Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 26, No 4, 877-887, 2011

J. Fac. Eng. Arch. Gazi Univ.
Vol 26, No 4, 877-887, 2011

BOĞMA SALDIRILARINA KARŞI DİNAMİK KANAL ATLAMALI YENİ BİR GÜVENLİK YÖNTEMİNİN TASARIMI VE BAŞARIM ANALİZİ

Murat ÇAKIROĞLU[1], A. Turan ÖZCERİT[1], Özdemir ÇETİN[2]
[1] Bilgisayar Mühendisliği Bölümü, Teknoloji Fakültesi, Sakarya Üniversitesi, 54187, Sakarya, Türkiye
[2] Elektronik Öğretmenliği Bölümü, Teknik Eğitim Fakültesi, Sakarya Üniversitesi, 54187, Sakarya, Türkiye
{muratc, aozcerit, ocetin}@sakarya.edu.tr

(Geliş/Received: 01.02.2010; Kabul/Accepted: 08.08.2011)

ÖZET

Kablosuz algılayıcı ağlar, kullanım kolaylığı, düşük kurulum maliyeti ve esneklik gibi avantajları sebebiyle askeri, tıbbi, ticari v.b birçok alanda kullanılmaktadır. Ancak askeri uygulamalar, bina güvenlik sistemleri, hasta takip sistemleri gibi güvenliğin ön planda olduğu uygulama alanlarında kullanılan kablosuz algılayıcı ağlarının her türlü saldırılara karşı dayanıklı olması beklenir. Bir algılayıcı ağının güvenliğinden emin olabilmek için, boğma saldırıları gibi düğüm iletişimlerini tamamen ya da kısmen engelleyebilen saldırı türlerine karşı da dayanıklı olması ve saldırılara rağmen görevlerini yürütebilmesi gerekmektedir. Bu çalışmada, kablosuz algılayıcı ağları için önemli bir tehdit unsuru olan boğma saldırılarının çözümüne yönelik dinamik kanal atlamalı bir güvenlik yöntemi üzerinde odaklanılmıştır. Geliştirilen yöntem ile ağdaki düğümlerin yaklaşık olarak %96'sı saldırı tespitinden sonra 90-150 sn süre içerisinde ağ ile irtibatını yeniden sağlayabilmekte ve iletişimlerini yüksek başarımla devam ettirebilmektedirler. Ayrıca önerilen dinamik kanal atlamalı güvenlik sisteminin enerji tüketimi açısından düğümlere getirdiği ek yük en kötü koşullarda bile %11 civarındadır.

Anahtar Kelimeler: Kablosuz Algılayıcı Ağları, Boğma Saldırıları, Kanal Atlama, Güvenlik.

DESIGN AND EVALUATION OF A NEW SECURITY METHOD WITH DYNAMIC CHANNEL HOPPING FOR JAMMING ATTACKS

ABSTRACT

Wireless Sensor Networks (WSNs) are used in many fields such as military, medical, industrial applications since they provide several advantages like ease of use, lower installation cost, and flexibility. Their practical use will be prevailing in the future as the new application areas are discovered. However, in some areas, such as military applications, building security systems, and patient monitoring systems, the security considerations cannot be overlooked. In such applications, WSNs are expected to be robust against potential attacks. To be assured of secure operations of WSNs, they are also expected to operate their functions in some severe adversary conditions such as jamming attacks that can even block communication between sensor nodes completely. In this paper, we have focused on a dynamic channel hopping method that is used against jamming attacks. Despite jamming attacks, 96% of the nodes can be reconnected to the network in 90-150 seconds and they continue operate with high performance rates. In addition, the method we proposed imposes approximately 11% extra overhead even though in worst cases in terms of energy consumption.

Keywords: Wireless Sensor Networks, WSN, Jamming Attacks, Channel Hopping, Security.

1. GİRİŞ (INTRODUCTION)

Kablosuz algılayıcı ağlar, sınırlı kapasiteye sahip, kısa mesafede kablosuz ortam üzerinden haberleşebilen düşük güçlü ve maliyetli algılayıcı düğümlerinden meydana gelmektedir. 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 kadar çok çeşitli alanlarda kullanılabilmektedirler [1,21].

Algılayıcı ağlar, çoğu uygulama için dış ortamda ve zor koşullar altında çalışmaktadırlar. Bu sebeple, düğümlerin fiziksel hasara uğrama riski diğer ağlara nazaran çok daha yüksektir. Örneğin, kötü niyetli kişiler tarafından düğümlerin kriptografik anahtarları öğrenilebilir, yazılımsal değişiklikler yapılarak düğümler saldırgan hale çevrilebilir [2]. Algılayıcı ağlardaki bu tür güvenlik açıkları çeşitli saldırı türlerinin geliştirilmesini de kolaylaştırmaktadır. Boğma türündeki hizmet engelleme (Jamming Style Denial of Service –J-Dos) saldırıları kablosuz iletim ortamındaki paketlerin bozulmasını ve böylece düğümlerin iletişimlerinin aksamasını ya da tamamen engellenmesini hedefleyen saldırı türüdür [3,4,5].

Kablosuz algılayıcı ağlarda boğma saldırılarının çözümüne yönelik olarak literatürde çeşitli çalışmalar önerilmiştir. Geliştirilen ilk çalışmada [9] saldırıların varlığını tespit ettikten sonra bu saldırıların kapsadığı alanı tayin ederek yönlendirme yollarının değiştirilmesini öngören protokol tasarımı gerçekleştirilmiştir. Bu protokolün en zayıf yönü ağın ancak belli bir kısmının boğma saldırılarına maruz kaldığının varsayılmasıdır. Ağın tamamının saldırı altında olması durumunda herhangi bir saldırı bölgesinin belirlenmesinden ve yönlendirme yollarının değiştirilmesinden söz edilemez. Xu ve diğerleri boğma saldırılarına yönelik olarak frekans atlama metodunun adaptif bir şekli olan ve "kanal sörfü" olarak adlandırılan bir yöntem geliştirmişlerdir [10]. Bu yöntemin en önemli dezavantajı ise tarama saldırganı gibi kanallar arası çalışan saldırgan türlerine karşı başarımlarının düşmesidir. Xu ve diğerleri gerçekleştirdikleri bir diğer çalışmada düğümlerin saldırı bölgesinden uzaklaşarak ağ ile yeniden irtibata geçmesi esasına dayanan "Uzaysal geri çekilme" metodunu önermişlerdir [11]. Ancak bu yöntemde, düğümlerin gezgin olduğu varsayılmaktadır. Günümüzde algılayıcı düğümlerinin çoğu uygulama için gezgin olmaması bu yöntemin en zayıf tarafıdır.

Çakıroğlu ve diğerleri [12] tarafından gerçekleştirilen çalışmada reaktif, rasgele, aldatıcı, sürekli ve periyodik küme saldırganı için ekstra uyuma, dinleme süresinin azaltılması ve periyot kaydırma yöntemleri önerilmiştir. Ancak bu yöntemler kesme saldırganı gibi enerjisini verimli kullanan zeki saldırgan türlerine karşı elverişli değildir.

Cagalj ve diğerleri kablosuz algılayıcı ağlarda boğma saldırıları için solucan deliği esasına dayanan üç çözüm yöntemi önermiştir [13]. Bu yöntemlerde, saldırıya uğrayan düğümlerin hayati bilgileri bir an önce saldırıdan uzak düğümlere nasıl aktarılacağı üzerine durulmuştur. Saldırı bölgesindeki bilgilerin diğer düğümlere aktarılması için üç farklı solucan deliği önerilmiştir. Üç yöntemde de solucan delikleri olasılıksal olarak oluşturulmaktadır. Bu yöntemlerden ilk ikisinin en büyük dezavantajı ağın farklı tip düğümlerle (kablolu düğüm çiftleri ve frekans atlama özelliğine sahip düğüm çiftleri) zenginleştirilme zorunluluğudur. Bu gereksinim, özellikle büyük ölçekli ağlarda maliyetin önemli ölçüde artmasına neden olacaktır. Üçüncü yöntemin en zayıf tarafı ise makul bir çözümün sağlanabilmesi için ağdaki düğümlerin oldukça fazla iletişim kanalına sahip olma zorunluluğudur (40 kanaldan fazla). Bu yöntemin bir diğer zayıf tarafı ise ağ içerisinde bazı düğümlerin sürekli kanallar arasında dinleme yaparak bilgilerin saldırı bölgesinden uzaklaştırması görevini üstlenmesidir.

Wood ve diğerleri geliştirdikleri dört boğma saldırgan türü için farklı çözüm yöntemleri önermiştir [8]. "Çerçeve maskeleme", "kanal atlama", "paket bölümleme" ve "fazladan kodlama" olarak adlandırılan yöntemlerin her birisi bir saldırı türüne yönelik olarak geliştirilmiştir. Geliştirilen bu yöntemlerin en zayıf yönleri; her saldırgan türüne uygulanabilir olmamasıdır. Örneğin çerçeve maskeleme ve fazladan kodlama yöntemleri sürekli, reaktif saldırgan gibi saldırgan türlerine karşı yetersiz kalmaktadır. Kanal atlama ve paket bölümleme yöntemleri ise sadece küme başı ile normal düğüm arasındaki gibi tek bir alıcı-verici arasındaki haberleşmeyi sağlamak üzere geliştirilmiştir. Bu yöntemler çok atlamalı haberleşme koşullarına uygun değildir.

Bu çalışmada literatürde sunulan boğma saldırgan modellerine karşı mevcut kanal çeşitliliğinden faydalanılmasını sağlayan dinamik kanal atlamalı güvenlik yöntemi tasarımı gerçekleştirilmiştir. Sunulan yöntemin katkıları:

- Literatürde bulunan farklı özelliklerdeki birçok boğma saldırgan modeline karşı düğümlerin yüksek başarımlı olarak iletişimlerine devam etmesine olanak sağlamaktadır.
- Kablosuz algılayıcı ağın kısa süre içerisinde saldırılara rağmen yeniden görevlerini yerine getirebilmesini mümkün kılmaktadır.
- Sınırlı kaynaklara sahip kablosuz algılayıcı düğümlerinin yapısına uygun olarak düşük enerji tüketim fazlalığına sahip olmasıdır.

Makalenin geri kalan kısımları şu şekilde düzenlemiştir. 2.Bölüm'de kablosuz algılayıcı ağları için önemli bir tehdit unsuru olan boğma saldırgan modelleri hakkında kısaca bilgi verilmiştir. 3.Bölümde boğma saldırıları için önerdiğimiz dinamik kanal atlama güvenlik yönteminin detayları açıklanmış ve 4. Bölümde geliştirilen yöntemin benzetim yoluyla gerçekleştirilen başarım analizleri

sunulmuştur. Çalışmadan elde edilen sonuçlar Bölüm 5'de irdelenerek makale sonuçlandırılmıştır

2. BOĞMA SALDIRGAN MODELLERİ (JAMMING ATTACK MODELS)

Literatürde fiziksel ve ortam erişim katman fonksiyonlarını etkileyen çeşitli saldırgan modelleri bulunmaktadır. Xu ve diğerleri [4,5] sürekli, aldatıcı, rasgele ve reaktif olmak üzere dört saldırgan modeli tanımlamıştır. Law ve diğerleri S-MAC [14] protokolü için dinleme aralığı, kontrol aralığı, veri paketi ve küme saldırganı olmak üzere enerji-etkin 4 saldırgan modeli önermiştir [6,7]. Wood ve diğerleri [8] ise kesme, aktivite, tarama ve darbe saldırgan modellerini geliştirmişleridir

3. BOĞMA SALDIRILARINA KARŞI ÖNERİLEN DİNAMİK KANAL ATLAMALI SAVUNMA YÖNTEMİ (THE PROPOSED DYNAMIC CHANNEL HOPPING DEFENSE METHOD AGAINST JAMMING ATTACKS)

Dinamik Kanal Atlama (DKA), düğümlerin boğma saldırılarından kurtulabilmesi için kanal çeşitliğinden faydalanmasını sağlayan bir yöntemdir. Günümüzdeki ticari düğümlerden olan MICA2, 500Khz genişliğinde 26 adet, MICAz düğümü ise 5 Mhz genişliğinde 16 adet girişimsiz kanala sahiptir. DKA metodu bu kanal farklılıklarından faydalanarak düğümlerin saldırıların olumsuz etkilerinden kurtulabilmesini hedeflemektedir. Önerilen bu yöntem, saldırıların başarılı bir şekilde tespit edilmesinden sonra düğümlerin farklı bir iletişim kanalına atlayarak ağ ile yeniden irtibata geçebilmelerini öngörmektedir.

Sürekli kanal değiştirme, kanal çoğullama işlemleri sebebiyle düğümlerin güç tüketiminin artmasına ve düğümler arasındaki senkronizasyonun sağlanabilmesi için de fazladan paket trafiğine neden olmaktadır. Güç tüketimi, kablosuz algılayıcı ağlarda ağ ömrünü belirleyen önemli bir tasarım ölçütü olması sebebiyle DKA yönteminde saldırgan türüne göre uygun olan bir yöntem seçilmektedir. Saldırganlar kanallar arası gezerek saldırmıyorsa, düğümler saldırının olmadığı geçerli bir başka kanala atlamakta ve ağ ile yeniden irtibata geçerek sürekli bu kanalda kalmaktadır. Eğer saldırganlar farklı kanallar arasında gezebiliyorsa, düğümler mevcut kanallar arasında rasgele dolaşarak iletişimlerini gerçekleştirmektedir.

Düğümlerin hangi zaman aralıklarında ve ne şekilde kanallar arasında gezeceği, düğümler arasındaki irtibatın hızlı bir şekilde yeniden nasıl kurulacağı gibi detayların daha anlaşılabilir bir şekilde sunulabilmesi için DKA yönteminde gerçekleştirilen görevler farklı aşamalarla ifade edilmiştir.

3.1. Saldırı Tespiti (Attack Detection)

Saldırı tespit işlemi, saldırı tespit biriminin görevi olmasına karşın DKA'nın çalışmasını tetikleyen bir işlem basamağıdır. DKA yöntemi, saldırı tespit biriminden gelen "Saldırı Var" sinyali ile aktif hale geçmekte aksi durumda ise pasif olarak beklemektedir. Bu çalışmada, boğma saldırılarını tespit etmek için daha önceki çalışmalarımızda gerçekleştirdiğimiz [15,20] yöntem kullanılmıştır.

3.2. Kanal Atlama ve Komşularla İrtibatın Yeniden Sağlanması (Channel Hopping and Reconnection with the Neighbors)

Saldırıların tespit edilmesinden sonra DKA yöntemi devreye girmekte ve düğümler saldırının etkilerinden kurtulmak üzere merkez kanaldan mevcut kanallar içerisindeki en son sırada yer alan kanala atlayarak komşuları ile yeniden irtibata geçmeyi beklemektedir. Saldırı tespiti yapan düğümlerin mevcut en son kanala atlamasının sebebi düğümlerin kanalları sırayla gezen tarama saldırganı etkisinde olabilme ihtimalidir. Tarama saldırganı merkez kanaldaki iletişimin bittiğini anlayınca kanalları sıra ile taramaktadır. Dolayısıyla en son kanala gelene kadar belirli bir süre geçmekte ve bu süre zarfında düğümler yeni kanalda birbirleri ile haberleşebilmektedirler.

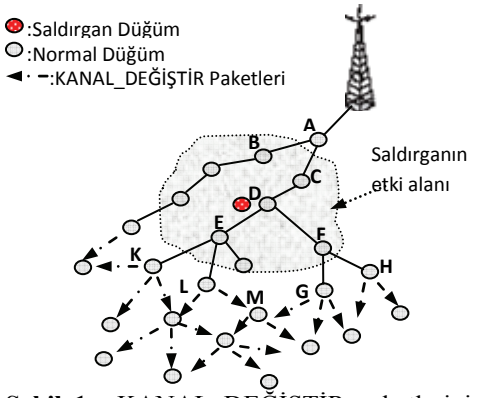
Kanal atlama işleminden sonra düğümler komşuları ile irtibata geçmeye çalışmaktadır. Bu çalışmada komşudan kastedilen ağaç tabanlı yönlendirme protokollerinde kullanıldığı gibi fiziksel komşuluktan ziyade mantıksal komşuluktur. Ağaç tabanlı yönlendirme protokollerinde çıkış düğümü (sink), ağacın kökünde bulunmakta ve düğümler ağacın köküne yani çıkış düğümüne ulaşmak için yönlendirme yolu üzerinde bulunan ve aralarındaki bağlantı kalitesinin en iyi olduğu komşusunu üst düğüm (parent node) olarak seçmektedir. Ayrıca düğümlerin paketlerini gönderdiği üst düğümleri olduğu gibi kendisini üst düğüm olarak seçen alt düğüm (child node) ya da düğümleri olacaktır. DKA yönteminde de düğümden kastedilen, fiziksel komşuluktan ziyade üst ve alt düğümlerdir.

Yeni kanala geçen düğümler komşuları ile irtibata geçebilmek için taşıyıcı sezme kurallarına da dikkat ederek belirli aralıklarla bu kanalda olduklarını gösteren küçük boyutlu işaret paketleri göndermektedir ve paketi alan düğüm de komşusuna cevap vermektedir.

3.3. Test ve Yayılma (Test and Propagation)

Merkez kanaldan en son kanala atlayarak komşuları ile irtibata geçen düğümler arasında belirli süreliğine test yayını başlar. Düğümler bu süre zarfında yeni geçtikleri bu kanalın da saldırıya maruz kalıp kalmadığını öğrenmeye çalışırlar. Eğer merkez

kanalda maruz kaldıkları saldırgan modeli sürekli, aldatıcı, rasgele, reaktif, dinleme aralığı, kontrol aralığı, veri paketi, kesme, aktivite ve darbe saldırganlarından birisi ise yeni kanalda yaptıkları test sonucunda bu kanalın temiz olduğunu anlayacak ve bu kanalda iletişimlerini devam ettireceklerdir. Ancak ağ içerisinde saldırıdan etkilenen ve onlara komşu olan düğümlerle geri kalan düğümler arasında kanal farklılığı sebebiyle iletişim kurulamayacaktır. Bu sorunu aşmak ve tüm ağın aynı kanala geçmesini sağlamak için kendisi bir saldırgan etkisinde olmayan ve komşularının yeni kanala geçtiğini bilen düğümler (sınır düğümler-K, L, G, H v.b), Şekil 1'de görüldüğü gibi test işleminden sonra yayın yaparak KANAL_DEĞİŞTİR paketlerini komşularına yaymaktadır. KANAL_DEĞİŞTİR paketinde atlanacak kanal bilgisi bulunduğu için böyle bir paket alan düğüm, paketin tüm ağa yayılabilmesi için bir kereye mahsus olmak üzere paketi yeniden yayınlamakta ve sonra yeni kanala geçmektedir.

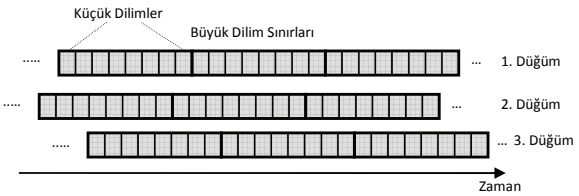


Şekil 1. KANAL_DEĞİŞTİR paketlerinin tüm ağa yayılması (Propagation of the CHANGE_CHANNEL Packets to Whole Network)

Eğer düğümlerin merkez kanalda maruz kaldıkları saldırgan türü tarama saldırganı ise düğümler merkez kanaldan mevcut en son kanala geçseler bile belirli süre içerisinde tarama saldırganı merkez kanalda iletişim olmadığını anlayacak ve kanalları taramaya başlayacaktır. Böylece düğümler yeni kanalda test aşamasındayken veya kalıcı iletişime başlamışken saldırarak ağı bozacaktır. Bu sebeple yeni kanala geçtiğinde yaptığı test sonucunda kanalın saldırıya maruz kaldığına karar veren düğümler, tarama saldırganın etkisi altında olduklarını varsayarak kanallar arasında rasgele dolaşmayı sağlayan Rasgele Kanal Atlama (RKA) algoritmasını çalıştıracaklardır.

3.4. Rasgele Kanal Atlama (Random Channel Hopping)

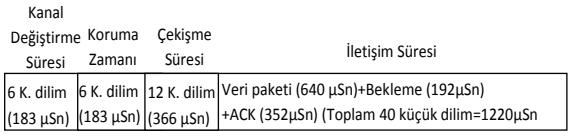
Boğma saldırısı sebebiyle merkez kanaldan farklı bir kanala atlayan düğümler, belirli bir süre sonra bu kanalın da saldırıya maruz kaldığını tespit ettiklerinde tarama saldırganının etkisi altında olduğunu varsaymaktadır. Bu durumda, düğümler saldırıdan kurtulmak için periyodik olarak ve sık aralıklarla kanallar arasında rasgele biçimde gezmeye başlarlar. RKA işlemi, yapılan test sonucunda düğümlerin yeniden saldırı etkisinde olduğunu tespit etmesi ile başlamaktadır. Bu yöntemde, düğümler mevcut kanallar arasında sözde rasgele sırada atlamaktadır. Kanallar arasındaki atlama zamanlarının belirlenmesi için zaman aralıkları, Şekil 2'de görüldüğü gibi McMAC [16] protokolünden esinlenerek küçük ve büyük dilimlere ayrılmaktadır. Küçük zaman dilimleri, kablosuz algılayıcı düğümünün gerçek zaman saatinin her bir tik atışına eş olarak seçilmiştir. Yani her bir küçük dilim 1/32768 saniyeye (30.5 µSn) karşılık gelmektedir. 64 küçük dilimden oluşan büyük dilimler ise 1952 µSn sürmektedir ve kanal değiştirme işlemi her büyük dilimin başlangıcında gerçekleşmektedir. Her düğüm kendine ait atlama zamanlamasını bağımsız bir şekilde seçmektedir ve Şekil 3'te görüldüğü gibi atlama sınırlarının eş zamanlı olması gerekmemektedir. Bu sebeple komşularından birisine paket göndermek isteyen düğüm, alıcı düğüm ile ortak bir kanalda buluşmalıdır. RKA yönteminde gönderici ile alıcı arasındaki buluşmayı gönderici belirlemektedir. Paket göndermek isteyen bir düğüm, alıcı düğümün hangi kanalda olduğunu tahmin ederek mevcut kanal atlama sırasını bırakmalı ve alıcı düğümün bulunduğu kanala geçmelidir. Bu kanalı dinledikten sonra eğer kanal boş ise alıcıya paketi göndermeli aksi takdirde kendi atlama sırasına dönmelidir. Gönderici düğüm yine aynı şekilde paket gönderimi bittiğinde kendi atlama sırasına dönmelidir.



Şekil 2. Rasgele kanal atlama zaman diyagramı (Timing Diagram of the Random Channel Hopping)

Şekil 3'de kanallar arasında atlamanın gerçekleştiği bir büyük dilimin detayları görülmektedir. Büyük dilimlerde kanal anahtarlama süresi olarak altı küçük dilim yani 183 µSn'lik bir süre ayrılmıştır. Birçok algılayıcı düğümde kullanılan CC2420 alıcı/verici tümdevresi yaklaşık olarak 132 µSn içerisinde bir kanaldan başka bir kanala geçebilmektedir [8]. Koruma zamanı ise alıcı düğüm ile verici düğüm arasındaki senkronizasyon hatalarını minimize etmek amacıyla kullanılmaktadır. Çekişme süresi farklı kanala geçerek bir alıcı düğüme paket gönderme sırasında çakışmayı en az indirmek için kullanılan süredir. İletişim süresi ise, veri paketi ve ACK'nın gönderilmesi için gerekli olan süredir. RKA yönteminde atlama süresini mümkün olduğunca kısaltmak için veri paket boyutları küçük seçilmiştir. Normalde 39 Bayt olan veri paketleri 20 bayt ile sınırlandırılmıştır. Ayrıca 802.15.4 mekanizmasının donanımsal olarak otomatik ACK gönderimi desteği

vermesi ile ACK iletimi için toplam 544 µSn süre gerekmektedir.

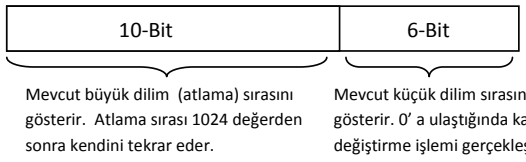


Şekil 3. Bir büyük dilimin ayrıntıları (The Details of A Big Slot)

Düğümler sözde rasgele atlama sırasını Formül 1 yardımıyla hesaplarlar. Formüldeki KS(n), n. büyük dilimdeki (n=1,2,…N) kanal sırasını, C ise mevcut kanal sayısını göstermektedir. $E_K(0)$, rasgele sayı üretecinin çekirdeğidir (seed) ve kanal sırası bu çekirdeğe göre üretilmektedir. Ayrıca çekirdek tüm düğümler tarafından paylaşılan bir paylaşımlı *K* anahtarı ile şifrelenmektedir. Dolayısıyla komşularının kanal atlama sırasını belirleyen çekirdek değeri ile şu anda hangi kanalda olduğunu bilen bir düğüm bir sonraki kanal sırasının ne olacağını da tahmin edebilmektedir.

$$KS(n) = E_K(n-1) \bmod C \quad (1)$$

RKA algoritmasında gönderici düğüm, alıcı düğümün hangi kanalda olduğunu gönderici ile alıcı arasında paylaşılan çekirdek bilgisi ve yerel saat bilgisi yardımıyla tahmin etmektedir. Her düğüm saat tiklerinde artan 16-bitlik bir yerel saat zamanlayıcısına sahiptir. Şekil 4'de görüldüğü gibi bu zamanlayıcının düşük değerlikli 6 biti düğümün ne zaman kanal değiştireceğini başka bir deyişle mevcut küçük dilimini, geri kalan 10 bit ise büyük dilim sırasını göstermektedir. Bir büyük zaman diliminin 64 küçük dilimden meydana gelmesi sebebiyle büyük dilimlerin değişmesi en düşük değerlikli 6 bit'e (2^6 =64) bağlıdır. Atlama sırası ise 2^{10} = 1024 değerden sonra kendini tekrar etmektedir.



Şekil 4. Düğümlerde bulunan yerel saat (Local Clock in the Nodes)

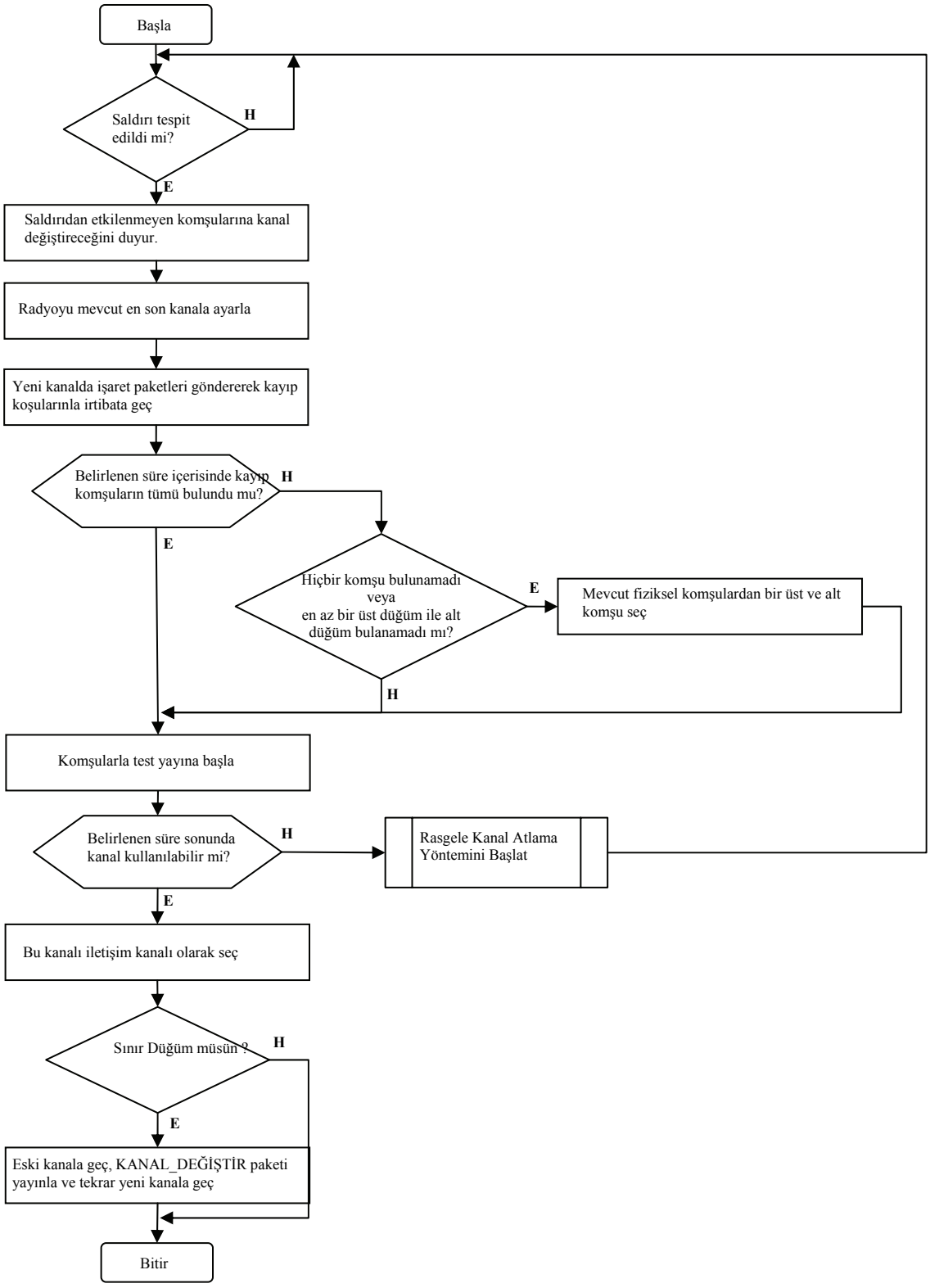
Yeni kanala geçildiğinde komşu düğümlerle irtibatın sağlanması sırasında paylaşılan yerel saat ve çekirdek bilgileri sayesinde rasgele kanal atlamasına başlayan düğümler 1-atlama uzaklıktaki komşularının ne zaman hangi kanalda olduğunu tahmin edebilmektedir. Yeni kanalda komşudan bir paket alan düğüm, bu komşusunun çekirdek bilgisini ve yerel saat bilgisini kendine ait komşu tablosuna kaydetmektedir. Ayrıca rasgele kanal atlama işleminin başlamasıyla birlikte düğümler belirli aralıklarla yerel saat bilgilerini paylaşarak bu bilgilerin güncel tutulmasını sağlamaktadır.

3.5. Senkronizasyon (Synchronization)

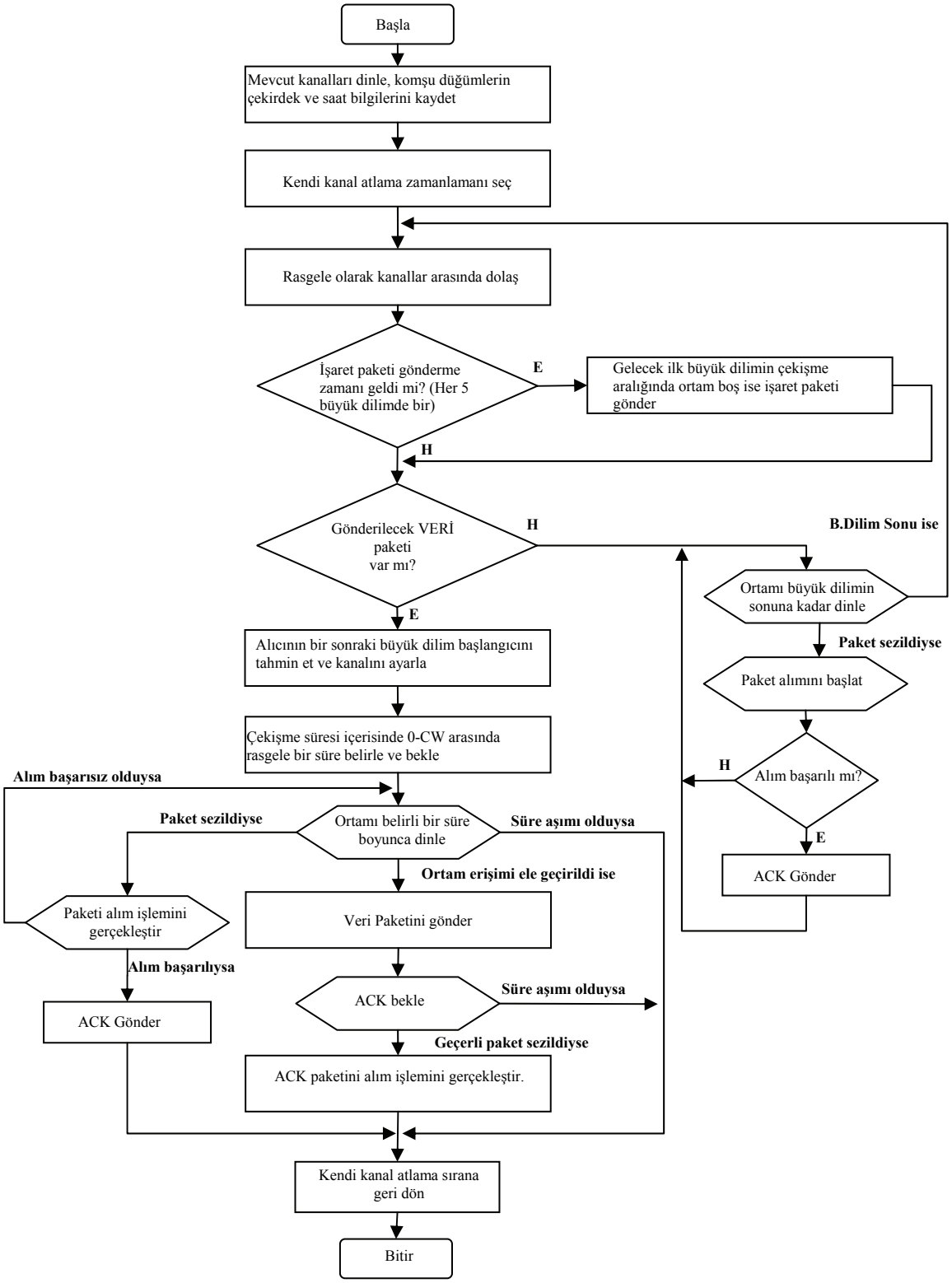
RKA metodunda düğümler birbirlerinin yerel saat ve çekirdek bilgileri yardımıyla komşularının gelecekteki atlama sıralarını tahmin edebilmekte ve böylece paket gönderimi sırasında aynı kanalda buluşmaktadırlar. Bir komşusundan yerel saat bilgisini alan bir düğüm, alınan saat bilgisi ile kendi saatini karşılaştırarak komşusunun atlama zamanlarını tespit edebilmektedir. Ancak düğümler arasındaki saat tiklerinin atış hızlarındaki farklar, küçük de olsa belirli bir süre sonra büyümekte ve düğümler arasında kanal atlama sürelerinin senkronizasyonunu bozulabilmektedir. Örneğin, gönderici düğüm alıcı düğümün kanalına geçtiğinde, alıcı düğümün yerel saatinin göndericiye oranla daha hızlı çalışması neticesinde mevcut kanalda iletişim mümkün olmayabilir. Bu sebeple, gönderici ile alıcı arasındaki saat farklarını gidermek için ikili (pair-wise) zaman senkronizasyon protokolüne ihtiyaç duyulmaktadır. Literatürde çeşitli senkronizasyon protokolleri bulunmaktadır. RKA metodunda da alıcı/verici arasındaki senkronizasyonu sağlamak için pratik senkronizasyon tekniğinden faydalanılmıştır [17]. Bu yöntemde, düğümler arasındaki saat sapma oranı, özyinelemeli en küçük kare yöntemi ile tespit edilmekte ve düğümler belirli aralıklarla paylaşılan senkronizasyon paketleri yardımıyla aralarındaki senkronizasyonu güncel tutmaktadır.

3.6. Kanal tahsisinin planlanması (Planning of Channel Allocation)

RKA yönteminde bir paket göndermek isteyen düğüm ilk önce göndermeyi hedeflediği komşusunun bir sonraki büyük zaman dilimine ne zaman başlayacağını ve hangi kanalda olacağını tahmin etmesi gerekmektedir. Alıcının büyük dilim başlangıç zamanı gelince, kendi kanal atlama sırasında alıcının olduğu kanala atlamalı ve çekişme süresi içerisinde (0-CW) rasgele seçtiği süre boyunca beklemelidir. Bu süre sonunda iletişim kanalını dinlemeli ve meşgul ise kendi atlama sırasına geri dönmelidir. Eğer kanal boş ise paketi göndererek ACK beklemeli ve zamanı gelince yine kendi atlama sırasına dönmelidir. RKA metodunda paket göndermesi gerekmeyen düğümler ise muhtemel bir alım işlemi için dinlemede kalmaktadır.



Şekil 5. DKA yönteminin genel akış diyagramı (The Flowchart of DCH Method)



Şekil 6. RKA algoritmasının akış diyagramı (The Flowchart of Random Channel Hopping Algorithm)

3.7. Dinamik Kanal Atlama Yönteminin Özeti (Summary of Dynamic Channel Hopping-DCH Method)

Belirli aşamalardan meydana gelen Dinamik Kanal Atlama yönteminin anlaşılmasını kolaylaştırmak için Şekil 5 ve 6'da akış diyagramları verilmiştir. Şekil 5'de dinamik kanal atlama yönteminin genel akış diyagramı görülmektedir. Saldırı tespitinde bulunan düğüm, saldırıdan etkilenmeyen komşularını kanal değiştireceğinden haberdar ederek mevcut en son kanala geçmekte ve yeni kanalda komşuları ile irtibata geçmeye çalışmaktadır. Düğüm komşularla irtibatını sağladıktan sonra test yayınına başlamakta ve kanalın yeniden bir saldırıya uğrayıp uğramadığını tespit etmektedir. Eğer kanalın bir saldırgan tarafından bozulduğu tespit edilirse, RKA algoritması çalıştırılmakta aksi durumda ise yeni kanal, iletişim kanalı olarak seçilmekte ve sınır düğümler tarafından seçilen bu kanal ağdaki tüm düğümlere duyurulmaktadır. Şekil 6'da ise DKA yönteminin bir alt metodu olan Rasgele Kanal Atlama algoritmasının akış diyagramı görülmektedir. Yeni kanala atlamasına rağmen bu kanalın da saldırıya uğradığını tespit eden düğümler rasgele kanal atlama algoritmasını çalıştırmaktadır. Bu algoritmada, düğümler ilk olarak mevcut kanalları belirli süre boyunca dinleyerek daha önce kanal atlamaya başlamış olan komşularının çekirdek ve yerel saat bilgilerini gönderilen işaret paketlerinden almakta ve kaydetmektedir. Tüm kanalları dinlendikten sonra, düğüm kendi zamanlamasını seçmekte ve rasgele kanal atlamaya başlamaktadır. Rasgele kanal atlamaya başlayan düğümler her beş büyük dilimde bir olmak üzere işaret paketi göndermelidir. Çekirdek ve yerel saat bilgilerini içeren bu paketler, kanal atlamaya yeni başlayan veya komşuları ile senkronizasyonunu kaybeden düğümlerin yeniden senkronize olmasını sağlamaktadır. RKA yönteminde, bir düğümün paket göndermesi gerektiğinde ilk olarak alıcı düğümün en yakın büyük zaman diliminin başlangıcı tayin edilmeli ve bu zaman diliminde o kanala atlanmalıdır. Daha sonra da çekişme için rasgele bir süre beklenmeli ve bu süre sonunda kanal boş ise paket alıcıya gönderilmelidir. Gönderilen paketin ardından ACK gelmesi beklenmeli ve kendi atlama sıralamasına geri dönülmelidir.

4. DİNAMİK KANAL ATLAMA YÖNTEMİNİN BAŞARIM ANALİZİ (PERFORMANCE EVALUATION OF DYNAMIC CHANNEL HOPPING METHOD)

Boğma saldırılarına karşı olarak geliştirilmiş olan Dinamik Kanal Atlama yönteminin başarım analizi detaylı benzetimler yardımıyla gerçekleştirilmiştir. Başarım analiz ölçütleri olarak, geliştirilen yöntemin saldırılara karşı ne kadar sürede cevap verebildiğini gösteren *cevap süresi*, düğümlerin saldırılara rağmen iletişimlerini hangi ölçüde devam ettirebildiğini gösteren *başarım oranı* ve önerilen DKA yönteminin düğümlerin enerji tüketimlerine getirdiği fazlalığı gösteren *enerji tüketim fazlalığı* parametrelerinden faydalanılmıştır. Benzetimlerde, DKA yöntemi anomali tabanlı saldırı tespit sistemi ile beraber kullanılmış [15] ve benzetimler OMNET++ [18] tabanlı benzetim yazılımı ile gerçekleştirilmiştir.

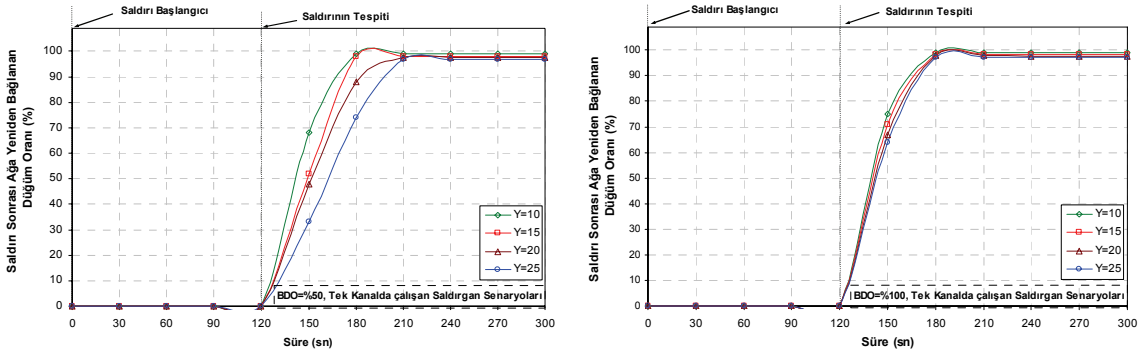
Tüm benzetim senaryolarında normal düğümler ile saldırgan düğümlerin güç kapasiteleri, güç tüketimleri, radyo iletim mesafeleri MICAz [19] düğümüne uygun olarak seçilmiştir. Geliştirilen yöntemin farklı düğüm yoğunluklarındaki başarımını belirleyebilmek için iletişim mesafesi r olan N=100 adet normal düğüm, uzunluğu ℓ olan bir kare alana, Formül 2 yardımıyla istenilen düğüm yoğunluğuna (Y) göre [6] rasgele olarak dağıtılmıştır. Bir adet çıkış (sink) düğümü ise merkeze yerleştirilmiştir.

$$Y = \sqrt{\frac{N.\pi}{\ell}}r \tag{2}$$

DKA yönteminin farklı saldırgan koşullarındaki başarımını ölçmek için ise toplam düğümlerin %50'sinin (Boğulmuş Düğüm Oranı=% 50) ve %100'nün (Boğulmuş Düğüm Oranı=% 100) saldırılara maruz kaldığı varsayılmıştır. Tarama saldırganın aslına uygun olarak bir kanalı 262 µSn'de tarayabildiği kabul edilmiştir. Her bir benzetim 36000 sn boyunca en az beş farklı topoloji ile tekrar edilmiş ve elde edilen sonuçların ortalaması sunulmuştur.

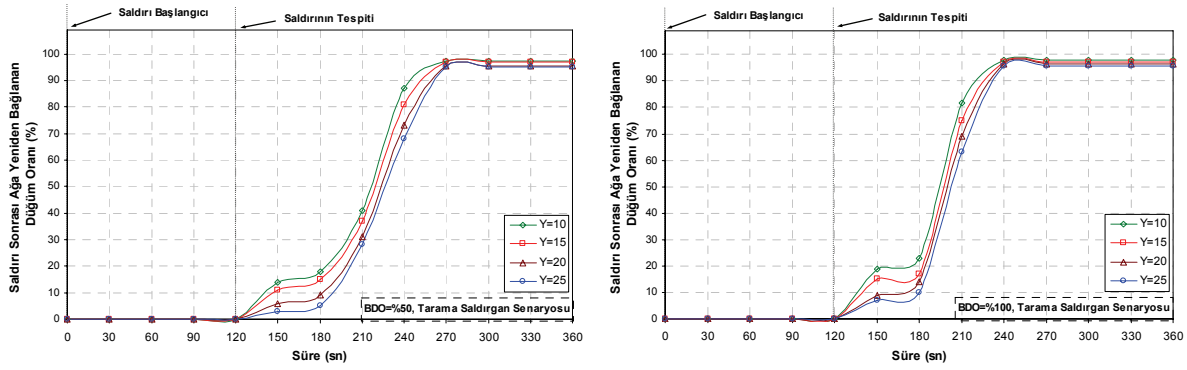
4.1. Cevap süresi (Response Time)

Şekil 7'de DKA yönteminin farklı ağ yoğunluklarında ve boğulmuş düğüm oranlarında, tek kanal frekansında çalışan saldırgan modellerine verdiği cevap süreleri görülmektedir. Tek kanal frekansında çalışan saldırgan türlerinden kastedilen sürekli, aldatıcı, rasgele, reaktif, dinleme aralığı, kontrol aralığı, veri paketi, küme, kesme, aktivite ve darbe saldırganlarıdır. Benzetimlerde düğümlerin 120. saniyeden sonra saldırı etkilerinden kurtulmaya başladığı görülmektedir. Bunun sebebi, kullandığımız saldırı tespit sisteminin saldırılar başladıktan 120 saniye sonra tespit işlemlerini bitirmesidir. Boğulmuş düğüm oranının %50 olduğu Şekil 7.a' da tüm ağın saldırı etkilerinden kurtulması yaklaşık olarak saldırı tespit edildikten 90 saniye sonra gerçekleşmektedir. Bu süre kanal değiştirme, komşular ile irtibata geçme, test işlemi ve KANAL_DEĞİŞTİR komutunun ağa yayılması gibi işlemlerden kaynaklanmaktadır. Boğulmuş düğüm oranının %100 olduğu Şekil 7.b'de ise tüm ağın saldırı etkilerinden kurtulması saldırılar tespit edildikten yaklaşık 60 saniye sonunda gerçekleşmektedir. BDO=100 iken düğümlerin saldırı etkilerinden daha çabuk kurtulmasının sebebi ağdaki tüm düğümlerin aynı zamanda saldırı tespiti yaparak kanal değiştirmesinden kaynaklanmaktadır. Böylece yeni kanalda komşularla irtibata geçme BDO=50 olması durumuna oranla daha çabuk sağlanmaktadır.



a) **b)**

Şekil 7. BDO=50 ve BDO=100 iken tek kanal frekansında çalışan saldırgan senaryoları için DKA yönteminin saldırılara verdiği cevap süresi. (The Response Time of DCH Method in Single Channel Jammers Scenarios-Jammed Node Ratio=50% and 100%)



a) **b)**

Şekil 8. BDO=50 ve BDO=100 iken kanallar arası çalışan saldırgan senaryoları için DKA yönteminin saldırılara verdiği cevap süresi. (The Response Time of DCH Method in Scan Jammer Scenarios-Jammed Node Ratio=50% and 100%)

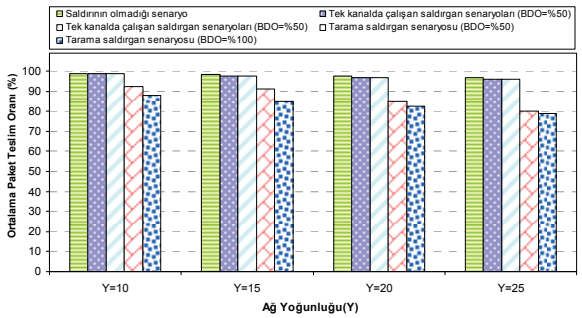
Grafiklerde dikkat edilecek hususlardan bir diğeri de ağ yoğunluğunun artması ile saldırı sonrası ağa yeniden bağlanan düğüm oranlarında da bir azalma olduğudur. Bunun sebebi, ağ yoğunluğun artması ile düğüm başına düşen komşu sayısının artması ve bazı düğümler ile irtibatın kurulmasında zorluk çekilmesidir.

Şekil 8'de DKA yönteminin farklı ağ yoğunluklarında ve boğulmuş düğüm oranlarında tarama saldırgan türüne karşı verdiği cevap süreleri görülmektedir. Bu grafiklerde de Şekil 7'de olduğu gibi yoğunluğun artması saldırı sonrası ağa yeniden bağlanan düğüm oranlarında bir azalmaya neden olmakta ve boğulmuş düğüm oranının fazla olması saldırıya verilen cevap süresini kısaltmaktadır. DKA yönteminin tek kanal frekansındaki saldırganlara verdiği cevap süresi ile tarama saldırganına verdiği cevap süreleri arasındaki en büyük fark, tarama saldırgan senaryosunda düğümlerin daha uzun süre sonra ağ ile irtibata geçebildiğidir. Bunun sebebi, düğümlerin test aşamasından sonra RKA metoduna başlamaları ve 1-atlama uzaklıktaki komşuları ile senkronize olmalarıdır.

4.2 Başarım oranı (Success Rate)

Şekil 9'da DKA yönteminin saldırı modellerine karşı elde ettiği başarım oranları görülmektedir. Başarım oranları geliştirilen yöntemin saldırılara cevap vermesinin ardından düğüm başına düşen ortalama paket teslim oranları ile ölçülmektedir. Şekillerde dikkat edilecek hususlardan birincisi DKA yönteminin tek kanalda çalışan saldırgan senaryolarında sağlayabildiği başarı oranının tarama saldırgan senaryosunda sağladığı başarıdan daha yüksek olmasıdır. Bunun sebepleri, RKA metodunu uygulayan düğümlerin bazılarının senkronizasyonu kaçırmaları ve tarama saldırganının bazı paketleri bozmasıdır. Şekillerdeki ikinci önemli nokta ise ağ yoğunluğunun artması ile DKA yönteminin tarama saldırgan senaryosundaki başarım oranının düşmesidir. Bunun nedeni de ağ yoğunluğunun artması ile düğümlerin komşu sayılarının artması ve neticede daha fazla çakışma olmasıdır. Şekillerdeki bir diğer önemli husus ise boğulmuş düğüm oranın %50'den %100'e yükselmesi yine DKA yönteminin tarama saldırgan türüne göre başarım oranını düşürmektedir. Bunun sebebi ise ağdaki artan tarama saldırgan sayısı ile düğümlerin paket bozulma ihtimallinin yükselmesidir. Sonuç olarak çoğu saldırı

senaryosunda düğümlerin teslim edebildiği paket oranları 0'a kadar düşmesine rağmen DKA yöntemi ile düğümler çoğu senaryo için paketlerin %80'ninden fazlasını teslim edebilmekte ve böylece iletişimlerine devam edebilmektedirler.



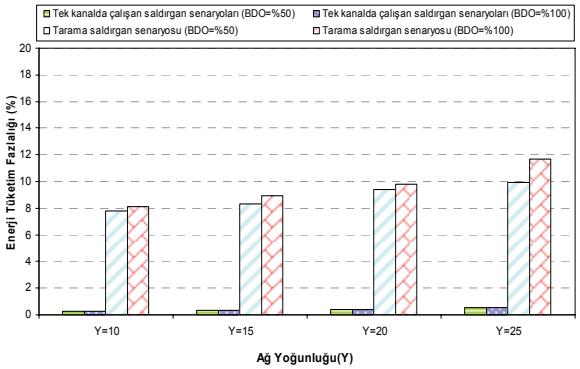
Şekil 9. Farklı ağ yoğunlukları ve boğulmuş düğüm oranlarındaki DKA yönteminin başarım oranı (The Success Rates of DCH Method in different network density and jammed node ratios)

4.3.Enerji tüketim fazlalığı (Energy Consumption Overhead)

Enerji tüketim fazlalığı (ETF), DKA yöntemi nedeniyle düğümlerin fazladan harcadığı enerji miktarını gösteren parametredir ve Formül 3 yardımıyla hesaplanmaktadır. Formüldeki $E_{Saldırı+DKA}$, düğümlerin saldırı altında ve DKA yöntemi aktifken harcanan enerji miktarını, $E_{SaldırıYok}$ ise düğümlerin bir saldırı etkisi altında olmadığında harcadığı enerji miktarını göstermektedir.

$$ETF = \frac{E_{Saldırı+DKA}}{E_{SaldırıYok}} \times 100 \qquad (3)$$

Şekil 10'da farklı senaryolarda bir düğümden elde edilen enerji tüketim fazlıkları görülmektedir. Şekildeki en önemli husus, tek kanal frekansında çalışan saldırgan senaryolarında DKA yönteminin neden olduğu enerji tüketim fazlalık değerleri çok düşük iken tarama saldırgan senaryosunda %8 ile %11 arasında olmasıdır. Bunun nedeni, tek kanal saldırgan senaryosunda düğümlerin farklı bir kanala atlayarak iletişimlerini bu kanalda sürdürmeleri, tarama saldırgan senaryosunda ise düğümlerin periyodik olarak kanallar arasında gezmesidir. Düğümlerin belirli aralıklarla kanal değiştirmesi ve aralarındaki senkronizasyonu sağlamak için senkronizasyon paketlerini göndermesi, DKA yönteminin tarama saldırgan senaryosunda neden olduğu enerji tüketim fazlalığının yüksek çıkmasına neden olmaktadır. Şekildeki bir diğer önemli husus ise ağ yoğunluğunun ve boğulmuş düğüm oranlarının artması ile tarama saldırgan senaryosundaki enerji tüketim fazlalık değerlerinin yükselmesidir. Ağ yoğunluğunun artması, düğümlerin komşu sayılarının artmasına ve düğümler arasında gönderilen senkronizasyon paket sayısının yükselmesine neden olmaktadır. Ayrıca tarama saldırısından etkilenen düğüm oranın artması ile düğümler arasındaki senkronizasyonu sağlayan paketlerin saldırganlar tarafından bozulma ihtimalini yükseltmekte ve bu sebeple senkronizasyonu korumak daha güçleşmektedir. Tüm bunlar çeşitli kontrol ve veri paketlerinin hatalı gönderimler sonucunda yeniden gönderilmesine ve böylece enerji tüketiminin artmasına yol açmaktadır.



Şekil 10. Farklı ağ yoğunlukları ve boğulmuş düğüm oranlarındaki enerji tüketim fazlalıkları (The Energy Consumption Overheads of DCH Method in different network densities and jammed node ratios)

5. SONUÇLAR (CONCLUSIONS)

Bu çalışmada, boğma saldırılarının etkisini en aza indirmek ve saldırılara rağmen düğüm iletişimlerinin devam edebilmesine imkân tanımak için düğümlerin var olan kanal çeşitliliğinden faydalanmasını sağlayan Dinamik Kanal Atlama (DKA) metodu geliştirilmiştir. Önerilen DKA yönteminde düğümler, saldırgan modelinin özelliğine göre çözüm yöntemini seçmektedir. Eğer düğümler tek kanal frekansında çalışan bir saldırganın etkisi altında ise merkez kanaldan geçerli olan en son kanala geçmekte ve bu kanalda kalarak iletişimlerini devam ettirmektedir. Ancak düğümler kanalları tarayarak saldıran bir saldırı modeline karşı çok kısa aralıklar ile var olan kanallar arasında rasgele şekilde atlamayı öngören Rasgele Kanal Atlama (RKA) algoritmasını kullanmaktadırlar. Geliştirilen DKA yöntemi yardımıyla düğümler oldukça kısa bir sürede (60–150 sn) saldırı etkilerinden kurtulabilmekte ve iletişimlerini çoğu senaryo için %80 değerinden daha yüksek bir başarım ile devam ettirebilmektedirler. DKA yönteminin enerji tüketimine getirdiği ek yük ise tek kanal frekansında çalışan saldırgan senaryolarında oldukça düşüktür. Tarama saldırgan senaryosundaki ek enerji yükü ise saldırının olmadığı normal koşullara oranla % 11 daha fazladır.

KAYNAKLAR (REFERENCES)

1. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci,"Wireless Sensor Networks: A Survey," **Computer Networks**, **Elsevier**, Cilt 38, Sayı 4, 393–422, Mart 2002.

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

3. A.D. Wood, J.A. Stankovic, "Denial of service in sensor networks," **IEEE Computer**, Cilt 35, Sayı 10, 54–62, Ekim. 2002.

4. W. Xu, W. Trappe, Y. Zhang, T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks", **In Proc. of ACM MobiHoc**, 46-57, 2005.

5. 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.

6. 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.

7. 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.

8. Anthony D. Wood, John A. Stankovic, Gang Zhou, "DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks", **SECON 2007**, Haziran 2007, San Diego, California, USA.

9. A. Wood, J. Stankovic, S. Son., "JAM: A jammed-area mapping service for sensor networks.", **24. IEEE Real-Time Systems Symposium**, 286 - 297, 2003.

10. W. Xu, A. T. Wood, W. Trappe,Y Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service", **in Proceedings of the 2004 ACM workshop on Wireless security**, 80-89, 2004.

11. W. Xu, A. T. Wood, W. Trappe,Y Zhang, "Channel Surfing: Defending Wireless Sensor Networks from", **IPSN'07 Cambridge**, 25-27, Massachusetts, USA, Nisan 2007.

12. M. Çakıroğlu, A.Turan Özcerit, "Denial Of Service Attack Resistant Mac Protocol Design For Wireless Sensor Networks", **J. Fac. Eng. Arch. Gazi Univ.**, Vol 22, No 4, 697- 707, 2007.

13. M. Cagalj, S. Capkun. J.-P. Hubaux, "Wormhole-Based Anti-Jamming Techniques in Sensor Networks", **IEEE Transactions on Mobile Computing,** Mayıs, 2006.

14. Wei Ye, J. Heidemann, Deborah Estrin, "An energy-efficient mac protocol for wireless sensor networks.", **IEEE INFOCOM**, USA, 1567–1576, Haziran 2002.

15. M. Çakıroğlu, A.Turan Özcerit, "Jamming Detection Mechanisms for Wireless Sensor Networks, **ACM Infoscale 2008**, Napoli, Italya, 4-6 Haziran 2008.

16. H. W. So, J. Walrand, J. Mo Jeonghoon, "McMAC: A Parallel Rendezvous Multi-Channel MAC Protocol", **IEEE Wireless Communications and Networking Conference**, **WCNC 2007**, 11-15 Mart 2007.

17. H. W. So, G. Nguyen, J. Walrand, "Practical synchronization techniques for multi-channel mac", **MobiCom '06: Proceedings of the he Twelfth Annual International Conference on Mobile Computing and Networking, ACM**, New York, USA, 2006.

18. **www.omnetpp.org**, OMNET++, Ayrık Olay tabanlı Simulator.

19. **Internet: Chipcon, CC2420 2.4GHz IEEE 802.15.4/ZigBee ready, RF Alıcı/Verici çalışma sayfası**, http://www.chipcon.com/files/CC2420_Data_Sheet_1_3.pdf

20. M. Çakıroğlu, A.T. Özcerit, "Design and Evaluation of a Query-based Jamming Detection Algorithm for Wireless Sensor Networks", **Turkish Journal of Electrical Engineering & Computer Sciences**, Cilt 19, Sayı 1, 1-19, Ocak 2011.

21. C. Bayılmış, et al.,"Development of Web-based Remote Monitoring System for Wireless Sensor Networks Using MATLAB Web Server", **J. Fac. Eng. Arch. Gazi Univ.** Vol 25, No 2, 371-379, 2010