Kablosuz Algılayıcı Ağlarda Güvenli Yönlendirme Protokolleri Üzerine Bir İnceleme

F. Yıldırım Okay, S. Özdemir, Ş. Sağıroğlu

***Özet*—Kablosuz algılayıcı ağlarda (KAA) yönlendirme ağın enerji verimliliğini doğrudan etkilediği için oldukça önemli bir konudur. Çok geniş bir kullanım alanı olan KAA'ların genelde askeri, medikal, kimyasal, çevresel, endüstriyel gibi açık ortam uygulamaları olduğu için bu ağlar fiziksel saldırılara karşı savunmasızdırlar. Ayrıca, KAA'ların tüm uygulama alanlarına uygun tek bir yönlendirme protokolü geliştirilmesi uygulamaların gereksinimlerinden dolayı mümkün değildir. Kötücül kişiler, sınırlı güç tüketimi olan algılayıcıların oluşturduğu KAA'ların güvenliğini, yönlendirme protokollerindeki açıklardan faydalanarak tehdit etmektedir. Özellikle, farklı saldırı yöntemleriyle saldırganlar ağın yaşam süresini kısaltmakta ya da ağ topolojisinde ciddi bozulmalar meydana getirebilmektedir. Bu makalede KAA'lardaki çeşitli yönlendirme saldırıları ve bu saldırılara karşı önerilen güvenli yönlendirme protokolleri incelenmiş, detaylı bir analiz yapılmıştır.**

***Anahtar Kelimeler*— KAA; yönlendirme; güvenlik; enerji etkinliği**

***Abstract*— Routing in wireless sensor networks (WSNs) is a very important issue due to its direct effects on the energy efficiency of network. WSNs, which has a wide spectrum of application fields such as military, medical, chemistry, environmental and industry, are so vulnerable to physical attacks. Also, it is not possible to develop a proper protocol for all application fields because of the distinct requirements of the applications. Malicious people may threat WSN security by taking advantage on routing protocol's vulnerability. In particular, attackers with different methods may reduce the lifetime of sensor networks or heavily corrupt network topology. In this article, various routing attacks and the proposed secure routing protocols against these attacks has been researched and analyzed in detail.**

***Key Words*— WSN; routing; security; energy efficiency**

I. GİRİŞ

KABLOSUZ algılayıcı ağlar (KAA) bir ortama yoğun bir şekilde dağıtılmış çok sayıda düğümden oluşmaktadır. Bu düğümlerin her biri düşük enerjili, düşük maliyetli, kısıtlı işleme ve hesaplama yeteneği olan çok fonksiyonlu küçük boyutlu cihazlardır. Düğümler algılama, hesaplama, haberleşme yeteneklerine sahiptir. Bu düğümler bir ortamdaki veriyi algılayıp, yerel bir karar sürecine bağlı olarak diğer düğümlere ya da baz istasyonuna yönlendirebilirler [1-2].

Geleneksel ağlardan farklı olarak KAA'ların tasarım ve kaynak kısıtlamaları bulunmaktadır. Limitli enerji kaynakları, kısa iletişim aralığı, düşük bant genişliği, kısıtlı işleme ve depolama KAA'ların kaynak kısıtları arasındadır. KAA'ların tasarım kısıtı ise uygulamaya bağımlı olmasıdır. Yapılacak olan uygulama ya da gözlemlenecek ortama göre KAA'larda ağın boyutu, dağıtım şeması ve ağ topolojisi değişkenlik göstermektedir [2].

KAA'lar çok farklı alanlarda uygulanabilmektedir. Bunlardan bazıları, çevresel görüntüleme, ortam görüntüleme, askeri operasyonlar, bilimsel araştırmalar, oluşabilecek felaketleri tahmin etme, tıbbi görüntüleme vb. uygulamalardır. Ancak KAA'ların açık ortamlarda uygulanması düğümlerin fiziksel saldırılara açık hale gelmesine sebep olmaktadır [3]. Bununla birlikte, KAA'larda yönlendirmenin de güvenlik gereksinimlerini basit düzeyde sağlaması beklenmektedir. Yönlendirme üzerine yapılan çalışmalarda ilk olarak Karlof ve Wagner [4] güvenlik konusunu gündeme getirmiştir. Sonrasında ise çeşitli çalışmalarda güvenli yönlendirme protokolleri incelenmiştir. Geleneksel ağlarda yönlendirme protokolleri mesaj erişilebilirliği kriterini garantilemeyi amaçlamaktadır. Mesaj bütünlüğü, kimlik doğrulama ve gizlilik kriterleri daha yüksek seviyelerde SSH, SSL gibi uçtan uca güvenlik mekanizmaları ile sağlanmaktadır. Ancak KAA'larda orta düğümlerin mesaj içeriğine doğrudan erişim gereksinimlerinden dolayı uçtan uca güvenlik mekanizmalarının kullanımını zor hale getirmektedir [4].

Literatürdeki çalışmalar incelendiğinde yapılmış olan çalışmaların daha çok KAA'lardaki yönlendirme protokollerinin güvenlik analizi üzerine olduğu görülmektedir [4,17-20]. Bu çalışmada KAA'lardaki yönlendirme üzerine yapılan saldırılar ve bu saldırılara karşı alınan önlemler üzerinde durulmaktadır. Literatürdeki KAA'lar için geliştirilmiş olan önemli yönlendirme protokolleri araştırılmış ve özetlenmiştir. İncelenen yönlendirme protokolleri özellikle güvenlik açısından ele alınmıştır. Öncelikle KAA'ların güvenliği üzerine yapılan araştırmalar incelenmiş, sonrasında yönlendirme protokolleri ile KAA'ların güvenliğinin nasıl sağlanabileceği konusundaki çalışmalar özetlenerek bir karşılaştırma verilmiştir. Ayrıca, ele alınan bu yönlendirme protokollerinin etkin oldukları saldırı türleri ve özellikleri belirtilmiştir.

Makalenin geri kalan kısmı şu şekilde düzenlenmiştir: II. Bölümde KAA'larda güvenlik konusu ele alınmıştır. III. Bölümde temel güvenlik gereksinimleri hakkında bilgi

F. Y.-O. Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümünde çalışmaktadır (feyzaokay@gazi.edu.tr).
S. Özdemir Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümünde çalışmaktadır (suatozdemir@gazi.edu.tr).
Ş. S Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümünde çalışmaktadır (ss@gazi.edu.tr).

verilmiştir. IV. Bölümde çeşitli yönlendirme saldırıları incelenmiş ve bu saldırılara karşı geliştirilen güvenlik mekanizmaları incelenmiştir. V. Bölümde literatürdeki güvenli ve enerji etkin yönlendirme protokolleri özetlenmiştir. Son olarak VI. Bölümde ise incelenen yönlendirme protokolleri üzerinden sonuç ve çıkarımlar yapılıp, geleceğe yönelik araştırılabilir konular üzerinde durulmuştur.

II. KAA'LARDA GÜVENLİK

KAA düşman hatlarının ya da sınır bölgelerin gözetlenmesi gibi görev kritik uygulamalarda tasarım yapılırken güvenlik gereksinimi göz önünde bulundurulmalıdır. Ayrıca hassas kişisel bilgilerin olduğu çalışma uygulamalarında, sağlık uygulamalarında ya da bazı ticari uygulamalarda da güvenlik önem arz etmektedir [5]. KAA'ların düşman ortamlarında dağıtımlarının yapılması, çoğu algılayıcı ağın çevresindekileri gözlemlemesi ve bu bilginin kolayca açığa çıkarılması, istenmeyen bilgi sızmalarının ortamdaki kişilerin gizliliğini ihlal etmesi ve iletişimin düşmanlar tarafından kulak misafiri olma ya da paket enjeksiyonuna sebep olmasından dolayı KAA'larda güvenlik oldukça önemlidir. Ayrıca, KAA'lar kısıtlı hesaplama, enerji ve hafızaya sahip olmaları, asimetrik yaklaşımların çok pahalı olması, kulak misafiri olmanın kolay olmasından kaynaklı kötücül mesajların ağ içerisine kolayca enjekte edilebilmesi, büyük ölçekli dağıtımlarda ölçeklenememesi ve fiziksel saldırılara karşı duyarlı olmasından dolayı KAA'larda güvenlik gereksinimlerinin sağlanması oldukça zor ve karmaşık hale gelmektedir [6]. Önceki çalışmaların çoğunda algılayıcı ağların birbirleri arasında işbirliği ve güven ilişkisi sağladıkları varsayılmaktadır. Ancak gerçek uygulamalarda bu güven ilişkisinin sağlanabilmesi için güvenliğin sağlanması gerekmektedir [7].

Açık anahtar kriptografisinin çok pahalı olması ve KAA yapısının limitli hesaplama gücüne sahip olmasından dolayı tercih edilmemektedir. Simetrik kriptografi ise hızlı ve düşük enerji tüketiminden dolayı tercih edilmektedir. Ancak simetrik şifrelemedeki temel problemlerden bazıları ise KAA'larda gizli anahtarın düğümler arasında nasıl paylaşılacağı ve gizliliğinin nasıl sağlanacağıdır. İletilen mesajın önemli olduğu askeri ve benzeri uygulamalarda bilginin düşman tarafından ele geçirilmesi, değiştirilmesi ya da taklit edilmesi ciddi güvenlik hasarlarına sebebiyet verebilmektedir. Bu nedenle anahtar yönetimi ve anahtar dağıtımı KAA'lardaki güvenliğin korunmasındaki temel gereksinimlerdendir [8,9].

III. KAA'LARDA GÜVENLİK GEREKSİNİMLERİ

Güvenlik gereksinimleri KAA'larda güvenlik üzerinde durulması gereken konulardan biridir. Bunun için çeşitli güvenlik gereksinimleri tanımlanmıştır. Gereksinimler bazı çalışmalarda birincil ve ikincil güvenlik hedefleri şeklinde ikiye ayrılmaktadır. Buna göre birincil gereksinimler gizlilik, bütünlük, kimlik doğrulama ve kullanılabilirlik gibi güvenliğin ana unsurlarıdır. İkincil gereksinimler ise, veri güncelliği, kendi-kendini örgütleme, zaman senkronizasyonu ve güvenli konumlandırma gibi etkenlerdir [7,11,12]. Bu gereksinimlerin dışında inkar edememe, güncellik gibi etkenler de bazı çalışmalarda incelenmektedir. Ayrıca ağdan ayrılan düğümlerin gelecek mesajları okunmasını ve ağa yeni katılan düğümlerin önceden gönderilmiş olan mesajları okumasını engelleyen ileri ve geri yönlü gizliliğin de olması önerilmektedir [15]. Gereksinimlerin çoğu geleneksel kablolu ve kablosuz ağlar için ortak olmasına karşın bu bölümde KAA'lardaki bazı gereksinimler üzerinde durulmaktadır [10].

A. Veri Gizliliği

KAA'larda veri gizliliği özellikle görev kritik uygulamalarda algılanan verinin yetkisiz kişilerce erişimlerinin engellenmesini garanti altına almaktır. Veri gizliliği ağ güvenliğindeki en önemli konudur. Çoğu uygulamada düğümler oldukça hassas bilgiler taşımaktadırlar. Bu bilginin güvenliğinin sağlanması için bilginin taşındığı kanalın güvenliğinin sağlanması gerekmektedir. Veri gizliliğindeki genel yaklaşımlar hassas bilginin gizli bir anahtar ile sadece alıcılar tarafından alınabilecek şekilde şifrelenmesidir, böylece güvenlik sağlanmaktadır. Dahası yönlendirme bilgisinin gizliliğinin sağlanması gerekmektedir. Çünkü kötücül kişiler tarafından yönlendirme bilgisi ile ağın performansı azaltılabilmektedir [13,14].

B. Bütünlük

Veri gizliliği verinin sadece alıcı tarafından alınmasını garanti ederken, iletilen bilginin değiştirilmesinden koruyamaz. Veri bütünlüğü ise verinin hiçbir şekilde değiştirilmemesini garanti eder [14]. Veri üzerinde kötücül düğümlerin yanlış veri enjektesi ya da kablosuz kanaldaki dengesiz durumlardan dolayı verideki bozulmalar ya da hata meydana gelmesi veri bütünlüğünü bozan etmenlerdir [11]. Bu nedenle mesaj kimlik kanıtlama doğrulama kodları (message authentication codes) ya da dairesel kodları (cyclic codes) veri bütünlüğü korunabilmektedir [14].

C. Veri Kimlik Doğrulama

Veri kimlik doğrulama alıcıya kaynağın doğru bir şekilde göndericiden gönderildiğini doğrulamaktadır. KAA'lar ortak kablosuz ortamı kullandıklarından saldırganlar kolaylıkla mesaj enjekte edebilir. Bu nedenle alıcının verinin doğru kaynaktan geldiğini doğrulaması gerekmektedir. Bu doğrulama işlemi kimlik doğrulama mekanizmaları ile yapılmaktadır. Kimlik doğrulama olmadan kötücül düğüm başka düğümleri taklit edebilir ve ağa zarar verebilir. Eğer iki düğüm iletişim halindeyse simetrik anahtarlama ile kimlik doğrulama sağlanabilmektedir. Ancak yayımlama türü iletişimde daha güçlü güven varsayımlarına ihtiyaç vardır. Bu nedenle doğrulamalı yayılım için asimetrik mekanizmaların kullanımına ihtiyaç duyulmaktadır [13].

D. Kullanılabilirlik

Kullanılabilirlik ağ hizmetlerinin hizmet engelleme saldırıları (DoS) karşısında hayatta kalmasını garantilemektedir. DoS saldırıları KAA'ların herhangi bir katmanında meydana gelebilir ve herhangi bir düğümü kalıcı

bir şekilde etkisizleştirebilir. Ayrıca aşırı iletişim ve hesaplama yükü KAA'lardaki düğümlerin bataryalarının tükenmesine sebep olabilmektedir. Askeri bir uygulama için düşünüldüğünde düğümlerden bazılarının kullanılabilirlikleri düzgün bir şekilde sağlanmazsa, düşman bu kısım üzerinden ağa sızabilir ve istenmeyen sonuçlara sebep olabilmektedir [14].

E. Veri Güncelliği

Veri güncelliği verinin yeni olduğunu ve eski bir mesajın yeniden gönderilmediğini garanti altına almaktadır. Gizlilik ve bütünlüğün sağlanmasının yanı sıra her bir mesaj için veri güncelliğinin de sağlanması gerekmektedir [11]. İki tip veri güncelliği sağlanmaktadır. Bunlardan ilki zayıf güncelliktir. Zayıf güncelleme ile kısmi mesaj sıralaması sağlanır ancak herhangi bir gecikme bilgisi bulundurmaz. Bazı algılayıcı ölçümleri için gereklidir. Güçlü güncellemede ise istek-cevap çifti ile tam bir sıralama ve gecikme tahmini sağlar. Ağ içerisindeki zaman senkronizasyonu için kullanışlıdır [13].

IV. SALDIRI MODELLERİ

KAA'lar kullandıkları iletim ortamının yapısından (yayılım türü iletişim/broadcast) dolayı güvenlik saldırılarına karşı oldukça kırılgandırlar. Ayrıca riski yüksek ortamlarda düğümlerin dağıtımlarının yapılmasından dolayı fiziksel olarak korunma sağlanamamakta ve bu durum KAA'ların kırılganlığını artırmaktadır. Geniş ölçekli algılayıcı ağlarında her bir düğümü gözetlemek ve korumak mümkün olmadığından fiziksel ya da mantıksal saldırılara açık haldedir. Saldırganlar farklı güvenlik saldırılarıyla KAA'ların yapısını bozabilmektedir. KAA'lardaki saldırılar genel olarak iki bakış açısıyla değerlendirilmektedirler. Bunlardan ilki güvenlik mekanizmalarına karşı yapılan saldırılar diğeri ise ana mekanizmalara (örneğin yönlendirme mekanizmaları) karşı yapılan saldırılardır [16]. Ağ katmanı üzerinde yer alan saldırılara yönlendirme saldırıları denmektedir [11]. Bu kısımda ağ katmanı üzerinde yer alan çeşitli yönlendirme saldırıları üzerinde durulmaktadır.

A. Yönlendirme Saldırıları

1) Aldatılmış, değiştirilmiş veya tekrar edilmiş yönlendirme bilgisi

Yönlendirme protokollerine karşı yapılabilecek en doğrudan saldırı şekli yönlendirme bilgisini hedef alan saldırılardır. Saldırgan ağ trafiğini bozmak için yönlendirme bilgisini aldatabilir, değiştirebilir ya da tekrar edebilir. Ayrıca yönlendirme döngüleri, ağ trafiğinin kendine çekilmesi ya da püskürtülmesi, kaynak yönlendiricilerinin genişletilmesi ya da kısaltılması, hata oluşturulması, ağın bölümlendirilmesi veya uçtan uca gecikmelerin artırılması gibi durumlar da bozulmalara sebep olabilmektedir [17].

2) Seçici İletme

Çok sekmeli ağlardaki önemli varsayımlardan biri ağdaki tüm düğümlerin gelen mesajı doğru bir şekilde diğer düğümlere iletmesi şeklindedir. Seçici iletme saldırısında, kötücül bir düğüm ağı ele geçirebilir ve bazı mesajları seçerek iletirken diğerlerini bırakabilmektedir [17].

3) Sinkhole

Sinkhole saldırısında düşman ele geçirdiği düğümlerle tüm ağın dikkatini çekerek ve yönlendirme bilgisi sahtekarlığı yaparak merkezde bir 'Sinkhole' oluşturur. Böylece komşu düğümler verilerini iletecekleri bir sonraki düğüm olarak ele geçirilmiş düğümü seçmektedirler. Bu saldırı türü kısaca komşu düğümlerin seçici iletmeyi kolay hale getirerek veri akışının ele geçirilmiş düğümler üzerinden olmasını sağlar [17]. Kablosuz ağlar özelleşmiş iletişim örüntüleri sayesinde sinkhole saldırılarına karşı duyarlıdırlar. Tüm paketler aynı varış noktasını paylaştıkları için ele geçirilmiş düğümün yalnızca baz istasyonuna tek bir yüksek kaliteli yönlendirme sağlaması yeterlidir. Böylece bu yönlendirme üzerinden veri iletimi sağlayan tüm düğümler etkilenecektir [18].

4) Sybil Saldırıları

Sybil saldırıları bir düğümün ağ içerisinde birden fazla kimlik sunması durumudur. Bu düğümler 'Sybil' düğüm olarak adlandırılmaktadır [19]. Bu saldırı ile dağıtık depolama, dispersite, çoklu yol, yönlendirme ve topoloji sürdürülebilirliği gibi hata toleransı şemalarının etkinliğini büyük ölçüde düşmektedir [17]. Sybil saldırıları ile ayrık gibi gözüken yollar aslında kötücül bir düğümün çoklu kimlik sunmasıyla oluşmaktadır. Sybil saldırıları kullanılarak kötücül düğüm aynı anda birden fazla yerde olabilmektedir. Böylece coğrafi yönlendirmeler için ciddi bir tehdit oluşturmaktadır. Ayrıca blok saldırıları gibi yönlendirme saldırılarının tespitinde Sybil saldırı ile yanlış davranış tespit mekanizmalarından kaçınılabilir [19].

5) Solucan Deliği

Solucan deliği ağdaki iki kısım arasında düşük gecikmeli bağlantı sağlamaktadır ve ağ mesajlarını tekrarlamaktadır [17]. Buna göre saldırgan ağdaki bir noktadan paketleri alır ve ağdaki diğer bir noktaya tünel açar. Bu noktadan mesajları tekrarlar. Birbirleri ile anlaşan iki saldırgan arasındaki tünel solucan deliği olarak adlandırılmaktadır. Solucan deliği ile tünelden geçirilen paketler diğer iletimi yapılan paketlerden daha çabuk iletilmektedir [20]. Bu saldırılar genelde seçici iletme ve kulak misafirliği ile birlikte kullanılmaktadır. Sybil saldırılar da bu birleşime eklendiğinde tespit edilmesi güç hale gelmektedir [17].

6) HELLO Taşkını

HELLO paketlerini kullanan çoğu protokol basit bir varsayımla paketlerin radyo iletim aralığı içerisinden gönderildiklerini yani gönderildikleri yerlerin komşu düğümler olduğunu kabul etmektedir. Ağ içerisindeki her bir düğüm komşularına HELLO paketleri göndererek varlığı hakkında bilgi vermektedir. HELLO taşkınında, saldırgan yüksek güçlü bir iletici kullanarak çok sayıda düğümü kandırabilir ve onları komşuluk sınırları içerisinde olduğuna inandırabilir. Saldırgan diğer düğümlerin radyo aralığı dışında yer almasına rağmen baz istasyonuna hatalı bir şekilde daha kısa bir yönlendirme yayınlayarak diğer düğümlerin

saldırgana ait HELLO paketi almalarını ve buraya iletim yapmalarını sağlar [17].

7) Onay mesajını aldatma

KAA'lardaki bazı yönlendirme algoritmaları onay paketlerinin iletimini gerektirmektedir. Saldırgan düğüm komşu düğümlerden paket iletimine kulak misafiri olabilir ve düğümü yanlış bilgi ile aldatabilir. Böylece saldırgan düğüm hakkında yanlış bilginin yayılmasına sebep olabilmektedir. Bu yanlış bilgilendirme zayıf bir düğümün güçlü gibi gösterilmesi ya da ölü bir düğümün canlı olarak gösterilmesi şeklindedir [17].

B. Saldırılara Karşı Geliştirilen Savunma Mekanizmaları

Aldatılmış, değiştirilmiş veya tekrar edilmiş saldırı türüne geliştirilmiş savunma mekanizması mesaj doğrulama kodlarının (MAC) kullanımıdır. Bu doğrulama kodları ile bir mesajın aldatılmış ya da değiştirilmiş olup olmadığı anlaşılabilmektedir. Ayrıca tekrar etme saldırılarına karşı önlem olarak sayaçlar ya da zaman damgaları kullanılmaktadır [13]. Seçici iletme ataklarına karşı geliştirilen savunma mekanizması veriyi göndermek için çoklu yol kullanımıdır. Ayrıca kötücül düğümün tespiti ya da mesaj iletiminin başarısız olduğu kabul edilip alternatif yollardan gönderilmesi sağlanabilir [17]. Sybil saldırılarına karşı geliştirilmiş savunma mekanizmalarından biri doğrulamadır. İki tip doğrulama bulunmaktadır. Bunlardan ilki doğrudan doğrulama olup, her bir düğüm diğer düğümlerin kimliklerinin geçerli olduğunu doğrulamaktadır. Diğeri ise dolaylı doğrulamadır. Buna göre düğümlerin kimlik birlikleri önceden doğrulanmıştır. Buna göre düğümler diğer düğümlerin doğruluğunu garanti eder ya da reddeder [19]. Paket bağlama ile solucan deliği saldırılarına karşı tespit ve savunma yapılmaktadır. Coğrafi ve geçici bağlamalar olmak üzere iki tip paket bağlama sunulmaktadır [20]. HELLO taşkını saldırısında bağlantı üzerinden alınan mesajla herhangi bir işlem yapılmadan önce bağlantının çift yönlülüğünün kontrolünü yapan mekanizmalar önerilmektedir [21]. Sinkhole saldırıları savunulması zor saldırılardandır. Bu nedenle yönlendirme protokollerinin bu saldırılara karşı tasarlanmış olması gerekmektedir. Bu saldırılara dayanıklı protokollerden biri coğrafi yönlendirme protokolüdür. Coğrafi yönlendirmeler baz istasyonundan başlatılmaksızın yerelleşmiş ilişkileri ve bilgileri kullanan bir yapı oluşturur.

Trafik baz istasyonunun fiziksel konumu üzerinden kendiliğinden yönlendirildiği için sinkhole saldırıları ile başka bir yere yönlendirmek oldukça zordur [17]. Ayrıca onay mesajını aldatma saldırılarına karşı kimlik doğrulama kullanılmaktadır ve güvenlikleri sağlanmaktadır [15]. Tablo1'de yönlendirme üzerine yapılan saldırılar ve bunlara karşı alınan önlemler listelenmektedir.

V. GÜVENLİ YÖNLENDİRME PROTOKOLLERİ

KAA'larda güvenli yönlendirme protokollerinin amacı güvenliğin temel unsurlarını kapsayacak şekilde bir mesajın bütünlüğünü, kimlik doğrulamasını ve kullanılabilirliğini sağlamaktır. Karlof ve Wagner yapmış oldukları çalışmada [17] güvenli yönlendirme protokolleri üzerine dikkatleri çekmesiyle birlikte KAA'larda güvenli yönlendirme protokolleri üzerine bazı yenilikçi çalışmalar yapılmıştır. Bu çalışmalardan bazıları tamamen güvenliği sağlarken, bazıları ise sadece seçili saldırı türlerine karşı güvenliği sağlamaktadır. Ayrıca bazı çalışmalarda güvenliğin yanı sıra enerji etkinliğinin de sağlanması önerilen protokolün temel amaçları arasındadır. Çalışmaların çoğu simetrik anahtarlama mekanizmasına dayanmaktadır. Buna karşın açık anahtarlama şifreleme mekanizmasını kullanan çalışmalarda bulunmaktadır. Bu kısımda KAA'larda güvenli yönlendirme protokolleri üzerine detaylı bir inceleme yapılmaktadır.

A. Güvenli Ortam Erişim Protokolleri

1) SIGF

Güvenli Üstü Kapalı Coğrafi İletim (GÜCİ/SIGF) [22] ayarlanabilir bir yönlendirme protokolü olup "yeterince iyi" bir güvenlik ve yüksek bir performans sağlamaktadır. Bu protokol Üstü Kapalı Coğrafi İletim (ÜCİ/IGF)'nin [23] güvenlik mekanizması eklenmiş halidir. Üç güvenlik seviyesini temsil eden üç farklı protokol içermektedir. Bunlar SIGF-0 (hiç durum olmaması), SIGF-1(yerel bir şekilde oluşturulmuş durum) ve SIGF-2 (komşuluk içerisinde ikili paylaşımlı durum) protokolleridir. SIGF-0 hiçbir yönlendirme bilgisinin devam ettirilmediği durum olmayan bir protokol olup IGF protokolünün basit düzeyde genişletilmiş halidir. IGF'deki bazı parametrelerin ayarlanabilir özellikte olmasını sağlar. Komşular hakkında iletim bilgisi ve geçmişi tutmadan non-deterministik ve dinamik bir şekilde bir sonraki sekme aktarımını seçmektedir. İletim alanının genişletilmesi ile daha fazla komşu düğümü dahil etmektedir. Bu durum komşuluklar içerisinde saldırganın seçilme ihtimalini azaltmaktadır.

TABLO I. YÖNLENDİRME SALDIRILARI VE SAVUNMA MEKANİZMALARI

SALDIRI TÜRLERİ	SAVUNMA MEKANİZMALARI
Aldatılmış, Değiştirilmiş veya Tekrar Edilmiş Yönlendirme Bilgisi	Çıkış filtreleme, kimlik doğrulama, gözetleme, mesaj doğrulama kodları
Seçici İletme	Artıklık kontrolü, çoklu yol kullanımı
Sinkhole	Kimlik doğrulama, gözetleme, artıklık, güvenlik protokolleri
Sybil Saldırıları	Kimlik doğrulama, deneme (probing)
Solucan Deliği	Kimlik doğrulama, coğrafi ve geçici bilgiler kullanılarak paketi bağlama
HELLO Taşkını	Kimlik doğrulama, çift yönlü bağlantıları doğrulama
Onay mesajını aldatma	Kimlik doğrulama

SIGF-0 IGF'ye göre acele ettirme saldırılarında karşı daha dayanıklıdır. Az miktarda verimsizlik olmasına rağmen, güvenliği önemli ölçüde artırmaktadır. SIGF-1 protokolü, SIGF-0 protokolündeki özelliklere ek olarak bir düğümün içeriden durumunu belirlemektedir. SIGF-1, SIGF-0 gibi çalışır ancak bir sonraki sekmenin seçimi her bir komşu düğüme atanan itibar değerine göredir. Bu değer düğüm tarafından depolanan ve sürdürülen durum bilgisinden türetilmektedir. SIGF-1 protokolü özellikle sybil saldırılarına karşı etkin bir koruma sağlamaktadır. SIGF-2 protokolü ise önceki protokollere ek olarak hizmet engelleme (DoS) saldırılarına karşı kriptografi kullanımını sağlamaktadır. Ayrıca komşu düğümler arasında gizlilik, kimlik doğrulama, bütünlük ve veri güncelliği kriterlerini sağlamaktadır. Yararlı yük şifreleme ile kulak misafiri olmayı engeller. Ağ planlayıcısı dağıtımdaki güvenlik ihtiyaçlarına göre gerekli SIGF protokolünü seçebilir ve ayarlayabilir. Sonuç olarak SIGF protokolü güvenlik, etkinlik ve performans arasında ayarlanabilir bir algoritma seçimi imkanı sağlar.

2) SDD

Doğrudan Difüzyon [25] protokolü KAA'lar için önemli bir veri merkezli yönlendirme protokolüdür. Güvenli Doğrudan Difüzyon (GDD/SDD) [24] protokolü ise Doğrudan Difüzyon algoritmasına bazı güvenlik parametreleri eklenmiş halidir. Doğrudan Difüzyon protokolü kimlik doğrulama ve bütünlük gereksinimlerinin eksikliği nedeniyle çeşitli saldırılara karşı oldukça kırılgan bir yapı göstermektedir. Saldırgan pozitif ya da negatif aldatmalarla veri akışının sırasının zorla değiştirilmesine sebep olabilir. Bu durum ise seçici iletme, kurcalama, DoS ya da kulak misafiri olma saldırıları gibi saldırılarla sonuçlanabilir. Ayrıca lap-top sınıfı saldırganlar solucan deliği saldırılarını sahte donatılar kullanarak sinkhole saldırıları yapabilir. SDD protokolü kimlik doğrulamalı yayın yapan immediate TESLA [26] kullanımına dayanmaktadır. Bu sayede yönlendirme ve veri mesajlarının kimlik doğrulaması ve bütünlüğü sağlanmaktadır. Ayrıca gizlilik ve saldırıların başarılarını engellemek için dayanıklılık ve hayatta kalma gereksinimleri de sağlanmaktadır. Sadece simetrik kriptografi kullanılır. Asimetri tek yönlü özet zincirleri ile sağlanmaktadır. Önerilen protokol değiştirilmiş LEAP'ın Doğrudan Difüzyon ile işbirliği ile ağın dışarısından gelen hemen hemen bilinen tüm saldırılara karşı koruma sağlamaktadır. Sadece düşük oranda veri yayılımı fazında problem oluşmaktadır. Saldırgan kulak misafiri olarak iletişimi dinleyebilir ve rastgele seçilen yol üzerinde bulunabilir.

3) SeRINS

Algılayıcı Ağlarda Güvenli Alternatif Yol Yönlendirme (AAGAYY/SeRINS) [27] protokolü çeşitli güvenlik mekanizmaları ve komşu raporlama sistemi ile güvenli yönlendirme sağlamaktadır. SeRINS protokolünün amacı ağı seçici iletme ya da sahte yönlendirme bilgisi tanıtımı saldırıları gibi içerden saldırılara karşı korumaktır. Bu çalışmada yazarlar saldırganların sadece az sayıda düğümü ele geçirdiğini kabul etmektedir. Ayrıca her bir düğüm baz istasyonuyla tek bir gizli anahtar paylaşıp bu anahtar üzerinden komşu düğümlerle iletişim kurduğunu kabul etmektedir. Son olarak ise tüm iletişim sekmeden sekmeye şifreleme ile korunduğu için dışarıdan saldırılara karşı ağa katılarak koruma sağladığını kabul etmektedirler. Üç farklı şema yapısı bulunmaktadır. Bunlar yönlendirme topolojisinin kurulduğu alternatif yol şeması, alt sekmelerin kimlik doğrulamasının yapıldığı komşu kimlik doğrulama şeması ve sahte tanıtım saldırıları gibi kötücül düğümleri belirleyen ve ortadan kaldıran komşu raporlama şemasıdır. SeRINS protokolünde her ikili komşu düğüm arasındaki güvenli kanallar sayesinde sybil saldırıları, sinkhole saldırıları, HELLO taşkını ve onay mesajını aldatma saldırıları gibi saldırılara karşı oldukça dayanıklıdır. Solucan deliği saldırılarına karşı ise paket bağlama gibi harici şemalarla savunma yapılmaktadır. Ayrıca seçici iletme saldırıları çoklu yol şeması ile önlenilirken, sahte yönlendirme bilgisi problemi ise komşu raporlama sisteminin tespit ve reaksiyon mekanizmaları ile çözülmektedir.

4) Temiz Bir Sayfa Yaklaşımı

Temiz bir sayfa yaklaşımında [28] güvenliğin ve etkinliğin ana amaç olarak tanımlandığı bir yönlendirme protokolü sunulmaktadır. Aktif saldırganların olduğu ortamda bile herhangi bir özel donanım gerektirmemekte ve mesaj dağıtımını gerçekleştirebilmektedir. Yüksek dereceli güvenlik ve düğümden düğüme yüksek kullanılabilirlik sağlamak amaçlanmaktadır. Asimetrik kriptografi kullanılmaktadır. Bu protokol önleme, tespit/iyileştirme ve dayanıklılığın kombinasyonundan oluşmaktadır. Önleme yaklaşımı saldırılar karşısında kriptografi mekanizmaları ile protokolü daha dayanıklı hale getirmeyi amaçlamaktadır. Önleme yaklaşımı etkin bir yaklaşım olmasına karşın bilinen saldırılara karşı önceden önlem almaktadır. Tespit yaklaşımı protokol katılımcılarının davranışlarını gerçek zamanlı gözetleme işlemi yapmaktadır. Kötücül bir düğüm tespit edildiğinde kötücül katılımcıların yok edilmesi ve ağ sırası ve işlevselliğinin yeniden sağlanması için iyileştirme teknikleri kullanılmaktadır. Tespit yaklaşımı daha çok bilinmeyen saldırılara karşı koruma sağlamaktadır. Dayanıklılık yaklaşımı ise saldırı anında bile kullanılabilirlik oluşturmayı amaçlamaktadır. Bu yaklaşım ele geçirilmiş katılımcıların ağ içerisindeki varlıklarını azaltmada iyi bir performans sergilemektedir.

5) INSENS

Kablosuz Algılayıcı Ağlarda Sızma Toleranslı Yönlendirme Protokolü (STYP/INSENS) [29] KAA'larda güvenliği sağlayan yönlendirme tabanlı bir yaklaşımdır. INSENS algılayıcı düğümler ve baz istasyonu arasındaki iletişimin kolay olması için her bir düğümde iletim tabloları oluşturur. Bu protokolün amacı KAA'larda tek bir ele geçirilmiş düğümün ağ içerisinde sadece yerel bir bölgede bozulmalara sebep olacağı sızma toleranslı güvenlik sağlamaktır. Başka bir deyişle düğümlerdeki saldırılar tamamen engellenmeye

çalışılmamaktadır. Sadece ağa verecekleri zararlar minimize edilmeye çalışılmaktadır. İki tip saldırı sınıfı için sızma toleransı sağlamak amaçlanmaktadır. Bunlar tüm ağı veri paketleri istilası yapan DoS-tipli saldırılar ve yanlış yönlendirme bilgisini de içeren hatalı kontrol paketleri yayılımına sebep olan yönlendirme saldırılarıdır. DoS saldırılarını önlemek için, bireysel düğümlerin tüm ağa yayın yapması engellenir. Yalnızca baz istasyonu yayın yapabilir. Ayrıca baz istasyonu herhangi bir kötücül düğüm tarafından kendini yetkili biri gibi gösterme saldırılarına karşı tek yönlü özet fonksiyonlarını kullanarak kimlik doğrulama yapar. Yanlış yönlendirme verilerinin sızmasını önlemek için yönlendirmeye ait olan kontrol bilgileri doğrulanır. İçeriden bir saldırgan bir düğümü ele geçirse ve paket iletimini engellese bile, INSENS artık çoklu-yol yönlendirme kullanarak kötücül düğüme uğramadan varış düğümüne iletim sağlayabilmektedir. Ayrıca her bir kaynak kısıtlı algılayıcı düğüm ile baz istasyonu arasında gizlilik ve kimlik doğrulama sağlamak için simetrik anahtar kriptografisini kullanmaktadır.

6) SPINS

SPINS [13] algılayıcı ağlarda güvenli iletişim sağlayan bir protokoldür. SPINS iki temel yapı içermektedir. Bunlar, güvenli ağ şifreleme protokolü SNEP [13] ve µTESLA [13] protokolüdür. SNEP protokolü veri gizliliği, iki kısımlı veri kimlik doğrulama ve eş düzeyde iletişim (düğümden baz istasyonuna) için veri güncelliği sağlamaktadır. SNEP, her bir mesaja sadece 8 baytlık ek yük ile düşük iletişim ek yükü sağlamaktadır. Ayrıca, anlamsal güvenlik ile şifreli mesajın içeriğine kulak misafiri olmayı önlemektedir. Veri kimlik doğrulama (MAC) ile verilerin yollayıcıdan gönderildiği durumlarda alıcı tarafından alındığını garanti eder. MAC'lerde bulunan sayaç değerleri ile tekrarlama mesajları engellenir. Böylece tekrarlama saldırılarına karşı da bir korunma sağlanmış olur. Ayrıca, eğer bir mesaj doğru bir şekilde doğrulanmışsa, kullanıcı bir önceki mesajı aldıktan sonra gönderici tarafından yollandığını bilmektedir. Bu da zayıf da olsa tazelik sağlamaktadır. Diğer bir güvenli yapı bloğu olan µTESLA protokolünde ise, standart TESLA'nın [30] algılayıcı ağlar üzerindeki bazı zorluklarına çözümler üretilmiştir. Son zamanlarda önerilen TESLA kimlik doğrulamalı yayın yapmak için geliştirilen bir protokoldür. µTESLA protokolü ile ilk olarak başlangıç paketindeki sayısal imzalamanın çok maliyetli olmasından dolayı simetrik anahtarlama kullanılmıştır. Her bir paket için bir anahtar bildirmek, alım ve gönderim için çok enerji gerektirdiği için her devirde bir kere anahtar bildirilmiştir. Son olarak ise, tek yönlü anahtar zinciri oluşturmak çok maliyetli olduğundan, µTESLA ile doğrulanan yollayıcı sayısı kısıtlanmıştır.

B. Enerji Etkin Güvenli Yönlendirme Protokolleri

1) KAA'lar için Güvenli ve Enerji Etkin bir Yönlendirme Protokolü

KAA'larda yönlendirmede güvenlik ve etkinlik problemlerinin adreslenmesinde Sen tarafından önerilen bu protokol [31] ile hatalı ya da ele geçirilmiş düğümler güvenilir bir şekilde tanımlanmakta ve yönlendirme yolu kullanılırken bu düğümlerden kaçınılmaktadır. Protokol tek bir yönlendirme yolu kullanmaktadır bu nedenle enerji etkindir. Önerilen protokol Lee tarafından önerilen yönlendirme şemasının [32] değiştirilmiş halidir. Bununla birlikte daha enerji etkindir ve daha az gecikmeye sebep olmaktadır. Protokol dayanıklı komşuluk gözetleme sistemine (NMS) dayanmaktadır. Bu sistem bir düğüm tarafından komşuluğun rastgele gözetlenmesine dayalı çalışır ve komşu liste kontrolü ile işbirliği yapan bir algoritma ile herhangi bir paket düşürme saldırısını tespit eder. Bu şema ile kötücül düğüm yönlendirme yolu içerisinde paket düşürme saldırısında bulunsa bile güvenilir sekmeden sekmeye paket dağıtımı yapılabilmektedir. Paket düşürme saldırısına karşı çoklu-yol yönlendirme ile savunma yapmaktadır. Her bir paket iletim düğümünün küme anahtarı ile şifrelenmektedir. Böylece iletim düğümünün tüm komşuları deşifreleyebilir ve kulak misafiri olabilir. Şifrelemenin küme anahtarı ile sağlanması düğüm ele geçirmelerine karşı dayanıklılık sağlar. Önerilen şema ayrıca yönlendirme bozma saldırılarına karşı da dayanıklıdır.

2) Kablosuz Algılayıcı Ağlar için Enerji Etkinliği ile Güvenli Bir Yönlendirme Protokolü

KAA'larda enerji etkin ve güvenli bir yönlendirme protokolü olan bu protokol [33] iyi bir veri dağıtım oranı, enerji dengelemesi ve yönlendirme etkinliği sağlamaktadır. Buna ek olarak önerdiği güvenlik mekanizmaları ile veri dağıtımında kimlik doğrulama ve gizlilik sağlamaktadır. Bu protokol ile daha iyi bir dağıtım oranı sağlamak için çıkış düğümüne yönelik grid yapısı kullanılmaktadır. İkinci olarak, en uzak ve en yüksek enerji yayılım düğümü araması ile kaynak düğümden çıkış düğümüne etkin bir yol bulunmaya çalışılmıştır. Son olarak ise protokol tasarımında güvenlik gereksinimleri düşünülmüştür. Güvenlik mekanizması olarak tek yönlü özet zincirleri, mesaj doğrulama kodları (MAC), simetrik şifreleme ve çeşitli önceden depolanmış paylaşılmış gizli anahtarlar kullanılmaktadır. Bu protokolde, yanlış bir paket çıkış düğümüne ulaşmaması için yol üzerinde düşürülür. Böylece enerji tüketimi azaltılır. Ayrıca çıkış düğümü tarafından yeni eklenen düğümlerin kimlik doğrulaması yapılır ve komşu düğümlerin komşuluk bilgisi oluşturmaları sağlanır. Herhangi bir düzensizlik bulunduğunda ise yönlendirme bilgisinin yeniden oluşturulması için çıkış düğümü görevlendirilir. Şüpheli düğümler raporlandıktan sonra bu düğümlerin kötücül oldukları ispatlanırsa çıkış düğümünün diğer düğümleri bilgilendirmesi sağlanır. Son olarak seçici iletme düğümleri yönlendirme protokollerine dahil olarak ağdaki düğüm sayısını kısıtlar ve böylece güvenliği sağlar.

TABLO II. GÜVENLİ YÖNLENDİRME PROTOKOLLERİ

YÖNLENDİRME PROTOKOLLERİ	ETKİN OLDUKLARI SALDIRI TÜRÜ	GÜVENLİK GEREKSİNİMİ	ÖZELLİKLERİ
SIGF [22]	Sybil, DoS, Kulak misafiri olma	Gizlilik, Kimlik doğrulama, bütünlük, veri güncelleme	Güvenlik, etkinlik ve performans arasında ayarlanabilir bir algoritma seçimi sağlar.
SDD [24]	Ağın dışarısından gelen tüm saldırılar	Kimlik doğrulama, bütünlük, gizlilik, dayanıklılık, hayatta kalabilme	İmmediate Tesla kullanımına dayanmaktadır. Doğrudan Difüzyon protokolü LEAP ile güvenli hale getirilmiştir.
SeRINS [27]	Seçici iletme, Sahte yönlendirme bilgisi tanıtımı, Sybil, Sinkhole, Hello taşkını, Solucan deliği	Kimlik doğrulama, Paket bağlama, Çoklu yol kullanımı, Komşu raporlama	Yönlendirme topolojisinin kurulduğu alternatif yol şeması, alt sekmelerin kimlik doğrulamasının yapıldığı komşu kimlik doğrulama şeması ve sahte tanıtım saldırıları gibi kötücül düğümleri belirleyen ve ortadan kaldıran komşu raporlama şemasına sahiptir.
Temiz bir Sayfa Yaklaşımı [28]	İçeriden ve dışarıdan gelen tüm saldırılar	Kullanılabilirlik	Aktif saldırganların olduğu durumlarda özel bir donanım gerektirmez ve mesaj dağıtımını yapabilir.
INSENS [29]	DoS-tipli, yönlendirme saldırıları	Kimlik doğrulama, gizlilik	Sızma toleranslı güvenlik ile ele geçirilmiş düğüm ağ içerisinde sadece yerel bir bölgede bozulmalara sebep olabilir.
SPINS [13]	Tekrarlama, kulak misafiri olma	Kimlik doğrulama, gizlilik, veri güncelliği	SNEP ve µTESLA olan iki temel bloktan oluşur.

3) SERP

KAA'larda Güvenli Enerji Etkin Yönlendirme Protokolü (GEEYP/SERP) [34] kaynak düğümden baz istasyonuna limitli enerji tüketimi ile kimlik doğrulamalı ve dayanıklı iletimini sağlamaktadır. SERP'in tasarımında üç ana amaç düşünülmüştür. Bunlar; ağ ömrünü uzatmak ve enerji etkin iletim sağlamak için enerji farkında organizasyon, hatalı rapor enjektesinin tespitini sağlayan güvenli iletim ve düğümlerin başarısız olmasının ağın performansını çok etkilememesi için dayanıklı ve esnek bir iletimdir. Protokol iki aşamada çalışmaktadır. Öncelikle ağın omurgası oluşturulur. Sonrasında ise güvenli veri iletimi sağlanır. Ağaç yapısı enerji tüketimini dengelemek için ağın omurgası olarak oluşturulur. Minimum sayıda iletim düğümü ağ içerisinde seçilir ve ağ omurgası periyodik bir şekilde yeniden oluşturulur.

Güvenli veri iletimini sağlamak için tek yönlü özet zincirleri ve önceden depolanmış paylaşılmış gizli anahtarlar kullanılır. Veri güncelliği için ise uygulamaya bağlı olarak isteğe bağlı anahtar yeniden güncelleme mekanizması kullanılır.

4) EENC

Düğüm Ele Geçirme Drenci ile Enerji Etkin Yönlendirme (DEGDEEY/EENC) [35] protokolü ele geçirilmiş düğümleri yok sayarak enerji tüketimi ile paket doğruluğu arasında dengeleme sağlamaktadır. Yönlendirme tabloları için karınca kolonisi algoritmasına dayalı güçlendirilmiş öğrenme kullanılmaktadır. Öncelikle ağdaki tüm düğümlere güven değeri atanmaktadır. Bu güven değeri paket düşürme oranı, iletim gecikme oranı gibi değişkenlere dayalı olarak hesaplanmaktadır. Bu değerler kullanılarak kötücül düğümlerin tespiti yapılmaktadır. Ağdaki her bir düğüm bir sekme mesafedeki komşularının güven değerlerini hesaplar. EENC protokolündeki amaç minimum enerji tüketimiyle güvenlik sağlamaktır. Bunun içinde komşulara ait güven değerleri depolanır. Protokol iki farklı yönlendirme protokolü ile karşılaştırıldığında enerji etkinliğinde yüksek performans sağlanırken başarılı paket iletiminin yapıldığı görülmektedir.

TABLO III. ENERJİ ETKİN GÜVENLİ YÖNLENDİRME PROTOKOLLERİ

ENERJİ ETKİN GÜVENLİ YÖNLENDİRME PROTOKOLÜ	ETKİLİ OLDUĞU SALDIRI TÜRÜ	ÖZELLİKLER
Güvenli ve Enerji Etkin bir Yönlendirme Protokolü [31]	Paket düşürme ve yönlendirme bozma saldırıları	Hatalı ya da ele geçirilmiş düğümler tanımlanıp, yönlendirmede bu düğümlerden kaçınılmaktadır.
Enerji Etkinliği ile Güvenli bir Yönlendirme [33]	Yanlış paket enjektesi	İyi bir veri dağıtım oranı, enerji dengelemesi ve yönlendirme etkinliği sağlar. Ayrıca veri dağıtımında kimlik doğrulama ve gizlilik sağlar.
SERP [34]	Hatalı rapor enjektesi	Kimlik doğrulama ve gizlilik ile dayanıklı veri iletimi sağlar. Veri güncelliği uygulamaya bağlı olarak sağlanır.
EENC [35]	Ele geçirilmiş düğüm	Enerji tüketimi ile paket doğruluğu arasında dengeleme sağlar. Karınca kolonisi algoritmasına dayalı güçlendirilmiş öğrenme kullanılır. Başarılı paket iletim oranı sağlanır.

VI. SONUÇ

KAA'lar çeşitli tasarım kısıtlarına sahip açık alanlarda uygulanabilir bir yapı göstermektedir. Bu nedenle ağ içerisinden ya da dışarısından çeşitli saldırılara maruz kalabilmektedir. Bu saldırılardan korunmak için güçlü güvenlik tedbirlerinin alınması gerekmektedir. Bu nedenle KAA'larda yönlendirme işlemi için çeşitli güvenlik ihtiyaçları oluşmaktadır. Özellikle yönlendirmeyi hedef alan saldırılar bulunmaktadır. Bu saldırılara karşı çeşitli güvenlik mekanizmaları geliştirilmiştir ve saldırılara karşı korunma sağlanmıştır. Bunun dışında ise bazı güvenli yönlendirme protokolleri ile yönlendirme işlemi güvenli hale getirilmeye çalışılmıştır. Bu makalede çeşitli yönlendirme saldırıları incelenip, bu saldırılara karşı geliştirilen savunma mekanizmaları üzerinde durulmaktadır. Tablo 1'de bu mekanizmalar özetlenmektedir. Ayrıca literatürdeki güvenli ve enerji etkin yönlendirme protokolleri incelenmiş ve özetlenmiştir. Geliştirilen protokollerin ne tür saldırılara karşı güvenlik sağladığı ve hangi güvenlik gereksinimlerini oluşturduğu Tablo 2'de gösterilmektedir. Buna göre bazı protokoller belirli saldırılara karşı güvenlik sağlarken, bazı protokoller ise tüm saldırılara karşı tam bir koruma sağlamaktadır. Ayrıca, gizlilik, bütünlük, kimlik doğrulama, kullanılabilirlik, veri güncelleme, dayanıklılık, hayatta kalma gibi güvenlik gereksinimleri tanımlanmaktadır. Bazı çalışmalarda ise güvenliğin sağlanmasının yanında enerji etkinliğinin de sağlanması ana amaçlar arasında gösterilmiştir. Böylece güvenli yönlendirme protokolleri ile güvenlik sağlanırken, gereksiz enerji tüketimi azaltılarak düğümlerin yaşam süreleri uzatılmıştır. Tablo 3'te ise bu protokoller sunulmaktadır. Enerji etkin güvenli bu protokoller paket düşürme, yönlendirme bozma, yanlış paket enjektesi, hatalı rapor enjektesi gibi saldırılara ve ele geçirilmiş düğümlere karşı etkinlik sağlamaktadır. Ayrıca kimlik doğrulama, gizlilik ve veri güncelliği gibi güvenliğin unsurları sağlanmaktadır. Enerjinin korunumu için 1) tekli-yol yönlendirme mekanizması, 2) yanlış bir düğümün çıkış düğümüne ulaşamaması için yol üzerinde düşürülmesi, 3) ağaç yapısının ağ omurgası olarak oluşturulmasını sağlayan enerji farkında organizasyonlar ve 4) kalan enerjinin bilgi ve yönetimi ile güven değerleri sayesinde etkin bir yönlendirmenin oluşturulması sağlanmaktadır.

Sonuç olarak, üzerinde durulan protokoller incelendiğinde her bir protokolün etkin olduğu saldırı türü, güvenlik gereksinimi ve özellikleri farklıdır. Uygulama alanının gereksinimine göre Tablo 2 ve Tablo 3'te özellikleri verilen protokollerden uygun olanı tercih edilmelidir.

KAYNAKLAR

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, Volume 38, Issue 4, 15 March 2002, pp. 393–422.

[2] J. Yick, B. Mukherjee, D. Ghosal, "Wireless sensor network survey," *Computer Networks,* vol. 52, 2008 pp. 2292–2330.

[3] E. Sabbah, K. D. ,Kang, "Guide to Wireless Sensor Network: Security in Wireless Sensor Network," Chapter 19, pp. 489-490

[4] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks,* vol.1, 2003, pp. 293–315.

[5] J. Kur, "Secure Routing Protocols for Wireless Sensor Networks," Yüksek Lisans Tezi, Masaryk Unıversıty Faculty of Informatics, 2008.

[6] E. Shi, A. Perrig, "Designing Secure Sensor Networks," *IEEE Wireless Communications*, 2004

[7] J. P. Walters, Z. Liang, W. Shi, ve V. Chaudhary, "Wireless Sensor Network Security: A Survey," *Security in Distributed*, Grid, and Pervasive Computing, Chapter 17, 2006 Auerbach Publications, CRC Press.

[8] A. Perrig,, J. Stankovic ve D. Wagner, "Security in Wireless Sensor Networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53-57, 2004.

[9] X. Chen, K. Makki, K. Yen ve N. Pissinou, "Sensor Network Security: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 2, 52-73, 2009.

[10] M. Megdadi, S. Özdemir, İ. Güler, "Kablosuz Algılayıcı Ağlarında Güvenlik: Sorunlar ve Çözümler", *Bilişim Teknolojileri Dergisi,* Cilt: 1, Sayı: 1, Ocak 2008.

[11] G. Padmavathi,, D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," *International Journal of Computer Science and Information Security*, vol. 4, no. 1, pp. 117-125, 2009.

[12] E. B. Ceyhan, Ş. Sağıroğlu, "Kablosuz Algılayıcı Ağlarda Güvenlik Sorunları ve Alınabilecek Önlemler," *Politeknik Dergisi,* vol. 16, no.4, pp. 155-163, 2013.

[13] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, D. E. Culler, "SPINS: Security Protocols for Sensor Networks," *ACM Journal of Wireless Networks*, vol. 8, no.5, 521-534, (2002).

[14] S. Özdemir, Y. Xiao, "Secure Data Aggregation in Wireless Sensor Networks: A Comprehensive Overview", *Computer Networks*, vol. 53, pp. 2022–2037, 2009.

[15] Y. Wang, G. Attebury, B. Ramamurthy, "A Survey of Security Issues In Wireless Sensor Networks," *IEEE Commun. Surveys Tutorials*, vol 8, pp. 2-23, 2006.

[16] A. K. Pathan, H. W. Lee, C. S. Hong, "Security in Wireless Sensor Networks: Issues and Challenges," *ICACT*, pp. 1043-1048, 2006.

[17] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Proc. First IEEE Int'l. Wksp. Sensor Network Protocols and Applications*, May 2003, pp. 113–127.

[18] M. Sadeghi, S. Alam, E. A. Gharb, "Security Analysis of Routing Protocols in Wireless Sensor Networks," *IJCSI International Journal of Computer Science Issues,* vol. 9, Issue 1, no 3, pp. 465-472, January 2012.

[19] J. Newsome, E. Shi, D. Song, A. Perrig, "The Sybil attack in sensor networks : analysis and defenses,". Proceedings of the 3rd International Symposium on Information Processing in *Sensor Networks*, pp. 259-268, ACM Press., 2004.

[20] Y.-C. Hu, A. Perrig, D.B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless Networks", *in: IEEE Infocom*, 2003.

[21] V. C. Giruka, M. Singhal, J. Royalty, S. Varanasi, "Security in wireless sensor networks," *Wiley Inter Science.*, 2006.,

[22] D. Anthony, L. F. Wood, , J. A. Stankovic, T. He, " Sigf: a family of configurable, secure routing protocols for wireless sensor networks," *In SASN '06: Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks*, pp 35–48, New York, NY, USA, 2006. ACM Press.

[23] B. Blum, T. He, S. Son, and J. Stankovic. "Igf: A state-free robust communication protocol for wireless sensor Networks,". In Technical Report, CS-2003-11. Department of Computer Science, University of Virginia, USA, 2003.

[24] X. Wang, L. Yang, ve K. Chen., "Sdd: Secure directed diffusion protocol for sensor Networks,". *In Security in Adhoc and Sensor Networks,* vol. 3313/2005 of Lecture Notes in Computer Science, pages 205–214, First European Workshop, ESAS 2004.

[25] C. Intanagonwiwat, R. Govindan, ve D. Estrin. "Directed diffusion: a scalable and robust communication paradigm for sensor Networks,". *In MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, pp. 56–67, New York, NY, USA, 2000. ACM Press.

[26] A.Perrig, R. Canetti, D. Song, ve D.Tygar. "Efficient and secure source authentication for multicast," *Proceedings of the Internet Society Network and Distributed System Security Symposium*, pp.35-46, 2001.

[27] S.-B. Lee ve Y.-H. Choi., "A secure alternate path routing in sensor Networks,". *Computer Communications*, vol. 30, issue 1, pp 153–165, December 2006.
[28] B. Parno, M. Luk, E. Gaustad, ve A. Perrig.Secure "Sensor Network Routing: A Clean-Slate Approach,". *In CoNEXT*, pp. 11-24, 2006.
[29] J. Deng,; R. Han, & S Mishra,. "INSENS: intrusion-tolerant routing in wireless sensor Networks,". Technical Report CU-CS-939-02, Department of Computer Science, University of Colorado at Boulder.
[30] A. Perrig, R. Canetti, J.D. Tygar, ve D. Song, "Efficient authentication and signing of multicast streams over lossy channels", *IEEE Symposium on Security and Privacy*, pp. 56-73, 2000.
[31] J. Sen, & A Ukil,. "A secure routing protocol for wireless sensor Networks,". *Proceedings of the International Conference on Computational Sciences and its Applications (ICCSA'10)*, pp. 277 – 290, Fukuaka, Japan, 2010.
[32] S-B. Lee, & Y-H. Choi, "A resilient packet-forwarding scheme against maliciously packet-dropping nodes in sensor Networks,". *Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 59-70, 2006.
[33] H. W. Ferng, D. Rachmarini, "A Secure Routing Protocol for Wireless Sensor Networks with Consideration of Energy Efficiency,"*IEEE Network Operations and Management Symposium (NOMS)*, pp. 105-112, 2012.
[34] A. K. Pathan and C. S. Hong, "SERP: secure energy-efficient routing protocol for densely deployed wireless sensor network", *Annales des Telecomm.,* pp. 529–541, 2008.
[35] K. Lin, Ch. F. Lai, X. Liu, X. Guan, "Energy efficiency routing with node compromised resistance in wireless sensor networks," *Mob. Netw. Appl*. vol. 17, pp. 75-89, 2012.

F. YILDIRIM OKAY 2010 yılında Çankaya Üniversitesi Bilgisayar Mühendisliği Bölümünden mezun olmuştur. Aynı üniversitenin İşletme Bölümünden Çift Anadalı bulunmaktadır. 2013 yılında Gazi Üniversitesi Bilgisayar Mühendisliği Bölümünden yüksek lisans derecesini almıştır. Aynı bölümde Araştırma Görevlisi olarak çalışmakla birlikte Gazi Üniversitesi Bilgisayar Mühendisliği Bölümünde doktora çalışmalarına devam etmektedir. Kablosuz algılayıcı ağlar, güvenlik, yapay zeka konularında çalışmaktadır.

S. ÖZDEMİR yüksek lisans derecesini 2001 yılında Syracuse Üniversitesinden almıştır. Doktora derecesini 2006 yılında Arizona State Üniversitesinden almıştır. Şu anda Gazi Üniversitesi Bilgisayar Mühendisliğinde öğretim üyesi olarak çalışmaktadır. Algılayıcı ağlar, kablosuz ağlar, ağ güvenliği ve veri madenciliği konularında çalışmaları bulunmaktadır.

Ş. SAĞIROĞLU Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü öğretim üyesidir. Zeki sistem kimliklendirme, tanıma ve modelleme, ve kontrol; yapay sinir ağları ve yapay zeka uygulamaları; sezgisel algoritmalar; endüstriyel robotlar; zeki anten analizli ve tasarımı; internet, web ve bilişim sistemleri ve uygulamaları; yazılım mühendisliği; bilgi ve bilgisayar güvenliği; biometri, elektronik ve mobil elektronik imza ve açık anahtar altyapısı; kötücül ve casus yazılımlar; sosyal ağlar gibi konularda çalışmaktadır. 100'e yakın SCI tarafından taranan uluslararası dergilerde yayımlanmış makalesi, 100'ün üzerinde ulusal dergilerde yayımlanmış makalesi, 200'ün üzerinde uluslararası konferans ve sempozyum bildirisi ile ulusal sempozyum, konferans ve çalıştaylarda sunulmuş pek çok bildirisi bulunmaktadır. Ayrıca, bilgi güvenliği ve biyometrik alanında alınmış patentleri bulunmaktadır.