Kablosuz Algılayıcı Ağlarda Güvenlik Sorunları ve Alınabilecek Önlemler

Eyüp Burak CEYHAN, Şeref SAĞIROĞLU
Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü,
Gazi Üniversitesi, Ankara, Türkiye

ÖZET

Günümüzde kablosuz algılayıcı ağların verimliliği ve kullanılabilirliği hakkında birçok çalışma olmasına rağmen bu ağların güvenliği konusunda yeterli miktarda çalışma yoktur. Peki, bu kablosuz algılayıcı ağları oluşturan trilyonlarca küçük algılayıcıların güvenliği nasıl sağlanacaktır? Bu ağların güvenliği, masaüstü bilgisayarlar kadar kolay değildir. Çünkü bu algılayıcıların işlemci gücü, hafıza, bantgenişliği ve enerji gibi bazı kısıtları vardır. Dolayısıyla yapısı çeşitli saldırılara açıktır. Bu çalışmada kablosuz algılayıcı ağların yapısı, bu ağların ana çalışma konuları, bu ağlarda güvenlik hedefleri, temel ağ saldırıları, güvenlik protokolleri, güvenli yönlendirme ve güvenli servis modelleri ele alınmıştır. Güvenliği sağlamak için çeşitli çözümler sunan makaleler incelenerek bu bildiriler ve makalelerde bulunan açıklıklarlistelenmiş, kablosuz algılayıcı ağ güvenliğinin nasıl sağlanması gerektiği üzerinde çalışmalar özetlenmiştir. Elde edilen bulgular sonuçta tartışılmıştır.

Anahtar Kelimeler : Kablosuz algılayıcı ağ; güvenlik; protokol; önlem; saldırı.

Security Issues on Wireless Sensor Networks and The Possible Precautions

ABSTRACT

Nowadays, there are lots of study which include wireless sensor networks' efficiency and usability but there aren't enough study that includes its security. Then, how can the security of trillions of small sensors (which form the wireless sensor network) be provided? The security of these networks is not as easy as security of desktop computers. Because, there are constraints which are CPU power, memory, bandwidth and energy in these sensors. Hence, its structure is vulnerable to various attacks. In this study, structure of wireless sensor networks, main study subjects of these networks, security goals on these networks, basic network attacks, security protocols, secured routing and secured service models are handled. By examining articles which offer solutions for security, the vulnerabilities in these articles are listed and the articles are summarized on how the security of wireless sensor networks must be provided.

Keywords : Wireless sensor network; security; protocol; protection; attack.

I. GİRİŞ (INTRODUCTION)

Donanım, üretim teknolojisi ve bilgi iletişimi teknolojisi geliştikçe çeşitli özel uygulamalar için ağ yapısı geliştirmek daha önemli hale gelmiştir. Kablosuz algılayıcı ağlar küçük, düşük maliyetli, kablosuz iletişimi kullanan, çok sayıda algılayıcılardan oluşan ve birçok çevreye uyarlanabilen, dolayısıyla doğa görüntülemesi, sağlık ve ev aletleri yönetimi gibi birçok uygulama alanında başarıyla kullanılmaktadır. Fakat kablosuz algılayıcı ağların kaynakları kısıtlıdır ve düşman alanlar gibi zorlu şartlar altında bile konumlandırılabilmektedir. Dolayısıyla kablosuz algılayıcı ağların iletim kanalları ile algılayıcı düğümleri arasındaki düğüm iletişimi çeşitli saldırılara açıktır [2].

Algılayıcı ağlar askeri, çevresel, nükleer ve daha birçok alanda rahatlıkla izleme, takip ve karar destek sistemi ön veri oluşturulması için kullanılmaktadır [6]. Bir algılayıcı ağın yapısında genel olarak kendi aralarında haberleşebilen birçok düğüm ve düğümlerin haberleştikleri istasyon veya sink bulunmaktadır [14]. Algılayıcılar ağ mimarisine göre kümeler, ağaç yapısı veya grid benzeri yapılar şeklinde bulunarak hem birbirleri hem de sink arasında haberleşmektedir. Yapıları gereği uygulamaya bağlı olarak değişmekle birlikte periyodik bir biçimde veriyi algılayıp işleyerek sinke iletirler. Veri iletim periyodu da uygulamaya göre değişmektedir [8].

Kablosuz algılayıcı ağlarda algılayıcı düğümler yani algılayıcılar bulunmaktadır. Ağdaki her bir algılayıcı bir mikroişlemci ve güç kaynağına sahiptir. Algılayıcı düğümler, ortamı gözlemleme, verileri işleme ve işlenmiş veya işlenmemiş veriyi diğer düğümlere iletme işlerini yaparlar. Veriyi ağdaki düğümlere iletmek için farklı iletim teknolojileri kullanılmaktadır. En sık kullanılan teknolojiler, güç kullanımının az olduğu Bluetooth ve ZigBee teknolojileridir. Kullanım ömrü, dayanıklılık ve hata toleransı gibi farklı parametrelere göre var olan teknolojiler arasında tercih yapılmaktadır. Ayrıca algılayıcı ağlarda algılayıcı düğümler tarafından gönderilen verinin nasıl bir yapıya sahip olacağını tanımlayan standartlar vardır. Verinin

* *Sorumlu Yazar (Corresponding Author)*
e-posta: ebceyhan@gazi.edu.tr
Digital Object Identifier (DOI) : 10.2339/2013.16.4, 155-163

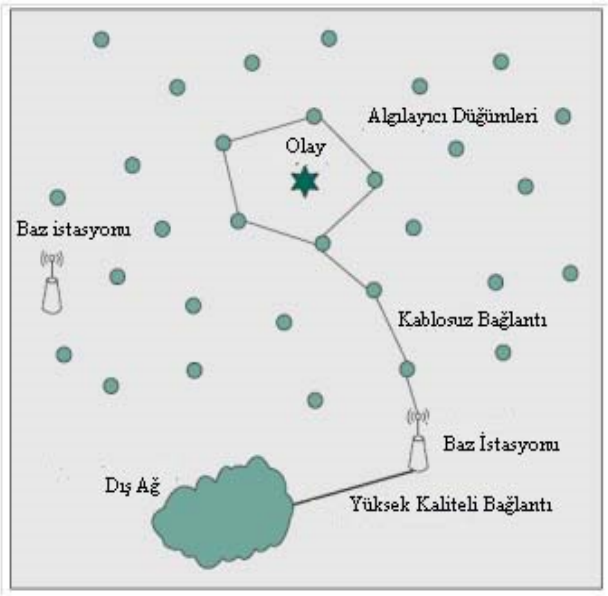
standart yapıda olması, farklı sistemlerin beraber çalışabilmesine olanak sağlar [10].

Bazı algılayıcı ağ uygulamalarında algılayıcılar binaların, kişilerin ve yolların bilgisi hakkında bilgi toplamakta ve bu bilgileri güvenli bir şekilde acil çağrı personeline iletmektedir [1].

Kablosuz algılayıcı ağlar gerçekleşmek üzere olan orman yangını, tsunami, volkan hareketleri gibi felaketleri tespit etmede de kullanılmaktadır [12].

Algılayıcılar genelde durağandır. Sensor düğümleri yerleştirildikten sonra çevreyi gözetlemektedirler. Bir olay olduğunda çevredeki sensor düğümlerinden biri olayı tespit eder, bir rapor oluşturur ve bu raporu baz istasyonuna kablosuz bağlantı aracılığıyla gönderir. Çevreyi gözetleyen düğümlerin aynı olayı farketmesiyle işbirliği gerçekleşebilir. Bu durumda bunlardan biri diğer düğümlerle işbirliği yaptıktan sonra sonuç raporu oluşturur. Baz istasyonu bu sonucu işler ve daha fazla işlemek için dış dünyaya yüksek kaliteli kablolu veya kablosuz bağlantı aracılığı ile iletir. Kablosuz algılayıcı ağ uzmanları, hazırladıkları komut veya sorguları ağa yayacak olan bir baz istasyonuna gönderebilir. Dolayısıyla bir baz istasyonu, kablosuz algılayıcı ağ ve dış dünya arasında bir ağ geçidi gibi davranmaktadır. Kablosuz algılayıcı ağların genel yapısı Şekil 1'de gösterilmektedir[9].

Özellikle teröristler tarafından planlanan birçok felaket senaryolarında, yetkisiz ulaşımlardan kişilerin yerini korumak zorunludur. Ayrıca, kimyasal, biyolojik veya diğer çevresel tehditlerin görüntülendiği uygulamalarda ağın ulaşılabilirliğinin etkilenmemesi hayatidir. Hatalı alarm oluşturan saldırılar, panik ataklara veya sinyaller için daha kötü ihmallere zorlayabilir. Sağlık hizmetlerinde de gizliliğin korunması önemlidir. Sadece yetkilendirilmiş kişilerin ağa ulaşması ve görüntülemesi sağlanmalıdır [3].



Şekil 1. Kablosuz algılayıcı ağların genel yapısı [9]

Bu çalışmada genel olarak güvenliği sağlamak için çeşitli çözümler sunan makaleler incelenerek kablosuz algılayıcı ağ güvenliğinin nasıl sağlanması gerektiği üzerinde durulmuştur. İkinci bölümde bu ağların ana çalışma konuları, üçüncü bölümde kablosuz algılayıcı ağlarda güvenlik hedefleri, dördüncü bölümde bazı kablosuz algılayıcı ağ saldırıları, son bölümde ise güvenlik protokolleri, güvenli yönlendirme ve güvenli servis örnekleri ele alınmıştır.

II. KABLOSUZ ALGILAYICI AĞ GÜVENLİĞİNİN ANA ÇALIŞMA KONULARI (MAIN STUDY SUBJECTS OF WIRELESS SENSOR NETWORK SECURITY)

Kablosuz algılayıcı ağların güvenliği araştırmalarında kullanılan dört ana tema vardır. Bunlar alt başlıklar şeklinde sırasıyla verilmiştir.

A. Anahtar Yönetimi (Key Management)

Kablosuz algılayıcı ağların dinamik yapısından ve kolay düğüm uzlaştırılabilmesinden dolayı, anahtar yönetimi çok komplekstir. Kendi kendini örgütleme özelliği anahtar yönetiminin zorluğunu artırır ve bu alandaki çalışma konularını ileri taşımaktadır [2].

B. Saldırı Tespiti ve Önlemler (Intrusion Detection)

Limitli iletişim ve hesaplama kapasitesinden dolayı kablosuz algılayıcı ağlar saldırılara açıktır. Birçok durumda, kablosuz algılayıcı ağları nasıl tasarladığımızın hiçbir önemi olmadan, saldırganlar ağa sızmanın bir yolunu bulabilmektedir. Saldırı tespit sistemleri bu saldırıları kural dışı olaylar tabanlı tespit edebilmektedir [2].

C. Güvenli Yönlendirme (Secure Routing)

Kablosuz algılayıcı ağlar, orta seviyedeki düğümün veri mesajının içeriğine ulaşmaya ihtiyaç duyduğundan veriyi iletmek için multi-hop yönlendirme ve kablosuz iletişim kullanmaktadır. Dolayısıyla birçok yönlendirme saldırısı olabilmektedir. Geleneksel uçtan uca güvenlik mekanizmaları kablosuz ağlarda birşey yapamamaktadır. Dolayısıyla yönlendirme güvenliğini ele alan birçok yaklaşım bulunmaktadır [2].

D. Güvenli Konumlandırma (Secure Positioning)

Kablosuz algılayıcı ağlarda, düşman çevrelerdeki koordinatlara ulaşma gibi bazı uygulamalarda konum bilgisi çok önemlidir. Bu tür uygulamalarda, birçok yönlendirme protokolleri veya diğer güvenlik mekanizmaları da konum bilgisi veya komşu düğümler arasındaki uzaklık bilgisine ihtiyaç duymaktadır [2].

III. KABLOSUZ ALGILAYICI AĞLARDA GÜVENLİK HEDEFLERİ (SECURITY OBJECTIVES ON WIRELESS SENSOR NETWORKS)

Literatür incelendiğinde, güvenlik hedefleri birincil ve ikincil olmak üzere iki sınıfa ayrılabilir. Birincil hedefler, gizlilik, bütünlük, kimlik doğrulama ve kullanılabilirlik gibi standart güvenlik hedefleridir.

İkincil hedefler ise veri güncelliği, kendi-kendini örgütleme, zaman senkronizasyonu ve güvenli konumlandırma gibi etkenlerdir [3]. Bunlar aşağıda kısaca özetlenmiştir.

A. Birincil Hedefler (Primary Objectives)

1. Veri Gizliliği (Data Privacy)

Gizlilik, mesajları pasif saldırgandan koruma kabiliyetidir. Böylelikle algılayıcı ağ üzerinden iletilen herhangi bir mesaj gizli kalabilmektedir. Bu, ağ güvenliğinde en önemli konudur. Bir algılayıcı düğüm komşularına verilerini ifşa etmemelidir [3]. Dinleme gibi pasif saldırılara karşı hassas verilerin korunması gerçekleştirilmelidir [5].

Bir algılayıcı ağ komşu ağlara algılayıcı okumalarını sızdırmamalıdır. Birçok uygulamalarda düğümler yüksek hassasiyetli veriler taşır. Hassas verileri gizli tutmanın standart yolu, veriyi sadece ilgili alıcının ulaşabileceği gizli bir anahtarla şifrelemektir. Bu şekilde gizlilik sağlanmış olur [1].

Birçok uygulamada, algılayıcı düğümler gizli anahtarlar gibi çok hassas veriler iletmektedir, dolayısıyla algılayıcı düğümler arasında güvenli kanallar oluşturmak önemlidir. Algılayıcı bilgisi ve açık anahtarlar gibi genel algılayıcı bilgisi de, trafik analiz saldırılarından korunmak için şifrelenmelidir. Yönlendirme bilgisi de, zararlı düğümün bu bilgiyi ağ performansını düşürmesi gibi belli durumlarda gizli kalmalıdır. Hassas verileri gizli tutmak için kullanılan standart yaklaşım veriyi sadece ilgili alıcının ulaşması için gizli bir anahtar ile şifrelemek böylelikle gizliliği sağlamaktır. Buna rağmen veri kümeleme protokolleri genelde şifrelenmiş veriyi kümeleyemez. Bu nedenle, bu kümeleme protokolleri, veri kümelemeyi gerçekleştirebilmek için ve kümelenmiş veriyi iletmeden önce şifrelemek için algılayıcı verisinin şifresini çözmelidir [4].

İlk bakışta doğru kişiyle konuştuğu anlaşılamayan durumlarda gizlilikten bahsetmek zordur. Gizlilik, herhangi bir anahtar kullanarak açılan oturumun şifrelenmesine dayalıdır. Fakat şu bilinmelidir ki, paylaşılan anahtar ve doğru zaman kaynağı olmadığı durumlarda bu teknikler yakın düğümlerle iletişim kurarken problem yaşatabilir [20].

2. Veri Doğrulama (Data Verification)

Kablosuz algılayıcı ağlar, paylaşımlı kablosuz ortam kullandıklarından dolayı, algılayıcı düğümler kötü niyetle bulaşan veya sahte paketi tespit etmek için doğrulama mekanizmalarına ihtiyaç duyarlar. Kaynak doğrulama iletişim kurduğu eş düğümün özelliğini garantilemek için bir algılayıcı düğümünü etkinleştirir. Kaynak doğrulama olmadan, düşman bir düğümü ele geçirebilir ve böylelikle kaynağa, hassas bilgiye yetkisiz erişim sağlayabilir ve diğer düğümler arasındaki işlemlere parazit sokabilir [4]. Veri doğrulama, gizli anahtarların gönderen ve alıcı düğümlerin paylaşması durumunda simetrik ve asimetrik mekanizmaları kullanarak sağlanabilir [3].

Mesaj doğrulaması algılayıcı ağlardaki birçok uygulama için önemlidir. Buna ağın tekrar programlanması gibi yönetimsel görevler ve algılayıcı düğümü görev döngüsünü kontrol etme de dahildir. Düşman mesajlara kolayca erişebileceğinden dolayı, alıcının gelen mesajdaki verinin güvenli bir kaynaktan gelip gelmediğinden emin olması gerekmektedir. Veri doğrulama, alıcıya gelen mesajın beklenen göndericiden gelip gelmediğini doğrulamayı sağlar [1].

Veri doğrulama simetrik mekanizmalarla sağlanabilir. Burada gönderici ve alıcı tüm iletilen verinin mesaj doğrulama koduyla (MAC) hesaplanması için gizli bir anahtar paylaşırlar. Doğru bir MAC'e sahip bir mesaj ulaştığında, alıcı bu mesajın gönderici tarafından gönderilmiş olduğunu anlamaktadır. Fakat bu tür doğrulama, ağ düğümlerinde daha güçlü güven unsurları yerleştirmeden dağıtım (broadcast) ayarlara uygulanamaz. Eğer bir gönderici doğrulamalı veriyi karşılıklı olarak güven duyulmayan alıcılara göndermek isterse, simetrik MAC kullanmak güvenli değildir: Alıcılardan herhangi biri MAC'i bilmektedir. Dolayısıyla göndericiyi taklit edebilir ve diğer alıcılara sahte mesajlar gönderebilir. Bu nedenle, doğrulanmış yayın için asimetrik bir mekanizma kullanmak gerekir [1].

3. Veri Bütünlüğü (Data Integrity)

Veri bütünlüğü, iletilen bir mesajın kesintiye uğramamasını garanti eder. Zararlı bir düğüm, mesajları keserek ağın düzgün çalışmasını engelleyebilir. Güvenilir olmayan iletişim kanallarından dolayı içeri sızan biri olmadan dahi veri değiştirilebilir. Bu nedenle mesaj doğrulama kodları veya döngüsel kodlar veri bütünlüğünü korumak için kullanılır [4]. Ağın bütünlüğünün tehlikede olduğu durumlar arasında, zararlı bir düğümün ağa hatalı veri sunması veya kablosuz kanalın zarara veya veri kaybından kaynaklanan istikrarsız durumlar sayılabilir [3]. Verilerin aktarım sırasında bozulması ve dışarıdan yapılacak kötücül bir müdahale ile veriye ulaşılamaması durumlarında verinin bütünlüğü bozulabilir [15].

4. Kullanılabilirlik (Usability)

Kullanılabilirlik, ağ servislerinin hizmet aksatma servis saldırılarına (DoS) karşı izlenebilirliğini garanti eder. DoS saldırısı kablosuz algılayıcı ağın herhangi bir katmanında gerçekleşebilir ve hedef düğüm veya düğümleri kısa süreli etkisiz hale getirebilir. DoS saldırılarına ek olarak, lüzımsuz iletişim veya hesaplamalar bir algılayıcı düğümün pil ömrünü bitirebilir. Örneğin savaş alanı gözetleme uygulamalarında bazı algılayıcı düğümlerinin kullanılabilirliği sağlanamazsa bu, düşman istilasına sebep olabilir. Bu gibi kullanılabilirlik kayıplarını tolere etmek için kablosuz algılayıcı ağlar çok sayıda düğümle donatılırlar [4]. Fakat algılayıcıların enerjisi tükenebilmektedir ve ağır çevre koşullarından kaynaklanan iletişim bağlantı kopuklukları da yaşanabilmektedir [19]. Dolayısıyla algılayıcılar,

iletilecek veri olmadığı durumlarda uyku moduna geçerek enerjilerini korumaktadırlar [7].

Askeri olmayan senaryoların çoğunda kullanılabilirlik, kullanıcılar için en önemli güvenlik özelliğidir. Bu sorunlardan bazıları radyo paraziti ve pil tükenmesidir. Örneğin radyo parazitinde, saldırgan kullanıcının sistemi kullanamaması için düğümler arasındaki bağlantıyı radyo frekansları arasında boğma (jamming) uygulayarak iletişimi kesebilir. Böylelikle kullanıcı bu sistemi kullanamaz hale gelir. Yine aynı şekilde, pil de kritik parametrelerden biridir. Uyku modunda düğümler çoğu vaktini tekrar uyanabilmek için geçirir. Bu durumda hizmet kullanımı atakları gerçekleştirilerek sistem kullanılamaz hale getirilip saldırgan istediği gibi iz bırakmadan hareket edebilir. Pil tükenmesi durumunda ise yine aynı şekilde kullanıcı pil tükendiği için sistemi kullanamaz hale gelir. Bu nedenle tasarımcılar bu gibi kullanılabilirlik problemlerini çözmek için önlemler almaktadırlar [20].

B. İkincil Hedefler (Secondary Objectives)[3]

Literatürde ikincil hedefler [3] nolu referansta detaylı şekilde açıklanmıştır. Aşağıda ise kısaca açıklanmıştır.

1. Veri Güncelliği (Data Freshness)

Gizlilik ve bütünlük sağlansa bile her mesajın güncelliğinden emin olmak gerekmektedir. Veri güncelliğinde, verinin var olduğu tespit edilir ve eski mesajların tekrarlanmadığından emin olunur. Bu problemi çözmek için zamanla ilgili sayaç, verinin güncelliğinden emin olmayı sağlama adına paketlerin içine eklenebilir [3].

2. Kendi Kendine Örgütlenme (Self-Organization)

Bir kablosuz algılayıcı ağ, her algılayıcı düğümünün farklı durumlarda kendi kendine örgütlenmesi ve temizlenmesi için yeterince bağımsız ve esnek olduğu tipik bir ad hoc ağdır. Algılayıcı bir ağda ağın yönetimi için sabit bir yapı yoktur. Bu doğal özellik, kablosuz ağ güvenliği için büyük bir açık oluşturmaktadır. Eğer bir algılayıcı ağda kendi kendine örgütlenme düşerse, saldırıdan veya riskli ortamlardan kaynaklanan zarar müthiş zarar verebilir [3].

3. Zaman Senkronizasyonu (Time Synchronization)

Çoğu algılayıcı ağ uygulamaları zaman senkronizasyonunun bazı yöntemleri üzerine kurulmuştur. Veriler iki algılayıcı arasında taşınırken bir paketin uçtan uca gecikmesini hesaplamaya ihtiyaç duyabilir. Daha işbirlikçi bir algılayıcı ağ, takip etme uygulamaları için grup senkronizasyonu içerebilir [3].

4. Güvenli Konumlandırma (Secure Localization)

Genelde, bir algılayıcı ağın özelliği ağdaki her algılayıcıyı tam ve otomatik olarak konumlandırmayı sağlama kabiliyetine bağlıdır. Algılayıcı ağ, hatanın lokasyonunu göstermek için lokasyon bilgilerini sağlayabilecek şekilde tasarlanmıştır. Buna rağmen, saldırgan güvenli olmayan konum bilgisini hatalı sinyaller rapor ederek kolayca manipule edebilir [3].

IV. KABLOSUZ ALGILAYICI AĞ SALDIRILARI (ATTACKS ON WIRELESS SENSOR NETWORKS)

Algılayıcı ağ saldırıları iç saldırılar ve dış saldırılar olmak üzere ikiye ayrılırlar. İç saldırılarda, saldırgan algılayıcı düğümleri ve gizli anahtarı ele geçirerek içten saldırır. Dış saldırılarda ise saldırgan gizli anahtar bilgisine sahip olmadan kendi algılayıcı düğümleri ile hedefindeki algılayıcı ağın işlevini bozacak şekilde saldırılar düzenler [15].

Bu bölümde en fazla kullanılan saldırı yöntemlerinden hizmet aksatma servis saldırıları, tekrarlama saldırıları ve düğümlerin ele geçirilmesi özet bir şekilde incelenmiştir.

A. Hizmet Aksatma Servis Saldırıları (DoS-Denial of Service)

En tehlikeli saldırılardan biri DoS saldırılarıdır. Bu saldırıların amacı sunucuya çok fazla hizmet talebi göndererek sunucuların kaynağını tüketip, düğümlerin kendi aralarında ve merkezle olan haberleşme kanalını gereksiz paketlerle doldurmaktır [16].

Bu saldırı yönteminde en fazla kullanılan atak Sybil saldırılarıdır. Bu saldırı yönteminde çok sayıda sahte kimliğe sahip kötücül bir düğüm, hedefteki düğümün işlevini bozarak merkeze ulaşacak bilgilerin değiştirilmesine sebep olmaktadır [17].

DoS saldırıları algılayıcı ağların işlevini bozmakta veya tamamen iptal etmektedirler. Algılayıcı ağlar genelde katmanlardan oluştuğu için ve saldırılara müsait bir yapı taşıdığından dolayı saldırılar katmanların herhangi birinde yapılabilmektedir [13].

B. Tekrarlama Saldırıları(Replay Attacks)

Kablosuz iletişim ortamındaki akan mesajı saldırganın keserek, tekrarlanan yeni oturumlar başlatarak düğümlerin meşgul edilmesi sağlanır [18].

C. Düğümlerin Ele Geçirilmesi (Node Capturing)

Saldırgan, sadece bir algılayıcı düğümünün kontrolünü ele geçirerek şifreleme anahtarlarını, depolanan verileri ele geçirebilmektedir [18].

V. KABLOSUZ ALGILAYICI AĞLARDA GÜVENLİK PROTOKOLLERİ, GÜVENLİ YÖNLENDİRME VE GÜVENLİ SERVİS ÖRNEKLERİ (SECURITY PROTOCOLS, SECURE ROUTING AND SECURE SERVICE SAMPLES ON WIRELESS SENSOR NETWORKS)

Literatürde, kablosuz algılayıcı ağlarda çeşitli güvenlik protokolleri, güvenli yönlendirme çeşitleri ve güvenli servis örnekleri bulunmaktadır. Yapılan bir çalışmada yazarlar SNEP ve µTESLA adında, kablosuz iletişim ve kısıtlı kaynaklı ortamlar için optimize edilmiş güvenlik yapı taşları üzerinde durmuşlardır. SNEP veri gizliliği, ikinci parti veri doğrulaması ve veri

güncelliğini sağlamak gibi önemli güvenlik unsurlarını sağlamaktadır. µTesla ise kısıtlı kaynaklı ortamlar için doğrulamalı yayın imkanını tanıyan yeni bir protokoldür. SNEP ile semantik güvenlik, veri doğrulaması ve cevaplama koruması, güncellik ve düşük haberleşme gideri gibi özellikler sağlanmıştır. Yine µTesla ile de simetrik kriptoloji tabanlı bir güvenlik sağlanmıştır. Yazarlar bu iki protokolü geliştirmiş ve düşük donanımlarda bile pratik olduklarını göstermişlerdir. Bunlara ek olarak yüksek seviyeli protokol oluşturmada bunların kullanılabileceğini göstermişlerdir. Tasarımlarının birçok elemanı evrenseldir ve diğer algılayıcı ağlara kolayca uygulanabilmektedir. Sürdürdükleri çalışmalarda, bu ağlar ile çevresel parametreleri ölçtürmüş ve hava temizlemesini ve ışıklandırma sistemlerini kontrol etmede kullanmayı denemişlerdir. Fakat üçüncü partilerin bu algılayıcı verilerini okumasındaki güvenlik açıklarını çözememişlerdir. Sınırlı platformlarına rağmen mesaj gönderme veya alma için harcanan enerjiyle harcanan enerji karşılaştırıldığında, güvenlik için harcanan enerji göz ardı edilebilecek kadardır. İletişim maliyetleri de düşüktür[1].

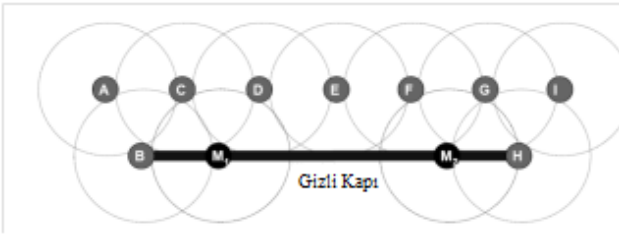
Ağ işlemeyi desteklemek için bir başka makalede yazarlar LEAP (Lokalize Şifreleme ve Kimlik Doğrulama Protokolü) adında, tasarlanan algılayıcı ağların en kritik yönetim protokolünü geliştirmişlerdir. Bu protokol aynı zamanda bir düğümün gizliliğini ihlal eden ağ komşularının etkisini kısıtlamaktadır. Bu protokol, düğümler arasında alınıp verilen farklı güvenlik gereksinimlerinin gözlenmesinden ve bu gereksinimleri birleştirerek tek bir anahtarlama mekanizması uygun olmadığından yola çıkılarak yapılmıştır. LEAP, her bir algılayıcı düğüm için dört tür anahtar kurulmasını destekler. Bunlar, baz istasyonu ile paylaşılan bir tek anahtar, başka bir algılayıcı düğüm ile paylaşılan bir ikili anahtar, birden fazla komşu düğümler ile paylaşılan bir küme anahtarı ve ağdaki tüm düğümler ile paylaşılan grup anahtarıdır. Bu anahtarların kurulması ve güncellenmesi için kullanılan protokol, iletişimde ve enerjideverimlidir ve baz istasyonunun ilişkisini en aza indirir. LEAP ayrıca tek yönlü anahtar zincirleri tabanlı yerel yayın kimlik doğrulama kullanımında verimli bir protokoldür. Yazarların performans analizi göstermektedir ki LEAP; hesaplamada, iletişimde ve depolamada çok verimlidir. Çeşitli saldırı modelleri altında yazarlar LEAP'in güvenlik analizini yapmıştır. Bu analiz de göstermektedir ki LEAP; Hello Floodsaldırıları, Sybil saldırıları ve Wormhole saldırıları gibi pek çok gelişmiş saldırılara karşı savunmada çok etkilidir. LEAP'de anahtar kullanımı ve anahtar güncelleme işlemleri verimlidir ve düğüm başına depolama gereksinimleri küçüktür [21].

Güvenliği sağlama amacıyla algılayıcı ağlarda rastgele anahtar üretimi üzerine yapılan bir çalışmada önyükleme problemi ele alınmıştır. Algılayıcı ağlarda anahtar oluşturma, önemli bir sorundur, çünkü asimetrik anahtar kripto sistemlerin, kaynak kısıtlaması olan algılayıcı düğümlerinde kullanımı uygun değildir. Ayrıca düğümler fiziksel olarak bir düşman tarafından yararlanılıyor olabilir. Yazarlar her düğüme önceden dağıtılan rastgele bir anahtar setini kullanarak anahtar oluşturmak için üç yeni mekanizma sunmuşlardır. Ilk olarak, q-kompozit anahtar düzeninde, yazarlar rastgele anahtar dağıtımını güçlendirmek için daha küçük ölçekli saldırılara karşı büyük ölçekli bir ağ saldırısı ihtimalini düşürmüşlerdir. İkinci olarak, çok yollu-takviye düzeninde, yazarlar diğer bağlantıların güvenliğinden yararlanarak herhangi iki düğüm arasındaki güvenliğin nasıl güçlendirileceğini göstermişlerdir. Son olarak, herhangi bir düğüm yakalandığında ağın geri kalanının haberleşmesinin gizliliğini mükemmel koruyan rastgele-ikili anahtar düzeni ve aynı zamanda düğümden düğüme kimlik doğrulama gösterilmiştir. Bu üç tasarının her biri rastgele anahtar protokollerinin tasarım alanında farklı bir uyuşma sağlar. Verilen bir uygulamada hangi tasarının en iyi olacağı en uygun uyuşmanın hangisinde olduğuna bağlıdır. Rasgele ikili düzen, üç düzenden en iyi güvenlik özelliklerine sahiptir. Yazarlar algılayıcı ağlar için anahtar yükleme düzeninde karakteristikleri karşılayan çeşitli kriterler belirlemişlerdir. Bunlar, düğüm yakalamaya karşı direnç, düğüm çoğaltmaya karşı direnç, geri alma ve ölçek gibi kriterlerdir. Yazarlar bu makalede her çözüm için birkaç öneri sunmuşlardır [22].

Algılayıcı ağların yörüngeleme protokolleri için mevcut çalışmalarda, düğümlerin limitli kapasitesinden dolayı ağ uygulamalarında optimizasyon ve güvenlik ele alınmaktadır. Yapılan bir çalışmada yazarlar algılayıcı ağlar için dizayn edilen protokollerin güvenlik boyutu ele almışlardır. Bu nedenle kablosuz algılayıcı ağlarda güvenlik yöntemleri oluşturmuşlardır. Kablosuz algılayıcı ağlarda güvenli yörüngeleme için tehdit modelleri ve güvenlik önerileri oluşturmuşlardır. Algılayıcı ağlar için iki saldırı sınıfı sunmuşlardır. Bunlar, sinkhole saldırıları ve Hello flood saldırılarıdır. Tasarsız ağlara ve eşler arası ağlara karşı yapılabilecek saldırılara karşı algılayıcı ağların nasıl korunabileceği gösterilmiştir. Algılayıcı ağlar için belli yörüngeleme protokolleri ve enerji koruma topoloji algoritmalarının güvenlik analizleri verilmiştir. Bu analizlere göre güvenli yörüngeleme protokolleri için alınabilecek önlemler ve tasarım önerileri sunulmuştur [23].

Birçok uygulama için kablosuz algılayıcı ağların kabulü ve kullanımında güvenli yönlendirme hayati bir değere sahiptir. Buna rağmen kablosuz algılayıcı ağlarda güvenli yönlendirmeyi sağlamak algılayıcı düğümlerin kapasitelerinin kısıtlı olmasından dolayı zor bir iştir. Yönlendirme protokolleri kablosuz algılayıcı ağlar için yıkıcı bir özelliğe sahip olabilmekte ve kablosuz algılayıcı ağlar için dayanıklı güvenlik mekanizmaları dizayn ederken büyük bir zorluk oluşturmaktadır. Yazarlar makalelerinde kablosuz algılayıcı ağlarda genel yönlendirme saldırılarının bazılarını ele almışlardır. Genel olarak, gizli kapı (wormhole) yönlendirme saldırıları bazı detaylarıyla

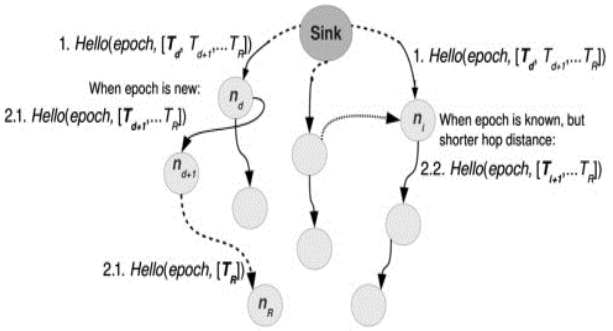
sunulmuştur. Bu saldırılar için çeşitli önlemler literatüre katılmıştır. Buna rağmen bu önlemlerin çoğunun geniş ölçekli kablosuz algılayıcı ağların kullanımı için etkili olmama gibi bazı kusurları bulunmaktadır. Kablosuz algılayıcı ağlarda bulunan içsel kısıtlamalardan dolayı yalınkat ve dayanıklı güvenlik mekanizmalarına ihtiyaç vardır. Wormhole yönlendirme saldırıları ve sunulan bazı yönlendirme saldırılarına karşı var olan protokolleri güçlendirme çok zordur. Yazarlar çalışmalarında kandırılmış (spoofed) yönlendirme bilgisi, seçici yönlendirme, yönlendirme gider deliği (sinkhole) saldırıları, sybil saldırıları, gili kapı (wormhole) saldırıları ve Hello flood saldırıları gibi bazı yönlendirme saldırılarından bahsetmişlerdir. Fakat geniş kapsamlı olarak wormhole saldırıları üzerinde durmuşlardır. Şekil 2'de gizli kapıya bir örnek verilmiştir. Wormhole saldırılara karşı önlemler arasında yönlendirme aşamaları süresince algılayıcı düğümleri arasında düşük zamanlı senkronizasyon sağlanması bulunmaktadır. Fakat bu teknik küçük kablosuz algılayıcı ağlarda limitli erişimi sağlamasına rağmen geniş ölçekli ağlarda uygun değildir. Bir diğer önlem ise coğrafi yönlendirme protokolleridir. Bu protokoller en kısa yol boyunca baz istasyonu trafiğini yönetir ve potansiyel reklamcılardan gelen reklamlara güvenmez. SeRWA adlı bir diğer güvenli yönlendirme protokolünde ise wormhole saldırıları özel donanıma sahip olmadan tespit edilebilmektedir. Sunulan öneriler arasında kablosuz algılayıcı ağlarda yer alan bu araştırma problemlerinin zengin alanında çalışmak için gizli kapı gibi saldırılarda anlamsızlığı gidermek için iyi dizayn edilmiş yeni yönlendirme protokollerinin ele alınması gerektiği belirtilmiştir [24].



Şekil 2. İki veya daha fazla kötü amaçlı düğümün birbirleri arasında kısa link oluşturması [24].

Doğru ve senkronize zaman, birçok algılayıcı ağ uygulamalarında, tutarlı algılama ve koordinasyon ihtiyacından dolayı çok önemlidir. Dış veya tehlikeli düğümler ile düşmanın ağ ve/veya uygulamalara saldırabileceği düşman ortamlarda, zaman senkronizasyonu, öneminden dolayı ilgi çekici bir konu haline gelmiştir. Yazarlar makalede, TinySeRSync protokolünün dizaynı, uygulaması ve değerlendirmesini açıklamışlardır. Bu makale üç katkıda bulunmaktadır: İlki, güvenli bir tek-sıçrama ikişerli zaman senkronizasyonu tekniğini donanım destekli zamandamgası doğrulamasıyla gerçekleştirmektedir. Önceki denemelerin aksine, bu teknik MICAz motes tarafından oluşturulan büyük veri hızını (MICA2 motesun aksine) ele alabilmektedir. İkincisi, bu makale yerel doğrulamalı genişbant için µTESLA genişbant doğrulama protokolünün yeni bir kullanımı tabanlı güvenli ve esnek bir global zaman senkronizasyonu protokolü oluşturmaktadır. Zaman senkronizasyonu sağlandığından dolayı çakışma da çözülür. Elde edilen protokol dış saldırılara karşı güvenli ve tehlikeli düğümlere karşı dayanıklıdır. Üçüncü katkı TinyOS üzerinde çalışan MICAz motes ve 60 MICAz motesun bir ağında alan deneyleri üzerinde hazırlanan tekniklerin bir uygulamasından oluşmaktadır [25].

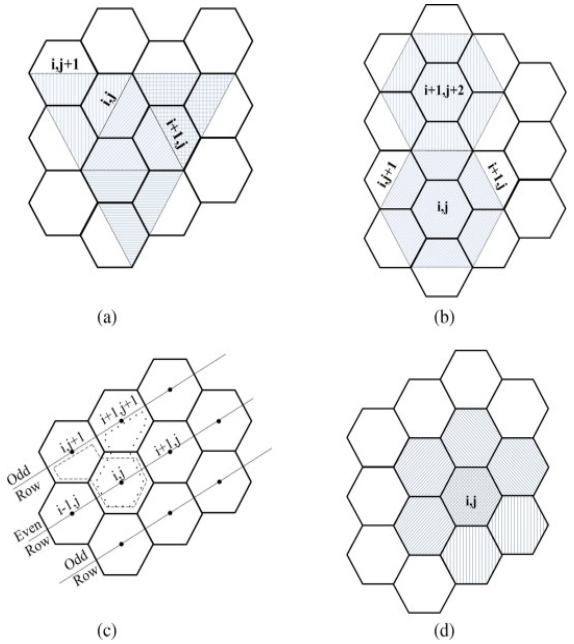
Yeni geliştirilen bir protokolde [26], güvenlik ve performans analizi ele alınmıştır. Bu çalışma, kablosuz algılayıcı ağlardakiağaç tabanlı yörüngeleme topolojilerinde seçici iletim saldırılarını etkilerini anlamaya ve sinkhole saldırılarının sebep olduğu ağ bozulmasını azaltmak için kriptografi tabanlı stratejileri incelemeye odaklanmıştır. Bu amaçla, çeşitli parameter setleri tabanlı zararlı saldırıların etkisi hakkında öncelikle bir simulasyon çalışması gerçekleştirmişlerdir. Bu çalışmaya dayalı olarak da, bu etkiyi açıklamak için tek fakat çok açıklayıcı bir metrik oluşturmuşlardır. Ayrıca iki adet kolay ve esnek topoloji tabanlı yeniden yapılandırma protokolleri geliştirmişlerdir. Yazarların simulasyon çalışmaları sonuçlarının detaylı analizleri, yeniden yapılandırma protokollerinin sinkhole saldırılarına karşı esnekliği artırmada, gizli anlaşmalar olduğunda bile pratik ve etkin olduğunu ortaya koymuştur. Şekil 3'de Resist-1'in genel yapısı gösterilmektedir.



Şekil 3. Resist-1'in genel yapısı [26]

Komşu algılayıcılar arasında anahtar dağıtımı, kablosuz algılayıcı ağlarda doğrulama ve gizlilik gibi güvenlik servisleri için çok öne çıkan bir konudur. Bugüne kadar biçok anahtar dağıtım tasarımı oluşturulmuştur fakat bunların çoğu güvenlik ve performans konularını ele almamışlardır. Yapılan bir çalışmada [27], yazarlar düşük kaynaklı algılayıcı ağlar için uygun yeni bir anahtar dağıtım protokolü geliştirmişlerdir. Şekil 4'de oluşturulan anahtar dağıtım modelleri gösterilmiştir. Bu protokolde her algılayıcı diğer algılayıcılarla bir gizli anahtar ve bazı genel anahtarlara sahiptir. Iki algılayıcı arasındaki bir genel anahtar, bir algılayıcının gizliliğini ve diğerinin kimliğini kullanarak oluşturulmuştur. Bu anahtar algılayıcılardan birinde saklanmıştır ve diğer algılayıcı güvenli bir iletişim gerektiğinde onu üretmektedir. Yazarlar bu protokolü, farklı anahtar dağıtım modelleri için geliştirmişlerdir. Hazırlanan model saldırılara karşı, bağlanabilirlik, ölçeklenebilirlik, bellek tüketimi ve

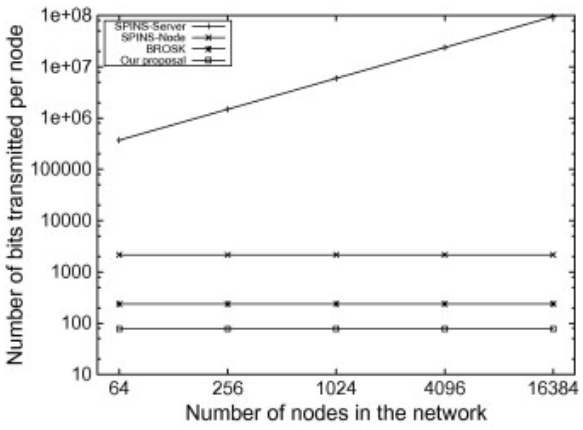
direnç tabanlı analiz edilmiştir. Önceki çalışmalarla karşılaştırıldığında, hazırlanan protokol düğüm saldırılarına karşı en esnek protokoldür. Buna ek olarak, düşük hafıza ihtiyacı ve düşük hesaplama yüküne sahiptir.



Şekil 4. Oluşturulan anahtar dağıtım modelleri, a)Düşük kaynak tüketimi b) Orta kaynak tüketimi c)İleri orta kaynak tüketimi d) Yüksek performans [27].

Kablosuz algılayıcı ağların askeriyede, reklamlarda ve evlerde artan uygulamalarıyla, ağdaki veriyi korumak kritik bir konu haline gelmiştir. TinySec gibi çeşitli güvenlik mekanizmaları KAA'larda güvenlik ihtiyacını ele almak için geliştirilmiştir. Buna rağmen, güvenlik maliyeti hâlâ bilinmeyen bir değer olarak kalmıştır. Bu maliyeti daha iyi anlamayı sağlamak için yazarlar KAA güvenliğinin 3 yönünü ele almışlardır [28].Bunlar şifreleme algoritmaları, blok şifreler için işlem yöntemleri ve mesaj doğrulama algoritmalarıdır. Yazarlar, MicaZ ve TelosB algılayıcılarda hafıza ve enerji tüketimini karşılaştırmışlardır. Deney sonuçları KAA ortamlarında kullanım için farklı güvenlik algoritmalarının uyumunu ve sistemlerinin güvenlik yapısını oluşturmak için KAA tasarımcılarının kullanabilmesini desteklemektedir.

Kablosuz algılayıcı ağlarda düşük ağırlıklı doğrulama modelleri üzerine yapılan bir çalışmada [29], bir anahtar yönetimi ve bir doğrulama protokolü oluşturulmuştur. Bu protokol çok düşük hesaplama ihtiyacı gerektiren basit simetrik kriptografi kullanımı tabanlıdır. Bu protokol literatürdeki diğer hazırlananlardan daha iyi sonuç vermektedir. SPINS ve BROSK protokolleriyle karşılaştırıldığında enerji harcanmasını %98 ve %67'lere kadar düşürmektedir. Şekil 5'de hazırlanan protokolün enerji tüketim miktarı gösterilmektedir. Ayrıca bu protokol,sadece bir yer değiştirme mesajı gerektirdiğinden dolayı, ağdaki düğümlerin sayısından bağımsız olarak, ağın boyutuna göre iyi ölçeklenebilmektedir.



Şekil 5. Enerji tüketimi [29].

Kablosuz algılayıcı ağlarda basit, düşük zamanlı, enerji tasarruflu kümeleme yapmak için hazırlanan bir protokolde yazarlar, ağ için artırılmış yaşam zamanı sağlayan, bir-seviye veri kümeleme gerçekleştirmişlerdir [30]. Hazırlanan protokol, bazı gezgin ve algılayıcı ağ yörüngeleme protokolleriyle karşılaştırılmıştır. Sonuçlar incelendiğinde, hazırlanan protokolünün diğer protokollerden verimlilik, gecikme, ortalama enerji tüketimi, ortalama ağ zamanı gibi kavramlarda daha başarılı olduğunu ortaya koymuştur. Bu protokol yörüngeleme için kriter olarak, kesin zaman ve düğüm enerjisini kullandığından dolayı güvenilirlik ve yoğunluğu azaltmayı sağlamaktadır.

Yapılan bir başka çalışmada [31], kablosuz algılayıcı ağlarda simetrik blok şifre işlemlerinin ileri yöntemleri üzerinde durulmuştur. Makale, bir kriptografik işlemde gizlilik ve doğrulamayı sağlamak için simetrik blok şifreleme işlemlerinin kullanılabileceği fikrini ortaya koymuştur. NIST tarafından onaylanan CMAC, CCM ve GCM/GMAC işlem yöntemleri kullanılmıştır. Doğrulanan şifreleme yöntemlerinin performansları literature oranla yüksek başarı sağlamaktadır.

Yeni bir veri kümeleme yöntemi geliştirilen bir çalışmada [32], yazarlar güvenli veri kümeleme için enerji verimli ve yüksek başarılı bir yöntem geliştirmişlerdir. Geliştirilen yöntemin ana fikri özel algılayıcı okumalarını göndermeden ve pil limiti olan algılayıcılardaönemli bir yük getirmedenveri kümelemeyi gerçekleştirmektir. Geliştirdikleri EEHA protokolünün performansını ölçmek için simülasyonlar sunmuşlardır. Yazarların analizleri ve simülasyonları EEHA'nın varolan yöntemden daha etkin ve doğru olduğunu göstermiştir.

Dinamilk şifre tabanlı kullanıcı doğrulama yöntemi üzerine yapılan bir çalışmada [33], hiyerarşik algılayıcı ağlar için bir protokol geliştirilmiştir. Yazarların sundukları yöntem, diğer varolan şifre tabanlı yaklaşımlarla karşılaştırıldığında daha iyi güvenliğe ve verime sahiptir. Ayrıca, bu yöntem baz istasyonu veya ağ geçidi düğümünün yardımı olmadan dinamik olarak kullanıcının şifresini değiştirmeyi sağlamaktadır. Dahası, bu yöntem varolan algılayıcı

ağda düğümlerin başlangıç dağılımından sonra dinamik düğüm eklemeyi desteklemektedir.

VI. SONUÇ VE TARTIŞMA (CONCLUSION AND DISCUSSION)

Kablosuz algılayıcı ağların kullanım alanı her geçen gün artmaktadır. Çevre, endüstri, askeri, sağlık, güvenlik ve reklam gibi uygulamalarda çeşitli algılayıcı ağ yapıları kullanılmaktadır. Bu uygulamaların güvenliğini sağlama adına çeşitli yöntemler geliştirilmektedir.

Güvenlik, kablosuz algılayıcı ağ uygulamalarında mutlaka üzerinde durulması gereken bir konudur. Gönderilen veriler kişiye özel ve kritik veriler olduğundan dolayı, bu verilerin güvenliğinin sağlanması hayati bir konudur. Kayıtlara yanlış verilerin geçirilmesi, farklı kaynaklardan yanlış bilgilerin sisteme geçirilmesi gibi saldırıların önüne geçilmesi için algılayıcı algılayıcıların kimlik doğrulamasından geçmesi büyük önem arz etmektedir. Kablosuz iletim teknolojileri girişim saldırılarının birçok çeşidine maruz kalabildiğinden ve hassas ve kritik veriler söz konusu olduğundan dolayı kablosuz algılayıcı ağlarda veri iletiminin güvenilirliğinin de sağlanması gerektiği görülmüştür.

Güvenlik için alınması gereken önlemler şunlardır [34]:

- Algılayıcı cihazlarının güç kaynağı, işlemci ve bellek gibi problemlerinin üzerinde durulması ve çözülmesi,
- Algılayıcı cihazlardan gelen verinin nasıl korunması ve nasıl dağıtılacağı iyi planlanmalı,
- Algılayıcı düğümlerin konumlandırılması, yapılabilecek saldıırıların önüne geçilebilmesi açısından önemli olduğundan, ağda kullanılan düğümlerin saldırıları önleyebilecek tedbirleri alabilecek şekilde planlanmalı,
- Kablosuz algılayıcı ağlarda iletişim saldırılarını, gizliliğe karşı saldırıları, algılayıcı düğüme yapılan saldırıları, güç kaynağına yapılan saldırıları ve anahtar yönetimindeki kriptoloji saldırılarını önleyebilmek için ağın dinlenmesinin önüne geçilmesi gerekmektedir. Ayrıca alışverişi sağlanan verilerin bütünlük ve doğruluğu takip edilmeli,
- İletim, algılayıcı düğümler arasında yapıldığından düğümlerin konumlandırılması, gelebilecek bir saldırının diğer düğümlere mümkün olan en az zararı vermesini sağlayacak şekilde yapılmalıdır.

Literatürde yapılan araştırmalarda, makalelerin çoğunluğunda kablosuz algılayıcı ağların nasıl daha verimli kullanılacağı gibi konular daha fazla bulunmasına rağmen güvenlik konusunda yeterince çalışmanın olmadığı sonucuna varılmıştır. Dolayısıyla bu çalışma ile literatürde var olan teknikler geniş çaplı ele alınarak,kablosuz algılayıcı ağların yapısı, bu ağların ana çalışma konuları, bu ağlarda güvenlik hedefleri, temel ağ saldırıları, güvenlik protokolleri, güvenli yönlendirme ve güvenli servis modelleri çeşitli öneriler ile de desteklenerek sunulmuştur. Güvenliği sağlamak için çeşitli çözümler sunan makaleler incelenerek bu bildiriler ve makalelerde bulunan öneriler toparlanmış, kablosuz algılayıcı ağ güvenliğinin nasıl sağlanması gerektiği üzerinde çalışmalar özetlenmiştir. Gelecek çalışmalarda, risk analizleri aracılığıyla maliyet de hesaba katılarak güvenli yeni bir kablosuz algılayıcı ağ modeli geliştirilmesi gerekmektedir.

VII. KAYNAKLAR (REFERENCES)

1) Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., Culler, D. E. “SPINS: Security Protocols for Sensor Networks”, ACM Journal of Wireless Networks, 8 (5), 521-534 (2002).
2) Xu, J.F., “A Defense System for Wireless Sensor Networks”, The Journal of China Universities of Posts and Telecommunications, 18(2), 119-122 (2011).
3) Padmavathi, G., Shanmugapriya, D., “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks”, International Journal of Computer Science and Information Security, 4 (1), 117-125 (2009).
4) Özdemir, S., Xiao, Y., “Secure Data Aggregation in Wireless Sensor Networks: A Comprehensive Overview”, Computer Networks, 53, 2022–2037 (2009).
5) Sang, Y., Shen, H., Inoguchi, Y., Tan, Y., Xiong, N., “Secure Data Aggregation in Wireless Sensor Networks: A Survey”, IEEE Seventh International Conference on Parallel and Distributed Computing, 315-320 (2006).
6) Rajagopalan, R., Varshney, P.K., “Data Aggregation Techniques in Sensor Networks: A Survey”, IEEE Communications Surveys&Tutorials, 8 (4), 48-63 (2006).
7) Naeem, T., Loo, K., “Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks”, International Journal of Digital Content Technology and Its Applications, 3 (1), 88-9 (2009).
8) Kwon, S., Ko, J., Kim, J., Kim, C., “Dynamic Timeout for Data Aggregation in Wireless Sensor Networks”, ACM The International Journal of Computer and Telecommunications Networking, 55 (3), 650-664 (2011).
9) Zhou, Y., Fang, Y., “Securing Wireless Sensor Networks: A Survey”, IEEE Communications Surveys &Tutorials, 10(3), 6-28 (2008).
10) Zubiete, E.D., Luque, L.F., Fernandez, L., Rodriguez, A.V.M., Gonzalez, I.G., “Review of Wireless Sensors Networks in Health Applications”, IEEE Engineering Medicine Biology Sociecty, 1789-1793 (2011).
11) Rahman, M.A., Alhamid, M.F., Gueaieb, W., El Saddik, A., “An Ambient Intelligent Body Sensor Network for E-Health Applications”,IEEE Medical Measurements and Applications, 22-25 (2009).

12) Singh, S., Verma, H.K., "Security for Wireless Sensor Network", International Journal on Computer Science and Engineering, 3 (6), 2393-2399 (2011).
13) Wang, Y., Attebury, G., Ramamurthy, B., "A Survey of Security Issues in Wireless Sensor Networks", IEEE Communications Surveys &Tutorials, 8 (2), 2-23 (2006).
14) Akyildiz, I.F., Weilian Su, Sankarasubramaniam, Y., Cayirci, E., "Survey on Sensor Networks", IEEE Communications Magazine, 40 (8), 102 - 114 (2002).
15) Meghdadi, M., Özdemir, S., Güler, İ., "Kablosuz Algılayıcı Ağlarında Güvenlik: Sorunlar Ve Çözümler", Bilişim Teknolojileri, 1 (1), (2008).
16) Nanda, R., Krishna, P.V., "Mitigating Denial Of Service Attacks in Hierarchical Wireless Sensor Networks", Network Security, 10, 14-18 (2011).
17) Ssu, K., Wang, W., Chang, W., "Detecting Sybil Attacks in Wireless Sensor Networks Using Neighboring Information", ACM Computer Networks, 52 (18), 3042-3056 (2009).
18) Tripathy, S., Nandi, S., "Defense Against Outside Attacks in Wireless Sensor Networks", IEEE Computer Communications, 31 (4), 818-826 (2008).
19) Bhatti, S., Xu, J., Memon, M., "Clustering and Fault Tolerance for Target Tracking Using Wireless Sensor Networks", 1 (2), 66-73 (2011).
20) [Stajano, F., Anderson, R., "The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks", 7th International Security Protocols Workshop,1796, 172-194 (1999).
21) Zhu, S., Setia, S., Jajodia, S., "LEAP: Efficient Security Mechanisms for Largescale Distributed Sensor Networks", ACM Conference on Computer and Communications Security, 62-72 (2003).
22) Chan, H., Perrig, A., Song, D., "Random Key Predistribution Schemes for Sensor Networks", IEEE Security and PrivacySymposium, 197-213 (2003).
23) Karlof, C., Wagner, D., "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures" Ad Hoc Networks, 1, 293-315 (2003).
24) Sharif, L., Ahmed, M., "The Wormhole Routing Attack in Wireless Sensor Networks (WSN)", First IEEE International Workshop on Sensor Network Protocols and Applications, 6 (2), 177-184 (2010).
25) Sun, K., Ning, P., Wang, C., "Tinysersync: Secure and Resilient Time Synchronization in Wireless Sensor Networks", Proceedings of the 13th ACM Conference on Computer and Communications Security, 264-277 (2006).
26) Fessant, F., Papadimitriou, A., Viana, A.C., Sengul, C., Palomar, E., "A sinkhole resilient protocol for wireless sensor networks: Performance and security analysis", Computer Communications, 35:2, 234-248 (2012).
27) Fanian, A., Berenjkoub, M., Saidi, H., Gulliver, T.A., "A high performance and intrinsically secure key establishment protocol for wireless sensor networks", Computer Networks, 55:8, 1849-1863 (2011).
28) Lee, J., Kapitanova, K., Son, S.H., "The price of security in wireless sensor networks", Computer Networks, 54:17, 2967-2978 (2010).
29) Delgado-Mohatar, O., Fúster-Sabater, A., Sierra, J.M., "A light-weight authentication scheme for wireless sensor networks", Ad Hoc Networks, 9:5, 727-735 (2011).
30) Misra, S., Thomasinous, P.D., "A simple, least-time, and energy-efficient routing protocol with one-level data aggregation for wireless sensor networks", Journal of Systems and Software, 83:5, 852-860 (2010).
31) Szalachowski, P., Ksiezopolski, B., Kotulski, Z., "CMAC, CCM and GCM/GMAC: Advanced modes of operation of symmetric block ciphers in wireless sensor networks", Information Processing Letters, 110:7, 247-251 (2010).
32) Li, H., Lin, K., Li, K., "Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks", Computer Communications, 34:4, 591-597 (2011).
33) Das, A.K., Sharma, P., Chatterjee, S., Sing, J.K., "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks", Journal of Network and Computer Applications, 35:5, 1646-1656 (2012).
34) Harjito, B., Han, S., "Wireless Multimedia Sensor Networks Applications and Security Challenges", IEEE Computer Society, 842-846, (2010)