Bilişsel Radyo Ağlarında Eşgüdümlü Saldırılar

Levent Altay[1,2], Gürkan Gür[1,2], Fatih Alagöz[2]

[1] Provus Bilişim Hizmetleri A.Ş., Progress Ar-Ge Merkezi, Ayazağa, İstanbul

[2] Boğaziçi Üniversitesi, Bilgisayar Mühendisliği Bölümü, İstanbul

levent.altay@provus.com.tr, gurkan.gur@provus.com.tr, fatih.alagoz@boun.edu.tr

Özet: Bilişsel radyo ağları (BRA) statik spektrum tahsisi sonucunda ortaya çıkan kanal yetersizliği problemine çözüm olarak öngörülmektedir. Dolayısıyla bilişsel radyo ağları yeni kablosuz uygulamalar ve hizmetlerinin ortaya çıkışıyla yoğunlaşan kablosuz ağ trafiğinin yarattığı ihtiyaçları karşılamak için hayati öneme sahiptir. Bununla birlikte, bilişsel radyo ağlarının pratik olarak kullanımının sağlanması ve yaşam ömürlerinin sürekliliği için güvenliklerinin sağlanması kritiktir. Bu nedenle, bu sistemlerin çalışabilmesi için yaşamsal önemi olan spektrum sezme mekanizmaları güvenlik açısından araştırılmak zorundadır. Bu çalışmada, bilişsel radyo ağlarında işbirlikçi spektrum sezme sistemine yönelik eşgüdümlü saldırılar tanımlanmakta ve analiz edilmektedir. İşbirlikçi spektrum sezmeye yönelik güven yönetimine dayalı bir adet karşı önlem önerilmektedir. Ayrıca, söz konusu sistemlerin eşgüdümlü saldırılardaki performanslarını göstermek amacıyla deneysel sonuçlar da sağlanmaktadır.

Anahtar Sözcükler: Bilişsel radyo ağları, işbirlikçi spektrum sezme sistemi, eşgüdümlü saldırılar.

Coordinated attacks on cognitive radio networks

Abstract: Cognitive radio networks (CRNs) are envisaged to alleviate the spectrum and capacity shortage aggravated by the static spectrum allocation. They are crucial for meeting the requirements of wireless traffic explosion emerging with new wireless applications and services. However, the security of CRNs is critical for their practical usage and widespread proliferation. Therefore, the fundamental mechanism of spectrum sensing in these systems has to be investigated from the security perspective. In this work, we define and analyze coordinated attack models for Cooperative Spectrum Sensing (CSS) in CRNs. We devise a simple yet effective countermeasure scheme based on trust management for cooperative sensing. We also provide experimental results to illustrate the performance of these systems under coordinated attacks.

Keywords: Cognitive radio networks, cooperative spectrum sensing, coordinated attacks.

1. Giriş

Yeni kablosuz ağ servisleri hayatımıza girdikçe kanal yetersizliği problemi spektrum yönetiminde karşılaşılan en büyük sorun haline gelmektedir. Bu problemle mücadele etmek için spektrumun paylaşımıyla ilgili çözümler ortaya konmuş olmasına rağmen yeterince etkin olamamaktadırlar. Oysaki *bilişsel radyo ağları (BRA)* etkin olarak kullanılmayan lisanslı spektrumların daha verimli kullanılmasına imkân vererek şu ana kadar kanal yetersizliği problemine yönelik en iyi çözüm olarak göze çarpmaktadır**[1]**.

Bilişsel radyo (BR) "kendi çalışma ortamını sezen ve bu ortam hakkında bilgi sahibi olan, bunlardan yararlanarak radyo çalışma parametrelerini dinamik olarak ayarlayabilen bir radyo veya sistem"**[2]** olarak tanımlanmaktadır. Bilişsel radyolar dinamik olarak spektruma erişim sağlamak maksadıyla;

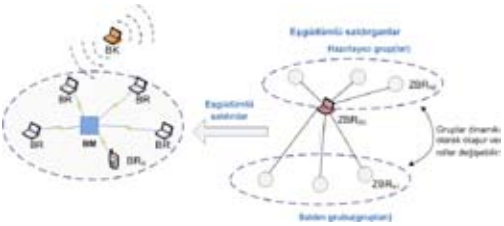
- *Spektrum sezme,*
- *Spektrum analizi,*
- *Spektrum değiştirme,*
- *Spektrum paylaşma*

işlevlerini *bilişim döngüsü* adı verilen süreçte yerine getirirler. Spektrum sezme, bilişim döngüsünü başlatan işlev olmasından dolayı diğer işlevlere nazaran daha fazla öneme sahiptir.

Spektrumun daha etkin kullanımı maksadıyla bilişsel radyolar boş veya daha az kullanılan kanalları belirlemek için *uyumlu filtreleme, dalga şekli tabanlı sezme, döngüsel durağanlık tabanlı sezme, enerji sezici tabanlı sezme* ve önerilmiş başka spektrum sezme yöntemlerini kullanmaktadırlar. Bahse konu yöntemleri kullanırken bilişsel radyolar (BR) hatalı sezme, yanılma veya kandırılmaya maruz kalabilmektedirler.

Bilişsel radyolar söz konusu problemlerin mevcut olduğu ortamlarda birincil kullanıcıların (BK) iletimine engel olmadan ve ikincil kullanıcılarla adil bir şekilde kanalları paylaşmak için ya tek başlarına ya da diğer bilişsel radyolarla beraber olarak spektrum sezme işlevini gerçekleştirirler. Bilişsel radyo ağlarında *işbirlikçi* (*kooperatif) spektrum sezme* (İSS) sistemi her bilişsel radyonun yerel olarak edindikleri sezme bilgileri veya kanalın boş veya dolu olmasına ilişkin kararlarının birleştirilerek kanalların kullanımıyla ilgili *genel karar*, alınması metodudur **[3].**

İSS sistemi beraberinde iletişim ek yüklerini de getirmektedir. Daha güvenilir sonuçlar alınmasına karşın yerel olarak elde edilen spektrum bilgilerinin gönderilmesinde, yerel kararların gönderilmesine nazaran daha fazla iletişim yükleri oluşmaktadır. İSS sistemi eğer ki yerel kararların gönderilmesine dayanıyorsa BM'nin vereceği genel karar VE, VEYA ve ÇOĞUNLUK yöntemleri kullanılarak alınmaktadır **[4]**. VE yöntemi uygulanıyorsa tüm yerel kararların kanalda birincil kullanıcının olduğuna yönelik olması gerekmekte, bir tane bile yerel karar kanal boş olarak gönderilirse genel karar kanalın boş olduğuna yönelik verilmektedir. VEYA yönteminde ise bir tane bile bilişsel radyo kanalda birincil kullanıcının olduğuna dair yerel karar gönderirse genel karar kanalın birincil kullanıcı tarafından kullanıldığı yönünde verilmektedir. ÇOĞUNLUK yönteminde ise belirlenmiş bir *k* değerinden daha fazla kullanıcının yerel kararı kanalın birincil kullanıcı tarafından kullanıldığına yönelikse genel karar da kanalın kullanıldığına yönelik olmaktadır. Anılan yöntemler bu bildirinin sonunda güvenlik açısından ayrıntılı olarak incelenmektedir.



Şekil 1 Saldırı ve önlem analizi için kullanılan model. ZBR_{SU} saldırgan bilişsel radyoları ZBR_{N1} ve ZBR_{N2} ise ZBR_{SU} ile eşgüdümlü saldırıya katılan hazırlayıcı ve saldırı gruplarını göstermektedir.

Zararlı bir amaç için bir araya getirilmiş ama tek tek ele alındığında saldırı olarak tespit edilemeyen eylemlerin toplamı *Eşgüdümlü saldırı* olarak tanımlanmaktadır **[5]**. Eşgüdümlü saldırı ya tek bir saldırgan tarafından sahte kullanıcılar yaratılarak ya da farklı saldırganların ortak bir amaç için eşgüdümlü olarak çalışmasıyla yapılmaktadır (Şekil 1). İSS sistemi doğası itibariyle eşgüdümlü saldırılara açık olmasına rağmen, yapılan literatür çalışmasında söz konusu mekanizmaya yönelik eşgüdümlü saldırıları inceleyen bir çalışmaya rastlanmamıştır. İşte bu sebeple bu çalışma İSS sistemine yönelik iki adet saldırı senaryosu geliştirmekte deneysel olarak bu saldırıları gerçeklemekte ve saldırıların etkisini azaltacak bir adet çözüm önerisini test etmektedir. Ayrıca çalışmanın sonunda farklı oylama mekanizmalarına yönelik analizler de bulunmaktadır.

Bildirinin ikinci bölümünde saldırıların test edileceği jenerik model açıklanmakta, üçüncü

bölümde iki adet saldırı senaryosu tanımlanmakta, dördüncü bölümde saldırı senaryoları ve çözüm önerisi test edilmekte ve beşinci bölümde diğer oylama mekanizızmalarına yönelik analizlerle bildiri sonlandırılmaktadır.

2. Bilişsel Radyo Ağlarında Güven Tabanlı İşbirlikçi Spektrum Sezme

Bu bölümde 3. bölümde detaylandırılan geliştirilmiş iki adet eşgüdümlü saldırı senaryosunun test edileceği ortam açıklanmaktadır. Bilişsel radyo ağımızda N adet bilişsel radyonun bulunduğunu varsayıyoruz. Bu N adet radyonun tamamı İSS sistemine katılmaktadır. Basitlik açısından sadece bir adet kanalın bulunduğunu kabul ediyoruz. Her bilişsel radyo sezme sonucunda birincil kullanıcının kanalda olması konusunda karar vermekte ve kararını Birleştirme Merkezi (BM)'ye göndermektedir. Eğer ki kararı kanalın meşgul olduğu yönündeyse gönderdiği karar biti 1 diğer türlüyse 0 olmaktadır. BM kendisine gönderilen tüm yerel kararları almakta ve ÇOĞUNLUK yöntemi kullanmaktadır. Bu çalışmada k değeri olarak $N/2$ seçilmektedir.

Kötü niyetli kullanıcıların veya hatalı karar gönderen bilişsel radyoların genel kararı etkilememesi maksadıyla BM her bilişsel radyonun gönderdiği yerel kararlara bir ağırlık uygulamaktadır. Bu ağırlıklar bilişsel radyoların verdikleri doğru veya yanlış kararlara göre ödül ve cezanın uygulanması sonucu ortaya çıkmaktadır. i'nci bilişsel radyonun Ödül skoru a_i, Ceza skoru p_i, katıldığı toplam karar verme sayısı s_i ve doğru karar verme sayısı r_i olmak üzere güven eşik değeri ε için Ödül ve Ceza skorları sırasıyla (1) ve (2) denklemleriyle hesaplanmaktadır.

$$a_i = \frac{\varepsilon}{s_i - r_i}$$

$$p_i = \frac{\varepsilon}{r_i} \qquad (1)\ (2)$$

Oylamaya katılan her bilişsel radyo için bir güven değeri t_i hesaplanmaktadır.

$$t_i = \begin{cases} \varepsilon, & s_i = 0 \\ \frac{r_i}{s_i}, & s_i \neq 0 \end{cases} \qquad (3)$$

İlk defa oylamaya katılan bir bilişsel radyo için güven değeri denklem (3) ile hesaplanırken güven değerlerinin güncellenmesi ise denklem (4) e göre yapılmaktadır.

$$t_i^{update} = t_{i-1} + a_i - p_i \qquad (4)$$

Her oylama öncesinde güven değerleri dikkate alınarak her bilişsel radyo için bir ağırlık w_i hesaplanmaktadır.

$$w_i = \begin{cases} 0, & t_i < \varepsilon \\ \frac{t_i}{\sum_{j=1, t_j \geq \varepsilon}^{N} t_j}, & t_i \geq \varepsilon \end{cases} \qquad (5)$$

(5) denklemine göre hesaplanan ağırlık değerlerine göre BM kanalın birincil kullanıcı tarafından kullanılıp, kullanılmadığına yönelik genel kararını denklem (6) yı kullanarak vermektedir.

$$D_{BM} = \begin{cases} H_1, & \sum_{i=1}^{N} w_i d_i \geq \frac{k}{N} \\ H_0, & diğer\ durumlar \end{cases} \qquad (6)$$

BM kanalın kullanım durumuna göre ya bilişsel radyoların kanalı terk etmesini veya adil bir şekilde kanalı kullanmalarını sağlamaktadır. Eğer ki yanlış karar sonucunda kanal etkin olarak kullanılmazsa veya birincil kullanıcıların kanalı kullanması engellenirse yanlış karar verilmesine sebep olan bilişsel radyolar cezalandırılmakta doğru karar verenlerse ödüllendirilmektedir. Güven değeri eşik değerinin altına düşen bilişsel radyoların ağırlıkları 0'a düştüğünden karar mekanizmasına ve kanal kullanımına katılamamaktadırlar.

Oluşturulan test ortamı **[6]** çalışması örnek alınarak oluşturulmuştur.

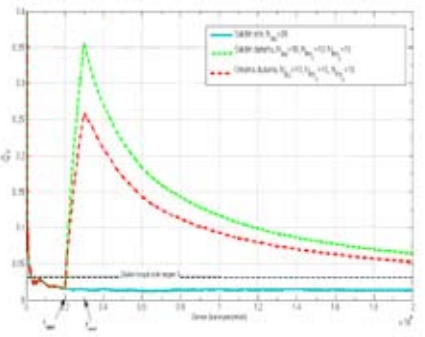
3. Bilişsel Radyo Ağlarında Eşgüdümlü Saldırı Modelleri

Eşgüdümlü saldırılarda her saldırganın saldırıya yönelik olarak rolleri bulunmaktadır. Eğer ki saldırganın rolü bulunulan ortamı saldırıya yönelik olarak hazırlamaksa *hazırlayıcı*, saldırıyı yapmak ise *saldırgan* olarak adlandırılmaktadır. Saldırganlar saldırıya yönelik olarak bu gruplardan en az birine veya ikisine de sahip olabilirler. Hazırlayıcı rolüne sahip olan saldırganların grubu hazırlayıcı grup (PG) ve saldırı rolüne sahip olan kullanıcılar ise saldırı grubu (EG) olmak üzere L adet PG alt grubu $|PG_l|=g_1$, $|PG2|=g_2$,.., $|PG_L|=g_L$ ve M adet EG alt grubu $|EG_l|=e_1$, $|EG_2|=e_2$,.., $|EG_M|=e_M$ şeklinde farklı sayıda saldırganlara sahip olabilirler.

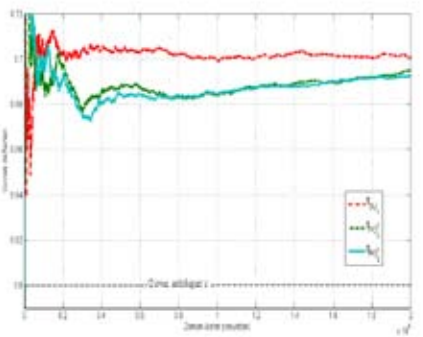
3.1 Eşgüdümlü birincil kullanıcı maskeleme saldırısı

Birincil kullanıcıyı maskeleme saldırısı hedeflenen birincil kullanıcıların kanalı kullanmalarını önlemeye yönelik yapılmaktadır. Eşgüdümlü birincil kullanıcıyı maskeleme saldırısı (EBKMS) ise eşgüdümlü saldırganların birincil kullanıcıların hedeflenen kanalda iletişimlerini devamlı olarak engelleyecek şekilde genel karar mekanizmasını etkileyecek kadar yanlış kararın BM'ye gönderilmesi şeklinde tanımlanmaktadır.

Saldırganlar EBKMS için birincil kullanıcı kanaldayken BM'ne kanalın boş olduğuna dair yerel kararlarını gönderirler. ÇOĞUNLUK yöntemine göre en az k kadar saldırganın saldırıya katılması gerekmektedir. Bu durumda $|PG| \geq N$ olmalıdır. Fakat yanlış karar gönderen saldırganlara birleşim merkezinden ceza uygulanacağından belirli bir karar döngüsünden sonra saldırganların güven değerleri eşik değerinin altına düşecek ve oylamaya katılamayacaklardır. Bu sebeple saldırgan alt grup sayısı L >1 olmalıdır. Bu şekilde bir grup saldırırken diğer grup karar döngüsüne girmeyecek, birincil kullanıcılar kanalda olmadığında ise tüm saldırganlar EG grubu üyesi olarak güven değerlerini artırmak için doğru karar gönderebileceklerdir. Ceza oranının yüksekliğine göre saldırgan ve hazırlayıcı grupların sayıları L ve M artırılabilmektedir.



Şekil 3 Hatalı tespit olasılıkları



Şekil 2 Güven değerleri

3.2 Eşgüdümlü bencil kullanıcı saldırısı

Bencil kullanıcı saldırısında saldırganlar kanalı diğer bilişsel radyolara kullandırmayarak adaletsiz olarak işgal etmektedirler. Eşgüdümlü bencil kullanıcı saldırısı ise (EBKS) eşgüdümlü saldırganlar bilişsel radyoların hedeflenen kanalda iletişim yapmalarını devamlı olarak engelleyecek şekilde genel karar mekanizmasını etkileyecek kadar yanlış kararın BM'ne gönderilmesidir şeklinde tanımlanmaktadır. EBKMS'e benzer şekilde bu saldırıda M >1 olması gerekmektedir. Bu saldırı şeklinde EG istenilen şekilde oluşturulabilir.

4. Deneysel sonuçlar

Eşgüdümlü saldırıların bilişsel radyo ağları İSS sistemine verebilecekleri zararları göstermek maksadıyla iki aşamalı bir deney tasarlanmıştır. Birinci aşamada oluşturulan modelin doğrulaması ve bu modele özgü olacak şekilde tespit olasılığı ve hatalı tespit olasılıkları hesaplanmaktadır. İkinci aşamada ise eşgüdümlü saldırılarda hesaplanan değerlerin değişimi ve önerilen önlem metodunun ne şekilde sisteme fayda sağladığı gösterilmektedir.

4.1 Birinci aşama parametre hesaplama

BM'nin doğru tespit olasılığı Q_d, birincil kullanıcıların tekil olarak doğru tespit olasılığı, P_d kullanılarak denklem (7) ile hesaplanmaktadır.

$$Q_d = \sum_{i=k}^{N} \binom{N}{i} P_d^i (1 - P_d)^{N-i} \qquad (7)$$

Fakat bu çalışmada ağırlıklı değerler kullanıldığından Monte Carlo metodu kullanılarak oluşturulan model için Q_d ve Q_f değerleri hesaplanmaktadır. Birincil kullanıcının kanalda bulunma olasılığı 0.5, oylamaya katılan bilişsel radyoların doğru karar verme olasılıkları ise 0.7 olarak atanmıştır. Monte Carlo metodu için gerekli rastgele olayları oluşturmak için (0,1) açık aralığında standart değişmeyen dağılımdan 0.5 ve 0.7 olasılıklarıyla çekim yapılmaktadır. Q_d birincil kullanıcının kanalda bulunduğunda bilişsel radyoların doğru karar verdikleri durum sayısının toplam karar sayısına bölümüyle, Q_f ise yanlış karar sayısının toplam karar sayısına bölümüyle hesaplanmaktadır. 10.000 bağımsız simülasyondan sonra sırasıyla Q_d ve Q_f bu model için 0.94 ve 0.02 bulunmuştur.

4.2 İkinci aşama birinci safha: Saldırı gösterim

3. bölümde tanımlanan saldırılar bu safhada gösterilmektedir. Bilişsel radyo, saldırı ve hazırlayıcı gruplarının eleman sayısı için 10 değeri atanmıştır. Simülasyon toplam 20.000 karar döngüsüyle çalışmaktadır. Saldırı, simülasyonun 2.000'nci karar döngüsünde başlayıp 3.000'nci döngüde bitmektedir. Atanan değerlerle EBKS için elde edilen güven ve Q_f değerlerini gösteren grafikler sırasıyla Şekil 2 ve 3'tedir.

Simülasyon sonuçlarından görüldüğü gibi saldırganlar güven değerlerini yukarıda tutarken yanlış tespit değerleri artmaktadır.

4.3 İkinci aşama ikinci safha: Önlem

Her saldırganın tekil eylemi normal eylemler olması sebebiyle bu tekil eylemlerin birleşimi olan eşgüdümlü saldırıları tespit etmek oldukça güçtür. Saldırganlar ceza mekanizmasından daha az etkilenmek için öncelikle güven değerlerini artırmak zorundadır. Bu sebeple BM ikinci bir eşik değeri kullanarak tüm kullanıcıların güven değerlerini başlangıç eşik değerine getirerek saldırının etkisini azaltabilir.

Metodumuzda bir adet saldırı tespit eşik değeri seçilmiştir. Bu değer Q_f için Lambda λ değeridir. Eğer ki hatalı tespit olasılığı, Q_f bu eşik değerini geçerse BM tüm bilişsel radyoların güven değerlerini eşik değerine düşürmektedir. Şekil 2'de görüldüğü gibi önleme metoduyla elde edilen Q_f değeri önleme mekanizmasına göre sisteme yeşil ve kırmızı doğrular arasında kalan alan kadar kazanım getirmektedir.

5. Tartışma ve sonuç

Oluşturduğumuz sistem ÇOĞUNLUK yöntemine göre çalışmaktadır. VE ve VEYA yöntemine göre sisteme baktığımızda ise;

VE yöntemi kullanıldığında eğer ki EBKMS yapılmak istenirse saldırgan sayısı ne olursa olsun karar mekanizması etkilenmeyecektir. Fakat EBKS için bir saldırganın olması yeterlidir.

VEYA yöntemi kullanıldığında ise sistem EBKS için daha zayıf EBKMS için daha güçlü olacaktır.

Söz konusu iki saldırı açısından bakıldığında ÇOĞUNLUK yöntemi söz konusu saldırılara karşı daha dayanıklı bir sistem oluşturmaktadır.

Bu çalışmada iki adet eşgüdümlü saldırı modeli tanımlanmakta ve bu saldırı modellerini gerçekleştirmek için güncel bir model örnek alınmaktadır. Bu modelde her iki saldırı modeli de deneysel olarak test edilip saldırıların teorik olarak gerçekleştirilebilecekleri ispat edilmektedir. Her iki saldırı modeli için de geçerli bir çözüm önerilmekte ve çözüm metodunun sağlayacağı fayda da deneysel olarak gösterilmektedir.

6. Teşekkür:

Bu çalışma Devlet Planlama Teşkilatının 2007K120610 numaralı TAM, 9130016 numaralı TUBITAK TEYDEB ve 10030 numaralı EUREKA ITEA2 ADAX projeleriyle desteklenmektedir.

7. Kaynaklar

[1] G. Gur, S. Bayhan, and F. Alagoz, "Cognitive femtocell networks: An overlay architecture for localized dynamic spectrum access [dynamic spectrum management]," **Wireless Communications, IEEE,** vol. 17, no. 4, pp. 62–70, 2010.

[2] http://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-SM.2152-2009-PDF-E.pdf **Report ITU-R SM.2152** (09/2009)

[3] Yucek, T.; Arslan, H., "A survey of spectrum sensing algorithms for cognitive radio applications," **Communications Surveys & Tutorials, IEEE ,** vol.11, no.1, pp.116,130, First Quarter 2009

[4] N. Armi, N. Saad, and M. Arshad, "Hard decision fusion based cooperative spectrum sensing in cognitive radio system," **ITB Journal of Information and Communication Technology,** vol. 3, no. 2, pp. 109–122, 2009.

[5] S. Braynov and M. Jadliwala, "Representation and analysis of coordinated attacks," **in Proceedings of the 2003 ACM workshop on Formal methods in security engineering, ser. FMSE '03. New York, NY, USA: ACM, 2003,** pp. 43–51. [Online]. Available:http://doi.acm.org/10.1145/1035429.1035434

[6] J. Feng, G. Lu, and Z. Bao, "Weighted-cooperative spectrum sensing scheme using trust in cognitive radio networks," **in Signal Processing (ICSP), 2012 IEEE 11th International Conference** on, vol. 3, 2012, pp. 1693–1696.