KABLOSUZ ALGILAYICI AĞLAR İÇİN BOZMA SALDIRILARINI TESPİT SİSTEMİ

Murat ÇAKIROĞLU, A.Turan ÖZCERİT
Sakarya Üniversitesi,Teknik Eğitim Fak., Elekt-Bilg. Bölümü
muratc, aozcerit@sakarya.edu.tr

ABSTRACT

The nodes of wireless sensor network (WSN) are scattered arbitrarily into the target field and they use a shared communication medium. The nodes are prone to external attacks and disturbances since they are in harsh environments without having specialized defensive measures. In this paper, we have developed a special detection mechanism used for Jamming-style Denial of Service (J-DoS) attacks, which disturb physical and medium access functions of WSNs, to differentiate the legitimate and adversary scenarios. According to the simulation results obtained, the legitimate scenarios can be separated from adversary ones having high detection rate and low false positive rate parameters. Having detected the type of the scenario, an appropriate solution can be followed accordingly.

Keywords: DoS, WSN, Security, Intrusion Detection, Attack, Jamming

1. GİRİŞ

Bozma türündeki hizmet engelleme (Jamming Style DoS) saldırıları kasıtlı olarak radyo sinyali göndererek kablosuz iletim ortamındaki paketlerin bozulmasını ve böylece düğümlerin iletişimlerinin aksamasını ya da tamamen engellenmesini hedefleyen saldırı türüdür ve kablosuz algılayıcı ağları için önemli bir tehdit unsurudur [4,6]. Literatürde MAC ve fiziksel katmanda çalışan DoS saldırgan türleri ile ilgili çok çeşitli çalışmalar bulunmaktadır. Xu ve diğerleri [6] sürekli, aldatıcı, rasgele ve reaktif olmak üzere dört saldırgan modeli tanımlamıştır. Law ve diğer S-MAC protokolü için dinleme aralığı, kontrol aralığı, veri paketi ve küme saldırganı olmak üzere enerji-etkin 4 saldırgan modeli önermiştir [5,7]. Wood ve diğerleri [11] ise kesme, aktivite, tarama ve darbe saldırganların modellerini geliştirmişlerdir (Detay bilgi için ilgili makalelere başvurulabilir).

Literatürde saldırgan türleri ile ilgili birçok çalışma bulunmasına karşın bu saldırıların tespitine yönelik çok az sayıda çalışma bulunmaktadır. Xu ve diğerleri [6], çalışmalarında tanımladıkları dört saldırgan türünü tespit etmek için iki farklı yöntem geliştirmişlerdir. Wood ve diğerleri [3] ise çalışmalarında tek tip saldırganı tespit etmek için kanal kullanım oranından faydalanmışlardır. Ancak son yıllarda daha zeki saldırgan modellerinin önerilmesi bu yöntemlerin yetersiz kalmasına sebep olmaktadır. Bu sebeple literatürde var olan bu tip zeki saldırganları yüksek başarım oranları ile tespit edebilecek bir tespit sistem ihtiyacı bulunmaktadır.

Bu makalede, bozma saldırıları için anomali temelli saldırı tespit algoritma (Anomaly based Jamming Detection Algorithm- AJDA) tasarımı gerçekleştirilmiştir. Sunulan yöntemin katkısı:

- Literatürde tanımlanmış olan farklı özelliklerdeki birçok bozma saldırgan türlerini tıkanıklık, kayıplı bağlantı koşulları ve donanımsal hatalar gibi doğal ağ durumlarından yüksek sezme ve düşük hatalı sezme oranları ile tespit edebilmesi,
- Herhangi bir ek donanıma ihtiyaç duyulmadan günümüz algılayıcı düğümlerinde kullanılabilmesidir.

Makale'nin geri kalan kısımları aşağıda açıklandığı gibi düzenlenmiştir: 2. Bölüm'de saldırı tespit ölçütleri ve 3. Bölüm'de geliştirilen basit saldırı tespit algoritmasının detayları açıklanmıştır. 4. Bölüm'de önerilen ileri seviye bozma saldırı tespit yöntemi sunulmuştur. 5. Bölüm'de benzetim ayarları ve kabulleri ile ilgili bilgi verilmiş ve 6. Bölüm'de elde edilen benzetim sonuçlarının sunulmasını takiben 7. Bölüm'de çalışmadan elde edilen sonuçlar irdelenmiştir.

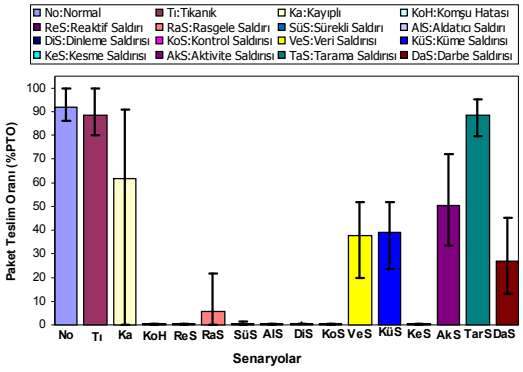
2. SALDIRI TESPİT ÖLÇÜTLERİ

Bir ağdaki iletişimi tamamen engelleyen veya aksatan bozma saldırıları ağ içerisinde bazı anormal durumların ortaya çıkmasına neden olmaktadır. Çarpışmaların ve hatalı paket alımlarının artması, iletişim kanalına erişim güçlüğü, yüksek sinyal güç göstergesi (RSSI) v.b. birçok parametre bozma saldırılarından etkilenmektedir. Bu parametrelerdeki anormal değerler bir saldırı göstergesi olabilir. Ancak bu gibi anormal durumlar kötü niyetli davranışlar sebebiyle meydana gelebileceği gibi doğal ağ koşulları sonucunda da oluşabilmektedir. Örneğin tıkanıklık, komşu düğümlerdeki yazılımsal veya donanımsal hatalar, çevresel şartların değişmesi ile meydana gelebilecek hatalar, saldırı senaryolarına benzer şekilde anormal durumların oluşmasına sebep olabilir. Zeki saldırı yöntemlerinin geliştirilmesi ve kablosuz algılayıcı düğümlerinin sınırlı donanımsal kaynaklara sahip olması bu

saldırıların başarılı bir biçimde tespit edilebilmesini zorlaştırmaktadır. Bu çalışmada benzer durumların oluşmasını neden olan doğal koşullar ile farklı bozma saldırı türlerini birbirlerinde ayırabilmek için MAC ve fiziksel katmandan elde edilen bazı sistem parametrelerinden faydalanılmaktadır.

3.1 Paket Teslim Oranı (PTO)

Bir düğümden gönderilen paket sayısının alıcıya ulaşan paket sayısı oranı paket teslim oranı verir. Düğümler gönderilen paketlerin alıcıya ulaştığını, alıcının gönderdiği bir ACK paketi ile denetler. Saldırganlar, düğümlerin gönderdiği paketleri bozarak PTO değerlerinin düşmesine neden olabilir. Ancak bir düğümdeki PTO değeri kayıplı bağlantı koşulları, komşu düğümde meydana gelebilecek hata durumlarında ve çakışmalar sebebiyle de önemli ölçüde düşebilmektedir. Bu sebeple tek başına paket teslim oranı yardımıyla tüm saldırı senaryolarının doğal ağ koşullarından ayrılması mümkün değildir.



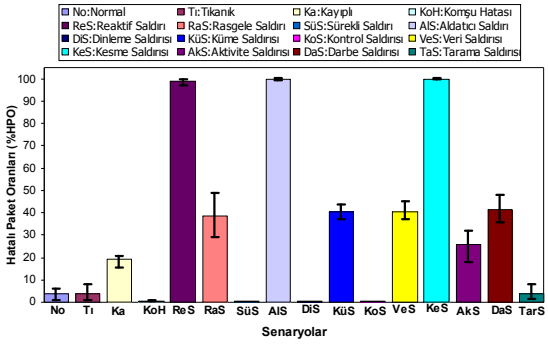
Şekil.1 Farklı senaryolarda bir düğümden ölçülen ortalama paket teslim oranları

Şekil 1'de farklı saldırı türlerinin veya ağ koşullarının etkisinde olan bir düğümden 60 saniye aralıklarla ölçülen paket teslim oranlarının minimum, maksimum ve ortalama değerleri görülmektedir. Birçok saldırı senaryosunda PTO değerleri oldukça düşmesine karşın komşu düğümde meydana gelebilecek bir hata (batarya sorunu v.b.), kayıplı bağlantı koşulları gibi bazı doğal ağ durumları sonucunda da düşebilmektedir. Bu gibi sebepler tek başına PTO parametresi ile saldırı tespitini güçleştirmektedir.

3.2 Hatalı Paket Oranı (HPO)

Bir düğümün aldığı bozuk paket sayısının alınan toplam paket ya da öntakı sayısına oranıdır. Düğümler paketin bozuk olup olmadığına CRC denetimi ile karar vermekte ve denetimden geçemeyen paketleri iptal etmektedirler. Aslında PTO gönderici açısından, HPO ise alıcı düğüm açısından bağlantı kalitesini gösteren benzer iki parametredir. Çoğu durumda bu iki parametre arasında ters orantı bulunmakta ve çarpışma nedeniyle bir düğümün HPO'su artarken, PTO'su düşmektedir. Ancak bazı senaryolarda HPO düşük kalırken, PTO değerleri de düşebilmektedir.

Şekil 2'de farklı senaryolarda bir düğümden ölçülen HPO değerleri görülmektedir. Çoğu saldırı durumunda hatalı paket oranlarının doğal ağ koşullarındakine oranla oldukça yüksek çıkması doğal şartlarla saldırı senaryolarını birbirinden ayrıştırmayı kolaylaştıracaktır. Ancak paket gönderilmesini engelleyen sürekli, dinleme ve kontrol aralığı saldırgan senaryolarında alınan geçerli bir öntakı ya da paket olmadığından hatalı paket oranları da sıfır seviyesindedir. Bu gibi saldırı senaryolarında düşük HPO'nun ölçülmesi bu saldırganların doğal ağ şartlarından PTO ve HPO yardımıyla ayrılmasını zorlaştırmaktadır.

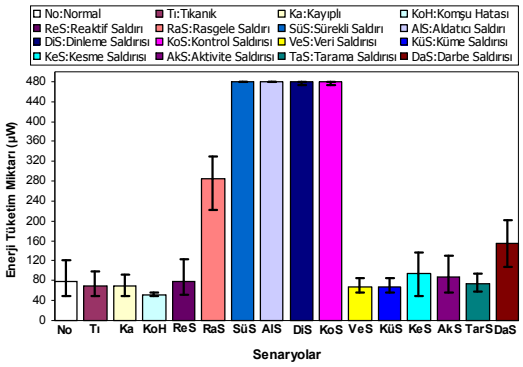


Şekil.2 Farklı senaryolarda bir düğümden ölçülen hatalı paket oranları

3.3 Enerji Tüketim Miktarı (ETM)

Düğümün belli bir süre içerisinde yaklaşık olarak harcadığı enerji miktarıdır. Bir MICA2 düğümün radyosu gönderim gücünün değişmediği (0 dbm) varsayıldığında gönderme modunda saatte 49.5 mW, alma modunda 28.86 mW ve uyuma modunda 3 µW güç harcamaktadır [13]. Radyo evrelerinde kaldığı süre ile yukarıdaki değerler çarpılarak düğümün belli bir süre içersinde harcamış olduğu yaklaşık enerji miktarı hesaplanabilir. Şekil 3'te farklı senaryolarda bir düğümden elde edilen enerji tüketim miktarları görülmektedir. Aldatıcı, sürekli, rasgele, dinleme ve kontrol aralığı saldırganları düğümlerin enerji tüketimlerinin önemli ölçüde artmasına neden olmaktadır. Bunun sebebi, aldatıcı saldırganın düğümleri sürekli alım modunda; sürekli saldırgan, dinleme aralığı ve kontrol aralığı saldırganlarının ise dinleme modunda tutmasıdır. Bu saldırganlar iletişim kanalını kesintisi meşgul ettikleri için düğümlerin geriçekilme (BACKOFF) durumunda kalmasına neden olmaktadır. Bu sebeple, BACKOFF durumunda kalan düğümler uyuma moduna geçemediklerinden enerjilerini daha çabuk tüketmektedirler. CC1000 radyonun aylak (IDLE) modunun olmaması nedeniyle de saldırı altındaki düğümler sürekli, dinleme aralığı ve kontrol aralığı saldırı senaryolarında aldatıcı

saldırgana eş güç tüketmektedir. Rasgele, sürekli, aldatıcı, dinleme aralığı ve kontrol aralığı saldırgan senaryolarında düğümlerin normal koşullara oranla çok daha fazla güç tüketmesi sayesinde bu saldırganların doğal ağ koşullarından ayrılması mümkün olacaktır



Şekil.3 Farklı senaryolarda bir düğümden ölçülen enerji tüketim miktarları.

3. GELİŞMİŞ BOZMA SALDIRI TESPİT YÖNTEMİ

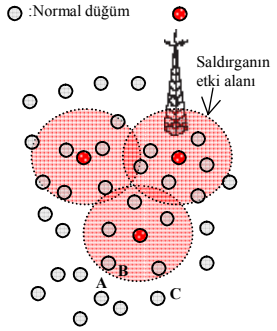
Çok çeşitli saldırı yöntemlerinin olması ve doğal ağ koşulları ile saldırı durumlarının birbirine karışması yüksek tespit oranlarına ve düşük hatalı alarm oranlarına sahip saldırı tespit yönteminin geliştirilmesini zorunlu kılmaktadır. Bu çalışmada bölüm 2'de detayları verilen paket teslim oranı (PTO), hatalı paket oranı (HPO) ve enerji tüketim miktarı (ETM) parametrelerinden faydalanılarak anomali temelli saldırı tespit yöntemi geliştirilmiştir. Anamoli temelli saldırı tespit yöntemlerinde saldırının olmadığı zamanlarda ağın normal durumlardaki sistem profili elde edilir ve daha sonra da bu profil yardımıyla anormal durumların tespiti gerçekleştirilir. Düğümler normal ağ koşullarını belirleyebilmek için saldırının olmadığı ağ kurulum aşamasında PTO, HPO ve ETM parametrelerini istatistiğini tutarak bazı matematiksel yöntemler yardımıyla eşik değerlerini belirlerler. Daha sonra saldırı tespitinde bu eşik değerlerinden faydalanırlar. Ancak ağ içerisinde meydana gelebilecek beklenmeyen veya önceden kestirilemeyen bazı doğal koşullar sezme oranlarının düşmesine ve hatalı sezme oranlarının artmasına yol açabilmektedir. Bu sebeple yüksek başarım elde edebilmek için eşik mekanizmasının bir başka ek mekanizma ile desteklenmesi gerekmektedir. Bu çalışmada paket teslim oranı, hatalı paket oranı ve enerji tüketim miktarı olarak adlandırılan parametrelerden faydalanılarak "sorgulama" tabanlı saldırı tespit yöntemi geliştirilmiştir. Yöntemin esası; PTO, HPO ve ETM parametrelerine göre saldırı altında olduğundan şüphe eden düğümün komşu düğümlere gönderdiği SORGU (QUERY) paketi ve buna karşılık komşulardan gelecek CEVAP (REPLY) paketlerine dayanmaktadır. Düğümler geçerli PTO (PTO_n) ile birlikte ağ kurulum aşamasında belirlediği eşik ($PTO_{eş}$) değerini SORGU paketine gömerek komşularına saldırı altında olup olmadıklarını sorarlar. SORGU paketi alan düğümler ise benzer şekilde kendi PTO_n v_e $PTO_{eş}$ değerlerini CEVAP paketine gömerek gönderir. SORGU paketi ya da CEVAP paketi alan düğümler bu paketlerdeki paket teslim oranlarına bakarak saldırı altında olup olmadıklarını değerlendirirler. Ancak sürekli ve aldatıcı saldırgan gibi iletişim kanalını kesintisiz meşgul eden saldırganlar SORGU-CEVAP paketlerinin gönderimini engellemektedir. Reaktif saldırgan gibi bazıları ise gönderilen sorgu paketlerin bozulmasına neden olmakta, Veri paketi saldırganı gibi saldırganlar ise SORGU-CEVAP paketlerine saldırmamaktadır.

Algoritmada gelişmiş sorgu tabanlı saldırı tespit yöntemi görülmektedir. Düğümler ağ kurulum aşamasında PTO, HPO ve ETM parametreleri için elde ettikleri eşik değerleri ile her örnekleme periyodunda ölçtükleri değerleri kıyaslarlar. Kodlardaki PTO_n, HPO_n ve ETM_n n. örnekleme periyodundaki paket teslim oranlarını, hatalı paket oranlarını ve enerji tüketim miktarlarını göstermektedir. Herhangi bir örnekleme anında eğer ölçülen PTO eşik değerinden küçük ve ETM eşik değerinden fazlaysa ya da HPO eşik değerinden fazlaysa, düğüm bu durumun tehlikeli olacağını düşünerek sorgu sürecini başlatır. Düğüm çekişme kurallarına da uyarak 3 örnekleme periyodu içerisinde SORGU paketi göndermelidir. Eğer bu süre zarfında hiçbir SORGU paketi gönderemez ise sürekli veya aldatıcı saldırgan gibi kanalı meşgul eden bir saldırıya maruz kaldığına karar verir ve rasgele bir zaman bekleyerek ZORLAMA SORGU paketi gönderir. Düğümler ZORLAMA SORGU paketini Şekil 4'te görüldüğü gibi doğrudan bir saldırganın etkisinden olmasa da dolaylı yoldan yani komşusu sebebiyle saldırgandan etkilenen sınır düğümlerin saldırı tespitini kolaylaştırmak için göndermektedirler. Bu gibi düğümlerin komşuları saldırgan etkisinde olduğu için PTO değerleri düşerken HPO ve ETM değerleri düşmeyebilmekte ve bu sebeple komşu düğümlerde meydana gelen hata durumlarına benzer bir senaryo söz konusu olmaktadır. Ancak böyle bir ZORLAMA SORGU paketi alan düğüm komşusunun saldırı altında olduğunu anlayabilmektedir. Belirlenen zaman dilimi içerisinde SORGU paketini gönderen bir düğüm CEVAP paketlerini beklemeye başlar ve SORGU-CEVAP oturumu için belirlenen sürenin dolması ile kendisine gelen CEVAP paketlerini değerlendir. Düğüm;

1. Kendisine gelen CEVAP paketlerinin sayısı komşu düğüm sayısından daha az ise
2. Eşik değerinden yüksek PTO'ya sahip olan komşu düğüm sayısı eşik değerinden düşük

PTO'ya sahip düğüm sayısından daha az ise saldırı altında olduğuna karar vermektedir.

Saldırı tespitinde en zor kısımlardan birisi de doğrudan saldırganın kapsama alanında olmadığı halde dolaylı yoldan saldırgandan etkilenen ve PTO'su düşen sınır düğümlerdir (Şekil 4'teki A ve C düğümleri gibi). Bu düğümlerin PTO değerleri düşse bile saldırganının kapsama alanında olmadıkları için HPO ve ETM değerleri düşmemekte ve komşu düğüm hata senaryosuna benzer bir durumun ortaya çıkmasına neden olmaktadırlar. Dolayısıyla saldırı durumu ile komşu hata durumu birbirine karışmaktadır. Ayrıca bu düğümler SORGU paketi gönderseler bile saldırgan etkisinde olmayan yüksek PTO'lu komşularından yeterli sayıda CEVAP paketi alabilmekte ve bu yüzden saldırı tespiti gerçekleştirilememektedir. Sınır düğümlerde saldırı tespitinde bazı özelliklerden faydalanılmaktadır. Şekil 4'teki A düğümü gibi bir sınır düğümün PTO'su eşik değerinden düşük, HPO ve ETM'si de eşik değerinden küçük çıkacaktır. Böyle bir durumda düğüm saldırı altında olup olmadığına karar vermek için hedefteki komşusundan bir SORGU, CEVAP ya da herhangi bir geçerli paket alıp almadığını kontrol etmektedir. Eğer herhangi bir SORGU ya da CEVAP paketi aldıysa ve bu paketteki PTO değeri $PTO_{eş}$'den daha düşükse (`hedefDugumPTODusuk=TRUE`) düğüm kendisinin de saldırı altında olduğuna karar verir. Ancak geçerli örnekleme periyodu içerisinde hedef düğümden SORGU / CEVAP paketleri ya da herhangi bir geçerli paket almadıysa (`hedefDugumYasiyor=FALSE`) düğümde bir arıza olduğuna varsayar. Reaktif saldırgan gibi paket gönderilmesini engellemeyen saldırgan senaryolarında düğümler paket gönderebildiği için sınır düğümler gelen paketlerden hedef düğümlerin yaşayıp yaşamadığını anlayabilmektedir. Ancak sürekli, aldatıcı, dinleme aralığı ve kontrol aralığı gibi saldırgan senaryolarında ise düğümler kanalın sürekli meşgul olması sebebiyle hiç paket göndermemekte ve dolayısıyla sınır düğümler tarafından yaşadıkları anlaşılamamaktadır. Bunu aşmak için ZORLAMA SORGU paketlerinden faydalanılmaktadır. Kanalı sürekli meşgul eden saldırgan senaryolarında düğümler normal şartlarda SORGU gönderememektedirler. Ancak sınır düğümlerinin bu düğümlerin saldırı altında olduklarını anlayabilmeleri için çekişme kurallarına aldırmadan rasgele zaman bekleyerek ve toplamda en fazla 3 kere olmak üzere ZORLAMA SORGU paketi gönderirler. Bu paketi alan sınır düğümler de böylece saldırı altında olduklarını anlayabilmektedirler.



Şekil.4 Bir saldırı senaryosu

4. BENZETİM AYARLARI

Bu çalışmadaki tüm saldırgan türlerinin ve sunulan saldırı tespit algoritmasının benzetimi ayrık durum tabanlı OMNeT++ [8] benzeticisi yardımıyla gerçekleştirilmiştir. 100 adet normal düğüm 500x500 m^2 bölgeye rasgele dağıtılmış 1 adet sink düğümü merkeze yerleştirilmiştir. Farklı saldırgan sayısının saldırı tespit yönteminin performansını ne ölçüde etkilediğini görmek üzere normal düğümlerin %25, %50, %75 ve %100'ü oranında 4 farklı saldırgan kapsama oranı ile tüm benzetimler gerçekleştirilmiştir. Normal düğümler ile saldırgan düğümlerin güç kapasiteleri, güç tüketimleri, radyo iletim mesafeleri aynıdır ve MICA2 [10] düğümüne

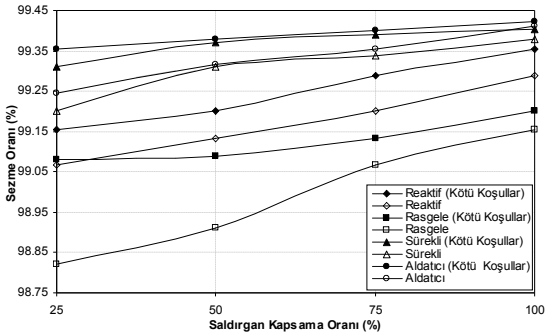
Algoritma. Gelişmiş bozma saldırı tespiti yöntemi.

```
if ((PTOn<PTOeş and ETMn>ETMeş) or (PTOn<PTOeş and HPOn>HPOeş))
  if (sorguSureciBasladi==FALSE)
     SorguGondermeyiDene();
     sorguSureciBasladi =TRUE
     sorguTimer(3*OrneklemePeriod)
     sorguCevapTimer(4*OrneklemePeriod)
  end if
else if (sorguTimerTasti==TRUE and sorguGonderildi==FALSE)
     SALDIRI=TRUE;
     if(gonderilenZorlamaSorgu<3)
        zorlamaSorguGonder(rasgeleZaman)
        zorlamaSorguGonderildi=TRUE;
     end if
else if(sorguCevapTimerTasti==TRUE)
        cevapPaketleriniDegerlendir();
else if (PTOn<PTOeş and HPOn<HPOeş and ETMn<ETMeş and zorlamaSorguAlindi==TRUE)
      SALDIRI=TRUE;
else if (PTOn<PTOeş and HPOn<HPOeş and ETMn<ETMeş and hedefDugumPTODusuk==TRUE)
      SALDIRI=TRUE;
else if (PTOn<PTOeş and HPOn<HPOeş and ETMn<ETMeş and !hedefDugumYasiyor and !zorlamaSorguAlindi)
      HATA=TRUE;
else if (PTOn > PTOeş)
      SALDIRI=FALSE;
end if
```

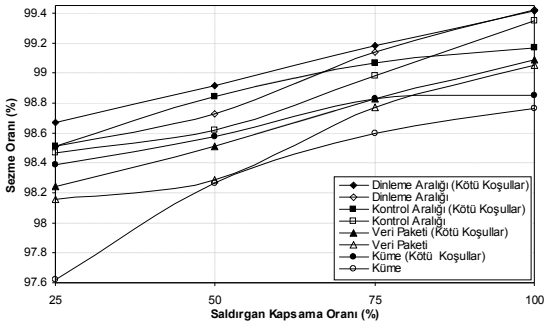
göre seçilmiştir. MAC katmanında S-MAC [2] protokolü kullanılmıştır ve dinleme süresi 100 msn, uyuma süresi 900 msn olarak (%10 duty cycle) ayarlanmıştır. Benzetimlerde paket üretimi, normal trafik için 1 pkt / 5 sn, yüksek trafik oranı için ise 2 pkt/sn olarak seçilmiştir. Hata durumlarını incelemek için toplam düğüm sayısının % 25'i oranında rasgele seçilen düğümler rasgele zamanda bozulmakta ve iletişim yapamaz hale gelmektedirler. İletim kanalındaki kayıpların benzetimini gerçekleştirebilmek üzere Gilbert-Elliott modeli olarak adlandırılan 2 durumlu ayrık Markov zinciri kullanılmıştır [12]. Tüm benzetimlerde paket teslim, hatalı paket oranları ve enerji tüketim miktarı sabit periyotlarla ölçülerek elde edilmektedir. Örnekleme periyodu olarak 60 saniye değeri seçilmiştir. Her bir benzetim için ilk olarak rasgele bir ağ topolojisi oluşturulmuş ve eşik değerlerinin tespiti için saldırı yokken 3600 sn boyunca ağın normal durum davranışları elde edilmiştir. Eşik değerleri elde edildikten sonra farklı saldırgan türlerini incelemek üzere 32400 sn daha benzetim devam etmiştir. Bu şekilde her bir benzetim en az 5 farklı topoloji ile tekrar edilmiş ve elde edilen sonuçların ortalaması sunulmuştur. Benzetimlerde kötü koşullar olarak adlandırılan senaryolar, kayıplı bağlantı koşulları, tıkanıklık ve düğümlerde hataların gerçekleştiği durumlardır.

5. BENZETİM SONUÇLARI

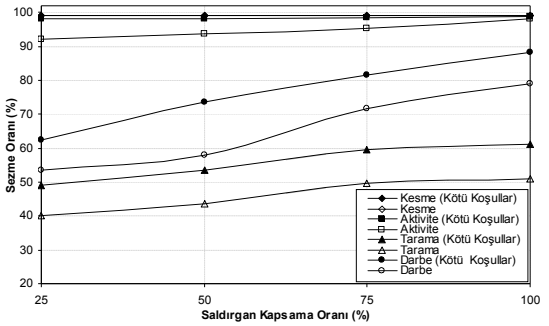
Sunulan saldırı tespit sisteminin başarımını ölçmek için farklı durumlardaki sezme oranları ve hatalı sezme oranları kullanılmıştır. Şekil 5, 6 ve 7'de tüm saldırganlar için farklı ağ koşulları ve farklı saldırgan kapsama oranlarındaki sezme oranları görülmektedir. Şekillerde dikkat edilecek hususlardan birincisi sezme oranlarının oldukça yüksek olmasına karşın %100 seviyesine ulaşamamasıdır. Bunun sebebi sorgulama sırasında en az 4 örnekleme periyodu boyunca saldırı tespit işlemi gerçekleştirilememesidir. Şekillerdeki ikinci önemli nokta ise saldırganlar tarafından kapsanan düğüm oranı arttıkça saldırı tespit oranlarının yükselmesidir. Bunun sebebi ise şekil 4'teki A düğümü gibi olan sınır düğüm sayısının azalmasıdır. Şekillerdeki bir diğer önemli husus da kötü bağlantı koşullarında (Kayıplı bağlantı, tıkanık ve hatalı düğümler senaryolarında) normal koşullara oranla daha yüksek sezme oranlarının gerçekleştirildiğidir. Bunun sebebi ise kayıplı bağlantı sonucunda SORGU/CEVAP paketlerinin bozulma oranının daha da artmasıdır. Tarama ve darbe saldırgan senaryolarının tespit değerleri diğer saldırganlar kadar yüksek değildir. Bunun sebebi ise bu iki saldırganın diğer saldırganlar kadar etkin olmaması ve ağa yeterince zarar verememesinden kaynaklanmaktadır.



Şekil.5 Reaktif, rasgele, sürekli ve aldatıcı saldırganlar için farklı şartlardaki sezme oranları.



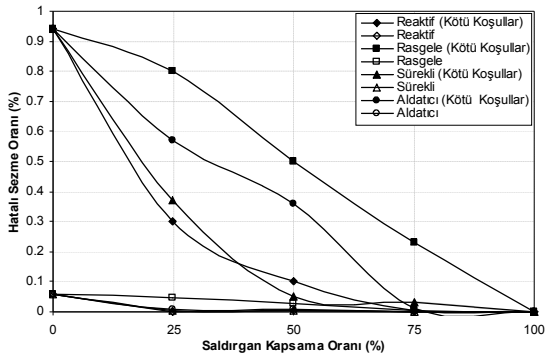
Şekil.6 Dinleme, kontrol aralığı, veri paketi ve küme saldırganları sezme oranları



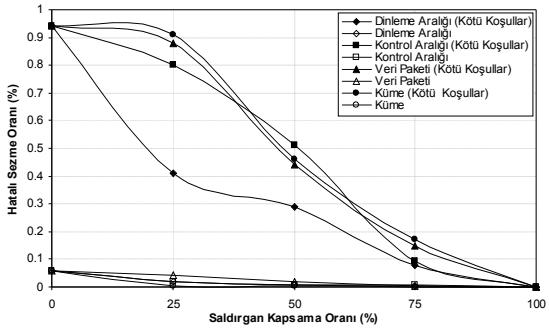
Şekil.7 Kesme, aktivite, tarama ve darbe saldırganları için farklı şartlardaki sezme oranları

Şekil 8, 9 ve 10'da tüm saldırganlar için farklı ağ koşulları ve farklı saldırgan kapsama oranlarındaki hatalı sezme oranları görülmektedir. Hatalı sezme oranlarında dikkat edilecek hususlardan birincisi kötü bağlantı koşullarında normal koşullara oranla daha yüksek hatalı sezme oranının gerçekleştiğidir. Bunun sebebi kayıplı bağlantı yüzünden PTO değerlerinin düşmesi, HPO değerlerinin de yükselmesidir. Ayrıca ağ içerisinde hatalı düğümlerin bulunması hatalı sezme oranlarının artmasına neden olmaktadır. Bir diğer önemli husus da saldırgan kapsama oranının artması ile hatalı sezme oranının düşmesidir. Saldırganlar tarafından doğrudan etkilenen düğüm sayısı arttıkça hatalı sezme tespitinde bulunan düğüm sayısı da azalmaktadır. Saldırgan kapsama oranının (SKO)

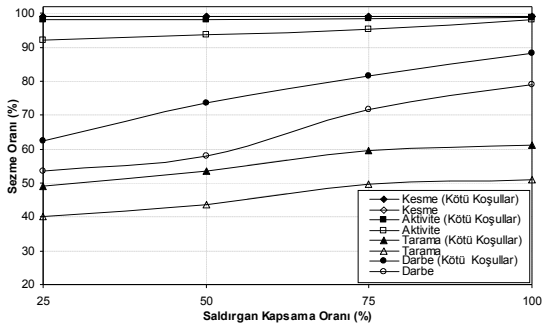
"0" olması aslında ağda hiç saldırgan bulunmaması manasına gelmektedir. Bu sebeple üç grafikte de SKO'nun "0" olduğu durumlardaki hatalı sezme oranları aynıdır. SKO'nun "0"dışındaki değerlerinde ölçülen hatalı sezme oranları saldırganlar tarafından kapsanmayan düğümlerin hatalı olarak gerçekleştirdiği saldırı tespit değerleridir.



Şekil.8 Reaktif, rasgele, sürekli, aldatıcı saldırganlar için hatalı sezme oranları



Şekil.9 Dinleme, kontrol aralığı, veri paketi ve küme saldırganları için hatalı sezme oranları



Şekil.10 Kesme, aktivite, tarama darbe saldırganları için hatalı sezme oranları

6. SONUÇLAR

Bozma saldırıları, çoğu zaman dış dünyada düşmanca koşullar altında çalışan ve sınırlı kaynaklara sahip olan kablosuz algılayıcı düğümleri için önemli bir tehdit unsurudur. Bu saldırıların üstesinden gelebilmenin ilk adımı saldırıları başarılı bir şekilde tespit edebilmekten geçmektedir. Bu makalede literatürde tanımlanmış olan bozma saldırılarının tespitine yönelik bir yöntem önerilmiştir. Geliştirilen yöntem ile birçok saldırgan türü yüksek tespit oranları ve düşük hatalı sezme oranları ile doğal ağ koşullardan ayrılabilmektedir. Yöntemin bir diğer üstünlüğü ise herhangi bir ek donanıma (DSP v.b) ihtiyaç duyulmadan günümüz kablosuz algılayıcı düğümleri üzerinde kullanılabilir olmasıdır. Bir sonraki çalışmada, sunulan saldırı tespit algoritmasını algılayıcı düğümleri üzerinde gerçekleyerek, gerçek ortam şartlarındaki başarımının ölçülmesi hedeflenmektedir.

KAYNAKLAR

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, Vol. 38, No. 4, pp. 393-422, March 2002.

[2] Wei Ye, J. Heidemann, Deborah Estrin. "An energy-efficient MAC protocol for wireless sensor networks," IEEE Infocom, pages 1567–1576, NY, June 2002.

[3] A. Wood, J. Stankovic, and S. Son., "JAM: A jammed-area mapping service for sensor networks," In 24th IEEE Real-Time Systems Symposium, pages 286- 297, 2003.

[4] A.D.Wood and J.A.Stankovic, "Denial of service in sensor Networks", IEEE Computer, 35(10):54–62, Oct.2002.

[5] 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, November 7, 2005, Virginia, USA.

[6] W. Xu, W. Trappe, Y. Zhang, and T. Wood. "The feasibility of launching and detecting jamming attacks in wireless networks", In ACM MobiHoc '05, page To appear. ACM Press, 2005.

[7] Y. Law, P. Hartel, J. den Hartog, and P. Havinga. "Link-layer jamming attacks on S-MAC," In 2nd European Workshop on Wireless Sensor Networks (EWSN 2005), pages 217–225. IEEE, 2005.

[8] www.omnetpp.org

[9] C. Hartung, J. Balasalle, and R. Han. "Node compromise in sensor networks: The need for secure systems"". Tech. Rep. Technical Report, CU-CS-988-04, Department of Computer Science, University of Colorado at Boulder, 2004.

[10] CrossBow Corporation, MICA2 Data Sheet, http://www.xbow.com.MICA2 data sheet

[11] Anthony D. Wood, John A. Stankovic, and Gang Zhou, "DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks", SECON 2007, June 2007, San Diego, California, USA

[12] En-Yi A. Lin, Jan M. Rabaey, Adam Wolisz "Power-Efficient Rendez-vous Schemes for Dense Wireless Sensor Networks", In Proceedings of ICC 2004, Paris, France

[13] CC1000,Low Power RF Transceiver Datasheet, http://focus.ti.com/lit/ds/symlink/cc1000.pdf