Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 29, No 1, 49-59, 2014

Journal of the Faculty of Engineering and Architecture of Gazi University
Vol 29, No 1, 49-59, 2014

KABLOSUZ ALGILAYICI AĞLARDA ORTAM ERİŞİM PROTOKOLLERİ

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

(Geliş/Received: 14.09.2012; Kabul/Accepted: 21.11.2013)

ÖZET

Kablosuz Algılayıcı Ağlar (KAA) son yıllarda hızla gelişen ve araştırmacıların üzerinde çalıştığı konulardan biridir. Çok geniş bir kullanım alanı olan KAA'lar, askeri, sağlık, kimyasal, çevresel, endüstri alanlarında kullanılabilmekte ve saptama, iz sürme, gözlemleme gibi işlevleri yapabilmektedirler. KAA'lardaki en büyük problemlerden birisi ağda bulunan algılayıcıların kısıtlı kaynaklara sahip olmalarıdır. Sınırlı kaynakların başında da batarya ömrü gelmektedir. Literatürde algılayıcıların yaşam süresini artıracak (batarya ömrünü uzatacak) birçok çalışma yapılmıştır. Ayrıca KAA'ların günümüzde hareketli düğümler içermeleri ve askeri uygulamalar gibi güvenliğin önemli olduğu alanlarda kullanılmaları sebebiyle hareketlilik ve güvenlik de KAA'larda üzerinde durulan diğer önemli başlıklar haline gelmiştir. KAA'larda iletim ortamına erişim problemi bahsedilen üç konuyu da doğrudan etkilemektedir ve bu nedenle literatürde ortam erişim protokolleri üzerine birçok araştırma bulunmaktadır. Bu çalışmada KAA'larda kullanılan ortam erişim protokolleri incelenmiş ve enerji etkinliği, hareketlilik ve güvenlik açısından değerlendirilmiştir.

Anahtar kelimeler: KAA, MAC, enerji etkinliği, hareketlilik, güvenlik

MEDIUM ACCESS CONTROL PROTOCOLS IN WIRELESS SENSOR NETWORKS

ABSTRACT

The recent development of Wireless Sensor Networks (WSN) is created a hot research area that attracts many researchers. WSNs have a wide range of application areas including military, chemical, environmental and industry fields. These networks can be used for applications such as surveillance, target detection and tracking. One of the biggest problems of WSN is that sensor nodes have strictly limited resources. The main limited resource is the battery life. In the literature, many studies have been conducted to increase the lifetime of sensor nodes (i.e., extend the battery life). Due to availability of mobile nodes and mission critical applications of WSNs, mobility and security are other important issues in WSNs. Problem of shared medium access is directly related to these issues and hence there are several studies on medium access protocols in the literature. In this study, medium access protocols of WSNs are examined and evaluated with respect to energy efficiency, mobility and security.

Keywords: WSN, MAC, energy efficiency, mobility, security

1. GİRİŞ (INTRODUCTION)

Kablosuz algılayıcı ağlar (KAA) genel olarak çok sayıda algılayıcı düğümden oluşmaktadır. Düşük enerjili ve akıllı bu düğümler, bir veya birden çok algılayıcı, işlemci, hafıza, güç kaynağı ile donatılmaktadır. Algılayıcı düğümlerdeki ana güç kaynağı bataryadır [1,2]. KAA'lar, birçok alanda kullanılabilmektedir. Genel olarak bu alanlar; çevresel görüntüleme, ortam görüntüleme, askeri operasyonlar, bilimsel araştırmalar, oluşabilecek felaketleri tahmin etme ve ortaya çıkarma, tıbbi görüntüleme ve yapısal sağlık görüntülemeleridir [3,4].

KAA'larda kullanılan algılayıcı düğümlerinin oldukça düşük enerjili ve değiştirilmesi çoğu zaman mümkün

olmayan bataryalara sahip olmalarından dolayı KAA'larda yapılan çalışmalar daha çok algılayıcı düğümlerinin yaşam sürelerini uzatmaya yöneliktir. Ağın ömrünü uzatma yollarından biri de etkin ortam erişim protokolleri (Medium Access Control (MAC)) geliştirmektir. Ortam erişim katmanı, iki düğüm arasındaki iletimden sorumludur. Düğümlerin paylaşımlı bir kanal üzerinden ne zaman ve nasıl iletim yapacağını belirlemektedir [5]. Etkin MAC protokolleri ile ağın yaşam süresinin uzaması için boşa harcanan enerji düşürülüp, enerjinin etkin kullanımı sağlanmaktadır. Enerji tüketimi kontrol altına alınarak batarya ömrü uzatılmakta ve KAA'larda birincil dereceden önemli olan enerji etkinliği sağlanarak yaşam süresi uzatılmaktadır [6,7]. KAA'lardaki MAC protokollerine ilişkin çalışmaların çoğunda algılayıcı düğümlerin statik olduğu varsayılmıştır. Ancak, MAC protokollerinin hareketlilik (mobilite) desteği olması günümüzde üzerinde çalışılan diğer bir konudur. Bu sayede, düğümler hareketli örüntülerdeki değişimlere karşı daha iyi adaptasyon sağlayabilmektedirler [8]. KAA'ların çoğu zaman askeri ve görev kritik alanlarda kullanıldığı düşünüldüğünde güvenlik de MAC protokolleri için oldukça önem arz etmektedir. Kötücül kişiler, sınırlı güç tüketimi olan algılayıcıların oluşturduğu KAA'ların güvenliğini, MAC protokollerindeki açıklardan faydalanarak tehdit etmektedir. Özellikle, farklı saldırı yöntemleriyle saldırganlar ağın yaşam ömrünü kısaltmaktadır.

Literatürde KAA'lardaki MAC protokolleri üzerine yapılmış olan bazı derleme çalışmaları bulunmaktadır [6, 9-12]. Bu çalışmalara bakıldığında enerji etkinliği odaklı MAC protokolleri üzerine incelemeler yapıldığı görülmektedir. Bu çalışmada ise literatürde KAA'lar için geliştirilmiş olan önemli MAC protokolleri KAA'ların yapısal ihtiyaçları göz önüne alınarak sınıflandırılmıştır. Her sınıf içerisindeki protokoller özelliklerine göre karşılaştırılmıştır. Enerji etkin ve hareketlilik desteği olan protokoller kendi aralarında karşılaştırılarak ne gibi özelliklere sahip oldukları incelenmiştir. Bunun yanı sıra avantaj ve dezavantajları belirlenmiştir. Çalışmada ayrıca KAA'ların güvenliği üzerine yapılan araştırmalar incelenmiş, sonrasında MAC protokolleri ile KAA'ların güvenliğinin nasıl sağlanabileceği konusundaki çalışmalar özetlenerek bir karşılaştırma verilmiştir. Yapılan literatür taramasında bu çalışmadaki gibi kapsamlı bir karşılaştırma ve sınıflandırma olmadığı görülmüştür. Dahası, MAC protokollerini enerji etkinliği, hareketlilik ve güvenlik özelliklerine göre sınıflandıran Türkçe derleme makalesi bulunmamaktadır. Konuyla ilgili yapılmış olan derleme çalışmalarına bakıldığında ise enerji etkinliği odaklı MAC protokollerinin incelendiği görülmektedir. Bu çalışmada, MAC protokolleri sadece enerji etkinliği odaklı değil, hareketlilik ve güvenlik odaklı olarak da incelenmekte ve protokoller sınıflandırılmaktadır. Çalışma aynı zamanda incelenen protokoller arasında detaylı karşılaştırma tabloları sunmaktadır.

Makalenin geri kalan kısmı aşağıdaki gibi düzenlenmiştir. 2. Bölümde MAC protokolü tasarımı hakkında bilgi verilmiştir. 3. Bölümde literatür çalışması ile enerji etkinliği, hareketlilik ve güvenlik odaklı MAC protokolleri özetlenmiştir. 4. Bölümde ise araştırmanın sonuçları ve geleceğe yönelik araştırılabilir konular üzerinde durulmuştur.

2. ORTAM ERİŞİM KONTROL PROTOKOL TASARIMI (MEDIUM ACCESS CONTROL PROTOCOL DESIGN)

MAC protokollerinin ağın yapısına, alt üst katmanların gereksinimlerine ya da parçaların yeteneklerine göre farklı fonksiyonları gerçekleştirmeleri beklenir. Çerçeveleme, ortam erişimi, güvenilirlik, akış kontrolü ve hata kontrolü MAC protokollerinin genel olarak sağlamaları gereken özelliklerdir [13].

KAA'lar için bir ortam erişim protokolü tasarlamak oldukça zordur. Çünkü KAA'ların sınırlı bir güç kaynağı, hafıza kapasitesi ve işleme yeteneği bulunmaktadır [14]. Yapılan son çalışmalarda ortam erişim katmanlarının enerji tüketimini azaltmanın yanı sıra güvenliğini de arttırmak temel görevler arasına alınmıştır [4,35,36,38,39,41,42,44]. Ayrıca hareketlilik ile geliştirilen protokoller yardımıyla düğümlerin dinamik ağ yapılarında da iyi başarım göstermeleri sağlanmaktadır [8,18,19].

2.1 Enerji Etkinliği (Energy Efficiency)

Ortam erişimde en önemli konulardan birisi düğümlerin yaşam sürelerini etkileyen enerji tüketimidir. Düğümler aşağıdaki şekillerde enerji tüketebilirler [6,15].

- ***Boşken dinleme:*** Özellikle IEEE 802.11 ve CDMA gibi MAC protokollerinde boşken dinleme çok yapılır. Bir mesajın gelip gelmeyeceğini bilmedikleri için devamlı dinlemede kalırlar. Bu da düğümlerin boşa enerji harcamalarına sebep olur.
- ***Çakışma:*** Birden fazla düğüm paketlerini alıcıya eş zamanlı gönderdiklerinde, bu paketlerde bozulmalar meydana gelir. Hasarlı paketlerin tekrar gönderiminde harcanan enerji ise boşa gitmektedir.
- ***Gecikme:*** Yapılan uygulamaya göre olması gereken gecikme süresi değişmektedir. KAA'larda gerekli hareketin yapılabilmesi için olaylar tespit edilir edilmez ana düğüme (sink node) iletilmelidir.

- ***Ek yük:*** KAA'lardaki veri paketleri oldukça küçüktür. Bu nedenle üst başlık ya da kontrol mesajları için ayrıca bir enerji israfı olabilmektedir.

2.2 Hareketlilik (Mobility)

Genelde KAA'ların sabit düğümleri kapsadığı düşünüldüğünden MAC katmanındaki araştırmalar genel olarak hareketlilik üzerine değildir. Bununla birlikte son zamanlarda hareketli düğümlerin daha geniş kullanım alanı bulmasıyla MAC katmanındaki hareketlilik üzerine yapılan çalışmalar artmıştır [8, 16-19].

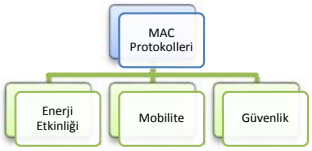
Statik ağlarda iletişimi sağlayan düğümler arasında herhangi bir hareketlilik bulunmamaktadır. Her bir düğüm bulunduğu konumdan iletişim sağlamaktadır. Mobil ağlarda ise düğümler hareketlidir. Düğümlerle ilişkili bir yol başarısız olduğunda yeni bir yol yeniden oluşturulabilmektedir [20]. Mobil düğümler fiziksel olarak ağın topolojisini değiştirebilmekte, ortamdaki olaylara veya amaçlanan hedef üzerindeki değişimlere tepki verebilmektedir. Mobil ağlar, kendini yapılandırma mekanizmasını destekleme, adaptasyon ve ölçeklenebilirlik ya da optimal performansı sağlama hususlarında umut vericidir [21]. Mobil ağlarda topolojik değişimler, çeşitli ağ protokollerinin çalıştırılmasından dolayı enerji tüketiminden ziyade daha çok düğümlerin hareketliliğine dayandırılmaktadır. Bu nedenle mobil ağlarda sistem başarımını arttırmak için hareketlilik yönetimi ve hata kurtarma enerji tüketiminden daha önemlidir [19].

2.3. Güvenlik (Security)

Düşman hatlarının gözetlenmesi ya da sınır bölgelerinin gözetlenmesi gibi hassas KAA uygulamalarında, algılayıcı düğümlerden baz istasyonuna gizli veri aktarımını sağlayan güvenlik protokolleri kullanılmalıdır. Ancak algılayıcı düğümlerin kısıtlı kaynaklara sahip olması, geleneksel güvenlik protokollerinin KAA'larda uygulanmasını zorlaştırmaktadır [22,23]. Ayrıca hareketlilik, düğümler arasındaki yüksek hata oranı, düğümlerin ara sıra kapanmaları ve sürekli değişim gösteren topolojileri nedeniyle algılayıcı düğümlerin güvenliğini sağlamayı zorlaştırmaktadır. Bu nedenlerden dolayı, KAA'lardaki güvenliği sağlamak ve bu zorluklarla başa çıkmak için daha sınırlı bir kablosuz algılayıcı güvenlik protokollerinin oluşturulması gerekmektedir [24]. Ayrıca, KAA'larda kullanılacak olan MAC protokolleri bu ağların kendilerine has özellikleri ve ele geçirilmiş algılayıcılar göz önüne alınarak tasarlanmış olmalıdır.

3. ORTAM ERİŞİM KONTROL PROTOKOLLERİ (MEDIUM ACCESS CONTROL PROTOCOLS)

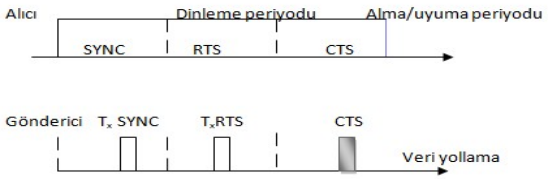
MAC protokollerinin algılayıcı ağlar üzerinde geniş bir kullanımı vardır. Algılayıcı ağlar üzerindeki farklı MAC protokollerinin bir özelliği sağlamak için diğer özelliklerden ödün vermeleri gerekebilmektedir. KAA'larda kullanılan MAC protokolleri enerji etkinliği, hareketlilik ve güvenlik özelliklerine göre sınıflandırılabilir.



Şekil 1. MAC Protokollerinin Sınıflandırılması (Classification of MAC Protocols)

3.1 Enerji etkinliği odaklı MAC protokolleri (Energy efficieny based MAC protocols)

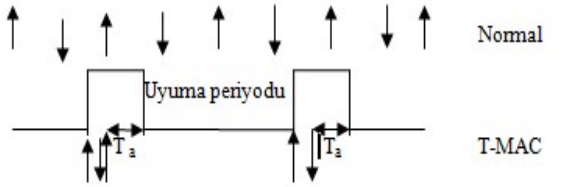
S-MAC (Sensör-MAC), KAA'lar için tasarlanmış IEEE 802.11'den esinlenilmiş bir MAC protokolüdür. Öncelikli amacı enerji tüketimini düşürmek iken, aynı zamanda ölçeklenebilirliği ve çakışmalardan kaçınmayı da sağlar [17]. S-MAC ile düğümler periyodik bir şekilde uyutulur, böylece boşken dinleme yapmaları engellenir. Fakat gecikme artar. Çünkü gönderici alıcının uyanmasını beklemek zorundadır. S-MAC protokolünde periyodik dinleme gecikmeyi artırıp, iş çıkarma yeteneğini (throughput) düşürmektedir. S-MAC, IEEE 802.11 [25] ile kıyaslandığında enerjinin korunması daha iyi sağlanmaktadır. Diğer bir özelliği ise, S-MAC'in trafik yoğunluğuna göre enerji harcama ve gecikme arasında bir ödünleşim oluşturmasıdır [7].



Şekil 2. S-MAC Mesajlaşma Senaryosu [7] (S-MAC Messaging Scenario)

T-MAC protokolü, S-MAC'teki trafik yoğunluğundaki düşük performansı iyileştirmek amaçlı geliştirilmiştir. S-MAC protokolü sabit bir dinleme uyuma görev döngüsü kullanırken, T-MAC protokolü uyumlu bir dinleme uyuma görev döngüsü kullanmaktadır [26]. T-MAC protokolü bekleme durumunu en düşük düzeylere çekebilmektedir. Böylece enerji etkinliği de sağlar. Her düğüm periyodik bir şekilde komşu düğümlerle iletişim sağlayabilmek için uyanır ve herhangi bir olay olmadığında ise uyuma moduna geçerler. T-MAC

protokolünde bir düğümde herhangi bir aktivasyon belirlenemiyorsa uyuma moduna geçerler. T-MAC boşken dinleme süresini değiştirmektedir. S-MAC ile kıyaslandığında çok daha az enerji harcaması oluşur. Ancak T-MAC protokolünde buna karşın gecikmeler daha fazla olmaktadır [27].

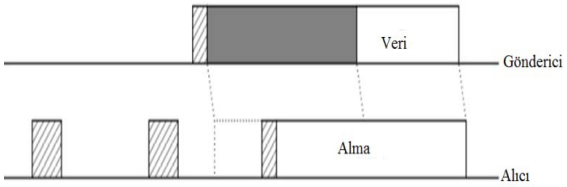


Şekil 3. T-MAC Protokolü [27] (T-MAC Scheme)

TRAMA, TDMA (Time Division Multiple Access)'e dayalı bir algoritmadır. TDMA çakışmaları engelleyen bir ortam erişimi sağlar [6]. TRAMA çakışmaları engellediği için enerji etkin bir protokoldür. Ayrıca iletim ya da alım yapmadığı durumlarda düşük güçte bekleme yapar. Bu da enerji tasarrufunu arttıran bir durumdur. TRAMA protokolü üç ana kısımdan oluşur. NP (Neighbor Protocol) denilen komşu protokolü, komşu düğümler hakkında bilgi toplar. SEP (Schedule Exchange Protocol) adı verilen program değişim protokolü iki sekmeli düğümler arasında bilgi ve program değişimini sağlar. AES (Adaptive Election Algorithm) adaptasyon seçim algoritması ise bilgiyi ileteceği ve alacağı düğümlerin seçilmesine karar verir. Geri kalan düğümler ise düşük enerjili güç modundadır [28].

WiseMAC protokolü [29], KAA'lar için geliştirilmiş bir protokoldür ve Spatial TDMA ve CSMA (Carrier Sense Multiple Access) with Preamble Sampling protokolleriyle benzerlik gösterir. Bu protokollerde tüm düğümler iki kanala sahiptirler. TDMA veri kanalına erişimde, CSMA ise kontrol kanalına erişimde kullanır. Ancak WiseMAC protokolü, sadece bir kanala ihtiyaç duyar ve kalıcı olmayan CSMA with Preamble Sampling ile boşken dinlemeyi azaltarak enerji tasarrufu sağlar. WiseMAC'ler S-MAC'lere göre çok daha iyi performans göstermektedirler. Değişken trafik yoğunlukları altında iyi bir performans sunmaktadır [29,30].

B-MAC [31] eşzamansız bir protokol olup, uyumlu ön işaretli örneklemeye dayalı olarak boşken dinlemeyi azaltmaktadır. ALOHA [32] protokolüne benzerlik gösteren çekişme tabanlı bir protokoldür. Her bir düğüm görev döngüsüne göre uyanıp herhangi bir ön işaret olup olmadığını kontrol etmektedir. Ön işaret göndericinin bir paket yollamak istediğini ve alıcının uyuma aralığından daha uzun süreceğini göstermektedir. Bir düğüm ön işaret nedeni ile uyandırılabilir ve uyanık tutulabilmektedir. B-MAC protokolü düşük trafik yoğunluğunda oldukça enerji etkindir. Ancak yüksek trafik yoğunluğunda başarısız olmaktadırlar. Enerji etkinliği ile gecikme arasında optimal bir denge sağlamaktadır.



Şekil 4. B-MAC Veri Transferi (B-MAC Data Transfer)

ADV-MAC [33], S-MAC ve T-MAC protokollerinden türemiş olup her bir düğümün harcadığı enerjiyi azaltarak düğümlerin yaşam ömürlerini uzatmaya yönelik bir protokoldür. Yeni çıkan bu teknik yüksek öncelikli uygulamalarda gecikmeleri ve paket kayıplarını azaltmayı amaçlamaktadır. Yapılan gelişmeler nedeniyle ADV-MAC protokolü, S-MAC'e göre daha güvenilirdir. Paketleri düşük öncelikli ve yüksek öncelikli olarak sıralayarak ayırmaktadır. Düşük öncelikli paketlere çekişme tabanlı yaklaşımlar uygulanırken, yüksek öncelikli paketlere ise TDMA tabanlı yaklaşımlar uygulanarak sistemin çok enerji harcamadan güvenilirliği sağlanmaktadır.

TA-MAC (Traffic-Adaptive MAC) [34] benzer şekilde S-MAC protokolünün değiştirilmiş hali olup çekişme tabanlı bir protokoldür. TA-MAC protokolü çakışma olduktan sonra geri çekilme prosedürü ile boşken dinlemedeki zamanı azaltarak ve farklı trafik yoğunluklarında çekişme pencerelerinin boyutlarını ayarlayarak çakışma olasılığını azaltıp enerji etkinliği sağlamaya çalışmaktadır.

İncelenen protokollerin KAA'larda enerji etkinliğini nasıl etkiledikleri Tablo 1'de verilmiştir. Ayrıca Tablo 2'de bu protokollerin özellikleri ve çekişme (CSMA) veya zaman paylaşımlı (TDMA) tabanlı olup olmadıkları özetlenmiştir.

Tablo 1. Enerji Etkin Ortam Erişim Protokolleri (Energy Efficient Medium Access Control Protocols)

PROTOKOLLER	BOŞKEN DİNLEME	ÇAKIŞMA	GECİKME	EK YÜK
S-MAC [7]	AZALTIR	AZALTIR	ARTIRIR	AZALTIR
T-MAC [27]	AZALTIR	AZALTIR	AZALTIR	AZALTIR
TRAMA [28]	AZALTIR	AZALTIR	AZALTIR	AZALTIR
WISE-MAC [29]	AZALTIR	AZALTIR	AZALTIR	ARTIRIR
B-MAC [31]	AZALTIR	AZALTIR	ARTIRIR	AZALTIR
ADV-MAC [33]	AZALTIR	AZALTIR	AZALTIR	AZALTIR
TA-MAC [34]	AZALTIR	AZALTIR	ARTIRIR	ARTIRIR

Tablo 2. Enerji Etkin Ortam Erişim Protokollerinin Türü ve Özellikleri (Type and Properties of Energy Efficient Medium Access Control Protocols)

PROTOKOLLER	TÜRÜ	ÖZELLİKLERİ
S-MAC [7]	CSMA	Periyodik dinleme ile boşken dinleme yapılmaz. Böylece enerji etkinliği sağlanır. Ölçeklenebilirlik sağlar. Çakışmalardan kaçınır. Periyodik dinlemeden dolayı gecikmeler artar. Ayrıca, iş çıkarma yeteneği düşer.
T-MAC [27]	CSMA	Uyumlu dinleme ile bekleme durumunu en düşük düzeylerde tutar. Bu özelliğiyle S-MAC'lere göre daha az enerji harcar. Buna karşın gecikme artar.
TRAMA [28]	TDMA	Çakışmaları azalttığından dolayı enerji etkin bir protokoldür. Düşük güçte bekleme yapar.
WISE-MAC [29]	CSMA	Boşken dinleme ile enerji tasarrufu sağlar. Farklı trafik yoğunluklarında enerji etkin bir performans gösterir.
B-MAC [31]	CSMA	Boşken dinleme azaltılarak enerji etkinliği sağlanır. Düşük trafik yoğunluğunda oldukça enerji etkinken, yüksek trafik yoğunluğunda bu etkinlik azalmaktadır.
ADV-MAC [33]	CSMA+TDMA	SMAC-e göre daha güvenilirdir. Paketleri düşük ve yüksek öncelikli olarak ayırarak paketlere CSMA veya TDMA tabanlı yaklaşımlar uygular.
TA-MAC [34]	CSMA	Çakışma olduktan sonra geri çekilme prosedürü ile boşken dinlemeyi azaltır. Ayrıca çakışma olasılığı azaltılır.

Tablo 3. Hareketli Ortam Erişim Protokolleri (Mobile Medium Access Control Protocols)

PROTOKOLLER	ENERJİ ETKİNLİĞİ	AVANTAJ	DEZAVANTAJ
MSMAC [18]	ARTIRIR	İyi bir hizmet kalitesi (QoS) performansı sunarlar.	Mobil düğümlerin ağ yapısını uzun ve sürekli taramalarından dolayı enerji kaybı oluşmaktadır.
SMACS [19]	AZALTIR	Düğümler komşu düğümleri keşfedebilmektedirler ve onlarla iletime herhangi bir yönetici düğüme ihtiyaç duymaksızın iletim başlatabilirler.	EAR algoritması enerji etkinliğini olumsuz etkilemektedir. Mobil düğümler sürekli kanalı dinlemek zorundadır.
MMAC [8]	ARTIRIR	Değişimlere karşı dinamik bir şekilde adapte olurlar.	Algılayıcı düğümlerin hareketsel davranışlarını tahmin etmek için halen üzerinde çalışılan bir problem olan konum bilgisini kullanmaktadır.

3.2. Hareketlilik odaklı MAC protokolleri (Mobility based MAC protocols)

MS-MAC [18] protokolü gözlemlenen düğümün hareketliliğine göre taranan ağ aralığını ayarlamaktadır. Herhangi bir hareketlilik gözlenmediğinde, her 5 dakikada bir, yeni bir komşu keşfedilir. Eğer herhangi bir hareketlilik gözlemlenirse, gerçek bağlantı koptuktan sonra kopukluğu azaltarak komşu keşfi yapılır. Dinamik ağ yapılarında ise bu durum dakika da iki komşu keşfine çıkar. Bu protokolün en büyük dezavantajı ise mobil düğümlerin uzun ve sık süren ağ yapısını taramalarından kaynaklanan enerji kayıplarıdır.

Sabit algılayıcı alanındaki mobil düğümler EAR (Eavesdrop and Register) algoritması ile KAA'lar için kendilerini koordine edebilecek hale gelirler. SMACS [19]'de her bir iletişim linki için tek bir süre dilimi ve frekans kanalı atanır. Yeni bir düğümün ağa katılması için de sabit bir global sinyal kanalı kullanılır. Mobil düğümler EAR algoritmasını çalıştırırlar. Sinyal kanalından yayınsal bir davet alarak, kendi dizilerindeki sabit düğümlere eklenirler. Ancak, kullanılan EAR algoritması enerji yönünden etkin değildir. Çünkü hareketli düğümler sürekli kanalı dinlemek zorundadırlar.

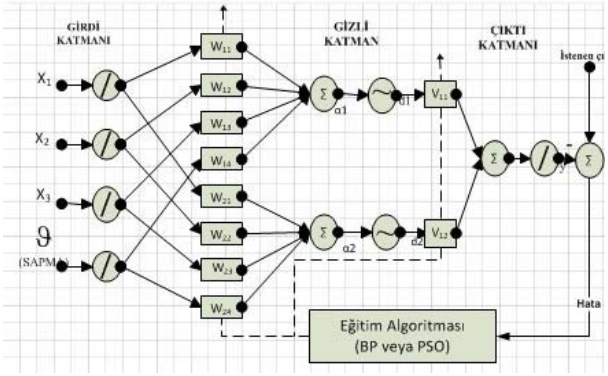
MMAC [8] protokolü, yüksek ve düşük hareketliliği olan algılayıcılı ortamlara uyum sağlayan bir hareketlilik yolu oluşturur. Dinamik bir şekilde uyum sağlar. Zamanlamaya dayalı bir protokol olarak çakışmaları engeller. MMAC protokolü, statik bir ağ ortamında performans olarak TRAMA ile benzer özellikler gösterirken, dinamik ağ yapısında hareketli düğümlerle enerji etkinliği, gecikme ve paket dağıtımlarında TRAMA, SMAC gibi protokollerden daha üstün bir performans göstermektedir. Tablo 3, hareketlilik odaklı MAC protokollerini özetlemektedir.

3.3 Güvenlik odaklı MAC protokolleri (Security based MAC protocols)

[35] numaralı çalışmada yazarlar farklı hizmet engelleme saldırılarını tespit edip, saldırını türüne en uygun çözümü üretebilecek AR-MAC adlı protokolün tasarımını yapmıştır. Simülasyon sonuçlarına göre, saldırıların etkinliği önemli ölçüde azalırken, düğümlerin yaşam sürelerinde artışlar meydana gelmiştir. Bu protokol, KAA'lardaki hizmet engelleme saldırı türlerinden olan sürekli saldırgan, aldatıcı saldırgan, reaktif saldırgan, rastgele saldırgan ve periyodik küme saldırılarını birbirinden ayırarak, saldırı türüne göre en uygun çözümü üretmektedir. AR-MAC protokolü, S-MAC protokolüyle kıyaslanarak performans analizi yapılmıştır. AR-MAC protokolünde, düğümlerin yaşam sürelerinin uzun olması sebebiyle, engellenen paket oranı da S-MAC ile kıyaslandığında daha düşük olmaktadır. AR-MAC protokolünde dinleme süresinin azalması ile paket gönderme oranları düşmektedir. Ancak düşük görev döngüsü ile yaşam ömürleri uzayan düğümlerin toplam engellenen paket oranları düşmektedir [35].

Sinir ağlarının KAA'lardaki güvenliğini sağlaması üzerine yapılan bir araştırmada [4], MAC'lere dayalı çok katmanlı algılayıcılar (MLP) kullanılmıştır. Bu çok katmanlı algılayıcılar KAA'lara karşı olası herhangi bir saldırıda değişen parametreler ve varyasyonlar göstererek güvenlik sağlamaktadırlar. Şüpheli bir durumla karşılaştığında protokol, düğümün fiziksel ve MAC katmanlarını kapatarak, güvenli hale getirmektedirler. Yapılan çalışmalara

göre MLP kullanımında bir düğümün yanlış uyarı vermesi, o düğümün kapatılmasına neden olabilmektedir. Bu nedenle yanlış uyarılar o ağın etkinliğini azaltmaktadır. Farklı saldırı türlerinde ağın yaşam süresi değişmektedir. Bu nedenle uygulanacak simülasyona göre bir enerji modeli oluşturulmalıdır [4].



Şekil 5. MLP yapısı (MLP Structure)

FSMAC [36] protokolü CSMA/CA [37] 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 hizmet engelleme 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. 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 [36].

SPINS protokolü [38], 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 doğrulaman kodu ile verilerin yollayıcıdan gönderildiği halde alıcı tarafından alındığını garanti eder. Veri kimlik doğrulama kodlarında 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 gönderildiğini bilmektedir. Bu da, zayıf bir 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 [38].

TinySec [39], KAA'larda güvenliği sağlamak amacıyla tasarlanmış bir link katmanı protokolüdür. Tamamlanmamış SNEP'in yerine tasarlanan bu protokol, erişim kontrolü, mesaj bütünlüğü ve gizliliğini sağlamaktadır [22]. IEEE 802.11 ve GSM'lerdeki güvenlik açıkları düşünülerek oluşturulmuştur. Klasik güvenlik protokollerinde güvenlikli hale getirmek için 16-32 bayt ek yük oluşmaktadır. Ancak bu durum KAA'ların küçük hafızası, zayıf işlemcisi, kısıtlı enerjisi nedeniyle istenilen bir durum değildir. TinySec güvenliği sağlamak için ortak bir anahtar kullanır. Ayrıca %10'dan az bir enerji, gecikme ve bant genişliği ek yükü eklemektedir [39]. TinySec'in en önemli özelliklerinden biri de kullanım kolaylığı ve şeffaflığıdır [40]. TinySec düşük enerji tüketimi ve hafıza kullanımı sağlarken, güvenlik konusunda istenen performansı gösterememektedir. Ayrıca, tekrarlama saldırılarına karşı koruma girişiminde de bulunmamaktadır. Güvenli bir iletişim için gerekli olan gizlilik, doğrulama ve de mesaj tekrarlama korumasını sağlarken aynı zamanda düşük enerji tüketimi yapamamaktadır [41].

SenSec [44], TinySec'e benzeyen bir link katmanı protokolüdür. TinySec iki farklı modda çalışırken, SenSec tek bir modda çalışmaktadır. TinySec-AE (Authenticated Encryption) modu ile benzer olan şifrelemeli doğrulama modunda çalışır. SenSec ile güvenliği artırıcı ve enerji tüketimini azaltıcı bazı iyileştirmeler yapılmıştır. Ayrıca hesaplamsal ve veri kimlik doğrulama kodu için gerekli olan maliyet azaltılmıştır. Çok-anahtarlamalı mekanizma ile tüm ağ yapısı farklı saldırı türlerine karşı dayanıklı hale gelmiştir. SenSec'deki anahtarlama mekanizması düğüm yakalama saldırılarına karşı kısmi esneklik sağlamaktadır [44].

Tablo 4. Güvenli Ortam Erişim Protokolleri (Secure Medium Access Control Protocols)

PROTOKOLLER	ETKİLİ OLDUĞU SALDIRI TÜRÜ	ÖZELLİKLERİ
ARMAC [35]	DoS Saldırısı	Farklı hizmet saldırılarında, saldırı türünü belirleyerek güvenliği sağlamaktadır. Herhangi bir ek donanıma ihtiyaç duymaz.
MLP'ye Dayalı MAC [4]	DoS Saldırısı	Herhangi bir saldırı anında değişen parametreleri izleyerek, düğüm üzerindeki fiziksel ve MAC katmanlarını kapatarak güvenliği sağlar.
FSMAC [36]	DoS Saldırısı	Merkezi bir kontrol yapısı bulunmayıp, dağıtık yapı gösterir. Her bir düğüm kendi kendini savunabilmektedir.
SPINS [38]	Tekrarlama Saldırısı Gizlice Dinleme Saldırısı	Anlamsal güvenlik ile kulak misafiri olmayı engeller. Gizlilik, bütünlük ve tazelik (freshness) özelliklerini sağlar.
TinySec [39]	Tekrarlama Saldırısı	Kullanım kolaylığı ve şeffaflık sağlar. Ayrıca erişim kontrolü, mesaj bütünlüğü ve gizliliği sağlar.
SenSec [44]	Kaba Kuvvet Saldırısı Tekrarlama Saldırısı	Çoklu anahtarlama mekanizması ile farklı saldırı türlerine dayanıklıdır.
MiniSec [41]	Tekrarlama Saldırısı	Anlamsal güvenlik sağlamaktadır. Ayrıca herhangi bir iletim ek yükü oluşturmaz.
TE_2S [42]	Tekrarlama Saldırısı Sahtecilik Saldırısı Güç Tüketme Saldırısı Uyumayı Engelleme Saldırısı	Herhangi bir ek paket kullanılamaz. Kimlik doğrulama sürecini azaltarak güç tüketme saldırılarının etkilerini azaltır.

MiniSec [41], güvenli bir ağ katmanı protokolüdür. ZigBee [43] gibi yüksek güvenlik seviyesi sağlarken, TinySec'den daha düşük enerji tüketmektedir [41]. Blok şifreleme modu olarak OCB (Offset Codebook) modunu kullanmaktadır [40]. MiniSec'de iki farklı işlem modu bulunmaktadır. Bunlar, tek yönlü paket yayını yapan MiniSec-U ve geniş paket yayını yapan MiniSec-B'dir [40]. İki işlem modu da anlamsal güvenliği sağlamaktadır. MiniSec-B işlem modunda ayrıca tekrarlama saldırılarına karşı da korunma sağlanmaktadır [44]. Ayrıca, herhangi bir iletim ek yükü de oluşmamaktadır [22].

TE_2S [42], çapraz-katmanlı güvenli şekil tasarımının MAC protokollerine entegrasyonudur. KAA'ları uyumayı engelleme gibi saldırılara karşı korumak için tasarlanmıştır. İki katmanlı güvenli iletim şeması 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 azalmaktadır. Böylece güç tüketme saldırılarının etkisi de azalmaktadır. Enerji analizine bakıldığında etkinlik sağlandığı gözlemlenmiştir. Ayrıca tekrarlama ve sahtecilik saldırılarına karşı da enerji etkin bir şekilde karşı koyabilmektedir. Tablo 4, güvenli MAC protokollerini özetlemektedir.

4. SONUÇ VE ÖNERİLER (RESULT AND SUGGESTIONS)

Bu çalışmada KAA'lardaki MAC protokolleri enerji etkinliği, hareketlilik ve güvenlik açısından karşılaştırmalı olarak incelenmiş ve özetlenmiştir. Bu alanda yeni çalışmaya başlayacak araştırmacılar için her alt başlık alandaki eksiklikleri listelemiştir. KAA'ların fiziksel özelliklerinden dolayı MAC protokolleri tasarlanırken üzerinde durulan başlıca konulardan biri enerji verimliliğini sağlamaktır. Enerji verimliliği sağlanarak düğümlerin, böylece ağın ömrü uzamaktadır. Bu çalışmada enerji tüketimine sebep olan bazı faktörler incelenmiş ve bunlar engellenmeye çalışılarak enerji tüketimi de azaltılmıştır. Bazı protokollerde enerji verimliliği sağlanırken gecikme, maliyet gibi istenmeyen artışlar meydana gelmektedir. Tablo 1'de enerji etkinliğini sağlamaya yönelik MAC protokollerinin enerji tüketimine sebep olan boşken dinleme, çakışma, gecikme ve ek yük gibi faktörleri ne şekilde etkilediği incelenmektedir. İlgili protokoller incelendiğinde enerji tüketimi açısından söz konusu faktörler arasında bir ödünleşim olduğu görülmektedir. Ağda enerji etkinliği sağlanırken genel olarak boşken dinleme ve çakışmada azalma görüldüğü, buna karşın bazı protokollerde gecikme ve ek yükte artış olduğu tespit edilmiştir.

Yakın zamanlı yapılan çalışmalarda sadece enerji etkinliği değil, hareketlilik ve güvenlik üzerinde de durulduğu gözlemlenmiştir. Hareketlilik ile dinamik yapıdaki ağ üzerinde enerji tüketiminin artmasının

önüne geçilmeye çalışılmıştır. Tablo 3'de hareketliliğin enerji etkinliğine etkisi ve bu protokollerin avantaj ve dezavantajları özetlenmiştir. Hareketlilik odaklı protokoller hizmet kalitesi ve dinamik ağ topolojisi yönetiminde iyileşme sağlarken; enerji kaybı ve konum bilgisi ihtiyacı gibi dezavantajlara sahiptirler.

Güvenlik odaklı yapılan çalışmalarda ise saldırı etkinliği düşürülerek, güvenli bir veri iletişimi gerçekleştirilmeye çalışılmıştır. Böylece, ağın yaşam süresini de artırmak hedeflenmiştir. Tablo 4 güvenlik amaçlı MAC protokollerini özetlemektedir. Buna göre güvenlik odaklı MAC protokolleri sahip oldukları farklı özellikler ile DoS saldırıları, tekrarlama saldırıları, gizlice dinleme saldırıları, kaba kuvvet saldırıları, sahtecilik saldırıları, güç tüketme saldırıları ve uyumayı engelleme saldırıları gibi çok çeşitli saldırı türlerinde etkin olabilmektedir. Bazı protokoller saldırı anında değişen parametreler gösterirken, bazı protokoller kullandıkları çoklu anahtarlama mekanizması ile saldırılara karşı dayanıklılık sağlar. Ayrıca anlamsal güvenlik ile gizlice dinleme saldırıları engellenirken, kimlik doğrulama süreci azaltılarak güç tüketme saldırılarının da etkileri azaltılmaktadır.

Sonuç olarak, KAA'lar için geliştirilen MAC protokolleri önemli konulardan biri olup halen gelişmeye açık olduğu görülmektedir. Güvenlik ve hareketlilik konularında yapılan çalışmaların henüz tam olarak istenen seviyeye gelmediği birçok çalışmada ortaya konmuştur. Ayrıca sağlanmaya çalışılan faktörlerden birinin iyileştirilmeye çalışılması diğer bir faktörün olumsuz etkilenmesine neden olabilmektedir. Örneğin, enerji etkinliği sağlanmaya çalışılan bazı protokollerde gecikmeler meydana geldiği gözlemlenmiştir. Benzer şekilde hareketlilik üzerine geliştirilen bazı protokoller de ise enerji verimliliği düşüktür. Bunun gibi geliştirilen bir faktör ile diğer olumsuz faktörlerin açığa çıkmasının önüne geçilmelidir. Üzerinde durulması gereken bir konuda yapılan çalışmaların çoğunlukla benzetim çalışması üzerinde yapılmış ve gerçek ortam üzerindeki etkinliklerin denenmemiş olmasıdır. Protokollerin benzetim çalışmalarındaki performansı gerçek ortamlarda da benzer şekilde gerçekleştirecekleri varsayılmıştır. Ancak gerçek ortamlarda bazı hesaba katılmayan faktörler olabilmektedir. Gerçek ortamlarda yapılacak çalışmalar, geliştirilen bu protokollerin asıl çalışma performanslarını sunacaktır. Ayrıca enerji etkinliğini hedefleyen MAC protokolü sayısının güvenliliği ve hareketliliği hedefleyen MAC protokolü sayısından oldukça fazla olduğu görülmüştür. Bu bağlamda güvenlik ve hareketlilik odaklı MAC protokolleri üzerine yapılan çalışmaların artırılması beklenmektedir.

5. KAYNAKLAR (REFERENCES)

1. Misra, S., Vaish, A., "Reputation-based role assignment for role-based access control in wireless sensor networks", **Computer Communications,** Cilt 34, 281–294, 2011.
2. Yick, J., Mukherjee, B., Ghosal, D., "Wireless sensor network survey", **Computer Networks,** Cilt 52, 2292–2330, 2008.
3. Sabbah, E., Kang, K. D., "Guide to Wireless Sensor Network", **Springer London,** 489-490 2009.
4. Kulkarni, R.V., Venayagamoorth, G. K., "Neural Network Based Secure Media Access Control Protocol for Wireless Sensor Network", **Proceedings of International Joint Conference on Neural Networks**, 14-19, 2009.
5. Cano, C., Bellalta, B., Sfairopoulou, A., Oliver, M., "Low energy operation in WSNs: A survey of preamble sampling MAC protocols", **Computer Networks**, Cilt 55, 3351-3363, 2011.
6. Demirkol, I., Ersoy, C., Alagoz, F., "Mac protocols for wireless sensor networks: a survey", **IEEE Communications Magazine**, Cilt 44, No 4, 115–121, 2006.
7. Ye, W., Heidemann, J., Estrin, D., "An Energy-Efficient MAC Protocol for Wireless Sensor Networks", **IEEE INFOCOM**, Cilt 2, 1567-1576, 2002.
8. Ali, M., Suleman, T., ve Uzmi, Z. A., "MMAC: A Mobility-Adaptive, Collision-Free MAC Protocol for Wireless Sensor Networks", **Proceedings 24th IEEE IPCCC'05**, 401-407, 2005.
9. Dener M., Bay, Ö. F., "Medium Access Control Protocols For Wireless Sensor Networks: Literature Survey", **G U J Sci**, Cilt 25, No 2, 455-464,2012.
10. Solehria, S. F., Jadoon, S., "Medium Access Control Protocol for Wireless Sensor Networks: a Survey", **IJVIPNS-IJENS**, Cilt 11, No 3, 16-21, 2011.
11. Gunn, M., Koo, S. G. K., "A Comparative Study of Medium Access Control Protocols for Wireless Sensor Networks", **IJCNS**, 695-703, 2009.
12. Yadav, R., Varma, S., Malaviya, N., "A Survey of Mac Protocols For Wireless Sensor Networks", **UbiCC Journal**, Cilt 4, No 3, 827-833, 2009.
13. Kurose, J. F., Ross, K. W., "Computer Networking: A Top-Down Approach Featuring the Internet", **Addison Wesley,** 2005.
14. Ray, S., Demirkol, I., Heinzelman, W., "ADV-MAC: Analysis and optimization of energy efficiency through data advertisements for wireless sensor networks", **Ad Hoc Networks,** Cilt 9, 876-892, 2011.
15. IEEE, IEEE Standard 802.11, Wireless LAN Medium Access Control (MAC) and Physical

Layer (PHY) Specifications, **LAN MAN Standards Committee of the IEEE Computer Society**, 1999.

16. Ali, M., Saif, U., Dunkels, A., Voigt, T., Römer, K., Langendoen, K., Polastre, J., Uzmi, Z. A., "Medium access control issues in sensor networks", **ACM SIGCOMM,** Cilt 3, 3-36, 2006.

17. Kuntz, R., Gallais, A., Noel, T., "From versatility to auto-adaptation of the medium access control in wireless sensor networks", **Journal of Parallel and Distributed Computing**, Cilt 71, 1236-1248, 2011.

18. Pham, H., Jha, S., "Addressing mobility in wireless sensor media access control protocol", **Networks and Information Processing,** 113-118, 2004.

19. Sohrabi, K., Gao, J., Ailawadhi, V., Pottie, G.J., "Protocols for self-organization of a wireless sensor network", **IEEE Personal Communications**, Cilt 7, No 5, 16–27, 2000.

20. Tilak, S., Abu-Ghazaleh, N., Heinzelman, W., "A taxonomy of wireless micro-sensor network models", **ACM Mobile Computing and Communications Review,** Cilt 6, No 2, 28–36, 2002.

21. Giordano, V., Ballal, P., Lewis, F., Turchiano, B., Zhang, J. B., "Supervisory Control of Mobile Sensor Networks: Math Formulation, Simulation, and Implementation", **IEEE Transactions On Systems, Man, And Cybernetics—Part B: Cybernetics,** Cilt 36, No 4, 806-819, 2006.

22. Boyle, D., Newe, T., "Securing Wireless Sensor Networks: Security Architectures", **Journal of Networks**, Cilt 3, No 1, 65-77, 2008.

23. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., Cayirci, E., "A survey on sensor Networks", **IEEE Communications Magazine,** Cilt 40, No 8, 102-114, 2002.

24. Ng, H. S., Sim, M. L., Tan, C. M., "Security issues of wireless sensor networks in healthcare applications", **BT Technology Journal**, Cilt 24, No 2, 138–144, 2006.

25. IEEE, 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, **IEEE Standard,** 1999.

26. Kim, J., Park, K. H., "An energy-efficient, transport-controlled MAC protocol for wireless sensor networks", **Computer Networks,** Cilt 53, No 11, 1879-1902, 2009.

27. Dam, T., Langendoen, K., "An adaptive energy-efficient MAC protocol for wireless sensor networks", **International Conference on Embedded Networked Sensor Systems**, 171-180, 2003.

28. Rajendran, V., Obraczka, K., Garcia-Luna-Aceves, J., "Energy-efficient, collision-free medium access control for wireless sensor networks", **Proceedings of the International Conference on Embedded Networked Sensor Systems (SenSys)**, 181–192, 2003.

29. Enz, C. C., El-Hoiydi, A., Decotignie, J-D., Peiris, V., "WiseNET: An Ultralow-Power Wireless Sensor Network Solution", **IEEE Computer**, Cilt 37, No 8, 62-70, 2004.

30. El-Hoiydi, A., "Spatial TDMA and CSMA with preamble sampling for low power ad hoc wireless sensor networks", **Proceedings of ISCC 2002, Seventh International Symposium on Computers and Communications**, 685 – 692, 2002.

31. Polastre, J., Hill, J., Culler, D., "Versatile low Power Media Access for Wireless Sensor Networks", **Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems (SenSys'04)**, 95-107, 2004.

32. El-Hoiydi, A., "Aloha with Preamble Sampling for Sporadic Traffic in Ad-hoc Wireless Sensor Networks", **IEEE International Conference on Communications,** 2002.

33. Jose, A. V., Khanna, N., Krishna, A. K., "Advanced Sensor MAC protocol to support applications having different priority levels in Wireless Sensor Networks", **6th International ICST Conference on Communications and Networking**, 340- 343, 2011.

34. Gong, H., Liu, M., Mao, Y., Chen, L., Xie, L., "Traffic Adaptive MAC Protocol for Wireless Sensor Networks", **In Proceedings of ICCNMC'05**, 1134-1143, 2005.

35. Çakıroğlu, M., Özcerit, A.T., "Kablosuz Algılayıcı Ağlarda Hizmet Engelleme Saldırılarına Dayanıklı Ortam Erişim Protokolü Tasarımı", **Gazi Üniv. Müh. Mim. Fak. Der.,** Cilt 22, No 4, 697-707, 2007.

36. Ren, Q., Liang, Q., "Fuzzy Logic-Optimized Secure Media Access Control (FSMAC) Protocol for Wireless Sensor Networks", **IEEE Computational Intelligence for Homeland Security and Personal Safety**, 37-43, 2005

37. Kleinrock, L., Tobagi, F. A., "Packet switching in radio channels: Part I—Carrier sense multiple-access modes and their throughput-delay characteristics", **IEEE Transactions on Communications,** Cilt 23, No 12, 1400–1416, 1975.

38. Perrig A., Szewczyk, R., Wen, V., Culler, D., Tygar, J. D., "SPINS: Security Protocols for Sensor Networks", **Wireless Networks,** Cilt 8, 521-534, 2002.

39. Karlof, C., Sastry, N., ve Wagner, D., "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", **In Second ACM Conference on Embedded Networked Sensor Systems**, 162-175, 2004.

40. Sultana, N., Ahmed, T., Hossain, S., "Study of a new link layer Security scheme in a wireless sensor network", **AIUB Journal of Science and**

Engineering (AJSE), Cilt 10, No 1, 79-86, 2011.

41. Luk, M., Mezzour, G., Perrig, A., Gligor. V., "MiniSec: Secure Sensor Network Communication architecture", **In Proc. of the 6th Int'l Conf. on Information Processinng in Sensor Networks**, 479-488, 2007.

42. Hsueh, C. T., Wen, C. Y., Ouyang, Y. C., "A Secure scheme for power exhausting attacks in wireless sensor networks", **Ubiquitous and Future Networks (ICUFN), 2011 Third International Conference on**, Cilt 15, No 17, 258-263, 2011.

43. ZigBee Alliance. Zigbee specication. Technical Report Document 053474r06, Version 1.0**, ZigBee Alliance**, 2005.

44. Krontiris, I., Dimitriou T., Soroush, H., Salajeghe, M., "WSN Link-layer Security Frameworks" **Athens I.**