DİPLOMA PROJESİ

RAPOR - 1

İSTANBUL ÜNİVERSİTESİ

MÜHENDİSLİK FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

Halil Hakan Tarhan
1306010039

KABLOSUZ SENSÖR AĞLAR VE KULLANIM ALANLARI

Mikroelektromekanik Sistemler (MEMS) ve Radyo Frekanslarındaki (RF) hızlı gelişim ; az güç tüketen , ucuz , ağ üzerinde kullanılabilir mikro sensörlerin geliştirilmesini mümkün kıldı.Bu sensör düğümleri çeşitli fiziksel bilgilerin ; sıcaklık , basınç , bir cismin hareketi vs. yakalanmasını sağlamaktadır.Bununla beraber çevrenin fiziki özelliğinin de nicel ölçümlerle eşlenmesini sağlayabilmektedir. [1]

Tipik bir Kablosuz Sensör Ağ (**Wireless Sensor Network** - **WSN**) kablosuz bir ortam aracılığı ile birbirine bağlanmış yüzlerce hatta binlerce sensör düğümününden oluşur.

Sensör düğümleri şu anda 35mm film teneke kutu içerisinde kendi pili, RF adaptörü, mikrokontrolörü ve sensör panosu (board) ile tümleşik bir yapı oluşturur. [2]

Bu düğümler kendi ağlarını kendileri organize ederler, önceden programlanmış bir ağ topolojisi söz konusu değildir.Pil ömrüne bağlı olan kısıtlamalar yüzünden , sensör düğümleri çok büyük bir zamanı düşük güç tüketimi ile "uyku" modunda geçirirler yada düğüm verisini işler.

WSN'ler güvenli izleme için yeni bir paradigma oluşturmuştur, büyük, pahalı makrosensörler kullanan,kullanıcıya kadar kablolamaya ihtiyaç duyan geleneksel sensörlü sistemlerin çok ötesinde bir performans göstermişlerdir .

WSN'lerin sağladığı yararlardan yada artı özelliklerden bazıları aşağıda kısaca açıklanmıştır. [1]

Herzaman heryerde ; Mevcut makrosensör düğümlerinin kapsamı ,maliyet kıstasları ve kurulum(plana göre yerleşim) sebepleriyle belirli fiziksel alanlarda dar olarak sınırlıdır.

Buna zıt bir şekilde WSN'ler insan bakımına gereksinim duymayan fiziksel olarak ayrılmış pek çok düğüm içerebilir. Düğüm bazında bakıldığında tek bir düğümün kapsamı küçük de olsa , yoğun olarak dağıtılmış düğümler eş zamanlı ve iş birliği prensipleriyle çalışabilir, böylece tüm ağın kapsamı genişletilmiş olur.

Ayrıca sensör düğümleri yaşam tehlikesinin olduğu alanlara bırakılabilir ve dört mevsim işlem yapabilir , bu yüzden bu düğümler algılama görevlerini her an yürütebilirler. [1]

Hataya karşı daha fazla tolerans; Bu kazanım WS düğümlerinin yoğun biçimde yerleştirilmesi sonucu sağlanmıştır. Aynı alan içerisinde komşu düğümlerden birbiriyle ilişkili veri alınması sonucunda sistemin hatayı tolere etme şansı , tek başına bulunan bir makrosensöre kıyasla çok daha büyüktür. Eğer bir makrosensör düğümü hata verir yada işlemi durur ise ; sistem, fonksiyonunu sensörün bulunduğu alanda tamamen yitirir. [1]

Bu durumun tam tersi olarak WSN'lerde eğer mikrosensör düğümlerinin küçük bir kısmı hata verirse , WSN kabul edilebilir derecede bilgi üretmeye devam edebilir , çünkü çıkarılan veri gereğinden fazladır. Bundan başka alternatif haberleşme yolları(route) , herhangi bir yönlendirme hatası olduğu takdirde kullanılabilir.

Geliştirilmiş doğruluk oranı: Tek başına bir makrosensör düğümü tek bir mikrosensör düğümünden daha doğru bir ölçüm yapsa bile , çok sayıda mikro düğümün topladığı veririn tek parça haline getirilmesi ile oluşan veri gerçekten dünyanın gerçekliğinden daha fazlasını yansıtabilir.Buna ek olarak ; bu veri , uygun algoritmalar eşliğinde işlenir ve ilişkilendirilir ve/veya kümelenirse genel sinyal geliştirilebilir ve ilişkisiz parazitin bir kısmı temizlenebilir. [1]

Düşük Maliyet: WSN'lerin makrosensörlü sistemdeki eşlerinden(karşıtlarından) daha düşük maliyetli olması beklenmektedir , bu beklentinin sebepleri ; küçültülmüş boyutları , düşük fiyatları ve bunlarla birlikte yerleşim/kurulum aşamasının kolaylığı olarak gösterilebilir. [1]

WSN Uygulamalarından Bazıları

WSN'ler[1] ;

- Sıcakık
- Nem
- Işık
- Basınç
- Nesne hareketleri
- Toprak bileşimi
- Gürültü seviyesi
- Bir nesnenin mevcudiyeti
- Belirli bir nesnenin ; ağırlık , boyut , hareket hızı , yönü , son konumu gibi fiziksel durumları izleyebilirler (monitoring) .

WSN lerin güvenilirlik, kendini organize etme , esneklik ve kurulum kolaylıkları sebebiyle mevcut ve olası uygulamaları geniş bir çeşitlilik kazanmaktadır. Aynı zamanda neredeyse tüm çevre ortamlarında uygulanabilirler , özellikle mevcut kablolu ağların çalışmasının imkansız olduğu yada kullanılamayacağı durumlarda kullanılabilirler örnek olarak ; savaş alanları, atmosferin dışı , derin okyanuslar vb.

Askeri Uygulamalar ; WSN'ler askeri komuta, kontrol, iletişim ,hesaplama, istihbarat, nezaret,keşif ve hedef tespit (C^4ISRT) sistemlerinin ayrılmaz bir parçası olmaya başlamıştır. [1]

Çevre Algılaması ve İzleme : Belirli bir coğrafi alana yayılan yüzlerce yada binlerce , ufak ,ucuz, kendini-ayarlayabilir kablosuz sensörler çevre izleme yada çevre kontrolü işlemlerinde geniş yelpazeli uygulamalarda kullanılabilir. [1]

Felaketten korunma ve kurtarma : WSN'ler belki de acil durumlarda yada felaket durumlarında yerleştirildikleri afet alanlarında etkili olabileceklerdir. Dağıtılmış WSN'ler aracılığı ile yapılan doğru ve zamanında yer tespiti, kurtarma operasyonlarında hayati önem taşır, yer tespitinin yanında ölü sayısı,potansiyel tehlikeler yada acil durumun kaynağı , kimlik tespit işlemleri ve kurtarılmayı bekleyen insanların tespiti de hayati verilerdir. [1]

Tıbbi Hizmetler : WSN'ler zamanında ve etkin sağlık hizmetlerinin sağlanması ile insanlık için daha sağlıklı bir çevrenin oluşturulmasında oldukça yardımcıdır. [1]

Akıllı Ev : WSN'ler tüm insanlık için daha rahat ve akıllı yaşam alanlarının oluşturulmasında rol alabilir.Bu tür uygulamalara örnek verirsek ;
Uzaktan ölçüm: WSN'ler gaz,elektrik, oda sıcaklığı gibi verileri kablosuz ağ aracılığı ile istenen noktaya iletebilir.Ya da parkmetrenin süresinin dolmak üzere olduğunu araç sahibine iletebilir. [1]

Akıllı alanlar : Son zamanlarda teknolojideki gelişmeler sonrasında , çeşitli kablosuz sensörlerin kişisel mobilya yada araçlara iliştirilmesi mümkün kılınmıştır, bu sayede otonom bir ağ oluşturulabilir.Örnek olarak , akıllı bir buzdolabı ailenin doktordan alınan diyet programına göre buzdolabının envanterini tutup , alışveriş listesini tutan kişisel dijital asistana alınacaklar listesini gönderebilir. [1]

Bilimsel Araştırmalar : Etkin bir şekilde yerleştirilmiş ve otomatik işlem yapabilen WSN'ler bilimsel araştırmaların daha yüksek,ileri ve derin ortamlara (uzayın ve okyanusun derinlikleri gibi) açılan yeni kapısıdır. [1]

Etkileşimli Çevreleme: WSN'ler mayın bilgisini toplama konusunda ümit vaad eden mekanizmalar üretmişlerdir. Ucuz ve ufak kablosuz sensörlerin yayılması ile küçük yaştaki çocukların eğitimi güçlendirmek için "akıllı anaokulları" tasarlanabilir , çocukları izleme ve aktivitelerini yönlendirme işlemleri için WSN'ler kullanılabilir. [1]

Nezaret~Gözetim Uygulaması: Anlık ve uzaktan gözetim WSN'lerden esinlenerek geliştirilen önemli uygulamalardan biridir.Örnek olarak ; çok sayıda akustik ağ sensörü ile belirlenen hedeflerin tespiti ve takibi belirli güvenlik kriterlerinin uygulandığı alanlarda kullanılabilir.WSN'ler bu gibi amaçlarla binalara, yerleşim alanlarına, hava alanlarına,tren istasyonlarına vs. yerleştirilerek ziyaretçilerin tanınması

ve anlık olarak ana komuta merkezine iletilmesi gibi görevleri yerine getirebilir.Benzer şekilde duman algılayıcıları evlere , otel odalarına , okullara yerleştirilerek olası kaza , yangın ve felaketlerin farkedilerek en hızlı biçimde gerekli müdahelenin yapılmasını mümkün kılarlar. [1]

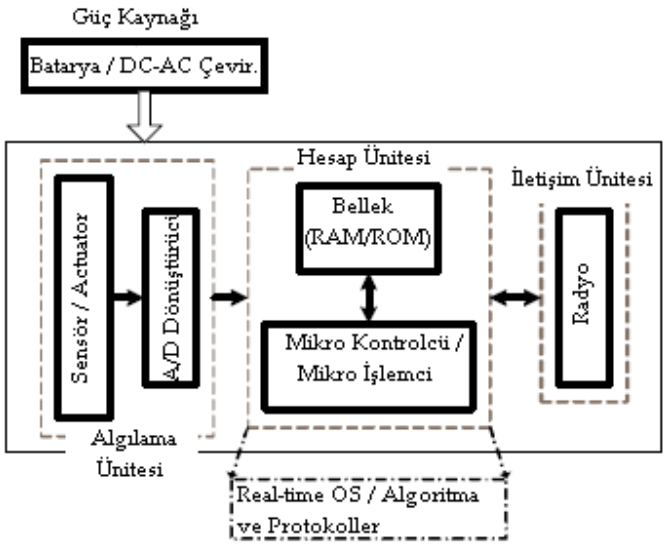
KABLOSUZ SENSÖR AĞLARIN MİMARİ YAPISI

Kablosuz Ad hoc Network'lar , düşük güç tüketen elektronik cihazlar ve kısa mesafe haberleşme sağlayan radyolar , akıllı sensörlerin geliştirilmesi , Sensör Network'ların yayılmasını olası kılan en önemli teknolojik etkenlerdir.
Sensor Network'ların yapısını şu katman/düzeyler altında toplayabiliriz[3];

- SN düğümlerinin üzerinde bulunan bileşenler (işlemci, haberleşme ünitesi, bellek, sensör ve/veya erişim düzeneği ve güç kaynağı)
- Düğüm (node) düzeyi
- Dağıtılmış Network Sistemi düzeyi

Sensor Network Düğümlerindeki Bileşenler[3] **:**

Bu düğümler genelde 6 tip bileşenden oluşur bunlar ; işlemci,bellek ünitesi , güç kaynağı , sensör ve/ veya erişim düzeneği ve son olarak , haberleşme alt sistemi (radyo) . Standart işlemcilerin DSP (Sayısal İşaret İşleme) ile takviye edildiği , yardımcı işlemciler ve ASIC üniteleri ile düşük enerji seviyelerinde çalışabildiği bu sayede yeterli yeteneklere sahip olduğu görünmektedir. Erişim düzenekleri (actuators) çağdaşlık bakımından henüz SN düğümlerinde kullanılabilecek seviyede değildir. Bu sebeple , dikkatler diğer beş bileşen üzerindedir. Şekil-1 de bir Mikro Sensör Düğümünün Sistem Mimarisi karakterize edilmiştir.



Şekil-1

Daha ayrıntılı biçimde bir Sensör Düğümünün bileşenlerinin işlevlerini ve/veya mimari yapısını inceleyelim;

İşlemci[3]**:** Berkeley BWRC araştırma grubu prototip olarak bir işlemciyi tasarlayıp gerçeklenmesini yaptı , bu işlemcinin ana hedef alanına ,kablosuz cihazlar için ses işleme ve ilişkili uygulamalar dahildir.Örnek olarak işlemci, müzede ziyaretçiler ile sergilenen öğeler arasında daha iyi etkileşimi sağlamak için kullanılabilir. Maia işlemcisi ARM8 çekirdeği ve etrafındaki 21 yardımcı işlemci ile geliştirildi. Bu 21 işlemci ; iki MAC , iki ALU , sekiz adres üreteci , sekiz gömülü hafıza ve gömülü düşük-enerjili FPGA içerir. Hedef ; düşük enerji seviyelerinde paralelliği sağlamaktır.ARM8 çekirdeği 32 bit ayarlanabilen bus'ı sayesinde , bellek haritası çıkarılmış uyduları ayarlayabilir , bununla birlikte iki çift I/O portunu kullanıp, uydunun yardımcı işlemcisiyle veri iletimini direkt bellek okuma/yazma işlemlerini uygulayıp sağlar.ARM8 ile uydu yardımcı işlemcisi arasındaki etkileşimler arayüz kontrol ünitesi üzerinden gerçekleştirilir.

Tüm uydular arasındaki bağlantı iki-seviyeli , hiyerarşik, ızgara-yapılı (mesh), yeniden ayarlanabilen network kullanılarak gerçekleştirilir. Bu network , maliyet, güç tüketimi ve sağladığı band genişliği bakımından olumlu bir yapı sağlar. 210 pinli çip 1.2 M transistor içerir ve 5.2 x 6.7 mm lik boyutlara sahiptir, 0.25-µm lik 6 metal CMOS içerisindedir.

Toplam enerji sarfiyatını azaltmak için ARM8 çekirdeği farklı gerilim değerlerinde çalışabilmektedir.Buna ek olarak çift aşamalı , pipeline(ardışık düzen) kullanan MAC (Media Access Control) ve ALU ayarlanabilen bir yapıya sahiptir.Adres üreteçleri ve gömülü bellek ünitesi , hesaplama ünitesine eş zamanlı/ çoklu veri akışı sağlar.Gömülü FPGA 5 girişin 4x8 lik bir dizisini ve üç çıkış CLB lerine sahiptir.Bu , aritmetik işlemler ve veri akış kontrol fonksiyonları için kullanılabilir.Arayüz kontrol ünitesi , senkron ARM8 çekirdeği ile asenkron veri yollarının senkronizasyonunu ve iletişimini koordine eder.Aynı zamanda ARM8 in uyduların ayarlarını yapabilmesini mümkün kılar.Bütün olarak hedeflenen hesaplama modeli, global olarak asenkrondur , lokal olarak senkron hesaplama yapar ve çoklu oran/değer işlemlerini destekler.

Bellek/Depolama ünitesi[3]**:** Sensör Network'un kullanım alanına göre seçilmesi gereken depolama şekli değişmektedir , örneğin anlık veriyi ana düğüme transfer etmesi gereken sistemlerde kullanılacak belleğin kapasitesi ile veriyi uzun zaman aralıkları sonrasında ana düğüme transfer eden sistemlerin bellek gereksinimleri birbirinden farklıdır. İki tip networkta da ana hedef az sayıda bağlantı kurup enerji sarfiyatını az tutmak ve bağlantının süresini olabildiğince kısa tutmaktır. Bazı sistemlerde yapılacak hesaplamalar için depolama ünitesinin kapasitesi önemli bir gereksinimdir. Mikro Disk üzerinde depolama yapan düğümlerde mevcuttur , bunlar nispeten daha büyük fiziksel boyutlara sahiptir.

Bellek seçiminde ilk seçenek giderek azalan maliyetleri ve yüksek kapasiteleri ile flash belleklerdir , ancak bunların aynı fiziksel bölgeye kaç sefer yazma/silme işlemi yapabileceği kuşkuludur. İkinci seçenek , nanoelektronik tabanlı MRAM'lerdir bunların da yakın gelecekte , çok sayıda alanda kullanıma destek vermesi beklenmektedir.

Güç Kaynağı[3]**:** SN'lerin gelişimindeki en büyük kısıtlamanın enerji olduğu bilinmektedir. Enerji kaynağı olarak iki kavram şu anda mevcut durumdadır ;
1.) Sensör düğümünü enerji kaynağı (şarj edilebilir) ile donatmak. Bu şekilde kullanım için iki seçenek mevcut : a.) Yüksek yoğunluklu batarya hücreleri ile donatım b.) Dolu batarya kullanımı . Dolu batarya daha temiz ve yüksel yoğunluklu bir enerji kaynağı olarak kullanılabilir. Ancak SN düğümlerinde kullanılabilecek fiziksel yapıya sahip değiller.
2.)Doğal kaynaklardan enerji üretimi ; Güneş enerjisi ile dolan hücreler yaygın olarak saat, hesap makinesi gibi cihazlarda kullanılmaktadır. Bunun yanında titreşimi enerjiye çeviren kaynaklarda kullanılabilir.Ortamın sıcaklığını enerji kaynağı olarak kullanabilen güç kaynakları üretilmiştir.

Sensör[3]**:** Sensör Network düğümlerinin amacı , hesaplama , analiz yada haberleşme değildir , algılamaktır (sense). Algılayıcı olarak kullanılan düğümlerin ilerlemesindeki en büyük engellerden birisi , algılama bileşeninin(sensör) yarı iletkenlerdeki hızlı ilerlemeyle paralellik sağlayamaması aynı hızla ilerleme kaydedememesidir.Kavramsal sınırlamalar sensörler için işlemci yada depolama ünitelerinden daha belirgin bir öneme sahiptir.Örnek verilmesi gerekirse ; sensörler gerçek dünya şartlarıyla yüzyüze gelmekte , hesaplama üniteleri ise tek bir çip içerisinde kontrol edilmiş bir ortamla karşı karşıyadır.Değiştiriciler (Transducer) sensör düğümlerinde ön uçta kullanılıp , enerjiyi bir formdan diğerine çevirme işini yaparlar.Bunlara ek olarak , sensörler 4 farklı bileşen daha içerebilirler ; Analog,A/D,Dijital ve Mikrokontrolcü.

En basit haliyle bir düğüm sadece değiştirici (Transducer) içerir ,fakat günümüz şartlarında bir düğüme birçok algılama görevi yüklendiği için , düğümlere işleme ve hesaplama üniteleri de eklenir.

Radyo[3]**:** Kısa mesafe radyolarının iletişim bileşeni olarak kullanımı son derece önemlidir çünkü ; enerji sarfiyatında mesaj alma verme – alıcı/verici işlemleri toplam sarfiyat üstünde en etkin kalemlerin başında gelir.

Radyonun dizayn ve seçim aşamasında en az 3 farklı katman dikkate alınmalıdır; Fiziki, MAC , ve Network.Fiziki katman diğer alıcı/verici yada alıcılarla fiziki bağlantıyı kurmakla yükümlüdür. Bu seviyedeki ana görevler ; sinyal kipleme (modülasyon) ve verinin şifrelenerek iletişimin , kanal gürültüsü ve sinyal karışmasından korunmasıdır.Band genişliğini etkin bir biçimde kullanmak ve geliştirme maliyetini azaltmak için yapılması gereken standart uygulama ; birden çok radyonun aynı ortamı

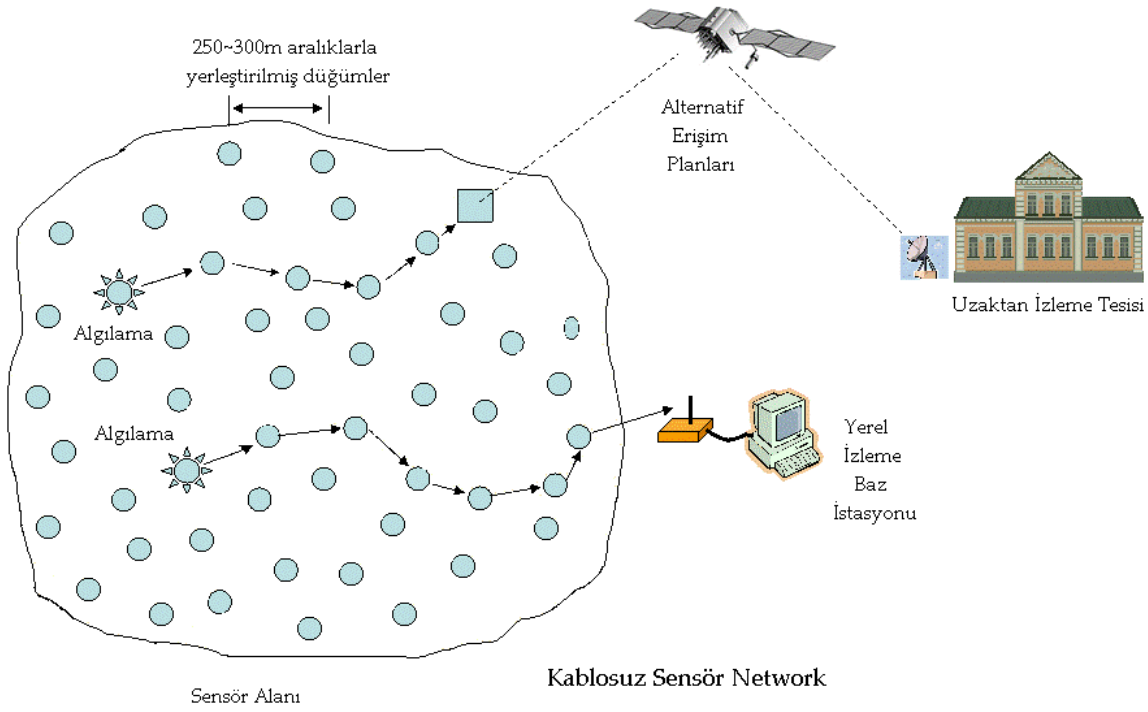
(birbirine bağlı) paylaşmasıdır.Ortamın paylaşımı (zaman veya frekans) MAC katmanı tarafından kolaylaştırılmıştır. Son olarak Network katmanı bir mesajın kaynaktan hedefe transfer edilebilmesi için izlemesi gereken yolun tespitinden sorumludur.

Kablosuz Sensör Network Mimarisi[4]

Kablosuz Sensör Network temel elemanları algılama, veri işleme ve haberleşme özelliğine sahip sensör düğümlerdir. Bilindiği gibi sensör düğümler, herhangi bir kablo olmaksızın, izleyecekleri ortama rastgele saçılmış halde bulunurlar. Şekil-2 bir Kablosuz Sensör Network mimarisini karakterize etmektedir. İzlemenin yapıldığı ortamda toplanan veri genelde 3 seviyede işlenilir[4].

1. İzlenilecek ortamdaki olaylar, sensör düğümler tarafından algılanır. Her bir sensör düğüm elde ettiği veriyi ayrı ayrı işlemektedir.
2. İkinci seviye de her düğüm algılayıp, işledikleri veriyi komşularına yollamaktadır.
3. Sensör ağ haberleşmesinde ki en üst katman, işlenmiş verinin baz (base) olarak adlandırılan merkeze yollanılmasıdır.

Baza gönderilen veri eğer başka kıstaslar eşliğinde tekrar analiz edilecekse yada başka amaçlar için kullanılacaksa bu işlemlerin yapılacağı sistemlere yada merkezlere iletimi sağlanır.



Şekil-2

KABLOSUZ SENSÖR AĞLARDA GÜVENLİK

Giriş[5]

Güvenlik ve Gizlilik birçok WSN (Wireless Sensor Network) uygulamasında aşırı derecede öneme sahiptir.

Bu uygulamalardan bazıları ; savaş alanlarında kullanılan hedef izleme ve takip sistemleri, kanun yaptırımı uygulamaları , otomotiv telemetrik uygulamaları , işyerlerinde odaların izlenmesi, benzin istasyonlarında sıcaklık ve basınç ölüçümleri ve orman yangın tespit sistemleridir.

Tüm bu uygulamalar çok sayıda yarara sahiptir ve geliştirilme potansiyelleri yüksektir; ancak , sensör bilgisi düzgün bir şekilde korunmaz ise ,bilginin yanlış sonuçlara yol açacak şekilde tahrip edilmesi olasıdır.

Sensör Network çalşmaları en hızlı biçimde askeri uygulamalarda kendini göstermektedir , bu alandaki güvenliğin önemi herkesce bilinmektedir.Savaş alanı hakkında bilgiyi , kimsenin hayatını riske atmadan toplayabilmesine karşın , tatmin edici bir şekilde korunmayan WSN'ler düşmanın eline geçtiğinde güçlü bir silah olarak kullanılabilir.Bu tip uygulamalar için sağlam güvenlik önlemleri alınmalıdır.

WSN'lerin ticari uygulamalarında ise "Gizliliğin Korunumu" meselesi , ağın güvenli ve stabil halde çalışır olması kadar önemle ele alınmalıdır.

Kişiler hakkındaki fizyolojik yada psikolojik bilginin güvenliği her kullanıcı tarafından korunması gereken bilgiler içerisindedir.WSN uygulamaları ne kadar yaygınlaşırsa ve karmaşıklaşırsa , bu sistemlerin yetkisiz kullanıcılara karşı korunmasının önemi artacaktır.Sensör Network uygulamaları çok çeşitli fiziksel ortamlarda ve kısıtlamalar altında çalışmaktadır.Sensör network düğümlerinin etkin bir şekilde kullanılması için her uygulama için farklı uyarlamalar ve tasarımlar gerekecektir.Çünkü güvenlik ve gizliliğin sağlanması önemli ölçüde hesaplama ve depolama kaynağının kullanılmasını gerektirir.Güvenliği sağlamak için gerekli mekanizmalar , hedef uygulamanın mimari yapısına ve içinde bulunduğu fiziksel çevreye uygun hale getirilmelidir.

WSN'ler geleneksel kablosuz ağlarla birçok önemli özelliği ortak olarak içlerinde barındırılar özellikle Mobil Ad Hoc ağlarla.

İki tip ağ da kablosuz haberleşme üzerine kurulmuştur, ad hoc ağlar yerleşim ve kurulumu ile ağ topolojisinin sabitlerini değiştirmiştir.

Kablosuz ağlar için önerilen birçok güvenlik önerisi WSN'lere uygulanabilir , ancak , kendine has özellikleri ile WSN ler yeni güvenlik mekanizmalarının oluşturulmasını gerektirmektedir.

Bu kısımda WSN'lere ait dört karakteristik özellik ile ortaya çıkan güvenlik açıkları ve çözüm önerileri anlatılmaktadır.

KABLOSUZ SENSÖR AĞLARIN GÜVENLİĞİNİ TEHLİKEYE ATAN ÖZELLİKLERİ [5]

Aşağıda açıklanan dört özellik ; Düşman Saha, Kaynakların Sınırlılığı , Ağ İçinde İşlem Yapma ve Uygulamaya Özel Mimari Yapı, WSN'lerin güvenliği konusunda dikkat edilmesi gereken özelliklerdir.

Düşman Saha[5]**:**

WSN'ler savaş alanları gibi düşman bölgelere yerleştirilebilir.Bu durumlarda düğümler fiziksel saldırıya karşı korunmasızdır. Güvenlik bilgisi , genelde kaybedilmesi (düşman tarafından tahrip edilmesi) muhtemel düğümlerden alınabilir. Kurcalanamayacak şekilde tasarlanan düğümler düşman sahalarda güvenliğin sağlanması için yapılması gereken işlemlerden biridir. Fakat yapılması gereken bu işlem basitlikten çok uzaktadır , bellek ve hesaplama gereksinimleri açısından kesinlikle pahalı bir işlemdir.Sensör düğümlerinin fiziksel olarak erişiminin mümkün olmasından dolayı , WSN'ler için güvenlik mekanizmaları bir yada daha çok düğümün tehlikeye atıldığı durumlarla ilgilidir.

Kaynakların Sınırlılığı[5]**:**

Sensör ağ düğümleri kompakt bir yapıda tasarlanmıştır bu yüzden boyut,enerji,hesaplama gücü , ve depolama noktasında sınırlıdırlar.Sınırlı kaynaklar gerçekleştirilmek istenen güvenlik algoritmalarını ve protokollerini sınırlandırırlar.
WSN'ler için güvenlik çözümleri ; güvenliğe harcanan kaynaklar ve elde edilen korunma arasından yapılan tercih tarafından tanımlı çözüm alanında işler. Sınırlı kaynaklar , düğümlerin yeni saldırı tiplerine karşı açık hale gelmesine sebebiyet verir örnek olarak : Sleep Deprivation Torture Attack verilebilir.

Ağ İçinde İşlem Yapma[5]**:**

WSN'in kullanılabilir enerjisinin büyük çoğunluğunu düğümler arasındaki haberleşme tüketir , enerjinin küçük bir kısmı algılama ve hesaplama için kullanılır.
Bu sebepten dolayı WSN'ler sınırlandırılmış işleme ve veri toplama gerçekleştirirler.

Bu tip iletişim tarzı için; uygun güvenlik mimarisi anlık komşuluk durumlarında bir grup anahtarının düğümler arasında paylaşılması ile oluşturulur.
Ancak, düğümlerin yakalanmasının olası olduğu ortamlarda ,gizli olarak atanmış paylaşılmış simetrik anahtar tehlike altındadır.

Uygulamaya Özel Mimari Yapı[5]**:**

Yukarıda anlatılan özelliklerinden ötürü WSN'ler uygulamaya göre değişen mimari yapılara sahiptirler.Genel amaçlı mimari yapının esnekliği kaynakların etkin kullanımını gerektirir.

WSN'ler neredeyse her yönden kaynakların tüketimini optimize etme ve performansı yükseltmek için uygulamanın özelliklerine göre ayarlanabilirler.
Bu,ağı dizayn eden kişiye çeşitli güvenlik açıklarını tespit etme ve bu açıklara göre güvenlik mekanizmalarını düzenleme izni verir.

KABLOSUZ SENSÖR AĞLARIN GÜVENLİĞİ İÇİN GEREKSİNİMLER

Bu bölümde kablosuz sensör ağlar tarafından gereksinim duyulan güvenlik özelliklerini ortaya koyacağız.

Dışarıdan Gelen Saldırılara Karşı Dayanıklılık[6]

Bir çok uygulama dışarıdan gelen saldırılara karşı güvenlik gerektirir.Gizlice dinleme (eavesdropping) yada Paket Enjeksiyonu (packet injection) gibi bilinen saldırlara karşı standart güvenlik tekniklerinin seviyesini yükseltmemiz gerekebilir; örnek olarak , şifrelenmiş primitifler kullanarak orjinalliği ve iletişimin gizliliğini ağ içerisindeki düğümler arasında sağlayabiliriz.

Buna ek olarak , düğümlerde meydana gelebilecek hatalara karşı dayanıklı mekanizmalar dizayn etmemiz gereklidir.Bu dayanıklılığa erişmek için büyük miktarlarda düğüm kullanmak ve gerekenden fazla sayıda düğüm bulundurmak (fazlalık) gereklidir böylece birkaç düğümde oluşabilecek hata sonrası sistemin bütünü fazlaca etkilenmez.Ayrıca işlevini kaybeden düğümlerin yerine geçen düğümler dolayısıyla ağın topolojisinde değişim meydana gelecektir , bunu anında farkedip yeni topolojiye göre iletişimi sağlayacak protokollere ihtiyaç vardır.

İç Krizlere Karşı Direnç[6]

Güvenlik-Kritik Sensör Ağlar , tehlike altındaki düğümleri göz önüne alan mekanizmaların üretilmesini gerektirir.İdeal olarak tehlike altındaki düğümleri saptayıp sahip oldukları kriptografik anahtarları geri alabilmeliyiz.Fakat pratikte bu herzaman mümkün değildir.Bu duruma alternatif tasarım yaklaşımı ; düğüm kaybına yada tehlike altında bulunmasına dayanıklı mekanizmalar tasarlamaktır , böylece azar azar sistemin düğüm kaybetmesi sistemin tümden kaybına değilde performansında küçük çaplı düşüşlere neden olur.

Güvenliğin Gerçekçi Seviyesi[6]

Genel olarak güvenliğin gereksinimleri tartışılırken , sensör ağların uygulamadan uygulamaya güvenlik gereksinimlerinin değişim göstereceği

unutulmamalıdır.Örnek olarak tıbbi gözlem cihazlarında insanın vucüduna yerleştirilmiş sensör düğümlerinden hastanın sağlık durumu izlenir , bu durumda güvenliğin amacı hastanın mahremiyetini gizlemektir.Fakat okyanustaki balığın durumunun izlendiği bir uygulamada balığın mahremiyetini gizlemek için bu kadar kafa yormayız.

Veri Gizliliği[6,7]

Bir sensör ağ kesinlikle sensör bilgisini komşu ağlara sızdırmamalıdır.Bir çok uygulamada (örn. anahtar dağıtımı) düğümler çok önemli veri iletirler. Hassas bilginin gizlenmesindeki standart yaklaşım , veriyi sadece planlanan alıcının sahip olduğu gizli bir anahtarla şifreleyip yollamaktır , böylece gizliliğe ulaşılmış olunur.Gözlenen iletişim modellerinde , baz ve düğümler arasında güvenli kanallar kurulur ve gerekli olduğu durumlarda diğer güvenli kanallar sonradan (geç önyükleme) devreye sokulur.

Algılanan verinin gizliliğinin garanti altına alınması veriyi , eavesdropper (kulakmisafiri) tipi saldırılardan korumak için önemlidir.Bunu sağlamak için standart şifreleme fonksiyonları kullanılabilir (örn: AES blok şifreleme) yada gizli bir anahtar iletişim halindeki bölümler arasında kullanılabilir.

Ancak , şifreleme tek başına yeterli bir çözüm değildir, bir eavesdropper alıcıya gönderilen şifreli anahtar üzerinde analiz yaparak , önemli veriye ulaşabilir.

Şifrelemeye ek olarak algılanan verinin gizliliği, baz istasyonlarında yanlış kullanımının engellenmesi için erişim kontrol kurallarına ihtiyaç duyar.

Örnek vermek gerekirse , kişisel yer tespit uygulaması verilebilir.Kişinin yerini tespit eden sensörlerin , algıladıkları veriyi bir Web Server'a yolladığını düşünelim , izlenen kişi , yerinin sadece kısıtlı bir grup tarafından bilinmesini isteyebilir , bu yüzden Web Server da erişim hakları kısıtlandırılmalıdır.

Veri Doğrulama/Kimlik Denetimi[7]

Sensör ağlarda mesaj doğrulama birçok uygulama için önemlidir. Sensör ağın tasarım kısmında, doğrulama birçok yönetici görevleri (örn. ağın yeniden programlanması yada sensör düğümünün iş çevriminin kontrolü) için gereklidir . Aynı zamanda , muhalif yada rakip kişiler kendi mesajlarını kolayca araya sokabilirler. Alıcıların , gelen mesajın yollandığı kaynağı/göndereni doğrulaması gerekmektedir.Veri doğrulama , alıcının mesajın gerçekten belirtilen gönderenden gelip gelmediğini kontrol etmesine olanak verir.

İki taraflı iletişim durumunda , veri doğrulama /kimlik denetimi sadece simetrik bir mekanizmayla sağlanabilir : Gönderen ve alıcı gizli bir anahtarı paylaşır bu anahtar sayesinde tüm haberleşmede kullanılan verinin MAC(Message Authentication Code)'ı hesaplanır.

Doğru MAC değerine sahip bir mesaj geldiğinde , "Alıcı" bu mesajın mesajda belirtilen "Gönderen" tarafından gönderildiğini anlar.

Bu tarzda bir doğrulama sistemi çok daha kuvvetli güvenik kriterleri ağ düğümlerine yerleştirilmediği müddetçe yayın ortamı(broadcast) tipindeki ağlara uygulanamaz.

Eğer güvenilir veri , karşılıklı olarak güvenin sağlanmadığı alıclara yollanmak isteniyorsa , simetrik MAC kullanımı güvenli değildir.Alıcılardan MAC anahtarını bilen biri gerçek Gönderen kimliğine bürünerek diğer alıcılara sahte mesajlar yollayabilir.
Bu yüzden asimetrik doğrulama yayın tipi ağlarda güvenliğin sağlanması için gerekli mekanizmadır.

Veri Bütünlüğü[7]

Haberleşmede veri bütünlüğü , alıcının aldığı verinin art niyetli kişilerce aktarım sırasında değiştirilmediğine karşı garanti verir.
SPINS(Security Protocols for Sensor Networks) ile veri bütünlüğünü , veri doğrulama ile sağlayabiliriz , veri doğrulama daha güçlü bir özelliktir.

Verinin Tazeliği[7]

Sensör ağlar anlık değişen verileri/ölçümleri algılayıp işlediği için , sadece gizlilik ve güvenliğin sağlanması yeterli değildir aynı zamanda her mesajın tazeliğinin de garanti edilmesi gerekir.

Verinin tazeliği verinin yeni olduğunu belirtir ve bu sayede art niyetli kişilerin eski mesajları tekrar göndermediğini garanti eder.
İki tip tazelik tanımlanabilir : zayıf tazelik , kısmi mesaj sırası sağlar, fakat gecikme zamanı bilgisini taşımaz, ve güçlü tazelik , istek-cevap çifti sırasının tamamını sağlar, ve gecikme tahminine izin verir.Zayıf tazelik sensör ölçümlerinde gereklidir, güçlü tazelik ise ağ içindeki zaman senkronizasyonu için kullanışlıdır.

Kullanılabilirlik[6]

Kullanılabilirliği sağlamak , sensör ağın ömrü boyunca fonksiyonelliğini yitirmeden çalışması demektir.DoS (Denial-of-service) saldırıları sık sık sistemin kullanılabilirliğinde kayıplara yol açar.Pratikte kullanılabilirlikteki kayıp ciddi sonuçlar doğurabilir.Üretim gözleme uygulamasında meydana gelebilecek kullanılabilirlik kaybı potansiyel bir kazanın önüne geçilmesini engelleyebilir bu da finansal kayıplara yol açar ; savaş alanındaki kayıplarda ise sonuç düşmanın bir arka kapı açmasıyla sonuçlanabilir.Çeşitli saldırılar sensör ağın kullanılabilirliğini tehlikeye atabilir.Kullanılabilirliğin sağlanması düşünülürken , düğüm kayıpları yada hataları ile sistemin tümden çökmesi engellenmeye çalışılmalıdır.

Hizmet Bütünlüğü[6]

Ağ katmanının üzerinde , sensör ağ genelde çeşitli uygulama-seviyesinde hizmet verir. Veri toplama/kümeleme sensör ağlardaki en yaygın hizmetlerden biridir. Veri toplama işleminde düğümler komşu düğümlerden veriyi alır , veriyi topladıktan sonra

ya baz istasyonuna yada veri üzerinde işlem yapacak olan düğümler varsa o düğümlere iletir.

Güvenli veri toplama göreceli olarak gerçek-dünya verilerinin ölçümünün doğru hesaplanmasını, ve bozulmuş düğümlerden gelen verinin tespit edilip hesaplamalara katılmadan atılmasını sağlar.

Hizmet örneği olarak zaman senkronlama hizmeti de verilebilir. Sensör ağlar için geçerli zaman senkronizasyon protokolleri güvenilir bir ortamın oluşturulmasını sağlar. Mevcut araştırma alanlarından birisi de kaybedilen düğümlerin varlığında zaman senkronizasyonu sağlayacak protokollerin geliştirilmesidir.

SALDIRILAR VE KARŞI TEDBİRLER [6]

Bu bölümde bilindik saldırılara karşı kablosuz sensör ağlarda alınabilecek tedbirleri inceleyeceğiz.

Gizlilik ve Kimlik Doğrulama[6]

Standart kriptografik teknikler eavesdropping, paket tekrarlama,sahte paket yollama gibi dış kaynaklı saldırılara karşı iletişim bağlantılarının güvenilirliğini ve gizliliğini koruyabilir.

Anahtar Tespiti ve Yönetimi [6]

İki sensör düğümünün güvenli ve doğrulanmış bir bağlantı kurması için , gizli bir anahtarın paylaşımının sağlanması gerekmektedir.Anahtar tespit problemi , ağ üzerindeki bir düğüm çifti arasında gizli anahtarın nasıl tespit edilip kurulması gerektiği konusunu irdeler. Saf bir fikir olarak kurulumdan önce gloabal bir anahtarın her düğüme yerleştirilmesi ve kullanılması düşünülebilir , bu düğümlerin kendi aralarında kolayca iletişimine imkan verirken aynı zamada muhalif kişilerin sadece bir düğümün anahtarını ele geçirdikten sonra istediği mesajları istediği düğümlere göndermesini ve veri transferini istediği anda takip edebilmesini sağlar.

Ortak Anahtar şifreleme, anahtar tesbiti için popüler bir metod olarak karşımıza çıkmaktadır, fakat hesaplama için harcanan kaynaklar göz önüne alındığında, düğümlerin sadece kurulum aşamasında bu değer ile ilklenmesine rağmen , birçok uygulama için fazla masraflı bir seçim olur.

Ortak anahtar şifreleme tekniğinin eksiklilerinden birisi DoS saldırılarına karşı ağda açık meydana getirmesidir, saldırgan sahte bir mesajı düğüme gönderebilir , böylece düğüm sadece mesajın sahte olduğunu tespit etmek için imza doğrulama gerçekleştirir bu bile sistemi saldırganın istediği gibi yorar.

Son zamanlarda , araştırmacılar , rastgele anahtar ön-dağıtım tekniklerinin anahtar tespit problemine çözüm üreteceği yönünde önerilerde bulunmuşlardır.

Fakat , mevcut algoritmaların ölçeklenebilirlik, düğüm uyuşmasının esnekliği , bellek gereksinimleri ve haberleşme genel giderleri açısından geliştirilmesi için daha fazla araştırma gereklidir.

Broadcast/Multicast Kimlik Doğrulama [6]

Broadcast ve Multicast birçok sensör network protokolü için zorunludur. Broadcast ve Multicast'de kaynak doğrulama , yeni bir araştırma konusunu ortaya atar.

Olası kazanımlardan birisi sayısal imza kullanmaktır, kaynak her mesajı özel anahtar (private key) ile imzalar ve tüm alıcılar mesajın doğruluğunu ortak anahtar kullanarak kontrol ederler.Ne yazıkki ortak anahtar şifreleme sensör ağlar için çok pahalı bir tekniktir.Bu problemi çözmek için Perrig (ve başka araştırmacılar)güvenli boradcast doğrulama sağlamak için μTesla protokolünü önermiştir bu protokol sensör düğümler arasında gevşek zaman senkronizasyonunu varsaymaktadır.

μTesla'nın arkasındaki temel fikir ; simetrik anahtar şifrelemeye , gecikmiş anahtar açımı ve tek yön fonksiyon anahtar zinciri ile asimetriyi getirmektir.

KULLANILABİLİRLİK ÜZERİNE [6]

Ağın kullanılabilirliği üzerine yapılabilecek saldırılar genellikle DoS saldırısı üzerinden tanımlanmıştır , DoS saldırılarının hedefi ağın farklı katmanları olabilir

Frekans Bozma(Jamming) ve Paket Enjeksiyonu [6]

Frekans bozma farklı katmanları hedef almış olabilir.Fiziksel katmanda saldırgan karıştırıcı RF sinyallerini iletişimi engellemek için yollayabilir. Saldırganın amacı , sensör düğümlerinin pillerini bitirmek için alakasız veri göndermek olabilir.

Fiziksel frekans bozma saldırılarına karşı standart savunma frekans sıçratma ve iletişim spektrumunun yayılmasıdır,bu teknikler saldırganın iletişimin frekansını bozabilmesi için daha fazla enerji harcamasını zorunlu kılar.

Bağlantı katmanı frekans bozma saldırısı MAC (medium access control) protokolünün sağladığı özellikleri sömürür.Örnek olarak , saldırı zararlı çarpışmalara ya da radyo kaynağının hileli paylaşımına neden olabilir.Savunma olarak , güvenli MAC protokollerinin tasarlanmasına ihtiyaç vardır.

Wood ve Stankovic bağlantı frekans bozma saldırısı üzerinde yaptıkları araştırmalar sonucu ; Çarpışma saldırılarına karşı hata düzeltici kodların kullanımını , Tüketim Saldırılarına karşı hız sınırlandırmayı , Haksızlık Saldırılarına (Unfairness attack)karşı küçük yapıların kullanımını önermişlerdir.

Ağ Katmanında ise , saldırgan zararlı paketleri enjekte edebilir . Doğrulama kullanarak alıcının zararlı paketleri saptaması ve anlık mesaj tazeliğinin ölçümü ile tekrarlanmış paketlerin saptanması sağlanabilir.

Sybil saldırısı [6]

Sybil saldırısı ; zararlı bir düğümün gayri meşru bir şekilde birden fazla kimlik talep etmesidir.Sybil saldırısı servisin kesintiye uğratılması için farklı katmanlarda kullanılabilir.

MAC katmanında , zararlı düğüme birden çok kimliğin sağlanması sonucunda,zararlı düğüm paylaşılmış radyo kaynağının büyük bölümünü kendisine ayırabilir , bunun sonucunda normal düğümlerin iletişimi için radyo kaynağının sadece küçük bir kısmı kalmıştır.

Yönlendirme Katmanında , Sybil saldırganı ağ trafiğini aynı niyetteki fiziksel varlık üzerinden geçirilmesi şeklinde yönlendirebilir.

Basit bir yönlendirme protokolü düşünelim, bu protokole göre bir düğüm ,sonraki düğüm olarak eşit olasılıktaki düğümler içerisinden komşu upstream (yukarı akım) düğümünü seçsin.

Çok sayıda kimliğin bir düğüm tarafından istenmesi ile , yüksek olasılıkla seçilen "sonraki" düğüm Sybil kimliğine sahip olacaktır.Bu sebeple oluşan açığı kullanarak saldırgan ,seçmeli gönderme (selective forwarding) yapabilir.

Sybil saldırlarına karşı birkaç savunma tekniği önerilmiş durumdadır. Umut vaad eden kazanımlardan biri anahtar öndağıtım işlemini kullanmaktır.

Temel fikir her düğümün kimlik bilgisini, ona verilen anahtarla ilişkilendirmek üzerine kurulmuştur , böylece A kimlikli düğümü aldatmaya çalışan düğüm A ya karşı gelen anahtara da sahip ise ancak istediği işlemi yapabilir, aksi takdirde ya ağ ile iletişim bağlantısını kuramaz ya da onay aşamasını geçemez.

YÖNLENDİRMEYE KARŞI ÇEŞİTLİ SALDIRILAR [6]

Ağ katmanında , muhalif/düşman kişi yönlendirmenin mevcudiyetini bozmak için çeşitli saldırıları birbirine bağlayabilir.

Yönlendirmenin mevcudiyeti eğer planlanan alıcı mesajı kabul etmez ise gözden çıkarılabilir.Tehlike altındaki düğümler arasında , gerçekleştirilebilecek saldırılardan birisi de paketleri düşürme ya da seçmeli gönderme gerçekleştirmektir.

Çok yollu yönlendirme, bu tür saldırılara karşı yapılacak savunmalardan birisidir.Bu yöntemin temel fikri birbirinden bağımsız çok sayıda yolun bir mesajın yönlendirilmesi için kullanılmasıdır , tüm yolların tehlike altındaki düğümler tarafından kontrol edilmeleri olası değildir.Daha karmaşık saldırılar sahte yönlendirme bilgisinin yayılmasını, sinkhole ve wormhole oluşturulmasını ve "Hello" taşma saldırılarını içerir.

HİZMET BÜTÜNLÜĞÜNE KARŞI GİZLİ SALDIRI[6]

Gizli saldırıda , saldırganın amacı ağın yanlış veri değerini kabul etmesini sağlamaktır.Veri kümeleme/toplama işleminde , yanlış veri değeri yanlış toplama sonucuna sebebiyet verir. Saldırganın bu hedefe ulaşmada kullanabileceği birkaç yol

vardır.Örnek olarak , bozulmuş bir sensör/toplayıcı önemli derece sapmış yada hayali değerler raporlayabilir.

Sybil saldırısı , tehlikeye atılmış bir düğümün toplanmış sonuç üzerinde daha büyük bir etkisinin olmasına izin verir.

Saldırgan ayrıca DoS saldırısı da gerçekleştirebilir , bu yüzden normal düğümler kendi sensör bilgilerini baz istasyonuna raporlayamayabilirler.

Przydatek (ve başkaları) SIA (Secure Information Aggregation) protokolünü gizli saldırılara karşı dayanıklı sistemlerin geliştirilmesi için önermektedir.

Zaman senkronizasyonunu göz önünde tutarsak : gizli saldırganın hedefi yanlış zamabilgisini yayarak düğümlerin senkronizasyonunu ortadan kaldırmaktır.Saldırgan senkronizasyon mesajlarını kesebilir yada geciktirebilir , veya yanlış senkronizasyon mesajları yollayabilir.

Veri kümeleme/toplama durumundakine benzer olarak , saldırgan Sybil ya da DoS saldırılarını , zaman senkronizasyon protokolünü bozmak için kullanabilir.Şu ana kadar , sensör ağlardaki zaman senkronizasyon protokolleri güvenilir bir ortam varsayımı üzerinde çalışmaktadırlar , bu nedenle bu protokoller çeşitli biçimlerdeki gizli saldırılara karşı özellikle daha hassastır.

UMUT VERİCİ ARAŞTIRMA YÖNTEMLERİ[6]

KOD ONAYLAMA[6]

Tehlike altındaki düğümlerle uğraşmak, sensör ağın güvenliğinin sağlanmasındaki en zor uğraştır.

Bu problemi çözmek için , her düğümde çalışan kodu , "kod onaylama" ile doğrulamak ilerisi için umut verici bir yöntemdir. Çünkü , düşman düğüm üzerinde çalışan kod ile normal düğüm üzerinde çalışan kod birbirinden farklı olmalıdır , düşman düğümleri bellek içeriklerini doğrulayarak saptayabiliriz.

"Kod onaylama"yı donanım yada yazılım üzerinden başaryla gerçekleştirebiliriz. Donanım güvenilir ekipmanlar ile donatılır ise ya da güvenilir kurumlar tarafından geliştirilir ise , örnek olarak : TCG (Trusted Computing Group) veya NGSCB (Next-Generation Secure Computing Base) çalıştırılacak kodun sistemin güvenliği tehlikeye atıp atmaması donanım tarafından da kontrol edilebilir.Bu kontrolü yapacak donanım elemanları üretilebilir.

Kod onaylama amaçlı kontrol donanımlarını sensör düğümlerine ekleyebilmemiz için , maliyetlerinin azaltılması , verimliliklerinin artırılması , ve enerji tüketimlerinin minimize edilmesi zorunludur.Aynı zamanda yazılım tarafında gerçekleştirilecek "kod onaylama" teknikleri ile de uğraşmalıyız , bu teknikler şu an için yeterli olmasa da , gelecek için umut veren bir çalışma alanıdır.

GÜVENLİ ART NİYET SAPTAMA VE DÜĞÜM İPTALİ[6]

Tehlike altındaki düğümler sensör ağ için zararlı olduğundan dolayı , bu düğümlerin zamanında saptanıp iptal edilmesi arzu edilen durumdur.
Chan (ve başkaları) problemin (örnek olarak,A düğümü B düğümünün art niyetli bir düğüm olduğunu farkederse , B düğümüne karşı oy kullanabilir) üstesinden gelmek için dağıtılmış oylama sistemini önermektedirler .Eğer yeterli sayıda düğüm B düğümüne karşı oy kullanmış ise , diğer tüm düğümler B ile iletişim kurmayı reddederler .

Bu teknikteki olası problem ise , art niyetli düğümlerin normal düğümleri karalamasıdır (normal düğümlerin aleyhinde oy kullanması) .Aynı zamanda , art niyetli bir düğüm kurban düğüm rolü yapabilir , normal bir düğüme karşı diğer düğümlerin aleyhte oy kullanmalarını sağlayabilir.

Örnek olarak , art niyetli düğüm, yukarı akım düğümünü gönderilen mesajı kaybetttiği şeklinde suçlayarak diğer düğümlere mesaj yollayabilir.
Daha kötüsü art niyetli bir düğüm , iki normal düğümü birbirlerini iptal etmekle uğraştırabilir.

Bu problemlere çözüm bulmak için kullanılabilecek yöntemlerden birisi her düğümün oy sayısını sabit bir sayı ile (m) sınırlandırmaktır , eğer saldırgan ,bir düğümü yakalamayı başarır ise sadece m oyu normal düğümler aleyhine kullanabilecektir.
Bunu sağlayabilmek için , kurulum öncesinde çalışmaz durumda iken düğümlerin oylarını bir anahtar halkasında depolarız. Anahtar kurulumu sırasında , her düğüm çifti komşusunun kendisine karşı oy kullanabilmesi için gerekli aktivasyon değerini değiş tokuş yapar.

GÜVENLİ YÖNLENDİRME[6]

Bir güvenli yönlendirme protokolü art niyetli faaliyetlere rağmen iletişimi sağlayabilmelidir.Bugüne kadar sensör ağlar için yönlendirme protokolleri , "yönetilen yayılma" (directed diffusion) ve "coğrafi yönlendirme" (geographic routing) , güvenli bir ortam varsaymaktaydılar.Bu arada güvenli yönlendirme protokolleri ad hoc ağlar için önerilmişti (örnek: Ariadne)

Ariadne birçok DoS tipi saldırıya karşı ağı korur.Ariadne etkin simetrik anahtar primitiflerini kullanır , fakat hala sensör ağların kaldıramayacağı kadar iletişim , bellek, paket başına işlem yükü açısından ağır gereksinimlere ihtiyaç duyar.
Ek olarak, genellikle sensör ağlar ad hoc ağlar kadar hareketli değildirler ,sensör ağların trafik modelleri ad hoc networklardan farklılık arz eder(sensör ağlarda yönlendirme çoğu zaman veri-merkezlidir)

GÜVENLİ YER TESPİTİ(LOCALIZATION) [6]

Güvenli yer tespiti sensör ağlarda önemli uğraş alanlarından biridir.Bu problem iki açıya sahiptir ; sensör düğümü kendi coğrafi koordinatlarını düşman sahada doğru olarak belirleyebilir , ve art niyetli sensör düğüm , altyapıya uymayan yanlış bir konum talep edemez .

Capkun ve Hubaux ilk problem üzerinde çalışmış ve güvenli mesafe sınırlama ve mesafe hesaplama tekniklerinin kullanımını geliştirmişlerdir.
Sastry, Shankar ve Wagner ile Capkun ve Hubaux ikinci problem üzerinde çalışmışlardır ve altyapının güvenli olarak konum taleplerini doğrulayabilmesini sağlayan mekanizmalar önermişlerdir.

Güvenli konum belirleme , güvenli coğrafi yönlendirme için ön gereksinimdir.Bu aynı zamanda wormhole ya da Sybil saldırılarına karşı savunma yapabilmemize yardımcı olur.

Wormhole saldırısı için , eğer bir yol aralarındaki mesafe coğrafi konum olarak normalden fazla olan ard arda iki düğüm içeriyorsa , bu durumda yolun doğruluğu hakkında şüphelenmeye başlamalıyız.Sybil saldırısı için , küçük bir coğrafi alanda düğümlerin yoğunlaşması şüpheli bir durumdur.Bu yüzden , güvenli yer tespiti güvenli sensör ağların önemli yapı taşlarından birisidir.

ETKİN KRİPTOGRAFİK PRİMİTİFLER [6]

Sensör ağlar hesaplama ve depolama kaynağı bakımından kısıtlı kaynaklara sahip olduğu için , Internet gibi ağlarda kullanılabilen klasik güvenlik çözümleri çoğu kez sensör ağlar için çok pahalıya mal olmaktadır.

Perrig (ve başkaları) SPINS protokol paketini, çeşitli kriptografik işlemleri gerçekleştirmek için etkin blok şifrelemeyi tasarlamışlardır.
Karlof, Sastry ve Wagner güvenlik ve verimlilik arasında seçimin yapılabildiği TinySec'i tasarladılar.

Bu alanda daha fazla araştırma yapmak gerekmektedir , özellikle anahtar tespiti ve sayısal imzalarda , etkin asimetrik kriptografik mekanizmalarının kullanımı üzerine.

KAYNAKLAR

1)**Quanhong Wang,Hossam Hassanein,Kenan Xu** :
Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems:
"A Practical Perspective on Wireless Sensor Networks"

2) http://en.wikipedia.org/wiki/Wireless_sensor_network

3)**Jessica Feng,Farinaz Koushanfar,Miodrag Potkonjak** :
Handbook of Sensor Networks Compact Wireless and Wired Sensing Systems :
"Sensor Network Architecture"

4)**Pınar Sarısaray** ; www.cs.itu.edu.tr/~orencik/DuyargaAglarindaGuvenlik.doc

5)**Sasha Slijepcevic,Jennifer L. Wong,Miodrag Potkonjak** :
Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems:
"Security and Privacy Protection in Wireless Sensor Networks"

6)**Elaine Shi , Adrian Perrig**: "Designing Secure Sensor Networks"

7)**Adrian Perrig, Robert Szewczyk, Victor Wen , David Culler, J. D. Tygar**:
"SPINS Security Protocols for Sensor Networks"