# Kablosuz Algılayıcı Ağlarda Güvenli Ortam Erişim Protokolleri

Feyza YILDIRIM OKAY, Suat ÖZDEMİR
*Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Maltepe, Ankara, 06570*
feyzaokay@gazi.edu.tr, suatozdemir@gazi.edu.tr

***Özet*—Kablosuz algılayıcı ağlar (KAA) son zamanlarda geliştirilen ve araştırmacıların üzerinde durduğu konulardan biridir. Çok geniş bir kullanım alanı olan kablosuz algılayıcı ağlar, askeri, sağlık, kimyasal, çevresel, endüstri ortamlarında kullanılabilmekle beraber, saptama, iz sürme, gözlemleme gibi işlevleri yapabilmektedirler. Kötücül kişiler, sınırlı güç tüketimi olan algılayıcıların oluşturduğu KAA'ların güvenliğini, ortam erişim kontrol protokollerindeki açıklardan faydalanarak tehdit etmektedir. Özellikle, farklı saldırı yöntemleriyle saldırganlar ağın yaşam ömrünü kısaltmaktadır. Bu makalede KAA'lardaki ortam erişim protokolleri üzerine gerçekleştirilen saldırılar ve bu saldırılara karşı geliştirilen protokoller özetlenmiş ve karşılaştırılmıştır.**

***Anahtar Kelimeler*—KAA; MAC; güvenlik; ağ ömrü**

***Abstract*—Wireless Sensor Networks (WSN) are one of the recent hot research areas that attracts researchers. WSNs have a wide range of application areas that include military, chemical, environmental and industrial applications. Due to their unattended nature malicious users attack WSNs by exploiting the weaknesses in medium access protocols. Especially, using different kind of attacks, attackers attempt to reduce the network lifetime. This paper summarizes the important attacks against the medium access control protocols of WSNs. The existing solutions to these attacks are also investigated and a comparison of these solutions is provided.**

***Key Words*—WSN; MAC; security; network lifetime**

## I. GİRİŞ

Kablosuz algılayıcı ağlar (KAA), genel olarak çok sayıda algılayıcı düğümden oluşmaktadır. Bu düğümlerin sayısı KAA'nın kullanılacağı uygulamaya göre değişmektedir. Her bir düğüm oldukça sınırlı bir işleme yeteneğine ve hafızaya sahiptir [1]. Düşük enerjili akıllı algılayıcı düğümler, bir veya birden çok algılayıcı, işlemci, hafıza, güç kaynağı, radyo ve çalıştırıcı ile donatılmaktadır. Batarya, algılayıcı düğümlerdeki ana güç kaynağıdır. Düğümlerin dağılacağı ortamın uygun olmasına göre ikinci güç kaynağı olarak güneş panelleri konulabilmektedir [2]. Genellikle KAA'lar fiziksel veya çevresel durumları görüntüleyen sistemlerdir. Kablosuz algılayıcılar birçok farklı uygulamada kullanılabilmektedir. Bunlar; çevresel görüntüleme, ortam görüntüleme, askeri operasyonlar, bilimsel araştırmalar, oluşabilecek felaketleri tahmin etme ve ortaya çıkarma, tıbbi görüntüleme ve yapısal sağlık görüntülemeleridir [3,4]. Algılayıcı düğümler oldukça düşük enerjili ve değiştirilmesi çoğu zaman mümkün olmayan bataryalara sahiptirler. İşlem ve iletişim kaynakları da oldukça kısıtlı olup, sınırlı bir ömürleri vardır [1]. Bu nedenle kablosuz algılayıcı ağlarda yapılan çalışmalar daha çok algılayıcı düğümlerin yaşam sürelerini uzatmaya yöneliktir.

Ortam erişim katmanı, iki düğüm arasındaki iletimden sorumlu olup görevi düğümlerin paylaşımlı bir kanal üzerinden ne zaman ve nasıl iletim yapacağını belirlemektedir [5]. Ortam erişim kontrolü (MAC) protokolleri ile ağın yaşam süresi uzatılmakta ve enerji tüketimi azaltılarak enerjinin daha etkin kullanılması sağlanmaktadır. Ayrıca, adaptasyon ve ölçeklenebilirlik ile araştırmacılar algılayıcı ağların yaşam sürelerini uzatmaya çalışmaktadırlar [6,7]. Diğer taraftan MAC protokollerinin hareketlilik (mobilite) desteği olması dikkat edilmesi gereken diğer bir konudur. KAA'ların çoğu zaman askeri ve görev kritik alanlarda kullanıldığını da düşünürsek güvenlik MAC protokolleri için oldukça önem arz etmektedir.

Bu çalışmada literatürde KAA'lar için geliştirilmiş olan önemli MAC protokolleri araştırılmış ve özetlenmiştir. İncelenen MAC protokolleri özellikle güvenlik açısından ele alınmıştır. KAA'ların güvenliği üzerine yapılan araştırmalar incelenmiş, sonrasında MAC protokolleri ile KAA'ların güvenliğinin nasıl sağlanabileceği konusundaki çalışmalar özetlenerek bir karşılaştırma verilmiştir. Ayrıca, ele alınan bu MAC protokollerinin etkin oldukları saldırı türleri ve özellikleri belirtilmiştir.

Makalenin geri kalan kısmı şu şekilde düzenlenmiştir: II. bölümde KAA'larda güvenlikten bahsedilmiştir. III. bölümde MAC protokolleri tasarımı hakkında bilgi verilmiş ve IV. Bölümde literatür çalışması ile güvenli MAC protokolleri arasında karşılaştırmalar yapılıp, avantaj ve dezavantajları belirtilmiştir. V. bölümde ise incelenen MAC protokolleri üzerinden sonuç ve çıkarımlar yapılıp, geleceğe yönelik araştırılabilir konular üzerinde durulmuştur.

## II. KAA GÜVENLİK

Düşman hatlarının ya da sınır bölgelerinin gözetlenmesi gibi hassas KAA uygulamalarında, algılayıcı düğümlerden baz istasyonuna gizli veri aktarımını sağlayan güvenlik protokolleri kullanılmalıdır. Ancak, KAA'ların düşük hafıza kapasitesi, sınırlı güç kaynağı, kısıtlı hesaplama yeteneği bulunması güçlü koruma sağlamasını zorlaştırmaktadır. Düğümler arasındaki yüksek hata oranı,

ara sıra kapanmalar yaşanması, ani iletişim girişimlerini kapsayan sürekli değişim gösteren topolojileri nedeniyle KAA'larda güvenliği sağlamak oldukça zordur. Ayrıca, algılayıcıların fiziksel olarak güvenlikleri sağlanamadığından, algılayıcı düğümleri kötücül kişiler tarafından ele geçirilebilmekte ya da yeniden programlanabilmektedir. Bu tip algılayıcı düğümler "ele geçirilmiş düğümler" (compromised nodes) olarak tanımlanır. Algılayıcı düğümler bir görevi tamamlamak için birbirleriyle etkileşim halinde ve koordine bir şekilde çalışırlar. Bir düğümün düşmanlar tarafından ele geçirilmesi ağ yapısındaki düğümler arasındaki koordinasyonu bozmaktadır [1]. Bu nedenle güvenliği sağlamak ve bu zorluklarla başa çıkmak için daha sınırlı bir kablosuz algılayıcı güvenlik protokollerinin oluşturulması gerekmektedir [8].

Şifreleme ve doğrulama işlemleri bir sistemi, kulak misafiri olma veya diğer saldırı türlerine karşı daha güvenli hale getirmektedir. Şifreleme veriyi düşmanlara karşı güvenli halde tutarken, doğrulama ise sistemi sahte verilerden korumaktadır [9]. Geleneksel ağlarla kıyaslandığında, KAA'lar düğümler arasındaki bazı işlemsel kısıtlar ve ağın yaşam ömrü için önemli olan enerjiyi korumak adına çok daha karmaşık bir yapı göstermektedir [10]. Diffie-Hellman anahtar değişimi veya RSA imzalama gibi açık anahtarlama kriptografileri limitli hafıza, hesaplamalar ve güç gibi nedenlerden dolayı KAA'larda çok fazla tercih edilmemektedir. Simetrik kriptografi ve özet fonksiyonları ise açık anahtar algoritmalarından daha hızlı ve daha çok işlemsel etkinliğe sahiptirler. Dolayısıyla KAA'lardaki güvenlik araştırmalarında ve geliştirilen güvenlik şemalarında çoğunlukla simetrik anahtar kriptografisi kullanılmaktadır. Simetrik şifrelemedeki temel problemlerden birisi, paylaşılan anahtarın düğümler arasında nasıl dağıtılacağıdır. Diğeri ise, dağıtılan bu anahtarın iletim sırasında gizliliğinin korunmasıdır. Düşman saldırısında bu anahtar ele geçirilmemelidir. Bu nedenle anahtar yönetimi ve anahtar dağıtımı KAA'lardaki güvenliğin korunmasındaki temel gereksinimlerdendir [11].

[32] nolu çalışmada güvenlik açığına sebep olan hizmet engelleme saldırına ortam erişim kontrol protokolleri üzerinden saldırı türüne uygun şekilde çözümler gerçekleştirilmiştir. Ayrıca düşmanlar tarafından ele geçirilen, imha edilen ya da kötücül düğümler sürekli mesaj yollayarak çevrelerindeki düğümlerin enerjisinin tüketimine sebep olabilmektedir. Bu tip saldırılara karşı etkin çözümler sunulmuştur. Düşman düğümlerin hareketli oldukları da varsayılarak düğümlerin bulundukları bölge karantinaya alınmakta ve komşu düğümlerin sadece kimlik doğrulama mesajları göndermeleri sağlanmaktadır.

## A. KAA'LARDA GÜVENLİK GEREKSİNİMLERİ

Genel olarak bahsedildiği gibi, güvenlik KAA'ların en önemli sorunlarından biri sayılmaktadır. Bu bölümde KAA'larda ne tür güvenlik gereksinimlerine ihtiyaç olduğunu açıklanmaktadır. Gereksinimlerin çoğu geleneksel kablolu ve kablosuz ağlar için ortak olmasına rağmen bu bölümde KAA'lar açısından güvenlik ön planda tutulmuştur [12].

### *1) Veri Gizliliği*

Veri gizliliği KAA'larda, veriye yetkisiz kişilerin erişiminin engellenmesini garanti altına almaktır ve hassas KAA uygulamalarındaki en önemli gereksinimden biridir. Algılayıcı ağdaki bir düğüm çevreden okuduğu verileri komşu düğümlere sızdırmamasının sağlaması gerekir [13,14]. KAA'ların uygulama alanlarından biri olan askeri uygulamalarda düğümler çok hassas veriler depolayabilmektedir. Ayrıca diğer birçok uygulamalarda düğümler anahtar dağılımı gibi çok hassas olan bu verileri kablosuz kanal üzerinden diğer algılayıcı düğümlerine aktarmak zorundadırlar. Aktarılan bu verilerin kötücül düğümlere karşı gizliliğinin sağlanması gerekmektedir. Çünkü kötücül düğümler bu verilerden yararlanarak ağın performansını düşürebilirler. Bu nedenlerle KAA'larda veri aktarımı için güvenli bir iletişim kanalı oluşturulması çok önemlidir. Hassas olan bu verileri gizli tutabilmek için verinin gizli bir anahtarla şifrelenmesi gerekmektedir.

### *2) Veri Bütünlüğü*

Veri gizliliği bir verinin kötücül düğümler tarafından ele geçirilmesi önleyebilirken, içeriğinin değiştirilmesini önleyemez. Veri bütünlüğü verinin yetkisiz kişiler tarafından değiştirilmemesini garanti etmektedir. Bir kötücül düğüm mesajları bozarak ağın düzgün çalışmasına engel olabilir. Dahası, doğrudan doğruya bir kötücül düğüm olmadan da mesajlar aktarım esnasında da bozulabilir. Bu nedenle veri bütünlüğü için MAC ya da dairesel kodları (cyclic codes) kullanmak zorunludur.

### *3) Kimlik Doğrulama*

KAA'lar ortak kablosuz ortamı kullandığından, kötücül düğümlerden gelen mesajları veya yanıltma paketlerini bulmak için, kimlik doğrulama mekanizmalarına ihtiyaç vardır. kimlik doğrulama metotları bir düğümün iletişim halinde olduğu düğümün kimliğini doğrulayabilmesini sağlamaktadır. Kötücül düğümler, kimlik doğrulamanın olmadığı durumlarda, başka bir düğüm gibi yaparak hassas bilgilere ulaşabilirler. Eğer sadece iki düğüm arasında veri iletişimi yapılıyorsa kimlik doğrulama gizli anahtar kriptografisi ile yapılabilir. Alıcı ve verici düğüm ortak bir gizli anahtar paylaşımı yaparak tüm mesajların doğrulama kodunu hesaplayabilir. Ancak buradaki problem ise gizli anahtarın alıcı ve verici düğümler arasında nasıl dağıtılacağıdır.

Yayımlama (broadcast) türü iletişimde kaynak doğrulama için daha kompleks çözümlere ihtiyaç vardır. Perrig et. al. µTESLA [14] adlı güvenli yayımlama protokolünde gizli anahtarların açıklanmasını geciktirerek gizli anahtar kriptografisi ile yayımlama türü iletişimde kaynak doğrulamayı başarmıştır. µTESLA her bir düğüme özel olarak gönderilmiş "özetlenmiş anahtar zincirlerine" (hashed key chains) bağlıdır. Ancak her bir düğüme anahtar zincirlerinin güvenli olarak gönderilmesi bir sorundur.

### *4) Erişilebilirlik*

Erişilebilirlik KAA'ların hizmet devamlılığını hizmet engelleme (denial of service/DoS) saldırıları sırasında da devam ettirebilmesidir. DoS saldırıları KAA'daki tüm katmanlarda olabilir ve düğüm etkisiz hale getirilebilir. DoS

yükü düğümün bataryasını beklenenden daha çabuk bitirebilir. Erişilebilirlik KAA'larda genelde algılayıcı düğüm artıklığı ile sağlanmaktadır.

## III. ORTAM ERİŞİM KONROL PROTOKOLLERİ TASARIMI

MAC protokollerinin ağın yapısına, alt üst katmanların gereksinimlerine ya da parçaların yeteneklerine göre farklı fonksiyonlar gerçekleştirmeleri beklenir. Çerçeveleme, ortam erişimi, güvenilirlik, akış kontrolü ve hata kontrolü MAC protokollerinin genel olarak ağ üzerinde sağlaması gereken özelliklerdir [15].

KAA'ların sınırlı bir güç kaynağı, hafıza kapasitesi, işleme yeteneği bulunmasından dolayı kablosuz algılayıcı ağlar için bir ortam erişim kontrol protokolü tasarlamak oldukça zordur. Sürekli değişen topolojiye sahip olmaları ağ yapısında dinamizm oluşturmaktadır. Tasarlanan MAC protokollerinin düğümlerdeki bu değişimlere adaptasyonları sağlanmalıdır [16]. Ayrıca bu protokollerin askeri, sağlık, çevresel ve kimyasal alanlar başta olmak üzere çok farklı alanlarda kullanılabilir olması hepsini kapsayan ortak bir ortam erişim kontrolünün tasarlanmasını oldukça zorlaştırmaktadır [17].

İyi bir MAC protokolünde olması gereken başlıca özellikler şu şekildedir [6,7,18]. Düğümler için ağın yaşam ömrü çok önemlidir. Bu nedenle, KAA'larda MAC protokolleri için öncelikle enerji etkinliği sağlanmalıdır. Diğer önemli husus da ölçeklenebilirliktir. Ağ genişliği, düğümün yoğunluğu ve topolojileri değişebilir. Ağ yapısına yeni bir düğüm eklendiğinde ağ üzerindeki etkileşimde ya da tüm ağın topolojisinde değişmeler meydana gelebilmektedir. İyi bir MAC protokolünün bu tip değişimlere karşı uyumlu olması gerekmektedir. MAC protokolleri için diğer önemli hususlar ise tarafsızlık, gecikme, iş çıkarma (throughput) yetenekleri ve bant genişliği kullanımıdır. Gecikme, iş çıkarma yeteneği veya tarafsızlık durumları yapılan uygulamaya göre değişebilmektedir. Gecikmede çevreden alınan bilgiler, çıkış düğümüne uygun harekete geçmesi için haber vermektedir. Tarafsızlıkta ise sınırlı bant genişliği olduğu durumlarda çıkış düğümü, tüm düğümlerden adil bir şekilde bilgi almaktadır. Geleneksel ağ yapıları için bunlar birinci dereceden önem arz ederler. Ancak KAA'da ise bunlar ikinci dereceden önemlidirler. KAA için en önemli konu ağın ve düğümlerin yaşam süreleridir.

Yapılan son çalışmalarda MAC protokollerinin güvenlik özelliği üzerinde de durulmuştur. Kötücül kişiler ağlar üzerindeki düğümleri ele geçirerek veya ağlardaki MAC protokollerinin açıklarından yararlanarak KAA'lar için tehdit oluşturulabilmektedir. Çünkü KAA'lar oldukça hassas bilgiler taşımaktadırlar [19]. Alana dağıtımı yapılan düğümler her zaman kurallara uygun düğümler olmayabilmektedir. Bazen düşmanlar tarafından kötücül bir düğüm yeni bir düğüm olarak tanıtılabilmektedir. Bu kötücül yeni düğümleri günümüzdeki kablosuz ağlar güvenlik teknolojisi ile kurallara uygun olan düğümlerden ayırt etmek oldukça güçtür. Bu nedenle kötücül düğümler, diğer normal olan düğümler tarafından kurallara uygun düğümler olarak kabul edilecektir. Kötücül düğümlerin bu şekilde kablosuz ağlara katılımını engellemek için erişim kontrolü ile kablosuz düğümlerin dağıtımlarının kontrol edilmesi gerekmektedir [31]. Ayrıca, KAA'larda kullanılacak olan MAC protokolleri bu ağların kendilerine has özellikleri ve "ele geçirilmiş algılayıcılar" göz önüne alınarak tasarlanmış olmalıdır. Yapılan çalışmalar farklı türdeki saldırılardan korunmayı amaçlamaktadır. Saldırı türlerinden biri olan hizmet engelleme saldırıları, farklı şekillerde olabilmektedir. Uyumayı engelleme, çakışma atakları, tüketme atakları ve karıştırıcı ataklar başlıca üzerinde durulan hizmet engelleme saldırılarıdır [20]. Örneğin uyumayı engelleme saldırıları, düğümü uyanık tutmaya çalışarak daha fazla güç harcanmasına neden olur. Herhangi bir güvenlik mekanizmasında algılayıcı düğümler veri almadan ve güvenlik özelliklerini kontrol etmeden önce uyanık olmalıdır. Güvenlik mekanizması olmadan, anti-düğümlerden biri sahte bir başlangıç yayınlayabilir. Alıcı gerçek ile sahte olanı ayırt edemezse, anti-düğümden aldığı sahte başlangıç ile veriyi alır ve işler. Bu şekilde veri iletimi devam eder ve alıcı saldırgan tarafından devamlı uyanık tutulur. Bu durumda ise düğümün bataryası çok hızlı bir şekilde tükenir [21].

Hizmet engelleme saldırıları MAC'lerde kullanılan protokollere, açıklarından faydalanarak iletişimi kesme, düğümlerin yaşam ömürlerini kısaltma gibi ağ güvenliğini tehdit edici zararlar vermektedir. Bozma türünde (jamming) ve ortam erişimlerinde hizmet engelleme türünde saldırılar yapılabilmektedir. Bozma türünde yapılan saldırılar kanala yayılan eş frekanstaki bir dalga sonucu fiziksel katmanlara ve ortam erişim katmanlarına zarar vermektedir. Ayrıca, erişim kurallarına aykırı bir şekilde çok sayıda paket göndererek ortam erişimin protokolüne zarar vermektedir [17,22,23].

## IV. GÜVENLİ ORTAM ERİŞİM PROTOKOLLERİ

MAC protokollerinin algılayıcı ağlar üzerinde geniş bir kullanım alanı vardır. Algılayıcı ağlar üzerindeki farklı MAC protokollerinin bir özelliği sağlamak için diğer özelliklerden ödün vermeleri gerekebilmektedir.

Güvenlik konusu KAA'lar için önemli olup güvenliğe dayalı çalışılan ortam erişim protokolleri şu şekildedir. [17] nolu çalışmada farklı DoS saldırıları tespit edilip, saldırı türüne en uygun çözümü üretebilecek bir AR-MAC protokolü tasarımı yapılmıştır. Bu protokol, KAA'lardaki hizmet engelleme saldırı türlerinden olan sürekli saldırgan, aldatıcı saldırgan, reaktif saldırgan, rastgele saldırgan ve periyodik küme saldırganlarını birbirinden ayırarak, saldırı türüne göre en uygun çözümü üretmektedir. Simülasyon sonuçlarına göre, saldırıların etkinliği önemli ölçüde azalırken, düğümlerin yaşam sürelerinde de artışlar meydana gelmiştir. Çalışmada AR-MAC protokolü, S-MAC [7] protokolüyle kıyaslanarak protokolün performans analizi yapılmıştır. AR-MAC protokolünde, düğümlerin yaşam sürelerinin uzun olması sebebiyle, engellenen paket oranı S-MAC ile kıyaslandığında daha düşük olmaktadır. AR-MAC protokolünde dinleme süresinin ile paket gönderme oranları azalmaktadır. Düşük görev döngüsü ile yaşam ömürleri uzayan düğümlerin toplam engellenen paket oranları düşmektedir.

Sinir ağlarının KAA'lardaki güvenliğini sağlaması üzerine yapılan bir araştırmada, MAC'lere dayalı çok

katmanlı algılayıcılar (MLP) [4] kullanılmıştır. DoS saldırılarını çakışma saldırıları, adaletsizlik saldırıları ve tüketme saldırıları olarak incelemiştir. Şekil 1'de yapısı gösterilen bu çok katmanlı algılayıcılar KAA'lara karşı olası herhangi bir saldırıda değişen parametreler ve varyasyonlar göstererek güvenlik sağlamaktadırlar. Düğümler için oldukça kritik olan bu parametler, çakışma oranı ($R_C$), paket isteği oranı ($R_T$) ve paket bekleme süresidir ($T_w$). Şüpheli bir durum anında parametler olağandışı bir şekilde değişmeye başlamakta ve MLP bu değişimlere göre saldırıyı tespit etmektedir. Sonrasında protokol, düğümün fiziksel ve MAC katmanlarını kapatarak, güvenli hale getirmeye çalışmaktadır. Bu sayede güç tasarrufu sağlanarak, ağın ömrü uzamış olmaktadır. Yapılan çalışmalar aynı zamanda düğüm üzerinde saldırı olmadığı halde aktivasyonunda normal şartlar altında bir artış meydana geldiğinde, MLP'lerin yanlış alarm verebileceğini ve düğümün kapatılmasına sebep olabileceğini de göstermektedir. Yanlış alarmlar sonucu ağ üzerindeki katmanlar kendilerini kapatarak ve bu nedenle gereksiz yere enerji harcayarak ağın etkinliğini azaltmaktadır. MLP'ye dayalı MAC protokolü ile farklı saldırı türlerinde ağın yaşam süresi değişmektedir. Bu nedenle uygulanacak benzetim göre bir enerji modeli oluşturulmalıdır.

FSMAC [24] protokolü CSMA/CA [25] protokolünün üzerine sızma tespit ve sızma savunma modülleri eklenerek oluşturulmuş yeni bir güvenli MAC protokolüdür. CSMA/CA protokolü daha çok ortak kanalın daha etkin ve adaletli bir şekilde nasıl kullanılacağını belirlemek için tasarlanmıştır. Ancak DoS saldırılarına karşı kırılgan bir yapı göstermektedir. Geliştirilen FSMAC ile her bir düğüm kendi kendini savunabilmektedir. Merkezi bir kontrol bulunmamaktadır. Her iki modül de dağıtık bir yapıdadır. Bu protokolün belirlenmesi için öncelikli olarak KAA'lar üzerindeki hizmet engelleme saldırıları çakışma atakları, haksızlık atakları ve tüketme atakları olmak üzere üç farklı sınıfa ayrılmıştır. Göstergeler olarak RTS varış oranı, ortalama bekleme süresi ve çakışma oranları tanımlanmıştır. Çünkü tüketme saldırılarında yüksek sayıda paket alınırken, haksızlık ve çakışma saldırılarında ortalama bekleme süresi uzamaktadır. Ayrıca, çakışma saldırılarında çakışmalar oldukça sık yer almaktadır. Bu nedenle gösterge olarak bu değerler ölçülüp, güvenli MAC protokolü tasarlanmıştır.

Sonuç olarak, FSMAC protokolü ile herhangi bir yanlış alarm olmadan tüm sızmalar tespit edilebilmektedir. Hizmet engelleme saldırılarına dayalı başarısız veri transferleri %25 oranında azaltılmıştır. Böylece başarısız iletişimden dolayı enerjinin boşa harcanması azaltılarak yarı yarıya enerji korunmuştur. [24].

Adrian Perrig ve arkadaşlarının önerdiği SPINS protokolü [14], SNEP ve µTESLA adlı iki güvenli yapı bloğundan oluşmaktadır. 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 algılayıcı ağlar üzerindeki bazı zorluklarına çözümler üretilmiştir. Son zamanlarda önerilen TESLA doğrulanmış 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.

TinySec [19], KAA'larda güvenliği sağlamak amacıyla tasarlanmış bir link katmanı protokolüdür. Tamamlanmamış SNEP'in yerine tasarlanan bu protokol, erişim kontrolü, mesaj bütünlüğü ve gizliliğini sağlamaktadır. IEEE 802.11 [26] ve GSM'lerdeki güvenlik açıkları düşünülerek oluşturulmuştur. Klasik güvenlik protokollerinde güvenlikli hale getirmek için 16-32 bayt ek yük oluşmaktadır. Ancak KAA'ları düşündüğümüzde küçük hafızası, zayıf işlemcisi, kısıtlı enerjisi ve 30 bayt paketleriyle ek yük oluşturmak istenilen bir durum olmamaktadır. TinySec, çeşitli donanımlara ve radyo platformlarına uyumlu olacak şekilde tasarlanmıştır. TinySec güvenliği sağlamak için ortak bir anahtar kullanır. TinySec'in 36 düğümü üzerinde yapılan çalışma ile bu link katmanı protokolünün uygun ve etkin olduğu saptanmıştır. Ayrıca %10'dan az bir enerji, gecikme ve bant genişliği ek yükü eklemektedir [27].

TinySec'de iki farklı işlem modu bulunmaktadır. Bunlar TinySec-AE (authenticated encryption) ve TinySec-Auth. (authentication only)'dir. TinySec-AE modunda TinySec veri yükünü şifreler ve paketleri MAC (message authentication code) doğrular. TinySec-Auth. modunda ise TinySec bütün paketi MAC ile doğrular. Veri yükü ise şifrelenmez. TinySec'in en önemli özelliklerinden biri de kullanım kolaylığı ve şeffaflığıdır [9].

TinySec düşük enerji tüketimi ve hafıza kullanımı sağlarken, güvenlik konusunda istenen performansı gösterememektedir. Ayrıca, düğüm yakalama saldırılarına karşı koruma girişiminde de bulunmamaktadır. Güvenli bir iletişim için gerekli olan gizlilik, doğrulama ve mesaj tekrarlama korumasını sağlarken aynı zamanda düşük enerji tüketimi yapamamaktadır [28].

SenSec [29], TinySec'e benzeyen bir link katmanı protokolüdür. TinySec iki farklı modda çalışırken, SenSec tek bir modda çalışmaktadır. TinySec-AE modu ile benzer olan şifrelemeli doğrulama modunda çalışır. SenSec ile güvenliği artırıcı ve enerji tüketimini azaltıcı bazı iyileştirmeler yapılmıştır. Ayrıca hesaplama ve MAC (mesaj doğrulama kodu) için gerekli olan maliyet azaltılmıştır. Çoklu-anahtarlamalı mekanizma ile tüm ağ yapısı farklı saldırı türlerine karşı dayanıklı hale gelmiştir. SenSec'deki bu anahtarlama mekanizması düğüm yakalama saldırılarına karşı kısmi esneklik sağlamaktadır. Kullandığı Skipjack-X blok şifresi ile SenSec, Skipjack blok şifresini kullanan TinySec'e göre tüketme saldırıları karşı daha

esnek yapı göstermektedir. Ayrıca, kaba kuvvet saldırılarına karşı da güçlü bir koruma mekanizması bulunmaktadır.

MiniSec [28] güvenli bir ağ katmanı protokolüdür. ZigBee [30] gibi yüksek güvenlik seviyesi sağlarken, TinySec'den daha düşük enerji tüketmektedir. Blok şifreleme modu olarak OCB (offset codebook) modunu kullanmaktadır [9].

MiniSec'de iki farklı işlem modu bulunmaktadır. Bunlar, tek yönlü paket yayını yapan MiniSec-U ve geniş paket yayını yapan MiniSec-B'dir [9]. İki işlem modu da blok şifreleme modu olarak OCB modunu kullanmaktadır. Ayrıca anlamsal güvenliği sağlamaktadır. MiniSec-B işlem modunda ayrıca tekrarlama saldırılarına karşı da korunma sağlanmaktadır [29]. Ayrıca, herhangi bir iletim ekyükü de oluşmamaktadır [19].

$TE_2S$ [21], çapraz-katmanlı güvenli bir yaklaşımla MAC protokol güvenliğini sağlar. KAA'ları uyumayı engelleme gibi saldırılara karşı korumak için tasarlanmıştır. İki katmanlı güvenli iletim protokolü önerilmiştir. Birinci katmanda oturum anahtar anlaşması yapılırken, ikinci katmanda veri iletimi yapılmaktadır. MAC protokolüne entegresinde herhangi bir ekstra paket kullanılmamaktadır. Bu protokol ile kimlik doğrulama süreci önemli ölçüde azaltmaktadır. Böylece gücü tüketen saldırıların etkisi de azalmaktadır. Enerji analizine bakıldığında etkinlik sağlandığı gözlemlenmiştir. Ayrıca, tekrarlama ve sahtecilik saldırılarına karşı da enerji etkin bir şekilde karşı koyabilmektedir.

## V. SONUÇ VE ÖNERİLER

KAA'ların fiziksel özelliklerinden dolayı MAC protokolleri tasarlanırken üzerinde durulan başlıca konulardan biri enerji etkinliğini sağlamaktır. Enerji etkinliği sağlanarak ağın ömrü uzatılmaktadır. Ancak bazı durumlarda enerji etkinliğini sağlamak gecikme ve maliyet artışı, güvenlik sorunları gibi istenmeyen durumlara neden olmaktadır. Literatürde bu problemleri önlemeye çalışan MAC protokolleri bulunmaktadır.

Yakın zamanda yapılan çalışmaların enerji etkinliği üzerine değil, özellikle güvenlik üzerinde de durulduğu gözlemlenmiştir. Bu protokollerde saldırı etkinliği düşürülerek, güvenli bir veri iletişimi gerçekleştirilmeye çalışılmıştır. Böylece, ağın yaşam süresini de artırmak hedeflenmiştir. Bu çalışmanın bir özeti olarak Tablo I'de farklı MAC protokollerinin hangi saldırı türlerinde etkin oldukları ve ne gibi özellikler gösterdikleri bilgileri yer almaktadır.

ARMAC protokolü hizmet engelleme saldırılarılarına karşı etkinlik sağlamakla beraber, farklı hizmet saldırılarına göre saldırı türünü belirleyerek bir güvenlik geliştirmektedir. MLP'ye dayalı MAC protokolü ve FSMAC protokolü de hizmet engelleme saldırılarına karşı etkinlik sağlamaktadırlar. MLP'ye dayalı MAC protokolünde herhangi bir saldırı durumunda değişen parametrelere göre fiziksel ve MAC katmanlarını kapatarak güvenlik sağlanırken, FSMAC protokolünde her bir düğüm kendi kendini korumaktadır. Bu durum dağıtık bir yapı göstermesinden kaynaklanmaktadır.

TABLO I
GÜVENLİ ORTAM ERİŞİM PROTOKOLLERİ

| PROTOKOLLER | ETKİLİ OLDUĞU SALDIRI TÜRÜ | ÖZELLİKLERİ |
|---|---|---|
| **ARMAC** | DoS Saldırısı | Farklı hizmet saldırılarında, saldırı türünü belirleyerek güvenliği sağlamaktadır. Herhangi bir ek donanıma ihtiyaç duymaz. |
| **MLP'ye Dayalı MAC** | DoS Saldırısı | Herhangi bir saldırı anında değişen parametreleri izleyerek, düğüm üzerindeki fiziksel ve MAC katmanlarını kapatarak güvenliği sağlar. |
| **FSMAC** | DoS Saldırısı | Merkezi bir kontrol yapısı bulunmayıp, dağıtık yapı gösterir. Her bir düğüm kendi kendini savunabilmektedir. |
| **SPINS** | Tekrarlama Saldırısı<br>Gizlice Dinleme Saldırısı | Anlamsal güvenlik ile kulak misafiri olmayı engeller. Gizlilik, bütünlük ve tazelik (freshness) özelliklerini sağlar. |
| **TinySec** | Tekrarlama Saldırısı | Kullanım kolaylığı ve şeffaflık sağlar. Ayrıca erişim kontrolü, mesaj bütünlüğü ve gizliliği sağlar. |
| **SenSec** | Kaba Kuvvet Saldırısı<br>Tekrarlama Saldırısı | Çoklu anahtarlama mekanizması ile farklı saldırı türlerine dayanıklıdır. |
| **MiniSec** | Tekrarlama Saldırısı | Anlamsal güvenlik sağlamaktadır. Ayrıca herhangi bir iletim ek yükü oluşturmaz. |
| **$TE_2S$** | Tekrarlama Saldırısı<br>Sahtecilik Saldırısı<br>Güç Tüketme Saldırısı<br>Uyumayı Engelleme Saldırısı | Herhangi bir ek paket kullanılamaz. Kimlik doğrulama sürecini azaltarak güç tüketme saldırılarının etkilerini azaltır. |

SPINS protokolü, tekrarlama ve gizlice dinleme saldırılarına karşı etkilidir. Kulak misafiri olmayı engellerken, ver gizliliği, bütünlüğü ve tazelik sağlamaktadır. TinySec protokolü tekrarlama saldırılarına karşı bir etkinlik sağlayıp veri bütünlüğü ve gizliliği sağlamaktadır. SenSec, TinySec'e benzer bir protokol olup TinySec'e ek olarak maliyet ve mesaj doğrulama kodu maliyetleri azaltılmıştır. Ayrıca, çoklu anahtarlama mekanizması ile farklı saldırı türlerine karşı bir koruma sağlamaktadır. MiniSec protokolü, anlamsal güvenlik sağlamaktadır. Ayrıca TinySec'den düşük enerji tüketimi sağlamaktadır. Son olarak $TE_2S$ protokolü tekrarlama, sahtecilik, güç tüketme ve uyuma saldırıları gibi birçok saldırı türüne karşı enerji etkinliği sağlamaktadır. Bu bilgilere ek olarak enerji etkinliği ve mobilite (hareketlilik) sağlamaya yönelik MAC protokollerine sayfa sınırlaması nedeniyle değinilmemiştir. Makalenin genişletilmiş versiyonunda bu konulara da değinilecektir.

Bu çalışmada elde edilen sonuçlar göstermiştir ki güvenli MAC protokolleri konusunda yapılan çalışmalar çoğunlukla benzetim ortamı üzerinde yapılmaktadır. Bu protokollerin gerçek ortam üzerindeki etkinlikleri denenmemiş ve sadece benzetim performansı gerçek ortamlarda da benzer şekilde gerçekleştirebilecekleri varsayılmıştır. Diğer KAA alanlarında yapılan çalışmalarda görüldüğü üzere, gerçek ortamlarda hesaba katılmayan bazı faktörler olabilmekte ve sonuçlar çok farklılık gösterebilmektedir. Dolayısıyla gerçek ortamlarda çalışılarak geliştirilecek protokoller bu protokollerin asıl çalışma performanslarını gösterecektir.

## KAYNAKLAR

[1] S. Misra, A. Vaish, "Reputation-based role assignment for role-based access control in wireless sensor Networks," Computer Communications 34 (2011) pp. 281–294

[2] J. Yick, B. Mukherjee, D. Ghosal, "Wireless sensor network survey," Computer Networks 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] R. V. Kulkarni, G. K. Venayagamoorth, "Neural Network Based Secure Media Access Control Protocol for Wireless Sensor Network" Proceedings of International Joint Conference on Neural Networks, Atlanta, Georgia, USA, June 2009 pp.14-19

[5] C. Cano, B. Bellalta, A. Sfairopoulou, M. Oliver, "Low energy operation in WSNs: A survey of preamble sampling MAC protocols," Computer Networks, 55 (2011) pp. 3351-3363

[6] I. Demirkol, C. Ersoy, F. Alagoz, "Mac protocols for wireless sensor networks: a survey," IEEE Communications Magazine, 44 4 (2006), pp. 115–121.

[7] W. Ye, J. Heidemann, D. Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks," IEEE INFOCOM, New York, Vol. 2, (June 2002) pp. 1567-1576

[8] H. S. Ng, M. L. Sim, C. M. Tan, "Security issues of wireless sensornetworks in healthcare applications," BT Technology Journal, 24 2 (2006), pp. 138–144.

[9] N. Sultana, T. Ahmed, S. Hossain, "Study of a new link layer Security scheme in a wireless sensor network," AIUB Journal of Science and Engineering (AJSE), Vol. 10, No. 1, August 2011

[10] X. Chen, K. Makki, K. Yen, N. Pissinou, "Sensor network Security: A survey," IEEE Communications Surveys & Tutorials, 11(2), Second Quarter 2009, pp. 52–73,

[11] J. Rehana, "Security of Wireless Sensor Network," TKK T-110.5190 Seminar on Internetworking, 2009

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

[13] D.W. Carman, P.S. Krus, B.J. Matt, "Constraints and approaches for distributed sensor network security," Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD, 2000.

[14] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar "SPINS: Security Protocols for Sensor Networks," Wireless Networks 8 (2002) 521-534

[15] J.F. Kurose, K.W. Ross "Computer Networking: A Top-Down Approach Featuring the Internet," (third ed.), Addison Wesley (2005).

[16] S.Ray, I. Demirkol, W. Heinzelman, "ADV-MAC: Analysis and optimization of energy efficiency through data advertisements for wireless sensor Networks," Ad Hoc Networks 9 (2011) pp. 876-892

[17] M. Çakıroğlu, A. T. Özcerit,. "Kablosuz Algılayıcı Ağlarda Hizmet Engelleme Saldırılarına Dayanıklı Ortam Erişim Protokolü Tasarımı," J. Fac. Eng. Arch. Gazi Univ.,Vol 22, No 4, (2007) pp. 697-707,

[18] W. Ye, J. Heidemann, D. Estrin, "Medium Access Control with Coordinated, Adaptive Sleeping for Wireless Sensor Networks," IEEE/ACM Transactions on Networking, 12 3 (2004), pp. 493–506.

[19] D. Boyle, Thomas Newe "Securing Wireless Sensor Networks: Security Architectures," Journal of Networks, Vol. 3, No. 1, January 2008

[20] P. M. Pawar, R. H. Nielsen, N. R. Prasad, S. Ohmori, R. Prasad, "Behavioural Modelling of WSN MAC Layer Security Attacks: A Sequential UML Approach,"; Journal of Cyber Security and Mobility, ( 2012) pp. 65–82

[21] C. T. Hsueh, C. Y. Wen, Y. C. Ouyang, "A Secure scheme for power exhausting attacks in wireless sensor Networks," Ubiquitous and Future Networks (ICUFN), 2011 Third International Conference on, , Volume: Issue: , 15-June 2011, pp. 258 - 263

[22] Y. Wei, P. Hartel, J. Den Hertog, P.Havinga, "Link layer Jamming Attacks on S-MAC," Proceeedings of the Second European Workshop on Sensor Network, İstanbul, Türkiye, 2005, pp. 217 – 225,

[23] Y. Wei, L. Lodewijk, V. Hoesel, J. Doumen, P. Hartel, P.Havinga, "Energy-Efficient Link-Layer Jamming Attacks against Wireless Sensor Network MAC Protocols", SANS'05, Virginia, USA, Kasım 2005

[24] Q. Ren, Q. Liang, "Fuzzy Logic-Optimized Secure Media Access Control (FSMAC) Protocol for Wireless Sensor Networks," CIHSPS 2005 - IEEE Iutemational Conference on Computational Intelligence for Homeland Security and Personal Safety Orlando, FL, USA, 2005

[25] L. Kleinrock, F.A. Tobagi, Packet switching in radio channels: Part I-Carrier sense multiple-access modes and their throughput-delay characteristics, IEEE Transactions on Communications 23 (12) (1975) pp. 1400–1416.

[26] IEEE Standard 802.11: Wireless LAN MediumAccessControl (MAC) and Physical Layer (PHY) Specifications, 1999

[27] C. Karlof, N. Sastry, D.Wagner, "TinySec: A Link Layer Securty Architecture for Wireless Sensor Networks," In Second ACM Conference on Embedded Networked Sensor Systems, SenSys 2004, (2004)

[28] M. Luk, G. Mezzour, A. Perrig, V. Gligor, "MiniSec: Secure Sensor Network Communication architecture,",In Proc. of the 6th Int'l Conf. on Information Processinng in Sensor Networks, ACM Press, (2007), pp. 479-488

[29] I. Krontıris, T. Dımıtrıou, H.Soroush, M. Salajeghe "WSN Link-layer Security Frameworks," Athens Information Technology, Greece

[30] ZigBee Alliance. Zigbee specication. Technical Report Document 053474r06, Version 1.0, ZigBee Alliance, June 2005

[31] Y. Zhou, Y. Zhang, Y. Fang "Access control in wireless sensor networks," Ad Hoc Networks 5 (2007), pp. 3–13

[32] G. F. Türker, İ. Tarımer "Türkiye'de Kablosuz Algılayıcı Ağlar ile Yapılan Teknolojik Uygulamalar Üzeirne Bir İnceleme," Muğla Üniversitesi, Elektronik ve Bilgisayar Eğitimi Bölümü, Muğla