Kablosuz Sensör Ağlarda Güvenli Yönlendirme

Halil Hakan TARHAN, Zeynep GÜRKAŞ AYDIN, M.Ali AYDIN

***Özet*— Kablosuz haberleşmenin her geçen gün kullanım alanını genişletmesi , mevcut sistemlerin kablosuz modelleriyle yer değiştirmesine sebep olmaktadır. Onlarca kullanım alanına sahip sensör ağların yerini esnek kullanıma sahip, daha az kurulum ve bakım maliyeti gerektiren kablosuz sensör ağlar almaktadır. Bu çalışmada kablosuz sensör ağların güvenlik gereksinimleri sıralanmış, ağın yaşam süresinin farklı yönlendirme algoritmaları kullanımından nasıl etkileneceğini göstermeyi amaçlayan simülatör programı geliştirilmiştir.**

***Anahtar Kelimeler*—Kablosuz Sensör Ağlar, Güvenli Yönlendirme, Simülasyon, Leach, Flooding, Pegasis**

I. GİRİŞ

Mikro elektromekanik Sistemler (MEMS) ve Radyo Frekanslarındaki (RF) hızlı gelişim; az güç tüketen, ucuz, ağ üzerinde kullanılabilir mikro sensörlerin geliştirilmesini mümkün kılmıştır. Bu sensör düğümleri çeşitli fiziksel bilgilerin; sıcaklık, basınç, bir cismin hareketi vs. yakalanmasını sağlamaktadır. Bununla beraber çevrenin fiziki özelliğinin de nicel ölçümlerle eşlenmesini sağlayabilmektedir. Tipik bir Kablosuz Sensör Ağ (Wireless Sensor Network - WSN) kablosuz bir ortam aracılığı ile birbirine bağlanmış yüzlerce hatta binlerce sensör düğümünden oluşur. 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 işler. WSN'lerin sağladığı yararlardan ya da artı özelliklerden bazıları aşağıda kısaca açıklanmıştır.

A. Her zaman her yerde

Mevcut makrosensör düğümlerinin kapsamı ,maliyet kıstasları ve kurulum (plana göre yerleşim) sebepleriyle belirli fiziksel alanlarda dar şekilde sınırlandırılmıştır. 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.

Halil Hakan TARHAN, *Bilgisayar Mühendisliği Bölümü, İstanbul Üniversitesi Mühendislik Fakültes, Avcılar –İstanbul tarhanhh@hotmail.com*
Zeynep GÜRKAŞ AYDIN, *Bilgisayar Mühendisliği Bölümü, İstanbul Üniversitesi Mühendislik Fakültes, Avcılar –İstanbul zeynepg@istanbul.edu.tr*
M.Ali AYDIN, *Bilgisayar Mühendisliği Bölümü, İstanbul Üniversitesi Mühendislik Fakültes, Avcılar –İstanbul, aydinali@istanbul.edu.tr*

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

B. Hataya karşı daha fazla tolerans

Bu kazanım WS (Wireless Sensor) 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 ya da 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.

C. 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 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]

D. Düşük maliyet

WSN'lerin makro sensörlü 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]

E. WSN Uygulamalarından Bazıları

WSN'ler ;

- 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.

1) Askeri Uygulamalar

WSN'ler askeri komuta, kontrol, iletişim, hesaplama, istihbarat, nezaret, keşif ve hedef tespit (C4ISRT) sistemlerinin ayrılmaz bir parçası olmaya başlamıştır. [1]

2) 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]

3) 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]

4) Tıbbi Hizmetler

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

5) 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]

6) 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]

7) 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]

8) 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]

9) 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]

II. KABLOSUZ SENSÖR AĞLARIN DONANIM ÖZELLİKLERİ VE MİMARİ YAPISI

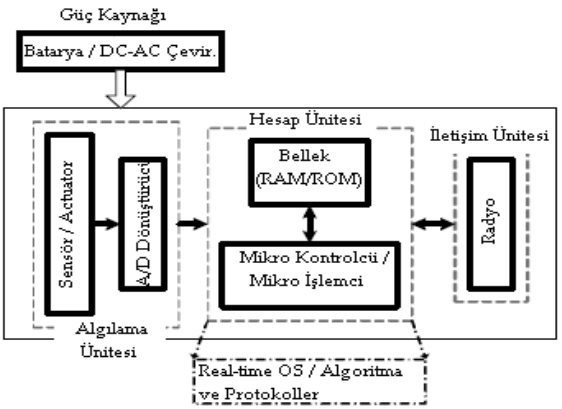
Tasarsız ağlar, düşük güç tüketen elektronik cihazlar ve kısa mesafe haberleşme sağlayan radyolar, akıllı sensörlerin geliştirilmesi, Sensör Ağ'ların yayılmasını olası kılan en önemli teknolojik etkenlerdir.

Sensör Ağlar'ın yapısını şu katman/düzeyler altında toplayabiliriz;

- SN (Sensor Network) düğümlerinin üzerinde bulunan bileşenler (işlemci, haberleşme ünitesi, bellek, sensör ve/veya erişim düzeneği ve güç kaynağı)
- Düğüm (node) düzeyi
- Dağıtılmış Ağ Sistemi düzeyi [2]

A. Kablosuz Sensor Network Düğümlerindeki Bileşenler

Bu düğümler genelde 6 tip bileşenden oluşur lar. Bunlar; işlemci,bellek ünitesi, güç kaynağı, sensör ve/ veya erişim düzeneği ve haberleşme alt sistemidir (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) de kullanışlılık 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. [2]



Şekil-1: Mikro Sensör Düğümünün Sistem Mimarisi

B. 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 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 Ağ çalışmaları en hızlı biçimde askeri uygulamalarda kendini göstermektedir, bu alandaki güvenliğin önemi herkes tarafından 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. 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. WSN'ler geleneksel kablosuz ağlarla (özellikle gezgin tasarsız ağlarla) birçok önemli özelliği ortak olarak içlerinde barındırılar.

İki tip ağ da kablosuz haberleşme üzerine kurulmuştur, tasarsız 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.

C. Kablosuz Sensör Ağlarda Güvenliği Tehlikeye Atan Özellikler

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 alınabilir. Sensör düğümlerinin fiziksel olarak erişiminin mümkün olmasından dolayı, WSN'ler için güvenlik mekanizmaları bir yada daha çok düğümün tehlikeye atıldığı durumlarla ilgilidir. [3]

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 sınırlandırırlar. Sınırlı kaynaklar, düğümlerin yeni saldırı tiplerine karşı açık hale gelmesine sebebiyet verir. Örnek olarak Sleep Deprivation Torture Attack verilebilir. [3]

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]

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]

D. Sensör Ağların Güvenliği İçin Gereksinimler

1) Dışarıdan Gelen Saldırılara Karşı Dayanıklılık

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.[4]

2) İç Krizlere Karşı Direnç

Güvenliği kritik olan 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. [4]

3) Güvenliğin Gerçekçi Seviyesi

Genel olarak güvenliğin gereksinimleri tartışılırken, sensör ağların uygulamadan uygulamaya güvenlik gereksinimlerinin değişim göstereceği unutulmamalıdır.[4]

4) Veri Gizliliği

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, gizlice dinleme (eavesdropping) 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.Şifrelemeye ek olarak algılanan verinin gizliliği, baz istasyonlarında yanlış kullanımının engellenmesi için erişim kontrol kurallarına ihtiyaç duyar.[4,5]

5) Veri Doğrulama / Kimlik Denetimi

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. [5]

6) Veri Bütünlüğü

Haberleşmede veri bütünlüğü, alıcının aldığı verinin art niyetli kişilerce aktarım sırasında değiştirilmediğine karşı garanti verir.[5]

7) Verinin Tazeliği

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. 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. [5]

8) Kullanılabilirlik

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. [4]

E. Saldırılar ve Saldırılara Karşı Tedbirler

Bu bölümde en çok bilinen saldırılara karşı kablosuz sensör ağlarda alınabilecek tedbirleri inceleyeceğiz.

1) Gizlilik ve Kimlik Doğrulama

Standart kriptografik teknikler gizlice dinleme(kulak misafiri olma), paket tekrarlama, sahte paket yollama gibi dış kaynaklı saldırılara karşı iletişim bağlantılarının güvenilirliğini ve gizliliğini koruyabilir. [4]

2) Anahtar Tespiti ve Yönetimi

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 genel bir anahtarın her düğüme yerleştirilmesi ve kullanılması düşünülebilir, bu düğümlerin kendi aralarında kolayca iletişimine imkan 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 metot 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. [4]

3) Tümegönderim/Çoğa Gönderim (Broadcast/Multicast) Kimlik Doğrulama

Tümegönderim (broadcast) ve çoğa gönderim (multicast) birçok sensör ağ 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 yazık ki ortak anahtar şifreleme sensör ağlar için çok pahalı bir tekniktir.[4]

4) Kullanılabilirlik

Ağın kullanılabilirliği üzerine yapılabilecek saldırılar genellikle DoS (Denial of Service) saldırısı üzerinden tanımlanmıştır, DoS saldırılarının hedefi ağın farklı katmanları olabilir [4]

i. 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.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. Ağ Katmanında ise, saldırgan zararlı paketleri enjekte edebilir. Doğrulama kullanarak alıcının zararlı paketleri saptaması ve anlık mesaj tazeliğinin ölçümü ile tekrarlanmış paketlerin saptanması sağlanabilir. [4]

ii. Sybil saldırısı

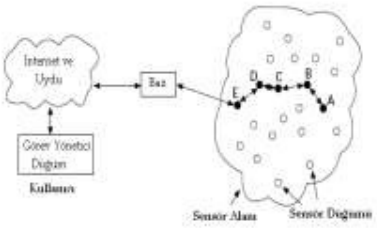
Sybil saldırısı; zararlı bir düğümün gayri meşru bir şekilde birden fazla kimlik talep etmesidir. Sybil saldırısı servisin kesintiye uğratılması için farklı katmanlarda kullanılabilir. MAC katmanında, zararlı düğüme birden çok kimliğin sağlanması sonucunda, zararlı düğüm paylaşılmış radyo kaynağının 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.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.[4]

iii. 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. Çok yollu yönlendirme, bu tür saldırılara karşı yapılacak savunmalardan birisidir.[4]

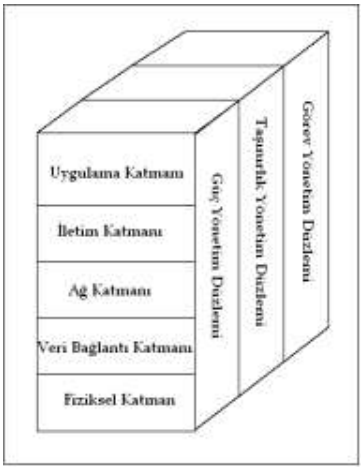
F. Kablosuz Sensör Ağlarda Haberleşme Mimarisi

Sensör düğümleri genelde Şekil-2'de karakterize edildiği gibi sensör alanına dağıtılmış haldedirler. Bu dağıtılmış düğümlerin herbirinin veriyi toplayıp baz istasyonuna yollama yetenekleri vardır. Verinin herhangi bir mimari altyapıya sahip olmadan baz istasyonuna yollanışı Şekil-2'de görülmektedir. Baz, görev yönetici düğümler; internet yada uydu aracılığı ile haberleşebilir. Sensör düğümlerin tasarımı birçok etken tarafından etkilenmektedir. Bunlar; Hata Toleransı, Ölçeklenebilirlik, Üretim Maliyetleri, Çalıştırma Ortamı, Sensör Ağ Topolojisi, Donanım Kısıtlamaları, İletim Ortamı ve Güç Tüketimidir . [6]



Şekil-2: Verinin baz istasyonuna yollanışı

Bu etkenleri hatırlattıktan sonra Sensör Ağların Protokol Yığınını inceleyelim;



Şekil-3: Senör ağ protokol katmanı

Şekil-2'de gösterilen Sensör Düğümü ve Baz tarafından kullanılan protokol yığını Şekil-3'de gösterilmiştir. Bu protokol yığını gücü ve yönlendirme bilincini birleştirir, veriyi ağ kurma protokolleriyle entegre eder, kablosuz ortam aracılığı ile gücü verimli bir şekilde kullanarak haberleşmeyi sağlar ve sensör düğümlerinin birbirleriyle ortak çalışmalarını daha verimli hale getirir. Bu protokol yığını Fiziksel Katman, Veri Bağlantı Katmanı, Ağ Katmanı, Taşıma Katmanı, Uygulama Katmanı, Güç Yönetim Düzlemi, Taşınırlık (Mobility) Yönetim Düzlemi ve Görev Yönetim Düzleminden oluşur.Fiziksel Katman basit fakat dayanıklı kipleme,iletim ve alım tekniklerini adresler. Ortamın gürültülü ve sensör düğümlerinin hareketli olmasından ötürü , ortam erişim kontrol (MAC - medium access control) protokolü güç faktörünü göz önünde tutmalı ve komşu düğümlerin yayınları ile çarpışmayı en aza indirebilmelidir. [6]Ağ katmanı iletim katmanı tarafından kendisine sağlanan verinin yönlendirilmesinden sorumludur. İletim katmanı, sensör ağ uygulamasının gereksinim duyması halinde veri akışının güçlendirilmesine yardım eder. Algılama görevlerine bağlı olarak , faklı tiplerde uygulama yazılımları, uygulama katmanı üzerine kurulup kullanılabilir. Bunlara ek olarak güç, taşınırlık ve görev yönetim düzlemleri sensör düğümleri arasındaki gücü, hareketleri ve görev dağılımını izler.

G. Yönlendirme Protokollerinde Kullanılan Modeller ve Ön Kabuller

1) Varsayımlar

Bir sensör düğümünün kibrit kutusu boyutlarında olması beklenmektedir. Birkaç yüz MHz lik işlemcisi, küçük belleği, radyo modemi, ADC'si (Analog/Digital Çevirici), sensörleri ve bataryası olması beklenir. Radyo menzili kontrol edilerek en az miktardaki enerji sarfiyatı ile istenilen alıcılara mesajların gönderebilmesine olanak sağlanır. [7]

2) Çalışma Modelleri

Çalışma modeli olarak iki yaygın tip vardır; sürekli-çalışma modeli ve sorgu-yanıt modeli. Önceleri, algılanan

verinin sürekli olarak ele geçirilmesi gerekmekteydi. Bu yüzden herhangi bir istek olmadan, sensör düğümlerinin aktif olması ve algılanan veriyi periyodik olarak baz istasyonuna göndermesi gerekirdi. Sorgu-yanıt tipinde ise, işlem yapan şahıs ağ üzerindeki herhangi bir düğümü bir sorgu ile sorgular. Bir protokol eğer harcadığı enerji toplamını ve geriye kalan erenji toplamının farkında ise bu protokole enerjisinden haberdar/bilinçli (energy-aware) diyebiliriz. [7]

3) Enerji Modelleri

Popüler enerji modeli aşağıda belirtilmiştir. l-bit uzunluğunda bir mesajı , d mesafesi boyunca gönderimi (transmit-T) için, radyonun ihtiyaç duyduğu enerji aşağıdaki formül ile hesaplanır.

$$E_{Tx}(l,d) = E_{Tx-elec}(l) + E_{Tx-amp}(l,d)$$

$$E_{Tx}(l,d) = \begin{cases} lE_{elec} + l\varepsilon_{friss-amp}\, d^2 & \text{if } d < d_{crossover} \\ lE_{elec} + l\varepsilon_{two-ray-amp}\, d^4 & \text{if } d \geq d_{crossover} \end{cases} \quad (1)$$

Alıcının l-bit uzunluğunda bir mesajı almak için ihtiyaç duyduğu enerji ise aşağıdaki formül ile hesaplanabilir.

$$E_{Rx}(l) = E_{Rx-elec}(l)$$
$$E_{Rx}(l) = lE_{elec}, \quad (2)$$

Bu eşitliklerde $E_{Tx\text{-}elec} = E_{Rx\text{-}elec} = E_{elec}$ alıcı yada verici devresini çalıştırmak için gerekli enerjidir. 1Mbps alıcı için 50nJ/bit lik tipik bir değere sahiptir. $\mathbf{d}_{crossover}$ mesafesi tipik olarak 86.2 m seçilmiştir , $\varepsilon_{friss\text{-}amp}$ mesafe **d** , $\mathbf{d}_{crossover}$ dan küçük ise ,verici amplifikatörü tarafından ihtiyaç duyulan enerjidir ve tipik olarak 10 pJ/bit/m^2 olarak seçilmiştir, $\varepsilon_{two\text{-}ray\text{-}amp}$ mesafe **d**, $\mathbf{d}_{crossover}$ dan büyük ise ,verici amplifikatörü tarafından ihtiyaç duyulan enerjidir ve tipik olarak 0.0013 pJ/bit/m^4 olarak seçilmiştir. Beamforming[1] için hesaplanan enerji 5 nJ/bit/signal olarak atanmıştır. [7].

III. PROGRAMIN AMACI

Kablosuz sensör ağlar yüzlerce, bazen binlerce sensör düğümünden oluşmaktadır. Bu düğümler kısıtlı kaynaklara sahiptir. Bu kaynaklar; işlemci, depolama, haberleşme ve enerji üniteleri olarak sıralanabilir. Sınırlı enerji tüm teknolojik gelişmelerin önündeki en büyük engellerden biridir. Bu etken zaten sınırlı kaynaklara sahip olan sensör düğümlerinde daha hayati bir öneme kavuşur.

Bunun nedenini anlamak için sensör ağların kullanım alanlarını incelemek gerekir. Kablosuz sensör ağlar askeri uygulamalar başta olmak üzere, çevre gözlem, tıbbi gözlem gibi alanlarda birçok amaca yönelik kullanılmaktadır. Özellikle askeri operasyonların her geçen gün çeşitlenip tüm dünyaya yayılması ve bu operasyonlarda çoğu zaman kablosuz sensör ağların kullanılmaya başlanması, dayanıklılık ve uzun yaşam süresini kablosuz sensör ağlar için olmazsa olmaz özellikler arasına katmıştır. Bu sebepten dolayı, kurulumu yapılan bir ağda hangi yönlendirme protokolünün kullanılacağına karar verilirken, hangi protokolün ağı ne kadar süre çalışır durumda tutabileceği, ne kadar sürede ne kadar enerji harcayarak kaç olayı algılayabileceği (sense) gibi bilgiler çok değerlidir. Bu çalışmada geliştirilen simülasyon programı bu amaca yönelik hazırlanmıştır.Program; düğüm sayısının, veri paketlerinin büyüklüğünün, algılama mesafesinin, düğümlerin başlangıç enerji değerlerinin isteğe uygun olarak girilebildiği bir simülasyon programıdır. Programda karşılaştırması yapılabilecek yönlendirme protokolleri; LEACH, Flooding ve PEGASIS'tir. Program, çalıştırıldıktan sonra, çıktı olarak bir metin dosyasına; Protokolün adı, düğüm sayısı, olay sayısı, algılanan olay sayısı, simülasyonun gerçekleştirildiği alanın boyutlarını, düğümlerin algılama mesafelerini, iletimi gerçekleştirilen paketlerin büyüklüğünü, başlangıç düğüm enerjisini, simülasyon boyunca düğümler arasında kurulan bağlantı sayısını, paketlerin iletimi için atılan toplam adım sayısını, kaybedilen düğüm sayısını, toplam harcanan enerji, algılanan olay başına harcanan enerji ,ilk düğüm kaybı zamanını yazar.

A. SensoNet

Geliştirilen simülasyon programının ismi SensoNet'tir. Şekil-4'teki açılış arayüzüne sahiptir. Programın kullanımı için form üzerindeki alanlar şu kriterlere uygun olarak doldurulmalıdır.

Node Number : Ağ üzerindeki düğüm sayısı girilmelidir. Alabileceği en büyük değer 500'dür.

Event Number : Ağ üzerinde oluşturulacak olay sayısıdır. Alabileceği en büyük değer 2000'dir.

dead(%) : Bu seçenek olay sayısına herhangi bir değer vermeyip , ağdaki ölü düğümlerinin oranının seçimine olanak tanır. Bu seçenek işaretlenip , sağındaki alana bir değer girilirse , ağdaki düğümlerdeki ölü düğüm oranı , girilen değere ulaşıncaya kadar ağda olay oluşturulur.

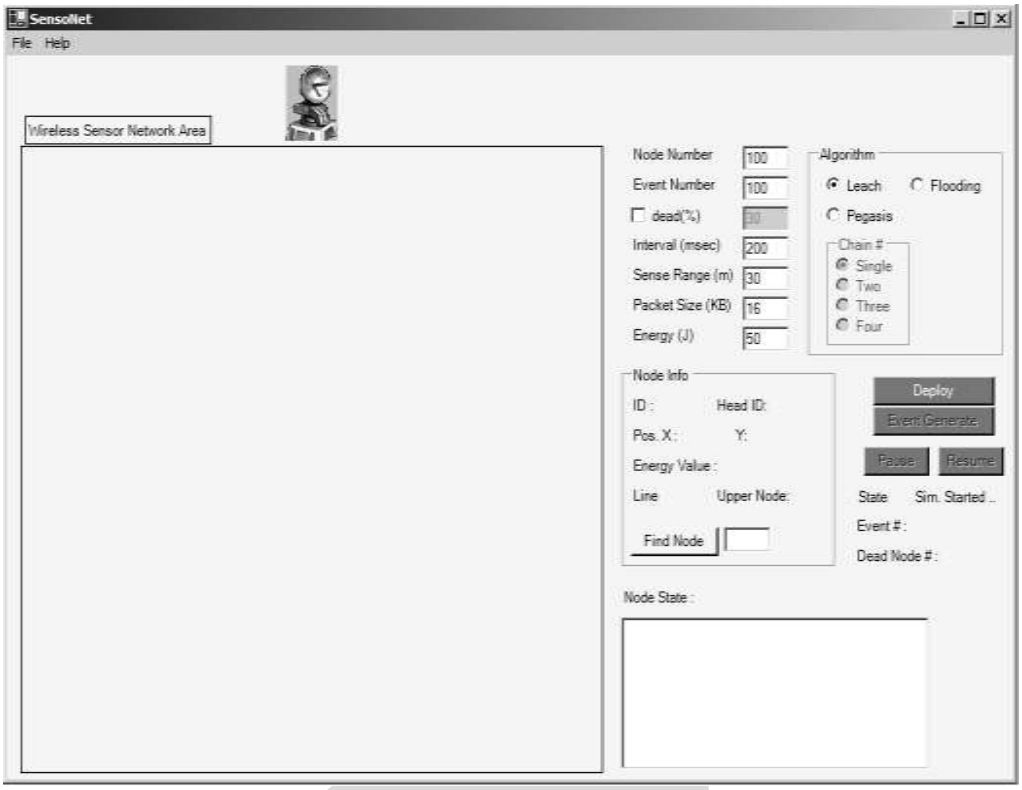
Interval (msec) : Ağ üzerinde oluşturulacak olayların arasındaki zaman aralığı bu alana girilmelidir. Birimi milisaniyedir.

Sense Range (m): Sensör düğümlerin alıcılarının menzili bu alana girilmelidir.Birimi metredir.

Packet Size (KB) : Düğümlerin iletecekleri veri paketlerin büyüklüğü bu alana girilmelidir.Birimi Kilobayt'tır.

Energy (J) :Düğümlerin ağın kurulum anında sahip olduğu enerji değeri bu alana girilmelidir. Birimi Joule'dür.

[1] Beamforming algoritması kullanıldığında, çok sayıda akustik sinyal birleştirilip sinyal sayısı azaltılır , oluşan sinyal diğer sinyallerin içeriğini de barındıran anlamlı bir sinyaldir .[8]



Şekil-4: SensoNet programının arayüzü

1) Simülasyon Sonuçları

Bu bölümde SensoNet kullanılarak yapılan simülasyonların sonuçları, algoritmaların karşılaştırılması amacı ile grafikler eşliğinde verilecektir. Bu bölüm boyunca düğümlerin algıladıkları ve baz istasyonuna doğru yönlendirdikleri verinin boyutu 32 KB'tır. Düğümlerin algılama mesafesi 30 m. , başlangıç enerjisi 50 Joule'dür.Baz istasyonu düğümlerin dağıtıldığı alanın üst kenarının orta noktasında konumlandırılmıştır.

D.S:Düğüm Sayısının,

O.S: Olay Sayısının kısaltılmışıdır.

Pegasis # 1: tek , Pegasis # 2: çift, Pegasis # 3: üç,

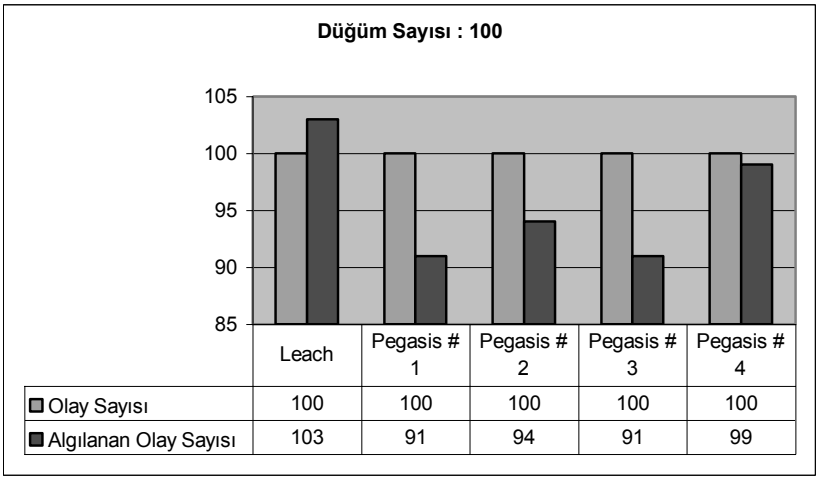
Pegasis # 4:dört zincirlemeli PEGASIS algoritmasını temsil etmektedir.

Şekil-5'de bulunan grafikte, 100 düğüm sayısına sahip kablosuz sensör ağ üzerinde oluşturulan olayların algılanma sayıları verilmektedir.Leach algoritması ağın sınırları içerisinde 100 olay olmasına rağmen 103 algılama yapmıştır. Bu sonuç , bir olayın birden fazla düğüm tarafından algılanmış olmasından kaynaklanmaktadır. Pegasis # 1, sadece 91 olayı algılayabilmiştir bunun sebebi zamanla oluşan düğüm kayıpları sebebiyle , kaybın olduğu bölgenin olayları algılayamaz hale gelmesi olabilir. Pegasis algoritmasında zincir sayısı arttıkça algılanan olay sayısının artması muhtemeldir.

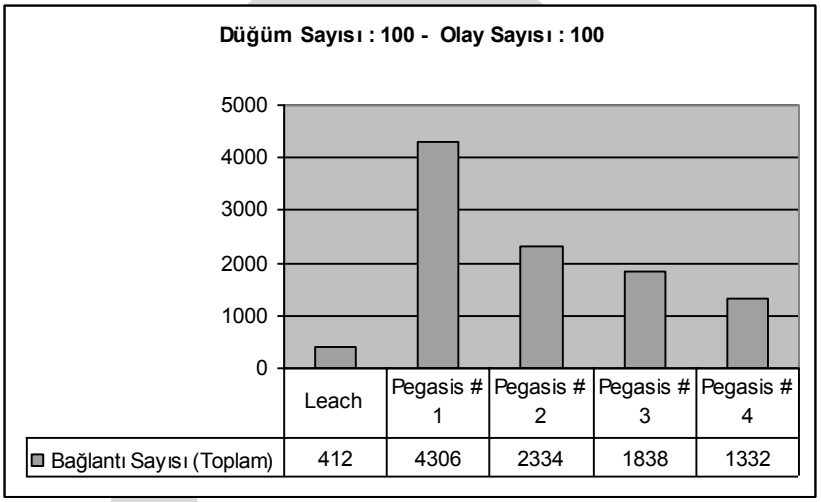
Şekil-6'daki grafik , düğümlerin 100 olay boyunca , algılanan olayların iletimi için toplam kaç adet bağlantı kurulmasına ihtiyaç duyduklarını gösterir. Leach küme başlarından baz istasyonuna doğrudan iletişim ile haberleşmeyi öngördüğü için Pegasis'in tüm modellerinden daha az bağlantıya ihtiyaç duymaktadır. Pegasisin modellerini kendi içinde değerlendirirsek zincir sayısı arttıkça oluşturulan bağlantı sayısı azalmaktadır.

Şekil-7'de bulunan grafik 100 düğüme sahip ağda 100 olayın algılanması ve iletimi için toplam kaç adım (hop) atılması gerektiğini gösteririr. Atılan adım sayısına paralel şekilde harcanan enerjinin de arttığı grafikten gözlemlenebilir.Algoritmalar için bağlantı sayıları ile ilgili grafikte söylediğimiz ilişki toplam adım sayıları ve harcanan enerji için de geçerlidir.

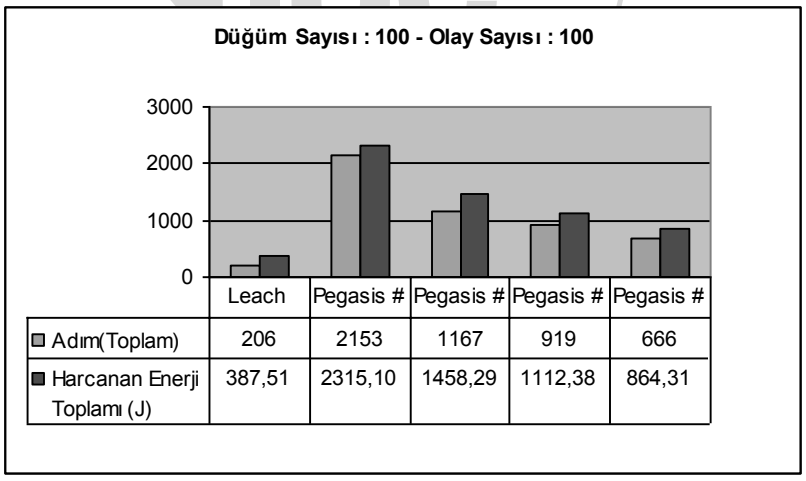
Şekil-8'deki grafikte kayıp (ölü) düğüm sayıları ve ilk düğüm kaybının ne zaman gerçekleştiğini görebiliriz. Leach algoritması hiçbir düğüm kaybı olmadan simülasyonun sona ermesini sağlamıştır. Pegasis algoritmasında zincir sayısı arttıkça düğümlerin dayanıklılığının arttığını görüyoruz. Hem kayıp düğüm sayısı azalmış hem de ilk düğüm kaybına kadar geçen süre uzamıştır.



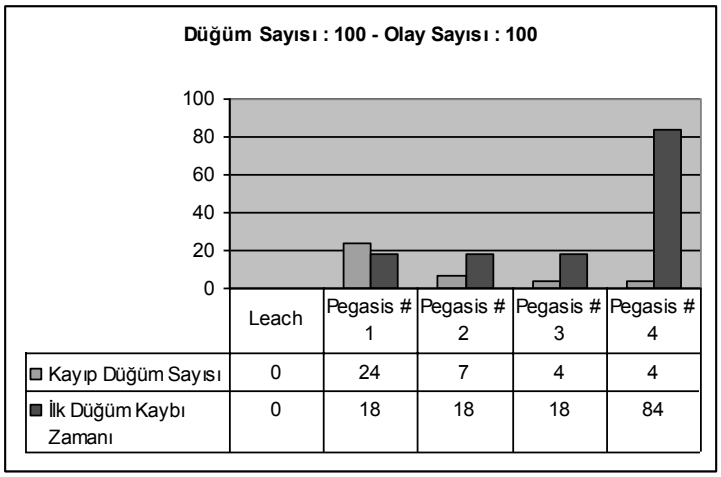
Şekil-5: Leach – Pegasis algoritmalarının algılanan olay sayıları bakımından karşılaştırması , D.S = 100



Şekil-6: Leach – Pegasis algoritmalarının kurulan bağlantı sayıları bakımından karşılaştırması , D.S = 100 , O.S = 100



Şekil-7: Leach – Pegasis algoritmalarının toplam atılan adım ve harcanan enerji bakımından karşılaştırması , D.S = 100 , O.S = 100



Şekil-8: Leach – Pegasis algoritmalarının kayıp düğüm sayısı ve ilk düğüm kaybı zamanı bakımından karşılaştırması , D.S = 100 , O.S = 100

IV. SONUÇ

Geliştirdiğimiz SensoNet programı ile farklı düğüm sayılarına sahip kablosuz sensör ağların, farklı sayıda olayların algılanması amacıyla Leach, Flooding ve Pegasis yönlendirme algoritmalarını kullanarak simülasyonunu gerçekleştirdik. Bu simülasyonlardan elde edilen veriler ışığında, bahsedilen üç algoritma için aşağıdaki değerlendirmeleri yapabiliriz.

Leach algoritması adım adım yönlendirme öngörmediği, doğrudan iletşim modelini kullandığından dolayı ağ üzerinde veri paketlerinin iletilmesi için Flooding ve Pegasis algoritmalarından daha az adım atılmasına ihtiyaç duyar. Adım sayısındaki düşüş, gecikme zamanı, kullanılan bandwidth, harcanan enerji ve buna bağlı olarak kayıp düğüm sayısı, kayıp düğüm sayısının ağın algılama kabiliyetini etkilemesi sonucunda algılanan olay sayısını ve algılanan olayın doğruluğunu doğrudan etkiler. Bu bakımdan yapılan simülasyon sonuçlarında Leach (Low Energy Adaptive Clusthering Hierarchy) algoritması diğer algoritmalara göre daha iyi sonuç vermiştir.

Flooding algoritmasının simülasyon sonuçlarına bakıldığında, ileri derecede kaynak sınırlılığı bulunan kablosuz sensör ağlarda kullanılması tavsiye edilebilir bir algoritma olmadığı anlaşılır. Adım sayısı, kullanılan bandwith, kurulan bağlantı sayısı, kopya (duplicate) paket sayısı, kayıp düğüm sayısı ve kayıp düğüm sayısına bağlı olarak ağın topolojisinde meydana gelen aşırı bozulma göz önüne alınarak bu çıkarım yapılabilir. Kayıp düğümlere bağlı olarak algılanan olayların doğruluk derecesi de tartışma konusudur.

Pegasis algoritmasının simülasyon sonuçlarına bakıldığında, zincirleme tekniği kopya paket sayısında önemli bir azalma sağlamıştır. Adım sayısı, kullanılan bant genişliği, kurulan bağlantı sayısı gibi değerleri, flooding algoritmasından onlarca kat daha iyidir. Zincir sayısındaki artış, atılan adım sayısı, kullanılan bandwith, kurulan bağlantı sayısı ve ölü düğüm sayıları üzerinde doğrudan etkiye sahiptir.

Aynı düğüm ve olay sayısı değerine sahip simülsyon sonuçları karşılaştırıldığında Pegasis # 1 ile Pegasis # 4 arasında, ölü düğüm sayısında 6 kata varan fark gözlemlenmiştir. Aynı zamanda zincirlemenin doğasında olan gecikme süresinin fazla oluşu zincir sayısı artırılarak önemli oranda düşürülebilmektedir. Zincir sayısının artırılması, ağa fazladan hesaplama maliyeti getirecektir, düğümlerin komşularının yer bilgisine sahip olması gerekir.

Her düğüm kaybı sonrasında, iletişimde kopmalar olmaması için, zincir(ler)in tekrar kurulmasına ihtiyaç duyulması olumsuz bir etkendir.

Sonuç olarak, her düğüme doğrudan iletişim izni verilemeyecek ağlarda Pegasis algoritması flooding yerine kullanılabilir. Doğrudan iletişimin herhangi bir kısıtlamaya tabi olmadığı ağlarda ise Leach algoritması tercih edilebilir.

REFERANSLAR

[1] Wang, Q., Hassanein, H., Xu, K., 2005; Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems: "A Practical Perspective on Wireless Sensor Networks" .
[2] Feng, J., Koushanfar , F., Potkonjak, M., 2005; Handbook of Sensor Networks Compact Wireless and Wired Sensing Systems : "Sensor Network Architecture" .
[3] Slijepcevic, S., Wong, J. L., Potkonjak, M. 2005; Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems ; "Security and Privacy Protection in Wireless Sensor Networks" .
[4] Shi, E., Perrig, A., 2004; "Designing Secure Sensor Networks" , Aralık.
[5] Perrig, A., Szewczyk, R., Wen, V., Culler, D., Tygar, J. D., 2001; "SPINS Security Protocols for Sensor Networks" , MobiCom
[6] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., Cayirci, E. 2002; A Survey on Sensor Networks, IEEE Communication Magazine.
[7] Ahmed, A. A., Shi, H., Shang, Y., 2003; A Survery On Network Protocols For Wireless Sensor Networks IEEE.
[8] Heinzelman, W. R., Chandrakasan, A., Balakrishnan, H., 2000; Energy-Efficient Communication Protocol for Wireless Microsensor Networks.

Halil Hakan TARHAN 18 Aralık 1983 İstanbul – Zeytinburnu'da doğdu. 1997 yılında Göztepe Gözcübaba Lisesi'nde ilköğrenimini tamamladı. 2001 yılında Kadıköy Kenan Evren Anadolu Lisesinde ortaöğrenimini tamamladıktan sonra İstanbul Üniversitesi Bilgisayar Mühendisliği Bölümü'nü kazandı. Haziran2006'da bölümünden mezun olmuştur. Şu an İstanbul Üniversitesi'nde yazılım geliştirici olarak çalışmaktadır.

Zeynep GÜRKAŞ AYDIN 17 Temmuz 1981 tarihinde Kırklaereli'nde doğdu. Lisans eğitimini Haziran 2003'de İstanbul Üniversitesi Bilgisayar Mühendisliğinde,yüksek lisans eğitimini Temmuz 2005'de İstanbul Üniversitesi Bilgisayar Mühendisliği bölümünde tamamladı.Aralık 2003 tarihinden itibaren İstanbul Üniversitesi Bilgisayar Mühendisliği Bölümünde Araştırma Görevlisi olarak çalışmaktadır. Çalışma konuları, ağ güvenliği ve bilgisayar ağları ve haberleşme,kablosuz ağlar ve gezginlik,sensor ağlardır.

M.Ali AYDIN 02Şubat 1979 tarihinde Herborn,Almanya'da doğdu. Lisans eğitimini Haziran 2001'de İstanbul Üniversitesi Bilgisayar Bilimleri Mühendisliğinde,yüksek lisans eğitimini Ocak 2005'de İstanbul Teknik Üniversitesi Bilgisayar Mühendisliği bölümünde tamamladı. Kasım 2001 tarihinden itibaren İstanbul Üniversitesi Bilgisayar Mühendisliği Bölümünde Araştırma Görevlisi olarak çalışmaktadır.Araştırma konuları, ağ güvenliği ve kriptografi,bilgisayar ağları ve haberleşme,optik ağlardır.