Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 29, No 4, 745-754, 2014

Journal of the Faculty of Engineering and Architecture of Gazi University
Vol 29, No 4, 745-754, 2014

KABLOSUZ ALGILAYICI AĞLARDA GÜVENLİ İZLEME SİSTEMİ TASARIMI

Murat DENER
Fen Bilimleri Enstitüsü, Gazi Üniversitesi, 06500, Ankara, Türkiye
muratdener@gazi.edu.tr

(Geliş/Received: 05.02.2014; Kabul/Accepted: 27.10.2014)

ÖZET

Düşük maliyetli algılayıcı mimarilerindeki gelişmeler Kablosuz Algılayıcı Ağlarını (KAA) yeni ve bilinen araştırma alanı yapmıştır. Bu ağlar çok sayıda sınırlı kapasiteli, kısa mesafeli vericiye sahip, düşük güçlü ve düşük maliyetli algılayıcının kolayca erişilemeyen ve çoğu zaman güvenilir olmayan bir ortama rastgele bırakılmasıyla oluşur. Bu özelliklerin den dolayı KAA'lar sağlık alanlarından askeri alanlara, bir binanın güvenliğinin sağlanmasından orman yangınlarının önceden tespitine kadar çok çeşitli alanlarda kullanılabilmektedirler. KAA'ların kullanıldığı birçok uygulamada algılayıcı düğümler ile izlenilen ortamdan algılanan verilerin analiz edilerek gözlemlenmesine ihtiyaç duyulmaktadır. Bu çalışmada TelosB algılayıcı düğümleri kullanılarak KAA için güvenli bir izleme sistemi tasarımı geliştirilmiştir. Algılayıcı düğümlerin elde ettiği veriler 128 bit şifrelenerek sunucuya gönderilmektedir. Gerçekleştirilen güvenli izleme sistemi sayesinde ortamdan algılanan ışık, nem ve sıcaklık değerleri web ortamında analiz edilerek, görsel grafikler yardımıyla izlenebilmektedir. Bununla beraber, gelişen teknolojiyle kullanımı gittikçe artan akıllı telefonlar yardımıyla da KAA mobil platformlar üzerinden izlenebilmesi mümkün olmaktadır.

Anahtar Kelimeler: Kablosuz Algılayıcı Ağlar, Güvenli İzleme Sistemi, TelosB

A SECURE MONITORING SYSTEM DESIGN FOR WIRELESS SENSOR NETWORKS

ABSTRACT

Developments in cost-effective sensor architectures have made Wireless Sensor Networks (WSNs) a new and popular filed of research. A wireless sensor network is created by randomly placing a large number of limited-capacity, low-cost, low-power sensors with a short range transmitter in an environment which is not easily accessed and mostly unsafe. WSNs are therefore used in a wide range of fields from healthcare field to military field, securing a building to pre-detection of forests fires. The detected data from an environment monitored by sensor nodes need to be analyzed and observed in many applications where a WSN is used. In this study, a safe monitoring system was developed for WSNs using TelosB sensor nodes. The data collected by sensor nodes is encrypted in 128 bit and transmitted to the server. With this safe monitoring system, detected light, humidity and temperature values from the environment are analyzed by web media and monitored by visual graphs. In addition, WSN can be monitored via mobile platforms by means of smart telephones that are increasingly used due to advancing technology.

Keywords: Wireless Sensor Networks, Secure Monitoring System, TelosB

1. GİRİŞ (INTRODUCTION)

Kablosuz Algılayıcı Ağlar (KAA) çok sayıda sınırlı kapasiteli, kısa mesafeli vericiye sahip, düşük güçlü ve düşük maliyetli algılayıcının kolayca erişilemeyen ve çoğu zaman güvenilir olmayan bir ortama rasgele bırakılmasıyla oluşur [1]. Her bir düğüm hesaplama, algılama ve iletişim yeteneklerine sahiptir [2]. Bu düğümler fiziksel bir alanda iş birliği içerisine girerek fiziksel dünyadan öğrendiklerini sanal dünya ortamına taşımaktadırlar [3]. Algılayıcı ağlarda fiziksel dünyadan, çeşitli algılayıcılar yardımıyla algılanan veriler kablosuz bir biçimde kulaktan kulağa olarak adlandırılan işbirliği yöntemiyle hedefleri olan bilgi

işlem ağına aktarılmaktadır. Bilgi işlem ağına olan geçit Baz istasyonu olarak adlandırılmaktadır. Bu istasyon hem algılayıcı düğümleri hem de haberleşme ağı ile iletişim kurabilen özel bir düğümdür. Baz düğümü enerji problemi olmayan statik ve hesaplama kabiliyeti yüksek bir düğüm olarak kabul edilir. Algılayıcı düğümleri ise kablosuz ve genellikle radyo teknolojisi ile iletişim kuran, enerji ve hesaplama kabiliyetleri kısıtlı birimlerdir. Bu birimler algılama alanındaki bazı durumları ve olayları algılamak ve takip etmek amacıyla otomatik olarak yerleştirilmekte ve kurulmaktadırlar. Sayıları ise uygulamaya göre yüzlerce hatta binlerce olabilmektedir. Küçük boyutlara sahip olmaları ise kullanılabilirlik açısından fiziksel bir gereksinimdir. Gözlem yapılacak ortama rasgele dağıtılabilen bu düğümler, birbirlerini tanıyabilmekte ve ortak gayret sarf ederek geniş bir alanda ölçüm vazifesini gerçekleştirebilmektedir. Bu özelliklerinde dolayı çok çeşitli alanlarda KAA'yı görmek mümkündür [4].

Savaş alanlarının gözetim altında tutulması, düşman hareketlerinin izlenmesi, arazi hakkında keşifte bulunmak, personel ve askeri araçların takip edilmesi, dost kuvvetlerin izlenmesi ve hedeflerin hız ve konumlarının tespit edilmesi gibi Askeri uygulamalarda, Hava durumu sistemleri, hava kirliliğinin tespiti, Sel, deprem, orman yangını gibi doğal afetlerin takip edilmesi, tarımsal faaliyetlerin izlenmesi gibi Çevresel uygulamalarda, Hastanede bulunan doktorların yerinin tespit edilmesi, Hastaların durumlarının takip edilmesi, Yaşlıların gözetim altında tutulması ve Çeşitli sağlıksal parametrelerin takip edilmesi gibi Sağlık uygulamalarında, Araçların izlenmesi ve tespit edilmesi, enerji hatlarının izlenmesi, Küçük çocukların aileleri tarafından takip edilmesi, ışıklandırma kontrolü, trafik ışıklarının kontrolü, yangın sistemleri gibi Ticari uygulamalarda, Zeki ev ortamları ve bina güvenlik sistemleri gibi Ev otomasyon uygulamalarında KAA kullanılabilmektedir.

KAA'ların kullanıldığı birçok uygulamada algılayıcı düğümler ile izlenilen ortamdan algılanan verilerin internet üzerinden gözlemlenmesine ve işlenmesine ihtiyaç duyulmaktadır. Bu çalışmada bu ihtiyacı karşılamak için güvenli izleme sistemi tasarlanmıştır. KAA'da ortamdaki algılayıcı düğümlerin algıladıkları sıcaklık, nem ve ışık değerleri eş zamanlı olarak WEB ve Veritabanı sunucusu üzerinden web ortamında ve mobil ortamda analiz edilebilmektedir.

Makalenin geri kalan bölümleri şu şekilde sıralanmaktadır. 2. Bölümde literatürde KAA için geliştirilen izleme sistemleri ve örnek çalışmalar anlatılmaktadır. 3. Bölümde geliştirilen sistemde kullanılan yazılım ve donanımlardan bahsedilmektedir. 4. Bölümde gerçekleştirilen izleme sistemi detaylı olarak sunulurken, 5. bölümde deneysel sonuçlar, 6. bölümde ise sonuçlar verilmektedir.

2. İLGİLİ ÇALIŞMALAR (RELATED WORKS)

Literatürde KAA'ların izleme sistemi olarak kullanılmasına yönelik çeşitli çalışmalar bulunmaktadır.

GreatDuckIsland [5] projesi Berkeley Üniversitesi ve Atlantis Koleji'nin ortak işbirliği sonucunda gerçekleştirilmiştir. Kuşların yaşam alanı seçimi üzerindeki etkileri, kuşların yuvada bulunma sürelerinin izlenmesi, üreme sezonu boyunca gerçekleşen çevresel değişiklikler ve bu durumların birbiri ile ilişkili olarak deniz kuşlarının davranışlarını nasıl değiştirdiği gibi durumları izlemek için gerçekleştirilmiş bir projedir. Projede 32 adet Mica algılayıcı düğüm aracılığıyla sıcaklık, nem ve atmosfer basıncı değerleri gözlemlenmiştir. ZebraNet [6] projesi, zebraların uzun dönemli hareket şablonları ve türler arası etkileşim bilgilerini elde edebilmek için geliştirilmiştir. Geliştirilen sistem Kenya'da iki zebra türünü incelemek ve konum bilgilerini alabilmek için zebraların boynuna yerleştirilmiştir. Her bir cihaz GPS ünitesi, mikro denetleyici, uzun ve kısa menzilli iki adet verici, yüksek yoğunluklu lityum-ion polimer piller ve bu pilleri şarj edebilmek için gereken güneş panellerinden oluşmaktadır. Algılayıcı düğüm her üç dakikada bir konum bilgisini kaydetmektedir. Sonoma Dust [7] projesi, California eyaletinde bulunan Sonoma bölgesinde 120 adet Mica2dot düğümü kullanılarak gerçekleştirilmiştir. Ortamda sıcaklık, nem ve foto sentetik aktif radyasyon değerleri ölçülmektedir. Projenin amacı sekoya ağaçlarının farklı hava şartları altındaki davranışını izlemektir. Bir diğer projede [8], Ekvatorda bulunan Tungurahua yanardağı gözlemlenmiştir. Algılayıcı düğümler üzerlerinde bulunan düşük frekans hassasiyetli mikrofonlar ile üç gün boyunca patlamakta olan yanardağdan bilgi iletilmiştir, ayrıca Revendator yanardağı ise düğümlere sismik ve akustik algılayıcılar eklenmesi ile 16 gün boyunca izlenmiştir. Buna ek olarak Lofar agro [9] projesinde patases bitkilerinde meydana gelen bakterilerin oluşma süresi analiz edilmiştir. Foxhouse [10] projesinde tilkilerin yaşamı izlenirken, SensorScope [11] projesinde ise buzulların durumu analiz edilmiştir. Bunların dışında bir kamyonun envanter bilgilerinin merkeze gönderilerek izlenmesinin sağlanması, gıda maddelerinin bulunduğu ortamın sıcaklık, nem gibi bilgilerinin sürekli takip edilmesi ve ürün kalitesinin kontrolü gibi ticari uygulamalarda da KAA kullanılmaktadır.

Görüldüğü gibi bu tarz uygulamalarda ortamdaki algılayıcı düğümlerin algıladıkları verileri gerçek zamanlı ve güvenli bir şekilde gönderilmesi, verilerin analiz edilebilmesi, grafiksel olarak gösterilebilmesi ihtiyacı hissedilmektedir.

Bu kapsamda tasarlanan ve geliştirilen birçok veri izleme sistemi vardır. Bu bölümde KAA için tasarlanmış ve geliştirilmiş görselleştirme araçları sunulmaktadır. SpyGlass [12], KAA'da hata ayıklama, değerlendirme ve algılanan verileri görselleştirerek kullanıcıya sunan Java tabanlı bir görselleştiricidir. Ancak bu yazılımda farklı uygulamalar için arayüzün düzenlenebilmesi için Java bilgisine ihtiyaç vardır.
Mote-View [13] izleme yazılımı Crossbow tarafından üretilen bir KAA görselleştirme aracıdır. Kullanıcı ve algılayıcı düğümler arasında bir arayüz sağlar. Mote-View yardımıyla düğümlerden okunan veriler analiz edilebilir, grafik şeklinde görülebilir. Bu yazılımın sadece yerel olarak sağlanması, bununla birlikte yazılımda sadece Mica2 ve MicaZ algılayıcı düğümlerine destek vermesi yazılımın dezavantajlarını oluşturmaktadır. TinyViz [14], TinyOS 1.x sürümüyle birlikte yüklenen bir görsel araçtır. Sistemde düğümlerin hareketleri izlenebilmektedir. Ancak, bu programın yerel olması ve yeni eklentiler yazılabilmesi için Java bilgisine ihtiyaç duyulması programın eksikliklerindendir. TinyViz, TinyOS 2.x. sürümünde yer almamaktadır.
Sure [15], yine Crossbow tarafından üretilen bir KAA görselleştirme aracıdır. TinyOS içerisinde bulunan bir Java uygulamasıdır. KAA'da ortamdan gelen verilerin izlenmesi ve görselleştirilmesi ile kullanıcılara yardımcı olmaktadır. TOSGUI [16], içerisinde barındırdığı birçok modüler bileşen sayesinde KAA ortamını görselleştirerek kullanıcılara sunar. Fakat düğümün donanımına bağımlı olarak çalışır. MSR Sense [17], yine ortamdan topladığı verileri görselleştirerek kullanıcılara ağı izlemesine olanak tanır, fakat görselleştirmenin gerçek zamanlı yapılamayışı ve platforma bağımlı olması yazılımın eksi yönlerini oluşturmaktadır. Bununla birlikte literatürde yer alan MonSense [18],NetTopo [19], Octopus [20], Trawler [21], SNAMP [22], MeshNetics [23], MARWIS [24], WiseObserver [25], SenseView [26], XbowNet [27] veri görselleştirme araçlarının platforma bağlı olmaları, sadece yerel olarak kullanılabilmeleri, sonuçların gerçek zamanlı izlenememesi gibi özelliklerinden dolayı dezavantajları bulunmaktadır.

Gerçekleştirilen çalışmanın yukarıda verilen çalışmalardan farkı özetle şunlardır.

- Kullanıcı internet tarayıcı dışında hiç birşeye ihtiyaç duymadan web ortamında KAA'dan elde edilen bilgileri izleyebilmektedir.

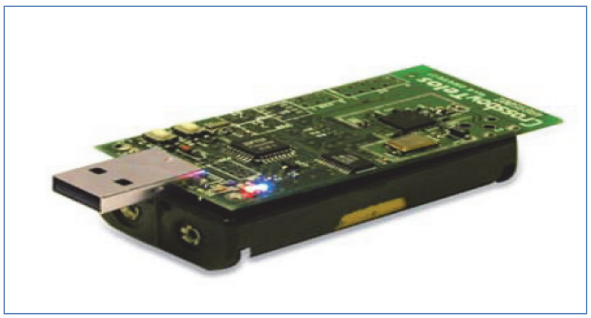
- Aynı zamanda mobil uygulama sayesinde, kullanıcı akıllı telefonuyla zamandan ve yerden bağımsız olarak dilediği zaman KAA'yı takip edebilmektedir.
- KAA'da dolaşan verilerin elde edilmemesi ve güvenli sağlamak için ortamdan algılanan veriler şifrelenerek baz istasyonuna iletilmektedir.

3. KULLANILAN YAZILIM VE DONANIMLAR (USED SOFTWARE AND HARDWARE)

Gerçekleştirilen güvenli izleme sisteminin tasarımında 5 adet TelosB düğümü kullanılmıştır. 1 düğüm baz istasyonu olarak görev yaparken, geri kalan 4 düğüm ise ortamda bulunmaktadır. Bu düğümler içerisinde yüklü olan TinyOS işletim sistemine verilerin gizliliğini garanti altına alabilmek için 128 bitlik XXTEA şifreleme algoritmasına ait modül yazılarak eklenmiştir.

3.1. TelosB (TelosB)

KAA'yı oluşturan algılayıcı düğümler Crossbow fimasından temin edilebilmektedir. Şu andaki mevcut algılayıcı düğümler Mica2, MicaZ ve TelosB sayılabilir. Mica2 ve MicaZ düğümlerini programlamak için programlama kartı gerekmektedir. TelosB düğümü ise doğrudan usb portuna takılıp kullanılabilmektedir. Akademik çalışmalarda en fazla tercih edilen algılayıcı düğümdür. Bu çalışmada bahsedilen avantajlar sebebiyle KAA prototipi oluşturmak için TelosB düğümleri tercih edilmiştir. TelosB [28] düğümü 48 KB kod, 16 KB veri hafızası içeren ve 8 Mhz'de çalışan TI MSP430 mikrodenetleyiciye sahiptir. Kablosuz iletişimi IEEE 802.15.4 uyumlu Chipcon CC2420 alıcı/verici tüm devresini kullanarak gerçekleştirilebilmektedir. Telosb Düğümüne ait resim Şekil 1'de verilmiştir.

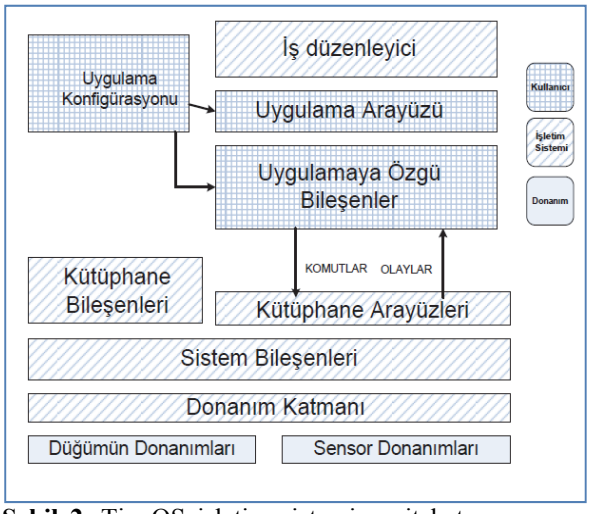


Şekil 1. TelosB Düğümü (TelosB Node)

3.2. TinyOS (TinyOS)

KAA'yı oluşturan bu algılayıcı düğümler içerisinde TinyOS [29] işletim sistemi yüklüdür. TinyOS işletim sistemi, KAA'nın gereksinimlerini karşılayacak şekilde tasarlanmıştır. TinyOS, KAA'da kullanılmak üzere www.tinyos.net sitesinde açık kaynak kodlu olarak dağıtılan bir gömülü işletim sistemidir. California ve Berkeley Üniversitelerinin ve Intel'in iş birliği ile geliştirilmesine başlanmıştır. Daha sonraları gelişerek TinyOS Alliances adında uluslararası bir birlik kurulmuştur. TinyOS işletim sistemi, C programlama dilinin bir varyasyonu olan Nesc programlama dili ile yazılmıştır. Klasik işletim sistemlerinden farklı olarak, işletim sisteminde çekirdek ve kullanıcı uygulamaları diye bir ayrım bulunmamaktadır. Bu yapı, programının tamamının

analizinin ve eniyilemenin daha etkin bir şekilde yapılabilmesine olanak sağlar. TinyOS işletim sistemi, güç tüketimini azaltmak ve çalışma ömrünü arttırmak için "acele et ve uyu" diye bilinen bir strateji izler. Bu strateji, olabildiğince az güç harcamak için mikrodenetleyicinin mümkün olduğunca uyuması prensibine dayanır. TinyOS işletim sisteminin nesneye yönelik olan yapısına ek olarak, TinyOS işletim sistemine özgü bir bileşen mimarisi vardır. Bileşen mimarisi, modüler ve kolayca birleştirilebilir bir şekilde geliştirilmiştir. Bileşen mimarisi, uygulama geliştirici için, birbirinden bağımsız bileşenleri kendi uygulamasına özgü bir şekilde bağlayarak, kolayca yeni bir uygulama geliştirmesine olanak sağlayacak şekildedir. Başka bir deyişle, TinyOS işletim sisteminde geliştirilen bir uygulama aslında o uygulamada kullanılan bileşenlerin listesi ve bunların birbirine bağlantılarını gösteren konfigürasyon dosyalarından oluşur. TinyOS işletim sisteminde her bir bileşen kendisine ait komutları ve olayları içerir. Bileşenin oluşturabildiği olaylar ve yürütmek için başka bileşenlere gönderdiği komutlar da genel olarak o bileşenin arayüzü olarak tanımlanır. Her bir bileşen Görevler, Komutlar, Olaylar, Yerel değişkenler ve yerel fonksiyonlar olmak üzere dört bölümden oluşur. NesC [30] programlama dilinde Modüller ve Konfigürasyonlar olmak üzere iki tip dosya bulunur. Modüller, modüllerin dışarıya verecekleri servisleri ve dışardan alacakları servisleri içeren arayüz tanımlarını içermektedir. Konfigürasyonlar ise, bileşenlerin birbirleri ile olan ilişkilerini içermektedir. Arayüzler ise bir bileşenin başka bileşenler ile olan ilişkilerini düzenlemektedir. Bu ilişkiler hizmet verme veya hizmet alma şeklinde olabilmektedir. TinyOS işletim sistemine ait katman yapısı Şekil 2'de verilmektedir.



Şekil 2. TinyOS işletim sistemine ait katman yapısı (The layer structure for TinyOS operating system)

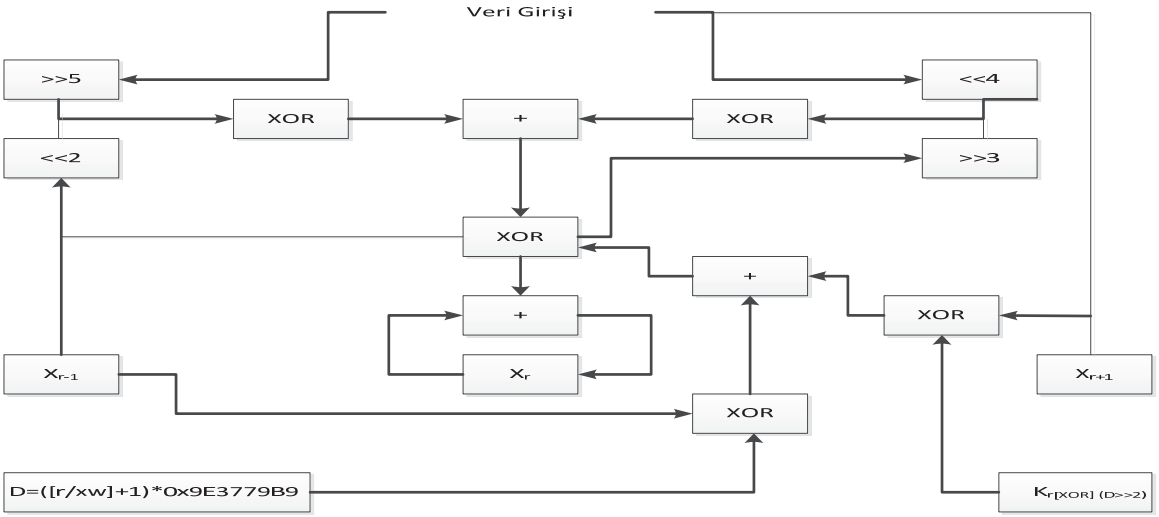
TinyOS işletim sistemi sayesinde algılayıcı düğümlere istenen özellik kazandırılabilir.

3.3. XXTEA (XXTEA)

Algılayıcı düğümlerin donanımsal kısıtları, kablosuz iletişim ortamı, gerçek zamanda işlem ihtiyacı, heterojen yapısı, düğüm sayısının fazlalığı, ölçeklenebilirlik ihtiyacı, gezginlik, uygulama ortam şartlarının ağırlığı ve maliyet gibi hususlardan kaynaklanan nedenlerle KAA pek çok güvenlik açığıyla karşı karşıyadır. Güvenliğin temel hedefi olan gizliliğin sağlanması, zaman ve hayati önemdeki amaçların gerçekleştirilebilmesi için çözülmesi gereken en önemli problemlerden birini oluşturmaktadır [31]. Düşman hatlarının gözetlenmesi ya da sınır bölgelerinin gözetlenmesi gibi hassas KAA uygulamalarında, algılayıcılardan baz istasyonuna gizli veri aktarımını sağlayan güvenlik protokolleri mutlaka kullanılmalıdır [32].

Veri gizliliği KAA'larda, toplanan veriye yetkisiz kişilerin erişiminin engellenmesini garantiye almaktadır ve hassas KAA uygulamalarında en önemli gereksinimden biridir. Bir algılayıcı düğümün çevreden okuduğu verileri komşularına sızdırmaması gerekir. Özellikle askeri uygulamalarda düğümlerde depolanan veriler çok hassas olabilir. Ayrıca birçok uygulamalarda düğümler çok hassas verileri, (örneğin, anahtar dağılımı) kablosuz iletim ortamı üzerinden diğer algılayıcı düğümlerine aktarmak zorundadırlar. Bunlara ilaveten yönlendirme verileri de kötücül düğümlere karsı gizli tutulmalıdır. Çünkü kötücül düğümler bu verilerden yararlanarak ağın performansını düşürebilirler. Bu nedenlerle KAA'larda veri aktarımı için güvenli bir iletişim kanalı oluşturulması çok önemlidir. Hassas verileri gizli tutmak için standart yaklaşım, verinin bir gizli anahtar ile şifrelenmesidir. Düşük enerji tüketimlerinden dolayı KAA' larda gizli anahtar altyapısına dayalı şifreleme algoritmaları kullanılmaktadır. Bu çalışmada ise literatürde enerji-gecikme-güvenlik kriterleri açısından en verimli algoritma olarak bilinen XXTEA algoritması kullanılmıştır [33]. Block TEA(XTEA) algoritmasının zayıf yönleri düzeltilerek dizayn edilmiştir. Cambridge Üniversitesinden Roger Needham ve David Wheeler bu algoritmayı geliştirmişlerdir. Algoritmayı tanıtan makale 1998 yılında yayınlanmıştır. XXTEA [34-37] algoritmasına ait özellikler aşağıda verilmiştir.

Anahtar boyutu = 128 bit, Blok uzunluğu = 64 bit, Döngü sayısı = 32, Güvenlik = 2076 yılına kadar, Bilinen atak = Yok. XXTEA, 8 aşamadan oluşur. 4. aşamadan 8. aşamaya kadar olan kısım 32 kere tekrarlanır. XXTEA, sola kaydırma, sağa kaydırma, toplama ve XOR operatörlerini kullanan bir algoritmadır. XXTEA'da bir turda yapılan işlemler Şekil 3'de gösterilmiştir.



Şekil 3. XXTEA Şifreleme Algoritması (XXTEA Encryption Algorithms)

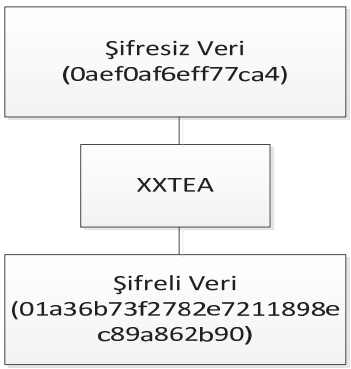
XXTEA'da yapılan işlemler aşağıda anlatılmıştır.

- Öncelikle giriş parametreleri ayarlanır.
- Şifrelemede kullanılacak 128 bitlik anahtar belirlenir.
- Şifrelenecek mesaj 64 bitlik bloklara ayrılır.
- Son mesaj 64 bit olana kadar 0 eklenir.
- Sum değeri 0'lanır.

Ardından 32 kere aşağıdaki işlemler tekrarlanır.

- Sum değeri ile Delta değeri toplanır. (sum += DELTA)
- Yandaki işlem ile e değeri belirlenir. (e = (sum >> 2) & 3)
- z mesajın ilk bloğu, y mesajın ikinci bloğu, k şifreleme anahtarı olmak üzere bu şekilde tüm mesaj blokları için aşağıdaki işlem gerçekleşir.
- (z>>5^y<<2) + (y>>3^z<<4)^(sum^y) + (k[p&3^e]^z)

Şekil 4'de gösterildiği gibi tüm mesaj blokları şifrelenir.



Şekil 4. Şifreleme (Encryption)

Ortamdan alınan 64 bitlik veri XXTEA algoritması yardımıyla şifrelenerek 128 bitlik hale dönüştürülmektedir.

4. GELİŞTİRİLEN GÜVENLİ İZLEME SİSTEMİ (DEVELOPED SECURE MONITORING SYSTEM)

Geliştirilen güvenli izleme sistemi ait mimari Şekil 5'te verilmektedir.

Gerçekleştirilen güvenli izleme sistemi ortamdaki düğümler, geçit düğümü, sunucular ve kullanıcı olmak üzere 4 bölümden oluşmaktadır.

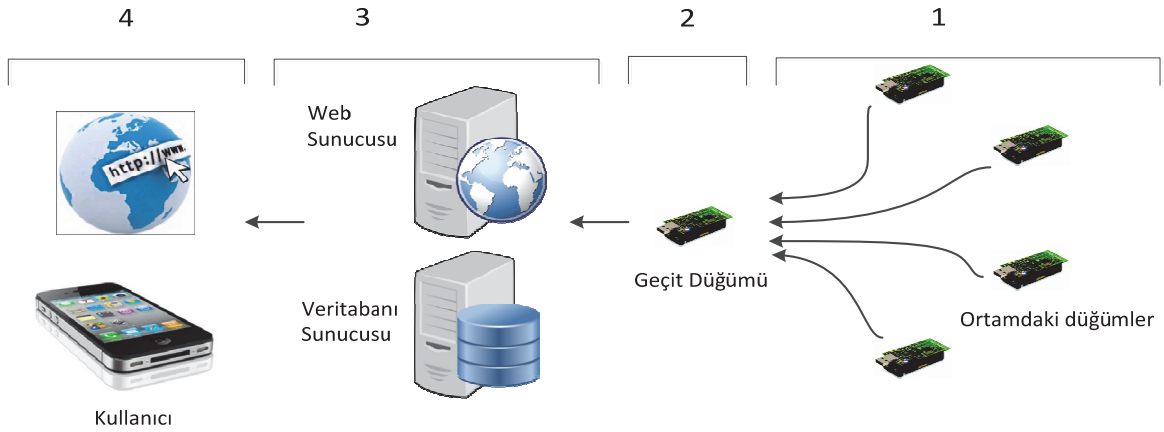
4.1. Ortamdaki düğümler (Nodes in Environment)

Bu düğümler algıladığı verileri XXTEA algoritması yardımıyla şifreleyerek geçit düğümüne göndermektedir. Uygulama dosyası Makefile, Başlık dosyası, Konfigürasyon dosyası ve Modül dosyasından oluşmaktadır. Bu yazılımlar NesC programlama dili ile kodlanıp düğümlere yüklenmiştir. Makefile ile kullanılacak dosya belirlenir.

```
COMPONENT= Environment
include $(MAKERULES)
```

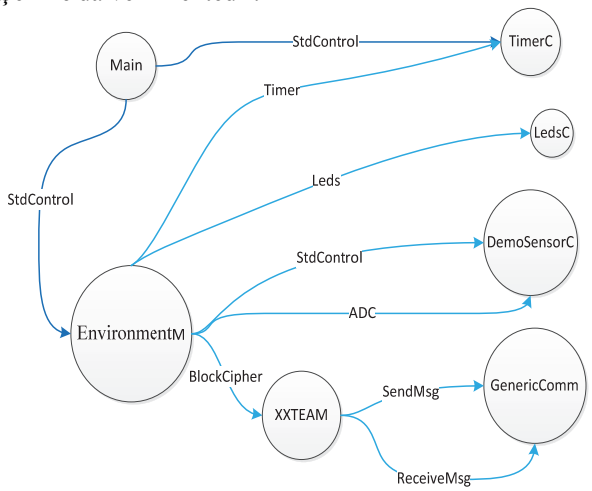
Başlık dosyasında ise baz istasyonuna hangi düğümün veri gönderdiği, verinin tipi ve veri tanımlanmaktadır.

```
typedef struct EnvironmentMsg{
        uint8_t source;
        uint8_t type;
        uint64_t data;
}
```



Şekil 5. Geliştirilen güvenli izleme sistemi mimarisi (Developed secure monitoring system architecture)

Konfigürasyon dosyasında kullanılan bileşenler ve arayüzler vasıtasıyla gerçekleştirilen bağlantılar kodlanmıştır. Konfigürasyon dosyasına ait diyagram Şekil 6'da verilmektedir.

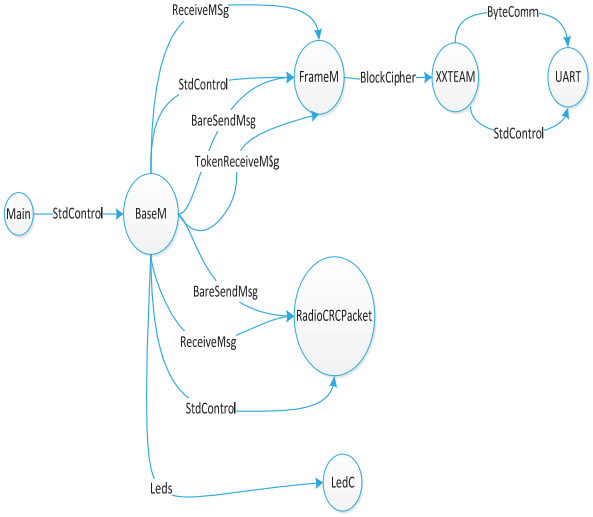


Şekil 6. Ortamdaki düğümler için konfigürasyon dosyasına ait diyagram (The configuration file diagram for nodes in the environment)

Modül dosyasında ise öncelike SensorControl ve CommControl bileşenleri başlatılmıştır. Ardından Timer.fired() olayıyla her 1 sn'de bir düğümün veriyi algılaması sağlanmıştır. dataTask() olarak tanımlanan görev ile veri hazır duruma getirilmiş, şifrelenmiş ve baz istasyonuna gönderilmiştir. Son olarak SensorControl ve CommControl bileşenleri durdurulmuştur.

4.2. Geçit düğümü (Base Node)

Baz istasyonunu ifade etmektedir. Bu düğüm ortamda bulunan düğümler tarafından gönderilen şifreli verileri alır ve şifresini çözdükten sonra asıl veriyi sunucunun seri portuna gönderirler. Uygulama dosyası Makefile, Başlık dosyası, Konfigürasyon dosyası ve Modül dosyasından oluşmaktadır. Bu yazılımlar NesC programlama dili ile kodlanıp düğümlere yüklenmiştir. Konfigürasyon dosyasında kullanılan bileşenler ve arayüzler vasıtasıyla gerçekleştirilen bağlantılar kodlanmıştır. Konfigürasyon dosyasına ait diyagram Şekil 7'de verilmektedir.



Şekil 7. Geçit düğümü için konfigürasyon dosyasına ait diyagram (The configuration file diagram for base node)

Modül dosyasında ise öncelikle Radio ve UART bileşenleri başlatılmıştır. Ardından ortamdaki düğümlerin gönderdikleri veriler alınmaktadır. Alınan paketin şifresi çözüldükten sonra sunucunun seri portuna gönderilmektedir. Son olarak Radio ve UART bileşenleri durdurulmaktadır.

4.3. Sunucular (Servers)

Web ortamında ve mobil ortamda kullanıcıların sisteme ulaşabilmesi için siteye ait dosyalar için depo vazifesi gören ve internet kullanıcılarının erişimine sunan web sunucusu ve geçit düğümü tarafından seri porta gönderilen verilerin tutulduğu PostgreSQL veritabanı sunucusu kurulmuştur. Veritabanına gelen verilerin paket formatı Şekil 8'de verilmektedir.

Şekil 8. Paket formatı (Packet Format)

Toplam paket boyutu, 80 bit TinyOS mesaj paketi başlığı, 8 bit kaynak düğümün adresi, 8 bit algılanan verinin tipi, 64 bit veri ve 16 bit CRC hata ayıklama biti olmak üzere 176 bitten oluşmaktadır.

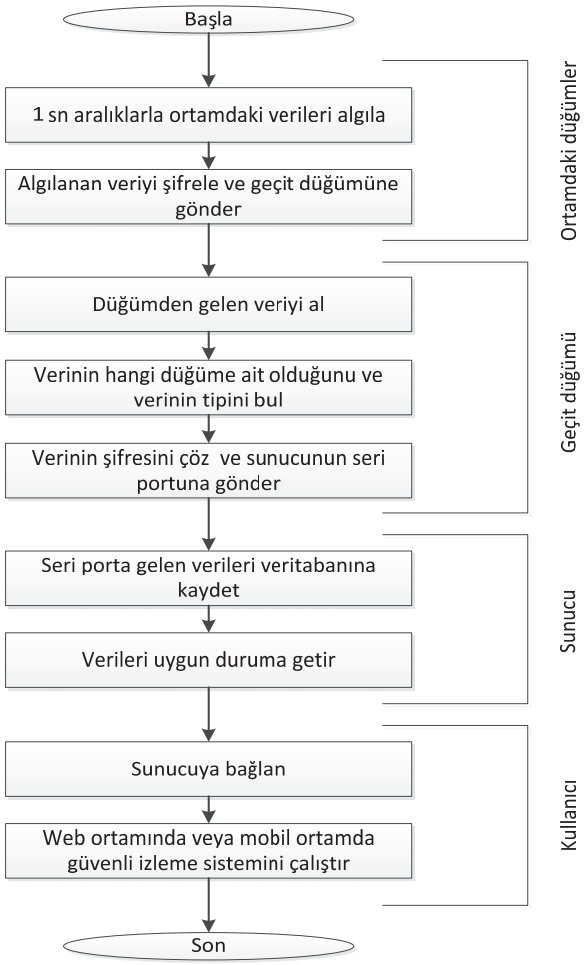
4.4. Kullanıcı (User)

Sunucu yardımıyla ortamdaki düğümlerden gelen gizli verilerin işlenerek ve görselleştirilmiş halini internet üzerinden veya mobil ortamdan görebilmektedir. Gerçekleştirilen güvenli izleme sistemine ait akış diyagramı Şekil 9'da verilmektedir.

Ortamdaki düğümler 1 sn aralıklarla ortamdan sıcaklık, ışık ve nem değerlerini algılayıp, algıladığı verileri şifreledikten sonra geçit düğümüne göndermektedir. Şifreli veriyi alan geçit düğümü, verinin hangi düğüme ait olduğunu ve verinin tipini bulduktan sonra verinin şifresini çözerek sunucunun seri portuna gönderir. Veritabanı sunucusu seri porta gelen veriyi kaydeder. Kaydedilen bilgiler web sunucuya aktarılarak görselleştirilebilir ve analiz edilebilir hale getirilir. Ardından sunucuya bağlanan kullanıcı, web ortamında tarayıcı yardımıyla veya mobil ortamda akıllı telefonu yardımıyla KAA güvenli izleme sistemini kullanabilir.

5. DENEYSEL SONUÇLAR (EXPERIMENTAL RESULTS)

Bu bölümde, gerçekleştirilen güvenli izleme sisteminin web tabanında ve mobil ortamda çalışması sonucunda elde edilen analiz ve görseller sunulmaktadır. Şekil 10'da KAA için geliştirilen güvenli izleme sistemine ait web tabanlı arayüz görülmektedir.



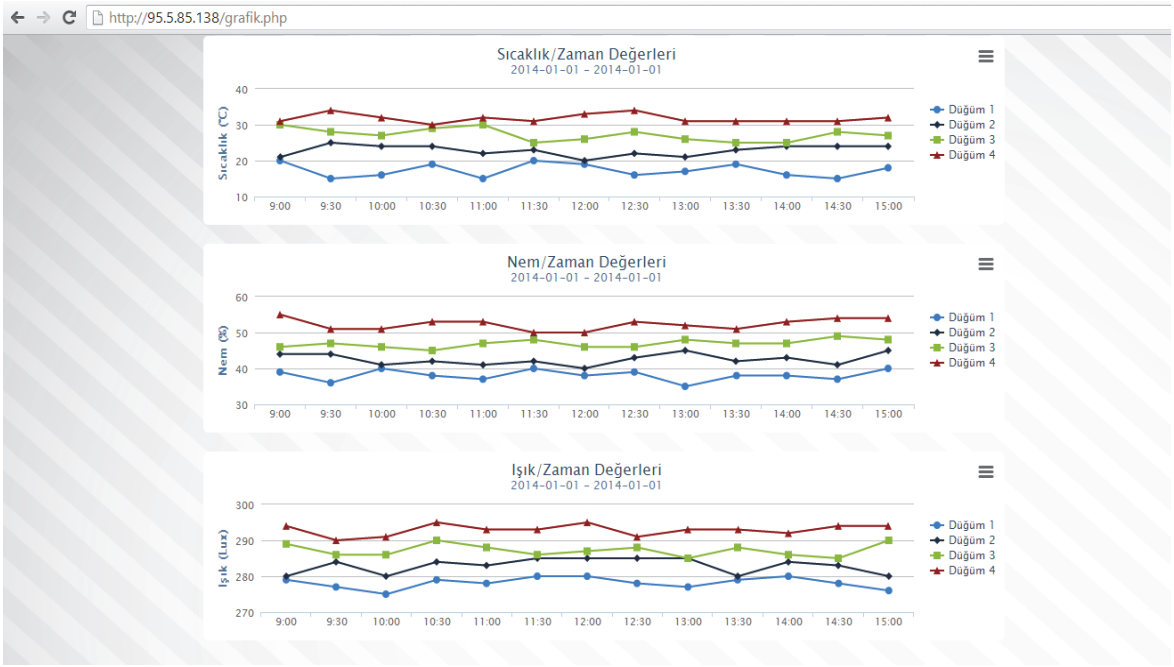
Şekil 9. Gerçekleştirilen güvenli izleme sistemine ait akış diyagramı (The flow chart for developed secure monitoring system)

Şekil 10. Geliştirilen güvenli izleme sistemine ait web tabanlı arayüz (The web based interface for developed secure monitoring system)

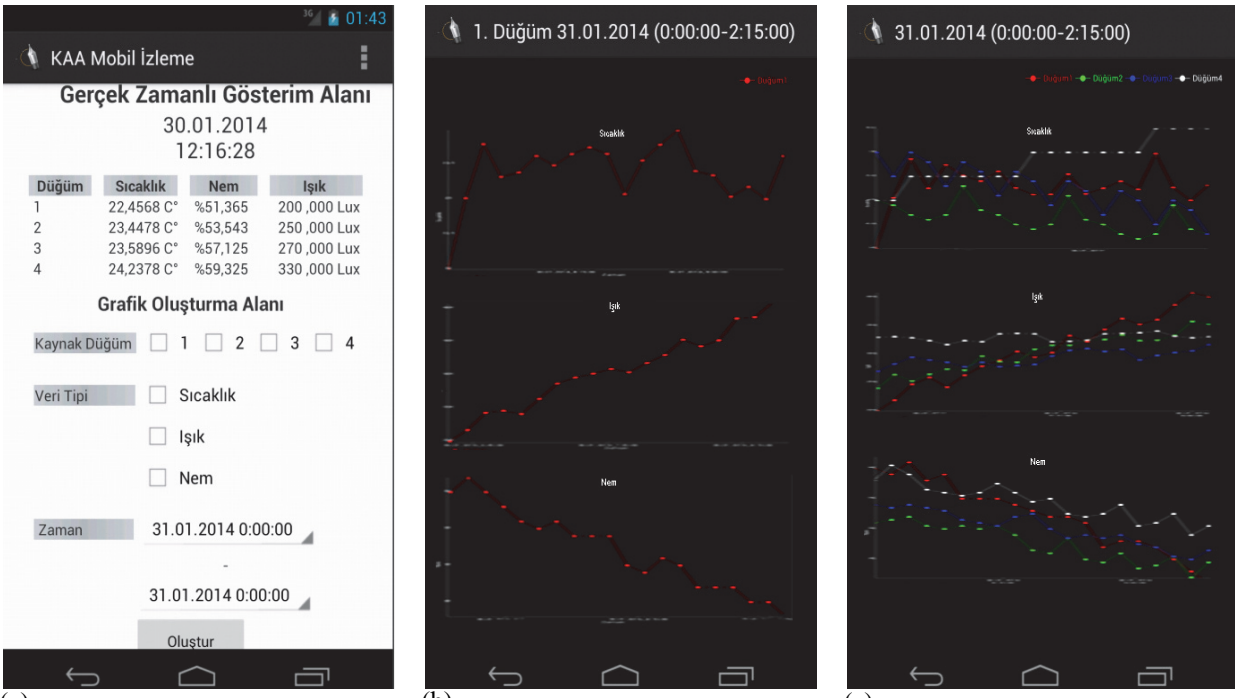
Arayüz iki bölümden oluşmaktadır. İlk bölümde anlık olarak ortamdaki düğümlerden elde edilen sıcaklık, nem ve ışık değerleri görülebilmektedir. İkinci bölümde ise istenilen zaman aralıklarında seçilen düğüme ve özelliğe göre grafik oluşturulabilmektedir. Bu bölümde tek bir düğüme ait bir özellik, tek bir düğüme ait tüm özellikler, bütün düğümlere ait tek bir özellik ve bütün düğümlere ait tüm özellikler gibi kombinasyonlar oluşturarak istenilen bilgiler görülebilmekte ve analiz edilebilmektedir. Şekil 11'de düğüm 1'e ait sıcaklık, nem ve ışık değerleri gösterilirken, Şekil 12'de ise bütün düğümlere ait sıcaklık, nem ve ışık değerleri gösterilmektedir.

Şekillerden de anlaşıldığı gibi geliştirilen sistem algılanan değerlerin grafiklerle gösterilmesine imkân tanımakta ve kullanıcıya esnek bir yapı sunmaktadır. Grafiklerin oluşturulmasında kullanıcının istediği zaman dilimini seçebilmesine olanak tanımaktadır. Karşılaştırma yapmak amacıyla düğümler ve algılanan değerler tek bir ekranda görülebilmektedir. Şekil 13'te ise geliştirilen güvenli izleme sistemine ait mobil tabanlı arayüzler görülebilmektedir.

Şekil 11. Düğüm 1'e ait sıcaklık, nem ve ışık değerleri (Temperature, humidity ans light values for Node 1)



Şekil 12. Bütün düğümlere ait sıcaklık, nem ve ışık değerleri (Temperature, humidity ans light values for all nodes)



(a) (b) (c)

Şekil 13. (a) Geliştirilen güvenli izleme sistemine ait mobil tabanlı arayüz (b) 1. düğüme ait algılanan değerler (c) Bütün düğümlere ait algılanan değerler (a) The mobile based interface for developed secure monitoring system (b) Sensed values for Node 1 (c) Sensed values for all nodes

Şekil 13'te görüldüğü gibi web tabanlı arayüz ile yapılabilen tüm işlemler mobil tabanlı olarak da yapılabilmektedir. (a) da ana arayüz bulunurken, (b) de düğüm 1 ait sıcaklık, ışık, nem değerleri gösterilmektedir. Aynı zamanda seçilen zaman aralığı ekranın üst kısmında verilmektedir. (c) de ise bütün düğümlere ait sıcaklık, ışık ve nem değerleri analiz edilebilmektedir.

6. SONUÇLAR (CONCLUSIONS)

Bu çalışmada WEB ve Veritabanı sunucusu kullanılarak KAA'da ortamda bulunan algılayıcı düğümlerin, ortamdan elde ettikleri sıcaklık, nem, ışık değerlerinin 128 bitlik şifrelenerek web ve mobil ortam üzerinden analiz edilebilmesini, görselleştirilmesini sağlayan güvenli bir izlemi sistemi geliştirilmiştir. Geliştirilen sistem kolaylıkla güncellenerek farklı amaçları olan ve farklı algılayıcı düğüm kullanılan uygulamaların ihtiyacını giderebilmektedir. Önerilen güvenli izleme sistemi KAA algılayıcı düğümlerinin kullanıldığı Askeri, Sağlık, Çevresel, Endüstriyel ve Ev Otomasyonu uygulamalarında kullanılabilir. Bir sonraki çalışmada TelosB düğümüne GSM+GPRS+GSM modül eklenerek ortamdan algılanan değerlerin cep telefonuna sms olarak gelmesi sağlanacaktır.

KAYNAKLAR (REFERENCES)

1. Akyıldız, I.F., Su, W., Sankarasubramaniam, Y., Çayırcı, E., "A survey on sensor networks", **IEEE Communications Magazine**, 40(8), 102-114, 2002.
2. Chong, C.Y., Kumar, S.P., "Sensor Networks : Evolution, opportunities, and challenges", **Proc IEEE**, 91(8), 1247-1256, 2003.
3. Khemapech, I., Duncan, I., Miller, A., "A survey of wireless sensor networks technology", Proceedings of the 6th Annual PostGraduate **Symposium on the Convergence of Telecommunications Networking and Broadcasting**, 2005.
4. Khemapech, I., Duncan, I., Miller, A., "A survey of wireless sensor networks technology", **Proceedings of the 6th Annual PostGraduate Symposium on the Convergence of Telecommunications Networking and Broadcasting**, 2005.
5. Szewczyk, R., Mainwaring, A., Polastre, J., Culler, D., "An analysis of a large scale habitat monitoring application", **In Proceedings of the second ACM conference on embedded networked sensor systems**, Baltimore, 2004.
6. Akyildiz, I.F., Vuran, M.C., Wireless Sensor Networks, **1st ed.: A John Wiley and Sons, Ltd, Publication**, 2010.
7. Tolle, G., Polastre, J., Szewczyk, R., Culler, D., Turner, N., Tu, K., Burgess, S., Dawson, T., Buon-adonna, P., Gay, D., Hong, W., "A Macroscope in the Redwoods", **In Proceedings of the 3rd ACM international conference on embedded networked sensor systems**, San Diego, 51-63, 2005.
8. Werner-Allen, G., Lorincz, K., Welsh, M., Marcillo, O., Johnson, J., Ruiz, M., Lees, J.,

"Deploying a Wireless Sensor Network on an Active Volcano", **IEEE Internet Computing**, 18-25, 2006.
9. Lofar project, http://www.lofar.org/, 2014.
10. Hakala, I., Tikkakoski, M., Kivela, I., "Wireless sensor network in environmental monitoring - case foxhouse", **In Proceedings of the second international conference on sensor technologies and applications**, France, 2008.
11. Barrenetxea, G., Ingelrest, F., Schaefer, G., Vetterli, M., Couach, O., Parlange, M., "SensorScope: Out-of-the-Box environmental monitoring", **Proceedings of the 7th international conference on information processing in sensor networks**, 332-343, 2008.
12. Buschmann, C., Pfisterer, D., Fischer, S., Fekete, S.P., Kröller, A., "SpyGlass: A Wireless Sensor Network Visualizer", **ACM SIGBED Review**, 2(1), 1-6, 2005.
13. Tuton, M., "MOTEVIEW: A sensor network monitoring and management tool," **In Proceedings of Second IEEE Workshop on Embedded Networked Sensors (EmNetSII)**, 11–18, 2005.
14. Levis, P., Lee, N., Welsh, M., Culler, D., "TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications", In Proceedings of SenSys'03, **First ACM Conference on Embedded Networked Sensor Systems**, 2003.
15. Surge Network Viewer, Crossbow Technology Inc.: http://www.xbow.com/Products/productsdetails.aspx?sid=, 2014.
16. Miyashita, M., Nesterenko, M., Shah, R.D., Vora, A., "Visualizing Wireless Sensor Networks: Experience Report," **International Conference on Wireless Networks**, 2005.
17. MSR Sense - MSR Networked Embedded Sensing Toolkit http://research.microsoft.com/nec/msrsense/, 2014.
18. Pinto, J., Sousa, A., Lebres, P., Gonçalves, G.M., Sousa, J., "MonSense - application for deployment, monitoring and control of wireless sensor networks", **Poster in ACM RealWSN'06**, 2006.
19. Shu, L., Wu, C., Zhang, Y., Chen, J., Wang, L., Hauswirth, M., "NetTopo: beyond simulator and visualizer for wireless sensor networks", **ACM SIGBED**, 5, 2008.
20. Jurdak, R., Ruzzelli, A.G., Barbirato, A., Boivineau, S., "Octopus: monitoring, visualization, and control of sensor networks", **Wireless Communications and Mobile Computing**, 2009.
21. Sentilla, "Tmote Invent User's Manual", **Moteiv Corporation**, 2006.
22. Yang, Y., Xia, P., Huang, L., Zhou, Q., Xu, Y., Li, X., "SNAMP: A Multi-sniffer and Multi view Visualization Platform for Wireless Sensor Networks," **IPN Progress Report**, 2005.
23. Meshnetics: "Meshnetics Demonstrated Integration of Wireless Sensor Data with SCADA System", available at: http://www.meshnetics.com/press_releases/MeshNetics_SensiLink_Press_Release_25Jun06.pdf, 2014.
24. Wagenknecht, G., Anwander, M., Braun, T., Staub, T., Matheka, J., ve Morgenthaler, S., "MARWIS: A Management Architecture for Heterogeneous Wireless Sensor Networks", **In Proceedings of the 6th International Conference on Wired/Wireless Internet Communications**, Finland, 177-188, 2008.
25. Castillo, J.A., Ortiz, A.M., López, V., Olivares, T., Orozco-Barbosa, L., "WiseObserver: A Real Experience with Wireless Sensor Networks", **In Proceedings of the 3nd ACM Workshop on Performance Monitoring and Measurement of Heterogeneous Wireless and Wired networks**, New York, USA, 23-26, 2008.
26. Luo, L., Aman, K., Nath S., ve Zhao F., "SenseWeb: Sharing and Browsing Environmental Changes in Real Time", **Microsoft**, 2008.
27. Rowe, A., Berges, M., Bhatia, G., Goldman, E., Rajkumar, R., Soibelman, L., Garrett, J., "Sensor Andrew: Large-Scale Campus-Wide Sensing and Actuation", CMU-ECE-TR-08-11 (A Technical Report), **Carnegie Mellon University**, 2008.
28. İnternet: Willow Technologies "TelosB Datasheet", http://www.willow.co.uk/TelosB_Datasheet.pdf, 2014.
29. İnternet: TinyOS, http://www.tinyos.net/, 2014.
30. İnternet: Wikipedia, "NesC", http://en.wikipedia.org/wiki/NesC, 2014.
31. Kumar, H., Sarma, D., Kar, A., "Security Threats in Wireless Sensor Networks", **IEEE**, 2006.
32. Mohit, S., "Security In Wireless Sensor Networks - A Layer Based Classification", **Cerias Tech Report**, 2007.
33. Devesh, C.J., Dhiren, R., Kankar, S.D., "Optimizing the Block Cipher Resource Overhead at the Link Layer Security Framework in the Wireless Sensor Networks", **Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008,** 2008.
34. İnternet: Wikipedia, "XXTEA", http://en.wikipedia.org/wiki/XXTEA (2014).
35. Wheeler, D., Needham, R.M., "XXTEA: Corrections to XTEA Technical report", **Computer Laboratory University of Cambridge**, 1998.
36. Schneier, B., "Applied Cryptography", Second Edition, John Wiley & Sons, Inc., New York, Ny, 1996.
37. Liu, S., Gavrylyako, O.V., Bradford, P.G., "Implementing the TEA algorithm on sensors" **Proceedings of the 42nd annual Southeast regional conference**, 64–69, New York, NY, USA, 2004.