Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 22, No 4, 697-707, 2007

J. Fac. Eng. Arch. Gazi Univ.
Vol 22, No 4, 697-707, 2007

KABLOSUZ ALGILAYICI AĞLARDA HİZMET ENGELLEME SALDIRILARINA DAYANIKLI ORTAM ERİŞİM PROTOKOLÜ TASARIMI

Murat ÇAKIROĞLU ve A. Turan ÖZCERİT
Elektronik – Bilgisayar Eğitimi Bölümü, Teknik Eğitim Fakültesi, Sakarya Üniversitesi, 54187, Sakarya
muratc@sakarya.edu.tr, aozcerit@sakarya.edu.tr

(Geliş/Received: 14.08.2006; Kabul/Accepted: 31.10.2007)

ÖZET

Kablosuz algılayıcı ağları, kendi başlarına çalışabilmeleri, ekstra bakım gerektirmemeleri ve çok çeşitli uygulamalarda kullanılabilmeleri sebebiyle hem endüstriyel hem de akademik çalışma alanlarında çok popüler bir konu haline gelmiştir. Bununla birlikte, algılayıcı düğümlerinin sınırlı donanımsal kaynaklara ve güç birimlerine sahip olması bazı çözüm bekleyen güvenlik açıklarına neden olmaktadır. Ortam erişim protokolünün açıklarından faydalanarak düğümlerin iletişimlerinin kesilmesine ya da anormal durumların oluşmasına ve böylece ağ ömrünün kısalmasına sebep olan hizmet engelleme (Denial of Service-DoS) saldırıları, kablosuz algılayıcı ağ güvenliği için önemli bir tehdit unsuru oluşturmaktadır. Kablosuz algılayıcı ağları için tasarlanan ortam erişim protokolleri arasında en yaygın olarak bilinen S-MAC (Sensor Medium Access Control – Algılayıcı Ortam Erişim Kontrolü) ve türevleri (T-MAC [1], D-MAC [2] v.b) bu tür saldırılara karşı savunmasızdır. Bu çalışmada, farklı DoS saldırgan türlerini tespit ederek saldırgan türüne göre uygun çözümün uygulanmasını sağlayan AR-MAC (Attack Resistant MAC - Saldırıya dayanıklı MAC) protokolünün tasarımı gerçekleştirilmiştir. Tasarlanan yeni protokol sayesinde herhangi bir ek donanıma ihtiyaç duyulmadan kablosuz algılayıcı ağları ortam erişim katmanındaki DoS saldırılarına karşı daha güvenli hale getirilerek düğümlerin yaşam süreleri uzatılmıştır.

Anahtar Kelimler: Kablosuz algılayıcı ağları, hizmet engelleme saldırıları, ortam erişim kontrolü, güvenlik, DoS, MAC.

DENIAL OF SERVICE ATTACK RESISTANT MAC PROTOCOL DESIGN FOR WIRELESS SENSOR NETWORKS

ABSTRACT

Wireless Sensor Networks (WSN) are very popular area of interest both in academic studies and industrial applications since they can work individually without additional maintenance and can be deployed in diverse applications. However, the limited source of the nodes cannot guarantee a sufficient level of security and also complicates the design and the implementation of the algorithms/protocols. DoS (Denial of Service) attacks that manipulate vulnerabilities of access protocol by disrupting network communication or arising exceptional cases and cutting network's lifetime are primary threats for wireless sensor networks. S-MAC (Sensor Medium Access Control) and its derivatives (T-MAC [1], D-MAC [2] etc.) which, are the most common medium access protocols designed for WSNs, are vulnerable against such attacks. In this paper, we have implemented the design of the AR-MAC (Attack Resistant MAC) protocol that detects the types of jammers and maintains the appropriate solution for each jammer type. By means of the new MAC protocol designed, the WSNs have been more robust to DoS attacks in MAC layer and the lifetime of the nodes have been extended under such attacks without additional hardware.

Keywords: Wireless sensor networks, WSN, denial of service attack, medium access control, security, DoS, MAC.

1. GİRİŞ (INTRODUCTION)

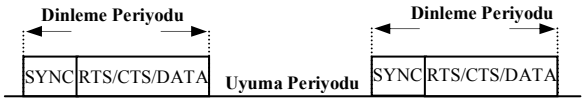
Kablosuz algılayıcı ağları, sınırlı kapasiteye sahip, kısa mesafede kablosuz ortam üzerinden haberleşebilen düşük güçlü ve düşük maliyetli algılayıcı düğümlerinden meydana gelmektedir [3]. Gözlem yapılacak ortama rasgele dağıtılabilen bu düğümler, birbirlerini tanıyabilmekte ve ortak gayret sarf ederek geniş bir alanda ölçüm vazifesini gerçekleştirebilmektedir. Bu özelliklerinden dolayı sağlık alanlarından askeri alanlara, bir binanın güvenliğinin sağlanmasından orman yangınlarının önceden tespitine kadar çok çeşitli alanlarda kullanılabilmektedirler.

Algılayıcı düğümlerinin sınırlı işlem yapabilme kabiliyetine sahip olması, çoğu senaryo için yenilenemez güç kaynakları ile beslenmeleri ve kablosuz ortam üzerinden haberleşmeleri sebebiyle kablosuz algılayıcı ağları diğer ağlara nazaran bazı saldırı türlerine karşı daha savunmasızdır. Bozma türündeki hizmet engelleme (Jamming Style DoS) saldırıları, fiziksel katmanı ve ortam erişim katmanını etkileyerek tüm ağın ya da belirli düğümlerin iletişimlerinin kesilmesine sebep olan saldırı türlerinden birisidir [4]. Bu tip saldırılarda, saldırgan düğümler radyo sinyalleri ile bozma paketleri göndererek, ortam erişim katmanının fonksiyonlarını aksatabilir veya sürekli bozma sinyali göndererek dost düğümlerin iletişimlerini engelleyebilir. Kriptografik yöntemlerin tam olarak çözüm üretemediği [4,5] bu saldırılara karşı kullanılan en etkin yöntemler; frekans atlama ve kod bölmeli çoğullama teknikleridir [6,7]. Fakat günümüz algılayıcı düğümlerinin güç sınırlamaları sebebiyle donanımsal olarak bu teknikleri desteklememelerinden dolayı bahsedilen yöntemlerin kablosuz algılayıcı ağlarında kullanılması güçleşmektedir. Bu çalışmada, yukarıda değinilen problemlerin aşılabilmesi için kullanılabilecek savunma yöntemlerinin geliştirilmesi üzerine odaklanılmıştır.

Makale'nin geri kalan kısımları ise şu şekilde düzenlenmiştir: Bölüm-2'de MAC protokolleri ile ilgili temel bilgiler açıklanmış, 3. bölümde ortam erişim katmanını etkileyen hizmet engelleme saldırı türleri ile ilgili bilgi verilmiştir. Bölüm-4'de saldırı senaryoları ve çözüm yöntemlerini gerçekleştirmek için kullanılan simülasyon parametre kabulleri ve detayları açıklanarak Bölüm-5'te saldırılara karşı dayanıklı olarak tasarlanan AR-MAC protokolünün detayları özetlenmiştir. Bölüm-6'da elde edilen simülasyon sonuçlarının sunulmasını takiben Bölüm-7'de çalışmadan elde edilen sonuçlar irdelenmiştir.

2. ORTAM ERİŞİM PROTOKOLLERİ (MEDIUM ACCESS PROTOCOLS)

Ortam erişim protokolü, paylaşımlı olan iletişim ortamının amaca uygun bir biçimde kullanılmasını sağlayan kurallar bütünüdür. Literatürde kablosuz



Şekil 1. S-MAC

ağlarda kullanılmak üzere çeşitli ortam erişim protokolleri sunulmuştur, ancak sunulan protokoller geleneksel kablosuz ağlar için tasarlandığından kablosuz algılayıcı ağlarında doğrudan kullanması mümkün değildir [3,8]. Uygulama alanlarının çok çeşitli olması sebebiyle, kablosuz algılayıcı ağlarda tüm uygulamaları kapsayabilecek şekilde bir ortam erişim standardı geliştirilmemiştir. Bu çalışmada, yapısı sebebiyle hizmet engelleme saldırılarına daha yatkın olan çekişme temelli (contention-based) ve dilim tabanlı (slotted-based) protokoller üzerinde çalışılmıştır.

Kablosuz algılayıcı ağları için geliştirilmiş olan çekişme temelli ortam erişim protokollerinin çoğu IEEE 802.11 standardından esinlenmiştir. IEEE 802.11 protokolünde gönderim yapmak isteyen düğüm, ortamı kısa bir süre dinler ve eğer herhangi bir iletişim algılamazsa kanalın boş olduğunu varsayarak gönderime başlar [9]. Bunun dışında 802.11 çarpışmadan kaçınmak için dört yönlü tokalaşma yöntemini kullanılır. Tokalaşmada ilk olarak gönderim yapmak isteyen düğüm isteğini diğer düğümlere duyurmak için RTS (Request to Send) paketini gönderir. Alıcı düğüm CTS (Clear to Send) paketi ile gelen trafiği kabul ettiğini duyurduktan sonra veri paketi iletilebilir. 802.11'de düğümler ortam erişim hakkını elde etmek için diğer düğümlerle çekişmek zorundadır. Çekişmeyi kaybeden düğümün beklemesi ve erişimi kazanmak için bir daha denemesi gerekmektedir. Kurallar kesin ve her düğüm için geçerlidir. Ancak kurallara uymayan bir düğüm düzenin bozulmasına sebep olabilir ve ortam erişim hakkının adil dağıtılmasını engelleyebilir. Örneğin ortam erişimini ele geçiren bir saldırgan düğüm, sürekli ortamı meşgul edebilir ve bu sayede diğer düğümlerin ortama erişmesini ve dolayısıyla iletişim yapmasını engelleyebilir.

S-MAC, kablosuz algılayıcı ağları için tasarlanmış olan ortam erişim protokollerinin en popüler olanıdır ve 802.11 protokolünden esinlenmiştir. 802.11'den en büyük farkı ise gereksiz güç tüketimine sebep olan ortamın sürekli dinlenmesi yerine periyodik dinleme/uyuma zamanlamasını kullanmasıdır. Güç tüketimini en az indirmek için de periyodik dinleme/uyumayla birlikte, çarpışmadan kaçınma, istem dışı alımı engelleme ve mesaj geçişi yöntemlerini kullanmaktadır [10]. Şekil-1'de S-MAC'in zamanlama diyagramı görülmektedir.

S-MAC protokolü ve türevleri (T-MAC), 802.11 gibi çarpışmayı engellemek için RTS-CTS sinyalleşmesini kullanır ve düğümler ortam erişimi için çekişirler.

Dolayısıyla 802.11 protokolü gibi ortam erişimini bozan saldırılara karşı savunmasızdır.

3. HİZMET ENGELLEME SALDIRILARI (DENIAL OF SERVICE ATTACKS)

Kablosuz algılayıcı ağlarındaki düğümler birçok durumda uzaktan gözlemlenecek ortama rasgele yerleştirilmektedirler. Böylelikle ortamda korunmasız olarak bulunan düğümler, kötü niyetli kişiler tarafından kolaylıkla ele geçirilebilir ve fiziksel hasara maruz bırakılabilir. Ayrıca yeniden programlanarak saldırgan düğümler haline de çevrilebilirler. Bu gibi unsurlar sebebiyle, algılayıcı ağlar diğer ağlara nazaran güvenlik açısından çok daha fazla risklere sahiptirler [4,5].

Bozma (jamming) türündeki hizmet engelleme saldırıları kablosuz algılayıcı ağlarında fiziksel ve ortam erişim olmak üzere iki katmanı etkilemektedir. İletişim kanal frekansına eş frekansta bir dalganın yayılması ile gerçekleştirilen hizmet engelleme saldırısı fiziksel katmanı etkisiz hale getirmektedir. Ortam erişimlerindeki hizmet engelleme saldırıları ise erişim kurallarının dışına çıkarak anormal sayıda paket göndermek suretiyle ortam erişim protokolünü etkisiz hale getirir. Saldırgan düğümlerin de normal düğümler gibi sınırlı güç kaynaklarına sahip olduğu düşünülürse, daha fazla enerji tüketimine sebep olan fiziksel katman saldırılarını kullanmak yerine MAC katmanın açıklarından faydalanarak saldırıda bulunmak çok daha verimli bir yöntemdir [11,12].

3.1 Saldırgan Türleri (Jammer Types)

Literatürde çekişme temelli ortam erişim protokolleri için beş farklı saldırgan türü tanımlanmıştır. Xu ve diğerleri [4], sürekli (constant), aldatıcı (deceptive), rasgele (random) ve reaktif (rective) olmak üzere dört farklı tür tanımlarken, Law ve diğerleri [12] çekişme temelli MAC protokolleri (S-MAC, T-MAC v.b.) için periyodik küme tabanlı saldırgan (periodic cluster based jammer) modeli geliştirmiştir.

a) **Sürekli Saldırgan (Constant Jammer):** Sürekli olarak iletişim kanalına rasgele uzunlukta paketler gönderir. Gönderim yapmak için ortamın boş olmasını beklemez. Paylaşımlı olan iletim kanalını sürekli olarak meşgul ettiği için diğer düğümlerin iletişimlerini tamamen kesebilir ancak sürekli saldırdığı için güç tüketimi açısından verimli değildir.

b) **Aldatıcı saldırgan (Deceptive Jammer):** Sürekli olarak rasgele bit göndermek yerine, MAC katmanında karşılığı olan yasal paketleri çok sık aralıklarla veya beklemeksizin ortama gönderir. Böylelikle dost düğümler, gelen paketleri almak için sürekli olarak alıcılarını açık tutarlar. Aldatıcı saldırgan da sürekli saldırgan gibi aralıksız saldırdığı için enerji kullanımı açısından verimli değildir. Fakat iletim kanalını ve normal düğümleri sürekli meşgul ettiği için düğümler arası iletişimin kesilmesine sebep olur.

c) **Reaktif saldırgan (Reactive Jammer):** Ortamı dinler, eğer iletim kanalı boşsa saldırmaz ancak herhangi bir iletişim olduğunu sezerse (geçerli bir öntakı aldığında) saldırmaya başlar. Böylece gönderilen paketlerin başarı ile alınmasını engeller. Ortamı sürekli dinlemesi sebebiyle reaktif saldırgan da diğer iki saldırgan gibi güç kullanımı açısından verimli değildir.

d) **Rasgele saldırgan (Random Jammer):** Rasgele zaman dilimlerinde saldırır ve uyur. Saldırdığı zaman dilimlerinde sürekli veya aldatıcı saldırgan gibi davranabilir. Rasgele saldırı tekniği diğer üç yöntem kadar etkili olmamakla birlikte sınırlı güç kaynağına sahip saldırgan türleri için daha elverişli bir yöntemdir.

e) **Periyodik Küme Saldırganı (Periodic Cluster Based Jammer):** Enerji korunumu açısından rasgele saldırgana, etkinlik açısından ise reaktif saldırgana benzemektedir. Saldırgan düğüm ilk olarak bulunduğu ortamdaki kümelerin iletişimlerini izler ve kümelerdeki veri paketlerinin varış süreleri, ortalama paket sayıları gibi değerlerin istatistiğini tutar. Paketler şifrelenmiş olsa bile paket boyutlarından veri paketlerini ayırabilir (veri paketleri kontrol paketlerine göre daha büyüktür). Elde ettiği istatistiksel bilgilere göre düğümler veri paketi gönderdiğinde saldırır ve diğer zamanlarda uyur. Enerji kullanımı açısından diğer saldırganlara göre daha verimlidir.

4. SİMÜLASYONDA KULLANILAN PARAMETRE KABULLERİ (SIMULATION ASSUMPTIONS)

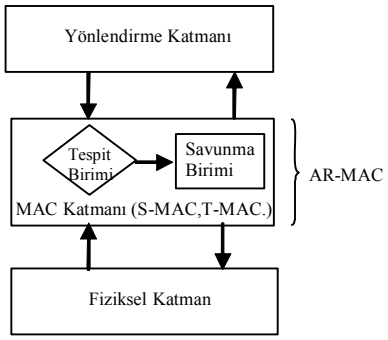
Hizmet engelleme saldırı türleri ve bu saldırılara karşı geliştirilen savunma yöntemleri ayrık olay tabanlı OMNET++ [13] simülatöründe gerçeklenmiştir. 100 adet dost düğüm ile birlikte 10 adet saldırgan düğüm 500m x 500m büyüklüğündeki bölgeye rasgele dağıtılmış ve 1 adet çıkış düğümü de merkeze yerleştirilmiştir. Dost düğümler ile saldırgan düğümlerin güç kapasiteleri, güç tüketimleri, radyo iletim mesafeleri eşdeğerdir ve MICA2 [14] düğümlerine uygun olarak seçilmiştir. Her bir düğümün başlangıçta 250mA/saat kapasitelik bir bataryaya sahip olduğu varsayılmıştır. Simülasyonlarda 1 paket / 5 saniye olmak üzere sabit trafik hızı kullanılmıştır ve düğümler en kısa yol algoritması ile çıkış düğümünün yolunu bulmaktadırlar. MAC katmanı için %10 görev çevrimine (93 msn dinleme, 930 msn de uyuma) sahip S-MAC [10] protokolü kullanılmıştır. Tablo 1'de simülasyon ayarlarının özeti verilmektedir.

Tablo 1. Simülasyon Ayarları

Alan	500 x 500 m^2
Topoloji	Rasgele yerleşim
Normal düğüm	100 adet
Saldırgan düğüm	10 adet
Çıkış düğümü	1 adet
İletim mesafesi	100 m
Taşıyıcı sezme	200 m
Başlangıç enerjisi	250 ma/saat
Uygulama Katmanı	CBR= 0.2 paket/sn
Yönlendirme katmanı	En kısa yol lgoritması
MAC protokolü	S-MAC (93/930 msn)
Kontrol Paketi	10 Bayt
Veri Paketi	40 Bayt

5. SALDIRIYA DAYANIKLI ORTAM ERİŞİM (AR-MAC) PROTOKOL TASARIMI (THE DESIGN OF ATTACK RESISTANT MAC PROTOCOL)

Saldırıya dayanıklı ortam erişim (AR-MAC) protokolünün blok diyagramı Şekil-2'de görülmektedir. AR-MAC, S-MAC ve T-MAC gibi çekişme temelli bir ortam erişim protokolüne, "saldırı tespit birimi" ile "savunma biriminin" eklenmesinden meydana gelmektedir.



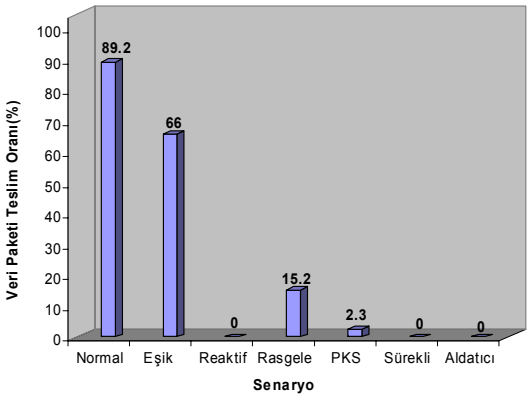
Şekil 2. AR-MAC protokolü (AR-MAC protocol)

5.1 Saldırı Tespit Birimi (Attack Detection Unit)

Saldırı tespit birimi fiziksel ve MAC katmanından gelen istatistiksel bilgilere göre düğümün saldırıya uğrayıp uğramadığına karar verir. Ayrıca düğümün hangi saldırı türüne maruz kaldığını savunma birimine bildirir. Bu birimde saldırıları tespit etmek için Xu ve diğerlerinin geliştirdiği yöntemden [4] faydalanılmıştır. Saldırı türünü tespit etmek için ise paket gönderim oranı ve hatalı çerçeve oranları arasındaki ilişkilerden yararlanılarak yeni bir yöntem geliştirilmiştir.

5.1.1 Saldırıların Tespiti (Detection of Attacks)

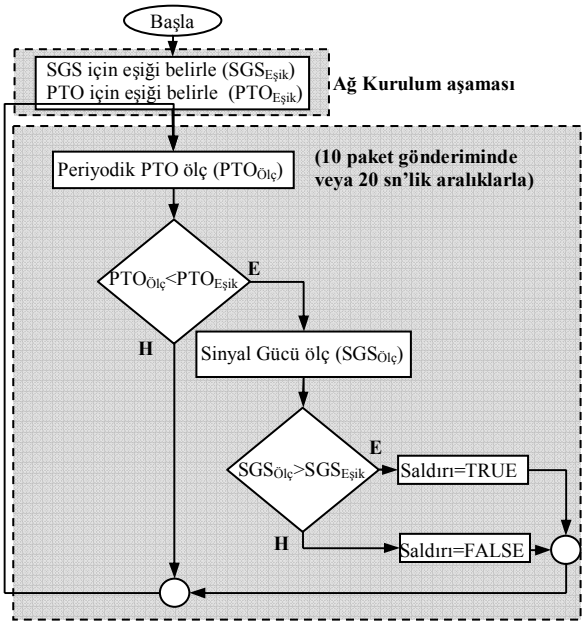
Düğümler saldırı tespitini paket teslim oranları ile ortamdan alınan sinyal güç seviyelerinin tutarlılığına bakarak gerçekleştirirler. Paket teslim oranı bir düğümün göndermiş olduğu veri paketlerinin hangi oranda alıcılara ulaştırabildiğini, sinyal güç seviyesi



Şekil 3. Farklı senaryolar için bir düğümden elde edilen ortalama paket teslim oranı (Packet delivery ratio means of a node under various scenarios)

ise iletim ortamındaki enerji seviyesini gösterir. Düğümler ağ kurulumu aşamasında periyodik aralıklarla PTO ve SGS değerlerini ölçerek normal durum koşullarındaki PTO ve SGS eşik değerlerini elde ederler. Normalde yüksek SGS değerlerine karşılık yüksek PTO, düşük SGS değerleri için ise düşük PTO değerlerinin elde edilebilmesi gerekmektedir. Ancak bozma saldırıları sebebiyle PTO önemli ölçüde düşerken (PTO << $PTO_{Eşik}$) SGS değerleri yüksek kalmaktadır. Hem PTO hem de SGS'nin eşik değerlerinin altında kalması ise komşu düğümlerdeki sorunların göstergesi olabilir.

On paket gönderiminde bir olmak üzere periyodik olarak ölçülen paket teslim oran ortalamaları Şekil 3'de görülmektedir. Saldırının olmadığı normal koşullarda elde edilen ortalama paket teslim oranları oldukça yüksektir. PTO için eşik değeri ağ kurulumu aşamasında en küçük beş paket teslim oranının ortalaması alınarak %66 bulunmuştur. Reaktif



Şekil 4. DoS saldırılarının tespit edilmesi (Detection of DoS Attacks)

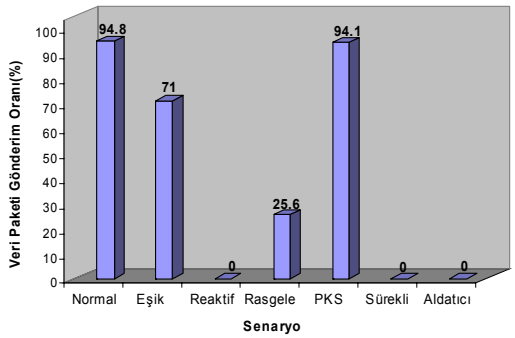
saldırgan gönderilen tüm RTS paketlerini bozduğu, sürekli ve aldatıcı saldırganlar da iletişim kanalını sürekli meşgul ederek veri paketi gönderilmesini engellediği için teslim oranının sıfır çıkmasına sebep olmuşlardır. Rasgele saldırgan ise rasgele zaman dilimlerinde saldırıp diğer zamanlarda uyduğu için bazı paketleri bozabilmektedir. Küme saldırganı düğümlerin iletişim modellerini doğru bir şekilde elde etmesine bağlı olarak veri paketlerinin çoğunun bozulmasını sağlayabilmektedir. Tüm saldırgan durumlarındaki teslim oranlarının eşik değerinin oldukça altına düşmesi saldırı senaryolarının tespitini kolaylaştırmaktadır

Şekil 4'de saldırıları tespit etmek için kullanılan akış diyagramı görülmektedir. Düğümler periyodik olarak ölçtükleri PTO'larını ağ kurulum aşamasında belirlenen eşik değerleri ile karşılaştırırlar. Ölçülen PTO'nun eşik seviyesinin altına inmesi ile sinyal güç seviyesi ölçümü gerçekleştirilir. Eğer PTO eşik değerinin altındaysa ve ölçülen SGS normal koşullarda elde edilen SGS değerinden yüksek ise algoritma saldırı olduğuna karar verir.

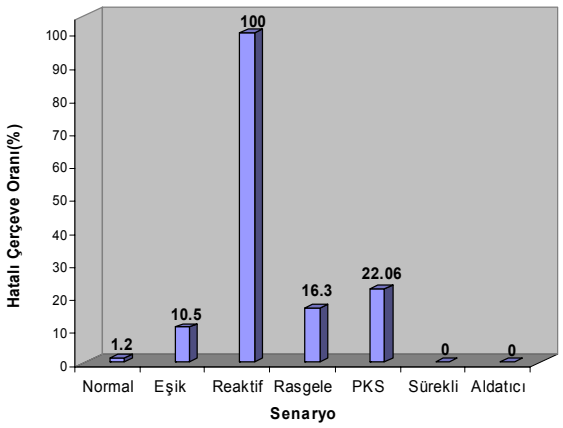
5.1.2 Saldırgan Türünün Tespiti

Saldırının varlığı tespit edildikten sonra uygun olan çözüm yönteminin seçilebilmesi için saldırgan türünün tespit edilmesi gerekmektedir. AR-MAC protokolü saldırgan türünü tespit etmek için paket gönderim oranı (PGO) ve hatalı çerçeve oranı (HÇO) parametrelerinden faydalanmaktadır. PGO bir düğümün veri paket gönderimini hangi oranda gerçekleştirebildiğini gösterirken hatalı çerçeve oranı düğümün aldığı tüm paketlerin hangi oranda bozulduğunu göstermektedir. Aslında HÇO ile PTO birbirini tamamlayan iki parametredir. Aralarındaki temel fark, HÇO'nun alıcı açısından başarıyla alınamayan paket oranını göstermesi iken PTO'nun gönderici açısından başarıyla ulaştırılabilen paket oranını göstermesidir.

Şekil 5'de farklı senaryolar için on paket gönderiminde bir olmak üzere periyodik olarak ölçülen paket gönderim oranlarının ortalamaları

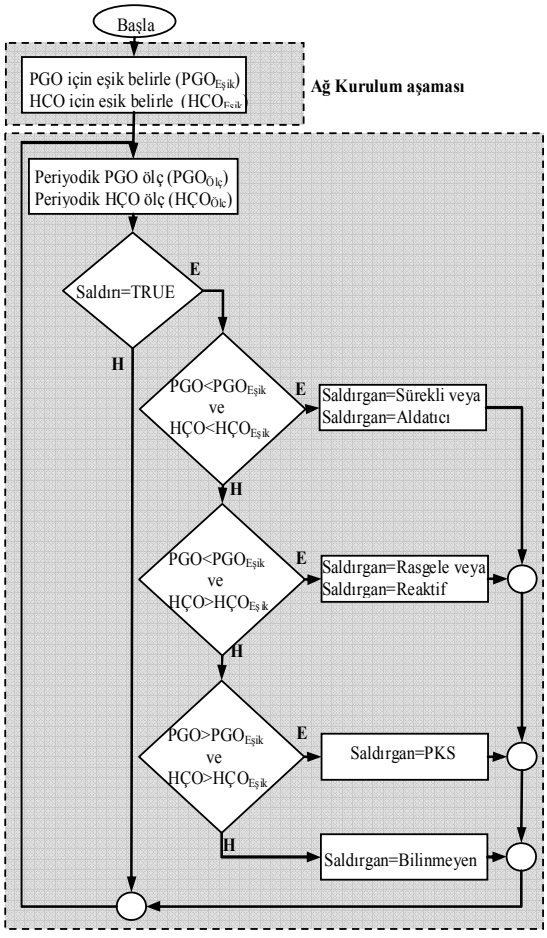


Şekil 5. Farklı senaryolar için bir düğümden elde edilen ortalama paket gönderim oranı (Packet send ratio means of a node under various scenarios)



Şekil 6. Farklı senaryolar için bir düğümden elde edilen ortalama hatalı çerçeve oranı (Bad Frame ratio means of a node under various scenarios)

görülmektedir. Reaktif saldırgan RTS paketlerinin çakışmasına sebep olduğu için veri paketlerinin, sürekli ve aldatıcı saldırganlar ise tüm paketlerin gönderimini engellemektedirler. Rasgele saldırgan aktif olduğu sürelerde RTS veya CTS paketlerinin bozulmasına sebep olarak düğümlerin veri paketlerini göndermesini engelleyebilmektedir. Periyodik küme saldırganı ise veri paketlerinin gönderilmesinden daha



Şekil 7. DoS saldırgan türünün tespit edilmesi (Detection of DoS Jammer types)

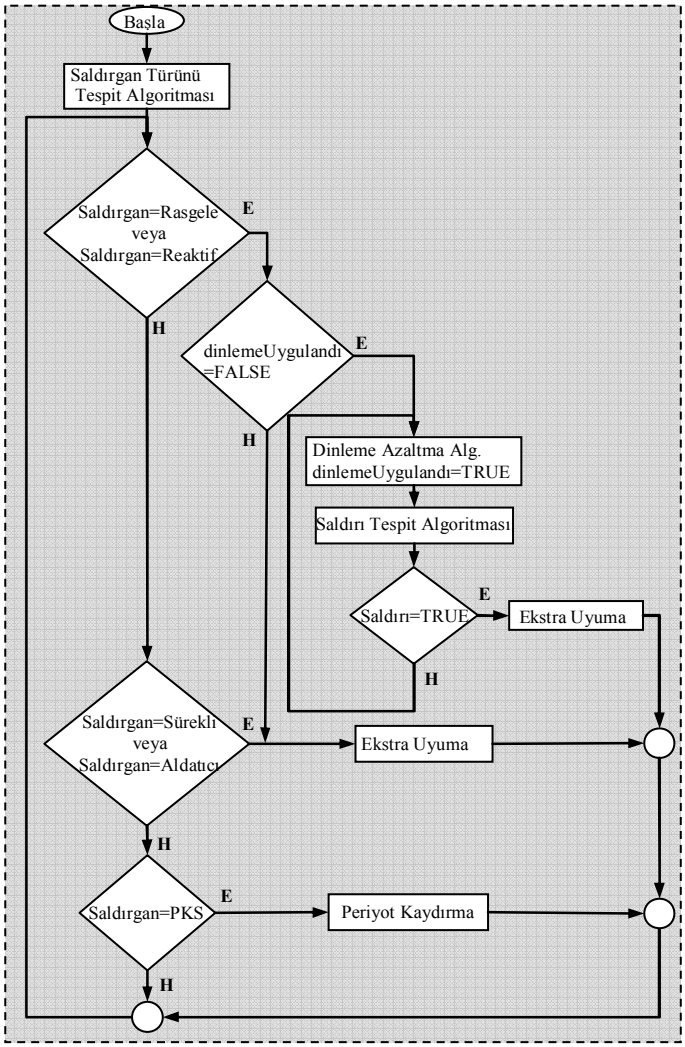
çok bozulmasına sebep olduğu için düğümün paket gönderim oranı normal senaryodaki gibi yüksek çıkmıştır. Sürekli, aldatıcı, reaktif ve rasgele saldırganlar için elde edilen paket gönderim oranları eşik değerlerinin altında iken sadece periyodik küme saldırganı senaryosunda düğümlerin PGO değerleri eşik değerinin üstündedir.

Şekil 6'da farklı senaryolar için on paket alımında bir olmak üzere periyodik olarak ölçülen hatalı çerçeve oranlarının ortalamaları görülmektedir. Reaktif saldırgan, gönderilmiş olan tüm RTS paketlerini bozduğu için düğümlerin aldığı paketlerin tamamının hatalı olmasına sebep olmuştur. Sürekli ve aldatıcı saldırı senaryolarında hiç paket gönderilemediği için düğümlerin aldığı geçerli bir paket yoktur ve bu sebeple hatalı çerçeve oranları sıfırdır. PKS'nin veri paketlerinin çoğunu bozmasına karşın reaktif saldırgan gibi yüksek hatalı çerçeve oranlarına neden olmamasının sebebi, PKS senaryosunda RTS ve CTS paketlerinin bozulmamasıdır. Rasgele saldırgan ise saldırdığı sürelerde paketlerin bozulmasını sağlayarak düğümlerin hatalı çerçeve almalarına sebep olmaktadır. Saldırgan türlerinden sadece sürekli ve aldatıcı saldırganlar eşik değerinin altında hatalı çerçeve oranlarına neden olmaktadır.

Şekil 7'de saldırgan türünü tespit etmek için kullandığımız akış diyagramı görülmektedir. Düğümler periyodik olarak ölçtükleri PGO ve HÇO değerlerini ağ kurulum aşamasında belirlenen eşik değerleri ile karşılaştırırlar. PGO'nun ve HÇO'nın eşik seviyesinin altına inmesi ile algoritma, saldırgan türünün sürekli veya aldatıcı saldırgan olduğuna karar verir. PGO'nun eşiğin altına inmesine karşın hatalı çerçeve oranlarının eşik seviyesinin üstünde olması durumunda ise algoritma saldırgan türünün reaktif ya da rasgele saldırgan olduğunu kabul eder. PGO ve HÇO'nun eşik seviyesinin üstünde olması durumunda ise saldırgan türü PKS olarak belirlenir.

5.2 Savunma Birimi (Defense Unit)

Savunma birimi, saldırı tespit biriminden gelen saldırgan türü bilgisine göre uygulanacak çözüm yöntemini belirler ve uygulanmasını sağlar. Bu birimde sürekli, aldatıcı ve reaktif saldırganlar için *ekstra uyuma*, periyodik küme saldırganı için *periyot*



Şekil 8. Saldırgan türüne göre uygun savunma yönteminin belirlenmesi (Determining a defense method for jammer types)

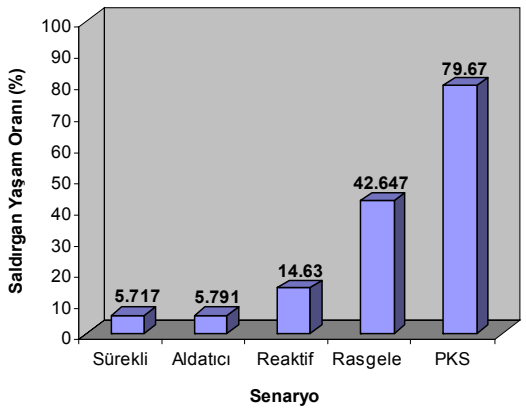
kaydırma ve rasgele saldırgan için *dinleme azaltma* algoritmaları çalıştırılır.

Şekil 8'de saldırgan türüne göre uygun olan üç savunma yönteminin seçilmesi görülmektedir. Enerjisini hızla tüketen sürekli, aldatıcı ve reaktif saldırganlar için *ekstra uyuma* yöntemi seçilmektedir. Periyodik küme saldırganı için ise periyot kaydırma yöntemi kullanılmaktadır. Ancak saldırganın reaktif veya rasgele olması durumunda iki farklı çözüm ortaya çıkmaktadır. Eğer saldırgan rasgele ise savunma yöntemi olarak dinleme azaltma algoritması tekniği kullanılmalı, reaktif saldırgan ise ekstra uyuma moduna geçilmelidir. Bu iki saldırgan türünü birbirinden ayırmak için öncelikle saldırgan türü rasgele kabul edilir ve dinleme azaltma yöntemi uygulanarak yeniden saldırı tespiti kontrol edilir. Eğer saldırgan rasgele ise bu yöntem sayesinde paket teslim oranları yükselmelidir. Eğer tersi durum söz konusu ise saldırgan türü reaktiftir ve çözüm olarak ekstra uyuma moduna geçilmelidir. *Ekstra uyuma*, *periyot kaydırma, ve dinleme azaltma* yöntemlerinin ayrıntılı çalışma prensipleri alt başlıklarda verilmektedir.

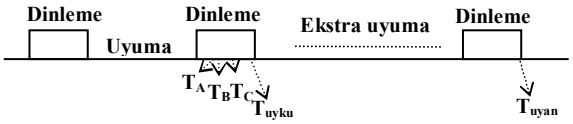
5.2.1 Ekstra Uyuma Yöntemi (Extra Sleeping Method)

Saldırı anında uyuma moduna geçme, pasif bir savunma tekniği olmasına rağmen, Şekil 9'da görüldüğü gibi enerjisini verimli kullanamayan ve her durumda enerjilerini hızlı tüketen sürekli, aldatıcı ve reaktif saldırgan türleri için etkin bir yöntemdir. Sürekli ve aldatıcı saldırganlar dost düğümlerin ancak % 5'i, reaktif saldırgan ise % 14'ü kadar yaşamlarını devam ettirebilmektedirler. Bu sebeple eğer tespit edilen saldırgan türü bu üç saldırgandan birisi ise düğümler belirli bir süre ekstra uyuma moduna geçmeli ve saldırganların enerjilerini tüketmelerini beklemelidir. Uyuma modunda düğümlerin alıcı ve vericileri pasif olmasına karşın algılama ve saklama birimleri aktiftir.

Şekil 10'da görüldüğü gibi düğümler *ekstra uyuma*



Şekil 9. Saldırgan düğümlerin yaşam oranları (Lifetime ratio of Jammer Nodes)

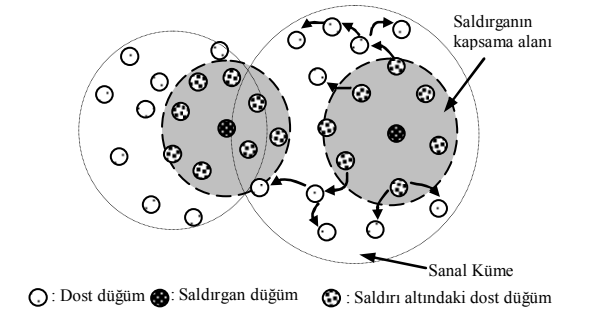


Şekil 10. Ekstra uyuma modu (extra sleeping)

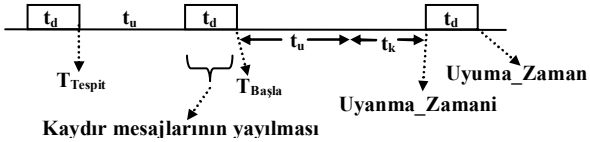
moduna geçmek için dinleme periyodunun bitmesini beklerler ve uyanma zamanlayıcısını kurarlar. Zamanlayıcının taştığı an uyanır ve ortamdaki PTO ve sinyal güç seviyelerini tekrar kontrol ederek saldırıların sürüp sürmediğini öğrenirler. Eğer saldırı devam ediyorsa uyumaya devam ederler. Şekildeki T_A, T_B ve T_C, A, B, ve C düğümlerinin saldırı olduğuna karar verdikleri anlardır. T_{uyku} ise tüm düğümlerin uyanma zamanlayıcılarını kurduğu andır, diğer bir ifadeyle dinleme zamanın bittiği andır. Düğümlerin *ekstra uyuma* moduna geçmek için dinleme periyodunun bitmesini beklemesinin nedeni eş zamanlı hareket edilebilmesini sağlamaktır. Saldırıların tespiti her düğüm içerisinde bireysel olarak yapılsa da savunma teknikleri için ortak hareket edilmelidir.

5.2.2 Periyot Kaydırma (Period Shifting)

Enerjisini koruyarak saldıran PKS belli bir süre boyunca düğümlerin iletişimlerini gözlemleyerek istatistiksel olarak bir sanal kümedeki iletişim zamanlarını, ortalama paket sayılarını, paketler arası varış sürelerini hesaplar. Elde ettiği istatistiksel bilgileri kullanarak, düğümler iletişim halinde iken saldırır ve düğümler uyuma halinde iken uyur. PKS, küme içerisinde elde ettiği istatistiklere göre saldırdığı için saldırganın bu bilgileri elde etmesini engellemek gerekir. Geliştirilen yöntemde, düğümler saldırının varlığını tespit ettikten sonra eş zamanlı olarak dinleme/uyuma periyotlarını zaman ekseninde önceden belirlenmiş süreler kadar sürekli olarak kaydırırlar. Küme içerisindeki iletişim zamanlarının sürekli değişmesi, saldırganın devamlı öğrenme konumunda kalmasına neden olmaktadır. Şekil 11'de bir saldırı senaryosu ve Şekil 12'de dinleme/uyuma periyotlarının zaman ekseninde kaydırılması görülmektedir. T_u MAC katmanı tarafından belirlenen uyuma, T_d dinleme ve T_k ise saldırı anında dinleme/uyuma periyodunun zaman ekseninde kaydırılacağı süredir. Sanal küme içerisindeki saldırgan düğümlerin etkisinde olan dost düğümler saldırı varlığını tespit ettikten bir sonraki dinleme süresinin bitiminde ($T_{Başla}$) periyot kaydırma işlemine başlayacaklardır. Ancak periyot kaydırma işleminin başlama zamanından sanal küme içerisinde olup da saldırganın etkisinde olmayan düğümlerin de haberdar olabilmesi gerekmektedir. Bu nedenle saldırıya uğradığını tespit eden düğümler saldırı tespitini gerçekleştirdikleri dinleme periyodundan sonraki dinleme aralığı içerisinde saldırı altında olduklarını gösteren önceliği yüksek ve küçük boyutlu KAYDIR mesajlarını saldırı etkisinde olmayan komşularına iletirler. Periyodik küme saldırganın büyük boyutlu



Şekil 11. Bir Saldırı Senaryosu (An Attacking Scenario)



Şekil 12. Dinleme / Uyuma periyodunun kaydırılması (Shifting Listen/Sleep Period)

veri paketlerine saldırması dost düğümlerin KAYDIR mesajlarını komşu düğümlere göndermesine ya da ulaştırmasına engel teşkil etmez. Böylelikle küme içerisinde dinleme/uyuma periyodunun değiştirilmesi gerektiği tüm düğümlere duyurulmuş olur.

Algoritma 1'de dinleme/uyuma periyodunun zaman ekseninde kaydırılma işlemi açıklanmaktadır. PKS saldırısına maruz kaldığını tespit eden düğümler içinde bulundukları dinleme süresinden bir sonraki dinleme süresinin başlangıcında uyanarak periyotlarını zaman ekseninde kaydıracaklarını gösteren KAYDIR mesajlarını rasgele süre bekledikten sonra komşularına gönderirler. Tüm düğümler KAYDIR mesajlarının gönderiminin yapıldığı dinleme periyodunun bitmesini bekleyerek senkronize olurlar ve uyanma sürelerini en az bir, en fazla dokuz dinleme süresi kadar kaydırırlar. Kayma süresi (T_k), *Kayma_orani* isimli tablodaki değerlere göre hesaplanır. *Periyod_Zamanlamasi* isimli fonksiyon yardımıyla da her defasında elde edilen yeni uyuma ve uyanma süreleri kullanılarak düğümlerin dinleme/uyuma periyotlarının zaman ekseninde kaydırılması sağlanır.

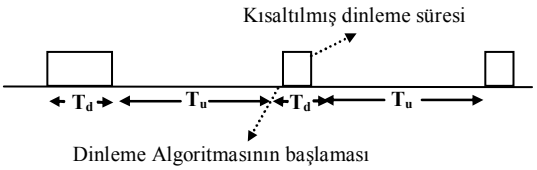
5.2.3 Dinleme Süresinin Azaltılması Yöntemi (Listen Time Reduction Method)

Rasgele saldırgan, rasgele seçtiği zaman aralıkları boyunca saldırır ve uyur. Bu sebeple enerji korunumu açısından periyodik küme saldırganına benzemektedir. Fakat belirli bir mantığa göre hareket etmemesi yani rasgele davranması sebebiyle çözüm üretilmesi zor olan saldırganlardan birisidir. Her ne kadar diğer saldırganlar kadar etkili olmasa da ağın güvenliğini bozmaktadır.

Algoritma 1. Dinleme/Uyuma zamanlamasının zaman ekseninde kaydırılması (Shifting Listen/Sleep period on the time axis)

```
Periyot_Kaydir() //Dinleme süresi içerisinde PKS tespit edildiğinde çağrılır
{
    i=0
    Kayma_orani[]={2,1,6,4,8,5,9,3,7}  // kaydırma katsayıları
    zamanlayıcı=sonrakiDinlemeSüresi;  //Zamanlayıcıyı sonraki dinleme süresine kur
    while(zamanlayıcıTaştı==FALSE);    //Zamanlayıcı taşana kadar bekle
    rasgeleSüre=uniform(0,0.010);       //0-10msn arasında rasgele değer ata

    /*KAYDIR paketini rasgele süre bekleyerek gönder*/
    Gonder (şimdikiZaman+rasgeleSüre, KAYDIR);
    zamanlayıcı=dinlemeSüresininSonu;  //Zamanlayıcıyı dinlemenin bitimine kur
    while(zamanlayıcıTaştı==FALSE);    //Zamanlayıcı taşana kadar bekle
    while(true)
    {
       Tk = Kayma_orani[i mod 9]* Td      //Kayma miktarını belirle
       Uyanma_Zamani = Tu + Tk            //Yeni uyuma zamanını belirle
      Sonraki_Uyuma_Zamani = Tu + Tk + Td // Yeni uyanma zamanını belirle
      i=i+1                              //Kayma oran sayacını arttır
     /*Yeni dinleme/uyuma zamanlamasını ayarla */
      Periyod_Zamanlamasi(Uyanma_Zamani, Sonraki_Uyuma_Zamani)
    }
}
```



Şekil 13. Dinleme süresinin azaltılması (Listen Time Reduction Method)

Rasgele anlarda saldırmanın nedeni, saldırı paketlerini dost düğümlerin iletişim anlarına denk getirmektir. Dost düğümlerin iletişim anları ile saldırganın saldırı anları çakışmaz ise saldırganın etkisi kalmayacaktır. Bu olasılığı en aza düşürmenin yollarından birisi de düğümlerin dinleme sürelerini azaltmaktır. Özetle, bir dinleme/uyuma periyodu içerisinde daha uzun süre uyumak ve daha kısa uyanık kalarak iletişimi gerçekleştirmektir. Bu savunma yönteminde de periyot kaydırma yönteminde olduğu gibi saldırgan etkisinde olmayan düğümlerin dinleme süresinin azaltıldığından haberdar edilebilmesi için yüksek öncelikli AZALT isimli bir paket gönderilmektedir. S-MAC ile birlikte gelen dinleme süresi 93 msn'dir. Bu süre saldırı durumunda 18,6 msn'ye (%2 duty cycle) kadar azaltılabilir. Böylelikle saldırganın saldırı paketlerini düğümlerin iletişim anlarına denk getirme olasılığı çok daha azalır.

6. Simülasyon Sonuçları (Simulation Results)

Bozma saldırılarına karşı tasarlanan AR-MAC protokolünün başarım değerlendirilmesi S-MAC protokolü ile kıyaslanarak gerçekleştirilmiştir. Kıyaslamada tüketme, bozma ve engelleme oranları olarak tanımladığımız ve saldırganların kablosuz algılayıcı ağına verdikleri zararın ölçülebilmesini sağlayan 3 parametreden faydalanılmıştır.

- **Tüketme Oranı (TO):** Düğümlerin saldırı sebebiyle yaşam sürelerinin ne kadar kısaldığını gösteren orandır ve bu oran yardımıyla bir saldırganın sebep olduğu enerji tüketimi hakkında bilgi sahibi olunabilir. Bir düğümün saldırı mevcut değil iken yaşam süresi Y_{Normal} ve saldırı altındaki yaşam süresi $Y_{Saldırı}$ varsayıldığında saldırganın tüketme oranı Formül-1 yardımıyla hesaplanabilir. Negatif çıkan değerler saldırı durumlarındaki düğüm yaşam sürelerinin normal koşullara göre uzadığını göstermektedir. Bir diğer ifadeyle, düğümler saldırı süresince ekstra güç tüketmeyip aksine daha az enerji harcamış demektir.

$$TO = \frac{Y_{Normal} - Y_{Saldırı}}{Y_{Normal}} \times 100 \qquad (1)$$

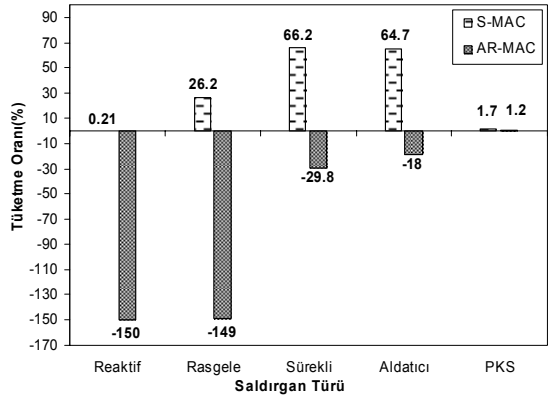
- **Engelleme Oranı (PEO):** Engelleme oranı normal düğümlerin göndermek istediği ancak gönderemediği paketlerin oranlarını vermektedir. Paylaşımlı olan iletim kanalının normal düğümlerden çok saldırganlar tarafından kullanıldığı durumlarda düğümler iletişim ortamına uzun süreler boyunca erişemez ve paket gönderemezler dolayısıyla gönderilemeyen paketler zaman aşımı nedeniyle iptal edilirler. Kablosuz algılayıcı ağının ömrü süresince düğümlerin göndermek istediği toplam paket sayısı $P_{İstenen}$, gönderebildiği paket sayısı ise $P_{Gönderilen}$ olduğunda paket engelleme oranı Formül–2 yardımıyla hesaplanabilir. Büyük çıkan engelleme oranları saldırganların çoğunlukla iletişim ortamına hâkim olduğu ve düğümlerin paket göndermelerini engellediğini göstermektedir.

$$EO = \frac{P_{İstenen} - P_{Gönderilen}}{P_{İstenen}} \times 100 \qquad (2)$$

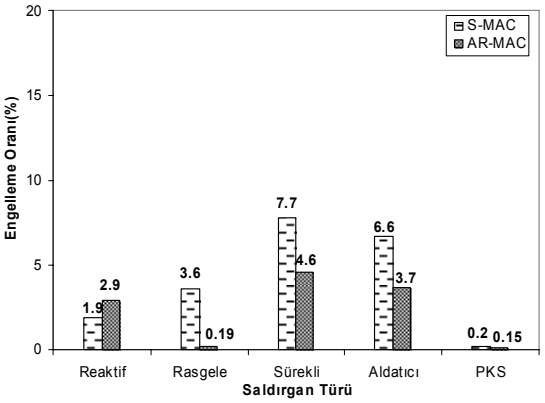
- **Bozma Oranı (BO):** Bozma oranı, düğümlerin gönderdiği paketlerden ne kadarının çakışma nedeniyle bozulduğunu göstermektedir. Düğümlerin gönderdiği toplam paket sayısı $P_{Gönderilen}$, alıcılara başarılı bir şekilde ulaştırabildiği toplam paket sayısı ise $P_{Ulaştırılan}$ olarak adlandırıldığında Formül–3 yardımıyla paket bozma oranı hesaplanabilir.

$$BO = \frac{P_{Gönderilen} - P_{Ulaştırılan}}{P_{Gönderilen}} \times 100 \qquad (3)$$

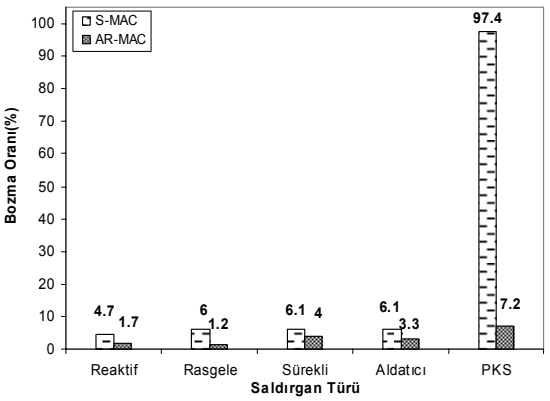
Şekil 14'de S-MAC ve AR-MAC protokolleri için elde edilen ortalama tüketme oranları görülmektedir. Sürekli ve aldatıcı saldırganlar sürekli paket göndererek dost düğümlerin BACKOFF (geriçekilme) durumunda kalmalarına sebep olmaktadırlar. S-MAC protokolünde bir düğüm BACKOFF durumundan ancak başarılı veya hatalı bir paket aldığında çıkabildiği için düğümler bu iki saldırı senaryosunda sürekli BACKOFF durumunda kalmakta (radyo dinleme durumunda) ve uyuma moduna geçemeyerek enerjilerini daha hızlı tüketmektedirler. Bu sebeple düğümlerin yaşam süreleri, saldırının olmadığı duruma göre sürekli saldırı için % 66, aldatıcı saldırı için ise % 64 oranında kısalmaktadır. Reaktif saldırgan gönderilen paketlerin çakışmasına sebep olduğu için düğümleri BACKOFF durumunda tutmaz ve dolayısıyla uyuma aralıklarında uyumalarını engellemez. Bu sebeple reaktif saldırı senaryosunda düğümlerin yaşam süreleri kısalmamaktadır. Düğümler AR-MAC protokolünde reaktif, sürekli ve aldatıcı saldırı senaryoları için uyuma moduna geçerek saldırıların bitmesini beklemektedir. Saldırılar devam ederken düğümlerin uyuması, S-MAC protokolünde olduğu gibi düğümlerin enerji kayıplarını ortadan kaldırmış ve yaşam sürelerinin kısalmasını engellemiştir. Bununla birlikte tüketme oranlarının negatif değerler çıkması, düğümlerin ekstra uyuması sebebiyle yaşam sürelerinin saldırının



Şekil 14. Farklı saldırgan türleri için elde edilen Tüketme oranları (Exhaustion ratios under various attack types)



Şekil 15. Farklı saldırgan türleri için elde edilen engelleme oranları (Block ratios under various attack types)



Şekil 16. Farklı saldırgan türleri için elde edilen bozma oranları (Collision ratios under various attack types)

olmadığı normal koşullara oranla daha da uzadığını göstermektedir.

Rasgele saldırı senaryosunda saldırı paketlerinin düğümlerin uyuma aralığına yakın zamanlara denk gelmesi durumunda düğümler BACKOFF modunda kalmakta ve uyuma moduna geçememektedir. Bu sebeple rasgele saldırgan, düğümlerin yaşam sürelerinin yaklaşık % 26 oranında azalmasına sebep olmaktadır. AR-MAC protokolünde uygulanan dinleme süresinin azaltılması yöntemiyle düğümlerin BACKOFF modunda kalma süreleri kısalmıştır buna ek olarak normal koşul altındakilere oranla daha düşük görev çevrimi (%2) sebebiyle düğümlerin enerji tüketimleri azalmış ve yaşam süreleri daha da uzamıştır. Periyodik küme saldırganı, reaktif saldırgana benzer olarak paket çarpışmasına neden olduğu için düğümlerin enerji tüketimini diğer saldırılara oranla düşük tutmaktadır.

Şekil 15'te engelleme oranları görülmektedir. Sürekli ve aldatıcı saldırganlar yaşamlarını devam ettirdikleri süre boyunca paket gönderimini tamamen engellemektedirler ancak normal düğümlere kıyasla daha kısa sürede ölmeleri düğümlerin yeniden paket gönderimine başlamasına ve toplam engelleme oranlarının normal değerlere yaklaşmasına sebep olmaktadır. Dolayısıyla, S-MAC protokolünde sürekli ve aldatıcı saldırganlar paketlerin toplam %6-7'sinin gönderimini engelleyebilmektedirler. AR-MAC protokolünde ise düğümlerin yaşam süresinin S-MAC'e göre daha uzun olması sebebiyle toplam engellenen paket oranı da S-MAC'den daha düşük olarak elde edilmiştir. Reaktif saldırgan paket gönderimini engellemekten daha çok bozulmasına sebep olmaktadır ve bu nedenle paketlerin yaklaşık % 2'sinin gönderimini engellemektedir. AR-MAC'te bu oran S-MAC'e göre daha fazladır. Bunun sebebi, düğümlerin ekstra uyuma sırasında paket gönderememesidir. Rasgele saldırgan, rasgele aralıklarla saldırdığı için bazı paketlerin gönderilmesini engellemektedir. AR-MAC protokolünde dinleme süresinin azaltılması, paket gönderme oranlarının düşmesine neden olsa da düşük görev çevrim süresi sebebiyle yaşam süreleri uzayan düğümlerin toplam engellenen paket oranları azalmaktadır. PKS de reaktif saldırgana benzer olarak paket gönderimini engellemediği için toplam engelleme oranları her iki protokolde de son derece düşüktür.

Şekil 16'da farklı senaryolar için elde edilen bozma oranları görülmektedir. Reaktif, sürekli ve rasgele saldırgan türleri için uygulanan ekstra uyuma algoritması ile AR-MAC protokolünde S-MAC'e nispeten daha düşük bozma oranları sağlanmıştır. S-MAC protokolünde gönderilen paketlerin toplam % 6'sını bozabilen rasgele saldırgan, AR-MAC protokolünde paketlerin yaklaşık % 1,2'sini bozabilmektedir. Daha önce de ifade edildiği gibi, bu dört saldırgan türü enerjisini normal düğümlere kıyasla daha çabuk tüketmektedirler ve bu nedenle engelleme ve bozma oranları saldırganlar öldükten sonra normal değerlere yaklaşmaktadır. Ancak periyodik küme saldırganın yaşam süresi, düğümlerin yaşam süresine yaklaştığı için toplam bozma oranı da son derece yüksektir. AR-MAC protokolünde uygulanan periyot kaydırma yöntemi sayesinde bozma oranları makul seviyelere düşmektedir.

7. SONUÇLAR (CONCLUSIONS)

Literatürde DoS saldırılarına karşı aktif bir şekilde çözüm üreten MAC protokol tasarımına yönelik sınırlı sayıda çalışma bulunmaktadır. Özellikle güvenliğin en önemli tasarım ölçütü olduğu askeri uygulamalarda, bina güvenlik sistemlerinde, biyolojik ve kimyasal saldırı tespit uygulamalarında kullanılan kablosuz algılayıcı ağlarının her türlü saldırılara karşı dayanıklı olması gereklidir. Enerji tüketiminin en önemli tasarım ölçütü olduğu algılayıcı ağlarda, yeterli donanımsal kaynaklara sahip olmayan kablosuz algılayıcı düğümleri DoS saldırılarına karşı savunmasızdır. Bu çalışmada, kablosuz algılayıcı ağlarını tehdit eden beş farklı hizmet engelleme saldırgan türünü birbirinden ayırarak saldırı türüne göre uygun çözüm üreten AR-MAC protokol tasarımı gerçekleştirilmiştir. Düğümlerin saldırı altında olup olmadığını tespit etmek için sinyal güç seviyesi ile paket teslim oranından, hangi tür saldırgana maruz kaldıklarını anlamak için ise paket gönderme ve hatalı çerçeve oranlarından faydalanılmıştır. Çalışmanın diğer önemli bir katkısı ise *ekstra uyuma*, *periyot kaydırma* ve *dinleme süresinin azaltılması* gibi yöntemlerin geliştirilerek bilinen DoS saldırılarına karşı çözüm üretilmesidir. Simülasyon sonuçlarına göre geliştirilen çözüm yöntemleri sayesinde düğümlerin saldırı altındaki yaşam süreleri önemli ölçüde artarken, saldırganların etkinliği azalmıştır. Bir sonraki çalışmada gerçek zamanlı uygulamalara yönelik olarak ekstra uyuma algoritması ile birlikte gönderim gücünün ayarlanarak (dinamik güç yönetimi) acil paketlerin güvenli bir şekilde merkezi yönetim birimine (sink yada baz istasyon) ulaştırılması hedeflenmektedir.

KAYNAKLAR (REFERENCES)

1. Van Dam, Tijs, K. Langendoen.,"An adaptive energy-efficient MAC protocol for wireless sensor Networks", **First ACM Conference on Embedded Networked Sensor Systems**, 171–180, Kasım 2003.
2. G. Lu, B. Krishnamachari, C.S. Raghavendra, "An adaptive energy-efficient and low- latency MAC for data gathering in wireless sensor networks," **Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS 2004)**, USA, 26-30 Nisan 2004.
3. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci,"Wireless Sensor Networks: A Survey," **Computer Networks,** Cilt 38, Sayı 4, 393–422, Mart 2002.
4. Wenyuan Xu, Ke Ma, Wade Trappe, Yanyong Zhang, "Jamming Sensor Networks: Attack and Defense Strategies," **IEEE Networks Special Issue on Sensor Networks**, Cilt 20, Sayı 3, 41–47, Mayıs/Haziran 2006.
5. A.D. Wood, J.A. Stankovic, "Denial of service in sensor networks," **IEEE Computer**, Cilt 35, Sayı 10, 54–62, Ekim. 2002.
6. A. Wood, J. Stankovic, S. Son., "JAM: A jammed-area mapping service for sensor networks.", **24. IEEE Real-Time Systems Symposium**, 286 - 297, 2003.
7. Q. Ren, Q. Liang, "Fuzzy logic-optimized secure media access control (FSMAC) protocol", **CIHSPS 2005**, 37 – 43, 31 Mart–1 Nisan 2005.
8. Sunil Kumar, Vineet S. Raghavan, Jing Deng, "Medium Access Control protocols for ad hoc wireless networks: a survey" **Ad Hoc Networks (ELSEVIER),** Cilt 4, Sayı 3, 326–358, Mayıs 2006.
9. "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications",**IEEE Standards 802.11**, 195–200, 1999.
10. Wei Ye, J. Heidemann, Deborah Estrin, "An energy-efficient mac protocol for wireless sensor networks.", **IEEE INFOCOM**, USA, 1567–1576, Haziran 2002.
11. Yee Wei, P. Hartel, J. Den Hertog, P.Havinga, "Link layer Jamming Attacks on S-MAC"**, Proceeedings of the Second European Workshop on Sensor Network**, 217 – 225, İstanbul, Türkiye, 31 Ocak-2 Şubat 2005.
12. Yee 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.
13. **www.omnetpp.org**, OMNET++, Ayrık Olay tabanlı Simulator.
14. **http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/MICA2_Datasheet.pdf**, MICA2 çalışma sayfası.