DÜZCE ÜNİVERSİTESİ | LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BİLİŞSEL RADYO AĞLARDA SPEKTRUM ALGILAMA VERİ SAHTECİLİK SALDIRILARINA KARŞI İŞ ÇIKARMA ORANININ ARTIRILMASI

HÜSEYİN DOĞAN

YÜKSEK LİSANS TEZİ

SİBER GÜVENLİK ANABİLİM DALI

DANIŞMAN

DOÇ. DR. M. ENES BAYRAKDAR

DÜZCE , 2024

T.C.

DÜZCE ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSİTÜSÜ

BİLİŞSEL RADYO AĞLARDA SPEKTRUM ALGILAMA VERİ SAHTECİLİK SALDIRILARINA KARŞI İŞ ÇIKARMA ORANININ ARTIRILMASI

HÜSEYİN DOĞAN

YÜKSEK LİSANS TEZİ

SİBER GÜVENLİK ANABİLİM DALI

DANIŞMAN

DOÇ. DR. M. ENES BAYRAKDAR

Düzce

Ağustos , 2024

T.C.

DÜZCE ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BİLİŞSEL RADYO AĞLARDA SPEKTRUM ALGILAMA VERİ SAHTECİLİK SALDIRILARINA KARŞI İŞ ÇIKARMA ORANININ ARTIRILMASI

Hüseyin DOĞAN tarafından hazırlanan tez çalışması aşağıdaki jüri tarafından Düzce Üniversitesi Lisansüstü Eğitim Enstitüsü Siber Güvenlik Anabilim Dalı **Yüksek Lisans Tezi** olarak kabul edilmiştir.

Tez Danışmanı

Doç. Dr. M. Enes BAYRAKDAR ……

Jüri Üyeleri

Üye Prof. Dr. Devrim AKGÜN ……

Üye Doç. Dr. M. Enes BAYRAKDAR ……

Üye Doç. Dr. Arafat ŞENTÜRK ……

Tez Savunması: 01.08.2024

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığını beyan ederim.

1 Ağustos 2024

Hüseyin DOĞAN

TEŞEKKÜR

Tez çalışmalarımın her aşamasında desteğini gördüğüm, engin tecrübelerini aktararak akademik olarak gelişmeme katkıda bulunan sayın danışman hocam, Doç. Dr. M. Enes BAYRAKDAR'a en içten teşekkürlerimi bir borç bilirim. Bu günlere gelmemde büyük pay sahibi olan ve bir çok fedakârlıklar gösterip beni destekleyerek her an yanımda olan çok kıymetli eşime ve aileme teşekkürlerimi sunarım.

1 Ağustos 2024 **Hüseyin DOĞAN**

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

BİLİŞSEL RADYO AĞLARDA SPEKTRUM ALGILAMA VERİ SAHTECİLİK SALDIRILARINA KARŞI İŞ ÇIKARMA ORANININ ARTIRILMASI

Hüseyin DOĞAN
Düzce Üniversitesi
Lisansüstü Eğitim Enstitüsü, Siber Güvenlik Anabilim Dalı
Yüksek Lisans Tezi

Danışmanı: Doç. Dr. M. Enes BAYRAKDAR
Ağustos 2024, 29 Sayfa

Bilişsel Radyo (CR) ağları, dinamik spektrum erişimi sağlar ve spektrum verimliliğini önemli ölçüde artırabilir. İşbirlikçi Spektrum Algılama (CSS), algılama doğruluğunu artırmak için CR kullanıcıları arasındaki uzamsal çeşitlilikten yararlanır. Ancak gerçekçi bir senaryoda, güvenilir CSS, Spektrum Algılama Verilerinde Sahtecilik (SSDF) saldırısına karşı savunmasızdır. Bir SSDF saldırısında, bazı kötü niyetli CR kullanıcıları kasıtlı olarak tahrif edilmiş yerel algılama sonuçlarını bir veri toplayıcıya veya Füzyon Merkezine (FC) bildirir ve ardından sezme kararını etkiler. Bu çalışmada, bir SSDF saldırısı için analitik bir model araştırıp böyle bir saldırıya karşı sağlam bir savunma stratejisi önerilmektedir. FC' nin saldırı parametrelerini elde etmek ve daha iyi bir savunma stratejisi kullanmak için öğrenme ve tahmin yöntemlerinin uygulanabileceği gösterilmektedir. Ayrıca, log-normal gölge sönümlü bir kablosuz ortam varsayarak SSDF saldırısının gücünü etkileyebilecek saldırı parametreleri tartışılmaktadır. Bu çalışmanın sonuçları, özellikle kötü niyetli kullanıcıların çoğunlukta olduğu durumlarda, SSDF saldırılarına karşı önerilen savunma yönteminin etkinliği gösterilmektedir.

Anahtar Kelimeler: Bilişsel Radyo Ağları, İşbirlikçi Spektrum Algılama, Spektrum Algılama Verilerde Sahtecilik Saldırısı, Kötü Amaçlı Kullanıcı

ABSTRACT

INCREASING THE THROUGHPUT RATE AGAINST SPECTRUM SENSING DATA FALSIFICATION ATTACKS IN COGNITIVE RADIO NETWORKS

Hüseyin DOĞAN
Düzce Üniversitesi
Graduate School, Department of Cyber Security
Master's Thesis

Advisor: Assoc. Prof. Dr. M. Enes BAYRAKDAR
August 2024, 29 Page

Cognitive Radio (CR) networks provide dynamic spectrum access and can significantly improve spectrum efficiency. Collaborative Spectrum Sensing (CSS) leverages spatial diversity among CR users to improve detection accuracy. However, in a realistic scenario, trusted CSS is vulnerable to Spectrum Sensing Data Falsification (SSDF) attack. In an SSDF attack, some malicious CR user reports deliberately falsified local sensing results to a data collector or Fusion Center (FC), which then influences the sensing decision. In this work, we investigate an analytical model for an SSDF attack and propose a robust defense strategy against such an attack. We show that learning and prediction methods can be applied to obtain FC's attack parameters and use a better defense strategy. We also assume a wireless environment with log-normal shadow damping and discuss the attack parameters that may affect the strength of the SSDF attack. Simulation results show the effectiveness of the proposed defense method against SSDF attacks, especially in cases where malicious users are in the majority.

Keywords: Cognitive Radio Networks, Collaborative Spectrum Sensing, Spectrum Sensing Data Spoofing Attack, Malicious User

1. GİRİŞ

Bilişsel radyo ağlar, genel olarak kablosuz haberleşme için kullanılan güncel bir teknolojidir. Bilişsel radyo ağlarda, birincil kullanıcılar ve ikincil kullanıcılar bulunmaktadır. İkincil kullanıcılar, lisanlı olan birincil kullanıcıların boş olan spektrumlarını fırsatçı olarak kullanmayı hedeflemektedirler. Böylece, spektrum verimli bir şekilde kullanılmaktadır. İkincil kullanıcı birincil kullanıcının boş spektrumunu kullanmakta iken, birincil kullanıcının spektrumu kullanma ihtiyacı olabilmektedir. Bu durumda, ikincil kullanıcının farklı bir spektruma geçerek haberleşmesine devam etmesi spektrum algılama olarak tanımlanmaktadır. Spektrum algıma işleminde, geçiş yapılacak olan frekans bantları önceden belirlenerek tanımlandığı için bilginin izinsiz olarak erişimi engellenmiştir. Bu çalışmada Bilişsel Radyo (CR) teknolojisi, lisanssız CR kullanıcılarına lisanslı Birincil Kullanıcıların (PU'lar) bir arada var olduğu lisanslı frekans bantlarının boş alanlarında fırsatçı bir şekilde çalışmasına izin vererek spektrum verimliliğini artırmak için önerilmiştir.

CR kullanıcılarının ana görevi, spektrum algılama olarak adlandırılan PU sinyallerinin varlığını belirlemektir. Spektrum algılama için enerji algılama, uyumlu filtre algılama ve döngüsel öznitelik algılama vb. gibi birkaç farklı yöntem vardır. Bunların arasında enerji algılama tekniği, basitliği ve verimliliği nedeniyle kullanışlı bir yöntemdir. İşbirlikçi Spektrum Algılama (CSS), çok yollu sönümleme, gölge sönümleme ve gizli istasyon sorununun etkilerine hâkim olmak için etkili bir yaklaşımdır. Ne yazık ki, CSS, Spektrum Algılama Verilerinde Sahtecilik (SSDF) saldırılarına karşı savunmasızdır. Bir SSDF saldırısında, bazı kötü niyetli CR kullanıcıları kasıtlı olarak tahrif edilmiş yerel algılama sonuçlarını bir baz istasyonuna veya Füzyon Merkezine (FC) gönderir ve ortak algılama performansını önemli ölçüde azaltmaktadır.

SSDF saldırılarına ilişkin literatürün çoğunda, kötü niyetli saldırganların azınlıkta olduğu ve nihai spektrum algılama kararı üzerinde çok az etkiye sahip olduğu varsayılmaktadır. Önerilen savunma stratejileri, kullanıcıların itibarına dayanmaktadır. Her kullanıcının itibarı, yerel algılama raporunu FC'nin küresel kararıyla karşılaştırarak elde edilmektedir. Ancak, çok sayıda kötü niyetli kullanıcının olduğu büyük saldırılarda uygun bir savunma yöntemi nadiren incelenmiştir. Kötü niyetli SSDF saldırganları çoğunlukta olduğunda, küresel karar oldukça güvenilmezdir ve itibara dayalı yöntemler daha az verimlidir. Aksine, FC'nin nihai kararı hakkında önceden bilgi gerektirmeyen yeni bir yaklaşım önermektedir. İlk olarak, spektrum algılamanın ilk aşamasında, algılama raporlarının ortalama değeri hesaplanır ve iki önemli saldırı parametresi tahmin edilmektedir. Bu parametreler hem dolu hem de boş frekans bantlarında belirli bir kullanıcıdan alınan raporların tahrif edilme olasılıklarıdır. Daha sonra elde edilen saldırı parametreleri, CSS performansını iyileştirmek için spektrum yöntemiyle kullanılmaktadır. Önerilen yöntem, SSDF saldırılarını geleneksel yönteminden daha iyi ele almakta ve yoğun saldırılarda doğru algılama olasılığını en üst düzeye çıkarmaktadır.

1.1. ARAŞTIRMANIN AMACI

İlgili çalışma CSS, merkezi ve merkezi olmayan ağda uygulanan potansiyel spektrum boşluklarını belirlemek için iyi bilinen bir yaklaşımdır, ancak birincil kullanıcı öykünme saldırısı (PUEA), SSDF ve gizli dinleme saldırısı gibi çeşitli saldırılara maruz kalması kolaydır. Bunlar arasında SSDF, CRSN'deki en iyi bilinen güvenlik tehdididir. SSDF saldırganlarının motivasyonu, diğer SU'ların erişim fırsatlarını boşa harcamak veya genel algılama olasılığını azaltarak PU'nun normal çalışmasını bozmaktır. Yanlış spektrum algılama raporları göndererek, MU'lar (Malicious Users) füzyon merkezinde (FC) spektrum kullanılabilirliği hakkında yanlış bir küresel karara neden olabilir. Özellikle, bazı dürüst SU'lar, gölgeleme ve sönümleme veya arızalı sensörden kaynaklanan kötü algılama performansları nedeniyle saldırgan olarak kabul edilebilir. Bununla birlikte, MU'lar veya bu kasıtsız saldırganlar, saldırganların ortak dağılımına ve dürüst kullanıcıların algılama olasılığına bağlı olarak sistemin algılama doğruluğunu düşürmektedir.

Saldırganın bakış açısından, SSDF saldırı stratejileri Her Zaman Evet saldırısı, Her Zaman Hayır Saldırısı, Her Zaman Yanlış Saldırı, Vur-Çalıştır saldırısı, olasılık saldırısı vb. olarak ayrılmaktadır. Veri tahrifat enjeksiyonu yoluyla CSS'nin güvenilirliği üzerindeki ciddi zararla başa çıkmak için SSDF saldırılarına karşı savunma için çeşitli çalışmalar araştırılıp en verimli şekilde çalışma yapılması amaçlanmaktadır.

1.2. ARAŞTIRMANIN YÖNTEMİ

Ele alınan sistem modeli, ağın merkezinden belirli bir kilometre uzaklıkta bulunan bir PU vericisi, bir FC ve küçük bir dairesel alana (~ 1 Km2). N CR kullanıcıları arasında kötü niyetli kullanıcılar olduğu ve PU vericisinin iletişim aralığının tüm ağı kapsadığı varsayılarak yapılacak işlemdir.

Üç tipik kötü niyetli kullanıcı vardır. Her Zaman Evet (AY) saldırganları her zaman PU sinyalinin varlığını bildirmektedir. Bu durumda yanlış alarm olasılığı artarak spektrum kaynağı boşa harcanmaktadır. Daima Hayır (AN) kötü niyetli kullanıcılar her zaman "kanal boş" uyarısı vererek yerel bir karar göndermektedir. Bu nedenle, FC aldatılabilmekte ve CR kullanıcılarının, PU sinyali fiilen mevcutken kanala erişmesine izin vermektedir. Daima Yanlış (AF) saldırganları, algılama sonuçlarının zıt değerlerini FC'ye göndermektedir. Bu nedenle, FC'nin her zaman yanlış bir algılama kararı vermesine neden olmaktadır. AF saldırıları altında hem spektrum kaybı hem de PU paraziti mümkündür.

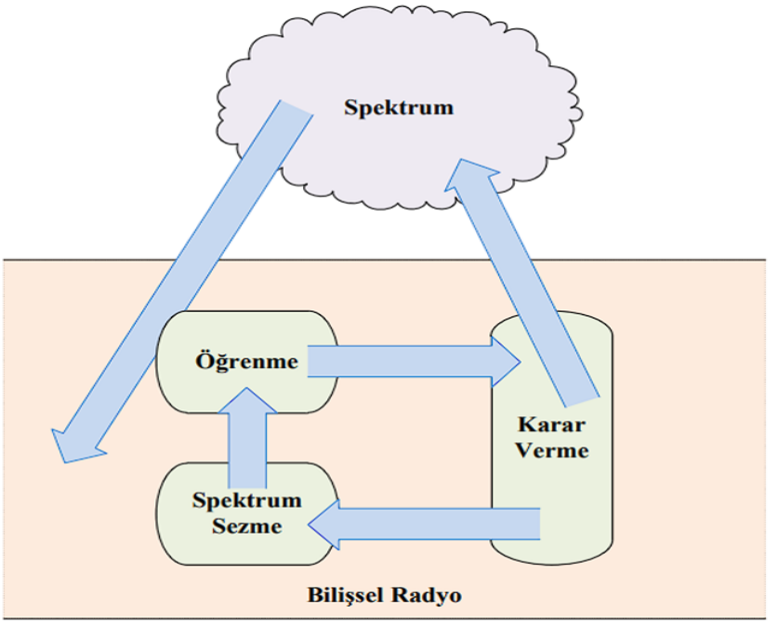
Önerilen şema iki aşamadan oluşmaktadır: birinci aşamada saldırı parametreleri tahmin edilmekte ve ikinci aşamada SSDF saldırılarının yıkıcı etkisini hafifletmek için tahmin edilen parametreler spektrum algılama yöntemi uygulanmaktadır. Burada, saldırı stratejisi varsayılarak ve saldırı popülasyonu ve FC'nin nihai kararı hakkında herhangi bir ön bilgi olmadan veri sahtecilik saldırılarına karşı iş çıkarma oranları tahmin edilmektedir. Bu oranların tahmini, CR kullanıcılarından alınan algılama raporlarına dayanmaktadır.

2. BİLİŞSEL RADYO AĞLARI

2.1. BİLİŞSEL RADYO AĞLARININ TEMEL FONKSİYONU

Bilişsel iletişim sistemlerinin iletişim sorunlarını çözebileceği ve temelini psikolojiye borçlu olduğu düşünülmektedir. Bilişsel insanların düşünce yapısını aydınlatmaya çalışan, güçlü ve etkili bir model olması nedeniyle insanların ilgisini çekmiş ve birden fazla alanda uygulamaları olmuştur. Bilişsel psikoloji, bilişsel süreçlerin tüm insan zihinsel faaliyetlerin altında yattığı fikrine dayanmaktadır. Mesela öğrenme süreci, ilk olarak bilginin önce algılanması, sonra anlaşılmasıyla daha sonra bilgiyle ilişkilendirilmesi olarak modellenebilirken, karar verme süreci, mevcut bilginin yorumlanması ve uygulanmasının algısal durumu olarak düşünülebilmektedir [1].

Bilişsel radyonun spektrum tespiti, spektrum karar analizi, spektrum hareketliliği ve spektrum paylaşımı olmak üzere en az dört ana işlevi vardır. Bilişsel radyo ağlarında spektrum gösteriminin tam olarak anlaşılabilmesi için kısa bir özet verilmiştir [4].



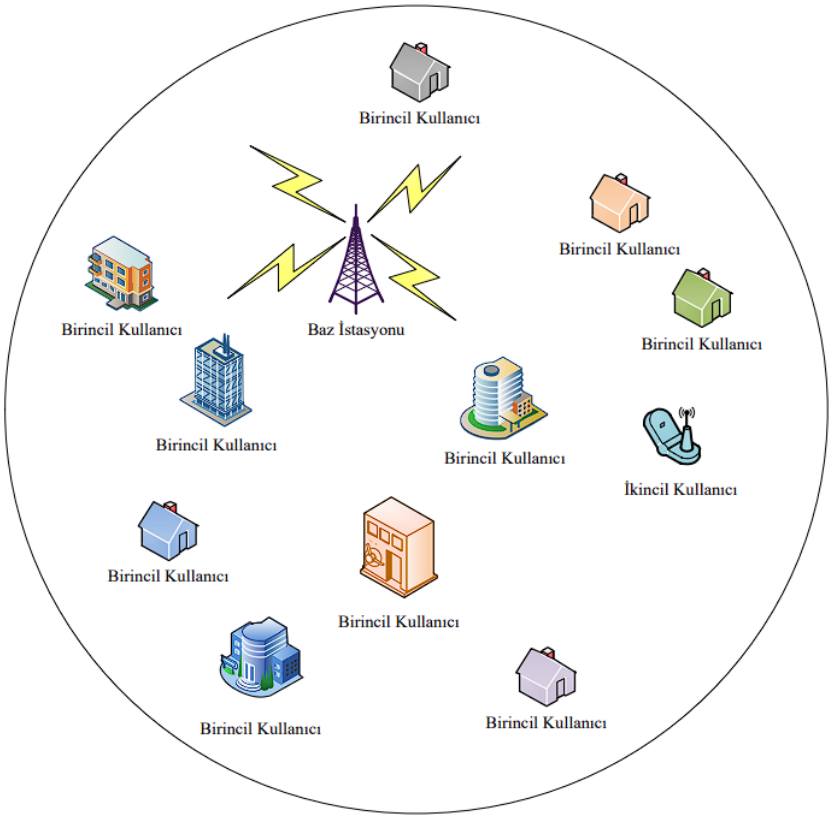
Şekil 2.1. Bilişsel radyo ortamı

Spektrum hissiyat, bilişsel radyonun ayrı spektrum bandındaki radyoyla iletiminden ötürü oluşan elektromanyetik etkileşimi ölçmesi yeteneği şekilde tanımlanabilmektedir. Ortamdaki spektrum kullanım bilgisi sağlanılmasında ötürü, bilişsel radyonun en mühim fonksiyonu spektrum sezme ile gözlenebilmektedir.

2.2. KABLOSUZ BİLİŞSEL RADYO AĞLARI

Bilişsel radyo ağ ortamında, genellikle aynı ortamda bir arada bulunan ikincil ağ ile bir birincil ağ bulunmaktadır. Birincil ağ, belli bir frekans bandında iletişim kurma lisansına

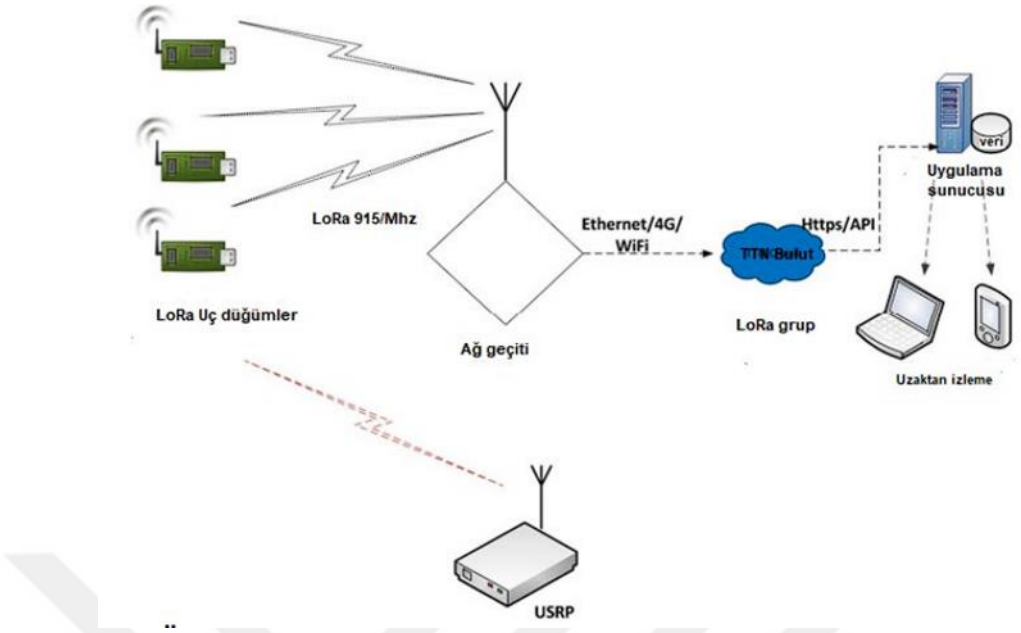
sahip var olan bir ağdır. Bu nedenle ana ağa lisanslı ağ da denir. Birincil ağ, merkezi bir ağ yapısı olabildiği gibi tasarlanmamış şekilde dağıtılmış bir biçimde iletişimi gerçekleştirebilmektedir. Birincil ağdaki lisanslı kullanıcılar sadece birincil ağ bünyesine özel lisanslı spektruma erişirler. Birincil kullanıcılar, mevcut lisanslı spektrumun yetkili kullanıcısı olduğu için spektrum kullanımında önceliğe sahiptir. Bu nedenle birincil kullanıcı, ikincil ağ yapısıyla hiçbir şekilde iş birliği yapmamaktadır. Diğer taraftan birincil kullanıcı iletişimleri hiç bir zaman ikincil kullanıcılar tarafından kesilmemelidir. Bunla beraber, ikincil ağın herhangi bir frekans kanalın da haberleşme yapılması için lisansı olmamaktadır. Bilişsel radyo ağının spektrum erişimi özelliği, ikincil kullanıcısını bütün birincil ağının olduğu frekans bandını çıkarcı biçimde kullanmasına izin vermektedir. İkincil kullanıcı aynı zamanda lisanssız spektrum kanalını da kullanabilmektedir. İkincil ağ, merkezi bir ağ bünyesinde olabilmekte ya da tasarımsız da iletişimi sağlanabilmektedir [5].



Şekil 2.2. Kablosuz bilişsel radyo ağı

2.3. LORA KULLANAN BİLİŞSEL RADYO AĞLARININ SPEKTRUM ALGILAMASI

Birden fazla kablosuz IoT uygulaması, birden fazla aydan birden fazla seneye dek değişim gösteren uzun pil ömrü gerektirmektedir. Bu cins uygulama, Long Range teknolojisi yükselişi de sayılması ile beraber az güçlü geniş alan ağındaki son gelişmeyi motive etmektedir. Bundan dolayı CRN'lere dengeli çalışan LoRa bu araştırmanın odak noktası olmaktadır [26].



Şekil 2.3. Örnek LoRa ile WAN tabanlı spektrum algılama mimarisi

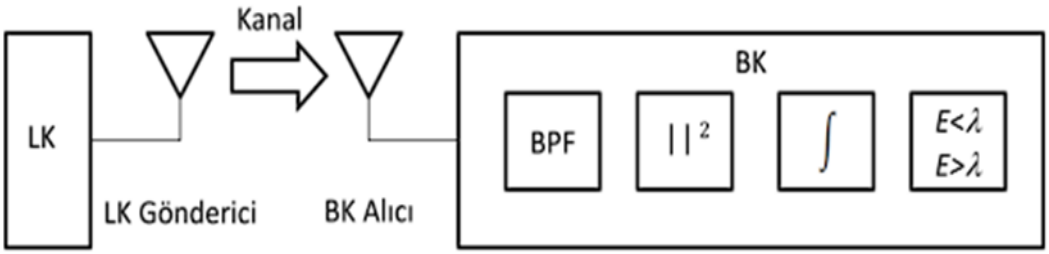
Şekil 2.3.'de gözlemlenen özgün bir LoRa- WAN ağı, uç cihazı yoluyla kablosuz ortamdan gelen paketi bir ana taşıyıcı arayüzüne gönderen çoklu ağ geçidinden oluşmaktadır. Bu nedenle toplanılan ilgiyi inceleyen mantıksal şekilde merkezileştirilen bir sunucu, bütün cihazı ile ağ yapılandırmayı dengeli tutmaktadır. Uç cihazlar, ağa erişimi sağlanılması için belli bir ağa geçidi ile ilişkilendirilmemektedir. Ağ geçidi kolayca bir bağlantı tabakası şekilde hizmet etmekte ve uç düğümden alınılan bütün paketi ağ sunucuya iletmektedir [26].

2.4. SPEKTRUM ALGILAMASI

Bilişsel radyoda spektrum algılama, yetkili kullanıcıların parazitten uzak kalmasını sağlamada önemli bir rol oynamaktadır. İşbirlikçi çeşitliliğin kullanımı, etkili spektrum algılama için en etkili yöntemlerden biri haline gelmiştir, bu nedenle işbirlikçi spektrum algılamanın literatürde bir yeri vardır. İşbirlikçi spektrum algılama, özellikle iletişimin zorlaştığı seyahat durumlarında en destekleyici yaklaşımlardan biri olarak kabul edilmektedir [19].

Spektrum algılamanın asıl amacı, birincil kullanıcı sinyallerinin yalnızca spektrumun belli bir bölgesindeki varlığını belirlemektir. Çok antenli sistemlerde spektrum algılamaya göre genel olarak aşağıdaki senaryolar kullanılabilmektedir. Bu senaryo, dar bant spektrum algılama yöntemleri arasında en sık kullanılan spektrum algılama yöntemi olmaktadır. Bu durumda ikincil kullanıcılar spektrumun boş olduğunu fark ettiklerinde ilgili spektrumu kullanarak kendi aralarında iletişim kurarlar. İlgili senaryolarda ikincil kullanıcı sayısı daha da çoğalabilir. İkincil kullanıcı kişilerde anten sayısıysa en düşük 2 olmakla birlikte daha çok olması sistemin algılama performansına pozitif etkisi olmaktadır [9].

Şekil 2.4.'de Enerji tabanlı spektrum algılamanın blok diyagramını göstermekte. LK, kanalın vericisi ile alıcısı arasındaki iletişim ortamı olan lisanslı kullanıcıyı, BK ise bilişsel radyo kullanıcısını anlatmaktadır. Ortaya çıkan sinyal bir bant geçiren filtreden (BPF) geçirilir. Filtreden geçen sinyal enerjilerinin karesi alınarak toplanmaktadır. Bu enerji değerlerinin örnek sayısı üzerinden ortalaması alınır. Son olarak önceden tanımlanmış bir eşikle karşılaştırılır [8].



Şekil 2.4. Enerji Tabanlı Spektrum Algılama Blok Diyagramı

Spektrum algılama problemlerinde rastlanılan zorlukların üstesinden gelmek ve algılama performansını iyileştirmek için işbirlikçi spektrum algılama (CSS) modeli önerilmektedir. CSS modeli 2 kademeli bir yapıya sahip olmaktadır. İlk kademede spektrum algılama fonksiyonu yerel SU tarafından gerçekleştirilir. 2. kademede her SU sağladığı veriyi karar merkezine rapor etmektedir [18].

2.5. SPEKTRUM KARARI VE ANALİZİ

Bilişsel radyo ağları, kullanılan uygulamanın QoS gereksinimlerine dair mevcut en iyi frekans bandını seçebilmelidir. Spektrum kararları kanal özellikleriyle (girişim, yol kaybı, kablosuz bağlantı hataları, bağlantı katmanı gecikmeleri) ve birincil kullanıcının çalışmasıyla yakından ilgilidir. Ayrıca spektrum kararları başka bilişsel radyo kullanıcılarının aktivitelerinden de etkilenmektedir. Spektrum karar verme iki kademeden oluşmaktadır. İlk olarak, her frekans bandı yalnızca bilişsel radyo kullanıcılarının gözlemlerine dair değil, aynı zamanda büyük ağlardan gelen istatistiklere de dayalı olarak karakterize edilmektedir. Daha sonra bu bilgilere dair en uygun frekans bandı seçilmektedir [13].

2.6. SPEKTRUM HAREKETLİLİĞİ

Spektrum hareketliliğindeki düşünce, frekans bantları sık sık değiştiğinde kesintisiz bağlantıyı sürdürmektir. Bilişsel radyo en uygun frekans bandını yakaladıktan sonra seçilen frekans bandındaki birincil kullanıcıların ayrı frekans bantlarında faaliyetlerini sürdürmeleri gerekebilmektedir. Bu duruma spektrum hareketliliği denmektedir. Bir bilişsel radyo kullanıcısı çalışma frekansını her değiştirdiği zaman, ağ protokolünün bu çalışma parametrelerine dair değişmesi gerekebilir. Bilişsel radyo ağlarında spektrum mobilite yönetiminin hedefi, spektrum geçişleri esnasında hızlı ve sorunsuz geçişler sağlayarak performans bozulmasını düşürmektedir. Hareketlilik yönetimi protokollerinin

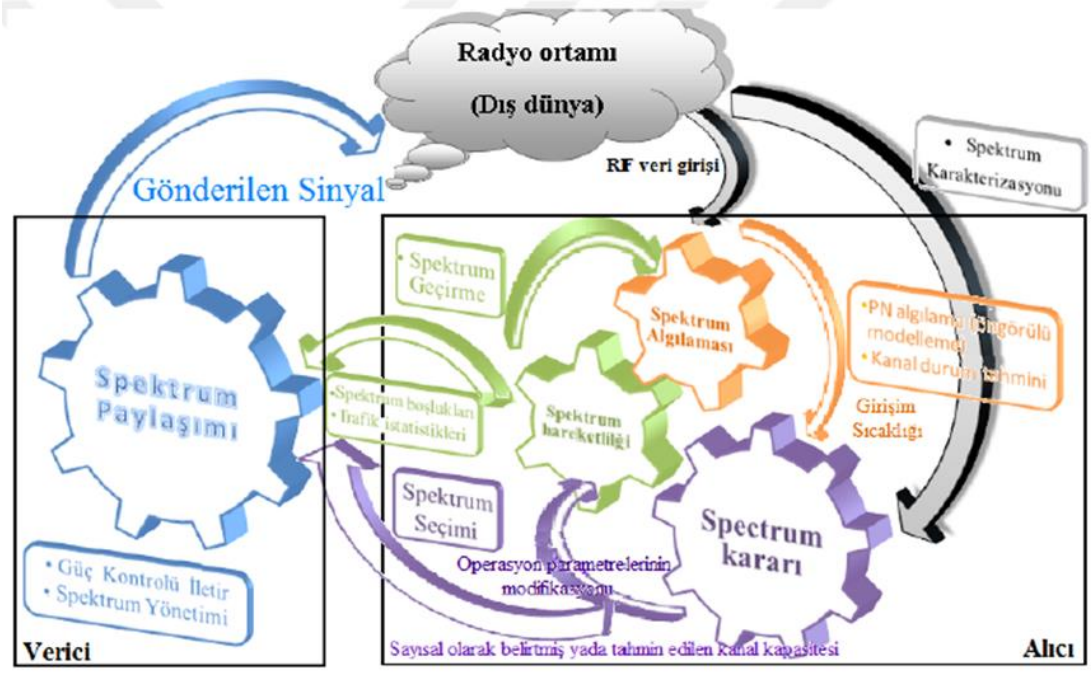
önemli gereksinimlerinden biri devir teslim süresi bilgisi olmaktadır. Bu bilgi algılama algoritmaları aracılığıyla sağlanabilmektedir [22].

Spektrum hareketliliğinde rastlanılan ilk zorluk, uygun spektrum bantlarının zamanla değişmesi nedeniyle gerekli QoS seviyelerinin elde edilememesidir. İkincisi, kullanıcılar bir yerden diğer bir yere hareket ettiğinde mevcut frekans bantları da değişmektedir. Bu nedenle spektrumun devamlı ataması önemli bir gecikme yaratır.

2.7. SPEKTRUM PAYLAŞMA

Spektrum paylaşım mekanizması, spektrum fırsatlarının herhangi bir lisans ya da ücret ödemediği için kendi aralarında eşit haklara sahip olunduğu düşünülen ikincil kullanıcı arasında paylaştırılmasına fırsat sağlamaktadır. İkincil kullanıcılar her zaman birincil kullanıcılara göre daha düşük önceliğe sahip olsa da ikincil kullanıcılar arasındaki hizmetler spektrum paylaşım algoritmaları düzenlenerek tanımlanabilir. Aşağıda paylaşılan yapı, ikincil ağın performansını dolaysız etkiler. Bu optimizasyon sorunu için önerilen, kural tabanlı ya da yapay zekâ algoritmalarıyla desteklenen, oyun teorisi analojileri, grafik renklendirme algoritmalarına dönüştürülen çözümler, ekonomik modellerden ilham alan pazarlık ile açık artırma türleri, iş sıralama algoritmalarına benzer birçok farklı çözüm önerilmiştir [21].

Şekil 2.5.'de birbirinden ayrı konumlar da bulunan bir vericiyle alıcı arasında olan bilişsel döngü gösterilmektedir. Her bir kullanıcı da alıcıyla verici çiftinin olduğu düşünüldüğün de şekilde görülen döngünün başka tarafta olunması gerekildiği açıktır. Görüldüğü üzere alıcıyla vericinin bilişsel birimi hep uyum içerisinde çalışmak zorunda olmaktadır. Bu uyumu sağlanılması için araların da farklı bir geri besleme kanalı mevcut olmaktadır [15].

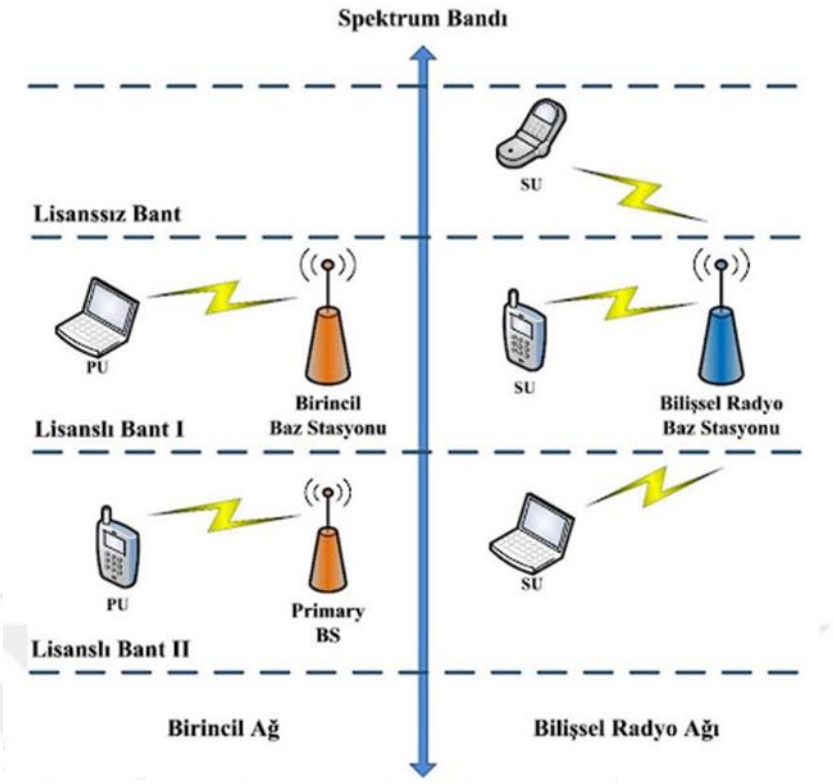


Şekil 2.5. Bilişsel döngü ve dört ana fonksiyonu

2.8. BİLİŞSEL SPEKTRUM PAYLAŞMA

Radyo kanalının paylaşılması doğası sebebiyle bilişsel radyo kullanıcısı koordine edilmesi gerekmektedir. Spektrum paylaşım için 4 yönden bakılabilmektedir [22]:

- **Mimari:** Spektrum atama merkezileştirilebilir veya dağıtılabilir. Merkezi atama yönteminde baz istasyonu frekansları bilişsel radyo kullanıcılarına tahsis eder. Dağıtık bir yapıda spektruma erişim, yerel politikalar dikkate alınarak her kullanıcı tarafından gerçekleştirilir. Kablosuz bilişsel radyo ağ ortamı Şekil 1.5.'te gösterilmektedir. Merkezi yapıdaki birincil ağ ve ikincil ağ ile bilişsel radyo ağ ortamını görebilirsiniz. Bilişsel radyo ağları merkezi bir yapıya sahiptir ve bilişsel radyo erişim noktalarının ikincil kullanıcı iletişimlerini kontrol ettiği ve düzenlediği ağ yapısı ile tanımlanmaktadır.
- **Spektrum atama:** Çözümler üzerinde iş birliği yapmak için bir kullanıcıdan diğer kullanıcılara olan girişim ölçümleri ile faydalanmaktadır. Bu modellerde kullanılan genel yaklaşım, hücresel yapının alan içerisinde girişim bilgisini paylaşmasını sağlamaktır. Bu, merkezi ve dağıtılmış modeller arasında etkin bir biçimde denge oluşturur. İşbirlikçi olunmayan sistemde yalnızca tek bir kullanıcı göze alınmaktadır. Başka bilişsel radyo kullanıcısının girişimi göz önüne alınmamakta ve bu biçimde spektrum kullanışı azalmaktadır.
- **Spektrum erişim tekniği:** Overlay ile Underlay spektrum paylaşımı tekniği ile iki şekilde ayrılmaktadır. Overlay paylaşımında, kullanıcı ağa erişmek için spektrumda ilk kullanıcının kullanılmayan bölümlerini kullanmaktadır. Bu durum birincil ağda girişimi azaltmaktadır. Underlay spektrum paylaşımındaysa yayılı spektrum tekniğinden yararlanmaktadır.
- **Faaliyet alanı:** Her bir bilişsel radyo ağ içerisindeki spektrum erişimi düzenlenilmesi ağ içerisi spektrum paylaşımı yöntemleriyle yapılmaktadır. Ağarası spektrum paylaşımı bilişsel radyo mimarisi, birden fazla sistemin örtüşen bölgeye ve spektrum yerleştirilmeye fırsat tanımaktadır.



Şekil 2.6. Kablosuz bilişsel radio ağ ortamı

2.9. YATAY VE DİKEY SPEKTRUM PAYLAŞMA

Yatay paylaşım teknolojisi, spektrumun ağlar arasında ikincil kullanıcının kendi arasında spektrum paylaşımı olmaktadır. Dikey spektrum paylaşımı, birincil kullanıcılar ile ikincil kullanıcılar arasında uygulanan paylaşımdır ve teknolojisi, literatürde bilişsel radyo ağları için bir paradigmayla bilinmektedir [15].

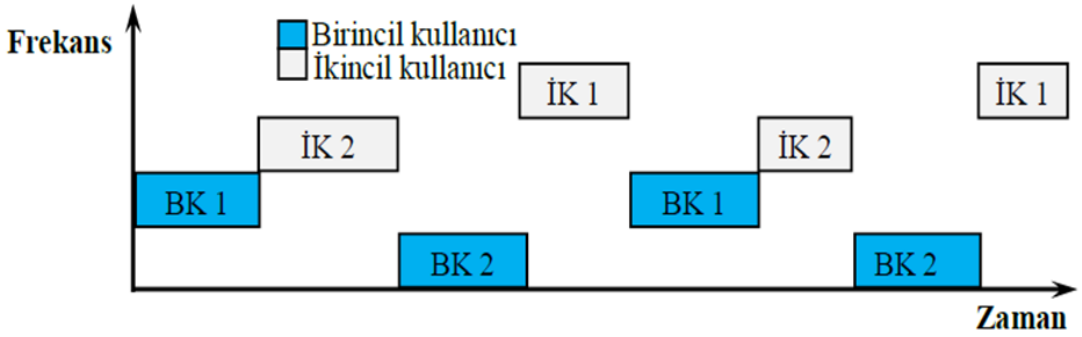
Öncelikle elektronik pazarı endüstri sınıflandırmaya dair yatay, dikey ile çapraz çizgiye ayrılmaktadır. Dikey pazarlar yalnızca belirli bir endüstriye özgü belli mal ve hizmetleri sunarken, yatay pazarlar birden fazla ayrı endüstride kullanılan mal ve hizmeti sunmaktadır. Ayrıca Diagonal Pazar yerleriyse, belli alıcıları ile satıcıları veya birden fazla sektörde kullanılabilecek belirli ürünleri desteklemek için özelleştirilmiş hizmetler konusunda uzmanlaşmıştır [23].

2.10. SPEKTRUM PAYLAŞMA PARADİGMALARI

Birinci kullanıcı ile ikinci kullanıcı kişilerde spektrumun eş zamanlı paylaşımına göre, literatürde 3 ayrı paradigma önerilmektedir. Araştırmacı kişilerin üstüne en fazla odaklanıldığı bu paradigma, boşlu kovalama, alta yayma ve üstüne bindirme şeklinde bilinmektedir.

2.10.1.Boşluk Paylaşma Paradigma

Bilişsel radyoya göre ilk motivasyon boşluk kovalama paradigması olunup, fırsatçı iletişim düşüncesine dayanmaktadır. Burada ikincil kullanıcı, radyo spektrumun olası beyaz boşluğunu süre içerisinde olanak bulundukça geçici olarak kullanmaktadır. Buna temsili bir örnek şekil 2.7.'de verilmektedir [15].



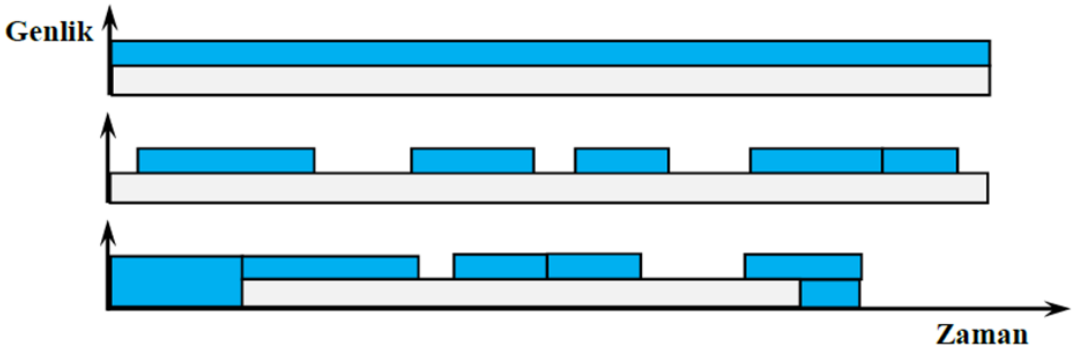
Şekil 2.7. Birincil ve ikincil sinyallerin iç içe iletilmesi

Zamanla birincil sistemler (BK1 ve BK2) aracılığıyla kullanılmayan spektrum boşluklarının ikincil kullanıcılar (IK1 ve IK2) aracılığıyla kullanıldığı görülmektedir. Birincil kullanıcı kanal zaman paylaşımını koordine edilirken, ikincil kullanıcı boş spektrumdan faydalanmak için birincil kullanıcıyı uzay-zaman-frekans boyutunda sürekli izleyerek spektrum boşluklarının paylaşımını koordine eder. Yani ikincil kullanıcıların (IK1 ve IK2) kanal kullanım önceliği birincil kullanıcılara göre daha düşük olduğundan, birincil kullanıcılar (BK1 ve BK2) kanalı kullanmak istediklerinde ikincil kullanıcıların spektrumu ertelemeden hemen boşaltmadan gerekmektedir [12].

Aynı zamanda, birincil kullanıcıların etkinlikleri zamana ve konuma göre değişiklik göstermekte, bu da boşluk tespitini zorlaştırmakta ve diğer taraftan alıcıdaki mevcut donanımın özelliği de bilişsel alıcıların geniş bir bant genişliği üzerinden spektral boşluğu arayabilme hızını sınırlamaktadır. Bu durum iş birlikli algılamayla hesap yükünü düşürerek kısmen çözülse de erteleme ile veri meblağsını düşürülmesine neden olmaktadır. Boşluk kovalama yönteminin zorluğuna bir çare, 2 ya da daha çok kullanıcı aynı anda aynı spektrum bölgeyi kullanılması biçiminde olabilmektedir. Bu yöntemle spektrum altına yayma ya da üzerine bindirme biçiminde paylaşılmaktadır.

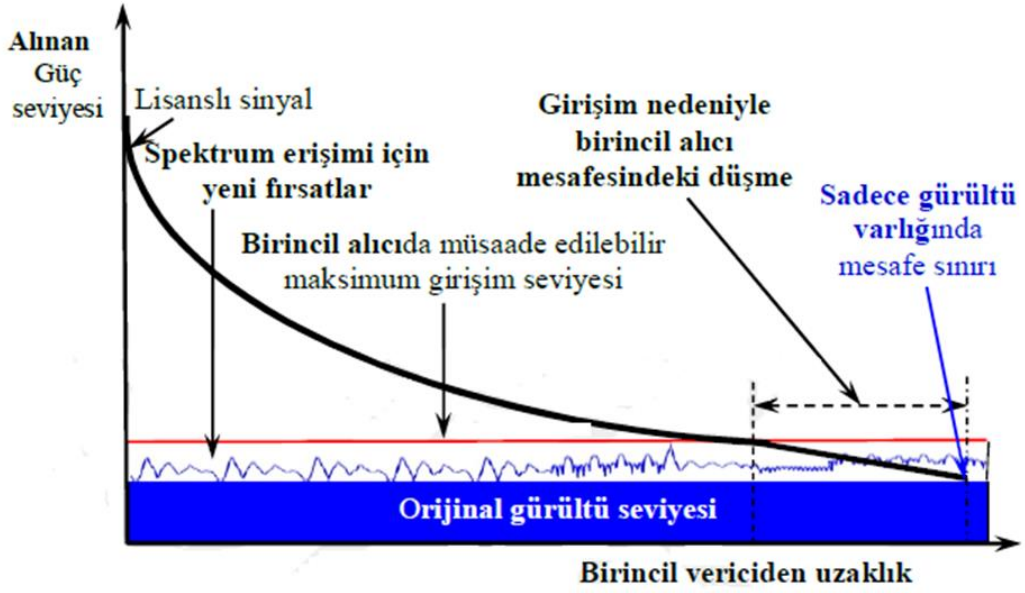
2.10.2. Altına Yayma Paradigması

Genişletme yönteminin gereksinimleri ile kısa takip tekniğinin gereksinimleri tamamen farklıdır. İkincil kullanıcılar radyo spektrumunu birincil kullanıcılarla aynı anda kullanır ve izin verilen girişim sıcaklığını aşmaz. Bu nedenle Şekil 2.8'de gösterilen yaklaşımda olduğu gibi birincil kullanıcı etkinliğini izlemeye gerek yoktur. Bu spektrum paylaşım modeline altın uzantı adı verilmektedir ve Şekil 2.9'da gösterilmektedir [15].



Şekil 2.8. İkincil sinyalin, altına yayma şeklinde spektrumu paylaşması

Şekilde görüldüğü üzere birincil kullanıcı ile ikincil kullanıcıların spektrumun bir arada bulunması, ikincil kullanıcının birincil kullanıcıya müdahale etmeden birincil kullanıcıya sinyal göndermesi ve dolayısıyla girişim sıcaklığının izin verilen sınırı aşmaması durumunda mümkündür. Bu, ultra geniş bant sistemlerinin çalışmasına benzer.



Şekil 2.9. Altına yaymalı spektrum paylaşımında mesafe etkisi

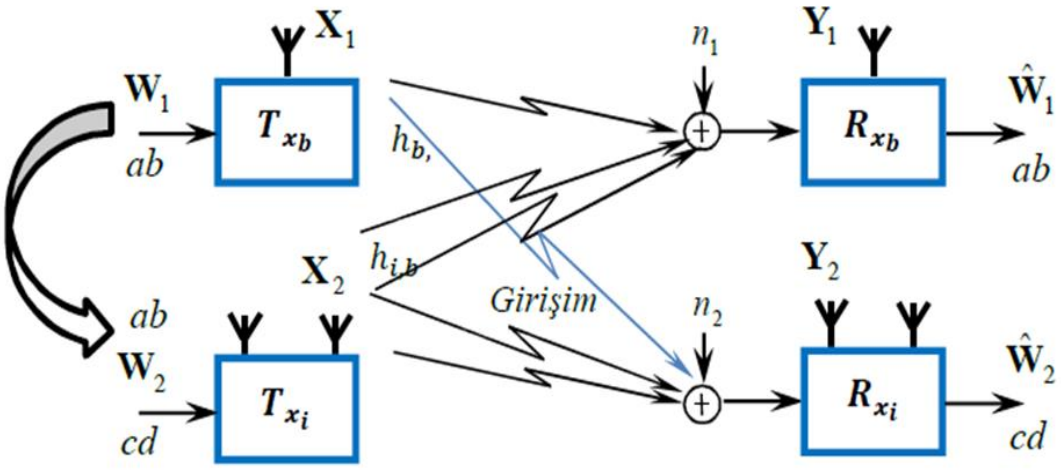
İkincil kullanıcı kişiler, spektral şekilde aktif kanalda iletim fırsatı verilmesi için ilk alıcı gürültü düzeyinin üstünde fakat ilk alıcı zararlı görülmeyecek bir girişim marjini tanımlanmaktadır. Bu marjin içerisinde kalınması şartı ile, ikincil kullanıcı kişilere spektruma erişim izni verilmektedir. Örneğin, ikincil transmisyon neticesinde, bilişsel alıcı da meydana gelen istenilmeyen sinyal düzeyi her zaman alıcı izin verilen girişim sıcaklığının aşağısında olması gerekmektedir [11].

2.10.3. Üzerine Bindirme Paradigması

Aynı spektruma eş zamanlı erişimin başka bir yöntemi de üzerine bindirme teknolojisidir. Üzerine bindirmeyle boşluk izleme yöntemlerini birleştirip bir arada kullanan

çalışmalarda olmaktadır. Yöntem esas olarak birincil vericinin, alıcısına gönderilen bilgiyi iletimden önce ikincil (bilişsel) verici aracılığıyla bilinmesini sağlamasına dayanmaktadır. Bu durum Şekil 1.9'da gösterilmektedir. Bu diyagram, bir SISO birincil kullanıcısıyla bir MIMO ikincil (bilişsel) kullanıcısı olan 2x2 bilişsel radyo iletişim sistemini göstermektedir. Burada alt simge b bilişsel anlamına gelir ve i ikincil anlamına gelir. Aşağıdaki şekilde görüldüğü üzere yardımcı verici, ana vericiyle tek taraflı iş birliği yaparak W1 mesaj bilgisini almaktadır. Bu bilgi ile kendi W2 mesajını kodlayıp gönderilerek birincil vericinin ikincil alıcı kişiye müdahale etmesini önleyebilir. Ancak ikincil vericinin birincil alıcıya müdahale etmesini önlemesi mecburiyetindedir [15].

Aslında en doğru yol, birincil sistemin ikincil sistem iletişim olanağını sunması için uyguladığı iş birliği karşılığıyla, gücün bir bölümünü birincil sisteme ayırtarak, birincil alıcı kişiye (kendisi ekstra bir işlem yapılmasına gerek kalınmadan kanalda ikincil sistemin hiç olmamış gibi normal bir biçimde veriyi alınabilmesi için) lazım olan ayarlamayı yapılarak W1 verisi birincil kişiye gönderilerek onun sinyal kalitesini iyileştirmektedir. Aynı zamanda ikincil alıcı kodlama ya da huzme oluşturulma yolu ile birincil vericiden ulaşan girişimden etkisi olmadan sinyali almaktadır. Fakat bu sistem, ikincil sistemin tüm kanal bilgisi ile birincil verici güç düzeyi bilgisine sahip olunmasını gerekmektedir.

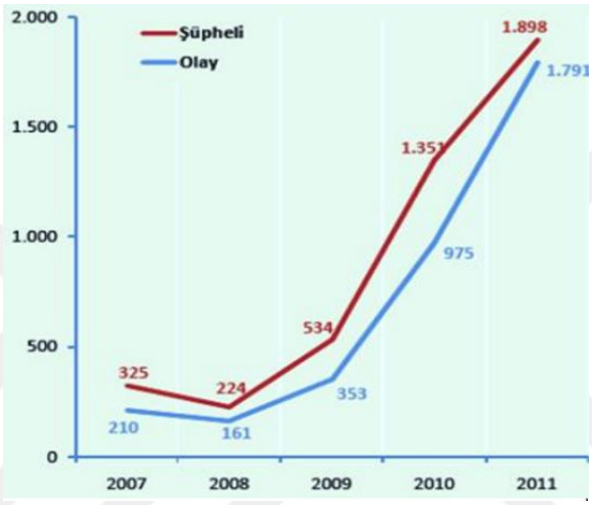


Şekil 2.10. Üzerine bindirme yöntemiyle spektrum paylaşılması

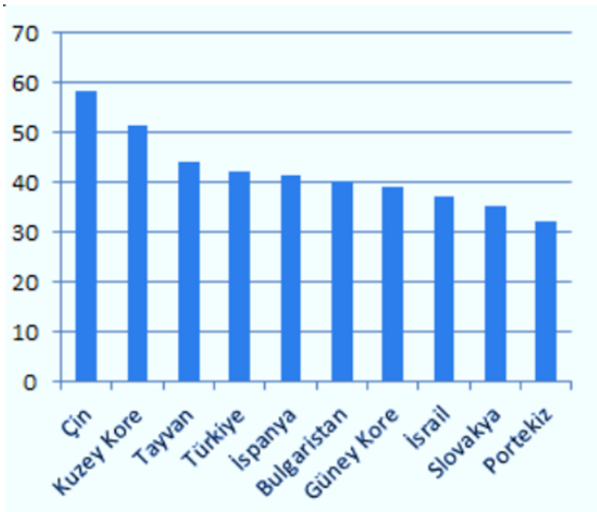
3. SİBER SALDIRI TÜRLERİ

3.1. SİBER SALDIRI TÜRLERİ

2011 polis raporuna göre ülkemizdeki siber suçlar, Şekil 3.1'de gösterildiği gibi son 2 senede hızlı bir büyüme eğilimi gösterdi. Şekil 3.2'den de görülebileceği gibi Türkiye, dünyada siber saldırılara karşı en savunmasız on devletten biri durumuna gelmiştir. Akıllı telefonlar, mobil uygulamalar, çevrimiçi bankacılık ve bunlar aracılığıyla gerçekleştirilen diğer çevrimiçi işlemler siber saldırıların hedefidir [24].



Şekil 3.1. Türkiye'de Bilişim Suçu Artışı



Şekil 3.2. Malware Türkiye Sıralaması

Polis raporundan, ülkemizde kamu kurumları ve özel kuruluşların bilgi sistemlerine internet üzerinden izinsiz erişim, protesto, gasp vb. amaçlar ile verilere el konulması

benzer hedeflerde işlendiği ile hızlı bir artışla gözlemlenen emniyet raporunda gözlemlenmektedir [24].

3.1.1. MALWARE SİBER SALDIRISI

Günümüzde kötü amaçlı kodun dinamik analiz sürecini otamatikleştiren araçlar hızla popülerlik kazanıyor. Antivirüs şirketleri "sandbox" ismi verilen platformları ürün haline getirerek büyük şirketlere satıyor.

Dinamik analiz süreci birden fazla önemli veriyi sağlanılmasını sağlamaktadır. Bu verinin analizi aşaması tamamlanılması ile zararlı olanların bulaştığı sistem de nasıl kaldırılması gerekildiği hakkın da analiste göre yol haritası niteliğinde olmaktadır. Mesela, bu "sandbox" aracı zararlı yazılımın "registry" operasyonu "load time" ile "run time" yüklenilen "kütüphaneler" alakalı etraflı bir şekilde bilgi sunabilmektedir. En fazla kullanılmakta olan "sandbox" sisteminden bir tanesi "Anubis" ücretsiz bir servis olmaktadır. Zararlı kodun "local" sistem üstünden veya bir "URL" aracılığıyla yüklenilerek analiz edilmesini fırsat tanımaktadır [17].

Zararlı yazılımlar [6];

- Sistemi çalışılmasını bozma,
- Sistem güvenliği tehlikeye atma,
- Sisteme izinsiz bağlantı hakkın tanınması,
- Reklam,
- İstenilmeyene e-posta,
- Dosyayı şifre koyup karşılığın da ücret istenilmesi,
- Hassas bilgiyi (kredi kartı, banka şifresi vb.) sağlanılması,
- Büyük ölçekli servis dışı bırakılma saldırısı (DDoS) yapılma,
- Ülkeler arası istibarat ile strateji bilgiyi sağlamaya benzer,

Fazla bilinilen zararlı yazılım tipi aşağıda açıklanmaktadır [14]:

- Virüs, yürütülene bilir dosyayı çalıştırılmasıyla çalışılması tetiklenen, olduğu ortamdan diğer ortama geçme hedefli ile veri veya donanım zararı verilmesi üzere tasarlanan zararlı koddur.
- Büyük virüs, Microsoft veya Excel'e benzer uygulamanın başlangıç esnasında çalışan kodu olunan bölme eklenilmiş virüstür. Kendini üretip diğer bilgisayara bulaşabilmektedir.
- Dosya virüsü yürütülebilir dosyaya bulaşan virüs olmaktadır. Yürütülen dosya çalıştığı esnada virüs kodu birlikte çalışmaktadır.
- Polimorfik virüs, zararlı kodun birden fazla kodlama ile kod çözme işleminin geçmesi ile oluşmaktadır. Her mutasyon döngüsün de yeni bir şifreleme rutinine sahiptir. Belirlenmesi zor olmakta ama kodda meydana gelen yüksek entropiyle belirlenebilir.
- Gizli Virüsler, sistemde olan zararlı yazılım belirleme sistemi etkisiz hale getirerek çalışmaktadır. Tespit sistemi yanlış analarım vermektedir.

3.1.2. PHISHING SİBER SALDIRISI

Oltalama saldırısı, en çok maddi hasara sebep olunan saldırı cinsinden bir tanesidir. Bu saldırı yöntemin de saldıran kişi, bilinilen yasal bir siteye benzer bir site kendisine özgü alan ismi üstünden internet kullanımına açılmakta ve bağlanılan kurbanın kullanıcı ismi, şifre, banka bilgisi, şahsi bilgilerine benzer özel veriyi almayı hedeflemektedir.

Günümüzde phishing saldırıları, mağdurlara tanıdık bir şahıs veya kurumdan geliyormuş gibi davranan e-postaların gönderilmesiyle başlıyor. E-posta, kullanıcıları kötü amaçlı içeriğe yönlendiren bir bağlantı içerir. Kullanıcı bu bağlantıya tıklarsa, saldırgan tarafından yönetilen ancak meşru bir kuruluşa ait gibi görünen bir web sayfasına yönlendirilecektir. Ziyaret edilen sayfada kullanıcılardan hassas bilgilerin çalınması için tasarlanmış bir form bulunuyordu. Bu yöntem kullanılarak kullanıcının hesap erişim bilgileri veya kredi kartı bilgileri çalınabilmektedir. Volkamer'in yapmış olduğu çalışmaya dair Oltalama saldırısının kişiler üstünde başarılı olunmasının 5 sebebi şu biçimde sıralanmaktadır [7];

- Kullanıcınn URL yapısı hakkın da yeterli bilgiye sahip olmaması,
- Kullanıcının güvenilir URL yapısı nasıl olacağı ile alakalı yeterli bilgiye sahip olmaması,
- Tarayıcı üstünde tekrardan yönlendirme veya gizli URL'ler ile kullanıcının hedef URL'i görmemesi/inceleyememesi,
- Kullanıcının URL'e farkın da olunmadan tıklamayı veya URL'in zararlı olup olmadığını araştırarak kadar vaktin olunmaması,
- Kullanıcının temiz bir URL ile zararlı URL arasın da farkı ayırt edememesi,

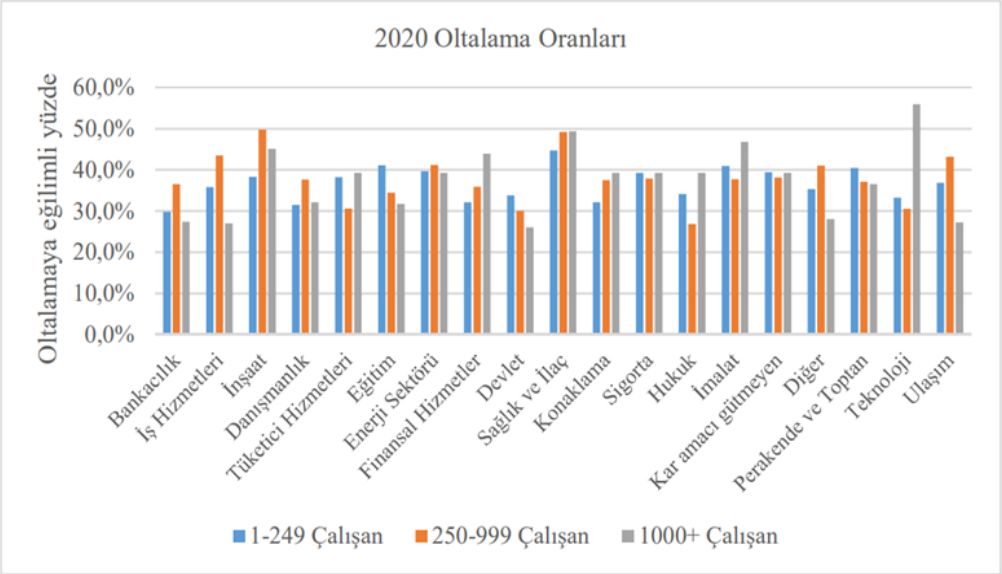
Türkiye Oltalama saldırısından en fazla etkilenilen devletler arasında bulunmaktadır. APWG aracılığıyla Oltalama saldırısı konusunda dünya genelinde 45 devlet üstünde uygulanan bir araştırmada Türkiye Çin'in sonrasında %42, 88'lik etkilenilme oranıyla ikinci en fazla etkilenilen devlet halinde olunduğu gözlenmektedir. Oltalama saldırısından en fazla etkilenilen devletler Tablo 3.1'de gösterilmektedir [24].

Tablo 3.1. Oltalama Saldırısından En fazla etkilenilen devletler

Sıralama	Ülke	Etkilenme Oranı (%)
1	Çin	47,09
2	Türkiye	42,88
3	Tayvan	38,98
4	Guatamala	38,56
5	Ekvator	36,54
6	Rusya	36,02
7	Peru	35,75
8	Meksika	35,13
9	Venezuela	34,77
10	Brezilya	33,13

"Phishing Industry Benchmark Report (2020)" çalışmasında, farklı sektörlerdeki çalışanların phishing saldırılarına karşı savunmasızlığını belirlemek amacıyla 19 sektör,

17.000 şirket, 4 milyon kullanıcı ve 9,5 milyon phishing test saldırısının yer aldığı deneysel bir ortam oluşturuldu. . Şekil 3.3.'de gösterilen grafikte, kimlik avına karşı savunmasız çalışanların yüzdesi, her sektördeki çalışan sayısına göre 3 bölüme ayrılmıştır.



Şekil 3.3. Farklı Endüstrilerde Oltalama Saldırılarına Eğilim Kıyaslaması

Tüm sektörler ve kuruluşlar genelinde ortalama kimlik avı yüzdesi %37,9'dur; bu oran sektöre göre değişiklik göstermektedir. Ancak kullanıcıların, kuruluşun kimlik avı saldırılarına karşı son savunma hattı olma konusundaki başarısızlığını göstermektedir. Bu ortalama, her üç çalışandan birinin şüpheli bir bağlantıya veya e-postaya tıklayabileceği veya dolandırıcılığa yol açan talimatları izleyebileceği anlamına geliyor.

Şekil 3.4'deki grafiği incelediğimizde, 1.000'den fazla çalışanı olan kuruluşların, kimlik oltalama saldırılarına karşı diğer büyüklükteki kuruluşlara göre daha savunmasız olabileceğini görmekteyiz. Bu yaşananlardan aslan payı teknoloji sektörüne aittir. Orta ölçekli işletmeler arasında kimlik oltalama saldırılarına karşı en savunmasız olanlar sağlık, ilaç ve inşaat sektörleridir. Küçük şirketler arasında, sağlık ve ilaç sektörlerindekiler kimlik oltalama saldırılarına karşı daha savunmasızken, eğitim sektöründeki daha küçük şirketler, başka büyüklükteki şirketlere göre kimlik oltalama saldırılarına karşı daha savunmasızdır [17].

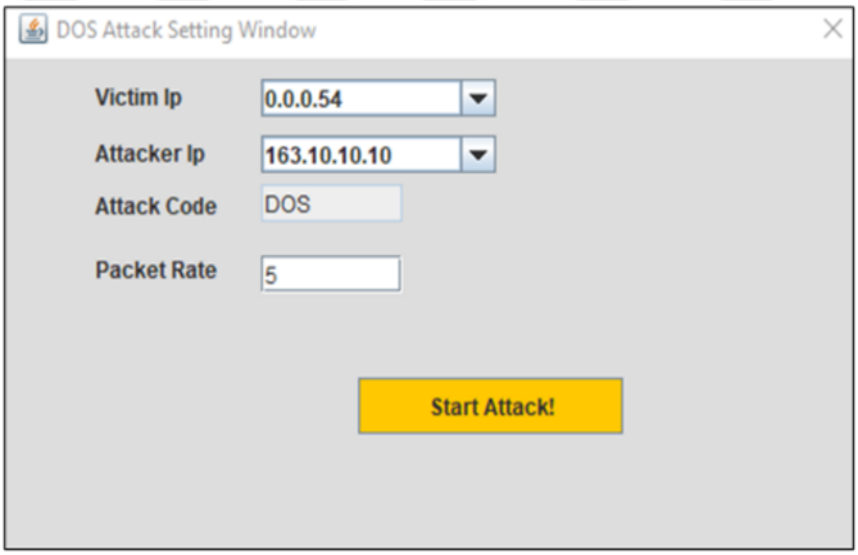
3.1.3. DOS VE DDOS SİBER SALDIRISI

DoS; Bir sistemi veya hizmeti aşırı yükleyerek kullanılamaz hale getirmek için tasarlanmış bir saldırıdır. Bu saldırı cinsinde amaç internet uygulamasının kendisi değil, uygulamayı barındıran sunucular ve kaynaklardır. DoS saldırısı nedeniyle bir sunucu veya sistem hizmet dışı olabilir. Bundan dolayı uygulama sahibi firma veya birey; iş kaybı, maddi kaybıyla itibar kaybı yaşayabilmektedir. Şekil 3.4.'de görüleceği üzere DoS saldırısı tek bir merkezden yine tek bir merkeze uygulanılan saldırı şeklinde adlandırılmaktadır [20].

Şekil 3.4. DOS saldırı senaryosu

DoS saldırılarını engellemek için birçok yazılımla donanım çözümü geliştirilmiş olsa da güvenlik açıklarına sahip cihazlar ya da web sitesi yine de DoS saldırısından etkilenebilmektedir. Bunun başlıca nedenleri arasında ağ ekipmanlarının güncellenmemesi, deneyimsiz güvenlik ya da IT personeli ve yanlış güvenlik politikaları sayılabilir.

Bu araştırmada ağ bileşenleri tanımlanıp farklı ölçeklerde ağ simülasyonları başlandıktan sonra kontrol ara yüzün de çalıştırılıp OSPF protokolüyle yönlendirici de yönlendirilme tablosu oluşturulmakta. Simülasyon ekrarnın da saldırı modeli şeklinde DoS modeli seçilmesi halinde Şekil 3.5.'da DoS saldırısı yapılandırılma pençesi açılmaktadır [16].



Şekil 3.5. DoS saldırısı yapılandırma penceresi

Bir saldırganın DDoS saldırısı gerçekleştirmesinin ilk kuralı, DDoS saldırganının kurbanı olarak seçtiği cihaza erişebilmesini sağlamaktır. İlgili IP adreslerine ve arayüzlere erişildikten sonra saldırı trafiği eş zamanlı olarak kurban cihaza yönlendirilebilir. DDoS saldırısı etkisiyle oluşan paket sayısı ile paketin kurban cihaza erişme zamanına dair çoğalmaktadır. Saldırının elemanı olan cihazın sayısı, yapılan saldırının boyutu ile hedefine dair değişiklik göstermektedir. Bu sayı aynı zaman da saldırıyı yöneten birey veya grubun ellerinde güce ve yeteneğe bağlı olmaktadır [3].

Saldırı trafiğinin hedef aldığı kurban cihaz, türlü yazılım ve araçları kullanılarak, fiziksel katmandan uygulama katmanına kadar arayüzlerine gelen trafikle alakalı her şeyi izleyebilir. Ağ trafiğini izlemeye yönelik araçlarla, gelen paketlerin kaynak IP adresi, aynı kaynak IP adresinden kaç paket gelindiği, seri gelen paketlerin ne zaman gönderilmeye başladığı ne kadar süreyle ve hangi arayüze gönderildiği gibi bilgilere ve diğer bilgilere ulaşılabilir. Bu bilgi paketin bir özelliği temsil eder. Tüm özellikler aslında matematiksel bir denklemdeki değişkendir. Bu değişkenler, denklemin sonuçlarından beklenilen saldırı türünü bulmak için hangi eylemlerin yapılması gerektiğine dair ipuçları sağlar.

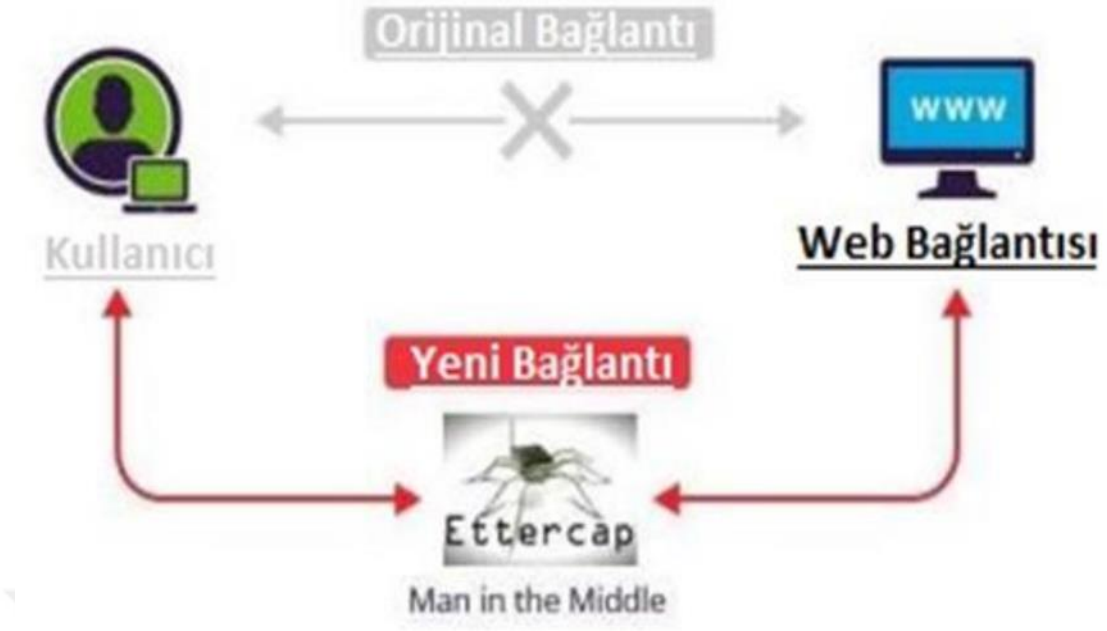
En etkili DDoS atağı, mobil telefon, PC ya da IOT cihazına bulaşılan zararlı yazılım yüzünden gerçekleşmektedir. En büyük DDoS saldırısından biride 2016 senesinde Amerika'da ki DNS sunucusuna uygulanılan saldırıdır. Bu saldırı neticesinde bir an da dünyadaki en büyük 85 web sitesi ortadan kalktı. Bu saldırı da 1.2 terabitliğe benzer yoğun talep gönderilmektedir.

DDoS saldırıları doğal şekilde çalışan ağ servislerine sürekli istek gönderilerek sistemi meşgul eder ve bir süre sonra sistemin çalışamaz duruma gelmesine neden olur. Bu yönden DDoS saldırına göre, siber saldırganın kapasite üzeri sorgu gönderilmesi gerekmektedir [25].

3.1.4. MAN IN THE MIDDLE SİBER SALDIRISI

Ortadaki adam saldırısı (MITM), bir ağ cihazı ile kurban bilgisayar arasındaki yetkisiz erişim yolu ile verinin şifrelenmesi ve şifrelenmemiş verilerin izlenilmesi ilkesine dayanan bir saldırıdır.

MITM saldırıları OSI modelinin ikinci katmanında (veri bağlantı katmanı) uygulandığından, saldırgan başarılı olursa bütün trafiği kontrol edebilir. Bu hakimiyet, şifrelenmemiş trafikten şifreli "HTTPS" trafiğine kadar sınırsız olmaktadır. Başarılı bir MITM saldırısında bir saldırganın neler yapabileceği tamamen bilgi ve becerilerine bağlıdır ve spektrum bilinçli veri sahteciliği saldırısının önemi tamamen onların hayal gücüne bağlıdır. Güvenlik tedbirleri minimum sayıda saldırı içerir, ancak bunlar ağ güvenliğine yönelik iyi bilinen saldırı türleridir [10].



Şekil 3.6. MITM atağının örnek resmi

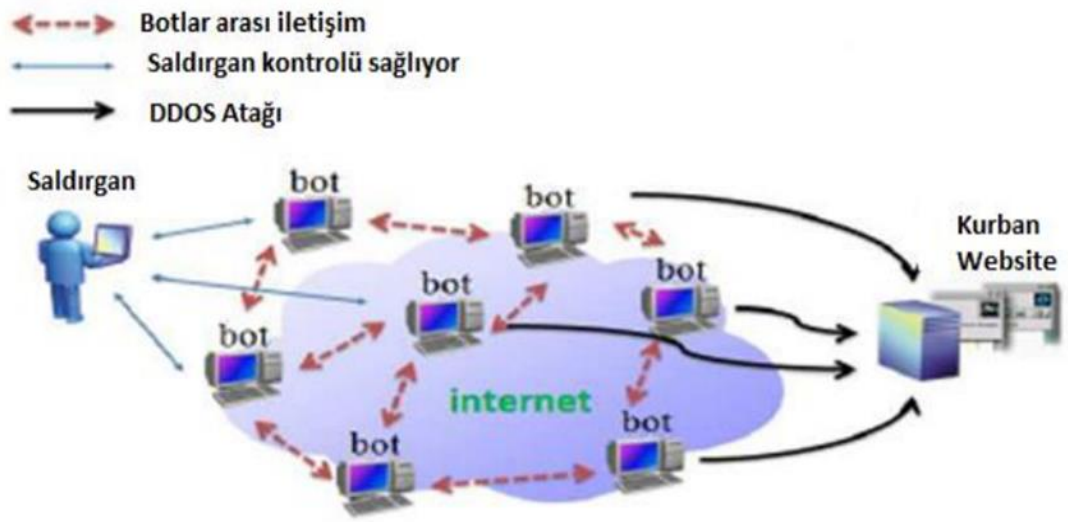
Ortadaki adam saldırısının belli başlı özelliği şu şekildedir:

- Dinlenme: Saldırgan, 2 yönlü arasında olan iletişimi dinler ve veriyi izlemektedir. Bu nedenle, kullanıcının şahsi bilgisini, şifresini ya da başka hassas verisini ele geçirmektedir.
- Manipülasyon: Saldırgan iletişimi manipüle edilerek gönderilen veriyi değiştirebilmektedir.
- Yönlendirme: Saldırgan, iletişimi yönlendirilerek mesajı diğer bir kişiye iletmektedir ya da amaçlanan bireyin mesajı almasını engelleyebilmektedir. Bu biçimde, kullanıcı arasında olan doğrudan iletişim kesilebilmektedir.
- Bu tür saldırıdan korunulması içi güvenli iletişim kanalı kullanılması, güçlü şifreleme yöntemi kullanılması, güvenilir ağa bağlanması ile kullanıcıya bilinçlenmesiyle güvenlik tedbirlerini uygulanması önemli olmaktadır.

3.1.5. BOTNET SALDIRISI

"Robot" anlamına gelen "BOT", belli görevleri insanlardan daha hızlı gerçekleştirilen ve tekrarlayan bir uygulama olmaktadır. "BOTNET", bir ağ üzerinden birbirine bağlanan birden fazla BOT'un kullanılmasıdır. BOTNET saldırısının 3 belli başlı unsuru vardır: Bot, bir komut ve kontrol (C&C) sunucusu ve bir Botmaster'dır. Botlar, bilgisayarlara bulaşan ve birbirlerine spam, önemli bilgiler ve şifreler göndermek üzere bot yöneticisi aracılığıyla kontrol edilebilen kötü amaçlı yazılımlardır. Ek olarak, bir ağı veya bilgisayarı devre dışı bırakarak günlük işleyişi bozabilir, kalıcı hasara neden olabilir ve ciddi ekonomik ve politik hasara neden olabilir [2].

Şekil 3.7.'de botlar arası iletişim saldırgan ile ddos atağı temsili şeklinde gösterilmektedir.



Şekil 3.7. Botnet saldırısı

2012 senesinde İran, binlerce yüksek performanslı uygulama sunucusu içeren bir botnet kullanarak ABD bankalarına büyük bir DDoS saldırısı başlattı. Saldırganlar, saniyede 60 GB'ı aşan torrentler oluşturmak için "itsoknoproblembro" adlı yeni bir araç kullanılmaktadır. Büyük finans kurumları ekonomik yavaşlamalar ve zaman zaman aksaklıklar yaşamıştır. En büyük 3 Amerika Birleşik Devletleri bankasına dair uygulanan saldırının İran'dan kaynaklandığı açıklandı fakat bu hal hiçbir zaman belirlenmemiştir [2].

4. MATERYAL VE METOT

Bilişsel radyo ağ yapısında spektrum algılama işlemi sırasında bilgi güvenliğini sağlamak için spektrum algılama yaklaşımı kullanılmıştır. Bu yaklaşıma göre, geçiş yapılacak olan kanallar önceden belirlenmektedir. Kanallar önceden belirlendiği için veri sahtecilik saldırılarına karşı oluşabilecek kanallar tespit edilerek hedef kanallar listesine alınmamaktadır.

Spektrum algılama yaklaşımı için önerilen bilişsel radyo ağ yapısında, birincil kullanıcılar, ikincil kullanıcı ve baz istasyonu görülmektedir. İkincil kullanıcıların iletişimi devam ederken birincil kullanıcıların kanal kullanımına ihtiyaç duyduğu durumlarda spektrum algılama işlemi yapılmaktadır. Daha sonra, elde edilen istatistik sonuçlarına göre, spektrum iş çıkarma oranları ile yapılacak olan hedef kanalları belirlemektedirler.

$$E[T_{pro}] = \frac{1}{\mu} + G_p * \frac{1}{\mu} * \frac{T_0}{1 - G_p T_0} \qquad (1)$$

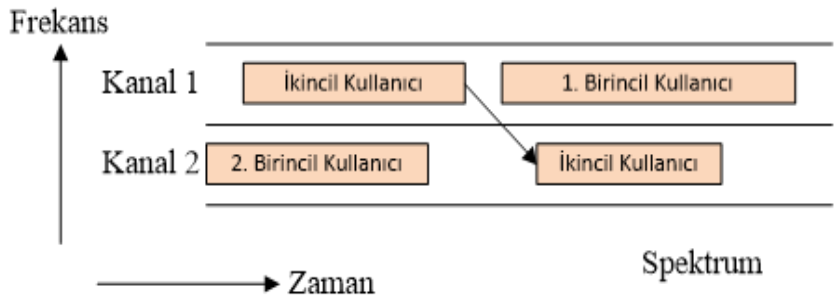
Denklem (1)'de, önceden tanımlı spektrum algılama veri sahtecilik saldırılarına karşı iş çıkarma oranının eşitliği görülmektedir. Bu denklemde; G_p birincil kullanıcıların yükünü, T_d servis süresini, $E[T_{pro}]$ toplam servis süresini ve T_0 ikincil kullanıcıların ilk defa spektrum veri sahtecilik saldırılarına karşı iş çıkarma işleminin başladığı zamanı göstermektedir. μ, ortam kullanım sıklığını temsil etmektedir. Servis süresi Denklem (2)'deki gibi hesaplanmaktadır

.

$$1 = T_d * \mu \qquad (2)$$

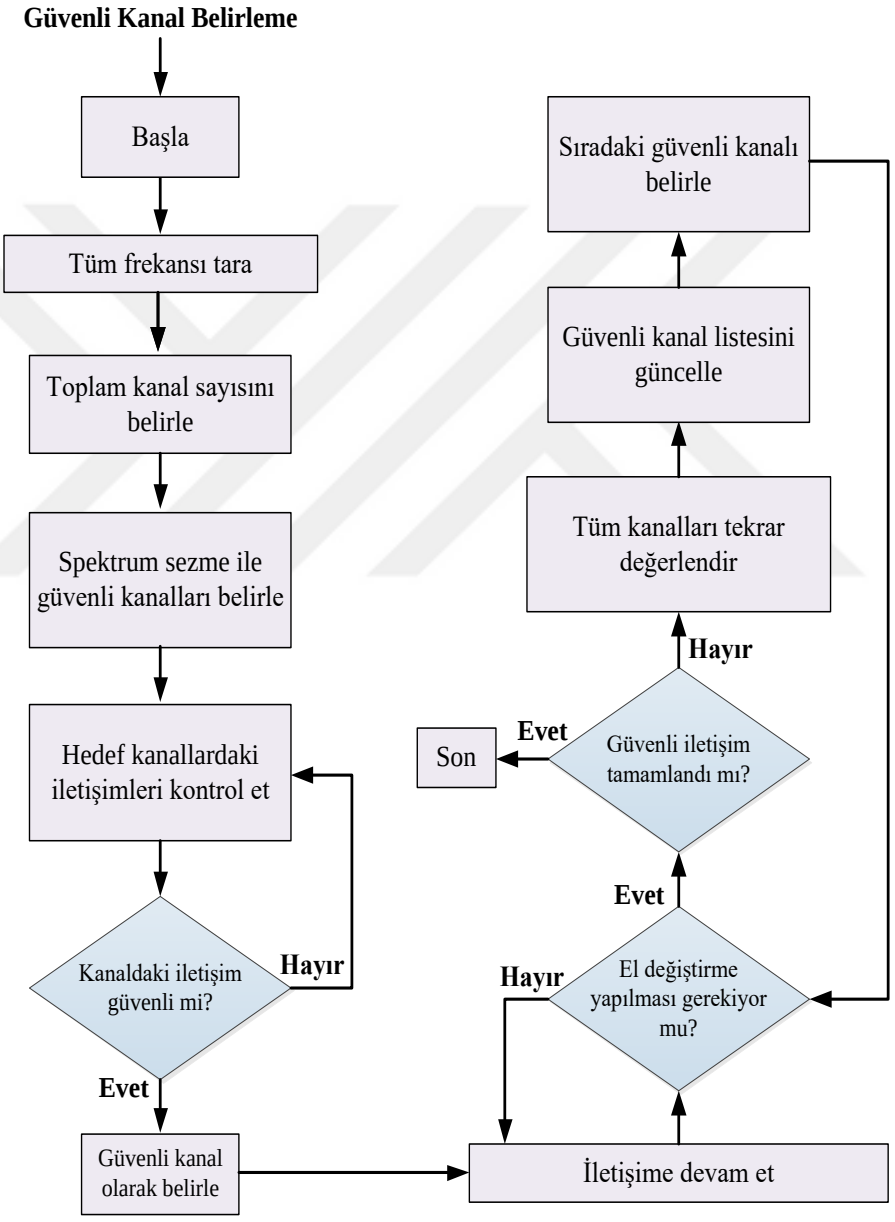
Farklı T_d ve T_0 değerleri için benzetim modeli üzerinde sonuçlar elde edilmiştir. λ_p birincil kullanıcıların ortalama yükünü, G_p birincil kullanıcıların yükünü ve N_p birincil kullanıcı sayısını temsil etmektedir. Denklem 3'te, bu üç parametre arasındaki hesaplama formülü verilmektedir.

$$\lambda_p = \frac{G_p}{N_p} \qquad (3)$$



Şekil 4.1. Güvenli haberleşme için spektrum algılama işlemi.

Şekil 4.1.'de, güvenli haberleşme için gerçekleştirilen spektrum algılama işlemi görülmektedir. İlk olarak, ikincil kullanıcının 1 numaralı kanalı kullandığı görülmektedir. Biraz zaman geçtikten sonra 1 numaralı birincil kullanıcı 1 numaralı kendi kanalını kullanma ihtiyacı duymaktadır. Bu durumda, ikincil kullanıcının kanal değiştirmesi gerekmektedir. 2 numaralı kanalda belirli süre boyunca 2 numaralı birincil kullanıcının iletişim yaptığı sonrasında ise iletişimini sonlandırdığı görülmektedir. İkincil kullanıcı bu durumda, kanal değiştirme işlemini önceden güvenli olduğu yaklaşım ile belirlenen 2 numaralı kanala yapmaktadır.



Şekil 4.2. Güvenli haberleşme için spektrum algıma işleminin akış şeması.

Şekil 4.2.'te, güvenli haberleşme için önerilen spektrum algılama işleminin akış şeması görülmektedir. İlk olarak, tüm frekans taranmaktadır. Frekanstaki toplam kanal sayısı

belirlenmektedir. Spektrum sezme yöntemi ile güvenli kanallar belirlenmektedir. Hedef kanallardaki iletişimler kontrol edilmektedir. Mevcut kanaldaki iletişimin güvenli olup olmadığı sorgulanmaktadır. Güvenli değil ise, hedef kanallardaki iletişimler tekrar kontrol edilmektedir. Güvenli ise, mevcut kanal güvenli olarak belirlenerek iletişime devam edilmektedir. El değiştirme işleminin yapılıp yapılmayacağı kontrol edilmektedir. El değiştirme gerekmiyorsa iletişime devam edilmektedir. Gerekiyorsa, güvenli iletişimin tamamlanıp tamamlanmadığı kontrol edilmektedir. Tamamlandıysa akış şeması sonlandırılmaktadır. Tamamlanmadıysa, tüm kanallar tekrar değerlendirilmektedir. Güvenli kanal listesi güncellenmektedir. Bu işlemler veri sahtecilik saldırılarına karşı mevcut kanalların kontrol edilip el değiştirme işlemin başarılı bir şekilde yapılmasını sağlamaktadır. Sonrasında, sıradaki güvenli kanal belirlenerek işlem akışı devam etmektedir.

4.1. BULGULAR

Güvenli bir haberleşme için kullanılan bilişsel radyo ağlarda spektrum algılama işlemi aynı zamanda toplam haberleşme süresinde de büyük avantaj sağlamaktadır. Bunun yanında, güvenli kanal bulma işlemi oldukça düşük bir hata oranı ile gerçekleştirilmiştir.

Tablo 4.1. Benzetim Modeli Parametreleri

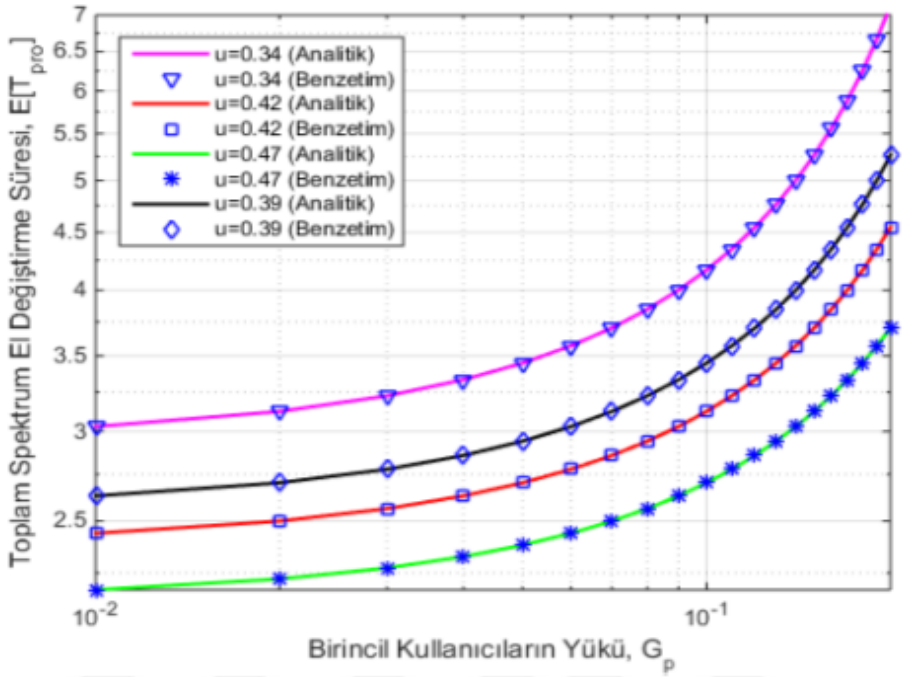
Parametre	**Değer**	**Birim**
Ortalama veri hızı	1000	Kbps
Modülasyon tekniği	-	BPSK
Ortalama iletim gücü	20	Mw
Ortalama gecikme	5	µs
Benzetim süresi	3600	S
Ortalama anten kazancı	2	Db
Ortam erişim tekniği	-	TDMA
Yaklaşık kapsama alanı	~ 5	m^2
Yol kaybı modeli	-	Serbest
Mevcut frekans	2400	Mhz

Tablo 4.1'de, benzetim modelinin parametreleri verilmektedir. Parametreler verilirken değerleri ve birimleri de ayrı ayrı belirtilmiştir. Modülasyon tekniği ve ortam erişim tekniğinin değerleri olmadığı için birim kısmında bu teknikler belirtilmiştir. TDMA, zaman bölmeli çoklu erişim tekniğini temsil etmektedir. BPSK ise, iki faz anahtarlamalı kaydırma tekniğini temsil etmektedir.

Tablo 4.2. Benzetim Yazılımı Bilgisayar Özellikleri

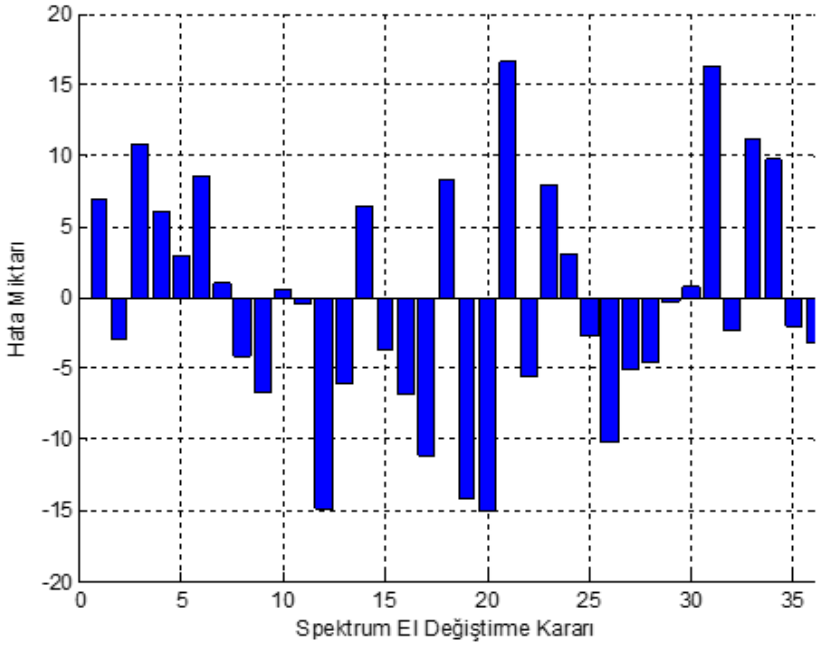
Özellik Bilgisi	**Değer**
Bilgisayar işlemcisi	Intel(R) Core(TM) i7-4700HQ
Bilgisayar dahili hafızası	12 GB
Bilgisayar dahili görüntü kartı	Intel(R) HD Graphics 4600
Bilgisayar işletim sistemi	Windows 10 Pro x64
Benzetim yazılımı	Riverbed
Bilgisayar harici görüntü kartı	NVIDIA GeForce GT 750M
Benzetim yazılımı modülü	Kablosuz haberleşme
Benzetim yazılımı versiyonu	18.7.1 (Build 142 32-bit)
Benzetim yazılımı işlemci tipi	586
Benzetim yazılımı işlemci sayısı	8

Tablo 4.2'de, benzetim yazılımı için kullanılan bilgisayarın özellikleri verilmektedir. Hem bilgisayarın hem de benzetim yazılımının karakteristik özellikleri ayrı ayrı belirtilmiştir. Ekran kartı dahili ve harici olmak üzere iki farklı şekilde verilmiştir. Benzetim yazılımında bir çok farklı modül olduğu için kablosuz haberleşme modülü kullanıldığı vurgulanmıştır.



Şekil 4.3. Spektrum algılama işleminin toplam gecikme süreleri.

Şekil 4.3.'te, spektrum algılama işleminin toplam gecikme süreleri görülmektedir. Ortam kullanım sıklığının farklı değerleri için, birincil kullanıcıların yükü arttıkça el değiştirme süreleri de artmaktadır. El değiştirme sürelerinin artması veri sahtecilik saldırılarının kontrolünü zorlaştırması sebebi ile veri sahtecilik saldırılarına karşı iş çıkarma oranını da olumsuz yönde etkilemektedir.



Şekil 4.4. Veri sahtecilik saldırılarına karşı iş çıkarma hata oranları.

Şekil 4.4.'te, Veri sahtecilik saldırılarına karşı iş çıkarma hata oranları görülmektedir. Hata oranlarının %15 ile-%15 arasında değiştiği fakat yoğun olarak %5- %10 bandında olduğu görülmektedir. Güvenli bir el değiştirme sağlamasının avantajı yanında hata oranlarının bu kadar düşük olması kabul edilebilir bir durumdur.

Tablo 4.3. Benzer Çalışma ile Karşılaştırma

Makale	**Ortalama Hata Oranı**	**Toplam Gecikme**
Bu Makale	% 8	3,8 µs
Turkyilmaz vd. (2023)	% 17	4,7 µs

Tablo 4.3.'te, literatürdeki benzer çalışma ile karşılaştırma verileri verilmektedir. Ortalama hata oranı ve toplam gecikme parametreleri incelendiğinde önerdiğimiz çalışmanın daha iyi sonuçlar verdiği net bir şekilde görülmektedir. Hem parametre hem de veri güvenliği açısından bu yaklaşımın kullanılabilir olduğu net bir şekilde gözler önüne serilmektedir.

5. SONUÇ

Bilişsel radyo ağlarda sistem modeli, spektrumu boşta (serbest) için algılanacak bir birincil kullanıcıdan (PU), PU'nun spektrumunu algılayan 'S' ikincil kullanıcılardan, karar sonuçlarını sonuçlandıran ve tahsis eden bir füzyon merkezinden (FC) oluşur. Boşta spektrumu SU'ya. 'U', SU'ların 'S' sayısı içindeki kötü niyetli kullanıcıların sayısı olsun. Tespit edilecek kötü niyetli kullanıcılar (MU)'lar üç koşula tabidir:

- Her zaman 'evet' – SU, öyle olmadığında her zaman spektrumun boşta olduğunu bildirir.
- Her zaman 'Hayır'- SU her zaman spektrumun meşgul olmasa bile meşgul olduğunu bildirir.
- Yaramaz – gerçek rapordan bağımsız olarak rastgele raporlar.

Bir zaman dilimi 't' üzerindeki her SU, spektrumu algılar ve algılanan sonucu bir spektrum algılama tekniği kullanarak füzyon merkezine gönderir. Her SU, Veri sahtecilik saldırılarına karşı iş çıkarma hata oranlarının değerlerine göre tahmin eder.

"K", bir "T" zaman aralığı boyunca spektrumu algılayan SU'ların sayısı olsun ve "M", tüm saldırı stratejileriyle ilgili MU'ların sayısı olsun. Ayrıca füzyon merkezi en fazla kabul edilen modeldir.

"K", bir "T" zaman aralığı boyunca spektrumu algılayan SU'ların sayısı olsun ve "M", tüm saldırı stratejileriyle ilgili MU'ların sayısı olsun. Ayrıca füzyon merkezinin, tüm SSDF saldırgan türlerini tanımlamak için önemli potansiyele ve birikmiş verilere sahip en güçlü kullanıcı olduğu düşünülmektedir. Kanal koşullarının iletim (kontrol kanalları) için mükemmel olduğu varsayılır ve tüm SU'lar, PU'nun varlığını ve yokluğunu tespit etmek için spektrum algılama tekniğini kullanır. Ayrıca CR sisteminin kapsama alanının küçük olduğu varsayıldığından yol kaybı ihmal edilmektedir.

Sonuç olarak bilişsel radyo ağlarda, birincil kullanıcılar lisanslı kullanıcılar ve ikincil kullanıcılar da lisanslı olmayan kullanıcılar veya fırsatçı kullanıcılar olarak tanımlanmaktadır. İkincil kullanıcıların temel hedefi, lisanlı olan birincil kullanıcıların boş olan spektrumlarını çeşitli tekniklerle tespit ederek fırsatçı olarak kullanmaktır. İkincil kullanıcı birincil kullanıcının boş frekans spektrumunu kullanırken, birincil kullanıcının kendi spektrumunda iletişim kurma ihtiyacı olabilmektedir. Bu durumda, ikincil kullanıcının iletimini sonlandırması veya farklı bir spektruma geçerek haberleşmesine devam etmesi gerekmektedir. Bu çalışmada, spektrum algılama tekniği kullanılarak bilişsel radyo ağlarda güvenli bilgi iletimi yapılmıştır. Bu çalışmada kullanılan spektrum algılama işleminde ise, geçiş yapılacak olan frekans bantları önceden belirlenerek tanımlandığı için bilginin izinsiz olarak erişimi engellenmiştir. Bu işlemler sonucu veri sahtecilik saldırılarına karşı hem önlem alınmış olup hem de verilerin daha güvenli ve hızlı iletilmesi sağlanmıştır.

Gelecek çalışmalarda, bilişsel radyo ağlarda yanlış sezme işlemine sebep olabilecek durumlara karşı güvenlik önlemleri ele alınabilir.

KAYNAKÇA

Ağaoğlu, E. (2010). Bilişsel Radyo Şebekelerinde Yapay Sinir Ağları ile Spektrum Yöntemi. Ankara Üniversitesi Fen Bilimleri Enstitüsü Elektronik Mühendisliği Anabilim Dalı Yüksek Lisans Tezi.

Atasever, S. (2019). Siber Terör ve DDoS. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi* 23 (1), 238-244.

Başkaya, D. (2020). Çevrimiçi Sistemlerde Makine Öğrenme Yöntemi İle Dağıtılmış Hizmet Reddi (DDoS) Saldırılarının TEspiti. Ankara: Ankara Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Yüksek Lisans Tezi.

Bayrakdar, M. E. (2015). Bilişsel radyo ağlarında spektrum el değiştirme. *SAÜ Fen Bil Dergisi* 19 (3), 291-302.

Bayraktar, M. E. (2017). Kablosuz Bilişsel Radyo Ağlarında Spektrum El Değiştirme İçin Öncelik Kuyrukları ve Yapay Zeka Teknikleri. *Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi,* 6 (2), 303-315.

Bulut, İ. (2017). Analiz Sürecini Atlatmaya Çalışan Zararlı Yazılımlar ve Derin Öğrenme Temelli Zararlı Yazılım Tespiti. İstanbul: Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Yüksek Lisans Tezi.

Büber, E. (2017). Oltalama Saldırılarında Kullanılan URL'lerin Makine Öğrenmesi Teknikleri ile Tespit Edilmesi. İstanbul: Marmara Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Yüksek Lisans Tezi.

Çakır, A. C. (2015). Bilişsel Radyoda Enerji Sezme Tabanlı Spektrum Algılama. 4th International Vocational Schools Symposium.

Çiflikli, C. (2017). Bilişsel Radyo Sistemleri için Kör Spektrum Algılama Yöntemlerinin Farklı Haberleşme Kanallarındaki Performans Analizi. *Gaziosmanpaşa Bilimsel Araştırma Dergisi* 6, 122-132.

Dicle, S. Z. (2022). Ortadaki Adam Saldırısı (MITM). *Avrupa Bilim ve Teknoloji Dergisi* 42, 100-107.

Hamid, M. (2008). Dynamic spectrum access in cognitive radio networks: Aspects of mac layer sensing. Karlskrona Blekinge Teknoloji Enstitüsü Elektrik Mühendisliği Anabilim Dalı Yüksek Lisans Tezi.

Haykin, S. (2005). Cognitive radio: brain-empowered wireless communications. *IEEE Journal on Selected Areas in Communications,* 23 (2), 201-220.

İngök, S. (2012). Bilişsel Radyoda Özdeğer Tabanlı Spektrum Sezme Yöntemleri. İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü Elektronik ve Haberleşme Mühendisliği Anabilim Dalı Yüksek Lisans Tezi.

İpekbayrak, M. (2019). APT Yazılımı ve APT ile Yapılan Saldırılara Karşı Güvenlik Yazılımı. İstanbul: İstanbul Üniversitesi Cerrahpaşa Lisansüstü Eğitim Enstitü Bilgisayar Mühendisliği Anabilim Dalı Yüksek Lisans Tezi.

Jahja, B. (2015). Bilişsel Radyo Ağlarında Spektrum Paylaşma. Uludağ Üniversitesi Fen Bilimleri Ensitütüsü Elektronik Mühendisliği Anabilim Dalı Yüksek Lisans Tezi.

Kara, Ş. (2022). Siber Güvenlik Analizi İçin Yeni Bir Siber Saldırı Simülatörü Geliştirilmesi. Sakarya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar ve Bilişim Mühendisliği Anabilim Dalı Yüksek Lisans Tezi.

Kılıç, E. T. (2015). Siber Saldırıları İzleme Yöntemleri ve Zararları Yazılım Analizi. Gazi Üniversitesi Kazaların Çevresel ve Teknik Araştırması Anabilim Dalı Yüksek Lisans Tezi.

Koçkaya, K. (2019). Bilişsel Radyo Ağlarında Çevrimiçi Öğrenme Tabanlı İşbirlikçi Spektrum Algılama Algoritmasının Sönümlü Kanallardaki Başarımı. *International Symposium on Innovative Approaches İn Scientife Studies* 4 (1), 153-157.

Kulaç, S. (2013). Enerji Verimli İşbirlikçi DTV Spektrum Algılama. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi* 28 (1), 77-84.

Masum, E. (2017). Dağıtık Servis Dışı Bırakma Saldırılarının İncelenmesi ve Korunma Yöntemleri. Ankara: Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Disiplinlerarası Adli Bilimler Anabilim Dalı Yüksek Lisans Tezi.

Oktuğ, S. (2014). Genişbant Bilişsel Radyo Ağları Tasarım ve Uygulamaları. İstanbul Sanayi Odası- İstanbul Teknik Üniversitesi .

Sadreddini, Z. (2018). Bilişsel Radyo Ağlarında Çok Ölçütlü Karar Verme Yöntemlerine Dayalı Yeni Bir Spektrum Yönetim Modeli. Trabzon: Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Doktora Tezi.

Sevinç, N. (2008). Tedarik Zinciri Yönetiminde Bilgi Teknolojilerinin Kullanılması ve Önemi. Edirne: Trakya Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı Yüksek Lisans Tezi.

Şahinaslan, Ö. (2013). Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma. Edirne: Trakya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Yüksek Lisans Tezi.

Tek, S. (2022). Türkiye ve Dünyada Gerçekleştirilen Siber Saldırı Yöntemlerinin ve Bu Saldırılara Karşı Alınan Önlemlerin İncelenmesi. Edirne: Trakya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Yüksek Lisans Tezi.

Yalçın, S. (2021). LPWAN Standartları Tabanlı Bilişsel Radyo Ağları İçin Spektrum Algılama Yaklaşımı. *Adıyaman Üniversitesi Mühendislik Bilimleri Dergisi* 15, 535-547.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı :HÜSEYİN DOĞAN

Yabancı Dili :İNGİLİZCE

ÖĞRENİM DURUMU

Derece	Alan	Okul/Üniversite	Mezuniyet Yılı
Y. Lisans	Siber güvenlik	Düzce Üniversitesi	2024
Lisans	Bilgisayar mühendisliği	Erciyes Üniversitesi	2019
Lise	Fen	Şeker Anadolu Lisesi	2012

YAYINLAR

Hüseyin Doğan, M. Enes Bayrakdar, Bilişsel Radyo Ağlarda Spektrum Algılama Veri Sahtecilik Saldırılarına Karşı İş Çıkarma Oranının Artırılması, 4. Ulusal Bilimsel Araştırmalar Kongresi, 73-96, 16-17 Temmuz 2024, Ankara, Türkiye.