar ve sunucuların yanında günlük hayatta kullandığımız her türlü cihazın internete bağlanması ile bu cihazlara ait özel şifreleme algoritmaları, bağlantı modelleri ve güvenlik katmanlarının tasarlanmasına ihtiyaç duyulmaktadır. Nesnelerin İnterneti teknolojisi, Uluslararası Telekomünikasyon Birliği (ITU) tarafından IoT (Internet of Things) olarak tanımlanmıştır. ITU'nun bilgi teknolojileri konusundaki düzenlemelerindeki gelişmelere yönelik yayımlanan "Telekomünikasyon Reformlarındaki Eğilimler" raporunda, genişbant bağlantıların yaygınlaştığı ve "Nesnelerin İnternet'i" (IoT) konusunun öneminin arttığı belirtilmektedir. Raporda mobil şebekelerde oransal olarak en fazla trafik artışının "Makinelerarası İletişim" (M2M) haberleşmesinde görüldüğü ve gelecekte de mobil şebekelerdeki trafik artışının önemli bir kısmının M2M kaynaklı olacağı ifade edilmektedir [1].

Günlük hayatta sıklıkla kullandığımız IoT, GSM, Web, RFID ve diğer tüm haberleşme sistemlerinde bilgilerin iletilmesi, dağıtılması ve saklanması güvenli yöntemlerle gerçekleştirilmelidir. Modern toplumda internet ağlarının gelişmesi ile birlikte, bilgilere olan erişim kolaylaşırken güvenlik sorunlarını günden güne artmaktadır. Günümüzde bir bilginin üçüncü şahıslardan korunması ve eksiksiz bir şekilde iletilmesi kritik bir sorun haline gelmiştir. Sistemler arası haberleşmede verinin güvenli bir şekilde taşındığından emin olmak gerekir. Bunun en sağlıklı yolu ise gönderilen verinin çeşitli yöntemler ile şifrelenmesidir. Örneğin, bir arkadaşımıza e-posta aracılığı ile ileti göndermek istediğimizde, gönderdiğimiz iletiler birçok donanımdan geçerek arkadaşımızın e-posta hesabına iletilmektedir. Fakat bu iletinin yolda başkaları tarafından okunup okunmadığını veya üzerinde değişiklik yapılıp yapılmadığını bilemeyiz. Bu tür sebeplerden dolayı kriptoloji hayatımızda büyük öneme sahip bir bilim dalı haline gelmiştir [2].

Kriptoloji, bir şifre bilimidir. Çeşitli verilerin güvenli bir ortamda belirli bir sisteme göre şifrelenerek karşı tarafa iletilmesi ve karşı tarafta verinin sağlıklı bir şekilde çözülebilmesi kriptolojinin ana amacıdır. Günümüzde kriptoloji biliminden faydalanan sistemler yalnızca bilgisayarlar değildir. Örneğin, ATM cihazları, modemler, IP Telefonlar, RFID cihazlar, otomasyon cihazları, medikal ekipmanlar ve cep telefonları gibi birçok alanda kriptolojiden faydalanılmaktadır. Bu tür sistemlerin yazılımsal ve donanımsal altyapısında kriptoloji biliminden faydalanılmadığı takdirde bilgilere kolayca erişilebilir ve illegal olarak faydalanılabilir. Nesnelerin İnterneti teknolojisinin yaygınlaşması ve çeşitli cihazların internet erişebilmesi ile kriptoloji günden güne önem kazanmakta, veri güvenliği alanında yeni yöntem ve çözümler aranmaktadır. Bu alanda yeni bir çözüm üretmek adına bu çalışma kapsamında, mikrodenetleyici mimarisine sahip Arduino platformu üzerinde WEP protokolünü kullanan bir şifreleme altyapısı tasarlanmış ve WAN içerisinde bulunan iki nokta arasında kriptolu bir kanal oluşturularak güvenli bir haberleşme altyapısı kurulmuştur.

Mikrodenetleyici yapısına sahip platformların IoT teknolojisinde kullanımını kapsayan ve internet üzerinden



Şekil 1: Literatür Örneği

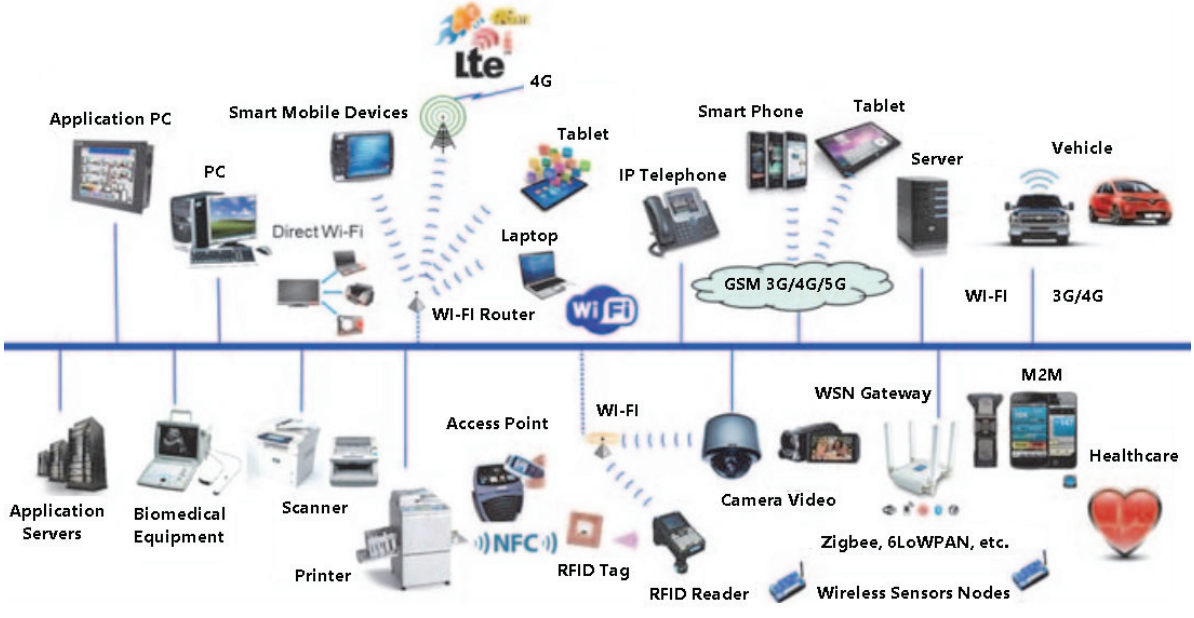
kriptolu veri iletimi sağlamaya yönelik yapılan çalışmalara örnek olarak, Luleå üniversitesinden James King 2015 yılında gerçekleştirdiği "A Distributed Security Scheme to Secure Data Communication between Class-0 IoT Devices and the Internet" isimli çalışması verilebilir. Aynı zamanda oluşturduğum yapıya ilham kaynağı olan bu çalışmada, şekil 1'de görüldüğü gibi ilk olarak Arduino platformu ile sensör verileri toplanmış ve AES-128 algoritması ile şifrelenmiştir. Şifrelenen veriler yerel ağda bulunan Raspberry Pi platformuna gönderilmiştir. Raspberry Pi, verileri yerel bir server'a yedeklemiş ve yönlendirici üzerinden uzak ağda bulunan server'a iletmiştir. Server kriptolu verileri AES-128 algoritması ve paylaşılan anahtar yardımıyla çözmüş ve depolayarak kendi ağında bulunan diğer cihazlar ile paylaşmıştır [3]. Bu tür çalışmalar çeşitli yöntem değişiklikleri ile sayısız farklı şekilde gerçekleştirilebilmektedir.

James King'in çalışmasından farklı olarak yapılan bu çalışmada internet üzerinden Raspberry Pi - Web Server haberleşmesi yerine iki tarafta da ethernet arayüzüne sahip Arduino cihazları kullanılmıştır. Veriler Arduino üzerinden toplanarak şifrelenmiş ve ethernet arayüzünden yönlendiriciye gönderilmiştir. Böylece fazladan bir platform kullanılmayarak tek noktadan veri gönderim ve alımı gerçekleştirilmiştir. Buna ek olarak haberleşme yapısını oluştururken WEP (Wired Equivalent Privacy) protokolünde bulunan mesaj bütünlük kontrolü, IV (Başlangıç Vektörü) ve RC4 algoritması kullanılmıştır.

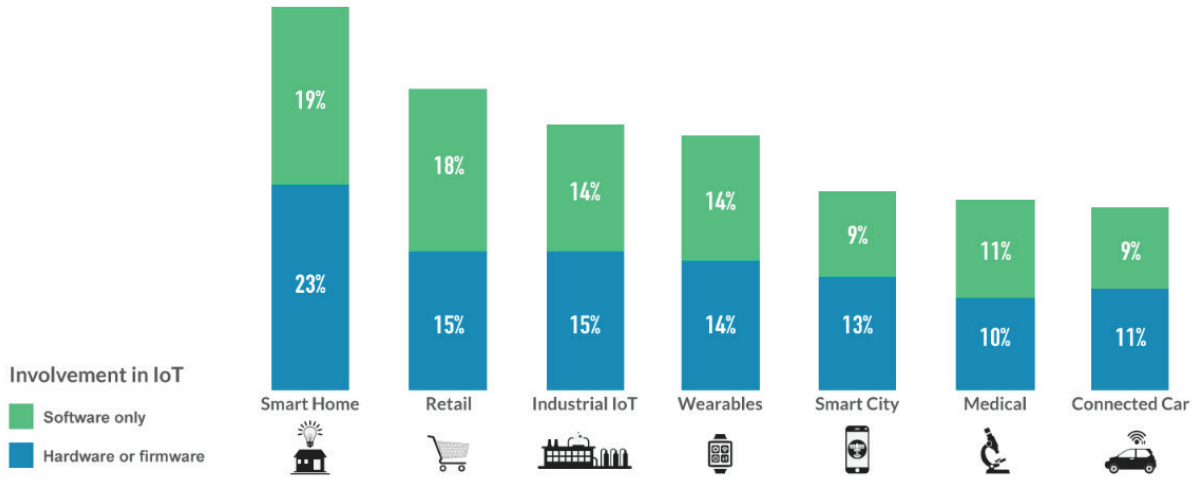
II. NESNELERİN İNTERNETİ TEKNOLOJİSİ

Günümüzde çevresindeki cihazlar ile IP haberleşmesi gerçekleştiren ve karşılıklı veri paylaşımı yaparak akıllı bir ağ oluşturmuş cihazların yaygınlaşması ve bu cihazların birçok uygulamaya dahil edilmesi ile IoT teknolojisi oluşmuştur. IoT teknolojisi sadece bilgisayar ve server gibi cihazların internete bağlanması olarak algılanmamalıdır. Örneğin; RFID cihazları, medikal cihazlar, VoIP cihazları, otomobiller, cep telefonları ve bu çalışma kapsamında inceleyeceğimiz mikrodenetleyici mimarisini kullanan cihazlar da IoT teknolojisi kapsamında kullanılabilmektedir. Kısaca IoT Şekil 2'de görüldüğü gibi çeşitli haberleşme protokolleri sayesinde birbirleri ile haberleşerek akıllı bir ağ oluşturmuş cihazlar sistemidir [4].

Bu cihazlar üzerindeki veri güvenliğinin sağlanması amacıyla verileri uçtan uca şifrelemenin gerekliliği son yıllarda oldukça ön plana çıkmaktadır. Örneğin; iş yerinizde kimlik kontrolü yapılan giriş kapısındaki dahili bir cihazın, kapıdan giren kişilerin kimlik kartlarından okuduğunu ve kişisel bilgileri anlık olarak harici bir sisteme gönderdiğini düşündüğümüzde ilk aklımıza gelen kişisel verilerin güvenli bir şekilde iletilip iletilmediği olacaktır. Giriş yapan kişilerin bilgilerinin çalınarak farklı e-mail adresine gönderiminin sağlanması , dışarıdan bir cihazın verileri dinlemesi ve kişilerin bilgilerini okuması söz konusu olabilmektedir. Bu nedenle IoT ekosisteminde güvenli bir kriptografik yapının kurulması oldukça önem arz etmektedir.



Şekil 2: Nesnelerin İnterneti Ekosistemi [4]



Şekil 3: Nesnelerin İnterneti Teknolojisinin Genel Kullanım Alanları [5]

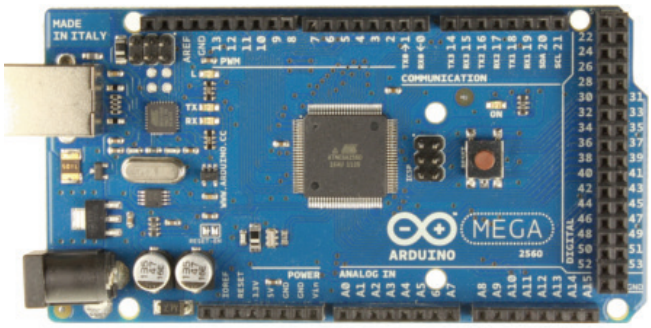
2015 yılının son çeyreğinde yapılan araştırmalarda VisionMobile araştırma şirketinin raporuna göre Nesnelerin İnterneti teknolojisi gelecek vaadeden ve en çok yatırım yapılan Mobil, Desktop ve Cloud uygulamaları ile birlikte ilk 4'te yer almıştır. Nesnelerin İnterneti teknolojisi ile 2015 yılında yaklaşık 10 milyar olan akıllı cihaz sayısının 2020 yılında 50 milyar'a çıkacağı öngörülmektedir Nesnelerin İnterneti teknolojisinin genel kullanım alanları ise şekil 3'te görüldüğü gibi akıllı ev teknolojileri, alışveriş sektörü, endüstride kullanılan sistemler, giyilebilir teknolojiler, şehir içi lokasyon uygulamaları, medikal uygulamalar ve otomobil sistemleri olarak sıralanmaktadır [5].

Günümüzde Nesnelerin İnterneti teknolojisini kullanılarak gerçekleştirilen geniş ölçekli örnek uygulamalar şu şekildedir;

- Köprü ve tren yollarını sensörler vasıtası ile yapısal olarak incelenmesi ve gerekli durumlarda kurumların haberdar edildiği uygulamalarda [6, 7].
- Tedarik zincirinde kritik konumda bulunan üretim donanımlarının yönetiminde [4, 8, 9].
- Tıp teknolojilerinde kullanılan medikal sistemlerin (işitme, kalp ritmi, kan şekeri vb. ölçüm cihazları) takibinde [10, 11].
- Ev otomasyonlarında ışık şiddeti, ısı ayarı, havalandırma, iklimlendirme ve güvenlik donanımlarının kontrolünde [12, 13, 14].
- Hava ve su kalitesi, atosfer ve toprak ölçümleri, afet ve acil durum uyarı donanımları gibi çevresel kalite sistemlerinde kullanılmıştır [15, 16].

İnternet ağı üzerinde veri alışverişi yapabilen tüm cihazlar IoT ekosistemine dahildir. İnternet üzerinden direk olarak veri alışverişi yapamayan fakat çeşitli IO birimlerine sahip cihazlardan aldığımız verilerin, internet ile etkileşimde bulunmasını istediğimizde Arduino ve Raspberry Pi gibi ara cihazlar kullanmamız gerekmektedir. Bu çalışma kapsamında oluşturulan sistemde Arduino cihazı tercih edilmiştir.

Şekil 4'te görülen Arduino Mega platformu, Processing/Wiring dilini kullanan ve üzerinde bulunan fiziksel giriş çıkışların yönetilmesine olanak sağlayan açık kaynak kodlu programlanabilir fiziksel platformdur. Arduino birçok protokol ile uyumlu çalışabilmektedir. Örneğin; Flash, Processing, MaxMSP, C Sharp gibi bir çok yazılım ile entegre şekilde kullanılabilmektedir. Atmel firmasının geliştirmiş olduğu ve Atmega serisi işlemci mimarisine sahip bir fiziksel programlama platformu olup, kullanıcılara çeşitli projeler geliştirme imkanı sunan bir gömülü sistemdir. Bu çalışma kapsamında incelenen Arduino Mega 2560, Atmega 2560 mikrodenetleyici tabanlı bir Arduino kartıdır. Toplamda 54 adet IO pini vardır. Bunlardan 14 tanesi PWM çıkışı 4 tanesi seri port çıkışı, 16 tanesi ise analog girişi olarak tasarlanmıştır. Bunların yanında 16 MHz kristal osilatörü, USB bağlantısı, adaptör girişi, ICSP çıkışı ve bir reset butonu vardır. Arduino'ya fiziksel eklenti eklemek suretiyle yeni fonksiyonlar elde edilebilir. Örneğin, bu çalışma kapsamında internet üzerinden veri alış verişi sağlamak amacıyla Ethernet Shield kullanılmıştır [17, 18, 19].



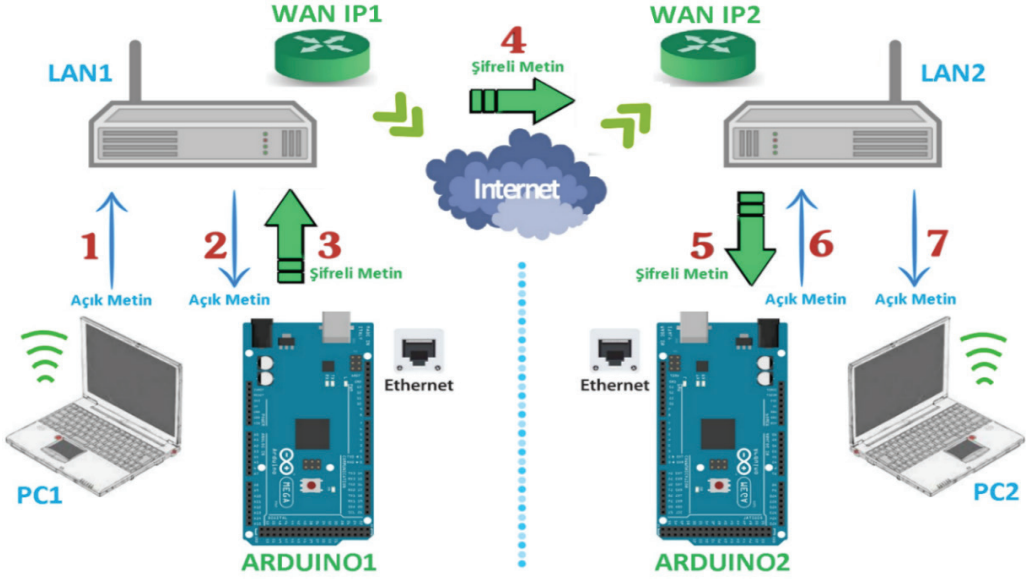
Şekil 4: Arduino Mega 2560 Üstten Görünüş [17]

III. PROGRAMLANABİLİR FİZİKSEL PLATFORMLAR ARASINDA WEP ALGORİTMASI İLE KRİPTOLU VERİ HABERLEŞMESİ UYGULAMASI

Bu çalışma kapsamında, programlanabilir mikrodenetleyici yapısına sahip Arduino cihazı yardımıyla WAN üzerindeki iki noktayı birbiri ile kriptolu bir şekilde haberleştirecek yapının oluşturulması hedeflenmiştir. Oluşturulacak bu yapı birçok IoT uygulamasına uyarlanarak, uzaktan cihaz kontrolü sağlayan sistemlerde bir güvenlik katmanı olarak kullanılabilmektedir.

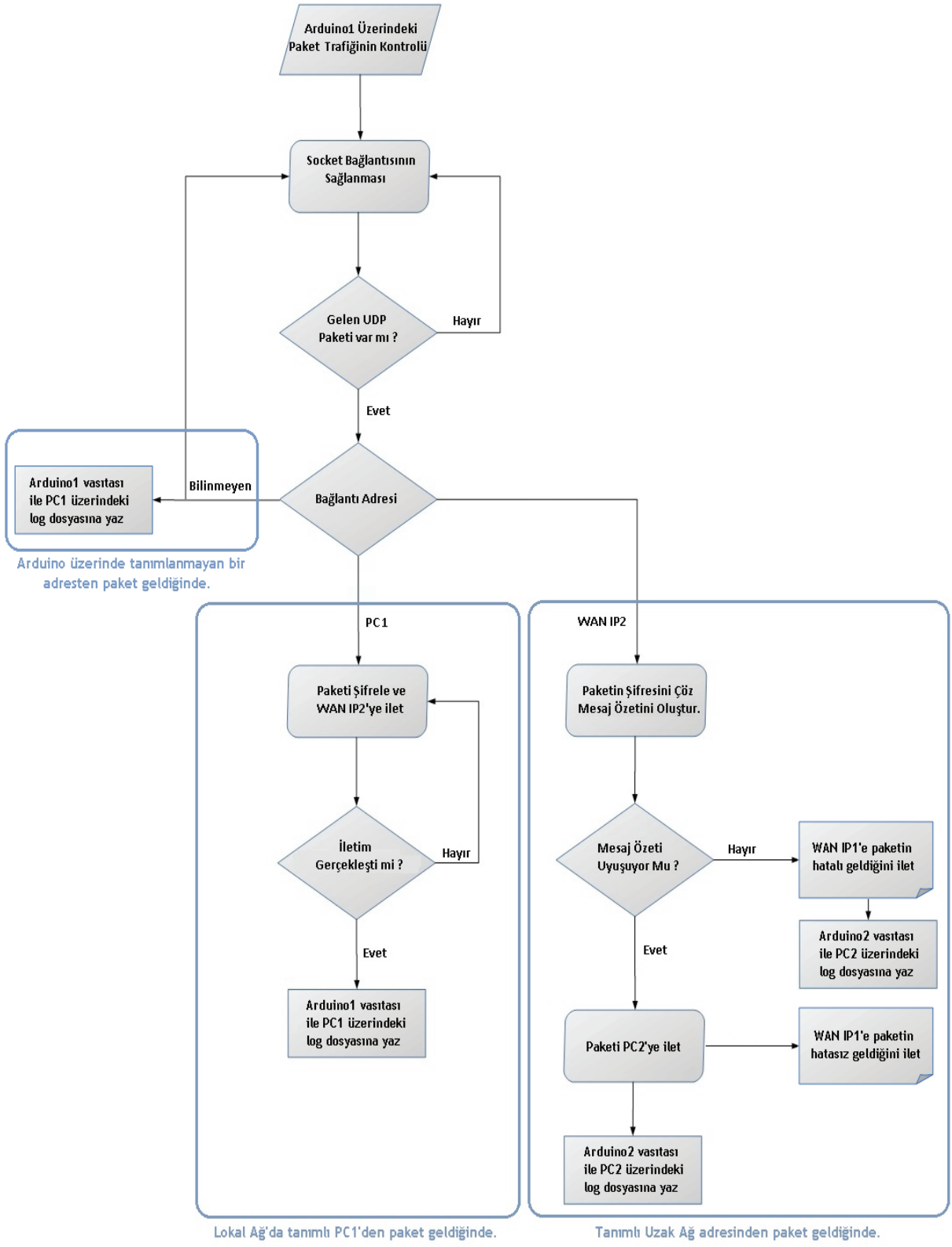
İlk aşamada, WAN üzerinde iki farklı noktada bulunan yerel ağ'lara bağlı programalanabilir fiziksel platformların asenkron veri alışverişi gerçekleştirebilmesi sağlanmıştır. İkinci aşamada, bu platformun üzerinden akacak paket trafiğini IP'lerine göre ayıran ve kriptolama işlemini yapan yazılım fonksiyonları oluşturularak, platform üzerine IDE yardımı ile işlenmiştir. Üçüncü aşamada ise platformun bulunduğu yerel ağda bulunan bilgisayarlara yüklemek üzere bir kontrol arayüzü oluşturulmuştur. Bu arayüz sayesinde cihaza çeşitli uzunluktaki paketler gönderilerek, cihazdan performans verileri ve paket trafiği izlenmiştir. Böylece, WAN üzerinde bulunan her iki ağda tanımlı yönlendirici, bilgisayar ve Arduino cihazlarının yardımıyla güvenli bir veri akışı sağlanmıştır.

Şekil 5'te yerel ağlar arası tek taraflı veri iletimi gösterilmiştir. Tasarlanan sistemde yerel ağlar asenkron haberleştiği için aynı işlem tersi yönde de geçerlidir. Oluşturulan bu sistem, uçtan uca bağlı olan IoT ekosisteminde oluşabilecek güvenlik problemlerine çözüm olarak önerilmiştir.



Şekil 5: Tasarlanan Çözüm Platformu

Sonuç olarak yerel ağa bağlı Arduino cihazlarının görevi, üzerine gelen paketin IP ve Port adresine bakarak paket içeriğini kriptolama veya kriptosunu çözme işlemini gerçekleştirerek paketi gerekli IP'ye yönlendirmektir. Arduino cihazının kendi içerisindeki yazılım yardımıyla gerçekleştirdiği bu yönlendirme modeli şekil 6'daki veri akış diagramındaki gibidir. Bu akış diagramında Arduino devamlı olarak kendi IP'si üzerindeki paket trafiğini dinleyerek, gelen paketin kaynak adresine göre hareket eder. Eğer bilinmeyen bir IP adresinden paket geldiyse bunu yerel ağında bulunan bilgisayara ait kullanıcı arayüzüne iletir. Kullanıcı arayüzündeki yazılım bunu geçmişe yönelik olarak loglar. Eğer yerel ağda bulunan tanımlı bilgisayardan paket geldiyse, Arduino bu paketin şifreleneceğini ve uzak adrese gönderileceğini bilir. Aynı şekilde, uzak adresten bir paket geldiğinde, Arduino uzak adresten paket geldiğini anlayarak gerekli aksiyonları gerçekleştirir.



Şekil 6: Arduino Üzerindeki Veri Akış Diagramı

III.1. **Genel Kriptografi Yapısının Tasarımı**

Programlanabilir fiziksel platformlarda ethernet üzerinden alınan UDP veya TCP paketlerinin ağ üzerinde kriptosuz bir şekilde uzak IP'ye iletilmesi oldukça sakıncalı bir yöntemdir. Bağlantı boyunca yolda bilgiler dinlenebilir, çalınabilir veya değiştirilebilir. Örneğin; Evimizde bulunan cihazların otomasyonunu IoT teknolojisi ile uzaktan gerçekleştiriğimizi düşünelim. Eğer yolda biri bu verileri okur ve cihazlara gönderdiğimiz komutları değiştirir ise bu durum kötü sonuçlar doğurabilir. Gelecek teknolojisinde birçok cihazın bu yöntemle internete çıkacağını düşündüğümüzde, gerekli güvenlik önlemlerini almamız oldukça önemli hale gelmektedir.

Kriptoloji biliminde kullanılan şifreleme algoritmalarının programlanabilir fiziksel platformlara olan uyumlulukları incelendiğinde, donanıma uyarlanabilirliği, değişken işlemlerinin RAM üzerinde kapladığı alan, anahtar uzunlukları ve bir seferde şifrelenecek bit uzunluğu dikkate alınması gereken en önemli konulardır. Asimetrik algoritmalarda iki adet anahtar kullanılması, anahtar dağıtımındaki zorluklar ve donanıma uygunluk, simetrik algoritmalara göre oldukça azdır. Bu nedenle, oluşturulacak kriptografi yapısında simetrik algoritmalar incelenmiştir.

Simetrik algoritmalar içerisinde oluşturacağımız kriptografi yapısına ve Arduino donanımına en uygun olanına karar verme aşamasında anahtar uzunluğunun yüksek olması, hızlı olması ve döngü sayısının fazla olması en ideal seçim olacağından WEP protokolünde kullanılan RC4 algoritması tercih edilmiştir. Tablo 1'de bu çalışma kapsamında incelenen algoritmalar kıyaslanmıştır.

Tablo 1: AES, DES, Blowfish ve RC4 Algoritmalarının Kıyaslanması

Parametreler	AES	DES	Blowfish	RC4
Anahtar Uzunluğu (Bit)	128-256	56	32-448	40-2048
Döngü Sayısı	10, 12, 14	16	16	256
Şifreleme Yöntemi	Blok	Blok	Blok	Akış
Hızın Anahtara Bağımlılığı	Var	Yok	Yok	Yok

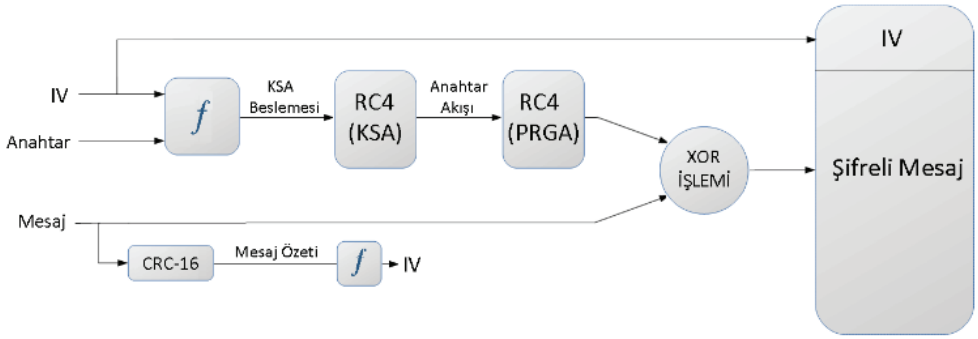
Arduino için kriptografi yapısını tasarlamadan önce kod üzerinde aşağıdaki tanımlamalar yapılmalıdır.

- Maximum UDP paket boyutu,
- IP, MAC, Port, Gateway ve Subnet tanımlamaları,
- TCP/IP haberleşmesi için Ethernet.udp kütüphanesinin eklenmesi

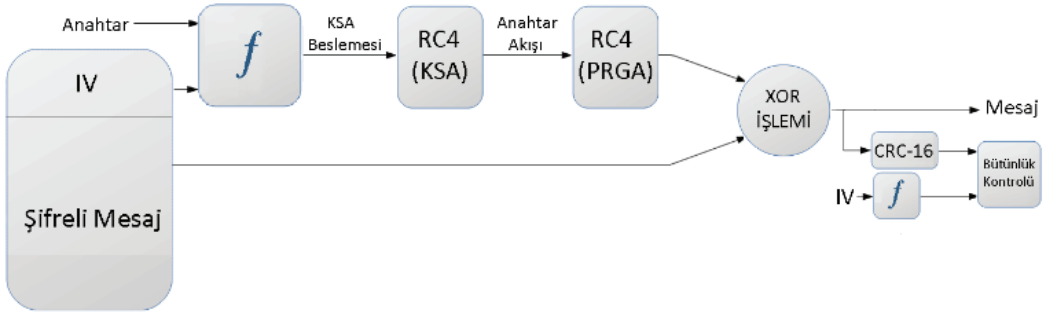
Arduino üzerinde UDP paketi açıldıktan sonra şekil 7'deki gibi kriptolama işlemine sokulur. Kriptola işleminde tasarlanan basamaklar aşağıdaki gibi belirlenmiştir;

- IV(Initialization Vektor) : Gönderilecek her paket içerisindeki mesajın başına eklenir.Birçok oluşturulma yöntemi vardır. Bu çalışma kapsamında CRC-16 algoritmasının çıktısı ile bir fonksiyona girilerek oluşturulmuştur. Ayrıca anahtar ile karıldığı için elimizde IV olmadan şifreli veri çözülememektedir.
- Anahtar: RC4 KSA adımında anahtar akışını oluşturmak için ihtiyaç duyulan ve her iki tarafın sahip olduğu gizli anahtardır.
- KSA Beslemesi: RC4'ün anahtar akışını oluşturmak için aldığı giriş parametresidir.
- RC4 KSA: RC4 algoritmasının ilk kısmı olarak anahtar akışını sağlar. Her mesaj için çıkışında 40 ile 256 bit uzunluğunda bir anahtar oluşturur.
- Mesaj: Kullanıcı tarafından gönderilen veya alınan açık mesajdır. Bu mesaj, ASCII, hexadecimal, decimal, binary veya octal bir değer olabilir.
- CRC-16 Algoritması: Mesaj bütünlüğünü teyit etmek amacıyla kullanılır, gönderilen mesajın özetini çıkarır.
- RC4 PRGA: RC4 algoritmasının ikinci kısmı olarak PRGA(sözderastsal (rastgele) sayı üreteci) işlemini yerine getirir.
- Şifreli Mesaj: RC4 algoritmasının PRGA ile oluşturduğu şifrelenmiş veriyi alınır ve verinin başına IV eklenir.

Kripto çözme işlemi için Şekil 8'deki gibi kriptolama işleminin tersi uygulanır. Burada dikkat edilmesi gereken nokta başlangıç vektörünün UDP içerisindeki şifreli verinin başlığından okunarak elde edilmesidir. Elimizde bulunan gizli anahtar ve başlangıç vektörü vasıtası ile KSA beslemesini elde etmekteyiz. Geri kalan işlemler kriptolama işlemindeki gibi anahtar akışını RC4 PRGA işlemine sokmak ve XOR işlemine tabii tutarak açık mesajı elde etmektir.Açık mesaj elde edildikten sonra CRC-16 algoritması çalıştırılarak mesaj özeti çıkarılır. Son olarak CRC-16 algoritması ile elde edilen mesaj özeti ve başlangıç vektörü ile elde edilen mesaj özeti karşılaştırılarak mesaj bütünlüğü kontrol edilir.



Şekil 7: Tasarlanan Kriptografi Yapısı (Şifreleme)



Şekil 8: Tasarlanan Kriptografi Yapısı (Şifre Çözme)

Şifrelenmiş veri oluşturulduğunda paket tekrar birleştirilir ve Uzak IP'ye iletilir. Yol boyunca paket dinlendiğinde, içerisi okunduğunda ve ya değiştirildiğinde karşıdaki sistem bunu algılar ve gerekli aksiyonu alır. Şekil 7 'de bu çalışma kapsamında oluşturulan Arduino kriptografi yapısının şifreleme aşaması, Şekil 8'de ise şifre çözme aşaması görülmektedir.

III.2. **RC4 KSA Döngüsü ile Anahtar Akışının Oluşturulması**

Anahtar Çizelgesi Algoritması (KSA), başlangıç vektörü ve gizli anahtarın bir fonksiyona sokulması ile elde edilen, 40 ile 2048 bit arasında bir uzunluğa sahip olan anahtarı, bir başlangıç S permütasyonuna dönüştürür. Bu kapsamda KSA, durum ve anahtar akışının yaratılması işlemlerini içerir; bu diziler için iki tane 256 bayt uzunluğunda dizi kullanılır. 256 olası tüm baytlar için permütasyon işlemi yapılır. Permütasyon değişken anahtar uzunluğunun bir fonksiyonudur. Permütasyon işlemi (S) 40 ile 256 arasında değişken bir sayıdaki anahtar ile ilklendirilir. İşlemler sırasında kullanılan 8 bitlik indeks işaretleyicisi, sayıcısı i ve j vardır.

RC4 algoritmasının KSA adımındaki dizi başlangıç atamaları aşağıdaki gibi belirlenmektedir.

S[0], S[1], S[2],……, S[255] - S durum dizisi,

T[0], T[1], T[2],……, T[255] - T geçici vektör,

K, 1 ile 256 bayt arasında değişken uzunluğuna sahip gizli anahtar olarak tanımlanır.

Şekil 9'da KSA adımındaki tüm işlemler gösterilmiştir. KSA ilk aşamada muhtemel kelime değerlerini içeren S durum dizisi ve içerisi anahtar (K) ile doldurulmuş T dizisi oluşturulur (bkz. Eş.1 ve Eş.2).

$S[i]\ i,\ 0 \le i \le 255$, durum dizi ataması **(1)**

$T[i]\ K[\ i \bmod \text{anahtar uzunluğu}]\ ,\ 0 \le i \le 255$ **(2)**

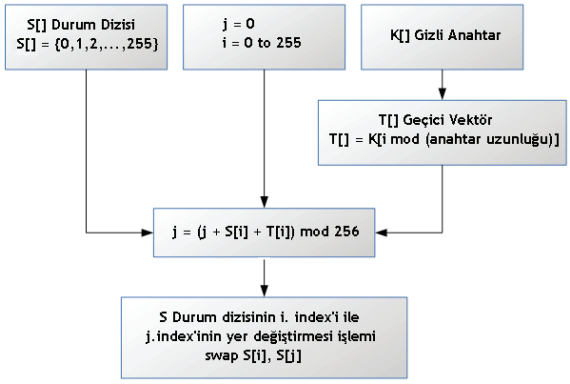
Şifreleme kısmında S dizisinin içeriği rastsal olarak sıralanmış değerler değerler ile değiştirilir. Her bir adımda dizinin i index'i bir arttırılır ve her adımda i index'i ve S dizisi içersindeki i. değer'e bağlı olarak j değeri oluşturulur (bkz. Eş.3).

Şifreleme:

for i = 0 to 255 do

$j = (j + S[i] + T[i]) \bmod 256$ **(3)**

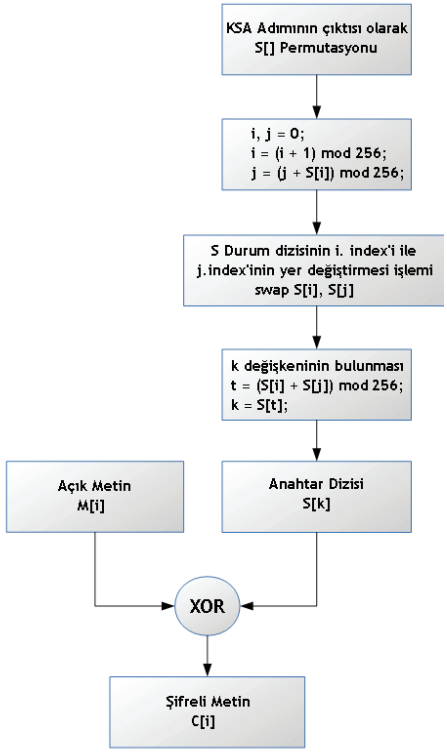
swap S[i], S[j]



Şekil 9: KSA Adımındaki Veri Akışı

III.3. **RC4 PRGA Döngüsü ile Kriptolu Verinin Oluşturulması**

Sözde rastsal üreteç aşamasında (PRGA aşaması), KSA çıktısında ürettiğimiz S permutasyonu kullanılarak şekil 10'daki gibi sırasıyla; i ve j değerleri hesaplanır, S durum değeri içerisinde yer değiştirme işlemi yapılır ve elde edilen k değişkenine bağlı olarak anahtar dizisi oluşturulur. Daha sonra anahtar dizisi düz metin ile XOR işlemine sokularak şifreli metin elde edilir.



Şekil 10: PRGA Adımındaki Veri Akışı

Başlangıç olarak KSA'da olduğu gibi her bir adımda dizinin i index'i bir arttırılır ve her adımda i index'i ve S dizisi içersindeki i. değer'e bağlı olarak j değerini oluşturur (bkz. Eş.4).

$$i, j = 0;$$
$$i = (i + 1) \bmod 256; \quad \textbf{(4)}$$
$$j = (j + S[i]) \bmod 256;$$

Üretme adımında ise sırasıyla S dizisi içerisinde i ve j indexleri yer değiştirilir, index değerlerinin toplamının modundan bulunan sayının karşılık geldiği değer k değerimiz olur (bkz. Eş.5).

$$\text{Swap } (S[i], S[j]);$$
$$t = (S[i] + S[j]) \bmod 256; \quad \textbf{(5)}$$
$$k = S[t];$$

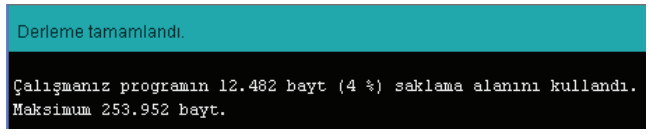
Son adımda ise düz metin ile anahtar dizisi XOR işleminden geçirilerek şifreli metin C elde edilir (bkz. Eş.6).

$$C_1 = M_1 \oplus S[k] \quad \textbf{(6)}$$

IV. **SONUÇLAR VE ÖNERİLER**

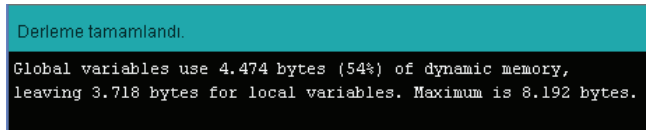
Yapılan bu çalışmada, programlanabilir fiziksel platformlardan biri olan Arduino cihazı yardımıyla internet ağı üzerindeki iki noktayı kriptolu şekilde haberleştirmek amaçlanmıştır. Oluşturulan bu yapı Nesnelerin İnterneti alanına uyarlanarak, uzaktan cihaz kontrolü sağlayan sistemlerde bir güvenlik yöntemi olarak kullanılabilmektedir.

Bu çalışma kapsamında oluşturulan kripto yazılımını, Arduino üzerindeki 256 KB alana sahip Flash RAM'e yüklediğimizde, toplamda 12.482 byte'lık yani %4'lük alanı kaplamaktadır. Şekil 11'de Arduino IDE'nin Flash RAM alanına ait rapor çıktısı görülmektedir.



Şekil 11: Arduino Cihazındaki Flash RAM Kullanım Miktarı

Değişken ve dinamik işlemlerin yapıldığı 8 KB alana sahip SRAM üzerinde ise toplamda 4.474 byte'lık yani %54'lük alanı kaplamaktadır. Şekil 12'de Arduino IDE'nin SRAM alanına ait rapor çıktısı görülmektedir.



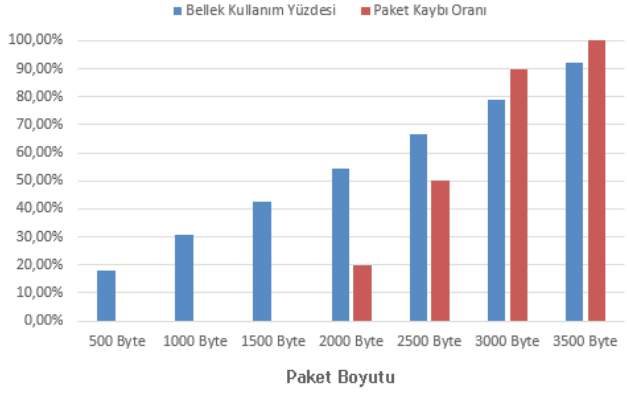
Şekil 12: Arduino Cihazındaki SRAM Kullanım Miktarı

İletilecek ve alınacak max. UDP paket boyutu 1500 byte olarak sınırlandırılmıştır. Bunun nedeni daha sağlıklı veri alışverişi gerçekleştirmek ve SRAM üzerinde kullanılan değişken alanını azaltmaktır. SRAM üzerinde toplamda 4.474 byte'lık alan kullanılmıştır. Gelen ve giden UDP paketi için 1500'er byte'lık toplamda 3000 byte'lık 2 adet değişken tanımlanmıştır. Bunun dışında kalan 1474 byte ise anahtar, geçici vektörler ve sabit değişkenler için kullanılmıştır.

İletilecek ve alınacak max. UDP paket boyutu 1500 byte'ın üzerine çıktığında SRAM üzerinde kullanılan değişken alanı artmakta ve paket kayıpları oluşmaktadır. Tablo 2 ve şekil 13'te Arduino üzerinde yapılan bellek testinin sonuçları görülmektedir. Paket boyutu 2000 byte'a yaklaştığı durumda paket kayıpları başlamakta ve veri iletiminde aksaklıklar yaşanmaktadır. Paket boyutu arttıkça kullanılan belleğin iki kat artmasının sebebi gelen ve giden paketler için bellekte iki ayrı değişken tanımlanmış olmasıdır.

Tablo 2: Arduino Üzerinde İşlenen Paket boyutunun Paket kaybına Oranı

Paket Boyutu	Kullanılan Bellek	Kullanım Yüzdesi	Paket Kaybı
500 Byte	1474 Byte	% 17.99	0%
1000 Byte	2474 Byte	% 30.92	0%
1500 Byte	3474 Byte	% 42.41	0%
2000 Byte	4474 Byte	% 54.61	20%
2500 Byte	5474 Byte	% 66.82	50%
3000 Byte	6474 Byte	% 79.02	90%
3500 Byte	7474 Byte	% 92.24	100%



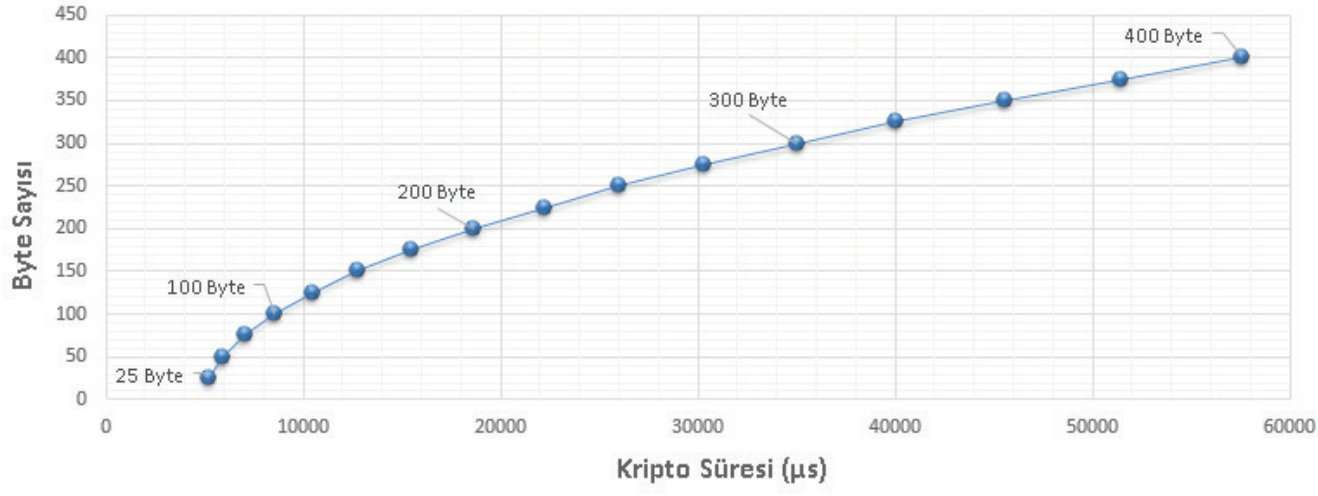
Şekil 13: Test Sonuçlarının Grafiksel Gösterimi

Tablo 3'te ise Arduino üzerinde çalışan RC4 algoritmasını test etmek amacıyla çeşitli uzunluklardaki veriler sıralı biçimde gönderilerek, bu verilerin ne kadar sürede şifrelendiği ölçülmüştür. RC4 algoritması AES algoritması gibi anahtar uzunluğunun hıza bağlı olduğu bir algoritma değildir. Bu nedenle ölçümlerde veri boyutu ve kripto süresi baz alınmıştır. Yapılan testler sonucunda Arduino cihazının saniyede ortalama 13000 byte'lık veriyi paket kaybı olmadan şifrelebildiği görülmüştür.

Bellek kullanımı ve kripto süreleri kullanılan cihazdan cihaza değişmektedir. Bu çalışma kapsamında kullanılan Arduino Mega 2650 dışında Nesnelerin İnterneti teknolojisine dahil olan Raspberry Pi ve Intel Galileo gibi cihazlar için bu test sonuçları farklılık göstermesi beklenmektedir. Bunun nedeni cihazların kullandığı bellek ve işlemci kapasitelerinin farklı olmasıdır. RC4 algoritmasının Arduino Mega 2560 üzerindeki test sonuçları ise şekil 14 ve tablo 3'teki gibidir.

Tablo 3: RC4 Algoritmasının Arduino Üzerindeki Test Sonuçları

Veri Boyutu	Kripto Süresi (µs)
25 Byte	5160 µs
50 Byte	5896 µs
75 Byte	7024 µs
100 Byte	8556 µs
125 Byte	10472 µs
150 Byte	12784 µs
175 Byte	15496 µs
200 Byte	18604 µs
225 Byte	22212 µs
250 Byte	26016 µs
275 Byte	30320 µs
300 Byte	35004 µs
325 Byte	40054 µs
350 Byte	45588 µs
375 Byte	51472 µs
400 Byte	57604 µs



Şekil 14: Test Sonuçlarının Grafiksel Gösterimi

Geçmiş dönemlerde RC4 algoritması WPA (WI-FI Protected Access) uygulamasında kullanılmış fakat kablosuz haberleşme alanındaki kimlik denetimlerine uygun görülmemiştir. Bu çalışma kapsamında kullanılabilecek Arduino, Raspberry Pi ve Intel Galileo gibi cihazların hepsi sıradan bir bilgisayar gibi WI-FI yerine fiziksel olarak Router'a bağlanarak IP alabilirler. Bu nedenle RC4 algoritmasının bu açığından etkilenmezler.

Programlanabilir fiziksel platform üzerinde oluşturduğumuz akış ile internet üzerinden veri alışverişi sağlayabilir, alınan ve gönderilecek veri üzerinde çeşitli işlemler gerçekleştirebilir ve yönlendirme tarzı kurallar belirleyebiliriz. Kullanacağımız cihaz direk olarak router üzerinden internete açıldığı için internetten gelecek bir saldırı ya da cihaz üzerinden fiziksel olarak veri okuma şeklinde oluşacak donanımsal bir saldırı sonucunda şifreleme algoritması çözülebilir ve veriler güvensiz hale gelebilmektedir. Bu durumda cihazlar üzerindeki güvenlik açıklarını belirlemek ve bu açıkları gidermek oldukça önemlidir. Bu kapsamda dikkat edilmesi gereken başlıca unsurlar şu şekildedir:

- SD Kart üzerinde veri saklayan cihazlarda SD Kart'ın çalınması veya kopyalanması durumunda saklanan verilerden kripto yapısı çözülebilir.
- Programlanabilir fiziksel platformların çoğunda veri alışverişi SPI pinleri vasıtasıyla yapıldığı için bu pinler fiziksel yöntemler ile dinlenilebilir.
- Flash RAM üzerine direk olarak müdahale edilerek içerisindeki yazılım çalınabilir.

Bu unsurların dışında, cihaz üzerinde IP ve MAC filtreleme, kriptoloji algoritmalarından faydalanma, kimlik denetimi sağlama vs. gibi güvenlik önlemlerinden en az birinin sağlandığından mutlaka emin olunmalıdır.

Oluşturulan kriptolu haberleşme sisteminden birçok farklı alanda farklı yöntemler ile yararlanılabilmektedir. Örneğin;

- Arduino ile Web sunucusu arasında, güvenli yöntemler ile veri haberleşmesi gerçekleştirilmek istenildiğinde,
- Bilgisayar üzerinden şifreli komutlar vasıtası ile Arduino'ya fiziksel olarak bağlı (IO giriş-çıkış'ları üzerinden bağlı) olan cihazların yönetilmesinde,
- Bilgisayar veya akıllı telefon ile Arduino'ya ait anlık verilerin internet üzerinden kriptolu olarak takip edilmesinde kullanılabilmektedir.

KAYNAKLAR

[1] Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı (2015) Uluslararası Elektronik Haberleşme Sektöründe Gelişmeler Bülteni, Sayı 92, 3-7.

[2] Nathan, S. (2013) International Cryptography Regulation and the Global Information Economy, 8-9.

[3] King, J. (2015) A Distributed Security Scheme to Secure Data Communication between Class-0 IoT Devices and the Internet, 7-22.

[4] Ovidiu, V., Peter. F., (2014) Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, 28-33

[5] VisionMobile IoT Report (2015) http://www. visionmobile. com/ reports/, Son Erişim Tarihi: 02.11.2015

[6] IoTBridge Company (2015) http://www.iotbridge.eu/ technology, Son Erişim Tarihi: 05.01.2016

[7] WIND Company (2014) The Internet Of Trains, 2-3.

[8] DHL Trend Research Company (2015) Internet Of Things In Logistics, 14-22.

[9] Cognizant Company (2014) Designing for Manufacturing's 'Internet of Things', 3-6.

[10] Niewolny, D. (2012) How the Internet of Things Is Revolutionizing Healthcare, 4-5.

[11] Healey, J., Neal, P., Beau, W. (2015) The Healthcare Internet of Things Rewards and Risks, 8-12.

[12] Vinay, S. (2015) Home Automation Using Internet of Things, International Research Journal of Engineering and Technology (IRJET), 21-28

[13] Mamata, K., Neethu K., Jadhav P., Syedali A.R., (2015) Implementation of Internet of Things for Home Automation, International Journal of Emerging Engineering Research and Technology, 6-22

[14] Piyare R., (2013) Internet of Things: Ubiquitous Home Control and Monitoring System using Android based Smart Phone, 2-12.

[15] Intel Company (2012) The Internet of Things and Energy & Environment Policy Principles, 3-4.

[16] Cisco Company (2015) Harnessing the IoT for Global Development, 2-9.

[17] Gupta, P. (2013) Implementing Security in a Personal Security Device, Master Thesis, The University of California Los Angeles , Los Angeles, USA, 9-23.

[18] ATMEL Company (2015) Arduino Ethernet, https://www.arduino.cc/en/Main/ArduinoBoardEthernet/ , Son Erişim Tarihi: 17.02.2016

[19] ATMEL Company (2015) Arduino Ethernet Shield, https://www.arduino.cc/en/Main/ArduinoEthernetShield, Son Erişim Tarihi: 17.02.20