Kablosuz Sensör Ağlar ve Güvenlik Problemleri

Şafak DURUKAN ODABAŞI[1] A.Halim ZAİM[2]

[1,2]Bilgisayar Mühendisliği Bölümü, İstanbul Üniversitesi, İstanbul

[1]e-posta: sdurukan@istanbul.edu.tr [2] e-posta: ahzaim@istanbul.edu.tr

Özetçe

Günümüzde iletişim teknolojilerindeki en büyük gelişmeler kablosuz iletişim teknolojileri alanında yaşanmaktadır. Bu teknolojilerden sensör ağlar, üzerinde en çok çalışma yapılan konulardan biridir. En basit haliyle, kablosuz sensör ağları, kablosuz olarak birbirleriyle bilgi alışverişi yapan sensörler ve bunların bir merkezden izlenmesini sağlayan ağlardır. Kablolu sensör ağlarına göre bu yetenek neyin izlenebileceğini, nasıl izlenebileceğini, ne sıklıkla izlenebileceğini ve ne maliyetle izlenebileceğini değiştirebilmektedir. Bir çok uygulama alanı olan sensör ağlar en yaygın olarak askeri alanlar, kampüsler ve ofis ortamlarında kullanılır. Kablosuz sensör ağları oldukça işlevsel bir yapıya sahiptir. Bu yapılarının teknolojik anlamda bir çok getirisi olduğu gibi, bunun yanında veri güvenliği bakımından sistemin duyarlı olmasına neden olmaktadır. Veri güvenliğinin ve bütünlüğünün sağlanması için güvenlik mekanizmalarının olması gerekmektedir. Düğümlerin hareketli olması, bu nedenle de topolojinin sıkça değişmesi ve kurulan yolların bozulması, ortaya çıkacak olan problemlerin giderilmesini sağlayacak yönlendirme protokollerini zorunlu kılmaktadır. Veri dağıtımı sırasında kullanılan protokoller sayesinde veri kaybı minimuma indirilmeye çalışılmaktadır. Bu çalışmada, kablosuz sensör ağların genel yapısı, avantaj ve dezantajları ile kullanım alanları açıklanarak; ortaya çıkabilecek güvenlik problemleri üzerinde durulmuştur. Ayrıca bu problemlerin giderilmesi için kullanılan veri iletim protokolleri ve bunların çalışma prensipleri de incelenmiştir.

1. Giriş

Sensor ağlar, fiziksel dünya ile etkileşimde bulunmak amacıyla ortama yerleştirilmiş küçük boyutlu sensör düğümlerden oluşur. Bu düğümler duyarga alanı olarak adlandırılan fiziksel bir alanda otonom bir şekilde bir işbirliği içerisine girerek, fiziksel dünyadan öğrendiklerini sanal dünya ortamına taşımaktadır.
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]. En basit haliyle, "kablosuz sensör ağları", kablosuz olarak birbirleriyle bilgi alışverişi yapan sensörler ve bunların bir merkezden izlenmesini sağlayan ağlardır. "Kablolu" sensör ağlarına göre bu yetenek neyin izlenebileceğini, nasıl izlenebileceğini, ne sıklıkla izlenebileceğini ve ne maliyetle izlenebileceğini değiştirmektedir.

2. Kablosuz Sensör Ağlar

Tipik bir Kablosuz Sensör Ağ (Wireless Sensor Network - WSN) kablosuz bir ortam aracılığı ile birbirine bağlanmış yüzlerce hatta binlerce sensör düğümünden oluşur. Sensör düğümleri bir film teneke kutu içerisinde kendi pili, RF adaptörü, mikro kontrolörü 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 ya da düğüm verisini işlerler. 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'ler genel olarak [1]:

- Nem
- Sıcaklık
- 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 imkânsız olduğu ya da kullanılamayacağı durumlarda kullanılabilirler. Genel olarak sensör ağların kullanım alanlarını şu şekilde sıralayabiliriz [1]:

Askeri Uygulamalar: WSN'ler askeri komuta, kontrol, iletişim, hesaplama, istihbarat, nezaret, keşif ve hedef tespit (C4ISRT) sistemlerinin ayrılmaz bir parçası olmaya başlamıştır.

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

Felaketten korunma ve kurtarma: WSN'ler belki de acil durumlarda ya da 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 ya da acil durumun kaynağı, kimlik tespit işlemleri ve kurtarılmayı bekleyen insanların tespiti de hayati verilerdir.

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

Akıllı Ev: WSN'ler tüm insanlık için daha rahat ve akıllı yaşam alanlarının oluşturulmasında rol alabilir. Bu tür uygulamalara örnek verirsek; 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.

Akıllı Alanlar: Son zamanlarda teknolojideki gelişmeler sonrasında, çeşitli kablosuz sensörlerin kişisel mobilya ya da 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.

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.

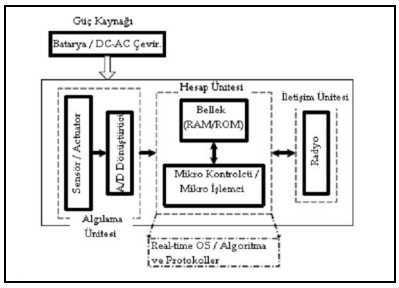
Etkileşimli Çevreleme: WSN'ler mayın bilgisini toplama konusunda ümit vaad eden mekanizmalar üretmişlerdir. Ucuz ve ufak kablosuz sensörlerin yayılması ile küçük yaştaki çocukların eğitimini güçlendirmek için "akıllı anaokulları" tasarlanabilir, çocukları izleme ve aktivitelerini yönlendirme işlemleri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

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 fark edilerek en hızlı biçimde gerekli müdahalenin yapılmasını mümkün kılarlar.

1.1. Kablosuz Sensör Ağların Mimari Yapısı

Sensor ağların (SN) yapısını şu katmanlar altında toplayabiliriz[3];

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

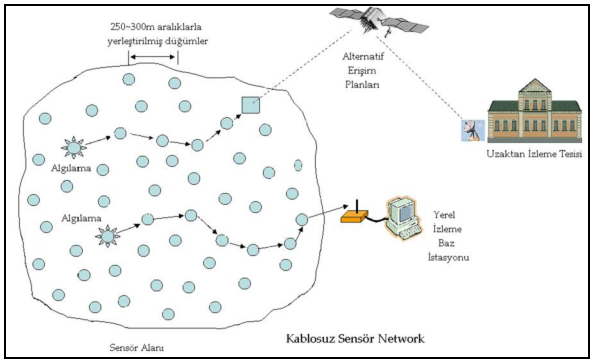


Şekil 1: Mikro sensör düğümünün sistem mimarisi.

Kablosuz sensör ağ 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 ağ mimarisini karakterize etmektedir. İzlemenin yapıldığı ortamda toplanan veri genelde 3 seviyede işlenilir [4].

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

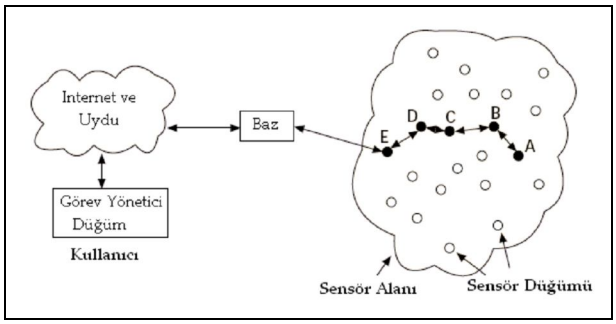
Bazen gönderilen veri eğer başka kıstaslar eşliğinde tekrar analiz edilecekse ya da başka amaçlar için kullanılacaksa bu işlemlerin yapılacağı sistemlere ya da merkezlere iletimi sağlanır.



Şekil 2:Kablosuz sensör ağ mimarisi.

2.1. Sensör Ağlarda Haberleşme Mimarisi

Sensör düğümleri genelde Şekil 2'de karakterize edildiği gibi sensör alanına dağıtılmış haldedirler. Bu dağıtılmış düğümlerin her birinin veriyi toplayıp baz istasyonuna yollama yetenekleri vardır. Verinin herhangi bir mimari altyapıya sahip olmadan baz istasyonuna yollanışı Şekil 3'de görülmektedir. Baz, görev yönetici düğümle internet ya da uydu aracılığı ile haberleşebilir.



Şekil 3: Sensör ağ haberleşme mimarisi.

Sensör düğümlerin tasarımı birçok etken tarafından etkilenmektedir. Bunlar; hata toleransı, ölçeklenebilirlik, üretim maliyetleri, çalıştırma ortamı, sensör ağ topolojisi, donanım kısıtlamaları, iletim ortamı ve güç tüketimidir. [5]

2.2. Sensör Ağlarda Veri Dağıtım Protokolleri

2.2.1. LEACH

LEACH (Low-Energy Adaptive Clustering Hierarchy) algoritması enerji-bilinci değildir ve sürekli-çalışma modelini varsayar [5]. Diğer birçok yönlendirme protokolünden farklı olarak, LEACH adım adım (hop-by-hop) yönlendirme izlemez.

2.2.2. Doğrudan Yayılma (Directed Diffusion)

Doğrudan yayılma, veri-merkezli(data-centric) yönlendirme temelli sensör ağlarda bilgi dağıtımı için bir iletişim örneğidir. Veri merkezli yönlendirmede, tüm ilgi veri üzerindedir, düğümün konumunda değildir.

2.2.3. PEGASIS

PEGASIS (Power-Efficient GAthering in Sensör Information Systems) protokolü, her devrede baz istasyonuna sadece bir düğümün iletim yapmasına izin verir, düğümlerin sadece yakın komşularıyla iletişim kurmasına izin verilir [5]. Çalışma senaryosu ve radyo modeli bakımından LEACH ile PEGASIS arasında fark yoktur. PEGASIS iki kavram üzerine odaklanmıştır: zincirleme ve veri birleşimi.

2.2.4. SPIN

SPIN (Sensör Protocols for Information via Negotiation) protokolü, bireysel sensörlerin gözlemlerinin ağdaki tüm düğümlere yayılmasında kullanılan protokoller ailesindendir. SPIN klasik taşma (flooding) ile alakalı üç probleme çözüm getirmeye çalışır [5]: iç patlama/göçme (implosion), örtüşme (overlap) ve kaynak-bilgisizliği(sourceblindness).

2.2.5. GEAR

GEAR (Geographical and Energy-Aware Routing) algoritması sorgu-yanıt modelini kullanır. Her düğümün, kendi konumunu, enerji seviyesini, komşularının konumları ve enerji seviyelerini bildiğini varsayar. Tablo 1 üzerinde protokollerin çözmeye çalıştıkları problem, tasarım hedefleri, varsayımlar, çalısma ve enerji modelleri, performans ölçümleri ve simülasyon teknikleri özetlenmistir.

Tablo 1: Sensör Ağlarda Kullanılan Protokollerin Karşılaştırılması

Protokol	Enerji Modeli	Performans Ölçütleri		Yönlendirme Şeması		Simülasyon (ns-2 simulator)	
		Ömür	Diğer	Adres-merkezli	Veri-merkezli	Boyut	Karşılaştırma
LEACH	Açıklanan enerji modeli	√	Harcanan enerji toplamı	√		100	Doğrudan iletişim, min. İletimli enerji yönlendirme,statik kümeleme
Doğrudan Yayılım	İletim : 660 mW Alım : 395 mW Bekleme:35 mW		Harcanan enerjinin ortalaması		√	50-250	Omniscient multicast,taşma
PEGASIS	Açıklanan enerji modeli	√		√		100	LEACH
SPIN	İletim: 600 mW Alım:200 mW		Saniyede yayılan veri,saniyede harcanan enerji, birim enerji başına yayılan veri		√	25	Taşma ve gossiping
GEAR	Alım veya iletimde 1 enerji birimi	√			√	400-4800	GPSR

Protokol	Problem	Tasarım Hedefi	Varsayımlar*		Çalışma Modeli		
			Düğümün sahip olduğu bilgi	Global ID ler	Sürekli çalışma	Sorgu Yanıt	Enerji Bilinçli
LEACH	Düğümlerden algılanan veriyi toplar ve Baza gönderir	Min. Enerji , max. ömür		√	√		
Doğrudan Yayılım	Sorguyu bazdan R bölgesine yollar ve algılanan veriyi aynı yolla baza geri getirir.	Min. Enerji				√	
PEGASIS	Düğümlerden algılanan veriyi toplar baza gönderir.	Min. Enerji , max. ömür	Tüm düğümlerin konumları	√	√		
SPIN	Sensör gözlemlerini ağdaki tüm düğümlere yayar . Bu göçme,örtüşme ve kaynak-bilgisizliğine çözüm içerir.	Birim zaman ve enerji ile max.veri yayılımı	Enerji seviyesini	√	√	√	√
GEAR	Bazdan R bölgesindeki düğümlere sorguyu yollar.	Max. ömür	Konumlar ve enerji seviyeleri			√	√

3. Kablosuz Sensör Ağlarda Güvenlik

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 ölçümleri 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 çalışmaları en hızlı biçimde askeri uygulamalarda kendini göstermektedir. Bu alandaki güvenliğin önemi herkesçe 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 ya da 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 ağ uygulamaları çok çeşitli fiziksel ortamlarda ve kısıtlamalar altında çalışmaktadır. Sensör ağ 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.

3.1. Kablosuz Sensör Ağların Güvenliğini Tehlikeye Atan Özellikler

3.1.1 Düşman Saha: 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 elde edilebilinir [6].

3.1.2 Kaynakların Sınırlılığı: 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 sınırlandırılırlar.

3.1.3 Ağ İçinde İşlem Yapma: 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.

3.1.4 Uygulamaya Özel Mimari Yapı: Yukarıda anlatılan özelliklerinden ötürü WSN'ler uygulamaya göre değişen mimari yapılara sahiptirler. Genel amaçlı mimari yapının esnekliği kaynakların etkin kullanımını gerektirir.

3.2. Kablosuz Sensör Ağların Güvenliği İçin Gereksinimler

3.2.1. *Dışarıdan Gelen Saldırılara Karşı Dayanıklılık:*

Birçok uygulama dışarıdan gelen saldırılara karşı güvenlik gerektirir. Gizlice dinleme (eavesdropping) ya da paket enjeksiyonu (packet injection) gibi bilinen saldırılara karşı standart güvenlik tekniklerinin seviyesini yükseltmemiz gerekebilir. Örnek olarak, şifrelenmiş primitifler kullanarak orijinalliği ve iletişimin gizliliğini ağ içerisindeki düğümler arasında sağlayabiliriz [7]. 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 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 fark edip yeni topolojiye göre iletişimi sağlayacak protokollere ihtiyaç vardır.

3.2.2. İç Krizlere Karşı Direnç:

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 her zaman mümkün değildir. Bu duruma alternatif tasarım yaklaşımı; düğüm kaybına ya da tehlike altında bulunmasına dayanıklı mekanizmalar tasarlamaktır, böylece azar azar sistemin düğüm kaybetmesi sistemin tümden kaybına değilde performansında küçük çaplı düşüşlere neden olur.

3.2.3. Güvenliğin Gerçekçi Seviyesi:

Genel olarak güvenliğin gereksinimleri tartışılırken, sensör ağların uygulamadan uygulamaya güvenlik unutulmamalıdır [7]. Örnek olarak tıbbi gözlem cihazlarında insanın vücuduna 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.

3.2.4. Veri Gizliliği:

Bir sensör ağ kesinlikle sensör bilgisini komşu ağlara sızdırmamalıdır [7]. Birçok 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 [8]. 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(kulak misafiri) tipi saldırılardan korumak için önemlidir. Bunu sağlamak için standart şifreleme fonksiyonları kullanılabilir (örn: AES blok şifreleme) ya da 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.

3.2.5. Veri Bütünlüğü:

Haberleşmede veri bütünlüğü, alıcının aldığı verinin art niyetli kişilerce aktarım sırasında değiştirilmediğine karşı garanti verir [8]. SPINS(Security Protocols for Sensor Networks) ile veri bütünlüğünü, veri doğrulama ile sağlayabiliriz. Çünkü veri doğrulama daha güçlü bir özelliktir.

3.2.6. Verinin Tazeliği:

Sensör ağlar anlık değişen verileri algılayıp işlediği için sadece gizlilik ve güvenliğin sağlanması yeterli değildir, aynı zamanda her mesajın tazeliğinin de garanti edilmesi gerekir [8]. Çeşitli saldırılar sensör ağın kullanılabilirliğini tehlikeye atabilir. Kullanılabilirliğin sağlanması düşünülürken, düğüm kayıpları ya da hataları ile sistemin tümden çökmesi engellenmeye çalışılmalıdır.

3.2.7. Hizmet Bütünlüğü:

Ağ katmanının üzerinde, sensör ağ genelde çeşitli uygulama-

seviyesinde hizmet verir [7]. Veri toplama/kümeleme sensör ağlardaki en yaygın hizmetlerden biridir. Veri toplama işleminde düğümler komşu düğümlerden veriyi alır, veriyi topladıktan sonra ya baz istasyonuna ya da 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.

3.3. Saldırılar ve Karşı Tedbirler

Bilindik saldırılara karşı kablosuz sensör ağlarda alınabilecek tedbirler şunlardır:

3.3.1. Gizlilik ve Kimlik Doğrulama:

Standart kriptografik teknikler eavesdropping, paket tekrarlama, sahte paket yollama gibi dış kaynaklı saldırılara karşı iletişim bağlantılarının güvenilirliğini ve gizliliğini koruyabilir [7].

3.3.2. Anahtar Tespiti ve Yönetimi:

İki sensör düğümünün güvenli ve doğrulanmış bir bağlantı kurması için, gizli bir anahtarın paylaşımının sağlanması gerekmektedir [7]. Anahtar tespit problemi, ağ üzerindeki bir düğüm çifti arasında gizli anahtarın nasıl tespit edilip kurulması gerektiği konusunu irdeler. Saf bir fikir olarak kurulumdan önce global bir anahtarın her düğüme yerleştirilmesi ve kullanılması düşünülebilir, bu düğümlerin kendi aralarında kolayca iletişimine imkân verirken aynı zamanda 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 tespiti 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.

3.3.3. Broadcast/Multicast Kimlik Doğrulama:

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 [7]. Ne yazık ki ortak anahtar şifreleme sensör ağlar için çok pahalı bir tekniktir. Bu problemi çözmek için güvenli broadcast doğrulama sağlamak için µTesla protokolü önerilmiştir. 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.

3.3.4. Kullanabilirlik Üzerine:

Ağın kullanılabilirliği üzerine yapılabilecek saldırılar genellikle DoS saldırısı üzerinden tanımlanmıştır [7]. DoS saldırılarının hedefi ağın farklı katmanları olabilir.

3.3.5. Frekans Bozma(Jamming) ve Paket Enjeksiyonu:

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 [7]. 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 (Unfairnessattack) 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 belirlenmesi sağlanabilir.

3.3.6. Sybil saldırısı:

Sybil saldırısı; zararlı bir düğümün gayri meşru bir şekilde birden fazla kimlik talep etmesidir [7]. 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 kalır. 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.

3.3.7. Yönlendirmeye Karşı Çeşitli Saldırılar:

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 [7]. 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.

3.3.8. Hizmet Bütünlüğüne Karşı Gizli Saldırı:

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 ya da hayali değerler raporlayabilir. Sybil saldırısı, tehlikeye atılmış bir düğümün toplanmış sonuç üzerinde daha büyük bir etkisinin olmasına izin verir [7].
Saldırgan ayrıca DoS saldırısı da gerçekleştirebilir. Bu yüzden normal düğümler kendi sensör bilgilerini baz istasyonuna raporlayamayabilirler. SIA (Secure Information Aggregation) protokolü gizli saldırılara karşı dayanıklı sistemlerin geliştirilmesi için önerilmektedir. Zaman senkronizasyonunu göz önünde tutarsak; gizli saldırganın hedefi yanlış zaman bilgisini yayarak düğümlerin senkronizasyonunu ortadan kaldırmaktır.
Saldırgan senkronizasyon mesajlarını kesebilir ya da 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.

4. Sonuç

Kablosuz sensör ağlar, ileriki yıllarda günlük hayatta daha fazla yer alarak, oldukça yüksek bir kullanım alanına ulaşacaktır. Özellikle akademik alanda bu konuyla ilgili çalışmalar gün geçtikçe artmaktadır. Fakat burada dikkati çeken bir özellik, yapılan çalışmaların tek bir problem üzerinde yoğunlaşması nedeniyle herhangi bir standartın ortaya koyulmayışıdır.
Etkili bir yönlendirme protokolünün ortaya konması ve mevcut güvenlik önlemlerinin farklılaştırılarak birlikte kullanılır hale getirilmesi genel olarak sensör ağlarla ilgili ortaya çıkacak sorunlara daha fonksiyonel bir bakış açısıyla çözüm getirecektir.

5. Kaynakça

[1]. Q. Wang, K. Xu and H.S. Hassanein, "A Practical Perspective on Wireless Sensor Networks," Chapter 9, Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems (Ilyas/Mahgoub, Eds), CRC Press, July 2004 .

[2]. http://en.wikipedia.org/wiki/Wireless_sensor_network

[3]. J. Feng,F. Koushanfar,M. Potkonjak, "Handbook of Sensor Networks Compact Wireless and Wired Sensing Systems:Sensor Network Architecture", CRC Press, ISBN 0-8493-1968-4

[4]. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci.,"A Survey on Sensor Networks", *IEEE Communications Magazine,* August 2002.

[5]. A. A. Ahmed, H. Shi, and Y. Shang, "A Survery On Network Protocols For Wireless Sensor Networks", *IEEE Communications Magazine* 2003.

[6]. I. Mohammad, Mahgoub, Imad. "Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems", CRC Press, ISBN 0-8493-1968-4

[7]. E.Shi, A. Perrig, "Designing Secure Sensor Networks", *IEEE Communications Magazine, December* 2004.

[8]. A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar, "SPINS: Security Protocols for Sensor Networks", *ACM Portal Wireless Networks Magazine, Volume 8*, pp. 521–534, 2002