T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KABLOSUZ ALGILAYICI AĞLAR İÇİN DİNAMİK KANAL ATLAMALI GÜVENLİK SİSTEMİ TASARIMI

DOKTORA TEZİ

Murat ÇAKIROĞLU

Enstitü Anabilim Dalı : ELEKTRİK ELEKTRONİK MÜH.

Enstitü Bilim Dalı : ELEKTRONİK

Bu tez 11/08/2008 tarihinde aşağıdaki jüri tarafından Oybirliği ile kabul edilmiştir.

Prof. Dr. Hüseyin EKİZ
Jüri Başkanı

Yrd. Doç Dr. A.Turan ÖZCERİT
Üye

Prof. Dr. Etem KÖKLÜKAYA
Üye

Doç. Dr. Akif KUTLU
Üye

Doç. Dr. İsmail ERTÜRK
Üye

TEŞEKKÜR

Bu doktora çalışmasında danışmanlığımı yapan Yrd. Doç. Dr. Ahmet Turan ÖZCERİT hocama, bana ve bölümdeki tüm arkadaşlarıma daima destek olan Dekanımız Prof. Dr. Hüseyin EKİZ hocama, benim bu günlere gelmemde çok fazla emeği bulunan anne, baba ve ablam'a, doktora süresince bana hep destek olan tüm bölüm arkadaşlarıma ve beni sürekli motive eden her zaman maddi manevi desteğini esirgemeyen eşime teşekkür etmeyi bir borç bilirim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

ABSTS :Anomali tabanlı Boğma Saldırıları Tespit Sistemi
ACK : ACKnowledgement (Kabul)
ADC : Analog to Digital Converter
DKA : Dinamik Kanal Atlama
AKS : Alt Kontrol Sınırı
BDO : Boğulmuş Düğüm Oranı
BER : Bit Error Rate
CDMA : Code Division Multiple Access
CRC : Cyclic Redundancy Check
DCF : Distributed Coordination Function
CSMA : Carrier Sense Multiple Access
CSMA/CA : Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD : Carrier Sense Multiple Access with Collision Detection
CTS : Clear to Send
CW : Contention Window
DARPA : Defense Advanced Research Projects Agency
DoS : Denial of Service
DSN : Distributed Sensor Network
DSSS : Direct Sequence Spread Spectrum
ETF : Enerji Tüketim Fazlalığı
ETM : Enerji Tüketim Miktarı
FHSS : Frequency Hopping Spread Spectrum
FDMA : Frequency Division Multiple Access
GPS : Global Position System
HES : Hizmet Engelleme Saldırıları
HPO : Hatalı Paket Oranı
IDS : Intrusion Detection System

IEEE : Institute of Electrical and Electronics Engineers
ISM : Industries, Scientific, Medical
ISO : International Standards Organization
KAA : Kablosuz Algılayıcı Ağlar
LLC : Logical Link Control
MAC : Medium Access Control
MEMS : Micro Electro Mechanical System
MIT : Massachusetts Institute of Technology
NAV : Network Allocation Vector
NASA : National Aeronautics and Space Administration
OMNET : Objective Modular Network Test-bed in C++
PBO : Paket Bozma Oranı
PBO : Paket Engelleme Oranı
PDR : Packet Delivery Ratio
PDAS : Periyodik Dinleme Aralığı Saldırganı
PKAS : Periyodik Kontrol Aralığı Saldırganı
PKS : Periyodik Küme Saldırganı
PTO : Paket Teslim Oranı
P2P : Peer to Peer
RKA : Rasgele Kanal Atlama
RTS : Request to Send
RSSI : Received Signal Strength Indicator
SFD : Start of Frame Delimiter
S-MAC : Sensor Medium Access Control
SOSUS : Sound Surveillance System
SYNC : Synchronization Packet
SYO : Saldırgan Yaşam Oranı
TDMA : Time Division Multiple Access
TinyOS : Tiny Operating System
T-MAC : Timeout MAC
TO : Tüketme Oranı
ÜKS : Üst Kontrol Sınırı
VPA : Veri Paketi Saldırganı

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar Kelimeler: Kablosuz Algılayıcı Ağlar, Güvenlik, Sızma tespiti, Boğma Saldırıları

Kablosuz Algılayıcı Ağ (KAA)'lar, bakım gerektirmeden uzun yıllar çalışabilmeleri ve çok çeşitli alanlarda kullanılabilmeleri sebebiyle hem endüstriyel uygulamalarda hem de akademik çalışmalarda çok popüler bir alan haline gelmiştir. KAA'ları meydana getiren düğümler, genellikle iki adet standart pil ile beslenen, veri saklama/işlem kapasitesi sınırlı olan ve kısa mesafeli kablosuz ortam üzerinden haberleşen tümdevrelerdir. Kaynakları sınırlı olan bu düğümlerin, çoğu uygulama için dış dünyada bulunması ve kablosuz ortam üzerinden haberleşmesi KAA'ların çeşitli saldırılara maruz kalma riskini arttırmaktadır.

Radyo sinyalleri göndererek ortamdaki paketlerin bozulmasına veya iletişim ortamının sürekli meşgul olmasına neden olan boğma saldırıları (jamming attacks) KAA'lar için son derece ciddi tehditlerden birisidir. Bu saldırılar, düğümlerin iletişimlerini engelleyerek belirli bir süreyle servis dışı kalmalarına sebep olabildiği gibi enerji kaynaklarının hızlı bir şekilde tükenmesine yol açarak düğüm ömrünün azalmasına da sebep olabilmektedir. Özellikle güvenliğin en önemli tasarım ölçütü olduğu askeri ve tıbbi uygulamalarda kullanılan KAA'ların boğma saldırılarına karşı korunması kaçınılmaz bir gerekliliktir.

Bu tez çalışmasında, KAA'larını boğma saldırılarına karşı dayanıklı hale getirmek üzere boğma saldırgan modellerinin tespit edilmesine imkân tanıyan Anomali tabanlı yöntem kullanılarak yeni bir Boğma Saldırı Tespit Sistem (ABSTS) tasarımı gerçekleştirilmiştir. Saldırıların tespitinden sonra düğümlerin bu saldırılara rağmen iletişimlerini gerçekleştirebilmesine ve olumsuz saldırı etkilerinden kurtulabilmesine olanak sağlayan Dinamik Kanal Atlama (DKA) adında yeni bir savunma yöntemi tasarlanmıştır. Gerçekleştirilen detaylı benzetim sonuçlarına göre, çeşitli boğma saldırgan modelleri, geliştirilen ABSTS yöntemi ile yüksek sezme ve düşük hatalı sezme oranları sağlanarak tespit edilebilmektedir. Boğma saldırılarına karşı savunma yöntemi olarak geliştirilen DKA metodu sayesinde ise düğümler farklı saldırı senaryolarına rağmen iletişimlerini yüksek başarım oranlarıyla devam ettirebilmektedir.

A SECURITY SYSTEM DESIGN WITH DYNAMIC CHANNEL HOPPING METHOD FOR WIRELESS SENSOR NETWORK

SUMMARY

Keywords: Wireless Sensor Networks, Security, Intrusion Detection, Jamming Attacks

Wireless Sensor Networks (WSNs) are of high interest both in research studies and in industrial applications since they can work for a long time without additional maintenance. The nodes building a WSN, which are typically supplied by standard batteries, are in fact integrated circuits communicating relatively in a short distance and have a very limited data processing/storing capacity. As they communicate in wireless medium and generally located outside, they are prone to high risk of attacking scenarios.

The jamming attacks, emitting radio signals continuously to the wireless medium in order to disturb an ongoing communication, corrupting packets or keeping the channel busy all the time, are one of the most destructive threats for WSNs. Not only can they cause the nodes to be out of service but also shorten their operational working cycles. The WSNs must have robust and adaptive counter measures against such potential threats especially in military and medical applications in which system faults cannot be tolerated in any case.

In this thesis, in order to detect jamming attacks, an anomaly based jamming detection mechanism (AJDM) has been designed. Since the AJDM itself cannot guarantee a healthy operation mode of wireless communication, a dynamic channel hopping (DCH) method has also been designed to preserve the proper networking conditions. According to the simulation results, the well-known attacking scenarios can be detected by the AJDM by maintaining high detection rates along with low false positive rates. Additionally, the nodes continue normal mode of operation by using the DCH when a jamming attack is launched by an adversary node.

BÖLÜM 1. GİRİŞ

Bilgi çağı olarak adlandırılan yüzyılımızda, bilgilerin daha hızlı ve kolay bir şekilde işlenmesi yönünde talep sürekli artarken tasarımcılar artan bu talepleri karşılamak üzere daha küçük olmasına karşın daha gelişmiş özelliklerdeki donanımları tasarlamaya çalışmaktadır. Bu arz-talep ilişkisi ve rekabet ortamı teknolojik ürünlerin maliyetlerinin düşmesine ve böylece kullanımının yaygınlaşmasına yol açmaktadır. Kablosuz iletişim teknolojileri de bu rekabet ortamından nasibini almış ve günümüzde dizüstü bilgisayarlar, cep telefonları, cep bilgisayarı, küresel konumlandırma cihazları gibi kablosuz olarak haberleşen birçok ticari ürün dünya çapında milyonlarca kişi tarafından kullanılır hale gelmiştir. Son yıllarda işlemci, hafıza ve radyo frekans ile çalışan alıcı/verici teknolojilerindeki gelişmeler çok çeşitli algılayıcıların (sensör) kablosuz olarak haberleşebilen cihazlara entegre edilebilmesinin önünü açmış ve sonuçta bir bölgenin uzaktan gözlemlenmesine, izlenmesine ve çeşitli multimedya iletişimlerin gerçekleştirilmesine olanak sağlayan kablosuz algılayıcı ağlarının geliştirilmesini sağlamıştır. Kablosuz olarak haberleşen bu küçük ve taşınabilir cihazlardan oluşan algılayıcı ağlar sağlık alanlarından askeri alanlara, bir binanın güvenliğinin sağlanmasından orman yangınlarının önceden tespitine kadar çok çeşitli alanlarda kullanılmaya başlanmıştır [1].

Kablosuz algılayıcı ağlar, diğer kablosuz ağlardan kendine has bazı farklılıklar sebebiyle ayrılmaktadır. Örneğin kablosuz algılayıcı ağlarda düğüm yoğunluğu diğer ağlara oranla son derece fazla iken veri iletim hızları oldukça düşüktür. Bunun yanında ağı meydana getiren algılayıcı düğümlerinin boyutları diğer ağlardaki düğümlere göre çok küçük (birkaç cm^3), gönderme/alma güçleri ise oldukça düşüktür. Kablosuz algılayıcı ağları diğer kablosuz ağlardan ayıran en önemli farklardan birisi de algılayıcı düğümlerinin son derece kısıtlı donanımsal kaynaklara sahip olması ve enerji kaynaklarının çoğu uygulama için yenilenememesidir. Genelde 8-bitlik bir işlemciye, kilobayt seviyesinde kod ve veri hafıza birimlerine

sahip olan algılayıcı düğümlerinden oluşan kablosuz algılayıcı ağlar için geliştirilen uygulamaların veya protokollerin bu sınırlamaları dikkate alması gerekmektedir. Ayrıca kablosuz algılayıcı düğümlerinin yaşam sürelerini, pil ömürleri belirlediği için geliştirilen protokol veya uygulamalar mümkün olan en düşük güç tüketimini hedeflemelidir. Kablosuz algılayıcı ağlarını diğer ağlardan farklı kılan bir diğer özellik de düğümlerin genelde dış ortamda ve zor koşullar altında çalışma gerekliliğidir. Örneğin bir bölgenin ekolojik yapısının gözlemlenmesini sağlayan kablosuz algılayıcı ağı çeşitli çevresel zorluklarla karşı karşıyadır. Düğümlerin sel, fırtına, yangın v.b gibi doğal afetlere maruz kalması muhtemel olabileceği gibi yüksek basınç, sıcaklık ve nem gibi zor koşullarda altında da çalışması gerekebilir. Bunun dışında ağdaki düğümlerin bir kısmı rüzgâr, sel v.b. sebebiyle yer değiştirebilir, kaybolabilir veya bozulabilir. Tüm bunların da ötesinde ve belki de en kötüsü, düğümler kötü niyetli kişiler tarafından çalınabilir, zarara uğratılabilir veya kötü amaçlı olarak yeniden programlanabilir. Böylece yeniden programlanan düğümler ağdaki bilgilerin çalınmasını, değiştirilmesini veya bozulmasını sağlayarak ağın güvenirliğinin yitirilmesine sebep olabilir. Literatürdeki çalışmalarda, ticari algılayıcı düğümlerinin kurcalamaya karşı dayanıklı olmaması sebebiyle birkaç dakika içerisinde yeniden programlanabildiği gösterilmiştir [2]. Kablosuz algılayıcı ağlardaki bu güvenlik açıkları çeşitli saldırı türlerinin üretilmesini kolaylaştırmakta ve araştırmacıları bu saldırılara karşı çözüm yöntemleri geliştirmeye zorlamaktadır. Hizmet engelleme saldırıları kablosuz algılayıcı ağlar için belki de en zararlı ve en tehlikeli saldırılardan olması sebebiyle diğer saldırı türlerinden ayrılmakta ve araştırmaların en fazla çözüm aradığı saldırılar haline gelmektedir.

Bir ağdan beklenen görevleri/hizmetleri aksatmak ya da tamamen engellemek üzere gerçekleştirilen kötü niyetli herhangi bir müdahale manasına gelen Hizmet Engelleme (Denial of Service-DoS) saldırıları geleneksel ağlarda olduğu gibi kablosuz algılayıcı ağlarda da sıkça rastlanılan bir saldırı türüdür. Bu saldırılar donanımsal arazılar, yazılımsal hatalar, kaynakların tükenmesi gibi koşulların ortaya çıkmasına ve dolayısıyla ağın kendisinden beklenen işlemleri yerine getirememesine sebep olmaktadır [3]. Literatürde yönlendirme, ortam erişim ve fiziksel katmanının fonksiyonlarını bozulmasına/aksamasına sebep olan çeşitli DoS saldırı türleri bulunmaktadır.

Karlof ve diğerleri gerçekleştirdikleri çalışmada kablosuz algılayıcı ağlarında yönlendirme katmanının çalışmalarını bozmayı ya da engellemeyi hedefleyen altı tür hizmet engelleme saldırısı olduğunu göstermiştir [4]. Detayları 3. Bölümde verilen Hello Flood, Sybil, solucan deliği (Wormholes), çıkış deliği (Sinkholes), yanlış yönlendirme (Misdirection) ve seçmeli iletim (Selective forwarding) saldırılarının genel amacı, düğümlerin yönlendirme yollarını değiştirmek, bozmak ve böylece iletişimlerin aksamasına, paket kaybının ve enerji tüketiminin artmasına yol açmaktır.

Wood ve diğerleri ortam erişim katmanını etkileyen DoS saldırılarını çarpışma (collision), tüketme (exhaustion) ve eşitsizlik (unfairness) olmak üzere üç kategoride toplamaktadır [3]. MAC katmanındaki boğma saldırıları olarak adlandırılan bu saldırılar düğümlerin paylaşımlı olan iletişim kanalına erişmek için kullandığı kuralları ihlal etmekte ve böylece iletişimin aksamasına ya da bozulmasına yol açmaktadır. Bu çalışmadan esinlenerek MAC katmanını etkileyen birçok boğma türündeki hizmet engelleme saldırıları geliştirilmiştir. Xu ve diğerleri yaptıkları çalışmada çarpışma saldırganı ile aynı görevi gören reaktif (reactive) saldırgan modelini ve tüketme saldırganı ile aynı görevi gören aldatıcı (deceptive) saldırgan modellerini algılayıcı düğümleri üzerinde gerçeklemiştir [5]. Law ve diğerleri ise ilk olarak S-MAC protokolü için dinleme aralığı, kontrol aralığı ve veri paketi saldırgan modellerini tanımlarken, ikinci çalışmalarında farklı ortam erişim protokolleri için enerji-etkin saldırgan modelleri geliştirmiştir [6,7]. Wood ve diğerleri gerçekleştirdikleri bir diğer çalışmada; kesme (interrupt), aktivite (activite), tarama (scan) ve darbe (pulse) saldırgan modellerini tanımlamıştır [8]. MAC katmanındaki boğma saldırıları ile ilgili detaylı bilgiler Bölüm 4'de verilmektedir.

Wood ve diğerleri gerçekleştirdikleri çalışmada fiziksel katmandaki hizmet engelleme saldırılarını boğma saldırıları ve kurcalama saldırıları olarak iki kategoride toplamıştır [3]. Fiziksel katmandaki boğma saldırıları MAC katmanındaki saldırılara benzer şekilde düğüm iletişimlerini tamamen kesmeyi hedeflemektedir. Fiziksel ve MAC katmanındaki boğma saldırıları birbirleriyle ilişkili olmakla beraber aralarındaki en büyük fark, MAC katmanındaki boğma saldırılarının ortam erişim kurallarının açıklarından faydalanması, fiziksel katmandaki boğma saldırılarının ise

sürekli veya aralıklarla kanal frekansına eş frekanslı sinyal göndererek iletişim kanalını düğümler tarafından kullanılmasını engellemesidir. Literatürde kablosuz algılayıcı ağlar için sürekli (constant) ve rasgele (random) olmak üzere iki tür fiziksel katman saldırganı geliştirilmiştir [5]. Saldırganlar isimlerinde de anlaşılacağı üzere sürekli ve rasgele aralıklarla kanal frekansına eşit frekanslı sinyal göndermekte ve böylece iletişim kanalını meşgul etmektedirler. Kurcalama olarak adlandırılan bir diğer fiziksel katman DoS saldırılarında ise düğümlerin ele geçirilmesi, fiziksel olarak hasara uğratılması ya da kötü amaçlı olarak programlanması hedeflenmektedir.

MAC ve fiziksel katman fonksiyonlarını felç ederek düğüm iletişimlerinin tamamen kesilmesine ve enerji tüketimlerinin artmasına neden olan boğma saldırıları, kablosuz algılayıcı ağlar için en tehlikeli saldırıların başında gelmektedir. Ancak literatürde, son derece tehlikeli olan bu saldırıların tespitine ve çözümüne yönelik çok fazla sayıda çalışma bulunmamaktadır. Kablosuz algılayıcı ağlar için oldukça yeni ve bakir olan konu bu tezin de çıkış noktasını oluşturmuş ve çeşitli boğma saldırı türlerinin ilk önce başarılı bir şekilde tespit edilmesi daha sonra da saldırılardan kurtulma yöntemlerinin geliştirilmesi hedeflenmiştir. Bu sebeple bir sonraki başlıkta geçmişte boğma saldırılarına yönelik olarak geliştirilmiş olan çözüm yöntemlerinin özetleri verilmiştir. Literatür özetinde verilen çalışmalara Bölüm 5 ve Bölüm 6'da detaylı bir şekilde değinilmiştir.

1.1. Literatürde Yapılan Çalışmaların Özetleri

Kablosuz algılayıcı ağlarda MAC ve fiziksel katmandaki boğma saldırılarının tespitine ve çözümüne yönelik olarak geliştirilen ilk çalışma Wood ve diğerleri tarafından gerçekleştirilmiştir [9]. Bu çalışmada sürekli saldırganın etkisi altında olan düğümler saldırı tespitini kanal kullanım oranının düşmesi ile gerçekleştirmektedir. Saldırı tespiti yapıldıktan sonra düğümler çekişme kurallarına uymayarak saldırıya uğradıklarını gösteren mesajları yayınlamakta ve bu mesajlar, saldırganın etki alanın sınırlarında olan düğümler tarafından saldırıdan etkilenmeyen düğümlere ulaştırılmaktadır. Böylece saldırıların etki alanı tayin edilmekte ve üst katman

haberdar edilerek yönlendirme yollarının saldırıdan etkilenmeyen bölgelere yönelmesi sağlanmaktadır.

Xu ve diğerleri gerçekleştirdikleri çalışmada; boğma saldırılarının tespitine yönelik yöntem geliştirmişlerdir. Çalışmada sürekli, aldatıcı, reaktif ve rasgele saldırgan modelleri iki farklı yöntemle tespit edilmiştir [5]. Birinci yöntem Paket Teslim Oranı (Packet Delivery Ratio-PDR) ve Alınan Sinyal Gücünün Göstergesi (Received Signal Strength Indicator-RSSI) parametrelerinin tutarlılığına göre saldırı durumları ile tıkanıklık, hata vb. doğal ağ koşullarını birbirinden ayırmaktadır. İkinci yöntem de ise PDR ile düğümlerin konum bilgileri arasındaki tutarlılığa göre tespit işlemi gerçekleştirilmektedir.

Xu ve diğerleri gerçekleştirdikleri bir diğer çalışmada ise boğma saldırılarına karşı iki çözüm yöntemi öne sürmüşlerdir. Kanal sörfü olarak adlandırılan birinci yöntemde düğümlerin saldırının olmadığı bir kanala geçmesini ve saldırı etkisinden kurtulmasını öngörmektedir [10,11]. İkinci yöntem ise düğümlerin saldırı bölgesinden uzaklaşarak saldırı etkilerinden kurtulmasını ve ağ ile yeniden irtibata geçmesini önermektedir [10].

Cagalj ve diğerleri ise kablosuz algılayıcı ağlarda boğma saldırıları için solucan deliği esasına dayanan üç çözüm yöntemi önermiştir [12]. Yöntemlerden birincisinde; ağa belli sayıda birbirleri ile kablo yoluyla bağlı düğüm çiftlerinin rasgele olarak yerleştirilmesi, ikincisinde belirli sayıda frekans atlama kabiliyetine sahip olan düğüm çiftlerinin yerleştirilmesi ve üçüncüsünde ise kanal değiştirme kabiliyetine sahip düğümler yardımıyla bilgilerin saldırı bölgesinin dışarısına çıkarılması hedeflenmiştir.

Wood ve diğerleri kesme, aktivite, tarama ve darbe saldırgan türleri 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.

Yukarıda sayılan tüm çalışmaların detayları Bölüm 5 ve Bölüm 6'da açıklanmakta ve dezavantajları sunulmaktadır. Ancak çalışmalar hakkında özet olarak, sadece belirli türdeki saldırıların tespit edilmesi veya çözüm yönteminin geliştirilmesinin hedeflendiği söylenebilir. Literatürde var olan tüm saldırı modellerini tespit eden ve bu saldırılara karşı çözüm üreten bir yöntem tasarımı henüz bulunmamaktadır.

1.2. Tez Çalışmasının Amacı, İzlenen Çalışma Yöntemi ve Katkıları

Sınırların uzaktan gözetlenmesi, kimyasal/nükleer sızıntıların tespit edilmesi, kalp ve şeker gibi riskli hastalıkları bulunan kişilerin kontrol altında tutulması, bir evin ya da işyerinin güvenliğinin sağlanması gibi çok önemli ve hayati görevleri yerine getiren kablosuz algılayıcı ağlarının fonksiyonlarını icra etmesi ve görevlerini aksatmaması son derece önemlidir. Sınırlı donanımsal kaynaklara ve çoğunlukla değiştirilemeyen enerji birimlerine sahip olan kablosuz algılayıcı ağlar, çok çeşitli türdeki saldırılara karşı son derece savunmasızdır ve böyle bir ağı hayati önem arz eden uygulama alanlarında kullanmak son derece risklidir.

Bu tez çalışmalarının ana amacı, KAA'larını boğma saldırılarına karşı daha dirençli hale getirmek için ilk olarak saldırıların varlığını tespit eden daha sonra da bu saldırılara rağmen düğümlerin iletişimlerini gerçekleştirebilmesine olanak sağlayan bir savunma yöntemi tasarlamak, benzetim yoluyla tasarımını gerçeklemek ve başarımını incelemektir. Bu amaçlar doğrultusunda ilk olarak literatürde sunulan tüm saldırı modellerinin etkinlikleri analiz edilerek kablosuz algılayıcı ağlarına verdikleri zararlar benzetim yoluyla gösterilmiştir. Elde edilen bu sonuçlar doğrultusunda saldırı modellerinin tıkanıklık, donanımsal hatalar, kötü bağlantı durumları gibi doğal ağ koşullarından ayrılmasına olanak sağlayan anomali tabanlı yöntem kullanarak yeni bir saldırı tespit sisteminin tasarımı gerçekleştirilmiştir. Son olarak da boğma saldırılarının etkilerini en aza indirmek ve saldırılara rağmen düğümlerin iletişimlerini devam ettirebilmesini sağlamak üzere kanal çeşitliliğinden faydalanılmasını sağlayan Dinamik Kanal Atlama yönteminin tasarımı gerçekleştirilmiştir.

Bu tez çalışmasında önerilen yöntemler ve bu çalışmayı klasik eşleniklerinden ayıran katkılar özetle şunlardır:

1. Tezin tamamlanma sürecine kadar literatürde sunulan tüm boğma saldırı modellerinin etkinliklerini ölçmek, KAA başarımı üzerindeki etkilerini tespit etmek ve birbirleri ile kıyaslayabilmek için bir yöntem tasarlanmıştır.

2. Literatürde var olan tüm boğma saldırı modellerinin sisteme ek yük getirmeden ve yüksek başarımla tespit edilmesine olanak sağlayan saldırı tespit sisteminin tasarımı gerçekleştirilmiştir.

3. Çeşitli boğma saldırıları altında olmalarına rağmen düğümlerin iletişimlerini devam ettirebilmesine ve işlevselliğini sürdürebilmesine olanak sağlayan bir saldırı savunma yönteminin tasarımı gerçekleştirilmiştir.

4. KAA'larının katmanlı ağ yapısı, güç tüketimi, farklı konumlandırma teknikleri gibi birçok detayın modellendiği modüler, kullanıcı arabirim destekli ve OMNET++ tabanlı benzetim arayüz yazılımının tasarımı gerçekleştirilmiştir. KAA'lar için tasarlanan benzetim yazılımdaki bu hazır modeller kullanılarak birçok uygulamanın benzetimi kolaylıkla gerçekleştirebilmektedir.

5. Literatürde sunulan tüm boğma saldırı modelleri, tasarımı gerçekleştirilen saldırı tespit sistemi ve saldırı savunma yöntemi, geliştirilen benzetim programı yardımıyla modellenerek önerilen yöntemlerin çeşitli koşullardaki başarım sonuçları sunulmuştur.

6. Kablosuz algılayıcı ağlarının güvenliğini ve güvenirliğini tehdit eden farklı türdeki saldırıların tespit edilmesi ve savulması için izlenebilecek bir yordam sunulmuştur.

1.3. Tez Organizasyonu

Tez organizasyonu aşağıda özetlenen yedi bölümden oluşmaktadır:

Bölüm 1:Giriş: Bu bölümde tez çalışmasına konu olan problemin tanımı, çalışmanın amacı, literatürde bu problemin çözümü üzerine yapılan çalışmaların özeti, tez çalışmasını literatürde yapılan çalışmalardan ayıran temel özellikler ile tez organizasyonu hakkında bilgi sunulmaktadır.

Bölüm 2: Kablosuz Algılayıcı Ağlar: Bu bölümde tez konusunun temel çalışma alanını oluşturan kablosuz algılayıcı ağları hakkında detaylı bilgi verilmektedir. Algılayıcı düğümlerinin yapısı, kablosuz algılayıcı ağ mimarisi, kablosuz algılayıcı ağ tasarımını etkileyen faktörler ve kablosuz algılayıcı ağının uygulama alanları bu bölümde anlatılan konuları oluşturmaktadır.

Bölüm 3: Kablosuz Algılayıcı Ağ Güvenliği: 3. Bölümde kablosuz algılayıcı ağlarının güvenliğini kısıtlayan unsurlar, güvenlik gereksinimleri ve kablosuz algılayıcı ağlarının güvenliğini tehdit eden saldırılar hakkında bilgi verilmektedir.

Bölüm 4: Boğma Şeklindeki Hizmet Engelleme Saldırgan Modelleri ve Analizi: Bu bölümde literatürde var olan 12 adet saldırgan modeli hakkında detaylı bilgi verilmektedir. Buna ek olarak tüm saldırgan modellerinin etkinliklerinin ölçülmesi için yöntem sunulmakta ve benzetim yoluyla elde edilen sonuçlar verilmektedir.

Bölüm 5: Boğma Saldırılarının Tespitine Yönelik Yeni Bir Yöntem Tasarımı ve Başarım Analizi: 5. Bölümde saldırı tespit sistemleri hakkında genel bilgi verildikten sonra literatürde kablosuz algılayıcı ağlar için geliştirilmiş olan saldırı tespit sistemlerinin özellikleri açıklanmaktadır. Son olarak da boğma saldırılarının tespitine yönelik olarak geliştirilmiş anomali tabanlı yeni bir saldırı tespit sisteminin tasarımı açıklanmakta ve detaylı benzetimler yoluyla elde edilen başarım sonuçları sunulmaktadır.

Bölüm 6: Boğma Saldırılarına Karşı Dinamik Kanal Atlamalı Yeni Bir Güvenlik Yönteminin Tasarımı ve Başarım Analizi: Bu bölümde literatürde boğma saldırılarına karşı geliştirilmiş olan çözüm yöntemleri açıklanmakta ve eksiklikleri dile getirilmektedir. Daha sonra ise boğma saldırılarına karşı geliştirmiş olduğumuz dinamik kanal atlama yönteminin özellikleri ve tasarım basamaklarını sunulmakta, en son olarak da benzetim yoluyla elde edilen başarım sonuçları verilmektedir.

Bölüm 7: Sonuçlar ve Değerlendirmeler: Sonuçlar ve Değerlendirmeler bölümünde, yapılan çalışmalardan elde edilen sonuçlar genel hatlarıyla değerlendirilerek çalışmanın bilime sağlayabileceği katkılar tartışılmaktadır. Daha sonra yapılabilecek çalışmalar için önerilerde bulunulmaktadır.

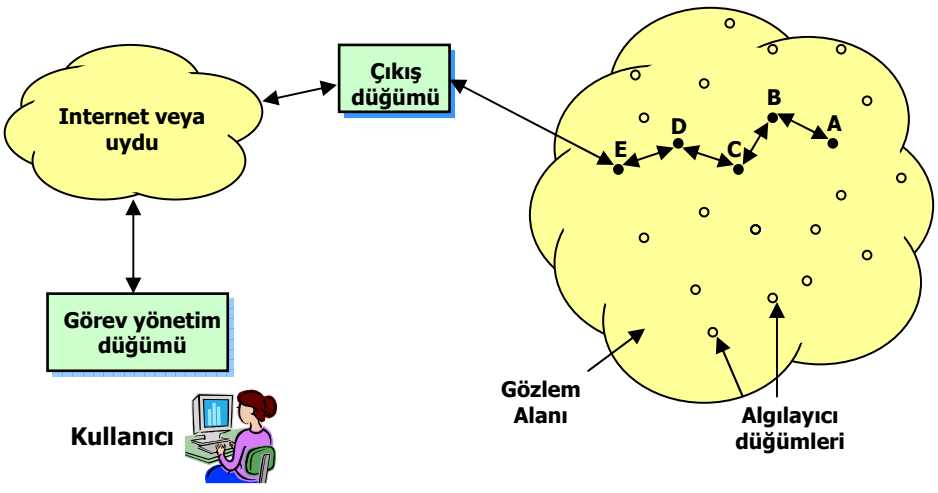
Ek-A: Modelleme ve Benzetim Ortamının Tanıtımı: Bu bölümde, modelleme/benzetim kavramları üzerinde durulmakta, günümüzde yaygın olarak kullanılan bilgisayar tabanlı benzetim yazılımlarının üstünlükleri ve zayıflıkları özetlenmekte ve son olarak da OMNET++ benzetim ortamının özellikleri, yapısı ve kullanım şekli kısaca açıklanmaktadır.

Ek-B: Kablosuz Algılayıcı Ağlara Yönelik OMNET++ Tabanlı Benzetim Modelinin Tasarımı: Bu bölümde, kablosuz algılayıcı ağlara yönelik olarak geliştirilen OMNET++ tabanlı benzetim modelinin tasarım detayları ve kullanım şekli açıklanmaktadır. Bu model, tez kapsamında geliştirilen yöntemlerin başarım analizlerinin gerçekleştirilmesi amacıyla kullanılmıştır.

BÖLÜM 2. KABLOSUZ ALGILAYICI AĞLAR

2.1. Giriş

Kablosuz algılayıcı ağlar (KAA), çok fazla sayıda küçük boyutlu, düşük maliyetli ve kısa mesafede kablosuz ortam üzerinden haberleşebilen algılayıcı düğümlerinden meydana gelmiş bir ağdır. Bu ağda, düğümler rasgele olarak ortama bırakabilmekte ve geliştirilen protokoller sayesinde kablosuz ortam üzerinden birbirileri ile haberleşerek kendi kendine organize olabilmektedir. Bu özellik, düğümlerin ortamdaki fiziksel büyüklük (ışık, sıcaklık, nem, basınç v.b.) değişimlerini çok atlamalı (multihop) yollar üzerinden merkezi ağ birimine iletmesini mümkün kılmaktadır. Kablosuz algılayıcı düğümlerinin düşük maliyetli olması, normal şartlarda erişimin imkânsız olduğu bölgelere kolaylıkla yerleştirilebilmesi ve uzun süreler boyunca bakım istemeden çalışabilmesi gibi özellikler kablosuz algılayıcı ağlarının çok çeşitli alanlarda kullanılabilmesini mümkün kılmaktadır. Şekil 2.1'de görüldüğü gibi tipik algılayıcı ağı gözlem alanından, algılayıcı düğümlerden, çıkış düğümünden ve görev yönetim düğümünden meydana gelmektedir [1].



Şekil 2.1. Kablosuz algılayıcı ağ örneği [1]

Gözlem Alanı: Belirli olayların olması beklenen ve algılayıcı düğümlerin yerleştirildiği alandır.

Algılayıcı düğümler: Ortamdaki verileri toplama ve çıkış düğümüne iletme görevini üstlenen düğümlerdir.

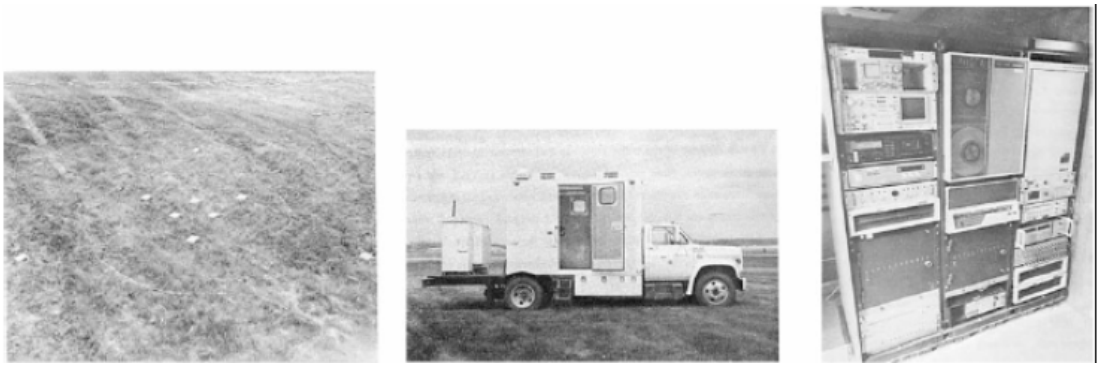
Çıkış düğümü: Çıkış düğümü, algılayıcı düğümlerden gelen paketlerin alınması işlenmesi ve saklanması ile görevli olan düğümdür. Gönderilecek toplam mesaj sayısının azalmasına yardım etmesi sebebiyle ağın toplam enerji tüketiminin azalmasına ve dolayısıyla ağ ömrünün uzamasına katkı sağlar. Çıkış düğümü, mevcut enerji miktarı, tampon bellek doluluk oranı v.b ölçütlere göre ağ tarafından dinamik olarak seçilebilir. İcra ettikleri görev gereğince veri toplama noktası olarak da adlandırılabilirler.

Görev yönetim düğümü ya da baz istasyon: Baz istasyon, ağdan gerekli olan bilgileri alan ve ağa kontrol bilgilerini göndermekle sorumlu olan merkezi kontrol noktasıdır. Ayrıca diğer ağlarla bağlantıyı sağlayan, güçlü veri işleme/saklama yeteneğine sahip ve kullanıcı ile arabirim sağlayan bir erişim noktasıdır. Baz istasyon olarak kullanılabilen dizüstü bilgisayar veya iş istasyonuna bilgiler radyo frekans, uydu veya İnternet ile iletilebilir.

2.2. Algılayıcı Düğümlerinin Tarihçesi

Algılayıcı düğümlerin tarihine bakıldığında ilk olarak Amerika Birleşik Devletleri (A.B.D) tarafından soğuk savaş yıllarında kullanıldığına şahit olmaktayız [14]. Okyanus tabanındaki kritik bölgelere yerleştirilen akustik algılayıcı içeren düğümler Sovyet denizaltılarını gözetlemek amacıyla kullanılmış ve geliştirilen algılayıcı ağı “Ses Gözetleme Sistemi” (Sound Surveillance System - SOSUS) olarak adlandırılmıştır. Kablolu algılayıcı düğümlerin kullanıldığı bu sistemde veriler farklı katmanlarda işlendikten sonra kablolu ortam üzerinden kıyılardaki merkezlere iletilmiştir. Modern algılayıcı ağ araştırmaları 1980’lerin başlarında yine A.B.D’de DARPA’da başlatılmıştır. Dağıtık algılayıcı ağ (Distributed Sensor Network - DSN)

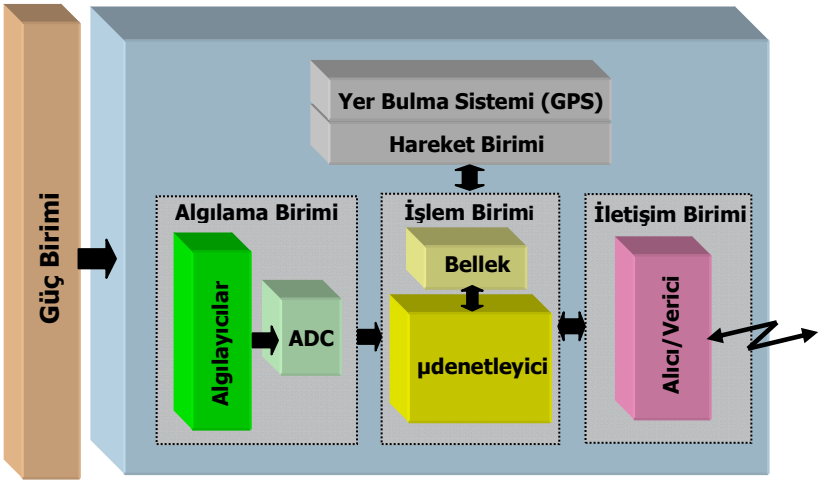
programı olarak adlandırılan projede düşük maliyetli, bağımsız birçok düğümün dağıtık olmasına rağmen birbirileri ile işbirliği içerisinde olmaları hedeflenmiştir [14]. 1980 ortalarında MIT (Massachusetts Institute of Technology) ses algılayıcılarından oluşan ve alçak uçuş gerçekleştiren uçakların takibini sağlayan örnek sistem geliştirmiştir. Altışarlı diziler halinde yerleştirilen mikrofonlar sayesinde uçakların ses sinyalleri ile algılanması hedeflenmiştir. Akustik algılayıcılardan gelen ses sinyallerinin işlenmesini sağlayan 512 KB hafızaya sahip bir bilgisayar ve üç adet işlemciden oluşan hareketli araç, algılama düğümünü meydana getirmektedir. Düğümler birbirleri ile mikrodalga sinyaller yardımıyla haberleşmektedirler. [14].



Şekil 2.2. MIT tarafından geliştirilen örnek algılayıcı ağ sistemi

2.3. Kablosuz Algılayıcı Düğüm Yapısı

Günümüzde kablosuz iletişim ve sayısal elektronikteki gelişmeler düşük güçlü, düşük maliyetli, çok fonksiyonlu ve kısa mesafede kablosuz ortam üzerinden haberleşebilen algılayıcı düğümlerinin gelişmesini sağlamıştır. Algılama, veri işleme, iletişim ve güç birimlerinden meydana gelen bu küçük algılayıcı düğümlerin ortak gayret sarf etmesi, algılayıcı ağlarının temel çalışma ilkelerini oluşturmaktadır. Şekil 2.2'de bir algılayıcı düğümün genelleştirilmiş mimarisi görülmektedir.



Şekil 2.3. Kablosuz algılayıcı ağ düğüm mimarisi [1].

Bir algılayıcı düğümünü meydana getiren birimler ve icra ettikleri görevler şunlardır:

- Algılama Birimi: Algılayıcılar ve ADC (Anolog/Digital Converter-Analog/Sayısal Çevirici)'lerden meydana gelen algılama birimi ışık, nem v.b. fiziksel büyüklüklerin ortamdan elde edilmesi ve bu büyüklüklerin işlem birimi tarafından işlenebilecek forma getirilmesinden sorumludur.

- İşlem Birimi: Mikrodenetleyici ve bellek birimlerinden oluşan işlem birimi, kod bellekte yüklü olan ve düğümlerin ağ içerisinde yapmakla yükümlü olduğu görev komutlarının işlenmesinden sorumludur. Kablosuz algılayıcı düğümlerinde algılama, veri işleme, gönderme/alma gibi sürekli kullanılan yordamların tanımlanmış olduğu ve daha kolay uygulama geliştirebilmeye imkân sağlayan gerçek zamanlı bir işletim sisteminden faydalanılır. TinyOS (Tiny Operating System) [13], kablosuz algılayıcı ağlarda en yaygın biçimde kullanılan işletim sistemlerinden birisidir ve kaynakları sınırlı olan algılayıcı düğümlerine uygun olarak küçük boyutludur.

- İletişim Birimi: Bir düğümü ağ içerisindeki diğer düğümlere bağlayan iletişim birimi, düşük güçlü RF alıcı/vericiden meydana gelmiştir. Algılayıcı düğümlerinde kullanılan alıcı/verici birimleri genellikle gönderme, alma, aylak ve uyku olmak üzere dört çalışma moduna sahiptir. Düğüm içerisinde alıcı/vericinin en fazla güç tüketen birim olduğu ve alıcı/vericide en fazla

gücün sırasıyla gönderme, alma, aylak ve uyuma modlarında harcandığı düşünüldüğünde, iletişim biriminin bir düğümün yaşam süresinin belirlenmesinde büyük önem taşıdığı anlaşılmaktadır. Bu sebeple, geliştirilen protokollerde alıcı/verici mümkün olduğu kadar uyuma modunda tutulmaya çalışılır.

- Güç Birimi: Güç birimi, dolaylı olarak tüm ağın ömrünü belirlemesi sebebiyle algılayıcı düğümlerinin en önemli birimidir. Boyut sınırlaması nedeniyle algılayıcı düğümlerde genellikle standart AA piller veya kristal hücreler başlıca kullanılan güç kaynaklarındandır. Bazı uygulamalarda güneş enerjisi ile şarj olabilen piller tercih edilebilmektedir. Böylelikle bir düğümün ömrü yaklaşık olarak 7–10 yıla kadar çıkabilmektedir.

- Hareket Birimi: Sadece gezgin olan düğümlerde bulunan hareket birimi düğümün hareket yönlerinin ve hızlarının yönetilmesinden sorumludur.

- Yer Bulma Sistemi: Her düğümde olma zorunluluğu olmayan yer bulma sistemi (Global Position System–GPS) düğümlerin küresel olarak konumlarını belirleyebilmesini sağlayan birimdir. Düğüm maliyetlerinin ve boyutlarının artmasına sebep olan GPS cihazlarının genellikle sınırlı sayıdaki düğümde bulunması tercih edilmekte ve diğer düğümler konumlarını bu düğümlere göre belirlemektedirler.

Günümüzde birçok üniversite ve şirket, akademik veya ticari amaçlı olarak algılayıcı düğüm üretmektedir. Tablo 2.1’de başlıca kablosuz algılayıcı düğümlerin özellikleri listelenmektedir.

Tablo 2.1.Başlıca kablosuz algılayıcı düğümleri ve özellikleri [98]

Algılayıcı Düğüm Türü ve Yılı	WeC 1998	Rene 1999	Rene2	Dot 2000	Mica 2001	Mica2Dot 2002	Mica2 2002	Telos 2004
Mikrodenetleyici								
Türü	AT90LS8535		ATMega163		ATmega128			TIMSP430
Program Belleği(KB)	8		16		128			60
Veri Belleği (KB)	0.5		1		4			2
Aktif Güç (mW)	15		15		8		33	3
Uyku Gücü (µW)	45		45		75		75	6
Uyanma Süresi (µS)	1000		36		180		180	6
Kalıcı Saklama Birimi								
Entegre	24LC256				AT45DB041B			STM24M0TS
Bağlantı Türü	I^2C				SPI			I^2C
Büyüklüğü	32				512			128
İletişim Birimi								
Alıcı/Verici	TR1000				TR1000	CC1000		CC2420
Veri Aktarım Hızı	10				40	38.4		250
Modülasyon Türü	OOK				ASK	FSK		O-QBPSK
Alım Gücü (mW)	9				12	29		38
Gönderim Gücü(mW)	36				36	42		35
Güç Tüketimi								
Min. Çalışma gerilimi	2.7		2.7		2.7			1.8
Toplam harcanan güç	24				27	44	89	41
Programlama ve algılayıcı arabirimi								
Genişleme	Yok	51-pin	51-pin	Yok	51-pin	19-pin	51-pin	10-pin
İletişim	IEEE 1284 (Programlama) ve RS 232							USB
Tümleşik Algılayıcılar	Yok	Yok	Var	Yok	Yok	Yok	Yok	Var

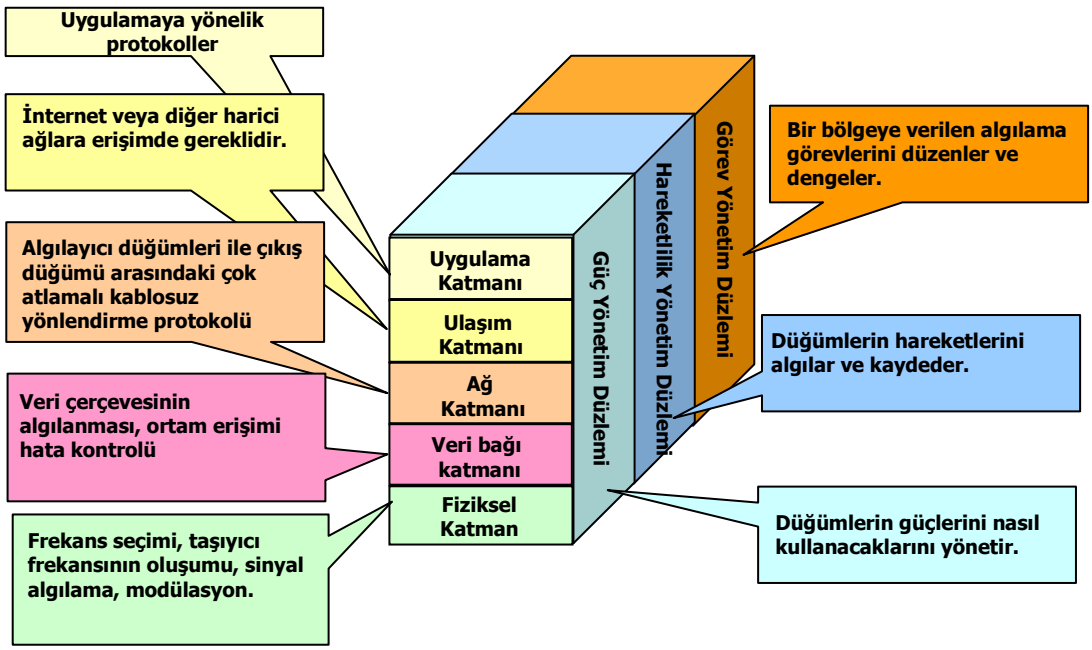
2.4. Kablosuz Algılayıcı Ağ Mimarisi

Kablosuz algılayıcı ağ mimarisi için beş katmanlı ve üç düzlemli protokol yığını tanımlanmıştır [1]. Protokol yığını Şekil 2.4'de görüldüğü üzere uygulama katmanı, ulaşım katmanı, ağ katmanı, veri bağı katmanı ve fiziksel katman olmak üzere beş katman ile birlikte güç yönetim düzlemi, hareketlik düzlemi ve görev yönetim düzleminden meydana gelmektedir. Düğümlerin ortak gayret sarf ederek kaynakların etkin bir şekilde kullanılmasını destekleyen yönetim düzlemleri, özellikle kaynak sıkıntısı olan kablosuz algılayıcı ağlar için büyük önem taşımaktadır.

- Güç yönetim düzlemi: Algılayıcı düğümlerinin güçlerini nasıl kullanacaklarını yöneten düzlemdir. Örneğin gücü azalan bir düğüm, komşularına gücünün yeterli olmadığını duyurabilir ve böylelikle mesajların yönlendirilmesine katılmayıp kalan gücünü algılama işlemlerine ayırabilir.

- Hareketlilik yönetim düzlemi: Algılayıcı düğümlerinin hareketlerinin algılanmasından ve kaydedilmesinden sorumlu düzlemdir. Düğümler hareketlilik düzlemi sayesinde komşularının takibini ve bölgesel algılama görevlerini gerçekleştirebilirler.

- Görev yönetim düzlemi: Düğümlere atanacak görevlerin planlanmasından ve yürütülmesinden sorumlu olan düzlemdir. Örneğin bir bölgedeki düğümlerin hepsinin aynı anda algılama işlemini gerçekleştirmesine gerek duyulmayabilir ve bazı düğümler güçlerine göre diğerlerinden daha fazla görev yürütebilirler. Bu durumda düğümler arasında görevlerin taksimini görev yönetim düzlemi gerçekleştirir.



Şekil 2.4. Kablosuz algılayıcı ağ mimarisi [1]

2.4.1. Fiziksel katman

Frekans seçimi, taşıyıcı frekansının oluşumu, sinyal algılama, modülasyon, gönderim ve alım işlemlerinin yürütüldüğü katmandır. Fiziksel katman, güç tüketimini doğrudan etkilediği için kablosuz algılayıcı düğüm tasarımında ayrı bir öneme sahiptir. Seçilen modülasyon tekniği, iletim hızı, gönderme gücü ve görev çevrim süresi gibi güç tüketimini etkileyen faktörler fiziksel katman tasarımı ile ilgili

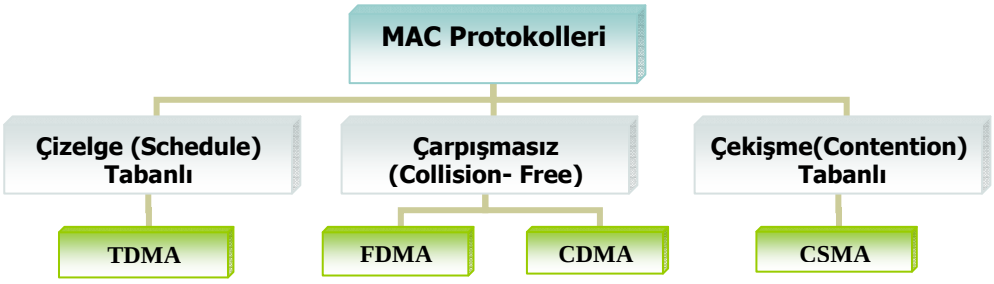
parametrelerdir. Fiziksel katman tasarımında önemli olan unsurlardan bir tanesi de haberleşme yöntemidir. Günümüz algılayıcı düğümleri genellikle kısa mesafeli kablosuz iletişim ile haberleşmektedir. Gönderim mesafesi, gönderim gücüne bağlı olduğu için algılayıcı düğümlerde genellikle kısa mesafeli iletişim tercih edilir. Düğümler ISM (Industrial, Scientific, Medical –Endüstriyel, Bilimsel, Tıbbi) bandı olarak bilinen lisansız frekanslarda haberleşmektedir. Avrupa ve Japonya'da 433 MHz/868 MHz frekansları genellikle tercih edilirken Amerika Birleşik Devletlerinde 915 MHz ve 2.4 GHz frekansları kullanılır [1].

Fiziksel katman tasarımında önemli olan unsurlardan bir diğeri de modülasyon tekniğidir. Kablosuz algılayıcı ağları çoğu durumda zor doğa koşulları altında çalışmak zorunda oldukları için seçilen modülasyon tekniğinin gürültüye, girişime ve boğma (jamming) saldırılarına karşı dayanıklı olması gerekmektedir. Frekans atlamalı yayılım spektrumu (Frequency-Hopping Spread Spectrum-FHSS) ve doğrudan sıralı yayılım spektrumu (Direct-Squence Spread Spectrum-DSSS) kablosuz ağlarda ve kablosuz algılayıcı ağlarda kullanılan modülasyon tekniklerindendir. Her iki teknikte girişime dayanıklı olmasına karşın DSSS tekniği dar bant girişimlerine FHSS'ye oranla daha dayanıklıdır. Ayrıca ultra geniş bant, darbe radyo ve darbe konum modülasyon teknolojilerinin kullanımı KAA'larda enerji tüketiminin azalmasına ve daha güvenilir iletişimin gerçekleşmesine olanak sağlayacaktır [1].

2.4.2. Veri bağı katmanı

Veri çerçevesinin algılanması, erişim ortamı ve hata kontrolünden sorumlu olan katmandır. Bir iletişim ağında noktadan noktaya ve bir noktadan çok noktaya iletişimin güvenilir ve adil bir şekilde yapılmasını sağlar. Veri bağı katmanı temelde mantıksal bağlantı kontrolü (Logical Link Control-LLC) ve ortam erişim kontrolü (Medium Access Control-MAC) olmak üzere iki kısımdan meydana gelmektedir. MAC, adil ve güvenli haberleşmenin yürütülebilmesi ve enerji tüketiminin düşürülmesi ile ilgili olarak önemli roller üstlenmektedir. Bu sebeple kablosuz algılayıcı ağlarda veri bağı katmanındaki çalışmalar genellikle ortam erişim kontrol mekanizması üzerine odaklanmaktadır. Literatürde kablosuz algılayıcı ağları için

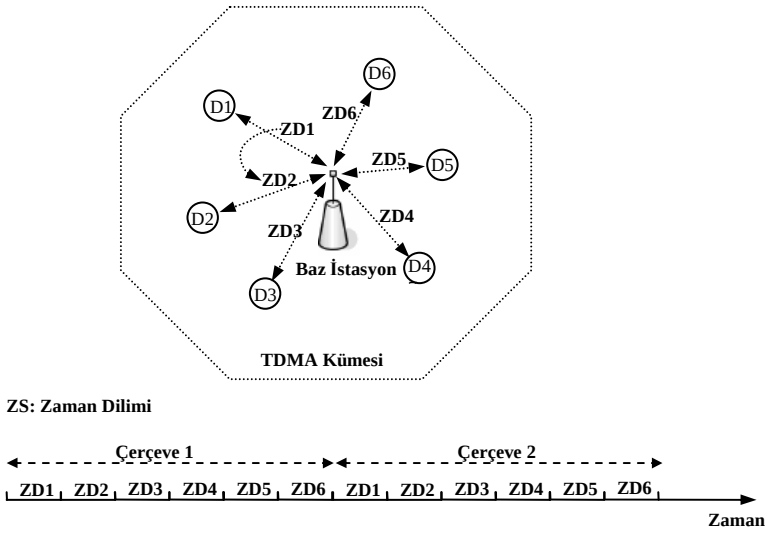
geliştirilmiş olan birçok çalışma bulunmaktadır. Geliştirilen MAC protokolleri şekil 2.5'de görüldüğü gibi üç ana kategoride toplanmaktadır [15].



Şekil 2.5. Ortam erişim protokol ailesi

2.4.2.1. Çizelge tabanlı ortam erişim protokolleri

Zaman çizelgesi esasına dayanan ortam erişim protokolleri çarpışmayı engellemek için hangi düğümün ne zaman iletişime başlayabileceğine karar veren merkezi çizelge algoritması kullanmaktadır. Zaman bölümlemeli çoğullama (Time Division Multiple Access-TDMA) ise paylaşımlı olan iletişimin kanalının N tane dilime (slot) ayrıldığı ve her zaman diliminde sadece bir düğümün gönderim yapabildiği çizelge tabanlı algoritmadır. TDMA, düğümlerin iletişim zamanlarının yönetilmesini sağlayan merkezi bir baz istasyona gereksinim duymaktadır. Şekil 2.6'da görüldüğü gibi baz istasyonun kapsama alanındaki düğümler ve baz istasyon, hücre yapısını oluşturmaktadır.



Şekil 2.6. TDMA yönteminin yapısı [15]

TDMA protokolleri düşük enerji ile çarpışmasız iletişim sunmasına rağmen bazı zayıflıklara sahiptir;

- Hareketli düğümler TDMA yapısı için önemli bir sorundur. Hareketli düğümlerin diğer düğümler ile iletişim kurabilmesi için baz istasyonla irtibat halinde olmaları gerekmektedir.
- TDMA düğümler ile baz istasyonlar arasında katı bir zaman senkronizasyonuna ihtiyaç duyulmaktadır.
- Özellikle düğüm yoğunluğu fazla olan ağlarda gönderim sırasının beklenmesi sebebiyle gecikmeler önemli ölçüde artmaktadır.

Literatürde kablosuz algılayıcı ağlar için TDMA esasına dayanan birçok MAC protokolü önerilmiştir. LEACH [16], PACT [17], TRAMA [18] ve LMAC [19] bu protokollerden başlıcalarıdır.

2.4.2.2. Çarpışmasız ortam erişim protokolleri

Çarpışmasız ortam erişim protokolleri çarpışmayı farklı radyo kanalları (frekans ya da kod) kullanarak engeller. Böylelikle iki düğüm arasındaki eş zamanlı iletişim girişimsiz ve çarpışmasız olarak gerçekleştirilir. Kablosuz iletişimde iki farklı çarpışmasız ortam erişim yöntemi kullanılmaktadır.

- FDMA (Frequency Division Multiple Access – Frekans Bölümlemeli Çoğullama): FDMA yönteminde frekans spektrumu, ayrı frekanslardaki bantlara ayrılmıştır. İletişim yapacak olan her bir düğüm çifti bu bantlardan birisini seçerek iletişimi gerçekleştirir. Farklı radyo kanalları sayesinde çarpışmasız bir biçimde eş zamanlı iletişim gerçekleştirilebilir.

- CDMA (Code Division Multiple Access- Kod Bölümlemeli Çoğullama): TDMA yönteminde var olan bütün spektrum zamanın belli bir bölümü için sadece bir düğüme tahsis edilirken FDMA yönteminde var olan spektrumun belli bir kısmı sürekli olarak bir düğüme tahsis edilir. Kod bölümlemeli

çoğullama tekniğinde var olan bütün spektrum her zaman bir düğüme tahsis edilebilir. CDMA tekniği tek bir taşıyıcı frekansı ve bir dizi dikey kodların kombinasyonları ile iletişimin geçekleştirilmesi esasına dayanmaktadır [20]. Bu teknikte gönderici düğüm, gönderim yapmadan önce göndereceği paketi belirli dikey kodlarla ÖZELVEYA işlemine tabi tutar. Alıcı düğüm ise gelen paketi aynı kodlarla tekrar ÖZELVEYA işlemine tabi tutarak orijinal bilgiyi elde eder.

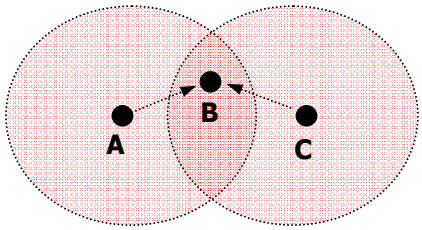
FDMA ve CDMA protokolleri aynı kablosuz ağın farklı kümeleri arasındaki iletişimde kullanılabilir. Her bir kümeye farklı frekans veya kod atanması sayesinde girişimsiz ve çarpışmasız bir biçimde kümeler arasında iletişim gerçekleştirilebilir. Ancak FDMA tekniği farklı radyo kanalları ile dinamik olarak haberleşebilmek için fazladan devrelere ihtiyaç duymaktadır. Daha fazla ve karmaşık devre beraberinde daha yüksek maliyeti getirmektedir. CDMA tekniğinin yüksek işlem yükü gerektirmesi ise düğümlerin enerji tüketimlerinin önemli oranda artması sebep olmaktadır [21]. Bu gibi sebepler CDMA ve FDMA tekniklerinin kablosuz algılayıcı ağlarda kullanılmasına engel teşkil etmektedir. Literatürde FDMA tekniğine göre SMACS [22] protokolü sunulmuştur. CDMA tekniği ile ilgili olarak önerilen çalışmalardan bazıları ise PicoRadio [23] ve DS-CDMA [24] protokolleridir.

2.4.2.3. Çekişme tabanlı ortam erişim protokolleri

Çekişme tabanlı protokoller, çarpışmayı tamamen engellemek yerine olma olasılığını azaltmaya çalışırlar. Tek kanallı radyo iletişiminde kanal tüm düğümler tarafından paylaşılmaktadır ve kanal tahsisi isteğe göre yapılmaktadır. Böyle bir durumda aynı anda birden fazla düğüm gönderim isteğinde bulunursa çarpışma kaçınılmazdır. Çarpışmayı engellemek ya da olasılığını azaltmak için iletim hakkını eline geçirmek isteyen düğümler arasında kanal tahsisini gerçekleştirecek dağıtık algoritmalar kullanılmaktadır. Çoğu dağıtık MAC protokolü çekişme esasına dayanır ve taşıyıcı duyarlı iletişim ve/veya çarpışmadan kaçınma mekanizmalarını kullanır. Bu yüzden gönderimden önce dinleme esasına dayanan taşıyıcı duyarlı çoklu iletişim (Carrier Sense Multiple Access - CSMA) olarak bilinirler. Kanalı dinlemenin amacı,

gönderime başlamadan önce meşgul olmadığından emin olmaktır. Eğer kanal meşgul değilse düğüm hemen iletime başlar. Eğer kanal meşgul ise rasgele bir zaman boyunca bekler ve bu süre bittikten sonra kanalı yeniden dinler (non-persistent CSMA türlerinde) ya da kanal boş olana kadar dinlemeye devam eder ve kanalın boş olduğunu tespit ettiğinde iletime başlar. [15]

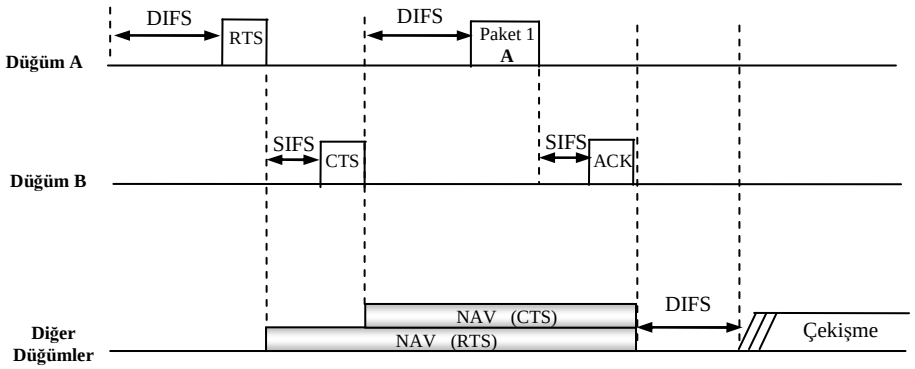
Çok atlamalı kablosuz ağlarda CSMA-tabanlı protokoller Şekil 2.7'de görüldüğü gibi gizli düğüm probleminin ortaya çıkmasına yol açmaktadırlar. Gizli düğüm problemi, birbirinin kapsama alanında olmayıp aynı komşu düğüme sahip düğümlerin birbirinin iletişimini engellemesi esasına dayanır. A düğümü, B düğümüne bir paket göndermeye başladığında; C düğümü, A'nın kapsama alanında olmaması sebebiyle iletişimi hissedemez ve kanalın boş olduğunu varsayarak B düğümüne paket gönderimini başlatabilir. Böyle bir durumda, B düğümü çarpışma nedeniyle paketi alamaz.



Şekil 2.7. CSMA protokollerinde ortaya çıkan gizli düğüm problemi

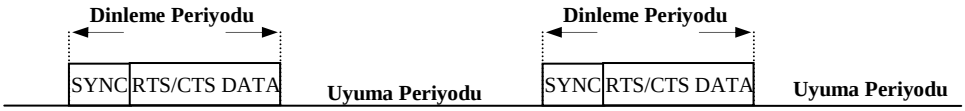
Literatürde fazladan kontrol sinyalleri kullanarak gizli düğüm problemi giderilmeye çalışılmıştır. El sıkışması yönteminde, veri paketi gönderiminden önce gönderici düğüm ile alıcı düğüm arasında kontrol paket değişimi olmakta ve böylece alıcı düğümün kapsama alanında olan komşu düğümler iletişimden haberdar olmaktadır. El sıkışması yöntemini kullanan en bilinen protokol IEEE 802.11 tarafından da desteklenen CSMA/CA (Collision Avoidance-Çarpışmadan Kaçınma) protokolüdür. Bu protokolde veri paketi göndermek isteyen düğüm ilk olarak küçük boyutlu RTS (Request to Send – Gönderim İsteği) paketi gönderir. Alım işlemini kabul eden düğüm ise CTS (Clear to Send) paketi ile cevap vererek gönderici ile alıcı arasındaki veri paketi akışının başlamasını sağlar. RTS/CTS paketini duyan komşu düğümler ise backoff (geri çekilme) durumuna geçerek iletimlerini ertelerler. Gizli düğüm

problemi, RTS paketlerinin çarpışma olasılığı dışında CSMA/CA tekniği ile büyük ölçüde çözüme kavuşmuştur. CSMA/CA yöntemi esas alınarak geliştirilen bir çalışmada (MACA) [25] RTS ve CTS paketlerine iletimin ne kadar süreceğini gösteren süre bilgisi eklenmiştir. Bu sayede RTS/CTS paketlerini duyan komşu düğümler, iletim erteleme sürelerini doğru bir şekilde tahmin edebilmekte ve RTS paket çarpışmalarının önüne geçilmektedir. Bir diğer çalışmada ise (MACAW) [26], gönderimin başarılı olup olmadığını gösteren ACK (Acknowledgement-Kabul) paketinin kullanılması önerilmiştir. IEEE 802.11 protokolü, CSMA/CA, MACA ve MACAW protokollerinin birleşimini, dağıtık eş güdüm fonksiyonu (Distributed Coordinator Function-DCF) içerisinde bulundurmaktadır. Şekil 2.8'de IEEE 802.11 ortam erişim fonksiyonunun çalışma mantığı görülmektedir. 802.11 protokolünde gönderim yapmak isteyen düğüm, ortam erişim hakkını elde etmek için diğer düğümlerle çekişmek zorundadır. Bu sebeple düğümler gönderimden önce ortamı dinler ve eğer ortam meşgul ise iletimi daha sonraki bir zamana ertelerler (rasgele bir süre boyunca bekler). İletişim ortamını DIFS (Distributed Coordination Function Interframe Space)'tan daha uzun bir süre boyunca boş bulan bir düğüm gönderim yapmak istediğini belirten bir RTS paketi gönderir. İlk RTS paketini gönderen düğüm, ortam erişim hakkını kazanmış olur. Gönderici ile alıcı arasında RTS-CTS-DATA-ACK şeklindeki paket değişimi ile iletişim sonlanır. İki düğüm iletişim halindeyken diğer düğümlerin ne kadar beklemesi gerektiği RTS/CTS sinyallerinde bulunan ve iletişimin ne kadar süreceğini gösteren süre kısmında belirtilmektedir. Düğümler kontrol paketlerinden elde edilen süre bilgilerini, NAV (Network Allocation Vector) olarak adlandırılan değişkenlerine kaydeder ve zaman ilerledikçe NAV değişkenini güncellerler ve NAV sıfıra eşit olana kadar ortam erişimi için herhangi bir girişimde bulunmazlar.



Şekil 2.8. IEEE 802.11 ortam erişim fonksiyonu

Literatürde kablosuz algılayıcı ağlar için CSMA tabanlı birçok MAC protokolü önerilmiştir. Kablosuz algılayıcı ağları için tasarlanmış olan ortam erişim protokolleri arasında en yaygın olarak bilinen S-MAC [27], 802.11 protokolünden esinlenerek geliştirilmiş protokollerden birisidir. S-MAC protokolünü 802.11'den ayıran en önemli fark, enerji tüketiminin azaltılmaya çalışılmasıdır. Güç tüketimini azaltmak için ise radyo alıcılarını sürekli çalıştırmak yerine periyodik olarak açılıp kapatılması öngörülmüştür. Şekil 2.9'da görüldüğü gibi düğümler periyodik olarak dinleme/uyuma zamanlamasını kullanmakta ve iletişimlerini dinleme süresi içerisinde gerçekleştirmektedirler. Böylece zamanın büyük bir bölümünde uyuma moduna geçerek enerji tüketimlerini önemli ölçüde azaltmaktadırlar.



Şekil 2.9. S-MAC protokolünün görev çevrimi

Literatürde S-MAC dışında T-MAC [28], D-MAC [29], WiseMAC [30], B-MAC [31] gibi CSMA tabanlı birçok MAC protokolü mevcuttur.

2.4.3. Yönlendirme katmanı

Paketlerin çok atlamalı yollar üzerinden çıkış düğümüne iletilmesi için gerekli olan protokolünün gerçeklendiği katmandır. Yönlendirme protokolü paketin hedefe ulaşabilmesi için gerekli olan en etkin yolu bulma görevini üstlenir. Kablosuz

algılayıcı ağlar için sunulan yönlendirme protokolleri Şekil 2.10'da görüldüğü gibi ağ yapısına göre, yolların belirlenme şekline göre ve ağ işlemlerine göre üç kategoriye ayrılmaktadır.

Şekil 2.10. Kablosuz algılayıcı ağları için sunulan yönlendirme protokollerinin sınıflandırılması [32]

Ağ yapısına göre yapılan sınıflandırma da sunulan protokoller düz ağ (Flat Networks) yönlendirme protokolleri, hiyerarşivsel ağ yönlendirme protokolleri ve konum tabanlı yönlendirme protokolleridir. Düz ağ yönlendirme protokollerinde tüm düğümler eşit görev üstlenmekte, hiyerarşivsel protokollerde hiyerarşisine göre farklı görevlere sahip olmakta ve konum bilgisine dayalı protokollerde ise yollar düğüm konumları baz alınarak belirlenmektedir.

Diğer sınıflandırma yöntemi, yönlendirme yollarının belirlenme şekline göredir. Proaktif protokoller, ağ içersindeki bütün yolları başlangıçta belirlerler ve bütün yollar düğümlerdeki yönlendirme tablolarında saklanır. Eğer yollarda her hangi bir değişiklik olursa değişiklik bilgisi tüm ağa yayılır. Bununla beraber reaktif protokoller, yolları başlangıçta değil sadece gerekli olduğunda belirlerler. Hibrit protokoller ise bu iki yaklaşımı beraber kullanmaktadır. Sabit olan ağlar için proaktif protokollerin kullanılması enerji tüketimi açısından daha verimli olabilir. Çünkü yolların belirlenmesi önemli ölçüde enerji tüketimini arttırmaktadır. Bir diğer sınıflandırma yöntemi ise ağda gerçekleştirilen işlem türlerine göredir. Adaptif

yönlendirme protokolleri bazı sistem parametrelerini ağ koşullarına göre uyarlayabilirler. Böyle protokoller çokluyol (multipath) tabanlı, sorgulama (query) tabanlı, müzakere (negotiation) tabanlı, hizmet kalitesi (QoS) tabanlı ve evreuyum (coherent) tabanlı olmak üzere beş kategoriye ayrılabilirler. Kablosuz algılayıcı ağlar için sunulmuş olan yönlendirme protokol özelliklerinin özeti tablo 2.2'de görülmektedir.

Tablo 2.2. Kablosuz algılayıcı ağ yönlendirme protokollerinin sınıflandırılması [32]

Protokol	**Sınıf**	**Gezginlik**	**H.Kalitesi**	**Çokluyol**	**Sorgulama**	**Müzakere**
SPIN [33]	Düz	Mümkün	Yok	Var	Var	Var
Directed Diffusion[34]	Düz	Sınırlı	Yok	Var	Var	Var
Rumor Routing[35]	Düz	Çok sınırlı	Yok	Yok	Var	Yok
GBR[36]	Düz	Sınırlı	Yok	Yok	Var	Yok
MCFA[37]	Düz	Yok	Yok	Yok	Yok	Yok
CADR [38]	Düz	Yok	Yok	Yok	Yok	Yok
COUGAR[39]	Düz	Yok	Yok	Yok	Var	Yok
ACQUIRE [40]	Düz	Sınırlı	Yok	Yok	Var	Yok
EAR[41]	Düz	Sınırlı	Yok	Yok	Var	Yok
LEACH[42]	Hiyerarşik	Sabit B.İstasyon	Yok	Yok	Yok	Yok
TEEN,APTEEN[43,44]	Hiyerarşik	Sabit B.İstasyon	Yok	Yok	Yok	Yok
PEGASIS[45]	Hiyerarşik	Sabit B.İstasyon	Yok	Yok	Yok	Yok
MECN &SMECN[46]	Hiyerarşik	Yok	Yok	Yok	Yok	Yok
SOP[47]	Hiyerarşik	Yok	Yok	Yok	Yok	Yok
HPAR[48]	Hiyerarşik	Yok	Yok	Yok	Yok	Yok
VGA[49]	Hiyerarşik	Yok	Yok	Var	Yok	Var
Sensor Aggregate[50]	Hiyerarşik	Sınırlı	Yok	Yok	Mümkün	Yok
TTDD[51]	Hiyerarşik	Var	Yok	Mümkün	Mümkün	Yok
GAF[52]	Konum	Sınırlı	Yok	Yok	Yok	Yok
GEAR[53]	Konum	Sınırlı	Yok	Yok	Yok	Yok
SPAN[54]	Konum	Sınırlı	Yok	Yok	Yok	Var
MFR, GEDIR[55]	Konum	Yok	Yok	Yok	Yok	Yok
GOAFR[56]	Konum	Yok	Yok	Yok	Yok	Yok
SAR[57]	H.Kalitesi	Yok	Var	Yok	Var	Var
SPEED[58]	H.Kalitesi	Yok	Yok	Yok	Var	Yok

2.4.4. Ulaşım katmanı

Özellikle düğümlerin doğrudan internet veya diğer harici ağlarla irtibat halinde olması istediğinde veri akışının sağlanmasında gerekli olan katmandır. Genellikle uygulamalarda kablosuz algılayıcı ağ düğümlerinin harici bir ağa doğrudan

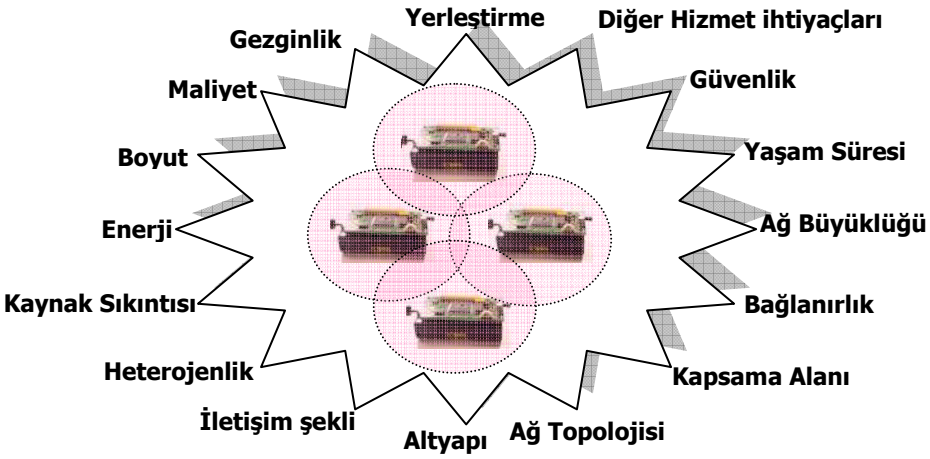
bağlanması gerekmez. Bu sebeple literatürde ulaşım katmanı ile ilgili çok fazla çalışma bulunmamaktadır.

2.4.5. Uygulama katmanı

Algılayıcı ağdan beklenen görevlerin türüne bağlı olarak farklı uygulama yazılımlarının geliştirildiği katmandır.

2.5. Kablosuz Algılayıcı Ağ Tasarımını Etkileyen Faktörler

Kablosuz algılayıcı ağları, gözlem yapılacak ortama kolay ve hızlı bir şekilde yerleştirilebilmeleri, kendi kendine organize olarak uzun yıllar kontrol edilmeksizin çalışabilmeleri gibi özelliklere sahip olması sayesinde çok çeşitli alanlarda kullanılabilmektedir. Ancak, bu gibi kolaylıklar beraberinde kablosuz algılayıcı ağlarında görevlerin yürütülmesini sağlayan protokol ve algoritmaların tasarımını zorlaştırmaktadır. Şekil 2.11'de kablosuz algılayıcı ağ tasarımı gerçekleştirirken dikkat edilmesi gereken hususlar görülmektedir [1,59].



Şekil 2.11. Kablosuz algılayıcı ağ tasarımını etkileyen faktörler

- Yerleştirme (Deployment): Kablosuz algılayıcı ağlarında düğümler rasgele dağıtılabilir veya isteğe bağlı olarak seçilmiş yerlere yerleştirilebilir. Yerleştirme işlemi kurulum aşamasında yapılabileceği gibi ağın kapsama

alanını genişletmek veya bozulan düğümler ile yenilerini değiştirmek için herhangi bir zamanda da yapılabilir. Bu sebeple KAA'lar için tasarlanan algoritmaların yerleştirme gereksinimlerini karşılayacak özellikte olmaları gerekmektedir.

- Gezginlik (Mobility): Düğümlerin konumları yerleştirme sonrası kasıtlı olarak veya kaza ile değişebilir. Örneğin rüzgâr, su v.b doğal etkenler düğümlerin yerleşim noktalarının değişmesine sebep olabilir. Bunun dışında bazı düğümler hareket kabiliyetine sahip olabilir ve bu sayede hareketli olarak gözlem görevlerini yürütebilirler. Sürekli olabileceği gibi zamana ve duruma göre gerçekleşebilen gezginlik, kablosuz algılayıcı ağ protokolleri için önemli bir tasarım ölçütüdür. Özellikle ortam erişim ve yönlendirme protokollerinin tasarım özelliği gezginliğe bağlı olarak değişebilir.

- Maliyet, Boyut, Sınırlı Kaynaklar ve Enerji: Kablosuz algılayıcı ağlarında düğüm sayıları uygulamaya göre binlere, on binlere ve hatta milyona ulaşabilir. Bu sebeple düğüm maliyeti çok önemlidir. Düğüm boyutları ise bir *tanecik* büyüklüğünde olabileceği gibi bir cep telefonu büyüklüğünde de olabilir. Düğümler, tıbbi uygulamalarda olduğu gibi bir insan vücudunun çeşitli bölgelerine yerleştirilebilir ve bu sebeple düğüm boyutlarının küçük olması beklenir. Düşük maliyet ve küçük boyutlar ise beraberinde kaynak sıkıntısını getirmektedir. Bir düğüm sınırlı işlem yapma kabiliyetine, saklama birimlerine ve enerji kapasitesine sahiptir. Bu sebeple KAA'lar için geliştirilen algoritma ve protokollerin çok karmaşık olmaması ve enerji tüketimini en aza indirmesi gerekmektedir. Enerjisi biten düğüm, çoğu uygulama senaryosu için bir daha kullanılamaz demektir. Bu sebeple geliştirilen algoritmalar birinci öncelik olarak enerji tüketimine odaklanmalıdır.

- Heterojenlik: Geçmişteki algılayıcı ağ uygulamalarında ağ içerisindeki düğümlerin tek tip olduğu (homojen) varsayılırdı. Ancak günümüzde kablosuz algılayıcı ağlarında her düğüm aynı özellikte olamamaktadır. Örneğin maliyetlerin ve boyutların artmasına sebep olan GPS gibi

konumlandırma cihazlarının her düğümde olması gerekmeyebilir. Geliştirilen yöntemlerle GPS cihazlarına sahip olmayan düğümler konumlarını GPS'e sahip olan düğümlerin konumlarına göre belirleyebilirler. Bu sebeple bir algılayıcı ağında heterojenliğin derecesi geliştirilecek olan algoritma ya da protokollerin karmaşıklığının artması ile yakından ilgilidir.

- İletişim Şekli: Kablosuz algılayıcı ağlarda radyo frekans ile iletişim dışında lazer, endüktif veya kapasitif bağlaşım (coupling), ses gibi farklı tekniklerle haberleşme gerçekleştirilebilmektedir. Maliyet ve kullanım kolaylığı gibi sebeplerle çoğu uygulamada radyo iletişimi tercih edilmektedir. İletişim şekli fiziksel katman ve ortam erişim katmanlarının fonksiyonları ile yakından ilgilidir.

- Altyapı (Infrastructure): Kablosuz ağlarda iletişim ağı altyapı-tabanlı ağlar ve tasarsız (ad-hoc) ağlar olmak üzere iki farklı yöntemle kurulabilir. Tasarsız ağlarda düğümler birbirleri ile herhangi bir altyapıya gerek duymadan haberleşebilirler. Bu sebeple çoğu uygulamada tasarsız ağ yapısı kullanılır. Fakat bunun yanında tasarsız ağlarda düğümler hem veri kaynağı hem de potansiyel bir yönlendirici olduğundan tasarsız ağlar için geliştirilen yönlendirme protokollerinin tasarımı altyapı tabanlı ağlara nazaran daha karmaşıktır.

- Ağ Topolojisi: Ağ topolojisi, kablosuz algılayıcı ağlarının önemli tasarım ölçütlerinden birisidir. Tek atlamalı ağlarda düğümler, diğer düğümler ile doğrudan haberleşebilirken çok atlamalı ağlarda haberleşme keyfi olarak belirlenen atlamalar üzerinden gerçekleşir. Topoloji, gecikme, sağlamlık ve kapasite gibi önemli ağ karakteristiklerini etkiler ve paketlerin yönlendirilme şeklini belirler.

- Kapsama Alanı: Bir düğümdeki algılayıcıların etkin alanı o düğümün kapsama alını belirler. Ağın kapsama alanı ise ağ içerisindeki düğümlerin gözlem yapılması gereken alanının ne kadarını kapsadığıdır. Kapsama alanın derecesi bilgi işlem algoritmalarını yakından ilgilendirmektedir. Düşük

kapsama oranı ile güvenilir bir gözlem yapılması mümkün değildir. Örneğin bir ev güvenlik sisteminde eve yerleştirilen düğümlerin evin her tarafını ya da önemli bölgelerini kapsamadığı düşünülürse şüpheli kişiler eve girse bile tehlike ağ tarafından sezilmeyecektir.

- Bağlanırlık (Connectivity): Düğümlerin fiziksel konumları ve iletişim mesafeleri bir ağın bağlanırlığını göstermektedir. Eğer düğümler arasında daima bir iletişim bağlantısı varsa bu ağ bağlı olduğu söylenebilir. Eğer düğümler genellikle ayrıksa ve bazen diğer düğümlerin iletişim alınana giriyorsa böyle iletişim de düzensiz (sporadic) iletişim olarak adlandırılır. Bağlanırlık veri toplama metotlarının ve iletişim protokollerinin tasarımını etkilemektedir.

- Ağ Büyüklüğü: Ağdaki düğüm sayısı ağın bağlanırlığı, kapsama alanı ve gözlem alanının büyüklüğüne göre belirlenir. Ağ birkaç adet düğümden meydana gelebileceği gibi binlerce adet düğümden de meydana gelebilir. Dolayısıyla kablosuz algılayıcı ağları için tasarlanacak olan protokollerin ölçeklenebilir olması yani birkaç düğüm için olduğu gibi birkaç bin düğüm için de uygun şekilde çalışabilmesi gerekmektedir.

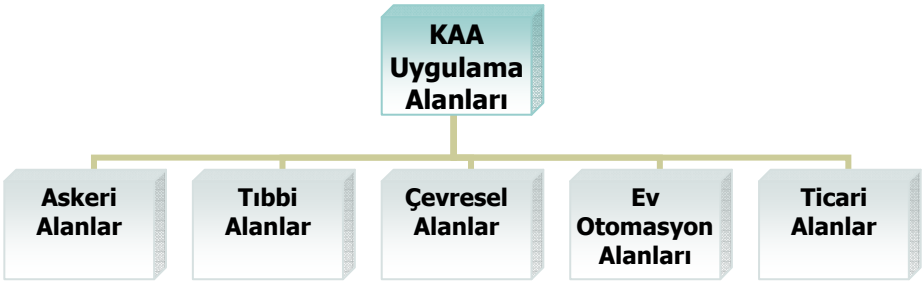
- Yaşam süresi: Uygulamaya bağlı olarak bir algılayıcı ağının yaşam süresinin birkaç saatten birkaç yıla kadar sürmesi beklenebilir. Yaşam süresi doğrudan enerji tüketimine ve düğümün güvenirliliğine bağlıdır. Enerji tüketimi de fiziksel düğüm tasarımından kullanılacak protokol tasarımına kadar algılayıcı ağ tasarımının her alanını etkileyen önemli bir faktördür.

- Güvenlik: Algılayıcı düğümleri güvenli olmayan dış ortamlarda çalışmak zorunda olabilir, bazı doğal koşullar sebebiyle hasara uğrayabilir veya kötü niyetli kişiler tarafından ele geçirilerek saldırgan düğüm olarak yeniden programlanabilir. Dolayısıyla kablosuz algılayıcı ağlar için tasarlanacak olan algoritma ya da protokollerin algılayıcı ağların doğasında olan bu güvenlik açıklarını kapatacak şekilde olması gerekmektedir.

- Diğer Hizmet Kalite Gereksinimleri: Kablosuz algılayıcı ağları bir olayın belirli zaman dilimi içerisinde rapor edilmesi, bazı düğümlerde hata olsa bile ağdan beklenen görevlerin aksamaması gibi hizmet kalite gereksinimlerini karşılaması gerekmektedir.

2.6. Kablosuz Algılayıcı Ağ Uygulama Alanları

Mikro elektronik ve mekaniksel sistem (MEMS) tasarımındaki gelişmeler sıcaklık, nem, basınç, titreşim, ses, görüntü ve kimyasal sızıntı gibi fiziksel büyüklüklerin sezilmesini sağlayan algılayıcıların kablosuz haberleşebilen düğümlere entegre edilebilmesini mümkün kılmaktadır. Bu sebeple günümüzde kablosuz algılayıcı ağlar birçok alanda gözlem ve denetim amacıyla kullanılmaktadır. Algılayıcı ağların kullanım alanları Şekil 2.12'de görüldüğü gibi beş ana kategori altında incelenebilir [1]. Ancak algılayıcı ağların uygulama alanları bunlarla sınırlı değildir.



Şekil 2.12. Kablosuz algılayıcı ağ uygulama alanları

2.6.1. Askeri alanlar

Birçok teknolojik başarı askeri gereksinimler sayesinde elde edilmektedir. Yine bir askeri gereksinim sebebiyle ortaya çıkmış olan algılayıcı ağlar günümüzde çok çeşitli askeri uygulamalarda karşımıza çıkmaktadır. Örneğin nükleer, biyolojik ve kimyasal saldırı tespiti, radyasyona maruz kalmaksızın kablosuz algılayıcı ağları ile gerçekleştirilebilir [60]. Kritik araziler, yollar, patikalar, geçitler, boğazlar kolay ve hızlı bir şeklide algılayıcı ağları ile kaplanabilir ve düşman kuvvetleri gözlemlenebilir [61].

2.6.2. Tıbbi alanlar

Kablosuz Algılayıcı ağları, özürlüler için arabirim oluşturma, hastalara teşhis koyma ve gözlem altında tutma, insanların psikolojik davranışlarının izlenmesi, hastane içerisindeki hasta ve doktorların izlenmesi ve gözlemlenmesi vb. birçok sağlık ile ilgili uygulama alanlarında kullanılmaktadır. Fransa'nın Grenoble tıp fakültesinde kurulan algılayıcı ağları yaşlıların düşme vb. davranışlarının gözlemlenmesine olanak sağlamaktadır [1]. Gerçekleştirilen bir başka uygulamada [62] ise hastane içinde ve dışında hastalarla ilgili detaylı bilgilerin toparlanması ve bu sayede kolay ve hızlı bir şekilde hasta tedavilerinin gerçekleştirilmesi hedeflenmektedir. Bu amaçla hastalara kalp atışını ve kalpteki oksijen yoğunluğunu ölçen küçük ve hafif algılayıcı düğümleri takılmaktadır.

2.6.3. Çevresel alanlar

Kablosuz algılayıcı ağları bitki ve hayvanların ortamlarında gözlemlenmesi [63,64], soyu tükenen hayvan türlerinin izlenmesi, okyanuslarda yeni canlıların keşfedilmesi gibi birçok ekolojik uygulamada kullanılmaktadır. Bunun dışında felaketlerin önceden tespiti algılayıcı ağ uygulamalarının en önemlilerindendir. Orman yangınlarının ve selin önceden tespit edilmesi [65], volkanik hareketliliğin sismik ve ses altı (infrasonic) algılayıcılar ile belirlenmesi [66], Tsunami'lerin [67] ve depremlerin sismik /hidroakustik algılayıcılar yardımıyla önceden tespiti [68] gibi birçok alanda kablosuz algılayıcı ağları kullanılabilmektedir. Kablosuz algılayıcı ağlarının bir diğer ilginç uygulama alanı ise uzay keşifleridir. NASA gezegen keşiflerinde kablosuz algılayıcı ağlarından faydalanmayı hedeflemektedir [69].

2.6.4. Ev otomasyon alanları

Kablosuz algılayıcı ağlar, merkezi ısıtma ya da soğutma sistemlerin verimi arttırmak amacıyla kullanılabilir. Merkezi ısıtma sistemlerinde bir oda diğerinden daha sıcak ya da daha soğuk olabilir veya gelen havakışı her tarafa eşit dağılmayabilir. Kablosuz algılayıcı düğümleri sıcaklık ve hava akışını kontrol etmek için odaların farklı bölgelerine yerleştirilebilir. Bu sayede tahminen %44 enerji tasarrufu sağlanabilir

[70]. Bir diğer uygulama alanı ise bina güvenliğinin sağlanmasıdır. Kritik bölgelere yerleştirilen düğümler izinsiz kişilerin binaya girmesini engellemenin yanında meydana gelebilecek gaz kaçağı, yangın v.b herhangi bir felakettin önceden tespit edilmesi amacıyla kullanılabilir.

2.6.5. Ticari alanlar

Stokların yönetilmesi, ürün kalitesinin ölçülmesi, zeki ofis alanlarının oluşturulması, kablosuz algılayıcı ağlarının ticari uygulama alanları arasındadır. British Petrol, petrol saklama ortamlarında meydana gelebilecek tehlikeli durumların tespiti ve petrol tankerlerinin motorlarındaki titreşim kontrolü için [71], Boeing firması ise uçak kanatlarındaki basıncın gözlemlenmesi [72] amacıyla algılayıcı ağları kullanmaktadır. Kablosuz algılayıcı ağlarının bir diğer ilginç uygulama örneği ise kuzey kutbundaki petrol borularının sıcaklığının kontrol edilmesidir. Isıtılmayan borular donma sebebiyle patlayacağından sürekli olarak sıcaklarının gözaltında tutulması gerekmektedir [71].

2.7. Sonuçlar

Bu bölümde son yıllarda bilgisayar ağları alanında oldukça popüler bir konu haline gelen kablosuz algılayıcı ağlarının temel özellikleri açıklanmakta, kablosuz algılayıcı ağ uygulamaları hakkında bilgi verilmekte ve kablosuz algılayıcı ağ tasarımını etkileyen faktörlerden bahsedilmektedir. Algılayıcı ağ tasarımını etkileyen bu faktörlerden *Güvenlik* konusu araştırmaya açık olan konuların başında gelmektedir. Bu sebeple tez çalışmasında KAA'ların *Güvenlik* sorunları üzerine odaklanılmakta ve bir sonraki bölümde KAA'ın güvenliği hakkında detaylı bilgi verilmektedir.

BÖLÜM 3. KABLOSUZ ALGILAYICI AĞ GÜVENLİĞİ

3.1. Giriş

Kablosuz algılayıcı ağlar (KAA), bir olayın veya bir bölgenin düşük maliyetli olarak uzaktan izlenmesine imkân tanıması sebebiyle son yıllarda askeri ve tıbbi uygulamalar, doğal felaketlerin tespiti, bina güvenlik sistemleri v.b. birçok alanda kullanılmaktadır [1]. Bu uygulamaların çoğunda algılayıcı ağının, çeşitli türdeki saldırılara karşı güvenilir bir şekilde çalışabilmesi son derece hayati önem arz etmektedir. Ancak, algılayıcı ağlarda düşük maliyetin sağlanabilmesi için donanımsal kaynakları sınırlı olan düğümlerin tercih edilmesi, geleneksel güvenlik tekniklerinin KAA'larda kullanılmasını zorlaştırmaktadır. Bununla birlikte, algılayıcı düğümlerinin çoğu uygulama için dış ortamda bulunması ve paylaşımlı olan kablosuz ortam üzerinden haberleşmesi saldırganların işini kolaylaştırmakta ve kablosuz algılayıcı ağlarının güvenlik açısından diğer ağlara nazaran daha fazla risk taşımasına sebep olmaktadır. Bu bölümde KAA güvenliğini irdelemek üzere ilk olarak ağ güvenliğini zorlaştıran unsurlardan bahsedilecek daha sonra KAA'lar için güvenlik gereksinimleri hakkında bilgi verilecek ve son olarak da KAA güvenliğini tehdit eden saldırı türleri özetlenecektir.

3.2. KAA Güvenliğini Zorlaştıran Unsurlar

KAA'lar, geleneksel ağlara oranla daha fazla sınırlamaya sahip özel bir ağ hüviyetindedir. Sınırlı donanımsal kaynaklar, güvenli olmayan iletişim kanalı, düğümlerin uzun süreler boyunca gözetimsiz çalışması gibi sebepler, geleneksel güvenlik tekniklerinin doğrudan KAA'larda kullanılmasını zorlaştırmaktadır. Güvenli bir ağ tasarımı gerçekleştirebilmek için bu sınırlamaları dikkate almak gerekmektedir.

3.2.1. Sınırlı kaynaklar

Bütün güvenlik teknikleri beraberinde sisteme ek yük getirmekte ve bu tekniklerin gerektirdiği işlevlerin gerçeklenebilmesi için veri/program belleklerinde belirli oranda bir alana ihtiyaç duyulmaktadır. Günümüzdeki kablosuz algılayıcı düğümleri, Bölüm 2'de açıklandığı gibi oldukça sınırlı kaynaklara sahiptir. Düğümler genellikle 4–8 Mhz hızında ve 8–16 bit uzunluğundaki işlemciye, ortalama 10 KB'lık veri belleğine, 64 KB'lık program belleğine ve 1 KB civarında da Flash belleğe sahiptir. Geliştirilen güvenlik tekniklerinin bu sınırlı kaynakları verimli bir şekilde kullanabilmesi gerekmektedir. Buna ek olarak, düğümlerin dış ortama rasgele yerleştirilmesi ve çoğu uygulama için pillerinin değiştirilememesi güç tüketimini KAA'larda en önemli tasarım ölçütü yapmaktadır. Seçilen güvenlik tekniğinin gerektirdiği işlemler (şifreleme, şifre çözme, şifre dağıtımı v.b.) güç tüketiminin artmasına ve böylece KAA'nın ömrünün önemli oranda kısalmasına sebep olmaktadır. Bu sebeple, geliştirilen güvenlik tekniğinin mümkün olan en az güç tüketimine hedeflemesi ve yeterince güvenli olması beklenir ki bu ikisi arasında çoğu durum için ters orantı bulunmaktadır.

3.2.2. Güvensiz iletişim kanalı

Kablosuz algılayıcı düğümleri, tek kanal frekansında paylaşımlı olan kablosuz ortam üzerinden haberleşirler. Radyo iletim mesafelerinin kısa olması ve düğümlerin zor çevresel koşullar altında çalışması, kanal hatalarının artmasına ve paketlerin kaybolmasına sebep olabilmektedir. İletim kanalından kaynaklanan hataların artması hata düzeltme yöntemlerinin kullanılmasını gerektirmektedir ancak bu yöntemler de sisteme önemli ölçüde yük getirmektedir. Bir başka husus da seçilen hata düzeltme mekanizmasının yetersiz kaldığı durumlarda önemli güvenlik paketlerinin (şifreleme/şifre çözme anahtarları) kaybolma ihtimalidir. Bu sebeple kablosuz algılayıcı ağlarda iletim kanalı, güvenliği zorlaştıran önemli bir unsur olabilmektedir.

3.2.3. Gözetimsiz çalışma

Uygulamanın türüne bağlı olarak, KAA'lar bir merkezi yönetim birimi olmaksızın ve uzun süreler boyunca gözetimsiz şekilde çalışabilirler. Kablosuz algılayıcı ağlarının genellikle uzaktan yönetilmesi, acil fiziksel müdahalelerin gerektiği gibi zamanında yapılmasını engelleyebilmektedir. Bu gibi sebepler, düğümlerin fiziksel saldırılara maruz kalma olasılığını diğer ağlara oranla daha da arttırmaktadır. Örneğin dış ortamda bulunan düğümlerin şifreleme/şifre çözme anahtarları ele geçirilebilir ve yeniden programlanarak ağın işleyişine zarar verebilen bir saldırgan düğüm haline çevrilebilir. Gerçekleştirilen çalışmada [2] günümüzde yaygın olarak kullanılan MICA düğümlerin birkaç dakika içerisinde bütün bilgilerine erişilebildiği ve yeniden programlanabildiği gösterilmiştir.

3.3. Güvenlik Gereksinimleri

Kablosuz algılayıcı ağlar, geleneksel bilgisayar ağlarının ihtiyaç duyduğu güvenlik gereksinimlerine ek olarak sadece kendine has olan güvenlik gereksinimlerine de sahiptir. Bu özel gereksinimlerin birçoğu KAA'ların dış ortamda olmalarından kaynaklanmaktadır.

3.3.1. Veri gizliliği (Data confidentiality)

Veri gizliliği, ağ güvenliğinin en önemli gereksinimlerinden birisidir ve kablosuz algılayıcı ağlar gibi potansiyel olarak yüksek riskli bir iletişim ortamına sahip ağlarda çok daha fazla önem taşımaktadır. Askeri veya sağlık uygulamaları gibi güvenlik gereksiniminin üst düzey olduğu alanlarda kullanılan KAA'larda düğümlerin algıladığı veriler çok gizli olabilir ve bu verilerin kötü niyetli kişiler tarafından öğrenilmemesi son derece önemlidir. Bilginin sadece alıcının bildiği gizli bir anahtarla şifrelenmesi işlemi ağ güvenliğinde veri gizliliğini sağlamanın en yaygın yoludur.

3.3.2. Veri bütünlüğü (Data integrity)

Kötü niyetli kişilerin bilgileri izinsiz olarak elde etmesi veri gizliliğinin sağlanması ile engellenebilmektedir ancak saldırganlar bilgileri elde edemese de değiştirebilir ya da bilgilere ekleme yapabilir. Örneğin, kimyasal sızıntının izlenmesini sağlayan bir KAA'ında düğümler sızıntının var olduğunu sezdiklerinde bu bilgiyi operatöre komşu düğümler üzerinden bir an önce bildirmelidirler. Böyle bir durumda, operatöre bildirilecek olan bilginin bütünlüğünün korunması da çok önemlidir. Aksi takdirde, kötü niyetli bir düğüm ya da düğümler tarafından kablosuz ortam üzerinden kolaylıkla elde edilebilen bu hayati bilgiler değiştirilerek veya eklenti yapılarak operatöre iletilebilir ve kimyasal sızıntı var olduğu halde operatör tehlikenin farkında olamayabilir. Veri bütünlüğünün bozulmasına sebep olan bir diğer durum ise zor doğa koşullarıdır. Sonuç olarak veri bütünlüğü gönderilen bir bilginin alıcıya gelene kadar yolda değişip değişmediğini anlamamızı sağlayan önemli bir güvenlik gereksinimidir.

3.3.3. Kimlik doğrulama (Authentication)

Bilgileri çalamayan veya değiştiremeyen saldırganların kullanabileceği bir diğer taktik de kendilerini normal bir düğüm gibi göstermek ve sahte paketler göndererek normal düğümleri yanıltmaktır. Kimlik doğrulama ise alıcı düğümün kendisine gelen bir paketin gerçekten de yasal bir düğümden gelip gelmediğini anlamasını sağlayan bir yöntemdir. KAA'larında ağın yeniden programlanması, algılayıcı düğümlerin görevlerinin paylaşımı gibi birçok yönetimsel süreçlerde kimlik denetiminin yapılması gerekmektedir. Düğümler arasında kimlik denetimi mesaj kimlik denetim kodu (Message Authentication Code-MAC) ile sağlanmaktadır. Gönderici düğüm, alıcı düğüm ile paylaştığı gizli bir anahtarlar yardımıyla göndereceği paket için MAC kodunu oluşturmakta ve alıcı düğüm kendisine gelen paketteki MAC kodunu kontrol ederek paketin geçerli bir düğümden geldiğini veya gelmediğini anlamaktadır.

3.3.4. Veri güncelliği (Data freshness)

Veri gizliliği ve veri bütünlüğü sağlansa bile güvenli bir iletişim için her bir mesajın günceliğinin de sağlanması gerekmektedir. Veri güncelliği mesajın yeni olduğunun veya eski bir mesajın tekrarlanmadığının göstergesidir. Bu gereksinim özellikle paylaşımlı anahtar tekniklerinin kullanıldığı uygulamalarda büyük önem taşımaktadır. Bu tekniklerde paylaşımlı olan anahtarların belirli zaman aralıklarında değiştirilmesi ve anahtar değişimden ağdaki tüm düğümlerin haberdar edilmesi gerekmektedir. Anahtarların tüm ağa yayılması uzun zaman alabilmekte ve bu süre zarfında saldırgan düğümler tarafından tekrarlama (replay) saldırı tekniğini kullanılarak bazı düğümlerin anahtar değişiminden haberdar olması engellenebilmektedir. Bu saldırı neticesinde anahtar değişimden haberdar olamayan düğümlerin ağ ile irtibat kopmakta ve ağ güvenliği sekteye uğramaktadır. Bir ağın güvenliğinin sağlanması için gerekli olan veri güncelliğini korumanın yollarından birisi ise iletilen her bir paket içerisine mesajın geçerli olduğu süreyi gösteren bir bilginin eklenmesidir.

3.3.5. Kendi kendine organize olma (Self-organization)

Çoğunlukla ad-hoc (tasarsız) ağ stratejisine sahip olan KAA'lar, kablosuz yerel alan ağlarında olduğu gibi bir merkezi ağ yönetim altyapısına sahip değildir. Böyle bir ağda düğümlerin her birisi potansiyel yönlendirici özelliğine sahip olmalıdır. Ayrıca çoğu uygulama için ortama rasgele olarak dağıtılan düğümler birbirlerini tanıyarak ağa dâhil olmalı ve ağdaki görevlerin yürütülmesini sağlamalıdırlar. Güvenlik gereksinimlerinden olan anahtarların paylaşımı ve dağıtımı düğümlerin kendi kendine organize olabilmesi ile yakından ilgilidir. Düğümler arasında organize olmada bir problem oluşursa güvenliğin sağlanması için gerekli olan süreçlerin işletilmesinde de aksaklıklar olacaktır. Bu gibi sebeplerden dolayı kendi kendine organize olabilme KAA'ların güvenliğinin sağlanmasında önemli bir gereksinimdir.

3.3.6. Zaman eşlemesi (Time synchronization)

Çoğu KAA uygulamasında düğümler, daha az enerji harcamak için belirli zaman aralıklarında alıcı/vericilerini kapatırlar veya gruplar halinde ortaklaşa hareket ederek ağ görevlerini yürütürler. Böyle bir durumda, görevlerde aksamaların olmaması ve enerji tüketiminin artmaması için düğümlerin eş zamanlı olarak hareket etmesi gerekir. Bu özelliklerden faydalanarak saldırı stratejileri geliştirilebilir ve düğümler arasındaki uyum bozulabilir. Bu yüzden zaman eşlemesi, KAA'ların güvenliğini kısıtlayan önemli unsurlardan birisidir.

3.3.7. Güvenli konumlandırma (Secure localization)

Kablosuz algılayıcı ağlarda uygulamanın türüne bağlı olarak düğümlerin algıladığı bilgilere ek olarak düğüm konum bilgilerine ihtiyaç duyulmaktadır. Düğümler konumlarını Küresel Konumlandırma Sistemleri (Global Position System-GPS) yardımıyla tespit edebilmektedir. Ancak maliyet ve boyut gibi sebepler yüzünden ağdaki tüm düğümlerin GPS cihazlarına sahip olması mümkün olmayacağı için geliştirilen konumlandırma tekniklerinde, sadece belirli düğümlerde GPS cihazlarının bulunmasına ihtiyaç duyulur. Diğer düğümler ise konumlarını bu düğümlerden elde ettikleri sinyal gücüne göre tespit ederler. Fakat geliştirilen bu yöntemlerde, ağda bulunan kötü niyetli düğümler hatalı sinyal gücü ile veya sinyallerin tekrarı ile düğümlerin konumlarını yanlış tespit etmelerine sebep olabilirler.

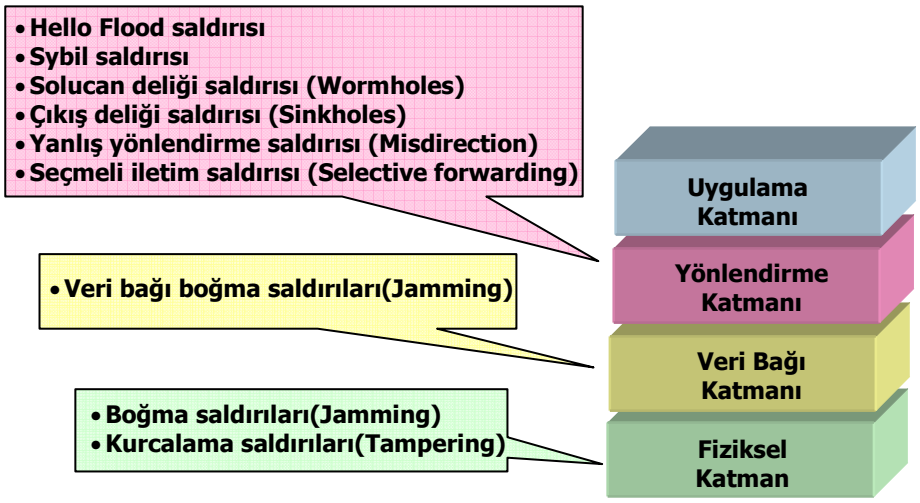
3.4. Kablosuz Algılayıcı Ağlarının Güvenliğini Tehdit Eden Saldırılar

Kablosuz algılayıcı ağlar, yapısı itibariyle farklı türdeki birçok saldırı türüne açıktır. Bu başlıkta kablosuz algılayıcı ağlarını tehdit eden en önemli saldırı türleri hakkında bilgi verilmektedir.

3.4.1. Hizmet engelleme saldırıları

Hizmet engelleme (Denial of Service-DoS) saldırıları, bir ağdan beklenen görevleri aksatmak ya da tamamen engellemek üzere gerçekleştirilen kötü niyetli herhangi bir girişimdir. DoS saldırıları donanımsal arazılar, yazılımsal hatalar ve kaynakların tükenmesi gibi istenmeyen durumların ortaya çıkmasına sebep olabilir ve bu durumlar sebebiyle ağ kendisinden beklenen görevleri gerçekleştiremeyebilir [3].

DoS saldırıları ilk olarak geleneksel bilgisayar ağları özellikle de internet tabanlı bilgisayarları tehdit eden bir saldırı olarak karşımıza çıkmış olmasına karşın kısıtlı kaynaklara sahip olan kablosuz algılayıcı ağları için de önemli bir tehdit unsuru olmuştur. Araştırmacılar literatürde kablosuz algılayıcı ağ mimarisini oluşturan fiziksel, veri bağı, yönlendirme ve uygulama katmanlarının farklı özellikteki DoS saldırılarına karşı savunmasız olduğunu göstermişlerdir [3,4,73,74]. Şekil 3.1' de farklı katmanlar için önerilen DoS saldırgan türleri görülmektedir.



Şekil 3.1. Kablosuz algılayıcı ağ katmanlarını etkileyen DoS saldırı türleri

3.4.1.1. Kurcalama saldırıları (Tampering)

Büyük ölçekli KAA'larda düğümlere fiziksel teması engellemek çoğu durumda imkânsızdır. Çevreye yerleştirilmiş olan algılayıcı düğümler yoldan geçen yolcular veya araçlar tarafından hasara uğratılabilir ya da tamamen yok edilebilir [74].

Düğümlerde meydana gelen bu gibi zararlar sebebiyle, KAA iletişiminde aksamalar meydana gelebilir. Bundan daha kötü bir senaryoda ise, kötü niyetli kişiler tarafından düğümler kurcalanarak hafızalarındaki veri veya şifreleme anahtarları ele geçirilebilir, kod hafızada bulunan program, kötü niyetli programla değiştirilerek düğümler saldırgan hale çevirebilir. Bu saldırgan, bütün şifrelere ve yasal kimlik denetimlerine (ID) sahip olduğu için ağ içerisinde her türlü yetkiye sahiptir. Bu şekilde fiziksel temas sonucunda yeniden programlanarak saldırgan hale gelen düğümler, dâhili saldırgan olarak adlandırılmaktadır. Programlama yöntemine göre sınıflandırmada kullanılan ikinci tanım ise harici saldırgandır. Harici saldırgan, ağda bulunan bir düğümün değiştirilerek saldırgan hale getirilmesi yerine kötü niyetli olarak programlanan yeni düğümlerin ağa bırakılması ile elde edilir.

Fiziksel saldırılara karşı geliştirilebilecek savunma yöntemleri; kurcalamaya karşı dayanıklı donanım, fiziksel kurcalamayı tespit edecek yazılım ve donanım, fiziksel kurcalamayı tespit eden düğümlerin kendi kendini yok etmesi ve kamuflaj olmak üzere dört başlık altında toplanabilir. Ancak bütün bu koruma yöntemlerinin en büyük dezavantajı, düğüm maliyetlerinin ve tasarım karmaşıklığının artmasına sebep olmasıdır. Özellikle binlerce ya da on binlerce düğüm içeren büyük ölçekli ağlarda düğüm başına yükselen maliyet önemli bir sorun olarak karşımıza çıkmaktadır [3,73,74].

3.4.1.2. Boğma saldırıları (Jamming)

Kasıtlı olarak radyo sinyali göndererek düğümlerin iletişimlerine girişim yapmak anlamına gelen boğma (jamming), kablosuz algılayıcı ağlar gibi tek kanal frekansında çalışan ağlar için basit ve etkili bir saldırı türüdür. Boğma saldırıları iki farklı katmanın fonksiyonlarını etkilemektedir. Fiziksel katmanı etkileyen boğma saldırılarında saldırgan düğümler, kanal frekansına eş frekanslı radyo sinyalleri yayarak iletişim kanalını meşgul ederler. Veri bağı katmanı etkileyen boğma saldırılarında ise saldırganlar ortam erişim protokol kurallarına uymayarak normal düğümlerin iletim zamanlarında paket gönderirler ve paket çarpışmalarına yol açarlar. Boğma saldırılarında amaç düğümlerin iletişimlerinin kesilmesini sağlamak ve güç tüketimini arttırarak yaşam sürelerini kısaltmaktır. Boğma saldırısına maruz

kalan bir düğümün komşuları ile ve dolayısıyla ağın tamamı ile iletişimi kopabilir. Böyle bir durumda, ağın kendisinden beklenen fonksiyonları yerine getirmesi mümkün değildir.

Geleneksel kablosuz ağlarda boğma saldırılarına karşı kullanılan savunma yöntemlerinden en bilineni yayılım spektrum (spread spectrum) iletişim metotlarıdır. Frekans atlamalı yayılım spektrumunda (Frequency-Hopping Spread Spectrum-FHSS) gönderilen sinyallerin frekansları belirli süreler boyunca değiştirilir. Böyle bir iletişimde alıcı ve verici senkronize olmalıdır. FHSS iletişim tekniği girişime ve atlama sıralamasını bilmeyen saldırganlara karşı dayanıklı olmasına rağmen frekanslar arasında sürekli değişim ve senkronizasyon gereksinimi sebebiyle güç tüketimini arttırmaktadır. Bir diğer iletişim şekli olan doğrudan sıralı yayılım spektrumunda (Direct-Sequence Spread Spectrum-DSSS) ise geniş bir bant aralığında olan sinyaller, sözde rasgele bit akışı ile yayılırlar. DSSS tekniğini gerçeklemek için FHSS tekniğine oranla daha fazla elektronik devreye ihtiyaç duyulmaktadır. Bu sebeple maliyeti daha yüksektir ve daha fazla enerji tüketimine sebep olmaktadır. Maliyetlerin ve güç tüketimlerinin artması sebebiyle günümüz ticari düğümlerinde genellikle boğma saldırılarına karşı dayanaksız, tek frekanslı iletişim tekniği tercih edilmektedir. KAA'ları için önemli bir tehdit unsuru olan boğma saldırılarına karşı düşük maliyetli çözüm yöntemlerinin geliştirilmesi, algılayıcı ağlarının güvenliğinin sağlanması açısından önemli bir eksikliktir.

3.4.1.3. Seçmeli iletim saldırıları (Selective forwarding)

Çok atlamalı ağlarda bir mesaj birçok atlama üzerinden geçerek hedefine ulaşmaktadır. En basit seçmeli iletim saldırılarında, saldırgan düğüm kendisine gelen paketleri iletmez ve paket kaybına yol açar. Bu saldırı yaklaşımında, komşu düğümlerin anormal bir durum olduğunu sezerek bir başka düğüme yönelme ihtimali vardır. Biraz daha etkin saldırı yaklaşımında ise saldırgan kendisine gelen paketlerin tümünü iletmemek yerine rasgele seçtiği bazı paketleri iletmez. Böylelikle şüphe çekmeden uçtan uca gecikmenin artmasına ve iletim maliyetlerinin yükselmesine sebep olur.

Seçmeli iletim saldırılarına karşı çoklu ayrık yönlendirme yolları kullanılabilir [75]. Birbirinden tamamen ayrı yönlendirme yollarının kullanılması tekniğinde, mesajların kaynaktan hedefe ulaşana kadar bir saldırgana rastlama olasılığının azalması prensibine dayanmaktadır. Ancak ağ içerisinde birbirinden tamamen ayrık yollarının sağlanması enerji-kısıtlı KAA'lar için oldukça zorlayıcıdır. Literatürdeki bir diğer çalışmada, seçmeli iletim saldırıları için alındı (ACK) tabanlı saldırı tespit yöntemi geliştirilmiştir [76]. Bu çalışmada, iletim yolu üzerinde bulunan her düğüm saldırganın varlığını tespit etmekle yükümlüdür. Eğer düğüm bir anormallik olduğunu tespit ederse, iletimin yönüne göre kaynak düğüme ya da baz istasyona bir alarm paketi göndermelidir.

3.4.1.4. Yanlış yönlendirme saldırıları (Misdirection)

Yanlış yönlendirme saldırganları kendilerine gelen mesajları, seçmeli saldırganlarda olduğu gibi doğrudan düşürmek yerine yanlış yönlere iletirler. Saldırganlar, sadece belirli bir düğümün gönderdiği paketleri saptırabileceği gibi belirli alıcılara gitmesi gereken paketleri de saptırarak hizmetlerin aksamasını sağlayabilirler.

Bu saldırılara karşı kullanılan savunma yöntemlerinde kimlik denetimi, mesajın bütünlüğü ve güncelliğinin sağlanması gerekmektedir. Kimlik denetimi ile yönlendirme güncellemelerinin saldırganlar tarafından değiştirilmesi, güncellik mekanizması ile yönlendirme bilgilerinin tekrarlanması, kriptografik bütünlük ile de yönlendirme mesajlarının saldırganlar tarafından değiştirilmesi engellenebilir. Ayrıca, KAA'larda yönlendirme amacıyla hiyerarşik yapının (küme başı v.b.) kullanılması ile yanlış yönlendirme saldırılarına karşı dayanıklı iletişim gerçekleştirilebilir [74].

3.4.1.5. Çıkış deliği saldırısı (Sinkholes)

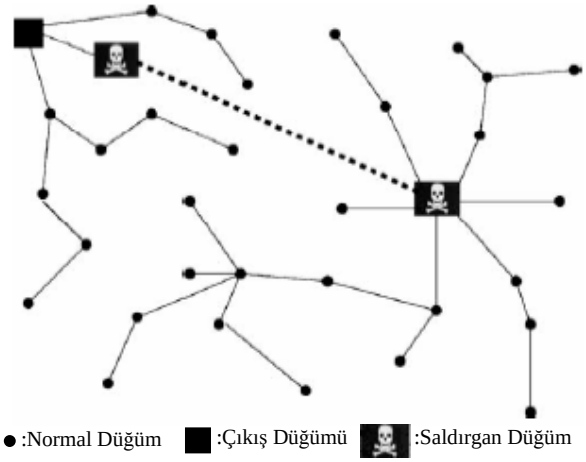
Çıkış deliği saldırılarında saldırganların amacı, bütün trafik akışını belli bir bölgeden saldırganların olduğu bölgeye çekmektir [4]. Böylelikle veri trafiği, çıkış düğümü yerine kendisini çıkış düğümü gibi gösteren saldırganlara akmaktadır. Bu saldırganlar ağdaki trafiği çekmek için baz istasyon yönünde yüksek kaliteli yola

sahip olduklarını bildiren mesajlar yayarlar. Normal düğümleri bu şekilde aldatarak trafiği çekerler. Saldırganlar ağdaki trafiği kendilerine doğru çektikleri için bu saldırı stratejisi ile birlikte birçok saldırı türü de kolaylıkla gerçeklenebilir. Örneğin, saldırgan kendilerine çektikleri paketlerden rasgele seçtiklerini iletip diğerlerini düşürebilir veya seçtikleri paketleri değiştirebilirler. Bu sayede çıkış deliği saldırıları ile seçmeli iletim saldırıları beraber kullanılabilir.

Yönlendirme topolojisini, kalan enerji miktarı ve uçtan uca gecikme gibi bilgilerin ilanına dayanarak belirleyen protokollerde çıkış deliği saldırılarının üstesinden gelmek oldukça zordur. Çünkü bu gibi bilgilerin doğruluğundan emin olmak mümkün değildir. Bu saldırılara karşı yönlendirme topolojilerini konum bilgilerine göre belirleyen coğrafik yönlendirme protokolleri kullanılabilir. Bu protokollerde trafik, fiziksel konuma göre yönlendirildiğinden saldırganların bir çıkış deliği oluşturması oldukça zordur [4].

3.4.1.6. Solucan deliği saldırısı (Wormholes)

Solucan deliği saldırılarında saldırganlar, ağın belli bir bölgesinden gelen mesajları yüksek hızlı bağlantılar ile ağın farklı bir bölgesine iletir [4]. Özellikle Şekil 3.2'de görüldüğü gibi, bir saldırganın çıkış düğümüne yakın diğerinin ise uzak olduğu durum düşünülürse; çıkış düğümüne uzak olan saldırgan kendisine gelen mesajları solucan deliği (wormhole) olarak adlandırılan yüksek hızlı iletim hattı ile diğer saldırgana, diğer saldırgan da çıkış düğümüne iletir. Bu şekilde normal düğümler çıkış düğümüne birkaç atlama uzaklıkta olduklarını zannederler. Hizmetlerin aksamasından ziyade ağ performansının arttırılması gibi gözüken bu durum aslında solucan deliğinin davranışları ile yakından ilgilidir [76]. Saldırganlar normal düğümleri kandırdıktan sonra yönlendirme yollarının çoğunun değişmesine sebep olurlar ve bu faaliyetlerini maksatlı olarak kestiklerinde ya da değişikliğe uğrattıklarında yönlendirme protokolünün çökmesine sebep olurlar. Bu şekilde yönlendirme yollarının değişmesini sağlayarak güç tüketiminin artmasına ve ağın tutarsız çalışmasına sebep olurlar.



Şekil 3.2. Solucan deliği saldırıları [4]

Çıkış deliği saldırılarında olduğu gibi solucan deliği saldırılarına karşı da yönlendirme topolojisinin, baz istasyon konum bilgilerine göre oluşturulduğu coğrafik yönlendirme protokolleri kullanılabilir [4,74].

3.4.1.7. Sybil saldırısı

Sybil saldırıları ilk olarak Douceur [77] tarafından P2P (Peer to Peer-Noktadan noktaya) ağlar için tanımlanmıştır. Daha sonra Karlof ve diğerleri [4] tarafından bu saldırıların kablosuz algılayıcı ağı yönlendirme katmanını tehdit eden bir saldırı türü olduğu gösterilmiştir.

Çoğu protokol, düğümlerin sadece bir adet kimliğe sahip olduğunu varsaymaktadır. Sybil saldırılarında saldırganlar birden fazla kimliğe sahiptir ve kendilerini aynı anda birçok yerdeymiş gibi gösterebilirler. Bu sebeple Sybil saldırıları topolojinin konum bilgisine göre belirlendiği coğrafik yönlendirme ve çok yollu yönlendirme protokolleri için önemli bir tehdit unsurudur. Ayrıca veri toplama, oylama ve kaynakların adil paylaşımı gibi uygulamalar için etkili bir saldırı türüdür.

Sybil saldırıları için geliştirilen çözümler kimlik denetim esasına dayanmaktadır. Newsome ve diğerleri gerçekleştirdikleri çalışmada [78], iki farklı yöntemle kimlik denetimini gerçekleştirmeyi önermişlerdir. Birinci yöntem radyo kaynak testi esasına dayanmaktadır. Bu testte her düğüm iletişim yapmak için komşularına farklı bir kanal tahsis eder ve rasgele seçtiği kanaldan paket göndererek o kanalı dinlemeye

başlar. Eğer kanalda iletişim sezerse gerçek bir kimliğe sahip komşu olduğunu anlar aksi durumda ise kanala atanan kimliğin sahte olduğuna karar verir. İkinci yöntem ise rasgele ön yüklemeli anahtar dağıtım esasına dayanır. Bu yöntemde, anahtar havuzunda sınırlı sayıda anahtar olduğu varsayılır. Rasgele bir kimlik üreten düğüm, fazla sayıda kimlik üretmeye yetecek kadar anahtara sahip olamaz böylelikle geçersiz kimlik ile ağ içersindeki mesajların şifresini çözemez.

3.4.1.8. Hello flood saldırısı

HELLO (Merhaba), çoğu protokolde ağın kurulum aşamasında kullanılan bir mesaj türüdür. Düğümler komşularına kendilerini bu mesaj sayesinde tanıtırlar. HELLO mesajını alan düğümler bu mesajların tek atlama uzaklıktaki komşularından geldiğini kabul eder ve komşu tablolarını oluştururlar. Ancak solucan deliği saldırılarında olduğu gibi güçlü alıcı/vericiye sahip saldırganlar uzak mesafelere de HELLO mesajını yayarak düğümlere kendisini tek atlamadaki komşuymuş gibi gösterebilir. Böylelikle yönlendirme yollarının yanlış kurulmasını sağlayarak paketlerin düşmesine sebep olur.

Bu saldırıların savunmasında Sybil saldırılarında olduğu gibi kimlik denetim yöntemi kullanılabilir. Düğümler güvenilir üçüncü bir düğüm kullanarak her bir komşusunun kimlik denetimini gerçekleştirir ve kimlik denetiminden geçemeyen paketleri iptal edebilirler [4,74].

3.4.2. Trafik analiz saldırıları

Kablosuz algılayıcı ağ uygulamalarında algılayıcı düğümler, genellikle birçok atlama üzerinden baz istasyona rapor bilgilerini iletirler. Raporlama periyodik olarak yapılabileceği gibi olay güdümlü olarak da yapılabilir. Periyodik raporlamada (proaktif algılayıcı ağlar) düğümler herhangi bir şey sezip sezmediklerine bakmaksızın periyodik zaman dilimlerinde çıkış düğümüne rapor bilgisi göndermek zorundadır. Olay güdümlü raporlama (reaktif algılayıcı ağlar) da ise düğümler sadece farklı bir olay algıladıklarında rapor bilgilerini çıkış düğümüne iletirler. Düşük güç tüketiminin en önemli ihtiyaç olduğu KAA uygulamalarında daha düşük güç

tüketimine sebep olan olay güdümlü raporlama tercih edilmektedir. Ancak bu raporlama tekniği çeşitli türdeki saldırılara imkân tanımaktadır. Örneğin saldırganlar paket akışını takip ederek hangi düğüm ya da düğümlerin bir olay algıladıklarını sezebilirler ya da gönderilen paket yoğunluğunun artmasına göre baz istasyonun yerini tayin edebilir ve baz istasyona yakın bir yere konuşlanarak çeşitli hizmet engelleme saldırılarını (boğma, seçmeli gönderim vb.) başlatabilir. Böylelikle baz istasyonla düğüm arasındaki iletişimi koparark ağın çökmesine sebep olabilir.

3.5. Sonuçlar

Bu bölümde kablosuz algılayıcı ağ güvenliğini sınırlayan unsurlar, güvenlik gereksinimleri ve kablosuz algılayıcı ağ güvenliğini tehdit eden saldırı türleri hakkında bilgi verilmiştir. Ayrıca saldırılara yönelik olarak literatürde geliştirilmiş olan çözüm yöntemleri hakkında özet bilgiler sunulmuştur. Ancak KAA güvenliğini tehdit eden saldırıların başında gelen boğma saldırılarına karşı düşük maliyetli ve başarılı çözüm yöntemlerinin geliştirilmesi, algılayıcı ağlarının güvenliğinin sağlanması açısından oldukça önemli bir eksiklik olarak karşımıza çıkmaktadır. Bu sebeple son yıllarda boğma saldırıları araştırmacılar için ilgi çekici bir çalışma alanı haline gelmiş ve bu doktora tezinin de temel motivasyonunu oluşturmuştur. Bu tezde, günümüz kablosuz algılayıcı ağlarının düşük maliyetli olarak boğma saldırılarına karşı dayanıklı hale getirilmesi hedeflenmiştir. Bir sonraki bölümde (Bölüm 4) literatürde sunulmuş olan boğma saldırgan modelleri ile ilgili detaylı bilgi verilecektir.

BÖLÜM 4. BOĞMA ŞEKLİNDEKİ HİZMET ENGELLEME SALDIRGAN MODELLERİ VE ANALİZİ

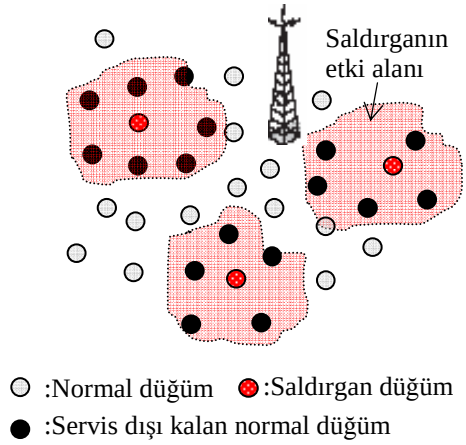
4.1. Giriş

Kasıtlı olarak radyo sinyali göndererek düğümlerin iletişimlerine girişim yapmak anlamına gelen boğma şeklindeki hizmet engelleme saldırıları, kablosuz ağlar için önemli bir güvenlik sorunu oluşturmaktadır. Bu saldırıların paylaşımlı olan iletişim kanalını meşgul ederek normal düğümlerin haberleşmesini engellemek ve çarpışmaya neden olarak normal düğüm iletişimlerinin aksamasına yol açmak gibi iki amacı bulunmaktadır. Boğma saldırıları, özellikle kaynakları sınırlı olan ve tek kanal frekansında haberleşen algılayıcı düğümleri için basit fakat etkilidir. Bu bölümde, kablosuz algılayıcı ağlar için tehdit olan saldırgan modelleri hakkında detaylı bilgi verilmekte ve saldırganların etkinliklerinin ölçülerek birbirleri ile kıyaslanabilmesi için tasarlanan yöntem sunulmaktadır. Ayrıca saldırganlar özelliklerine göre gruplandırılarak, çözüm yöntemlerinin daha kolay ve etkin şekilde gerçekleştirilebilmesine imkân sağlanmaktadır.

4.2. Boğma Saldırgan Modelleri

Literatürde, kablosuz algılayıcı ağlarındaki boğma saldırılarından ilk olarak Wood ve diğerlerinin gerçekleştirdiği çalışmada [3] bahsedilmektedir. Bu çalışmada, Şekil 4.1'de görüldüğü gibi K adet düğümün kablosuz algılayıcı ağ içerisine rasgele dağıtılması ve saldırganların sürekli veya aralıklı olarak sinyal göndererek N tane düğümü servis dışı bırakması öngörülmektedir. Ayrıca fiziksel katmanı etkileyen bu saldırıların dışında ortam erişim katmanın özelliklerinden faydalanılarak üç farklı türde saldırgan modelinin geliştirilebileceği vurgulanmaktadır. Çarpışma (collision) olarak adlandırılan birinci saldırgan modelinde, saldırganlar saldırı paketleri göndererek normal düğümlerin paketlerini bozmaya çalışırlar. Tek bir bayt bile

çarpışsa, paket CRC (Cyclic Redundancy Check-Çevrimsel Artıklık Denetimi) hatası vereceğinden bozulmuş demektir. CSMA/CA tabanlı ortam erişim protokolleri için RTS, CTS, DATA, ACK paketlerinden sadece ACK paketinin bozulması yeniden aynı sıra ile tüm paketlerin gönderilmesini gerektirmektedir. Bu saldırgan modeli, MAC katmanında tekrar gönderimlere neden olduğu için önemli ölçüde enerji tüketiminin ve gecikmenin artmasına sebep olmaktadır. Tüketme (exhaustion) olarak adlandırılan diğer saldırgan modelinde, saldırgan düğümler çok fazla sayıda RTS göndererek alıcıyı CTS göndermeye zorlarlar ve böylelikle alıcının güç tüketimini arttırarak pilinin hızlı bir şekilde tükenmesine yol açarlar. Eşitsizlik (unfairness) olarak tanımlanan bir diğer saldırgan modelinde ise, saldırganlar çekişme tabanlı ortam erişim protokollerinin kanal erişimi için düğümlere verdiği eşit önceliği bozarlar. Saldırgan düğümler çok kısa aralıklarla veya beklemeksizin paket göndererek iletişim kanalını meşgul ederler. Böylelikle kanal, normal düğümlerden çok saldırgan düğümler tarafından kullanılır.



Şekil 4.1. Bir saldırı senaryosu

Wood ve diğerlerinin önerdiği bu saldırgan modellerinden esinlenerek;

1. Xu ve diğerleri [5] sürekli, aldatıcı, rasgele ve reaktif saldırgan modellerini geliştirmişlerdir.
2. Law ve diğerleri ilk olarak S-MAC protokolü için bazı saldırı modelleri tanımlarken [6] ikinci çalışmalarında farklı ortam erişim protokolleri için enerji-etkin saldırgan modelleri geliştirmiştir [7].

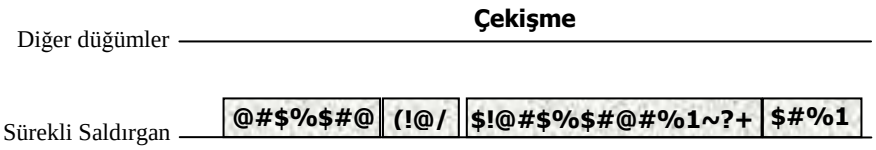
3. Wood ve diğerleri gerçekleştirdikleri bir diğer çalışmada [8] dört yeni saldırgan modeli tanımlamışlardır.

Literatürdeki çalışmalarda boğma saldırıları ile ilgili olarak genelde saldırgan modellerinin kablosuz algılayıcı düğümleri gibi sınırlı kaynaklara sahip oldukları varsayılmaktadır. Sınırsız güç kaynaklarına sahip ve birçok frekans bandına aynı anda saldırabilen saldırgan modelleri çalışmalarda ele alınmamıştır. Bu bölümde özellikleri açıklanan saldırgan modellerinin de algılayıcı düğümleri ile eş donanımsal kaynaklara sahip oldukları varsayılmaktadır.

4.2.1. Xu ve diğerlerinin geliştirdiği boğma saldırgan modelleri

4.2.1.1. Sürekli (Constant) saldırgan

Fiziksel katmanı etkileyen bir saldırgan modeli olan sürekli saldırgan Şekil 4.2'de görüldüğü gibi rasgele uzunluktaki paketleri sürekli olarak veya çok kısa aralıklarla iletişim kanalına gönderir. Bu sayede paylaşımlı olan iletişim kanalını meşgul ederek normal düğümlerin iletişim yapmasını engeller. Düğümlerin iletişimlerinin aksaması adına etkin bir saldırgan olmasına karşın, sürekli saldırdığı için enerji-etkin bir saldırgan değildir. Bu sebeple, sürekli saldırı stratejisi sınırlı güç kaynaklarına sahip olan saldırgan düğümleri için elverişli bir yöntem değildir.

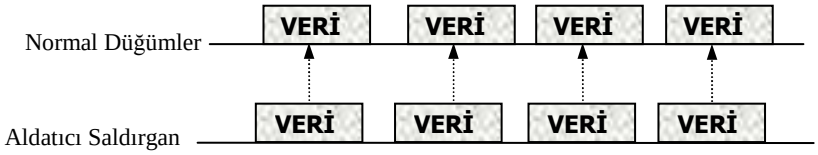


Şekil 4.2. Sürekli saldırgan

4.2.1.2. Aldatıcı (Deceptive) saldırgan

Aldatıcı saldırgan, rasgele uzunlukta paket göndermek yerine MAC katmanında karşılığı olan paketleri çok sık aralıklarla veya beklemeksizin iletişim kanalına gönderir. Saldırganların gönderdiği paketleri almak için alıcılarını sürekli olarak alma evresinde tutan normal düğümler bu nedenle enerjilerini çabuk tüketirler.

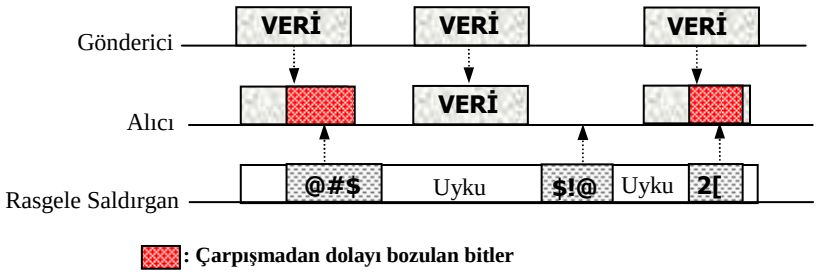
Aldatıcı saldırı stratejisi de sürekli paket gönderimini gerektirdiği için sınırlı kaynaklara sahip olan saldırgan düğümler için elverişli bir yöntem değildir.



Şekil 4.3. Aldatıcı saldırgan

4.2.1.3. Rasgele saldırgan

Rasgele saldırgan, rasgele zaman aralıklarında saldırır ve diğer zamanlarda radyosunu uyuma modunda tutarak enerjisini korur. Sürekli paket göndermediği için düğümlerin iletişimlerini tamamen engelleyemez. Ancak saldırdığı zamanlar, düğüm iletişimlerine denk gelirse çarpışmaya neden olur. Saldırdığı süre boyunca sürekli veya aldatıcı saldırgan gibi davranabilir. Rasgele saldırı stratejisi her ne kadar etkin olmasa da sınırlı güç kaynağına sahip saldırgan düğümler için elverişli bir yöntemdir.

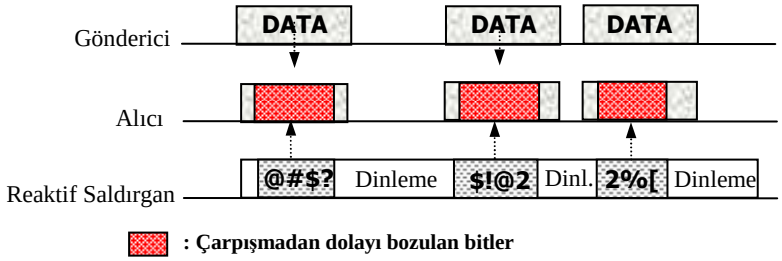


Şekil 4.4. Rasgele saldırgan

4.2.1.4. Reaktif saldırgan

Reaktif saldırgan, sürekli ve rasgele saldırgan gibi bilinçsiz bir şekilde saldırmak yerine sadece düğümlerin iletişim zamanlarında saldırır. Başka bir deyişle sadece iletişim kanalının meşgul olduğu durumlarda saldırır diğer zamanlarda dinlemede kalır. Saldırmaya bir paketin öntakısını sezdiğinde başlar ve böylece gönderilen paketlerin bozulmasını sağlar. Ortamı sürekli dinlemesi sebebiyle reaktif saldırgan da

aldatıcı ve sürekli saldırgan gibi güç açısından verimli değildir. Ancak reaktif strateji ile saldırdığı için diğer saldırganlara oranla tespiti daha zordur.

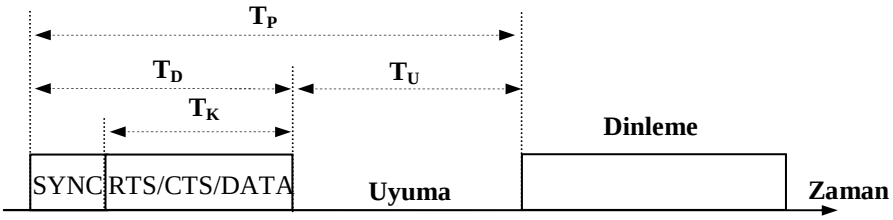


Şekil 4.5. Reaktif saldırgan

4.2.2. Law ve diğerlerinin geliştirdiği boğma saldırgan modelleri

4.2.2.1. Detaylı bilgi gerektiren boğma saldırıları

Law ve diğerleri gerçekleştirdikleri çalışmada [6], S-MAC protokolü için üç saldırgan modeli geliştirmiştir. Bu saldırganlar, MAC protokolünün bazı özelliklerinden faydalanarak enerji etkin bir şekilde düğümlerin iletişimlerini bozmayı hedeflemektedir. Şekil 4.6'da, S-MAC protokolünün zamanlaması görülmektedir. Bölüm 2'de de anlatıldığı gibi S-MAC protokolü enerji tüketimini azaltmak için periyodik dinleme/uyuma zamanlaması kullanmaktadır. Bu zamanlamaya uyan düğümler beraber bir şekilde hareket ederek ağ görevlerini yerine getirirler. Düğümler arasında dinleme/uyuma periyotlarının eş zamanlı olabilmesi için her düğüm belirli zaman aralıklarında SYNC paketi göndermek zorundadır. SYNC paketleri düğümlerin ne kadar süre (T_{uyuma}) sonra uyuma periyoduna geçeceklerini göstermektedir. Eğer bir düğüm SYNC paketi göndermeden başka bir düğümden böyle bir paket alırsa paketi alan düğüm, gönderen düğümün zamanlamasına uyar ve rasgele bir zaman ($T_{rasgele}$) bekleyerek kendi uyuma zamanı belirten (T_{uyuma} -$T_{rasgele}$) SYNC paketini yeniden gönderir. Bu şekilde tüm düğümler dinleme/uyuma periyotlarının eş zamanlı olmasını sağlarlar. Şekil 4.6'da görülen SYNC aralığı düğümlerin SYNC paketlerini gönderdiği, kontrol aralığı ise RTS-CTS-DATA-ACK gibi paketlerin iletiminin gerçekleştirildiği kısımdır.



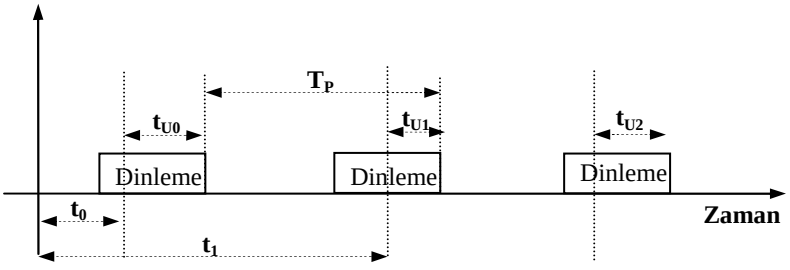
Şekil 4.6. S-MAC protokolünün zamanlama diyagramı [6]

Law ve diğerleri, S-MAC protokolünün sabit zamanlama kullanmasından faydalanarak çeşitli boğma saldırılarının gerçekleştirilebileceğini göstermiştir. S-MAC protokolünün veri bağı katmanında şifreleme yapılmadığı için saldırganlar, paketlerin içeriğine erişebilir ve SYNC paketleri yardımıyla düğümlerin dinleme/uyuma zamanlarını tahmin ederek uyuma zamanlarında uyuyup diğer zamanlarda saldırırlar. Bu yaklaşım ile üç farklı enerji-etkin saldırgan türü geliştirilebilir. Birincisi, bütün dinleme süresince saldıran periyodik dinleme aralığı saldırganı (PDAS), ikincisi, sadece kontrol aralığı boyunca saldıran ve diğer zamanlarda uyuyan periyodik kontrol aralığı saldırganı (PKAS) ve üçüncüsü ise sadece CTS paketlerini dinleyerek ardından gelen veri paketlerine saldıran veri paketi saldırganıdır (VPS). Saldırganlar Formül 4.1, 4.2 ve 4.3 den faydalanarak S-MAC protokolünün dinleme ve kontrol aralıkları ile periyot süresini tahmin edebilmektedir. Formüllerdeki t_0 ve t_1 dinlemeye başlandıktan sonra art arda alınan SYNC paket zamanları, t_{u0}, t_{u1} ve t_{u2} ise SYNC paketlerinden elde edilen uyuma zamanlarıdır. δ simgesi, gönderici düğümün taşıyıcı sezme ve DIFS için harcadığı süreyi temsil etmektedir.

$$T_P = t_1 + t_{u1} - t_0 - t_{u0} \quad (4.1)$$

$$T_D = \max(t_{u0}, t_{u1}, t_{u2}, ...) + \delta \quad (4.2)$$

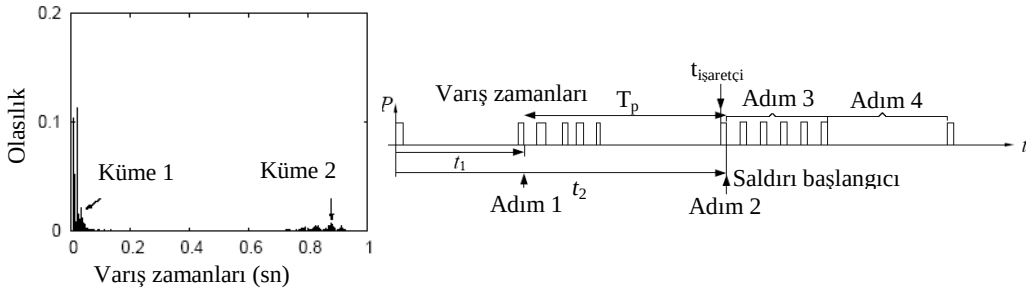
$$T_K = \min(t_{u0}, t_{u1}, t_{u2,} ...) - \delta \quad (4.3)$$



Şekil 4.7. S-MAC protokolünün parametrelerinin tahmini [6]

4.2.2.2. En az bilgi ile gerçekleştirilen boğma saldırıları

Law ve diğerleri gerçekleştirdikleri bir diğer çalışmada [7], şifrelenmiş paketler üzerinde tahmin yaparak veri paketlerinin bozulmasına sebep olan saldırgan modeli geliştirmiştir. Periyodik küme saldırganı (PKS) olarak isimlendirilen bu saldırgan, bulunduğu ortamdaki düğümlerin paket varış sürelerini belirli bir süre boyunca gözlemler ve kaydeder daha sonra da elde ettiği bu verilerin istatistikî sonuçlarından düğümlerin iletişim modellerini elde eder. Saldırganlar veri paketlerini, boyutlarının kontrol paketlerinden daha büyük olması sayesinde ayırabilmektedir. Saldırganın bulunduğu ortamda farklı dinleme/uyuma zamanlamasına sahip olan iki ya da daha fazla sanal küme olabilir. Bu kümlerin varış zamanları birbirine karışabilir. Periyodik küme saldırganı kümeleri birbirinden ayırmak için K-means kümeleştirme algoritmasından faydalanmaktadır [7]. Şekil 4.8.a'da iki farklı kümenin paket varış sürelerinin olasılığı, Şekil 4.8.b'de ise S-MAC protokolüne karşı yapılabilecek olan saldırı stratejisi görülmektedir.



(a) **(b)**

Şekil 4.8. Kümeler arası varış olasılıkları ve S-MAC protokolüne karşı yapılacak olan saldırı stratejisi

Law ve diğerlerinin geliştirdiği periyodik küme saldırgan algoritması aşağıda verilmektedir.

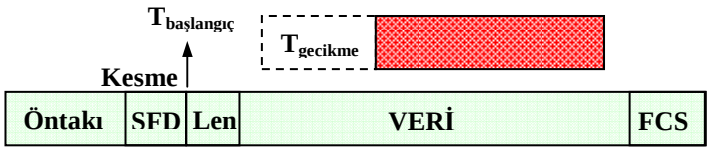
1. İlk Küme–2 varış zamanları gözlemlenene kadar bekle ve varış zamanını t_1 olarak kaydet.
2. Bir diğer Küme–2 varış zamanlarını bekle ve bunu da t_2 olarak kaydet, $T_P = t_2 - t_1$ formülünden kümenin periyodunu bul ve alınan paketlerin uzunluklarını L_p olarak kaydet (bayt olarak değil süre olarak).

3. $t_{işaretçi} = t_{şimdi}$ – Lp formülü ile işaretçiyi belirle ve c-1 paketle $\mu 1$ saniye aralıklarla saldır (c, küme-1 için ortalama paket varış sayısı; $\mu 1$, küme-1 için ortalama paketler arası varış süresi).
4. $t_{işaretçi}$ + Tp kadar uyu
5. İşaretçiyi $t_{işaretçi} = t_{şimdi}$ olarak ayarla, c adet paketle $\mu 1$ aralıklarla saldır.
6. 4. adımdan başlayarak adımları tekrarla

4.2.3. Wood ve diğerlerinin geliştirdiği boğma saldırgan modelleri

4.2.3.1. Kesme saldırganı

Yapı olarak reaktif saldırgana çok benzeyen kesme saldırganı, ortamdaki paket akışını sezmek için reaktif saldırgan gibi radyosunu sürekli dinleme evresinde tutmaz. Bunun yerine, daha az enerji harcamasını sağlayan pasif dinleme evresinde çalışır. Ortamdaki paket akışını ise donanımsal bir kesme ile algılar. Kesme saldırganı, Şekil 4.9'da görüldüğü gibi bir öntakı (preamble) ve SFD (Start of Frame Delimiter – Çerçeve Başlangıç Ayracı) sezdiğinde donanımsal bir kesme ile uyanır ve saldırıya başlar. Şekil 4.9'daki $T_{gecikme}$ (CC2420 için 128 μSn), kesme saldırganın paket gönderimine hazırlanması için geçen süredir.

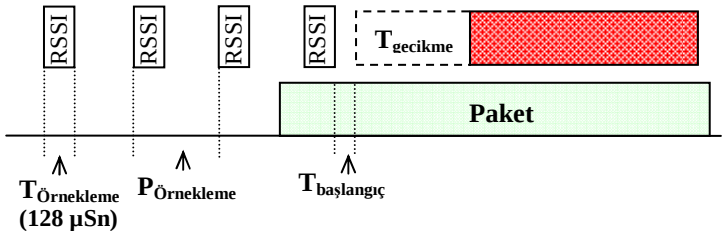


Şekil 4.9. Kesme saldırı stratejisi [8]

4.2.3.2. Aktivite saldırganı

Reaktif saldırgan boğma saldırısını başlatmak için bir öntakı beklerken, kesme saldırganı pasif dinlemede kalır ve bir öntakı ile SFD bekler. Ancak her iki saldırgan da öntakıların veya paketlerin tamamının şifrelenmesi halinde geçerli bir iletişim sezemeyecekleri için saldırı başlatamazlar. Aktivite saldırganı paketlerin şifrelenmesi durumunda iletişimin varlığını sezmek için Şekil 4.10'da görüldüğü gibi periyodik olarak ortamdan alınan sinyal seviyesini (Received Signal Strength Indicator - RSSI)

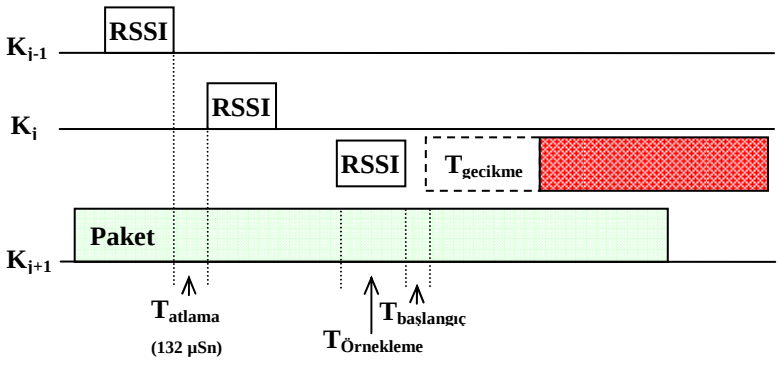
ölçer ve RSSI'nın belirli bir eşik değerinden yüksek olduğu anlarda düğümler arası iletişim olduğunu varsayarak saldırıyı başlatır. Ancak aktivite saldırganı, ortamdaki gürültüler sebebiyle normal düğüm iletişimi olmadığı zamanlarda da saldırı başlatabilir. Bu durumda daha fazla gönderim yaptığı için enerjisini hızlı tüketir.



Şekil 4.10. Aktivite saldırı stratejisi [8]

4.2.3.3. Tarama saldırganı

Sürekli, aldatıcı, rasgele, reaktif, periyodik dinleme aralığı, periyodik kontrol aralığı veri paketi, kesme ve aktivite saldırganlarının hepsi düğümlerin kanal değiştirmediğini ve haberleşmek için tek bir kanalda kaldıklarını varsaymaktadır. 2.45 GHz ISM bandı 80 MHz genişliğindedir ve IEEE 802.15.4 standardı, 5 MHz genişliğinde 16 adet kanala sahiptir. Düğümler, bu 16 adet kanalı kullanarak tek kanalda kalan saldırganların girişimlerinden kurtulabilirler. Tarama saldırganı, normal düğümlerin boğma saldırısını tespit ederek var olan kanallar arasında atlama yapmalarına karşılık geliştirilmiş bir saldırgan türüdür. Şekil 4.11'de görüldüğü gibi tarama saldırganı diğer saldırganlar gibi tek bir kanalda iletişimin varlığını sezmek yerine belirli bir süre boyunca bütün olası kanalları tarar ve iletişim olan kanalı tespit ettiğinde boğma saldırısını başlatır.



Şekil 4.11. Tarama saldırı stratejisi [8]

4.2.3.4. Darbe saldırganı

Düğümler kanallar arasında gezen tarama saldırganı gibi bir saldırgandan kaçmak için paketleri küçük parçalara bölerek her bir parçayı farklı kanaldan gönderebilirler. Böyle bir durumda, tarama saldırganı saldırmak için yeterli süre bulamayacaktır ve paketleri bozamayacaktır. Darbe saldırganı ise tek bir kanalda kalır ve paketin herhangi bir bölümünü bozmak için sürekli olarak küçük paketler gönderir. Paket parçalarından birisini bozmak paketin tamamının bozulması anlamına gelmektedir.

4.3. Boğma Saldırgan Modellerinin Etkinliklerinin Ölçülmesi ve Kıyaslanması

Düşmana karşı etkin bir savunma yöntemi geliştirebilmenin ilk adımı O'nu çok iyi tanımaktan geçmektedir. Dolayısıyla boğma saldırılarının üstesinden gelebilmek için bu saldırıların kablosuz algılayıcı ağına verdikleri zararı tanımlamak gerekmektedir. Literatürde sunulmuş olan saldırganların ağa verdiği zararı ölçmek ve birbirleri ile kıyaslayabilmek için bu çalışmada bazı değerlendirme ölçütleri tanımlanmış ve gerçekleştirilen benzetimler ile saldırganların etkinlikleri ölçülmüştür. İlerleyen kısımlarda, ilk olarak saldırganları değerlendirme amacıyla kullanıldığımız ölçütler açıklanmakta daha sonra ise bu ölçütlerden yararlanılarak gerçekleştirilen benzetimlerle saldırganların etkinlikleri ölçülmektedir.

4.3.1. Boğma saldırılarını değerlendirme ölçütleri

Boğma saldırılarının genel olarak iki amacı bulunmaktadır. Birinci amaç, düğümlerin paylaşımlı olan iletişim ortamına erişimini engelleyerek veya gönderilen paketlerin bozulmasını sağlayarak haberleşmelerini aksatmak, ikinci amaç ise güç tüketimini arttırarak düğümlerin yaşam sürelerini veya diğer bir ifadeyle ağın ömrünü azaltmaktır. Boğma saldırgan modellerinin etkinliklerini ölçmek ve birbiriyle kıyaslayabilmek, saldırganların yukarıda saydığımız bu amaçları hangi oranda gerçekleştirebildiğinin belirlenmesine bağlıdır. Bu sebeple tüketme oranı, saldırgan yaşam oranı, bozma oranı ve engelleme oranı olarak adlandırdığımız dört parametre yardımıyla boğma saldırgan modellerinin etkinlikleri tespit edilmeye çalışılmıştır.

- Saldırgan Yaşam Oranı (SYO): Saldırganların yaşam süresinin, normal düğümlerin yaşam süresine oranıdır. Bu oran yardımıyla bir saldırganın hangi ölçüde enerji-etkin bir saldırgan olduğu hesaplanabilir. Saldırganların yaşam süresi $Y_{Saldırgan}$ ve normal düğümlerin yaşam süresi Y_{Normal} olduğu varsayıldığında bir saldırganın yaşam oranı Formül 4.4 yardımıyla hesaplanabilir. %100 den büyük çıkan oranlar saldırganların normal düğümlere oranla daha uzun yaşadığını yani enerjisini daha verimli kullandığını göstermektedir. Bu oran ne kadar küçük olursa, saldırganın etkinliği de O oranda kısa olmakta ve ağa verdiği zararlar sınırlı kalmaktadır.

$$\text{Saldırgan Yaşam Oranı} = \frac{Y_{Saldırgan}}{Y_{Normal}} \times 100 \tag{4.4}$$

- Tüketme Oranı (TO): Tüketme oranı, düğümlerin saldırı sebebiyle yaşam sürelerinin ne kadar kısaldığını gösteren orandır ve bu oran yardımıyla bir saldırganın sebep olduğu enerji tüketimi hakkında bilgi sahibi olunabilir. Bir düğümün saldırı yokken ki yaşam süresi Y_{Normal} ve saldırı altındaki yaşam süresi $Y_{Saldırı}$ olarak varsayıldığında saldırganın tüketme oranı Formül 4.5 yardımıyla hesaplanabilir. Negatif çıkan değerler, saldırı durumlarındaki düğüm yaşam sürelerinin normal koşullara göre uzadığını göstermektedir. Bir diğer ifadeyle, düğümler saldırı süresince ekstra güç tüketmeyip aksine daha az enerji harcamış demektir.

$$\text{Tüketme Oranı} = \frac{Y_{Normal} - Y_{Saldırı}}{Y_{Normal}} \times 100 \tag{4.5}$$

- Paket Engelleme Oranı (PEO): Paket engelleme oranı, normal düğümlerin göndermek isteyip de gönderemediği paketlerin oranlarını vermektedir. Paylaşımlı olan iletim kanalının normal düğümlerden çok saldırganlar tarafından kullanıldığı durumlarda düğümler iletişim ortamına uzun süreler boyunca erişemez ve paket gönderemezler. Dolayısıyla gönderilemeyen paketler zaman aşımı nedeniyle iptal edilirler. Düğümlerin göndermek istediği paket sayısı $P_{İstenen}$, gönderebildiği paket sayısı ise $P_{Gönderilen}$

olduğunda paket engelleme oranı Formül 4.6 yardımıyla hesaplanabilir. Büyük çıkan engelleme oranları, saldırganların çoğunlukla iletişim ortamına hâkim olduğu ve düğümlerin paket göndermelerini engellediğini göstermektedir.

$$\text{Paket Engelleme Oranı} = \frac{P_{\text{İstenen}} - P_{\text{Gönderilen}}}{P_{\text{İstenen}}} \times 100 \quad (4.6)$$

- Paket Bozma Oranı (PBO): Paket bozma oranı, düğümlerin gönderdiği paketlerden ne kadarının çakışma nedeniyle bozulduğunu göstermektedir. Düğümlerin gönderdiği paket sayısı $P_{\text{Gönderilen}}$, alıcılara başarılı bir şekilde ulaştırabildiği paket sayısı ise $P_{\text{Ulaştırılan}}$ olarak adlandırıldığında Formül 4.7 yardımıyla paket bozma oranı hesaplanabilir.

$$\text{Paket Bozma Oranı} = \frac{P_{\text{Gönderilen}} - P_{\text{Ulaştırılan}}}{P_{\text{Gönderilen}}} \times 100 \quad (4.7)$$

4.3.2. Benzetim ayarları

Boğma saldırgan modellerini gerçeklemek ve birbirleri ile kıyaslamak için detayları EK.B'de verilen OMNeT++ [79] tabanlı benzetim yazılımı kullanılmıştır. 20 adet normal düğüm ve 20 adet saldırgan düğüm 300m x 300m büyüklüğündeki bölgeye rasgele dağıtılmış, bir adet çıkış düğümü ise merkeze yerleştirilmiştir. Saldırganların düğüm iletişimlerine verdiği zararı daha kolay ölçebilmek için her bir düğümün kapsama alanında en az bir adet saldırgan düğüm olacak şekilde yerleştirme işlemi gerçekleştirilmiştir. Normal düğümler ile saldırgan düğümlerin güç tüketimleri, radyo iletim mesafeleri aynıdır ve MICA2 [80] düğümüne uygun olarak seçilmiştir. Saldırgan düğümlerin ve normal düğümlerin 0.5 mA/saat kapasitelik pillere sahip olduğu varsayılmaktadır. Benzetimlerde 1 paket / 5 saniye olmak üzere sabit trafik hızı kullanılmıştır ve düğümler en kısa yol algoritması ile çıkış düğümünün yolunu bulmaktadırlar. MAC katmanı için %10 görev çevrimine (100 msn dinleme, 900 msn de uyuma) sahip S-MAC [27] protokolü kullanılmıştır. Temel benzetim ayarlarının özeti Tablo 4.1'de verilmektedir.

Tablo 4.1. Temel benzetim ayarları

Alan	300 x 300 m^2
Topoloji	Rasgele yerleşim
Normal düğüm sayısı	20
Saldırgan düğüm sayısı	20
Çıkış düğüm sayısı	1
İletim mesafesi	100 m
Taşıyıcı sezme mesafesi	200 m
Başlangıç enerjisi	0.5 ma/saat
Uygulama Katmanı	CBR= 0.2 paket/saniye
Yönlendirme katmanı	En kısa yol algoritması
MAC protokolü	S-MAC (100 msn dinleme, 900 msn uyuma)
Kontrol paket büyüklüğü	10 bayt
Veri paketi büyüklüğü	40 bayt

Saldırgan modellerinin kullandığı paket büyüklükleri ve bazı saldırı özellikleri Tablo 4.2'de görülmektedir. Benzetimlerde kullanılan değerler mümkün olduğunca çalışmalarda verilen orijinal değerlere uygun olarak seçilmiştir. Yaşam süresi, normal düğümlere nazaran daha az olan saldırganların yaşam oranlarını elde etmek için benzetimler ağ içerisindeki ilk düğüm ölene kadar devam etmiştir. Aksi durumda, yani yaşam süresi normal düğümlerden daha uzun olan saldırganların yaşam oranlarını elde etmek için ise benzetimler ilk saldırgan ölene kadar devam etmiştir. Her bir saldırı senaryosu en az beş farklı topoloji ile tekrar edilmiş ve elde edilen tüketme, yaşam, bozma ve engelleme oranlarının ortalaması alınmıştır.

Tablo 4.2. Boğma saldırgan modellerinin benzetim ayarları

Reaktif saldırı paketi	20 bayt
Sürekli saldırı paketi	0–48 bayt
Aldatıcı saldırı paketi	10 bayt
Rasgele saldırı paketi **Rasgele Saldırma oranı**	Max 0.100 msn saldır, max 0.900 msn uyu (%10)
PDAS, PKAS, VPS, PKS saldırı paketi	20 bayt
Kesme saldırı paketi **Saldırı için gönderim gecikmesi**	10 bayt $\approx 833\ \mu Sn$
Aktivite saldırı paketi **Ortalama RSSI örnekleme süresi** **RSSI örnekleme aralığı**	10 bayt 800 μSn bayt 10 msn
Tarama Saldırganı **Minimum atlama süresi**	132 μSn
Darbe Saldırganı saldırma süresi **Darbe Saldırganı durma süresi**	1,04 msn 2,91 msn (%35.7 görev çevrimi)

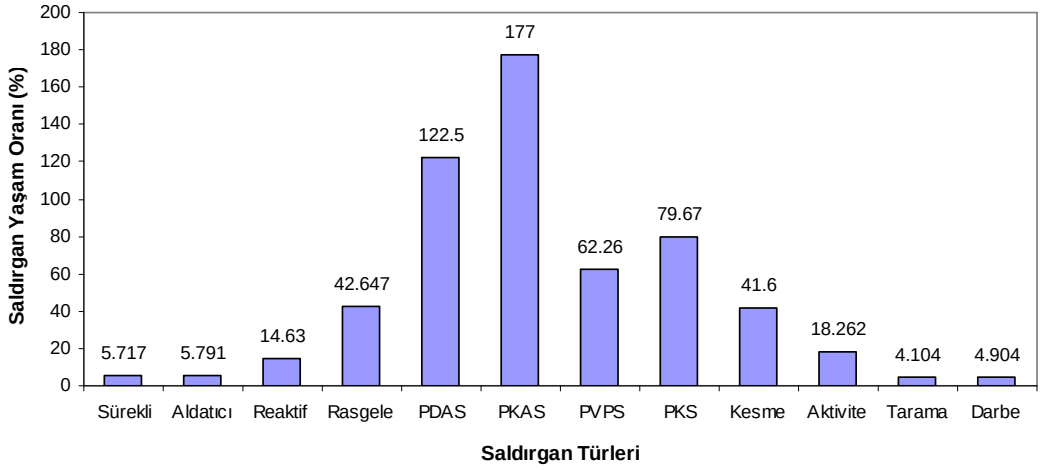
4.3.3. Benzetim sonuçları

4.3.3.1. Saldırgan yaşam oranı

Bir saldırganın normal düğümlere göre hangi oranda yaşamını sürdürebildiğini gösteren saldırgan yaşam oranları Şekil 4.12'de görülmektedir. Periyodik kontrol aralığı saldırganı (PKAS) ve periyodik dinleme aralığı saldırganının (PKAS) bulundukları ortamdaki normal düğümlere oranla daha uzun süre yaşamlarını devam ettirdikleri şekilden anlaşılmaktadır. Bu iki saldırgan dışındaki tüm saldırganlar normal düğümlerden daha kısa sürede ömürlerini tamamlamaktadırlar. PKAS'ın yaşamını uzun süre devam ettirebilmesinin birinci sebebi, normal düğümlerle senkronize olarak dinleme/uyuma çevrimlerine göre hareket edebilmesidir. İkinci sebebi ise PKAS'ın düğümlerin uyuma vakti gelince paket göndermeyi durdurarak uyuma moduna geçmesi, düğümlerin ise bu süre zarfında uyumak yerine dinlemede kalmasıdır. Saldırı altındaki düğüm kanala erişemediği için iletişimini erteler ve sürekli BACKOFF (Geriçekilme) durumunda kalır. S-MAC protokolünde bir düğümün BACKOFF durumundan kurtulması ancak RTS, CTS, DATA, ACK ya da hatalı bir paket aldığında gerçekleşir. Dolayısıyla saldırganlar, düğümlerin uyuma periyodu geldiğinde saldırıyı durdurup uyuma moduna geçseler bile normal düğümler geçerli veya hatalı bir paket alamadıkları için BACKOFF modundan kurtulamazlar ve uyuma moduna geçemezler. Uyuma aralığı boyunca uyanık kalmak enerji tüketimini önemli ölçüde arttırdığından düğümler enerjilerini PKAS'na oranla daha çabuk tüketirler. Benzer olaylar PDAS için de geçerlidir ancak PDAS'ın PKAS'a göre daha uzun süre saldırması (PDAS'ın tüm dinleme aralığı boyunca) daha fazla güç tüketimine neden olmaktadır.

Veri paketi saldırganının PKAS ve PDAS oranla daha düşük yaşam oranına sahip olmasının sebebi ise normal düğümleri uyuma süresince uyanık tutamamasıdır. Çakışan paketler için yeniden gönderim yapmak, uyuma aralığı boyunca dinlemede kalmaktan daha az enerji tüketimine neden olmaktadır. Ayrıca S-MAC protokolünde, Veri paketi göndermesine rağmen ACK alamayan düğümler uyuma moduna geçmektedirler. Bu sebeplerden dolayı VPS, PDAS ve PKAS'a göre daha düşük yaşam oranına sahiptir. Periyodik küme saldırganı ise normal düğümlerin iletişim

davranışlarını istatistiksel olarak belirlemektedir. Saldırganın enerji tüketimi komşu sayısı, trafik hızı ve elde edebildiği iletişim davranış bilgilerinin doğruluğu ile yakından ilgilidir.



Şekil 4.12. Farklı saldırgan modelleri için elde edilen yaşam oranları

Sürekli olarak paket gönderen sürekli ve aldatıcı saldırganlar, benzer yaşam oranlarına sahiptirler. Çok kısa aralıklarla veya kesintisiz olarak paket gönderimi bu iki saldırganın enerjilerini normal düğümlere göre çabuk tüketmelerine neden olmaktadır. Ortamı dinleyen ve bir iletişim sezdiğinde saldıran reaktif saldırgan, paket çakışmasına sebep olmaktadır. Ortamdaki iletişimin varlığını sezmek için radyosunu sürekli dinleme modunda tutması bu saldırganın da enerjisini çabuk tüketmesine sebep olmaktadır. Rasgele zaman aralıklarında saldıran veya uyuyan rasgele saldırgan ise sürekli, aldatıcı ve reaktif saldırganlara göre daha yüksek yaşam oranına sahiptir. Bunun sebebi, rasgele saldırganın belirli zaman dilimlerinde radyosunu uyuma moduna geçirmesidir.

Kesme saldırganın yaşam oranı PKAS, PKS ve VPS'den daha düşüktür. Bunun sebebi bu üç saldırganın normal düğümler gibi uyuma moduna geçebilmeleri, kesme saldırganının ise saldırmadığı zamanlarda pasif dinleme modunda kalarak kesme beklemesidir. Pasif dinleme, sürekli dinlemeye oranla daha az güç tüketimine sebep olsa da uyuma moduna göre daha fazla güç tüketimine neden olmaktadır (Pasif dinleme: 426 µA, Dinleme: 1.2 mA, Uyuma: 2 µA).

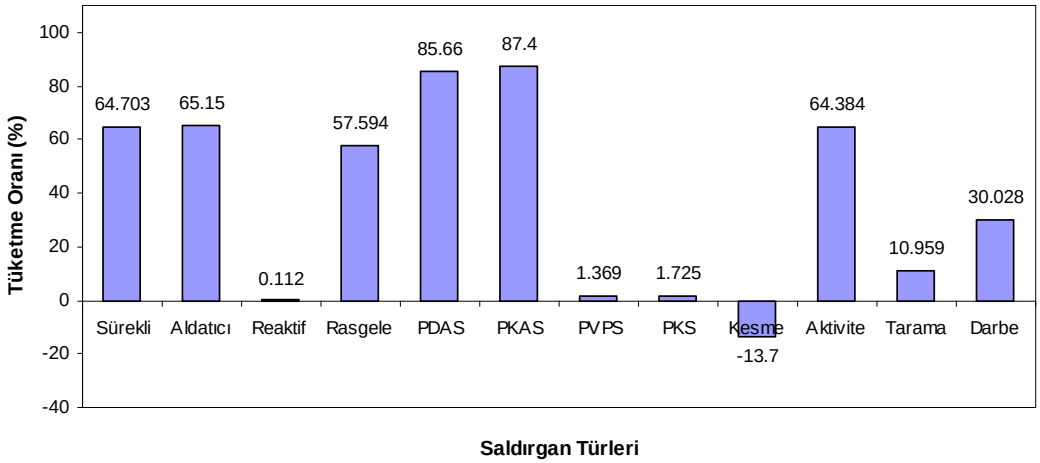
Aktivite saldırganı iletişimi sezebilmek için periyodik aralıklarda RSSI ölçümü gerçekleştirir. Yani radyosunu alım modunda uzun süre tutar ve bu sebeple enerjisini çabuk tüketir. Tarama saldırganı da sürekli kanal değiştirerek RSSI ölçümü gerçekleştirdiği için enerjisini hızla tüketir. Darbe saldırganının tarama saldırganına göre daha uzun ömürlü olma sebebi, tek bir kanalda kalarak küçük boyutlu paketlerle saldırmanın farklı kanallarda gezerek RSSI ölçümü yapmaya oranla daha düşük enerji tüketmesidir. Tarama ve darbe saldırganlarının sürekli paket gönderimi gerçekleştiren sürekli ve aldatıcı saldırganlara oranla daha düşük yaşam oranına sahip olmalarının sebebi ise Şekil 4.13'de görüldüğü gibi bu iki saldırganın normal düğümlerin enerji tüketimlerini darbe ve tarama saldırganlarına kıyasla daha fazla arttırmasıdır.

4.3.3.2. Tüketme oranı

Bir saldırganın ağdaki enerji tüketimini normal koşullara göre ne ölçüde arttırdığını veya ağ ömrünün ne ölçüde kısalmasına sebep olduğunu gösteren tüketme oranları (TO) Şekil 4.13'de görülmektedir. PKAS ve PDAS normal düğümlere oranla en uzun yaşayan iki saldırgan olmakla birlikte en fazla enerji tüketimine neden olan saldırganlardır. Sürekli ve aldatıcı saldırganlar düşük yaşam oranlarına sahip olmasına karşın aktif kaldıkları süre zarfında düğümlerin enerji tüketimlerinin önemli ölçüde artmasına neden olmaktadırlar. Aktivite saldırganı da sürekli ve aldatıcı saldırgana benzer şekilde yüksek tüketme oranına sahiptir. Bunun sebebi, ortam gürültüleri sebebiyle iletişim olduğunu varsayarak çoğu zaman saldırması ve dolayısıyla düğümleri BACKOFF durumunda bırakarak uyuma aralığında uyanık kalmalarını sağlamasıdır.

Tüketme oranları için dikkat edilmesi gereken husus çarpışmaya neden olan saldırgan modellerinin daha düşük tüketme oranına sahip olduğudur. VPS, PKS, reaktif saldırgan ve kesme saldırganı normal düğümlerin paketlerinin çarpışma sonucunda bozulmasına neden olmaktadır. Paketlerin yeniden gönderilmesi, enerji tüketiminin artmasına sebep olsa da ACK alamayan düğümlerin uyuma moduna geçmeleri enerji tüketiminin azalmasını sağlamaktadır. Diğer taraftan kanalı meşgul ederek paket gönderimini engelleyen saldırganlar, düğümleri uyuma aralığında da

dinleme konumunda tuttukları için enerji tüketiminin önemli ölçüde artmasına neden olmaktadır. Kesme saldırganı için tüketme oranın negatif çıkması düğümlerin saldırı sırasında enerji tüketimlerinin artması yerine azaldığının göstergesidir. Reaktif saldırgana oranla daha uzun süre yaşayan kesme saldırganı aktif olduğu süre boyunca düğümlerin enerji tüketimlerinin normal koşullara göre azalmasına ve sonuç olarak ağ ömrünün %13.7 oranında artmasını neden olmaktadır.



Şekil 4.13. Farklı saldırganlar için elde edilen tüketme oranları

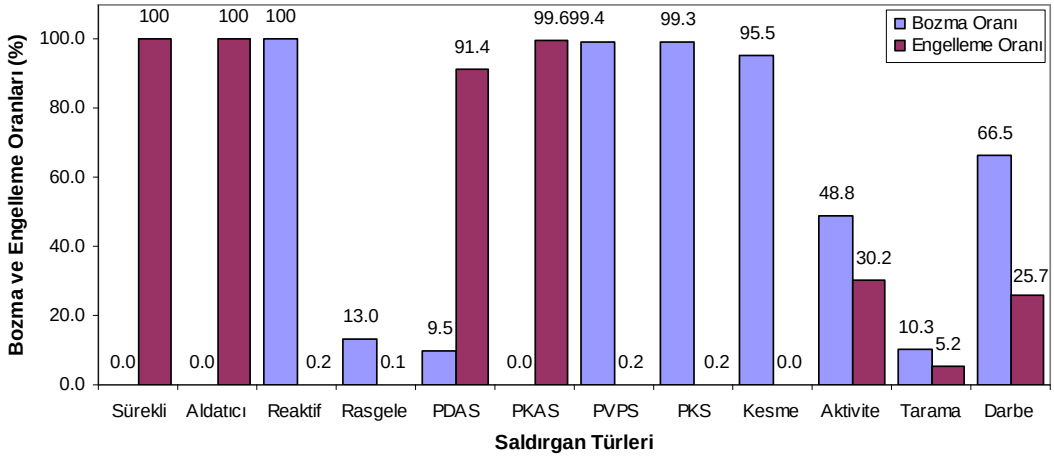
4.3.3.3. Paket engelleme ve paket bozma oranları

Farklı saldırı senaryoları için düğümlerin gönderemediği paketlerin yüzdesini gösteren *paket engelleme oranı* ve ulaştıramadığı paketlerin yüzdesini gösteren *paket bozma oranları* Şekil 4.14'de görülmektedir. Sürekli ve aldatıcı saldırgan gibi bazı saldırgan modellerinin yaşam sürelerinin normal düğümlere kıyasla çok kısa olması, ağ içerisinde bu saldırganların sebep olduğu toplam bozma ve engelleme oranlarının çok sınırlı olmasına sebep olmaktadır. Bunun sebebi saldırganların kısa sürede enerjilerini bitirmeleri ve geri kalan sürede bu oranların hızla normal değerlere dönmesidir. Bu açıdan saldırganların neden olduğu bozma ve engelleme oranlarının;

- Saldırganların aktif olduğu süre boyunca (ilk saldırganın enerjisini bitene kadar)
- Tüm düğümlerin enerjisi bitine kadar elde edilen toplam bozma ve engelleme oranları

olmak üzere iki kategoride incelenmesi, saldırganların saldırı stratejilerini ve verdikleri zararları tespit etmek açısından daha doğru bir yöntem olacaktır.

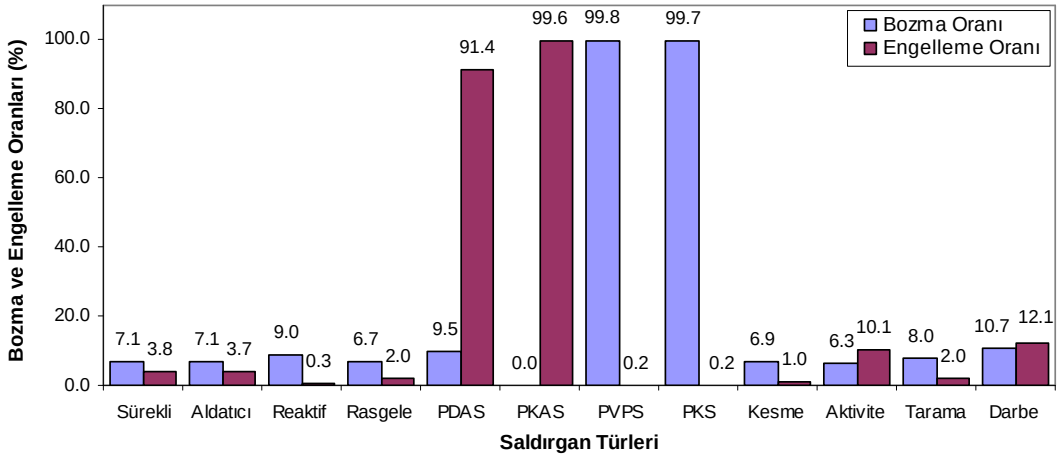
Şekil 4.14'de 12 farklı senaryo için saldırgan düğümlerin enerjisi bitene kadar ağdan elde edilen bozma ve engelleme oranları görülmektedir. Şekilden PDAS, PKAS, sürekli ve aldatıcı saldırganların yaşamlarını devam ettirdikleri süre boyunca paketlerin tamamına yakınının gönderimini engellediği anlaşılmaktadır. Reaktif, VPS, PKS, kesme ve darbe saldırganlarının ise paket gönderiminden ziyade gönderilen paketlerin önemli ölçüde bozulmasını sağladığı görülmektedir. Rasgele saldırgan için elde edilen %13'lük bozma oranı maksimum 0.900 msn uyuma ve 0.100 msn saldırma periyotları içindir. Rasgele saldırgan için saldırma oranının arttırılması bozma oranlarının yükselmesini sağlayacak ancak bunun yanında enerji tüketiminin de artmasına sebep olacaktır.



Şekil 4.14. İlk saldırganın enerjisi bitene kadar ölçülen bozma ve engelleme oranları

Şekil 4.15'de ise 12 farklı senaryo için ağdan elde edilen toplam bozma ve engelleme oranları görülmektedir. Yaşam oranları normal düğümlere nazaran daha kısa olan sürekli, aldatıcı, reaktif, rasgele, kesme, aktivite, tarama ve darbe saldırganlarının kısa sürede enerjilerini tüketmeleri, toplam bozma ya da engelleme oranlarının da tekrardan normal değerlere yaklaşmasına neden olmuştur. PDAS ve PKAS normal düğümlerden daha uzun süre yaşadığı için Şekil 14 ile Şekil 15 arasında bir fark gözlemlenmemiştir. PKS ve VPS için elde edilen bozma oranlarında ise şaşırtıcı

olarak çok küçük miktarda bir artış olmuştur. Bunun sebebi ise uzun süre yaşayabilen periyodik küme ve veri paket saldırganları ile birlikte birçok düğümün ölmesi ve geride kalan düğümlerin de paketleri ölen komşularına ulaştıramamasıdır. Bu sebeple de saldırganlar öldükten sonra da bozma oranları düşmemiştir.

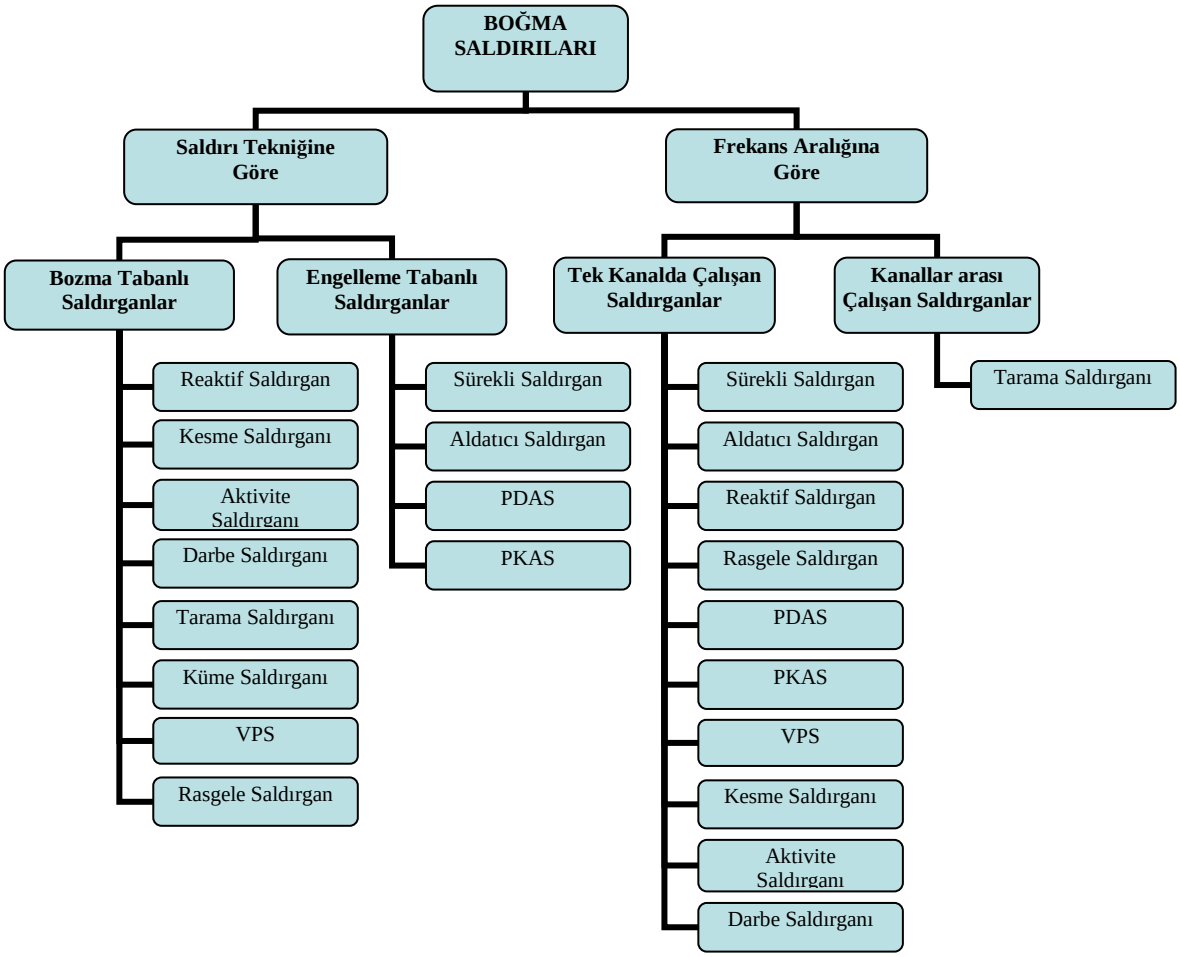


Şekil 4.15. Ağdaki tüm düğümler ölene kadar ölçülen toplam bozma ve engelleme oranları

4.4. Literatürdeki Boğma Saldırı Modellerinin Özelliklerine Göre Sınıflandırılması

Gerçekleştirilen benzetimler yardımıyla boğma saldırgan modellerinin etkinliklerinin ölçülmesi ve ağa verdikleri zararların tespit edilmesinden sonra saldırılara karşı uygun olan çözüm yöntemlerinin belirlenebilmesini kolaylaştırmak üzere bu çalışmada saldırgan modelleri karakteristik özelliklerine göre sınıflandırılmıştır. Literatürdeki boğma saldırı modelleri, saldırı tekniği ve frekans aralığı olmak üzere iki temel özelliğe göre kategorize edilebilir. Saldırı tekniği, bir boğma saldırgan modelinin en önemli karakterini ortaya koymaktadır. Genelde boğma saldırgan modelleri ya düğümlerin gönderdiği paketleri bozmayı hedeflemekte ya da iletişim kanalını meşgul ederek düğümlerin paket gönderimini engellemektedir. Paketlerin çakışma sebebiyle bozulmasına sebep olan saldırganlar bozma tabanlı saldırganlar olarak kategorize edilebilirken, iletişim kanalını sürekli meşgul ederek düğümlerin iletişim yapmasını engelleyen saldırgan türleri engelleme tabanlı saldırganlar olarak sınıflandırılabilirler. Saldırgan türlerinin bir diğer önemli karakterini ise saldırganın çalışabildiği frekans aralığı belirlemektedir. Literatürdeki birçok saldırgan, sadece merkez frekansta çalışarak düğümlerin iletişimlerini bozmayı/engellemeyi

hedeflerken tarama saldırganı mevcut iletişim kanallarını arasında gezerek düğüm iletişimlerini bozmaya çalışmaktadır.



Şekil 4.16. Literatürde sunulan boğma saldırgan modellerinin özelliklerine göre sınıflandırılması

4.5. Sonuçlar

Bu bölümde ilk olarak literatürde sunulan boğma saldırgan modelleri tanıtılmış, daha sonra bu saldırgan modellerinin etkinliklerinin ve kablosuz algılayıcı ağına verdikleri zararların belirlenebilmesi için geliştirilen yöntem açıklanmış ve son olarak da boğma saldırgan modelleri özelliklerine göre sınıflandırılmıştır. Saldırıların etkinlik süreleri ile kablosuz algılayıcı ağına verdikleri zararlar, Saldırgan Yaşam Oranı (SYO), Tüketme Oranı (TO), Paket Engelleme Oranı (PEO) ve Paket Bozma Oranı (PBO) olarak adlandırdığımız ölçütler yardımıyla ölçülmüştür. Elde edilen sayısal sonuçlara göre enerjisini en verimli kullanan saldırgan modelinin periyodik kontrol

aralığı saldırganı (PKAS) olduğu anlaşılmış ve bu saldırganın normal düğümlerin yaşam süresinin %77'si (SYO=%177) oranında daha uzun yaşadığı tespit edilmiştir. Enerjisini en verimsiz kullanan saldırgan modelinin ise tarama saldırganı olduğu ve bu saldırganın normal düğümlerin yaşam süresinin yaklaşık % 4.1 (SYO=%4.1) kadar yaşayabildiği belirlenmiştir. Düğümlerin enerjilerinin normal senaryolara göre ne kadar kısaldığını gösteren tüketme oranı sonuçlarına göre PKAS ve Periyodik Dinleme Aralığı Saldırganın (PDAS) düğüm enerjilerinin en çabuk tükenmesine yol açan saldırgan modelleri olduğu göze çarpmaktadır. Bu saldırganlar normal senaryolara göre düğümlerin yaşam sürelerinin yaklaşık %87 ve %85'lik oranlarında azalmasına yol açmaktadırlar. PEO ölçütlerine göre sürekli, aldatıcı ve periyodik dinleme aralığı saldırganlarının yaşadığı süre boyunca düğümlerin paket göndermelerini tamamen engellediği görülmüştür. Bununla birlikte PBO'ya göre ise reaktif, kesme, veri paketi ve küme saldırganlarının gönderilen tüm paketleri bozduğu tespit edilmiştir. Tablo 4.3'de boğma saldırgan modellerinin başarım analiz özeti sunulmaktadır.

Tablo 4.3. Boğma saldırgan modellerinin başarımı

Saldırgan Modeli	**Yaşam Süresi**	**İletişim Engelleme***	**Enerji Tükettirme**
Sürekli	Kötü	İyi	Orta
Aldatıcı	Kötü	İyi	Orta
Reaktif	Kötü	İyi	Kötü
Rasgele	Orta	Orta	Orta
PDAS	Çok iyi	İyi	İyi
PKAS	Çok iyi	İyi	İyi
VPS	İyi	İyi	Kötü
PKS	İyi	İyi	Kötü
Kesme	Orta	İyi	Kötü
Tarama	Kötü	Kötü	Kötü
Aktivite	Kötü	Orta	Orta
Darbe	Kötü	Orta	Orta

*Saldırganların yaşadığı süre boyunca

BÖLÜM 5. BOĞMA SALDIRILARININ TESPİTİNE YÖNELİK YENİ BİR YÖNTEM TASARIMI VE BAŞARIM ANALİZİ

5.1. Giriş

Ağ içerisine sızarak iletişime zarar vermeyi hedefleyen olumsuz aktivitelerin tespit edilmesi ve yetkili birimlere rapor edilmesi anlamına gelen Sızma Tespiti (Intrusion Detection), bir ağdaki güvenliğin sağlanması amacıyla kullanılan ilk savunma basamağıdır. Kablosuz algılayıcı ağlarda düğümler arasındaki iletişim kablosuz ortam üzerinden gerçekleştirilmekte ve sınırlı işlevsel kaynaklara sahip olan düğümler çoğunlukla dış ortamda bulunmaktadır. Bu gibi sebepler, kablosuz algılayıcı ağlarının diğer ağlara oranla daha fazla güvenlik riski taşımasına neden olmakta ve sızma tespit sistemlerinin kullanımını zorunlu kılmaktadır. Var olan sınırlı kaynakların tüketimini hızlandırarak ağ ömrünün kısalmasına sebep olan boğma saldırılarının tespit edilmesi kaynakların etkin kullanımı ve ağın güvenilirliği açısından son derece önemlidir. Bu bölümde, kablosuz algılayıcı ağları için önemli bir tehdit unsuru olan boğma saldırılarının tespit edilmesi üzerine odaklanılmaktadır. İlk olarak Sızma Tespiti kavramının detayları açıklanmakta, daha sonra kablosuz algılayıcı ağlar için geliştirilen sızma tespit yöntemleri özetlenmekte ve son olarak da boğma saldırılarına yönelik olarak geliştirilen bir Sızma Tespit Sisteminin (Instrusion Detection System-IDS) tasarımı ve başarım analizi sunulmaktadır.

5.2. Sızma Tespiti (Instrusion Detection)

Bilgisayar ağlarında iletişim normal trafik, kötü niyetli olmayan anormal trafik ve kötü niyetli trafik olmak üzere üç kategoride incelenebilir. Sızma tespit sisteminin başarısı bu trafik türlerini birbirinden doğru bir şekilde ayrılabilmesiyle yakından ilgilidir. Trafik türlerinin birbirinden ayrılamaması hatalı saldırı tespitlerine (false

positive detection) ya da saldırıların tespit edilememesine (false negative detection) neden olmakta ve saldırı tespit sisteminin güvenirliğini azalmaktadır.

Literatürde sızma tespit yöntem mimarileri fonksiyonel olarak iki ana kategoride toplanmaktadır [81]. Anomali tabanlı saldırı tespiti olarak adlandırılan ilk yöntemde, saldırgan düğümlerin normal dışı durumların oluşmasına sebep olduğu varsayılır. Bu yöntemde ilk olarak, normal şartlardaki sistem davranışları tespit edilir, daha sonra da bu davranışlar saldırı durumundaki sistem davranışları ile kıyaslanarak saldırı tespiti gerçekleştirilir. Birleşik (misuse) saldırı tespiti olarak adlandırılan ikinci yöntemde ise bilinen saldırı türlerini tanımlayan imzalar şüpheli durumlar ile kıyaslanarak saldırı tespiti gerçekleştirilir. Birleşik saldırı tespit yönteminin üstünlüğü tanımlanmış olan saldırı türlerinin basit ve hızlı bir şekilde tespit edilebilmesine olanak sağlamasıdır. Bu yöntemin zayıf tarafı ise yeni veya tanınmayan saldırı türlerinin tespit edilememesi ve saldırı imzalarının tutulduğu veritabanının sürekli olarak güncellenmesi gerektiğidir. Ayrıca kablosuz algılayıcı ağlarda çoğu uygulama için merkezi yönetim biriminin olmaması bilinen saldırı imzalarının dağıtımını ve günceleştirilmesini zorlaştırmakta ve dolayısıyla birleşik tespit yönteminin Kablosuz Yerel Alan Ağlarında ve diğer kablolu ağlarda olduğu gibi etkili olmasını engellemektedir. Anomali tabanlı saldırı tespit yönteminin üstünlüğü yeni veya bilinmeyen saldırı türlerinin de tespitine olanak tanımasıdır. Zayıf tarafı ise karmaşık bir yapıda olması ve daha fazla kaynak kullanımına ihtiyaç duymasıdır. Her iki yöntemin de kaynak sıkıntısı olan kablosuz algılayıcı ağlarda doğrudan kullanılması mümkün değildir. Yöntemler KAA'ların ihtiyaçlarına göre optimize edilmelidir.

5.3. Kablosuz Algılayıcı Ağları için Geliştirilen Sızma Tespit Sistemleri

Literatürde kablosuz algılayıcı ağları için genel sızma tespit sistem tasarımı ile ilgili çok fazla çalışma bulunmamakta ve geliştirilen saldırı tespit sistemleri de genellikle belirli türdeki saldırın teşhis edilmesine yönelik olarak kullanılmaktadır. Yu ve diğerlerinin gerçekleştirdikleri çalışmada [76] seçmeli iletim (selective forwarding) saldırılarının tespiti için alındı (ACK) tabanlı saldırı tespit yöntemi geliştirilmiştir. Bu çalışmada, iletim yolu üzerinde bulunan her düğüm saldırganın varlığını tespit

etmekle yükümlüdür. Eğer düğüm bir anormallik olduğunu tespit ederse iletimin yönüne göre kaynak düğüme ya da baz istasyona bir alarm paketi göndermektedir. Loo ve diğerleri makalelerinde [82] yönlendirme katman (aktif ve pasif çıkış deliği, periyodik yönlendirme hata) saldırılarının tespiti için anomali-tabanlı saldırı tespit sistemi geliştirmiştir. Önerilen yöntemde normal trafik davranış modelini elde etmek için bir kümeleştirme algoritmasından faydalanılmış ve daha sonra bu model anormal trafik durumlarını tespit etmek için kullanılmıştır. Önerilen bir diğer çalışmada [83] düğüm taklit (node impersonation) ve kaynak tüketme (resource depletion) saldırıları için belli aralıklar elde edilen paketler arası varış süresi ve alınan paketlerin sinyal gücü parametrelerinden faydalanarak anomali-tabanlı sızma tespit sistemi gerçekleştirilmiştir. Du ve diğerleri ise çalışmalarında [84] konumlandırma saldırılarının (Sessizlik saldırıları - Silence attack, Taklit saldırıları - Impersonation attack, Çoklu taklit saldırıları – Multi Impersonation attack, Mesafe değiştirme saldırıları – Range Change attack) tespitine yönelik anomali-tabanlı sızma tespit sistemi gerçekleştirmişlerdir.

Literatürde yönlendirme katman saldırıları ve konumlandırma saldırılarının tespitine yönelik çok sayıda çalışma bulunmasına karşın Boğma türündeki hizmet engelleme saldırılarının tespiti için sadece tek detaylı çalışma bulunmaktadır. Xu ve diğerleri [5], çalışmalarında tanımladıkları dört saldırgan modelini (sürekli, aldatıcı, reaktif ve rasgele) tespit etmek için iki farklı yöntem önermişlerdir. Birinci yöntemde paket teslim oranları (PTO) ile ortamdan alınan sinyal güç göstergesi (RSSI) dağılım tutarlılıklarına bakılarak normal koşullar ile saldırı durumları birbirlerinden ayrılmaktadır. Farklı senaryolarda RSSI değerlerine karşılık PTO dağılımları ölçülerek riskli ve risksiz bölgeler belirlenmiş ve PTO ile RSSI değerleri için eşik değerleri tespit edilmiştir. Eğer bir düğüm, eşik değerinden düşük PTO ve yüksek RSSI değeri ölçtüyse saldırı olduğunu varsaymaktadır. Bu önerilen yöntemin en zayıf yönü alıcı, gönderici ve saldırgan olmak üzere üç adet düğüm ile denenmiş olmasıdır. Geniş ölçekli ve yüksek yoğunluklu ağlarda, düğümlerin komşu sayılarının fazla olması çarpışma oranlarının yükselmesine yol açmaktadır [85]. Böylece PTO değerleri düşerken, düğümlerin ölçtüğü RSSI değerleri yüksek çıkmakta ve hatalı saldırı tespit oranlarının artmasına yol açmaktadır. Xu ve diğerlerinin geliştirdiği ikinci yöntem de ise yine PTO değerleri ile düğümlerin

konum bilgileri arasındaki tutarlılığa bağlı olarak tespit işlemi gerçekleştirilir. Bu yöntemin zayıf tarafı ise düğümlerin Küresel Konumlandırma Sistemi (Global Positioning System, GPS) gibi konum bilgisi sağlayan cihazlara ya da konumlandırma tekniklerine sahip olma zorunluluğudur. Ayrıca son çalışmalarda Xu ve diğerlerinin geliştirdiği dört saldırgan türünden daha zeki ve etkin saldırgan modelleri geliştirilmiştir (Detaylı bilgi için bkz. Bölüm 4). Bu gibi sebepler, PTO ve RSSI değerlerine göre tüm saldırı senaryolarının ayrıştırılmasını zorlaştırmaktadır. Boğma saldırılarının tespitine yönelik bir diğer çalışmayı da Wood ve diğerleri [9] gerçekleştirmiştir. Önerilen çalışmada sadece tek tip (sürekli saldırgan) saldırgan olduğunu varsayılmış ve saldırı tespiti, kanal kullanım oranın belirli bir eşik değerinin altına düşmesi ile belirlenmiştir. Ancak kanal kullanım oranı, komşu düğümlerde meydana gelebilecek yazılımsal veya donanımsal hata durumlarında, düğümlerin hareketi sebebiyle ve çevresel sebepler nedeniyle de düşebilir. Tek başına kanal kullanım oranı ile literatürde var olan tüm saldırı modellerinin başarılı bir şekilde tespiti mümkün değildir.

5.4. Anomali-Tabanlı Boğma Saldırı Tespit Sistemi (ABSTS)Tasarımı

Kablosuz algılayıcı ağlarının boğma saldırılarına rağmen üzerine düşen sorumlulukları yerine getirebilmesi ve işlevini sürdürebilmesi için öncelikle tüm bu saldırı türlerini başarıyla tespit edebilmesi ve daha sonra da uygun çözüm yöntemini kullanarak sorunun üstesinden gelebilmesi gerekmektedir. Bu gereksinimlerden ilham alarak literatürde tanımlı olan saldırı türlerinin tespitine olanak sağlayan Anomali tabanlı yöntem kullanılarak yeni bir Boğma Saldırı Tespit Sistemi-ABSTS tasarımı gerçekleştirilmiş ve bu bölümde tasarlanan sistemin özellikleri açıklanmıştır.

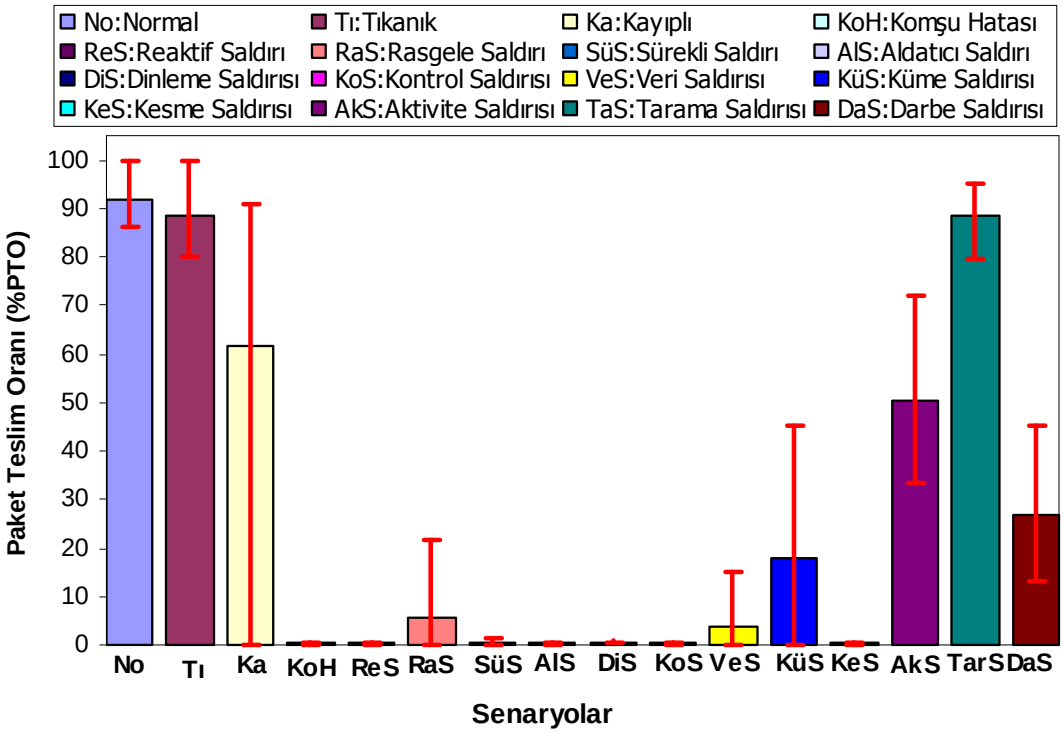
5.4.1. Boğma saldırıları için tespit ölçütleri

Bir ağdaki iletişimi tamamen engelleyen veya aksatan boğma saldırıları, ağ içerisinde bazı anormal durumların ortaya çıkmasına neden olmaktadır. Çarpışmaların ve hatalı paket alımlarının artması, iletişim kanalına erişim güçlüğü, yüksek sinyal güç göstergesi (RSSI) v.b. birçok parametre boğma saldırılarından etkilenmektedir. Anomali-tabanlı sistemler ise saldırı tespitini normal dışı (anormal) durumların

belirlenmesi esasına göre gerçekleştirmektedir. Bu sebeple boğma saldırılarının teşhis edilmesi için anomali-tabanlı sistemlerin kullanımı oldukça uygun gibi görünmektedir. Ancak parametrelerdeki anormal değerler kötü niyetli davranışlar sebebiyle meydana gelebileceği gibi doğal ağ koşulları sonucunda da oluşabilmektedir. Örneğin tıkanıklık, komşu düğümlerdeki yazılımsal veya donanımsal hatalar, çevresel şartların değişmesi ile meydana gelebilecek hatalar, saldırı senaryolarına benzer şekilde anormal durumların oluşmasına sebep olabilir. Daha zeki saldırı yöntemlerinin geliştirilmesi ve kablosuz algılayıcı düğümlerinin sınırlı donanımsal kaynaklara sahip olması bu saldırıların başarılı bir biçimde tespit edilebilmesini zorlaştırmaktadır. Başarılı bir saldırı tespit sistemi için normal durum ile anormal durum ayrımın çok iyi yapılması gerekmektedir aksi takdirde hatalı tespit işlemleri söz konusu olacaktır. ABSTS'de, benzer durumların oluşmasına neden olan doğal koşullar ile farklı boğma saldırı modellerini birbirlerinden ayırabilmek için MAC katmanından elde edilen bazı sistem parametrelerinden faydalanılmaktadır.

5.4.1.1. Paket teslim oranı (PTO)

Bir düğümden gönderilen paket sayısının alıcıya ulaşan paket sayısına oranı paket teslim oranı verir. Düğümler, gönderilen paketlerin alıcıya ulaştığını, alıcının gönderdiği bir ACK paketi ile denetler. Eğer 4-yönlü el sıkışma kullanılıyorsa (RTS/CTS/DATA/ACK) PTO, düğümün gönderdiği RTS ve DATA paketlerine karşılık aldığı CTS ve ACK paketlerinin oranlanması ile bulunabilir. Saldırganlar, düğümlerin gönderdiği paketleri bozarak PTO değerlerinin düşmesine neden olabilir. Ancak bir düğümdeki PTO değeri kayıplı bağlantı koşulları, komşu düğümde meydana gelebilecek hata durumları ve çakışmalar sebebiyle de önemli ölçüde düşebilmektedir. Bu sebeple tek başına paket teslim oranı yardımıyla tüm saldırı senaryolarının doğal ağ koşullarından ayrılması mümkün değildir.



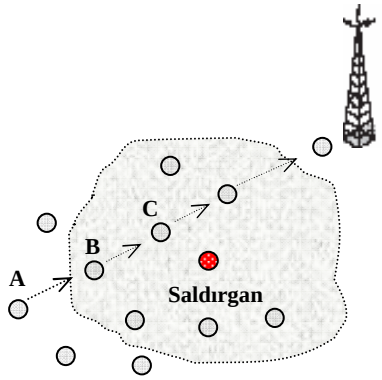
Şekil 5.1. Farklı senaryolarda bir düğümden ölçülen ortalama paket teslim oranları (Örnekleme Aralığı: 30sn, benzetim süresi: 3600 sn, hata çubukları minimum ve maksimum değerleri göstermektedir).

Şekil 5.1'de farklı saldırgan modelleri veya farklı ağ koşullarının etkisinde olan bir düğümden 30 saniye aralıklarla ölçülen paket teslim oranlarının minimum, maksimum ve ortalama değerleri görülmektedir. Reaktif ve kesme saldırganları, gönderilen RTS paketlerini bozarak düğümlerin CTS almasını, DATA göndermesini ve ACK almasını engellemektedir. Sürekli, aldatıcı, dinleme ve kontrol saldırganları ise iletim kanalını sürekli olarak meşgul ettiklerinden dolayı düğümlerin RTS göndermesini engellemekte ve dolayısıyla PTO değerinin sıfır çıkmasına neden olmaktadır. Rasgele saldırgan, rasgele zaman dilimlerinde saldırarak bazı paketlerin bozulmasına veya gönderiminin engellenmesine neden olmaktadır. Küme ve veri paketi saldırganları ise sadece VERİ paketlerini bozmaktadır. Aktivite saldırganın etkisi, iletim kanalında geçerli bir iletişimin varlığını doğru bir şekilde sezebilmesiyle ilgilidir. Tarama saldırganı düğümlerin iletişim yaptığı farklı kanalları tespit etmek için sırayla taramakta ve sezdiği kanala saldırı paketi göndermektedir. Ancak mevcut kanalları taraması sebebiyle çoğu zaman yavaş kalmakta ve iletişimi bozamamaktadır. Bu sebeple PTO değerleri çok etkilenmemektedir. Darbe saldırganı ise parçalara ayrılarak farklı kanallardan gönderilen paketleri tek bir kanalda kalarak

bozmaya çalışmaktadır. Bir düğümden ölçülen PTO, saldırılar dışında başka sebeplerden dolayı da düşebilmektedir. Komşu düğümde meydana gelebilecek bir hata (batarya sorunu v.b.) sonucunda PTO, saldırı durumlarına benzer şekilde düşebilecektir. Ayrıca kötü bağlantı koşullarının PTO değerlerinin düşmesine neden olması tek başına PTO parametresi ile saldırı tespitini güçleştirmektedir.

5.4.1.2. Hatalı paket oranı (HPO)

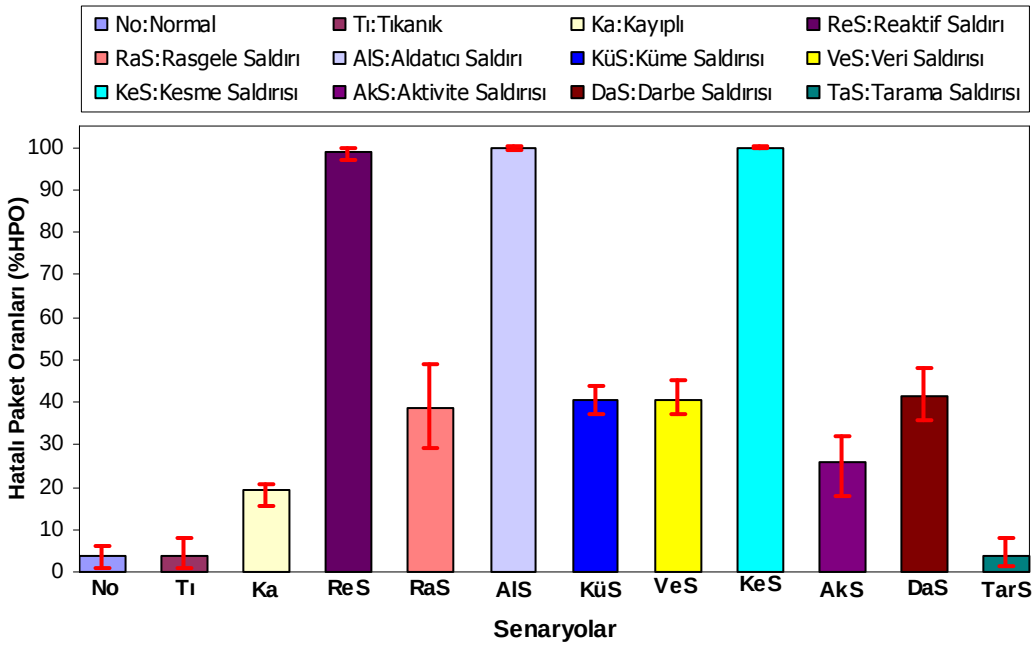
Bir düğümün aldığı bozuk paket sayısının alınan toplam paket ya da öntakı sayısına oranıdır. Düğümler paketin bozuk olup olmadığına CRC denetimi ile karar vermekte ve denetimden geçemeyen paketleri iptal etmektedir. Aslında PTO, gönderici açısından HPO ise alıcı düğüm açısından bağlantı kalitesini gösteren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



Şekil 5.2. Bir saldırı senaryosu.

Şekil 5.2'de "B" ve "C" düğümlerinin sürekli, dinleme aralığı veya kontrol aralığı gibi kanalı kesintisiz olarak meşgul eden saldırılar altında olduğu varsayıldığında bu iki düğüm herhangi bir paket gönderimi veya alımı gerçekleştiremez. Böyle bir senaryoda A düğümü gibi kendisi saldırgan kapsama alanında olmasa da veri akış yönüne göre bir sonraki komşusu saldırgan kapsama alanında olan sınır düğümlerin PTO değerleri komşu düğümden ACK paketi alamadığı için düşmektedir. Ancak doğrudan saldırılardan etkilenmediği için hatalı paket oranları (HPO) düşük çıkmaktadır. Diğer bir senaryoda ise B ve C düğümlerinin reaktif, rasgele, kesme,

aktivite, tarama, darbe, veri paketi ve küme saldırganları gibi iletişim kanalını sürekli meşgul etmeyen saldırganların etkisinde olduğu varsayıldığında A düğümünün HPO değerleri yüksek çıkmayacağı gibi PTO değerleri de düşük çıkmayacaktır. Bunun sebebi, B düğümünün saldırgan kapsama alanının sınırlarında bulunması ve bu saldırgan modellerinin B düğümünün A düğümüne ACK göndermesini engellememesidir.



Şekil 5.3. Farklı senaryolarda bir düğümden ölçülen minimum, maksimum ve ortalama hatalı paket oranları

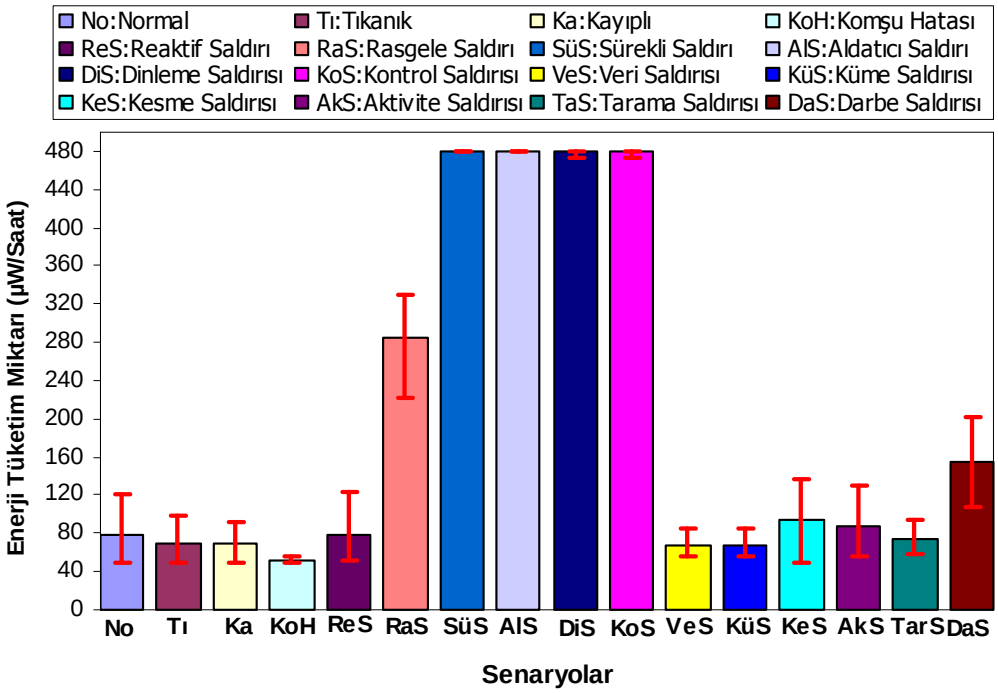
Şekil 5.3'te farklı senaryolarda bir düğümden ölçülen HPO değerleri görülmektedir. Çoğu saldırı durumunda hatalı paket oranlarının doğal ağ koşullarındakine oranla oldukça yüksek çıkması doğal şartlarla saldırı senaryolarını birbirinden ayrıştırmayı kolaylaştıracaktır. Ancak paket gönderilmesini engelleyen sürekli, dinleme ve kontrol aralığı saldırgan senaryoları ile komşu düğüm hata senaryolarında alınan geçerli bir öntakı ya da paket olmadığından hatalı paket oranları da sıfır seviyesindedir ve bu sebeple grafikte gösterilmemiştir. Bu gibi saldırı senaryolarında düşük HPO'nun ölçülmesi tüm saldırıları durumlarının doğal ağ şartlarından PTO ve HPO yardımıyla ayrılmasını zorlaştırmaktadır.

5.4.1.3. Enerji tüketim miktarı (ETM)

Bir düğümün belirli bir süre içerisinde yaklaşık olarak harcadığı enerji miktarıdır. ETM, bir düğümün radyosunun farklı evrelerde çalıştığı sürenin bilinmesi ile yaklaşık olarak hesaplanabilir. Bir MICA2 düğümün radyosu gönderim gücünün (0 dbm) değişmediği varsayıldığında gönderme, alma ve uyuma modlarında sırasıyla 16.5 mA, 9.6 mA ve 1 µA akım çekmektedir [86]. Yani 3V besleme gerilimi ile MICA2 düğümün radyosu gönderme modunda saatte 49.5 mW, alma modunda 28.86 mW ve uyuma modunda 3 µW güç harcamaktadır. Radyo evrelerinde kaldığı süre ile yukarıdaki değerler çarpılarak düğümün belli bir süre içersinde harcamış olduğu yaklaşık enerji miktarı hesaplanabilir.

Şekil 5.4'te farklı senaryolarda 3600 saniye boyunca ve 60 saniye aralıklarla bir düğümden ölçülen enerji tüketim miktarlarının minimum, maksimum ve ortalama değerleri görülmektedir. Tıkanıklık, kayıplı bağlantı, komşu düğüm hata ve bazı saldırı senaryolarında ölçülen ETM değerleri, normal senaryoda ölçülen ETM değerlerinden daha düşük çıkabilmektedir. Bunun sebebi düğümlerin bu senaryolarda normal senaryolara oranla daha az paket göndermeleri veya almalarından kaynaklanmaktadır. Ayrıca aldatıcı, sürekli, rasgele, dinleme ve kontrol aralığı saldırganları gibi bazı saldırı senaryolarında ise düğümlerin enerji tüketimleri doğal koşullara oranla önemli ölçüde yüksek çıkmaktadır. Aldatıcı saldırganın düğümleri sürekli alım modunda, sürekli, dinleme aralığı ve kontrol aralığı saldırganlarının ise dinleme modunda tutması bu sonucun ortaya çıkmasına neden olmaktadır. Sürekli, dinleme aralığı ve kontrol aralığı saldırganları iletişim kanalını sürekli meşgul ederek düğümlerin geriçekilme (BACKOFF) durumunda kalmasına sebep olmaktadır. S-MAC protokolünde bir düğüm BACKOFF durumundan ancak RTS, CTS, DATA, ACK ya da hatalı bir paket aldığında kurtulabildiği için düğümler uyuma zamanları gelmesine rağmen hiçbir paket alamadıkları için BACKOFF modundan kurtulamamakta ve dinlemede kalarak daha fazla enerji harcamaktadırlar. CC1000 alıcı/verici tüm devresinin aylak (IDLE) modunun olmaması nedeniyle de saldırı altındaki düğümler sürekli, dinleme aralığı ve kontrol aralığı saldırı senaryolarında aldatıcı saldırgana eş güç tüketmektedir. Rasgele, sürekli, aldatıcı, dinleme aralığı ve kontrol aralığı saldırgan senaryolarında düğümlerin normal koşullara oranla çok daha

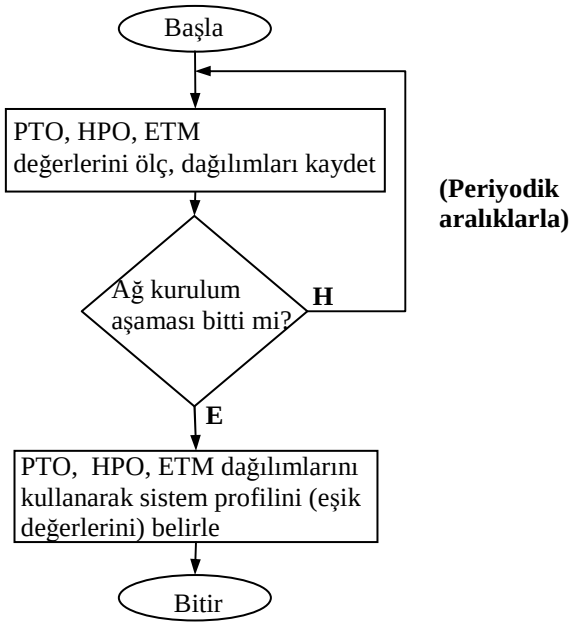
fazla güç tüketmesi sayesinde bu saldırganların doğal ağ koşullarından ayrılması mümkün olacaktır.



Şekil 5.4. Farklı senaryolarda bir düğümden ölçülen minimum, maksimum ve ortalama enerji tüketim miktarları

5.4.2. Anomalinin tespiti

Paket teslim oranı (PTO), hatalı paket oranı (HPO) ve enerji tüketim miktarı (ETM) olarak tanımladığımız sistem parametrelerinin saldırı durumlarından etkilenmesi anomali tespitinde bu parametrelerin kullanılmasını mümkün kılmaktadır. ABSTS içeren her düğüm normal koşullardaki sistem profilini belirlemek ve daha sonra şüpheli durumlarda elde edilen profil bilgileri ile kıyaslamak için PTO, HPO ve ETM parametrelerinden faydalanmaktadır. Düğümler ağ kurulum aşamasında yeterli bir süre boyunca PTO, HPO ve ETM parametrelerini periyodik zaman dilimlerinde ölçmekte ve daha sonra elde edilen bu veri dağılımları üzerinde bazı istatistiksel operatörler kullanılarak hangi durumların normal ya da anormal olduğunun belirlenmesini sağlayan eşik değerleri tespit etmektedirler. Şekil 5.5'te anomali tespitinde kullanılan eşik değerlerinin belirlenme aşaması görülmektedir.



Şekil 5.5. Anomali tespitinde kullanılan eşik değerlerinin elde edilmesi

Ağ kurulum aşamasında belirli süre boyunca toplanan PTO, HPO ve ETM dağılımlarında normal koşullar ile anormal koşulların ayrılmasına imkân sağlayan kritik değerlerin tespit edilebilmesi veri madenciliği yaklaşımları ile ilgili olup oldukça önemli ve karmaşık bir konudur. Veri madenciliği, toplanan veri gruplarından yarı otomatik olarak örneklerin elde edilmesi, kuralların belirlenmesi, değişikliklerin tespit edilmesi, verilerdeki olayların istatistiksel olarak keşfedilmesi olarak tanımlanmaktadır [81]. Günümüzde istatistik, yapay sinir ağları, gizli Markov modeli (Hidden Markov Model), vektör destek makineleri (Support Vector Machines), sinirsel bulanık (Neuro-Fuzzy) hesaplamalar, doğrusal genetik algoritmalar gibi çok çeşitli veri madencilik teknikleri sızma tespit sistemlerinde kullanılmaktadır. Fakat bu teknikler içerisinde en yaygın kullanıma sahip yöntem istatistiktir. İstatistik tekniğinin en büyük avantajı diğer yöntemlere oranla daha az hesap yükünün olmasıdır. Bu sebeple sınırlı donanımsal kaynaklara sahip olan algılayıcı düğümleri için daha elverişli bir yöntemdir.

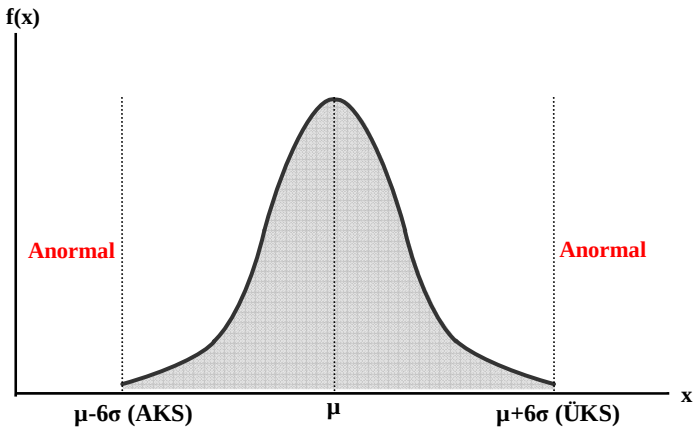
Önerilen ABSTS'de de normal koşulların belirlenmesinde istatistiksel yöntemlerden 6-Sigma (6σ) metodu kullanılmaktadır. Basit olmasına karşın etkili olan bu yöntemde normal olarak dağılan bir büyüklüğün ortalama ve standart sapma değerlerine göre üst kontrol sınırı (ÜKS) ve alt kontrol sınırı (AKS)

hesaplanabilmektedir. Formül 5.1 ve 5.2'deki μ, N adet verinin ortalama değeri, σ ise standart sapmasıdır. Normal dağılımda verilerin % 99,999660'ı ÜKS ile AKS değerleri arasındadır. Bu sebeple ÜKS'nin üstündeki veya AKS'nin altındaki bir değer Şekil 5.6'da görüldüğü gibi anormal olarak kabul edilebilir.

$$ÜKS = \mu + 6\sigma \quad (5.1)$$

$$AKS = \mu - 6\sigma \quad (5.2)$$

Paket teslim oranı için AKS, hatalı paket oranı ve enerji tüketim miktarı için ise ÜKS değerlerinin hesaplanması ile PTO, HPO ve ETM parametreleri için eşik değerleri tespiti edilmiş olur.



Şekil 5.6. PTO, HPO ve ETM parametreleri için eşik değerlerinin belirlenmesi

5.4.3. Temel boğma saldırı tespit yöntemi

Tablo 5.1'de temel saldırı tespit yöntemi görülmektedir. Düğümün ölçtüğü paket teslim oranlarının eşik değerlerinin altına düşmesi ve harcanan enerji miktarının eşik değerinden fazla olması sonucunda düğüm saldırı altında olduğunu karar vermektedir. Bunun dışında düğümün ölçtüğü PTO'nun eşiğin altında olması enerji tüketiminin normal, hatalı paket oranlarının ise fazla olması sonucunda yine saldırı altında olduğuna karar vermektedir. Ancak teslim oranları düşük olsa bile enerji tüketimi ve hatalı paket oranları normal durumdaysa düğüm komşularında bir hata meydana geldiğini tespit etmektedir.

Tablo 5.1. Temel saldırı tespit algoritması

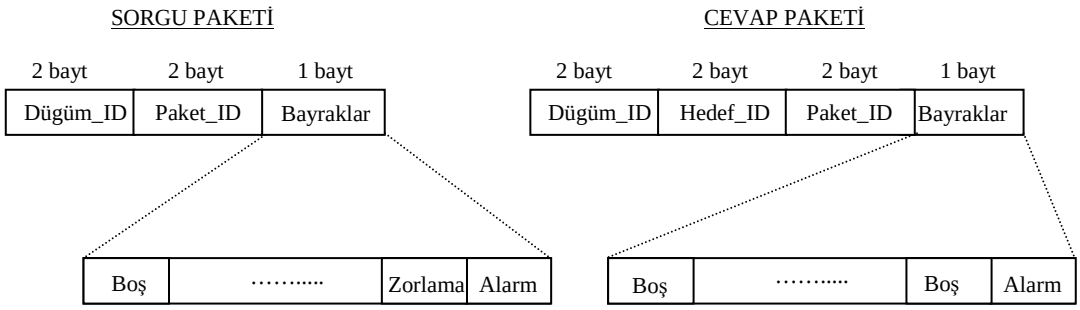
```
bool BOGMA,HATA=FALSE
/*Her örnekleme periyodunda çağrılır*/
TemelBogmaSezmeAlgoritmasi(){
  if (PTO<PTO_Eş and ETM_n>ETM_Eş and HPO_n>HPO_Eş)
     BOGMA=TRUE    // Aldatıcı,Rasgele,Darbe
  else if(PTO<PTO_Eş and ETM_n>ETM_Eş and HPO_n<HPO_Eş)
     BOGMA=TRUE    //Sürekli,Dinleme ve Kontrol Aralığı
  else if(PTO<PTO_Eş and ETM<ETM_Eş and HPO_n>HPO_Eş)
     BOGMA=TRUE   //Reaktif,Veri,Küme,Kesme,Darbe,
  else if(PTO_n<PTO_Eş and ETM_n<ETM_Eş and HPO_n<HPO_Eş)
     BOGMA=FALSE
     HATA=TRUE;
  else if (PTO_n>PTO_Eş)
    BOGMA=FALSE
  end if
}
```

Bu yöntemin başarılı bir şekilde senaryoları birbirinden ayırabilmesi eşik değerlerinin doğru bir şekilde belirlenebilmesine bağlıdır. Ağ içerisinde meydana gelebilecek ve önceden kestirilemeyen bazı doğal durumlar tek başına eşik mekanizmasının yetersiz kalmasına ve hatalı alarm durumlarının ya da sezilmeme durumlarının artmasına yol açmaktadır. Ayrıca Şekil 5.2'de görüldüğü gibi, A düğümüne benzere şekilde doğrudan saldırganın kapsama alanında olmadığı halde dolaylı yoldan saldırganın etkisinde olan düğümlerde (Sınır Düğümler) PTO değerleri düşmesine karşın ETM ve HPO değerleri normal seviyelerde kalabilmektedir. Komşusunda hata meydana gelen bir düğümde de benzer olarak PTO düşmekte, ETM ve HPO değerleri normal seviyelerde kalmaktadır. Dolayısıyla temel saldırı tespit metodunda sınır düğümlerdeki saldırı durumları ile HATA durumları birbirine karışabilmekte ve bu da hatalı alarm oranlarının yükselmesine ya da sezme oranlarının düşmesine neden olmaktadır.

5.4.4. Gelişmiş boğma saldırı tespit sistemi

Temel saldırı tespit yönteminin bazı doğal ağ koşullarından negatif yönde etkilenmesi ve sınır düğümlerinde saldırı tespitinde yetersiz kalması ortam koşullarına daha dayanıklı ve başarımı daha yüksek bir yöntem geliştirilmesini

zorunlu kılmaktadır. Bu sebeple temel saldırı tespit metodunda kullanılan eşik mekanizmasının bir başka ek mekanizma ile desteklenmesi gerekmektedir. Gelişmiş saldırı tespit yönteminde eşik mekanizmasının dezavantajlarını en aza indirmek üzere düğümlerin birbirlerinden faydalanarak saldırı kararını vermesini sağlayan sorgulama tabanlı saldırı tespit yöntemi geliştirilmiştir. Yöntemin esası; PTO, HPO ve ETM parametrelerine göre saldırı altında olduğundan şüphe eden düğümün komşu düğümlere gönderdiği SORGU (QUERY) paketi ve buna karşılık komşulardan gelecek CEVAP (REPLY) paketlerine dayanmaktadır. Düğümler Şekil 5.7'de görüldüğü gibi SORGU paketlerinde bulunan ALARM bayrağını kurarak kendisinin saldırı altında olma ihtimalinin yüksek olduğunu ve karar vermek için komşularının bilgilerinden faydalanacağını bildiren SORGU paketini gönderir. SORGU paketi alan düğümler ise PTO, HPO ve ETM değerlerine bakarlar. ($PTO<PTO_{Eş}$ ve $ETM>ETM_{Eş}$) ya da ($PTO<PTO_{Eş}$ ve $HPO>HPO_{Eş}$) şartlarının gerçekleşmesi durumunda CEVAP paketindeki ALARM bayrağını 1'e kurarak aksi durumda ise sıfırlayarak geri gönderirler. Ancak sürekli ve aldatıcı saldırgan gibi iletişim kanalını kesintisiz meşgul eden saldırganlar SORGU-CEVAP paketlerinin gönderimini de engellemektedir. Reaktif saldırgan gibi bazıları ise gönderilen sorgu paketlerin bozulmasına neden olmakta, veri paketi saldırganı gibi saldırganlar ise SORGU-CEVAP paketlerine saldırmamaktadır.



Şekil 5.7. SORGU ve CEVAP paketlerinin yapısı

Tablo 5.2'de gelişmiş sorgu tabanlı saldırı tespit yöntemi görülmektedir. `SorguTabanliSaldiriTespitAlgoritmasi` fonksiyonu her örnekleme periyodunda çağrılmaktadır ve bu fonksiyon harici bazı parametreleri de kullanarak koşul yapıları yardımıyla saldırı tespitini gerçekleştirmektedir. Fonksiyon, geçerli

PTO'nun eşikten küçük ve ETM'nin eşik değerinden fazla olması ya da PTO'nun eşikten küçük ve HPO'nun eşikten fazla olması gibi anormal bir durumda, anomalinin saldırılar sebebiyle ortaya çıktığından emin olmak için SORGU sürecini başlatmaktadır. Ancak gereksiz paket gönderimini engellemek üzere SORGU paketi göndermeye karar veren düğüm, gönderim yapmadan önce bir komşusundan SORGU paketi alıp almadığını kontrol etmektedir. Eğer bir SORGU paketi kendisine ulaştıysa SORGU göndermek yerine var olan SORGU/CEVAP trafiğinin bitmesini ve belirlenen zaman aşımının dolması beklemektedir. Düğüm eğer tüm komşularından CEVAP paketi aldı ise kendisine ulaşan CEVAP paketlerine göre saldırı kararını vermekte ve böylece gereksiz yere paket gönderiminin ve alımının önüne geçilmektedir. Düğüm SORGU göndermeden önce herhangi bir SORGU paketi almadıysa çekişme kurallarına da uyarak iki örnekleme periyodu içerisinde SORGU paketini göndermeye çalışmaktadır. Düğüm eğer bu süre zarfında SORGU paketi gönderemez ise sürekli veya aldatıcı saldırgan gibi kanalı meşgul eden bir saldırıya maruz kaldığına karar vermektedir. Belirlenen zaman dilimi içerisinde SORGU paketini gönderebilen bir düğüm CEVAP paketlerini beklemeye başlar ve CEVAP paketleri için belirlenen sürenin dolması ile kendisine gelen CEVAP paketlerini değerlendir.

Düğüm;

1. Hiç CEVAP paketi almadıysa
2. Aldığı CEVAP paket sayısı komşu sayısına oranla daha az ise VE sonraki atlama komşusundan CEVAP paketi gelmediyse
3. Aldığı CEVAP paket sayısı komşu sayısına oranla daha az VEYA eşit ise VE bir sonraki atlama komşusundan alınan CEVAP paketindeki Alarm bayrağı kurulu ise saldırı altında olduğuna karar vermektedir.

Doğrudan bir saldırgan etkisinde olan düğümler için yukarıdaki kurallara göre saldırı tespiti gerçekleştirilirken sınır düğümler için farklı kurallar gerekmektedir. Sınır düğümlerin sürekli, dinleme aralığı ve kontrol aralığı saldırıları altında PTO değerlerinin düşmesi, bu düğümler için saldırı tespitinin gerçekleştirilmesini zorunlu kılmaktadır. Ancak PTO düşmesine rağmen HPO ve ETM parametrelerinin saldırılardan etkilenmemesi, sınır düğümler için saldırı durumları ile komşu düğüm

hata durumlarının karışmasına yol açabilmektedir. Önerilen ileri saldırı tespit yönteminde bu sorunu aşmak için ZORLAMA SORGU paketlerinden faydalanılmaktadır. İletişim kanalını sürekli meşgul eden saldırıların etkisi altındaki düğümler normal şartlarda herhangi bir paket gönderememektedir. Ancak bu düğümler, sınır düğümlerin saldırı tespitini kolaylaştırmak için çekişme kurallarına aldırmadan rasgele süre bekleyerek ZORLAMA SORGU paketi göndermektedir. Saldırgan kapsama alanın sınırlarında bulunan düğümler sayesinde ZORLAMA SORGU paketleri sınır düğümlere ulaşabilmekte ve böylece sınır düğümlerinde saldırı durumları ile hata durumlarının ayrımı gerçekleştirilebilmektedir

Tablo 5.2. Gelişmiş boğma saldırı tespiti yöntemi

```
/*Her örnekleme periyodunda çağrılır*/
SorguTabanliSaldiriTespitAlgoritmasi(
{
  if ((PTO<PTO_Eş  AND ETM>ETM_Eş) OR (PTO<PTO_Eş  AND HPO>HPO_Eş))
    if(SorguAlindi=TRUE and  DigerleriİcinCevapBekleniyor=FALSE)
       CevapTimeriniKur(Simdi+2*OrneklemePeriyodu)
       DigerleriİcinCevapBekleniyor=TRUE
    else if ( DigerleriİcinCevapBekleniyor=TRUE  AND SorguTimerTasti=TRUE)
      if (CevapPaketSayisi=KomsuSayisi)
          CevapPaketleriniAnalizEt()
      else SorguAlindi=FALSE
      end if
    else if(SorguAlindi=FALSE)
      if (SorguSureciBasladi=FALSE)
          SorguGondermeyiDene()
          SorguTimeriniKur(Simdi+2*OrneklemePeriyodu)
          SorguSureciBasladi=TRUE
      else if(SorguTimeriTasti=FALSE AND SorguGonderildi=TRUE)
         SorguTimeriniDurdur()
         CevapTimeriniKur(Simdi+2*OrneklemePeriyodu)
      else if (SorguTimeriTasti=TRUE  AND SorguGonderildi=FALSE)
         BOGMA=TRUE;
         if(ZorlamaSorguSayisi<3)
            ZorlamaSorguGonder(Simdi+RasgeleZaman)
            ZorlamaSorguGonderildi=TRUE
           ZorlamaSorguSayisi++
         end if
      else if(CevapTimeriTasti=TRUE)
          CevapPaketleriniAnalizEt ();
      end if;
    end if;
    /*Sınır düğümlerde saldırı tespiti için geçerli şartlar */
  else if (PTO<PTO_Eş  AND HPO<HPO_Eş  AND ETM_n<ETM_Eş AND ZorlamaSorguAlindi=TRUE)
     BOGMA=TRUE;
  else if (PTO<PTO_Eş  AND HPO<HPO_Eş  AND ETM<ETM_Eş)
     HATA=TRUE;
  else
     BOGMA=FALSE;
  end if
}
```

5.5. Geliştirilen Saldırı Tespit Sisteminin Başarım Analizi

Geliştirilen ABSTS'nin başarım analizi, detayları EK.B'de verilen OMNET++ tabanlı benzetim yazılımı ile gerçekleştirilmiştir. İletişim mesafesi *r* olan, N=100 adet normal düğüm, uzunluğu ℓ olan bir kare alana, formül 5.3 yardımıyla istenilen düğüm yoğunluğuna (*Y*) göre [6] rasgele olarak dağıtılmıştır. Bir adet çıkış (sink) düğümü ise merkeze yerleştirilmiştir.

$$Y = \sqrt{\frac{N.\pi}{\ell} r} \tag{5.3}$$

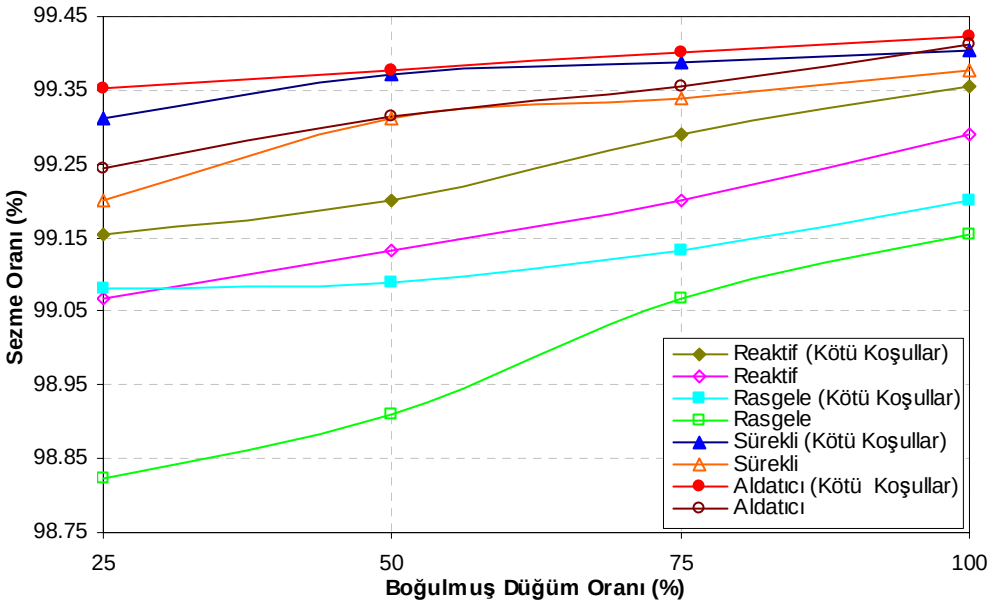
Saldırı tespit yönteminin farklı koşullardaki performansını ölçmek için %25, %50, %75 ve %100 olmak üzere boğma saldırılarına maruz düğüm oranları ile benzetimler gerçekleştirilmiştir. Normal düğümler ile saldırgan düğümlerin güç kapasiteleri, güç tüketimleri, radyo iletim mesafeleri MICA2 [80] düğümüne uygun olarak seçilmiştir. MAC katmanında, S-MAC [27] protokolü kullanılmış ve dinleme süresi 100 msn, uyuma süresi 900 msn olarak (%10 duty cycle) ayarlanmıştır. Tüm benzetimlerde kablosuz algılayıcı ağının proaktif yapıda olduğu varsayılmış ve paket üretimi, normal trafik için 1 paket / 5 saniye, yüksek trafik oranı için ise 2 paket / saniye olarak seçilmiştir. Hata durumlarını incelemek için toplam düğüm sayısının % 25'i oranında rasgele seçilen düğümler rasgele anlarda bozulmakta ve iletişim yapamaz hale gelmektedir. İletim kanalındaki kayıpları benzetebilmek için Gilbert-Elliott modeli olarak adlandırılan iki durumlu ayrık Markov zinciri kullanılmıştır [88]. Tüm benzetimlerde paket teslim, hatalı paket oranları ve enerji tüketim miktarı sabit periyotlarla ölçülerek elde edilmektedir. Örnekleme periyodu olarak 30 saniye değeri seçilmiştir. Bu sürenin kısa olmasının en büyük avantajı saldırıların çabuk bir şekilde tespitine olanak sağmasıdır. Fakat özellikle trafik yoğunluğu düşük olan ağlarda kısa örnekleme süresi hatalı sezme oranlarının önemli ölçüde artmasına yol açabilir. Bunun yanında uzun örnekleme periyodu ise hatalı sezme riskini azaltırken saldırı tespit süresinin uzamasına sebep olabilmektedir.

Her bir benzetim için ilk olarak rasgele bir ağ topolojisi oluşturulmuş ve eşik değerlerinin tespiti için saldırı yokken 36000 saniye boyunca ağın normal durum

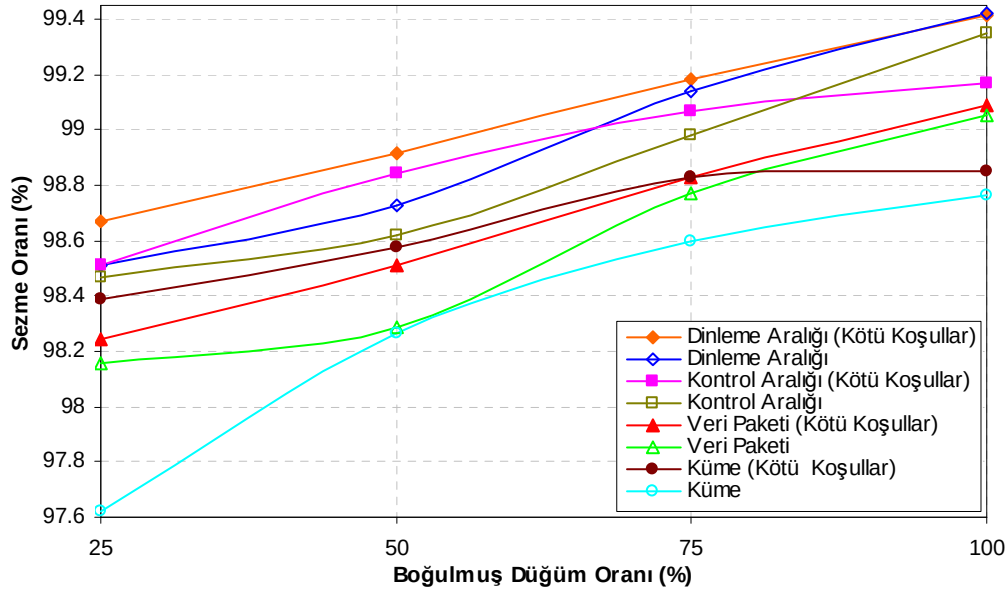
davranışları elde edilmiştir. Eşik değerleri elde edildikten sonra farklı saldırgan modellerini incelemek üzere 36000 saniye daha benzetim devam etmiştir. Bu şekilde her bir benzetim en az beş farklı topoloji ile tekrar edilmiştir ve elde edilen sonuçların ortalaması sunulmuştur. Geliştirilen saldırı tespit yöntemin başarım analizinde sezme oranları, hatalı sezme oranları, iletişim fazlalığı ve enerji tüketim fazlalığı parametrelerinden faydalanılmıştır.

5.5.1. Sezme oranları

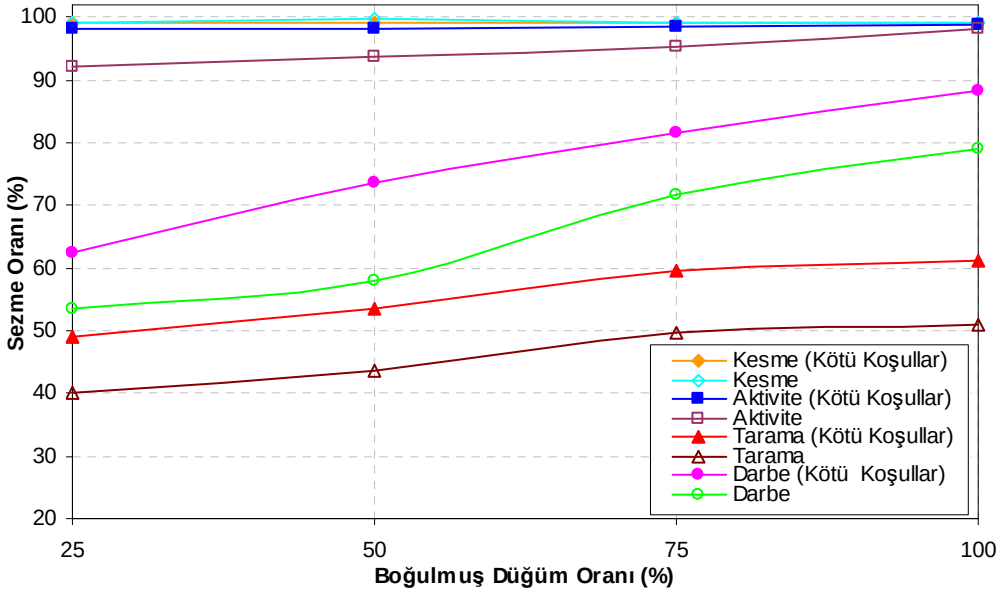
Geliştirilen ileri saldırı tespit yönteminin farklı ağ koşullarındaki sezme oranları Şekil 5.8, 5.9 ve 5.10'da görülmektedir. Şekillerde dikkat edilecek hususlardan birincisi sezme oranlarının oldukça yüksek olmasına karşın %100 seviyesine ulaşamamasıdır. Bunun sebebi sorgulama sırasında iki ila dört örnekleme periyodu boyunca saldırı tespit işlemi gerçekleştirilememesidir. Şekillerdeki ikinci önemli nokta ise saldırganlar tarafından etkilenen düğüm oranı arttıkça saldırı tespit oranlarının yükselmesidir. Bunun sebebi ise saldırı tespitinde kullanılan ağ parametrelerinin saldırılardan daha fazla etkilenmesi ve sınır düğüm sayısının azalmasıdır. Şekillerdeki bir diğer önemli husus da kötü bağlantı koşullarında (kayıplı bağlantı, tıkanık ve hatalı düğümler senaryolarında) normal koşullara oranla daha yüksek sezme oranlarının gerçekleştirildiğidir. Bunun sebebi ise kayıplı bağlantı sonucunda SORGU/CEVAP paketlerinin bozulma oranının daha da artmasıdır. Tarama ve darbe saldırgan senaryolarının tespit değerleri diğer saldırganlar kadar yüksek değildir. Bu iki saldırganın diğer saldırganlar kadar etkin olmaması ve ağa yeterince zarar verememesi sezilme ihtimalini de azaltmaktadır.



Şekil 5.8. Reaktif, rasgele, sürekli ve aldatıcı saldırganlar için farklı şartlardaki sezme oranları.



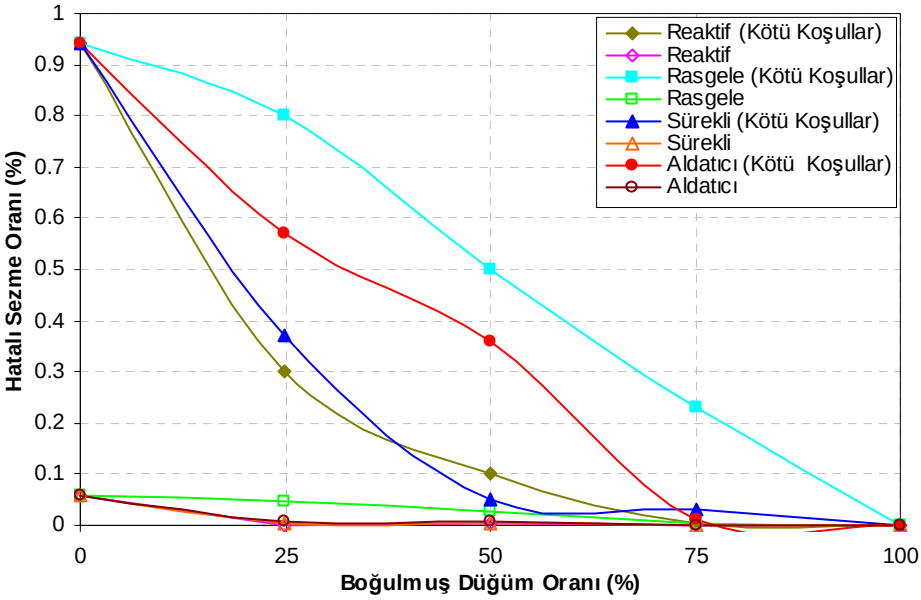
Şekil 5.9. Dinleme, kontrol aralığı, veri paketi ve küme saldırganları sezme oranları



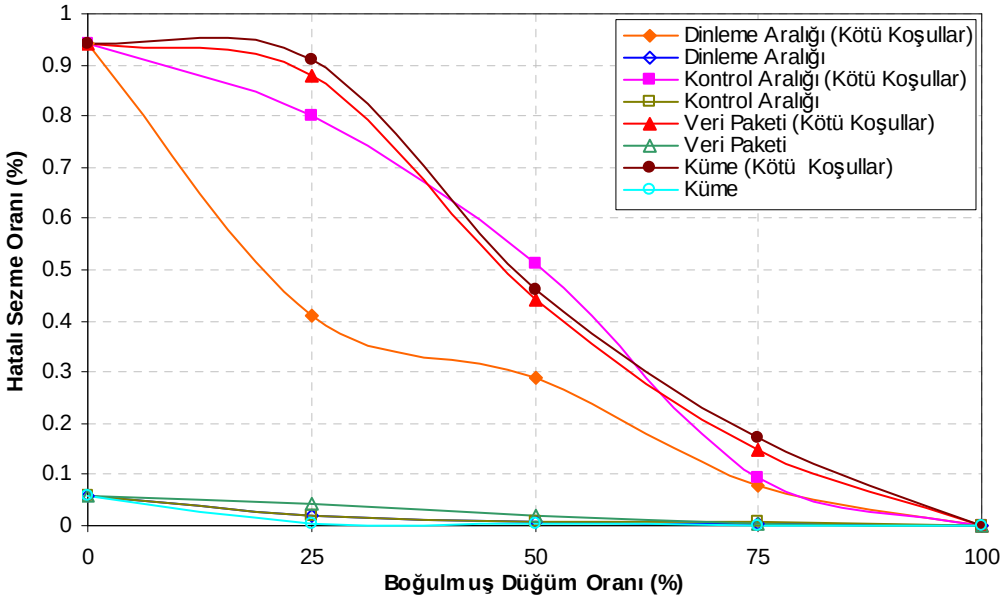
Şekil 5.10. Kesme, aktivite, tarama ve darbe saldırganları için farklı şartlardaki sezme oranları

5.5.2. Hatalı sezme oranları

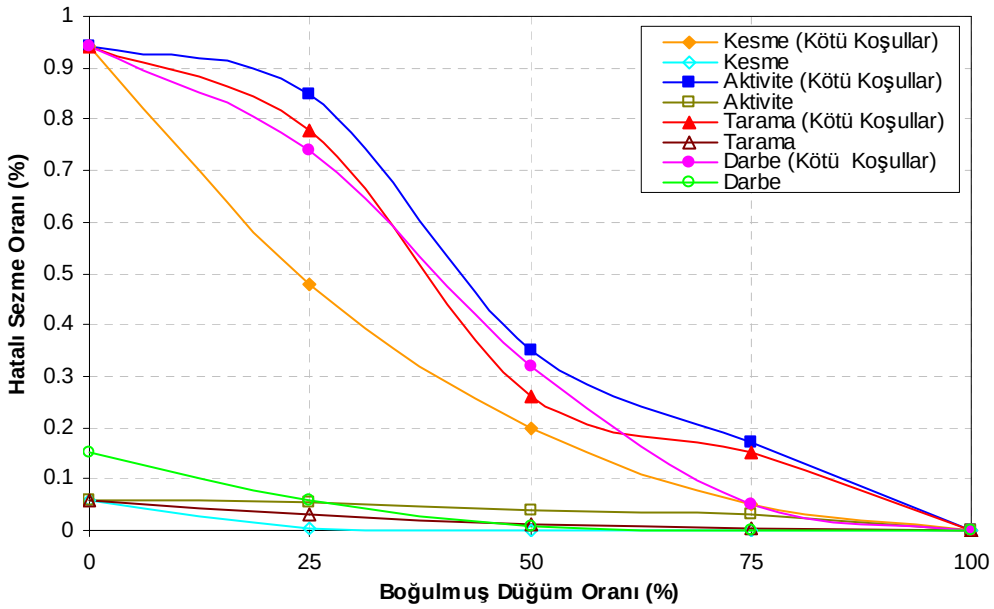
Geliştirilen ileri saldırı tespit yönteminin tüm saldırganlar için farklı koşullardaki hatalı sezme oranları Şekil 5.11, 5.12 ve 5.13'te görülmektedir. Hatalı sezme oranlarında dikkat edilecek hususlardan birincisi kötü bağlantı koşullarında normal koşullara oranla daha yüksek hatalı sezme oranının gerçekleştiğidir. Bunun sebebi, kayıplı bağlantı yüzünden PTO değerlerinin düşmesi, HPO değerlerinin de yükselmesidir. Ayrıca ağ içerisinde hatalı düğümlerin bulunması, hatalı sezme oranlarının artmasına neden olmaktadır. Bir diğer önemli husus da, saldırıya maruz kalan düğüm oranı arttıkça hatalı sezme oranının düşmesidir. Saldırganlar tarafından doğrudan etkilenen düğüm sayısı arttıkça hatalı sezme tespitinde bulunan düğüm sayısı da azalmaktadır. Boğulmuş düğüm oranının (BDO) "0" olması aslında ağda hiç saldırgan bulunmaması anlamına gelmektedir. Bu sebeple, üç grafikte de BDO'nun "0" olduğu durumlardaki hatalı sezme oranları aynıdır. BDO'nun "0"dışındaki değerlerinde ölçülen hatalı sezme oranları saldırganlar tarafından kapsanmayan düğümlerin hatalı olarak gerçekleştirdiği saldırı tespit değerleridir.



Şekil 5.11. Reaktif, rasgele, sürekli, aldatıcı saldırganlar için hatalı sezme oranları



Şekil 5.12. Dinleme, kontrol aralığı, veri paketi ve küme saldırganları için hatalı sezme oranları

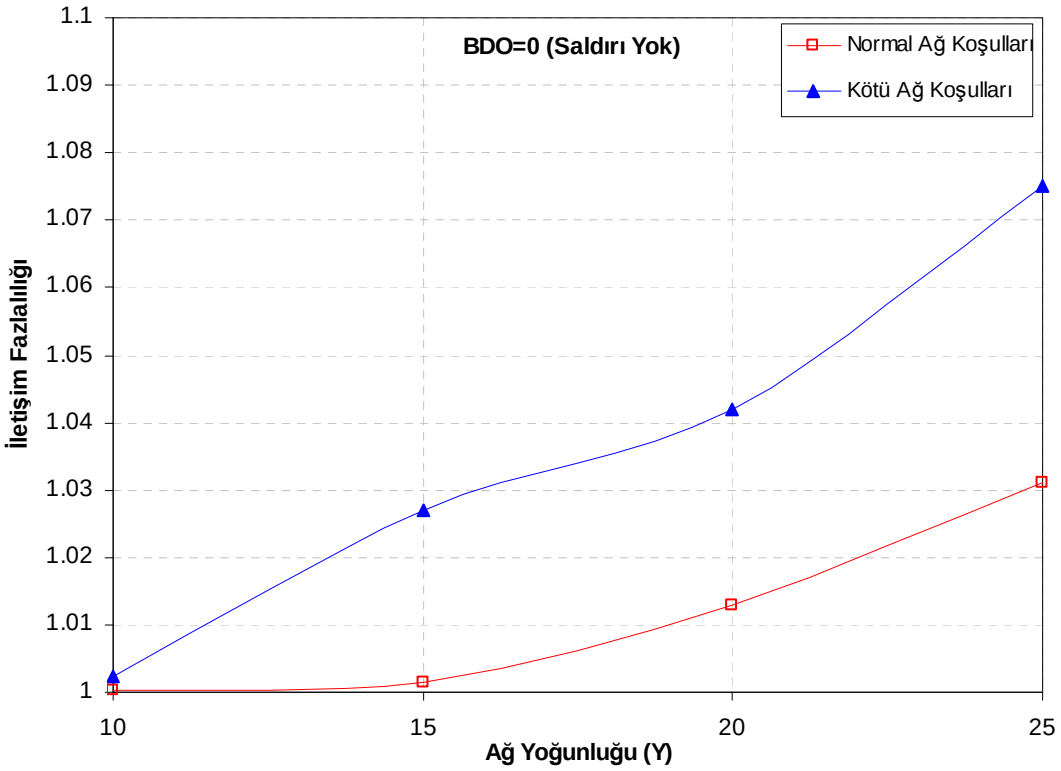


Şekil 5.13. Kesme, aktivite, tarama ve darbe saldırganları için hatalı sezme oranları

5.5.3. İletişim fazlalığı

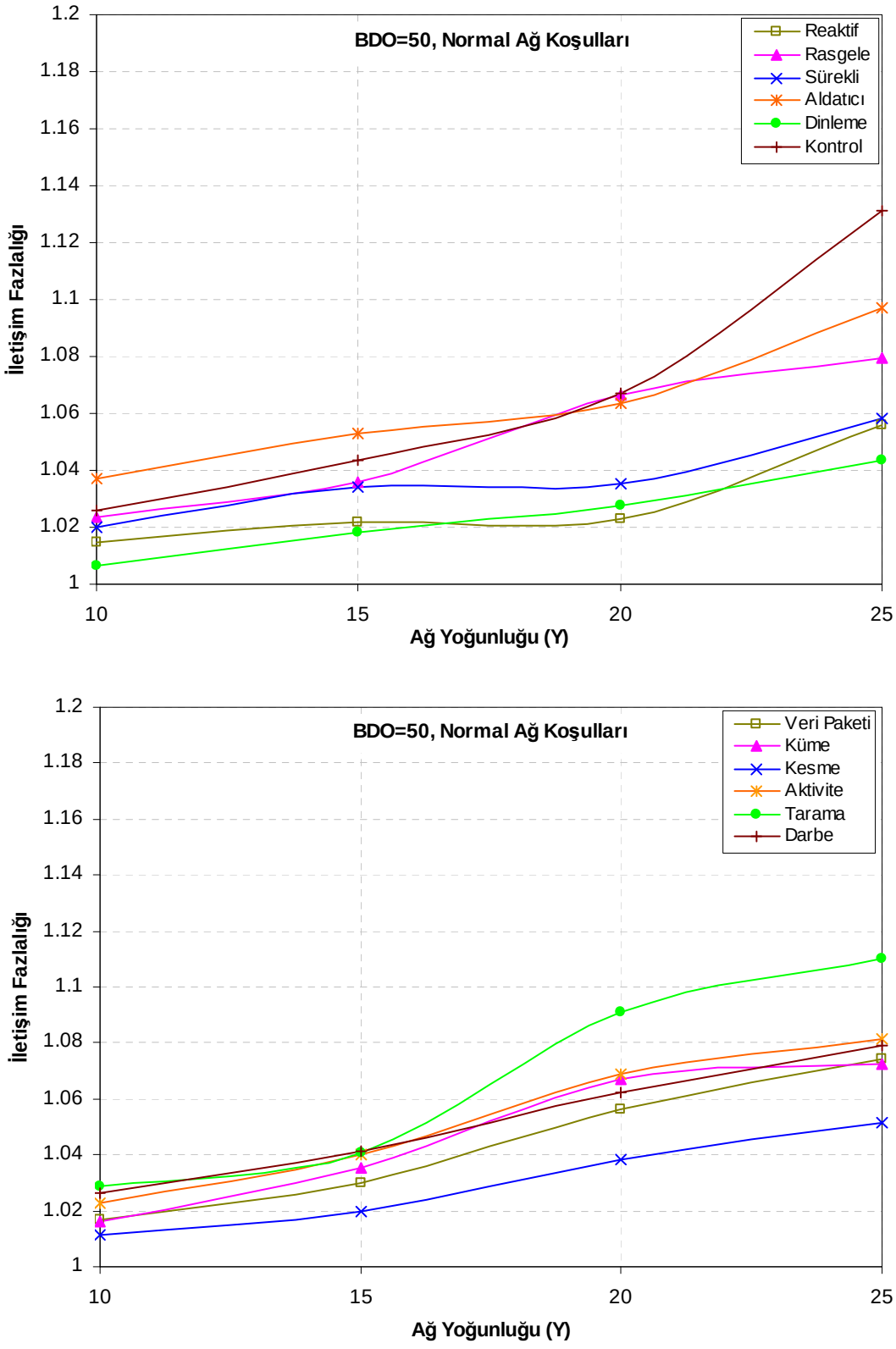
Geliştirilen ileri saldırı tespit yönteminde düğümlerin saldırı tespitini SORGU/CEVAP paketleri yardımıyla gerçekleştirmesi ağ içerisinde fazladan paket trafiğine sebep olmaktadır. Gönderilen ve alınan SORGU/CEVAP paket sayıları ise düğümlerin komşu sayısı (ağdaki düğüm yoğunluğu), saldırgan türü, saldırıdan etkilenen düğüm oranı ve doğal ağ koşulları ile yakından ilgilidir. Bu sebeple önerilen yöntemin meydana getirdiği iletişim yükünü incelemek üzere farklı düğüm yoğunluklarında ve farklı boğulmuş saldırgan oranlarındaki iletişim fazlalıkları sunulmaktadır. Şekil 5.14'te saldırının olmadığı (BDO=0) normal ve kötü ağ koşullarında düğüm başına düşen ortalama iletişim fazlalıkları görülmektedir. Şekilden ağ yoğunluğunun artması ile iletişim fazlalıklarının da arttığı gözlemlenmektedir. Ağ yoğunluğunun artması düğüm başına düşen komşu sayısının artmasına yol açmakta ve daha fazla SORGU/CEVAP paketi değişimine neden olmaktadır. Bu sebeple ağ yoğunluğu arttıkça iletişim yükü de artmaktadır. Diğer bir önemli husus da kötü ağ koşullarında elde edilen iletişim fazlalık değerlerinin normal ağ koşullarındakinden daha yüksek olduğudur. Bunun sebebi kötü bağlantı koşulları yüzünden düğümlerin çok daha fazla paketinin bozulması ve böylece PTO ve HPO değerlerinin negatif yönde etkilenerek düğümlerin daha sık SORGU/CEVAP paketi

gönderilmesidir. Geliştirilen ileri saldırı tespit yönteminin herhangi bir saldırının olmadığı durumda düğüm iletişimlerine getirdiği ek yük en fazla %7,5 civarındadır.

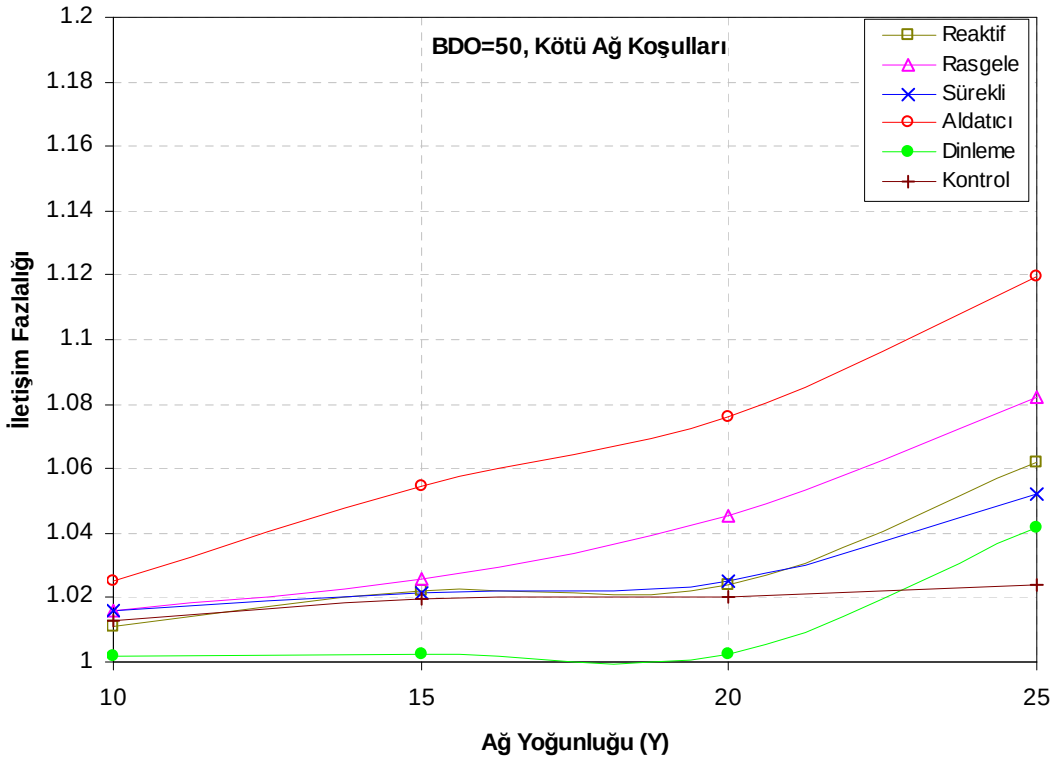


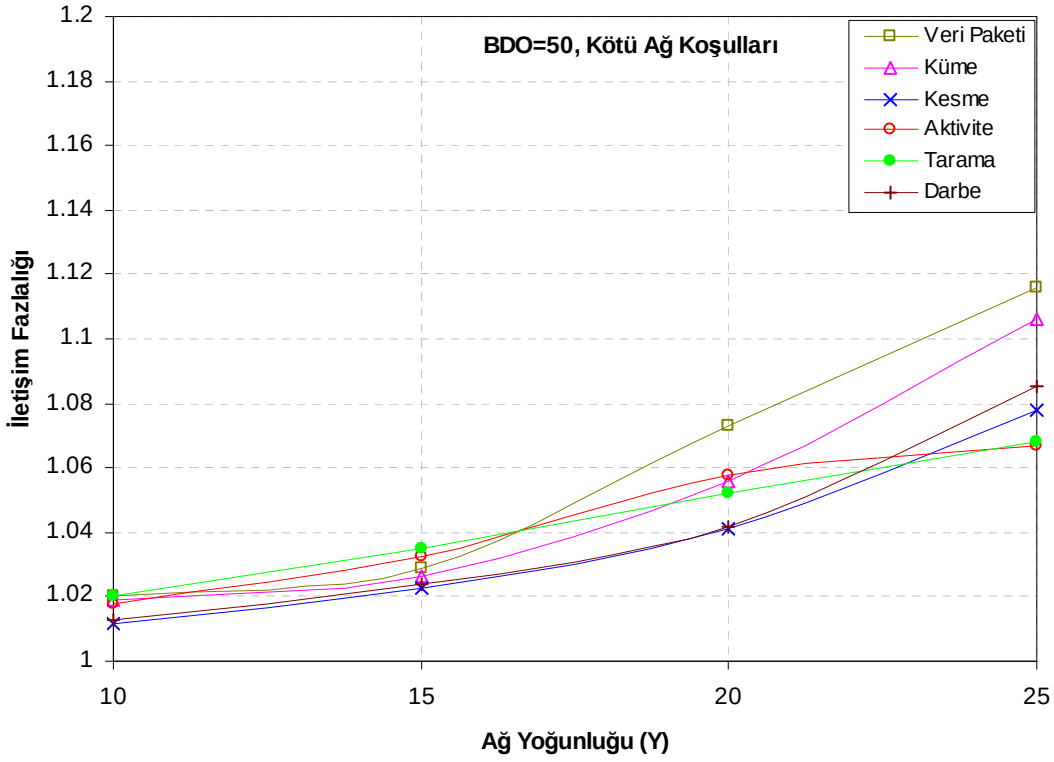
Şekil 5.14. Saldırının olmadığı farklı ağ koşullarında elde edilen iletişim fazlalıkları

Şekil 5.15'te normal ağ koşularında, Şekil 5.16'da ise kötü ağ koşularında ve %50 boğulmuş düğüm oranlarında düğüm başına düşen ortalama iletişim fazlalık değerleri görülmektedir. Saldırının olmadığı durumlara benzer olarak ağ yoğunluğu arttıkça iletişim fazlalığı artmaktadır. Bir ağdaki düğümlerin yarısının saldırganlar tarafından etkilenmesi durumunda geliştirilen ileri saldırı tespit yönteminin düğüm iletişimlerine getirdiği ek yük en fazla %12 oranındadır.



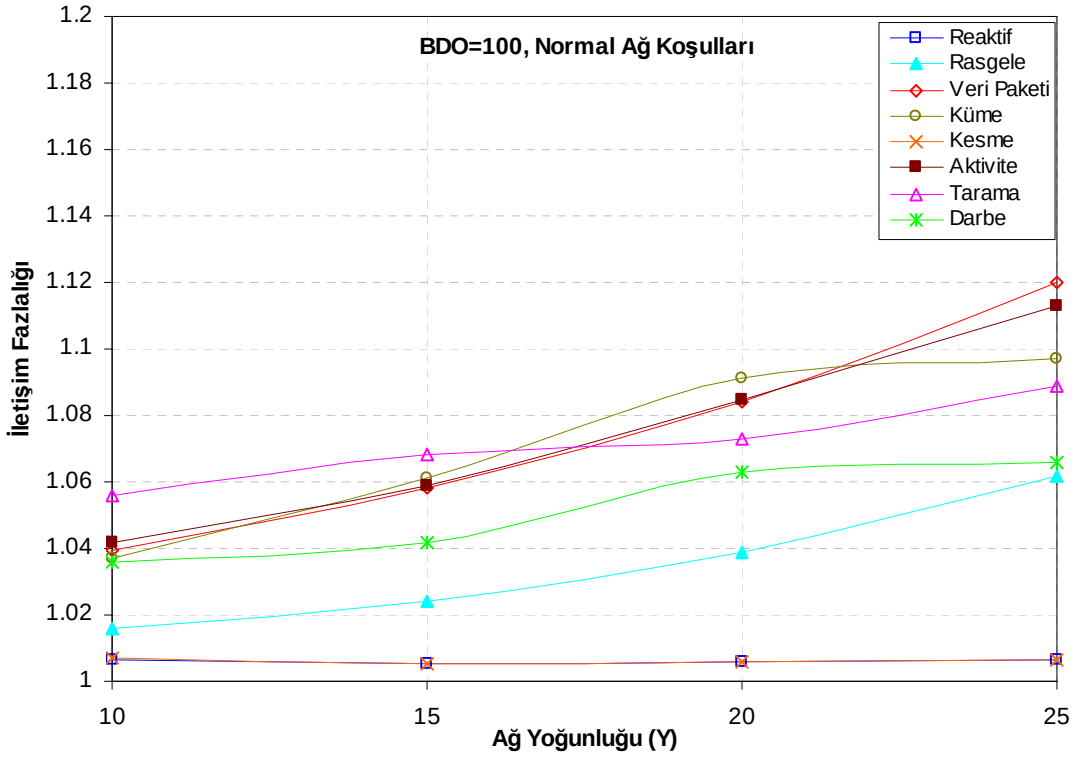
Şekil 5.15. Normal ağ koşullarında ve %50 boğulmuş düğüm oranında elde edilen iletişim fazlalıkları



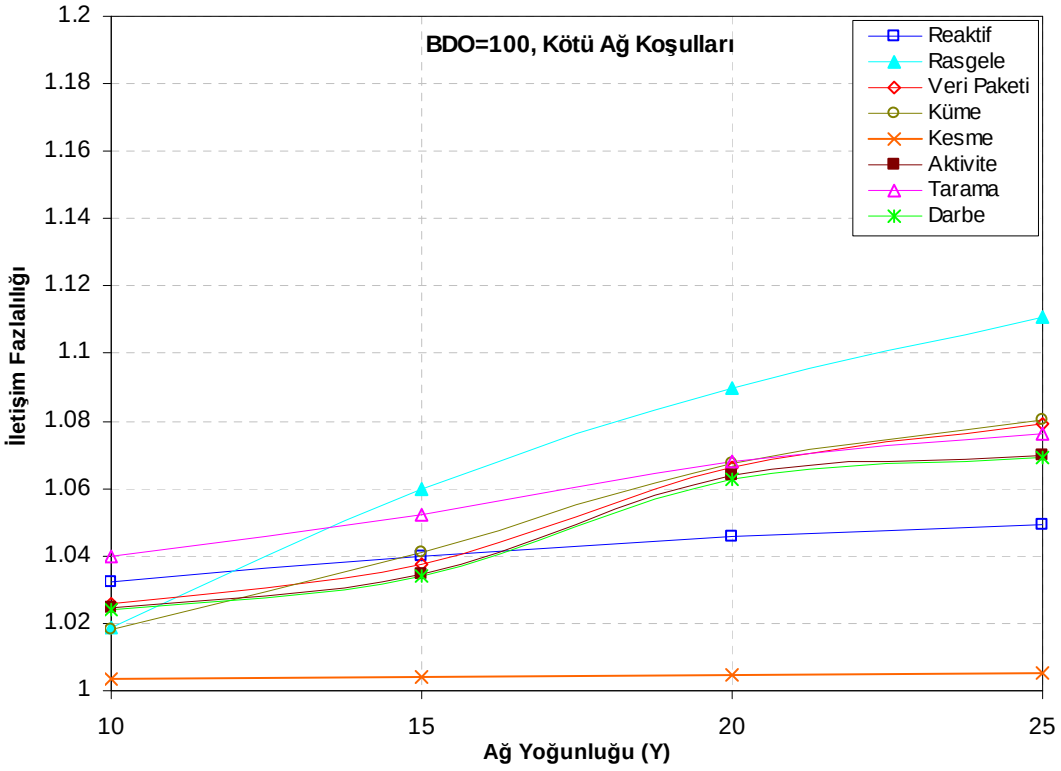


Şekil 5.16. Kötü ağ koşullarında ve %50 boğulmuş düğüm oranında elde edilen iletişim fazlalıkları

Şekil 5.17 ve Şekil 5.18'de Normal/kötü ağ koşullarında ve %100 boğulmuş düğüm oranında düğüm başına düşen ortalama iletişim fazlalık değerleri görülmektedir. Şekillerde sürekli, aldatıcı, dinleme aralığı ve kontrol aralığı saldırı senaryolarında düğüm başına elde edilen iletişim fazlalık değerleri bulunmamaktadır. Bu saldırı senaryolarında iletişim kanalının sürekli meşgul olması ve tüm düğümlerin bu saldırılardan etkilenmesi (BDO=100) sebebiyle hiçbir paket gönderilememektedir. Dolayısıyla düğüm başına gönderilen ya da alınan paket ortalaması '0' çıkmakta, iletişim fazlalık miktarı ise tanımsız olmaktadır. Şekillerdeki bir diğer önemli husus ise boğulmuş düğüm oranının %50'den %100'e çıkması ile düğüm başına düşen iletişim fazlalık değerlerinde küçükte olsa bir azalmanın gözlemlenmesidir. Bunun sebebi ise saldırılar tarafından etkilenen düğüm sayısının artması ile SORGU/CEVAP paketlerinin bozulma oranlarını yükselmesi ve bunun neticesinde daha az paket gönderimi ve alımının gerçekleşmesidir. Bir ağdaki düğümlerin tamamının boğma saldırılarına maruz kalması durumunda geliştirilen ileri saldırı tespit yönteminin sistem iletişimine getirdiği ek yük en fazla %11 civarındadır.



Şekil 5.17. Normal ağ koşullarında ve %100 boğulmuş düğüm oranında elde edilen iletişim fazlalıkları



Şekil 5.18. Kötü ağ koşullarında ve %100 boğulmuş düğüm oranında elde edilen iletişim fazlalıkları

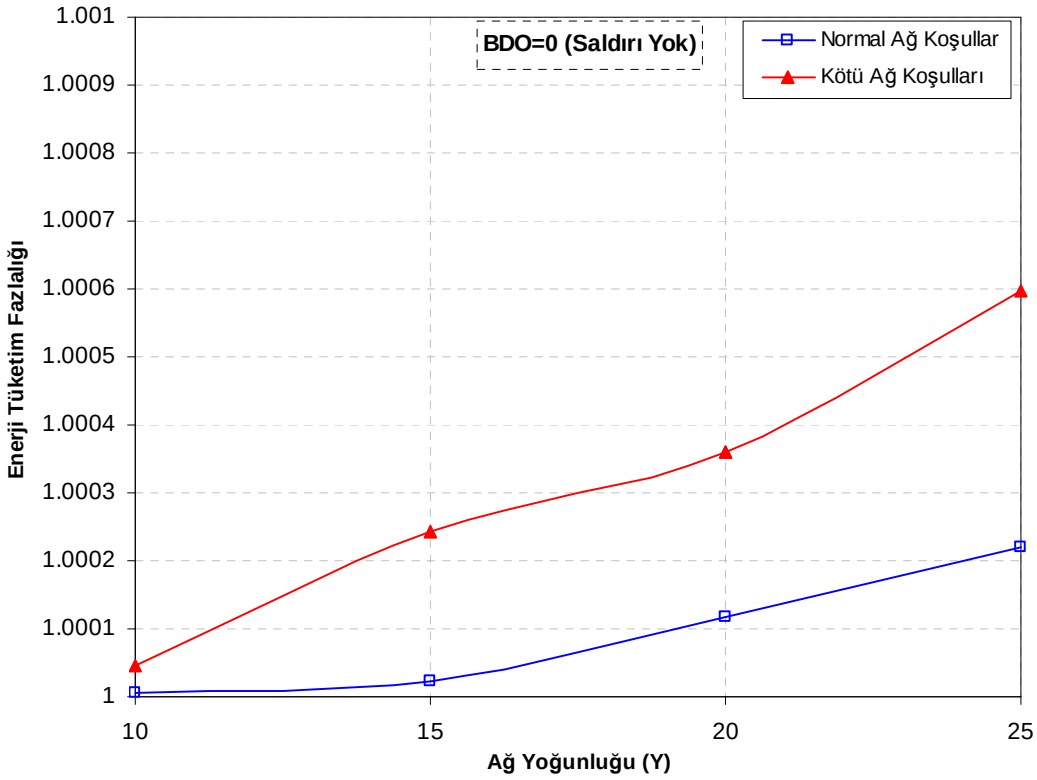
Geliştirilen ileri saldırı tespit yönteminin gerçekleştirilen detaylı benzetim sonuçlarına göre farklı ağ koşullarında ve saldırı durumlarında ağa iletişimine getirdiği ek yük en fazla %12 civarında çıkmaktadır.

5.5.4. Enerji tüketim fazlalığı (ETF)

Geliştirilen ileri saldırı tespit yönteminde düğümlerin saldırı tespitini SORGU/CEVAP paketleri yardımıyla gerçekleştirmesi ağ içerisinde fazladan paket trafiğine ve ekstra güç tüketimine neden olmaktadır. Önerilen ileri saldırı tespit yönteminin düğümlerin güç tüketimine getirdiği ek yük, SORGU/CEVAP yöntemi varken harcanan güç (G^{l}) ve SORGU/CEVAP yöntemi yokken harcanan güç (G) değerleri kullanılarak Formül 5.4 yardımıyla hesaplanmıştır.

$$ETF = 100x\frac{G^{l}}{G} \tag{5.4}$$

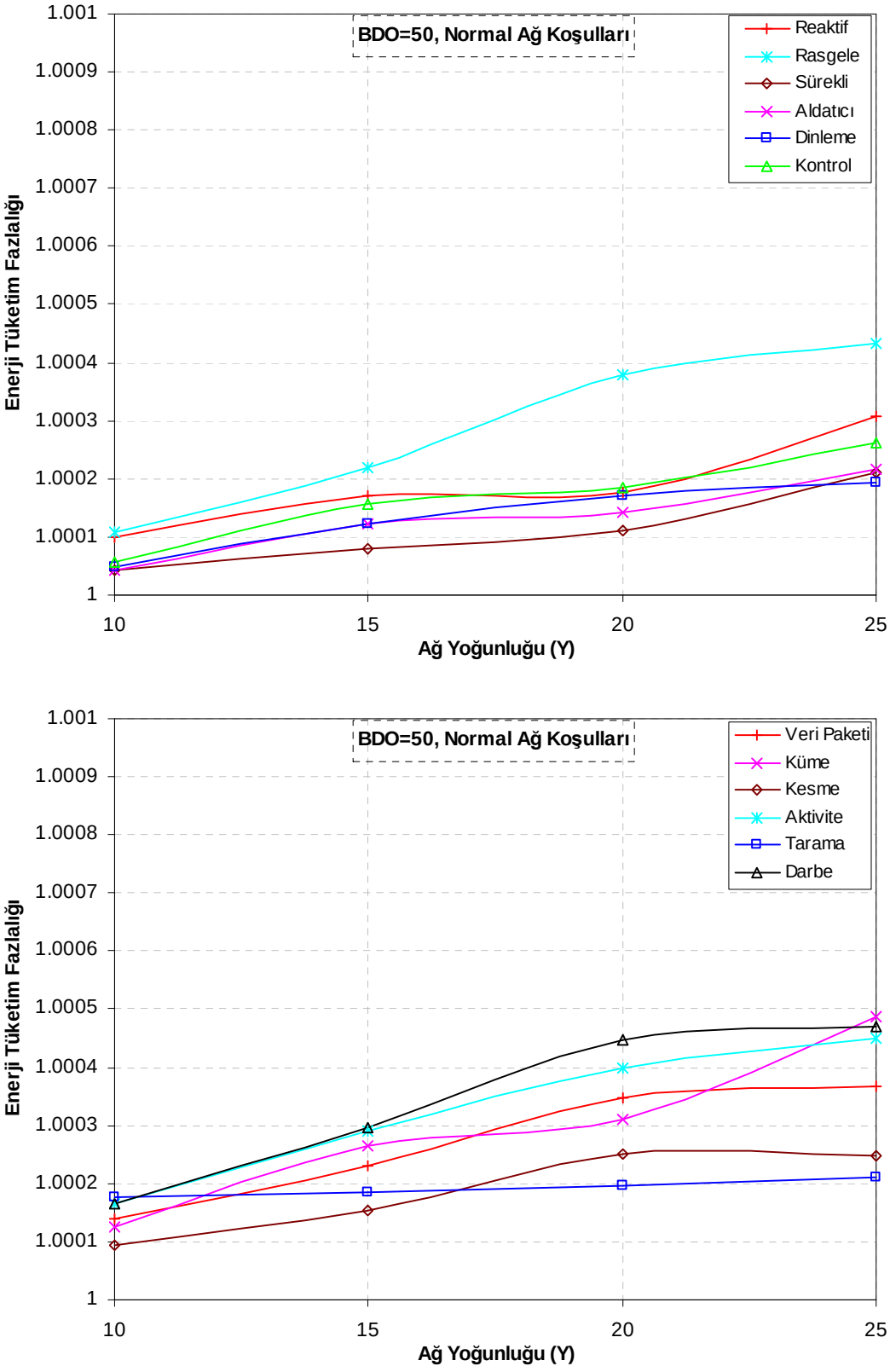
Önerilen yöntemin neden olduğu enerji tüketim fazlalığını tespit etmek için farklı düğüm yoğunluklarında ve farklı boğulmuş saldırgan oranlarında benzetimler gerçekleştirilmiştir. Şekil 5.19'da saldırının olmadığı (BDO=0) normal ve kötü ağ koşullarında düğüm başına düşen ortalama enerji tüketim fazlalıkları görülmektedir. Şekilden ağ yoğunluğunun artması ile iletişim fazlalığına benzer olarak yöntemin neden olduğu enerji tüketim fazlalılığının arttığı gözlemlenmektedir. Ayrıca kötü ağ koşullarından etkilenen PTO ve HPO parametreleri sebebiyle düğümlerin normal koşullara oranla daha fazla SORGU/CEVAP paketi gönderimi, yöntemin saldırının olmadığı kötü ağ koşullarında daha fazla enerji tüketmesine neden olmaktadır. Geliştirilen ileri saldırı tespit yönteminin herhangi bir saldırının olmadığı durumda düğümlerin güç tüketimine getirdiği ek yük en fazla on binde 5 oranındadır.



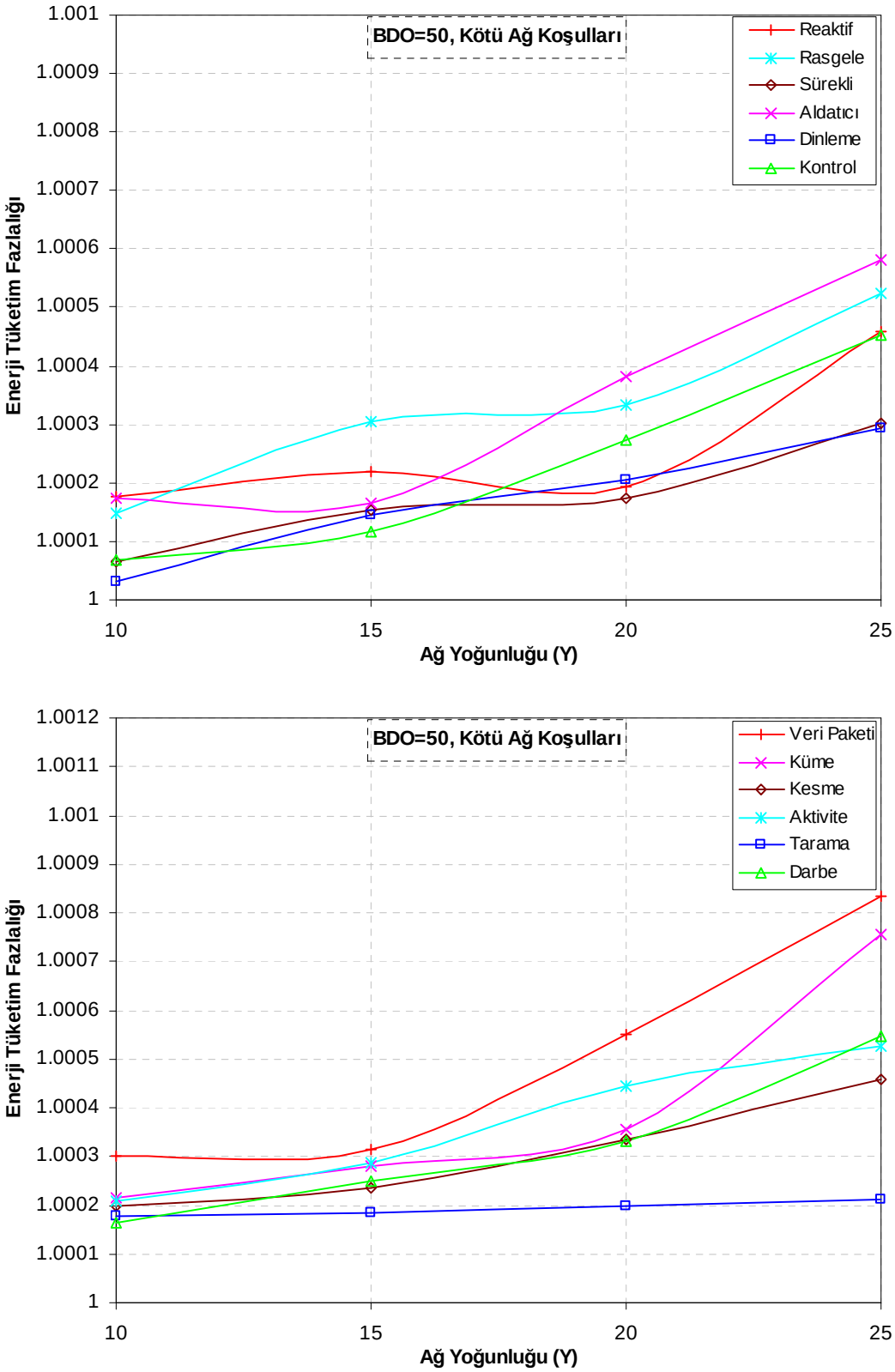
Şekil 5.19.Saldırının olmadığı farklı ağ koşullarında elde edilen enerji tüketim fazlalıkları

Şekil 5.20'de normal ağ koşularında, Şekil 5.21'de ise kötü ağ koşularında ve %50 boğulmuş düğüm oranlarında düğüm başına düşen ortalama enerji tüketim fazlalık değerleri görülmektedir. Saldırının olmadığı durumlara benzer olarak ağ yoğunluğu arttıkça enerji tüketim fazlalığı artmaktadır. Bir ağdaki düğümlerin yarısının

saldırganlar tarafından etkilenmesi durumunda geliştirilen ileri saldırı tespit yönteminin düğüm iletişimlerine getirdiği ek yük en fazla on binde 8 oranındadır.

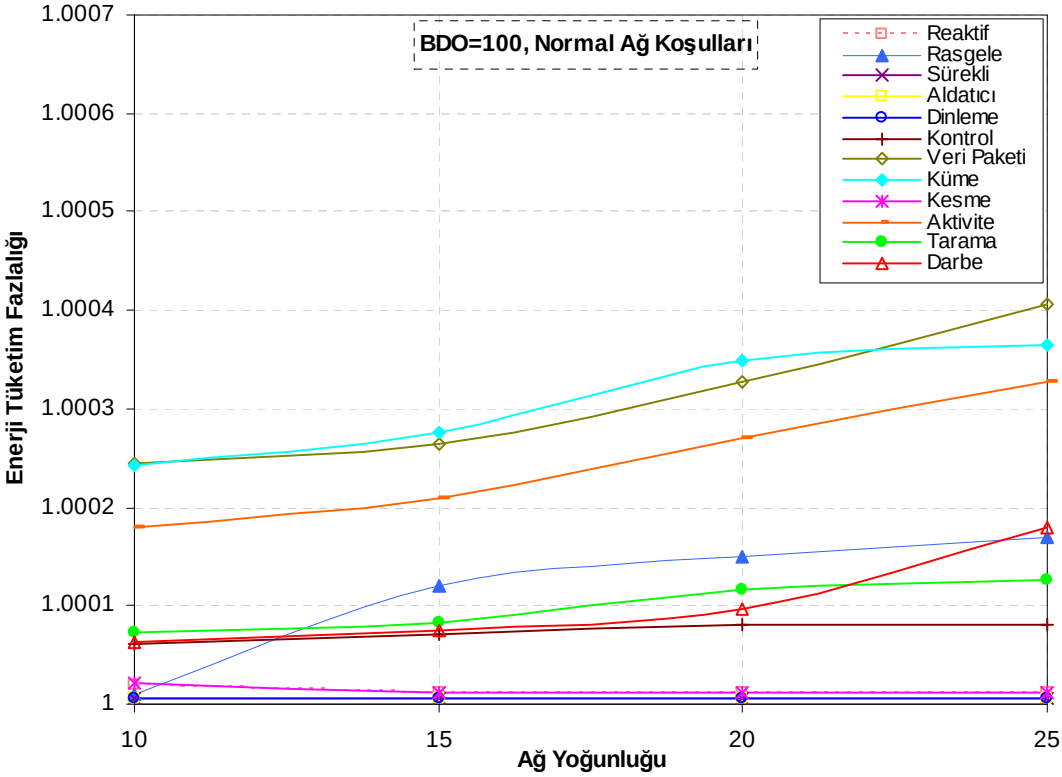


Şekil 5.20. Normal ağ koşullarında ve %50 boğulmuş düğüm oranında elde edilen iletişim fazlalıkları

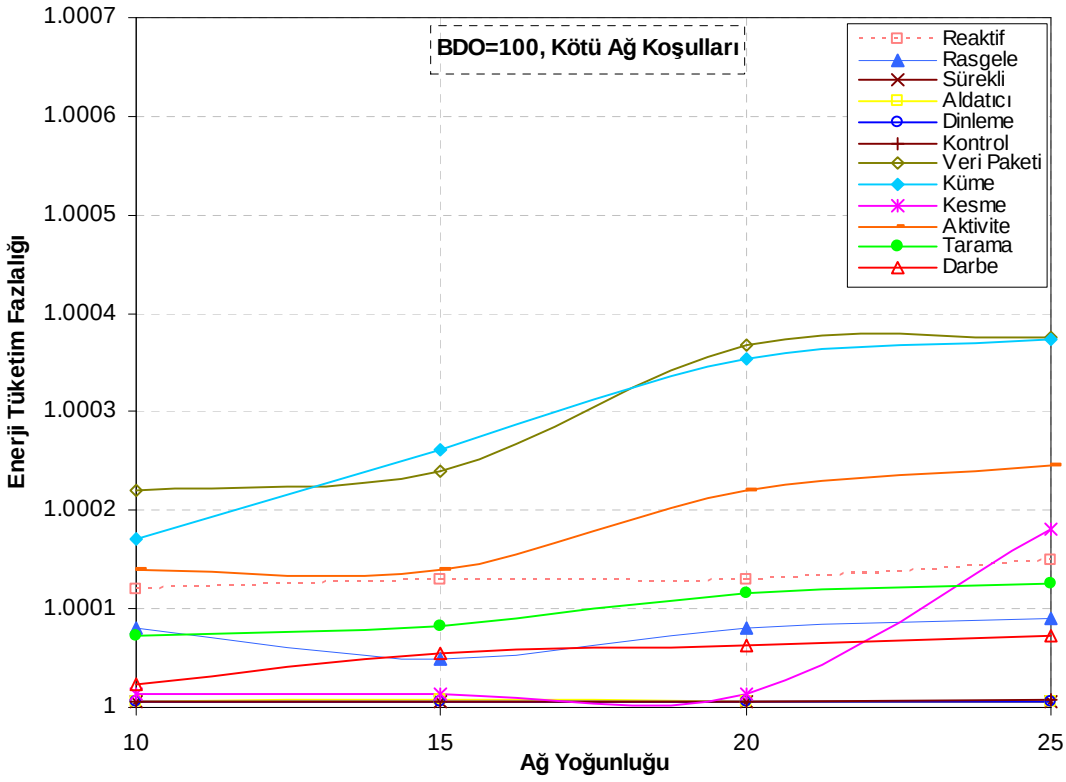


Şekil 5.21. Kötü ağ koşullarında ve %50 boğulmuş düğüm oranında elde edilen iletişim fazlalıkları

Şekil 5.22'de Normal ağ koşullarında, Şekil 5.23'de ise kötü ağ koşullarında ve %100 boğulmuş düğüm oranında düğüm başına düşen ortalama enerji tüketim fazlalığı görülmektedir. Bir ağdaki düğümlerin tamamının boğma saldırılarına maruz kalması durumunda geliştirilen ileri saldırı tespit yönteminin enerji tüketimine getirdiği ek yük en fazla on binde 4 civarındadır.



Şekil 5.22. Normal ağ koşullarında ve %100 boğulmuş düğüm oranında elde edilen enerji tüketim fazlalıkları



Şekil 5.23. Kötü ağ koşullarında ve %100 boğulmuş düğüm oranında elde edilen enerji tüketim fazlalıkları

5.6. Sonuçlar

Boğma saldırıları, çoğu zaman dış dünyada düşmanca koşullar altında çalışan ve sınırlı kaynaklara sahip olan kablosuz algılayıcı düğümleri için önemli bir tehdit unsurudur. Bu saldırıların üstesinden gelebilmenin ilk adımı saldırıları başarılı bir şekilde tespit edebilmekten geçmektedir. Bu bölümde literatürde tanımlanmış olan boğma saldırılarının tespitine yönelik enerji-verimli yöntem tasarımı geliştirilmiştir. Önerilen yöntem ile literatürdeki saldırgan modelleri yüksek tespit oranları ve düşük hatalı sezme oranları ile doğal ağ koşullardan ayrılabilmektedir. Ayrıca sunulan yöntemin düğüm iletişimlerine getirdiği ek yük en fazla %12 civarındayken, enerji tüketimine getirdiği ek yük ise en fazla on binde 7 civarındadır. Sunulan tespit sisteminde SORGU/CEVAP tekniğinin kullanması sebebiyle saldırıları tespit işlemi en fazla dört örnekleme periyodu (4x30=120 sn) içerisinde gerçekleştirilmektedir. Yöntemin bir diğer üstünlüğü ise herhangi bir ek donanıma ihtiyaç duyulmadan günümüz kablosuz algılayıcı düğümleri üzerinde kullanılabilir olmasıdır.

BÖLÜM 6. BOĞMA SALDIRILARINA KARŞI DİNAMİK KANAL ATLAMALI YENİ BİR GÜVENLİK YÖNTEMİNİN TASARIMI VE BAŞARIM ANALİZİ

6.1. Giriş

Kablosuz algılayıcı ağları, basitliği ve kullanım kolaylığı gibi avantajları sebebiyle askeri, tıbbi, ticari v.b birçok alanda kullanılmaktadır ve gelecekte daha yaygın bir şekilde kullanılması öngörülmektedir. Ancak askeri uygulamalar, bina güvenlik sistemleri, hasta takip sistemleri gibi güvenliğin çok önemli olduğu uygulama alanlarında kullanılan kablosuz algılayıcı ağlarının her türlü saldırılara karşı dayanıklı olması beklenir. Diğer bir ifadeyle, kablosuz algılayıcı ağı maruz kalabileceği bir saldırı durumunu tolere edebilmeli ve saldırılara rağmen hayati önem arz eden bilgileri doğru bir şekilde ve zamanda merkezi yönetim birimine iletebilmelidir. Bir algılayıcı ağının güvenliğinden söz edebilmek için boğma saldırıları gibi düğüm iletişimlerini tamamen ya da kısmen engelleyebilen saldırı türlerine karşı da dayanıklı olması ve saldırılara rağmen görevlerini yürütebilmesi gerekmektedir. Bu nedenle Bölüm 6'da kablosuz algılayıcı ağları için önemli bir tehdit unsuru olan boğma saldırılarının çözümüne yönelik yöntem üzerinde odaklanılmaktadır. Bölüme ilk olarak literatürde var olan savunma yöntemleri ve bu yöntemlerin zayıf yönleri özetlenerek başlanmaktadır. Boğma saldırıları için önerdiğimiz savunma yönteminin detayları açıklandıktan sonra geliştirilen yöntemin benzetim yoluyla gerçekleştirilen başarım analizi sunularak elde edilen sonuçlar irdelenmektedir.

6.2. Boğma Saldırıları İçin Geliştirilmiş Olan Çözüm Yöntemleri

Geleneksel kablosuz ağlarda boğma saldırılarına karşı kullanılan savunma yöntemlerinden en yaygını yayılım spektrum (spread spectrum) iletişim metodudur.

Frekans atlamalı yayılım spektrumunda (Frequency-Hopping Spread Spectrum-FHSS) gönderilen sinyallerin frekansları belli süreler boyunca değiştirilir. Böyle bir iletişimde alıcı ve verici senkronize olmalıdır. FHSS iletişim tekniği, girişime ve atlama sıralamasını bilmeyen saldırganlara karşı dayanıklı olmasına rağmen frekanslar arasında sürekli değişim ve senkronizasyon gereksinimi sebebiyle güç tüketimini arttırmaktadır. Bir diğer iletişim şekli olan doğrudan sıralı yayılım spektrumunda (Direct-Sequence Spread Spectrum-DSSS), geniş bir bant aralığında olan sinyaller rasgele bit akışı ile yayılırlar. DSSS teknolojisini gerçeklemek için FHSS teknolojisine oranla daha fazla elektronik devreye ihtiyaç duyulmaktadır. Bu sebeple maliyeti daha yüksektir ve daha fazla enerji tüketimine sebep olmaktadır. Maliyetlerin ve güç tüketimlerinin artması sebebiyle günümüz ticari düğümlerinde genellikle boğma saldırılarına karşı dayanaksız fakat düşük maliyetli olan tek frekanslı iletişim teknikleri tercih edilmektedir.

Kablosuz algılayıcı ağlarda boğma saldırılarına yönelik olarak geliştirilen ilk çalışmada [9] saldırıların varlığını tespit ettikten sonra bu saldırıların kapsadığı alanı tayin ederek yönlendirme yollarının değiştirilmesini öngören protokol tasarımı gerçekleştirilmiştir. Geliştirilen protokol, ağ içerisindeki her bir düğümün saldırı tespit modülüne sahip olduğunu ve saldırı durumlarının kanal kullanım oranı yardımıyla tespit edildiğini varsaymaktadır. Saldırı tespitini gerçekleştiren düğüm MAC katmanındaki çekişme kurallarını ihlal ederek JAMMED ya da UNJAMMED mesajlarını komşularına iletmekte ve bu mesajlar saldırganın etki alanının sınırlarında olan düğümler yardımıyla saldırıdan etkilenmeyen komşu düğümlere aktarılmaktadır. Yayınlanan bu mesajlar yardımıyla ortaklaşa olarak saldırı bölgesinin alanı belirlenmekte ve yönlendirme katmanına yolların değiştirilmesi için bilgi gönderilmektedir. Saldırı etkisinde olan düğümler, bilinçsizce enerji harcamak yerine uyuma moduna geçmekte ve saldırıların sonlanmasını beklemektedir. 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. Ayrıca saldırılar devam ettiği sürece saldırıların etkisinde olan düğümler ile ağın geri kalanı arasında bir iletişim kurulamamakta ve böylece o bölgenin gözetimi sağlanamamaktadır. Enerjisini hızlı tüketen sürekli

saldırı stratejisi yerine enerjisini verimli kullanan saldırgan türlerinin kullanıldığı varsayıldığında bu düğümler ile uzun süre irtibat kurulabilmesi mümkün değildir. Ayrıca bu yöntem sadece gezgin olmayan saldırgan türlerine yönelik olarak geliştirilmiştir.

Xu ve diğerleri boğma saldırılarına yönelik olarak frekans atlama metodunun adaptif bir şekli olan ve "kanal sörfü" olarak adlandırılan bir yöntem geliştirmişlerdir [10,11]. Bu yöntemde, düğümler bir frekanstan diğer frekansa sürekli atlamak yerine sadece bulundukları kanal saldırı altında olduğunda farklı bir kanala geçmektedir. Kanal sörfü yöntemi; "koordinasyonlu kanal sörfü" ve "izgesel kanal sörfü" olarak isimlendirilen iki alt metottan meydana gelmektedir. Koordinasyonlu kanal sörfü metodunda, ağdaki tüm düğümlerin saldırıdan kaçmak için birbirleri ile koordinasyonlu olarak farklı bir kanala atlaması ve ağ ile yeniden irtibata geçmesi gerekmektedir. Bu yöntemde saldırı tespiti yapan düğümler, önceden belirlenmiş atlama sırasına göre farklı bir kanala geçmekte ve komşuları ile bu kanalda haberleşmeyi beklemektedir. Kendisi saldırı altında olmasa da komşusu saldırı altında olan "sınır düğümler" ise belirli bir zaman içerisinde paket alamayınca komşusunun saldırıya uğramış olabileceğini düşünerek mevcut kanalları taramaktadır. Komşusunu farklı kanalda bulan bir sınır düğüm saldırı altında olmayan diğer düğümlere ağ içerisinde saldırı olduğunu ve merkez frekanstan farklı bir kanala atlandığını duyurmak için geçici olarak merkez frekansa geçmekte ve kanal değiştirme komutunu diğer komşularına yaymaktadır. Böyle bir paket alan düğüm de yine aynı mesajı yayınlamakta ve böylece tüm ağın frekansı değişmektedir. İzgesel kanal sörfü metodunda ise sadece saldırıya maruz düğümler kanal değiştirmekte diğer düğümler ise merkez kanalda kalmaktadır. Bu iki frekans bölgesi arasındaki haberleşmeyi sağlayabilmek için sınır düğümlerin her iki frekansa da çalışması gerekmektedir. Her iki metodunda birbirlerine göre avantaj ve dezavantajları olmasına karşın, tarama saldırganı gibi kanalları tarayarak saldıran bir saldırgana karşı etkinlikleri oldukça düşebilmektedir. .

Xu ve diğerleri gerçekleştirdikleri bir diğer çalışmada boğma saldırıları için 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.

Cagalj ve diğerleri kablosuz algılayıcı ağlarda boğma saldırıları için solucan deliği esasına dayanan üç çözüm yöntemi önermiştir [12] . Bu çalışmada, 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. İlk yöntemde, ağa belli sayıda birbirleri ile kablo yoluyla bağlı düğüm çiftlerinin rasgele olarak yerleştirilmesi ve bu düğümler sayesinde saldırı bölgesindeki hayati bilgilerin saldırıdan uzak düğümlere aktarılması hedeflenmiştir. İkinci olarak, ağa belirli sayıda frekans atlama kabiliyetine sahip olan düğüm çiftlerinin yerleştirilmesi ve bu sayede güvenli solucan delikleri yardımıyla bilgilerin saldırı bölgesinin dışına aktarılması düşünülmektedir. Son olarak da, kanal değiştirme kabiliyetine sahip düğümler yardımıyla koordinasyonsuz olarak düğümlerin kanal değiştirmesi ve bilgilerin böylece saldırı bölgesinin dışarısına çıkarılması hedeflenmektedir. 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 Uygulamada mevcut düğümler genelde 15/26 kanalı desteklemektedir.

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. “Kesme saldırganı” olarak adlandırılan saldırgan türünün bir öntakı ve arkadan bir SFD (Start of Frame Delimiter – Çerçeve Başlangıç Ayracı) sezdiğinde donanımsal bir kesme ile uyanarak enerji-etkin saldırı başlatmasına yönelik olarak çerçeve maskeleme yöntemi önerilmiştir. Bu yöntemde

SFD bir paylaşımlı anahtarla şifrelenmekte ve böylece kesme saldırganı var olan iletişimi sezemeyerek saldırıları başlatamamaktadır. Wood ve diğerleri iletim kanalındaki aktiviteyi RSSI ölçümünden yararlanarak saldırı başlatan aktivite saldırganına karşı kanal atlama yöntemini önermiştir. Bu yöntemde, düğümler mevcut kanallar arasında rasgele sıra ile atlamakta ve bu atlama sırası sadece alıcı ile verici düğüm tarafından bilinmektedir. Wood ve diğerleri mevcut kanalları tarayarak iletişim sezdiği kanala saldıran tarama saldırganına karşı paketlerin küçük parçalara bölünerek farklı kanallardan iletilmesini sağlayan paket bölümleme yöntemi ve son olarak da tek bir kanalda kalarak bölünen paketleri bozmaya çalışan darbe saldırganına karşı paketlerin bozulmaya karşı dayanımı arttırmak üzere "fazladan kodlama yöntemi" önermiştir. 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.

6.3. Dinamik Kanal Atlama Yönteminin Tasarımı

Literatürde boğma saldırılarına yönelik çeşitli savunma yöntemleri sunulmuş olmasına karşın tüm saldırı modellerine karşı çözüm üreten yöntem gereksinimi bulunmaktadır. Bu çalışmada Bölüm 4'te detayları verilen 12 adet boğma saldırı modeline rağmen kablosuz algılayıcı düğümlerinin iletişimlerini devam ettirebilmesine imkân tanıyan Dinamik Kanal Atlama (DKA) yönteminin tasarımı gerçekleştirilmiştir.

DKA, düğümlerin boğma saldırılarından kaçabilmesi 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.

Literatürde tek kanalda çalışan ve mevcut kanalları gezerek farklı kanallarda çalışabilen saldırgan modelleri bulunmaktadır. Sürekli, aldatıcı, rasgele, reaktif, dinleme aralığı, kontrol aralığı, veri paketi, kesme, aktivite ve darbe saldırganları tek kanal frekansında çalışan saldırgan modellerindendir (detaylı bilgi için bkz. Bölüm 4). Dinamik kanal atlama yönteminde, düğümler saldırının gerçekleştiği merkez frekanstan farklı bir kanala geçerek bu kanalda yeniden ağ bağlantılarını gerçekleştirmekte ve tüm ağ bu kanalda çalışmaktadır. Bu şekilde saldırgan merkez frekansta saldırılarını devam ettirirken düğümler girişimsiz bir başka kanalda iletişimlerini sürdürebilirler. Ancak düğüm iletişimlerinin tarama saldırganı gibi kanalları gezerek saldıran bir saldırgan tarafından bozulması durumunda merkez frekanstan farklı bir kanala geçmek ve daimi olarak bu kanalda iletişimi devam ettirmeye çalışmak mümkün olmayacaktır. Çünkü tarama saldırganı merkez frekansta belli bir süre iletişim olmadığını sezince kanalları taramaya başlayacak ve kısa süre içerisinde düğümlerin iletişim yaptığı kanalı bularak saldıracaktır. Bu sebeple DKA yöntemi tarama saldırganı gibi farklı kanallar arasında çalışan saldırganlara yönelik olarak düğümlerin rasgele sırayla ve hızlı bir şekilde kanallar arasında gezmesine olanak sağlayan Rasgele Kanal Atlama (RKA) metodunu kullanmaktadır. RKA, düğümlerin sözde rasgele sıra ile ve periyodik olarak kanallar arasında gezmesine ve kanal takibi yapan saldırganlara karşı düğüm iletişimlerinin daha dayanaklı olmasına yardımcı olmaktadır.

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 yöntem seçilmektedir. Eğer saldırganlar tek kanal frekansında çalışıyorsa düğümler geçerli bir başka kanala atlamakta ve ağ ile yeniden irtibata geçerek sürekli bu kanalda kalmaktadır. Eğer saldırganlar farklı kanallar arasında çalışabiliyorsa düğümler, RKA metodu ile periyodik olarak kanal değiştirmektedir.

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.

- Saldırı Tespiti: 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.

- Kanal Atlama ve Komşularla İrtibatın Yeniden Sağlanması: Kanal atlama, saldırı tespit işleminden sonra saldırı altında olduğuna karar veren düğümlerin merkez kanaldan mevcut kanallar içerisindeki en son kanala atlaması işlemidir. Kanal değiştiren bir düğüm yeni kanalda ağ ile yeniden irtibata geçmek için komşularının da bu kanala geçmesini beklemektedir.

- Test ve Yayılma: Düğümler atladığı yeni kanalda kayıp komşularını bulabilirlerse belirli bir süre boyunca kanalın bir saldırgan tarafından etkilenmediğinden emin olmak için test yayını gerçekleştirirler. Eğer test yayını sonucunda kanalın temiz olduğu anlaşılırsa düğümler bu kanalda kalarak iletişimlerini yeniden başlatmaktadır. Böyle bir durumda saldırı altında olan düğümler ile saldırıdan etkilenmeyen düğümler arasında frekans farklılığı olacağı için iki bölge arasında iletişim gerçekleşmeyecektir. Bu sorunu aşmak için saldırı bölgesine sınır olan düğümler, saldırıdan etkilenmeyen düğümlere kanalın değiştiğini duyurmalı ve bu bilgi tüm ağa yayın metoduyla ilan edilmelidir.

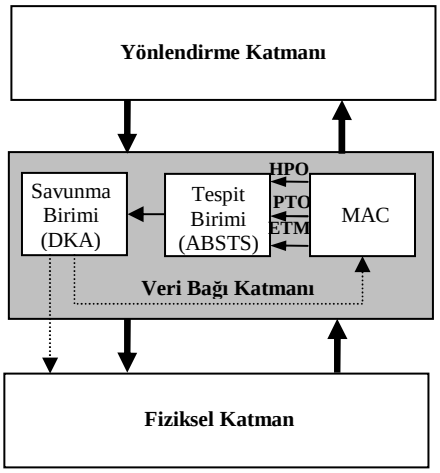
- Rasgele Kanal Atlama: Boğma saldırıları sebebiyle merkez kanaldan farklı bir kanala atlayarak komşuları ile irtibata geçen bir düğüm, yaptığı test sonucunda bu kanalda da saldırıya uğradığına karar verirse kanallar arasında gezerek saldıran bir tarama saldırganın etkisi altında olduğunu varsayar. Bu durumda düğümlerin periyodik olarak ve rasgele sırada mevcut kanallar arasında gezmesini sağlayan Rasgele Kanal Atlama yöntemi devreye girer.

- Senkronizasyon: Rasgele kanal atlama metodunda düğümler, birbirlerine paket gönderirken gönderici alıcının şu an hangi kanalda olduğunu ve ne zaman farklı bir kanala atlayacağını bilmelidir. Düğümlerin bu gibi bilgileri doğru bir şekilde tespit edebilmesi için aralarında bir senkronizasyon olması gerekmektedir.

- Kanal Tahsisinin Planlanması: Rasgele Kanal Atlama metodunun kullanılması durumunda paket göndermesi gereken bir düğüm kendi kanalından alıcının olduğu kanala ne zaman geçeceğine karar vermeli ve ayrıca ne zaman gönderimde ya da ne zaman alımda bulunacağını belirlemelidir. Gönderici ile alıcının bulunduğu kanallar farklı olabilir ya da aynı kanalda birçok düğüm aynı anda gönderime başlayabilir. Kanal tahsisinin planlaması tüm bu süreçleri kapsamaktadır.

6.3.1. Saldırı tespiti

DKA yönteminin uygulanabilmesi için ilk olarak boğma saldırılarının tespit edilmesi gerekmektedir. Bu sebeple DKA yöntemi Şekil 6.1'de görüldüğü gibi boğma saldırı tespit sistemi (detaylı bilgi için bkz. Bölüm5) ile birlikte kullanılmaktadır. ABSTS, boğma saldırılarını MAC katmandan elde ettiği paket teslim oranı, hatalı paket oranı ve enerji tüketim miktarı parametrelerine göre tespit etmektedir. Her örnekleme periyodunda ölçülen bu parametrelerdeki anormal değerler saldırı tespit algoritması tarafından değerlendirilerek tespit işlemi gerçekleştirilmektedir. Saldırı tespitinde SORGU/CEVAP tekniğinin kullanılması sebebiyle saldırıların başlamasını takip eden dört örnekleme periyodu sonunda tespit işlemleri bitmekte ve DKA yönteminin çalıştırıldığı savunma birimine sinyal gönderilmektedir.



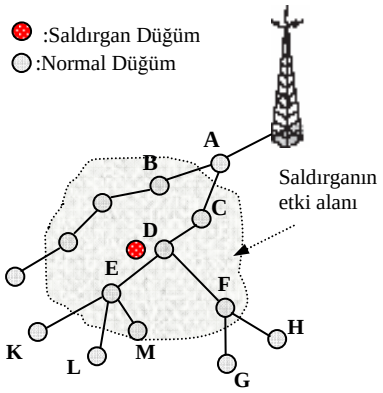
Şekil 6.1. Boğma saldırılarının tespiti edilmesi ve savunulması

6.3.2. Kanal atlama ve komşularla irtibatın yeniden sağlanması

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. Burada 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 sadece 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. Böyle bir paket alan düğüm ise komşusuna cevap vermektedir. Ancak düğümlerin farklı bir kanala geçerek yeniden irtibat kurabilmesinin bazı zorlukları vardır. Şekil 6.2'de bu zorlukları gösteren bazı saldırı senaryoları görülmektedir.



Şekil 6.2. Komşular ile irtibatının sağlanması sırasında karşılaşabilecekleri durumlar

1. D düğümünde olduğu gibi düğümün kendisinin ve tüm komşularının saldırı etkisinde olması durumu
2. F düğümünde olduğu gibi düğümün kendisinin ve üst düğümünün saldırı etkisinde olmasına rağmen alt düğümlerinin saldırıdan etkilenmeme durumu
3. E düğümünde olduğu gibi düğümün kendisinin ve üst düğümünün saldırı etkisinde olmasına karşın alt düğümlerinden bazılarının saldırılardan etkilenirken bazısının etkilenmeme durumu.
4. C düğümünde olduğu gibi düğümün kendisi ve alt düğümü saldırı altında olmasına karşın üst düğümün saldırılardan etkilenmeme durumu

Birinci durumda söz konusu tüm düğümler saldırı altında olduğu için farklı bir kanala atlama ve O kanalda yeniden irtibata geçme işleminde her hangi bir zorluk yoktur. Çünkü düğümlerin tümü yaklaşık olarak aynı zamanda (dört örnekleme periyodu sonunda) saldırı tespiti yaparak en son kanala geçmektedir. Ancak diğer durumlarda, bazı düğümlerin saldırıdan etkilenirken bazıların etkilenmemesi söz konusu olduğu için bu iki ayrı grup arasında bir ilişki kurulabilmesi gerekmektedir. Örneğin ikinci durumda saldırgan kapsama alanının sınırlarında bulunan F düğümü

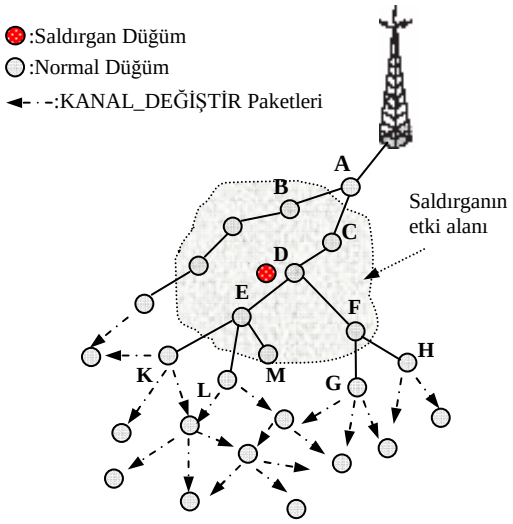
alt düğümleri ile iletişim gerçekleştirebilmesine rağmen üst düğümü (D) ile iletişim yapamamaktadır. D ve F düğümleri saldırılar başladıktan sonra dört örnekleme periyodu içinde saldırı tespitini gerçekleştirmekte ve en son kanala geçmektedir. Ancak G ve H düğümleri saldırıdan etkilenmediği için merkez kanalda kalmaya devam etmektedir. Bu sorunu aşmak için F düğümü saldırıdan etkilenmeyen G ve H düğümlerine merkez kanaldan en son kanala ne zaman atlayacağını gösteren bir paket göndermeli ve bu sayede yeni kanalda yeniden irtibat kurulmasını sağlamalıdır.

Üçüncü durumda saldırganın etkin kapsama alanında bulunan E düğümü, üst düğümü olan D ile ve alt düğümü olan M ile iletişim gerçekleştirememektedir. K ve L düğümleri ise saldırganın etki alanının dışında olmasına karşın üst düğümleri olan E düğümünün saldırganın etkin kapsama alanında olması sebebiyle saldırılardan etkilenmektedir. Geliştirdiğimiz anomali tabanlı tespit sistemi K ve L düğümleri gibi dolaylı yoldan saldırıdan etkilenen düğümlerde de saldırı tespit işlemine olanak sağladığı için E, K, L ve M düğümlerinin tümü dört örnekleme periyodu sonunda merkez kanaldan en son kanala atlamakta ve yeni kanalda irtibata geçebilmektedir.

Son durumda ise C düğümü ile C'nin alt düğümü olan D, saldırı tespiti yaparak merkez kanaldan son kanala geçmekte ancak A düğümü saldırı tespiti yapmadığı için merkez frekansta kalmaktadır. Eğer C düğümünün saldırganın etki alanının sınırında olduğu varsayılırsa C ile A arasında merkez frekansta iletişim kurulabileceğinden ikinci durumdaki gibi (C'nin bildirmesi ile) A düğümü kanal atlama işleminden haberdar olabilir. Ancak C düğümünün saldırganın etkin kapsama alanında olduğu düşünüldüğünde C ve D kanal değiştirirken A düğümü C'nin kanal değiştirdiğinden haberdar olamaz. Böyle bir durumda C ve A hiçbir zaman yeni kanalda irtibata geçmezler. DKA yönteminde bu sorunu aşmak için her bir düğüm alt düğümlerinden sorumlu tutulmaktadır. Eğer bir düğüm alt düğümlerinden birisi ya da daha fazlasından dört örnekleme periyodu boyunca geçerli bir paket alamazsa saldırıya maruz kaldığını/kaldıklarını düşünerek geçici süreliğine en son kanala geçmekte ve kayıp komşularını aramaktadır. Böylelikle yeni kanalda düğümler arası irtibat sağlanabilmektedir.

6.3.3. Test ve yayılma

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 kalmayacağını 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 6.3'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.



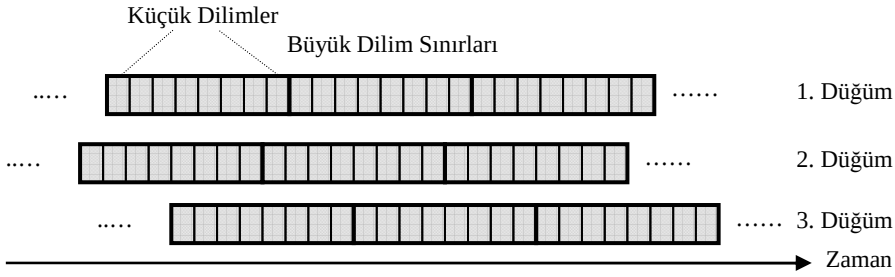
Şekil 6.3. KANAL_DEĞİŞTİR paketlerinin tüm ağa yayılması

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 varsaymakta ve RKA işlemine başlamaktadırlar.

6.3.4. Rasgele kanal atlama

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 kaçmak 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 6.4'de görüldüğü gibi McMAC [97] protokolüne benzer olarak 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) tekabül etmektedir. 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 6.4'te görüldüğü gibi atlama sınırlarının eş zamanlı olması gerekmemektedir. Bu sebeple komşularından birisine paket göndermek isteyen düğüm, alıcı düğüm ile ortak bir kanalda buluşmalıdır. Rasgele kanal atlama 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 6.4. Rasgele kanal atlama zaman diyagramı

Şekil 6.5'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. Rasgele kanal atlama 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.

Kanal Değiştirme Süresi	Koruma Zamanı	Çekişme Süresi	İletişim Süresi
6 K. dilim (183 µSn)	6 K. dilim (183 µSn)	12 K. dilim (366 µSn)	Veri paketi (640 µSn)+Bekleme (192µSn)+ACK (352µSn) (Toplam 40 küçük dilim=1220µSn

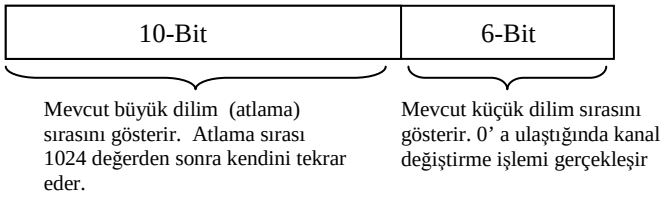
Şekil 6.5. Bir büyük dilimin ayrıntıları

Düğümler sözde rasgele atlama sırasını Formül 6.1 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.

$$KS(n)= E_K(n–1) \bmod C \qquad (6.1)$$

Rasgele kanal atlama yönteminde 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 6.6'da görüldüğü gibi bu zamanlayıcının düşük değerlikli 6 biti düğümün ne zaman kanal değiştireceğini yani şu andaki mevcut küçük dilimini, geri kalan 10 bit ise kaçıncı büyük dilimde olduğunu 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 6.6. Düğümlerde bulunan yerel saat

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 komşu tablosuna kaydetmektedir. Ayrıca rasgele kanal işleminin başlamasıyla birlikte düğümler belirli aralıklarla yerel saat bilgilerini paylaşarak bu bilgilerin güncel tutulmasını sağlamaktadır.

6.3.5. Senkronizasyon

Rasgele kanal atlama 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 bu saat bilgisi ile kendi saatini karşılaştırarak komşusunun atlama zamanlarını tayin edebilmektedir. Ancak düğümler arasındaki saat tiklerinin atış hızlarındaki farklar küçük de olsa belirli bir zaman sonrasında büyümekte ve düğümler arasında kanal atlama zamanlarının senkronizasyonu bozulabilmektedir. Bunun sonucunda gönderici düğüm alıcı düğümün kanalına geçtiğinde, alıcı düğümün yerel saatinin göndericiye oranla daha hızlı ilerlemesi neticesinde o kanalı terk etmiş olabilir. Bu sebeple gönderici ile alıcı arasındaki saat farklarını gidermek için ikili (pair-wise) zaman senkronizasyon protokolüne ihtiyaç duyulmaktadır. Literatürde bu amaç için geliştiriliş çeşitli senkronizasyon protokolleri bulunmaktadır [88,89]. Rasgele kanal atlama metodunda da alıcı/verici arasındaki senkronizasyonu sağlamak için pratik senkronizasyon tekniğinden faydalanılmıştır [88]. Bu yöntemde düğümler arasındaki saat sapma oranı, özyinelemeli en küçük kare (recursive least square) yöntemi ile tespit edilmekte ve düğümler belirli aralıklarıyla paylaşılan senkronizasyon paketleri yardımıyla aralarındaki senkronizasyonu güncel tutmaktadır.

6.3.6. Kanal tahsisinin planlanması

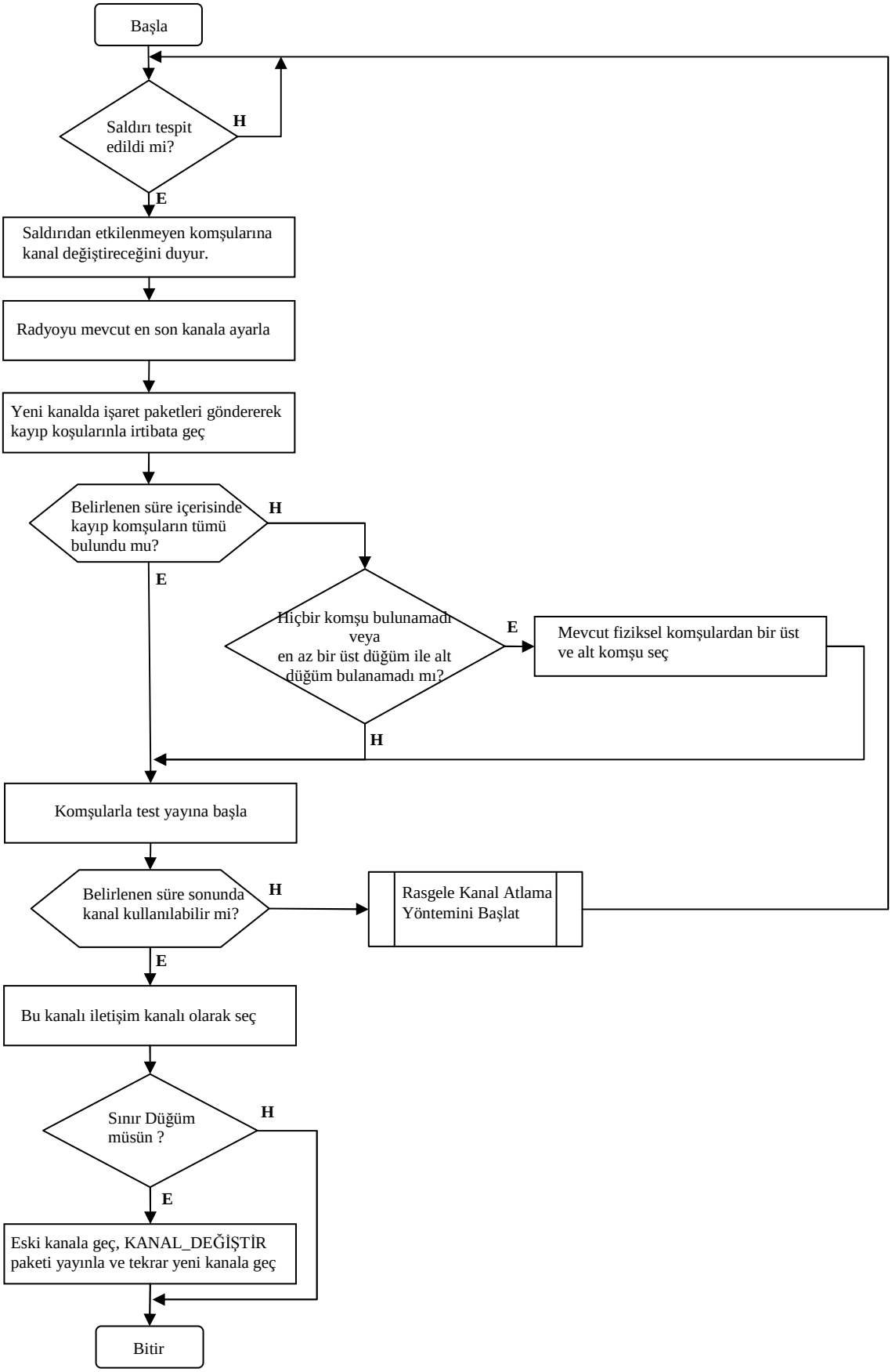
Rasgele kanal atlama yönteminde bir paket göndermek isteyen düğüm ilk önce paket göndermeye niyet ettiği komşusunun bir sonraki büyük zaman dilimine ne zaman başlayacağını ve hangi kanalda olacağını tahmin etmesi gerekmektedir. Alıcının büyük dilim başlangıç zamanı gelince kendi kanal atlama sırasında alıcının olduğu kanala atlamalı ve çekişme süresi içerisinde 0 ile CW (Contention Window-Çekişme Penceresi) arasında rasgele olarak seçtiği süre boyunca beklemelidir. Bu süre sonunda iletişim kanalını dinlemeli ve kanal meşgul ise kendi atlama sırasına geri dönmelidir. Eğer kanal boş ise paketi göndererek ACK cevabını beklemeli ve zamanı gelince yine kendi atlama sırasına dönmelidir. Rasgele kanal atlama metodunda

paket göndermesi gerekmeyen düğümler ise muhtemel bir alım işlemi için dinlemede kalmaktadır.

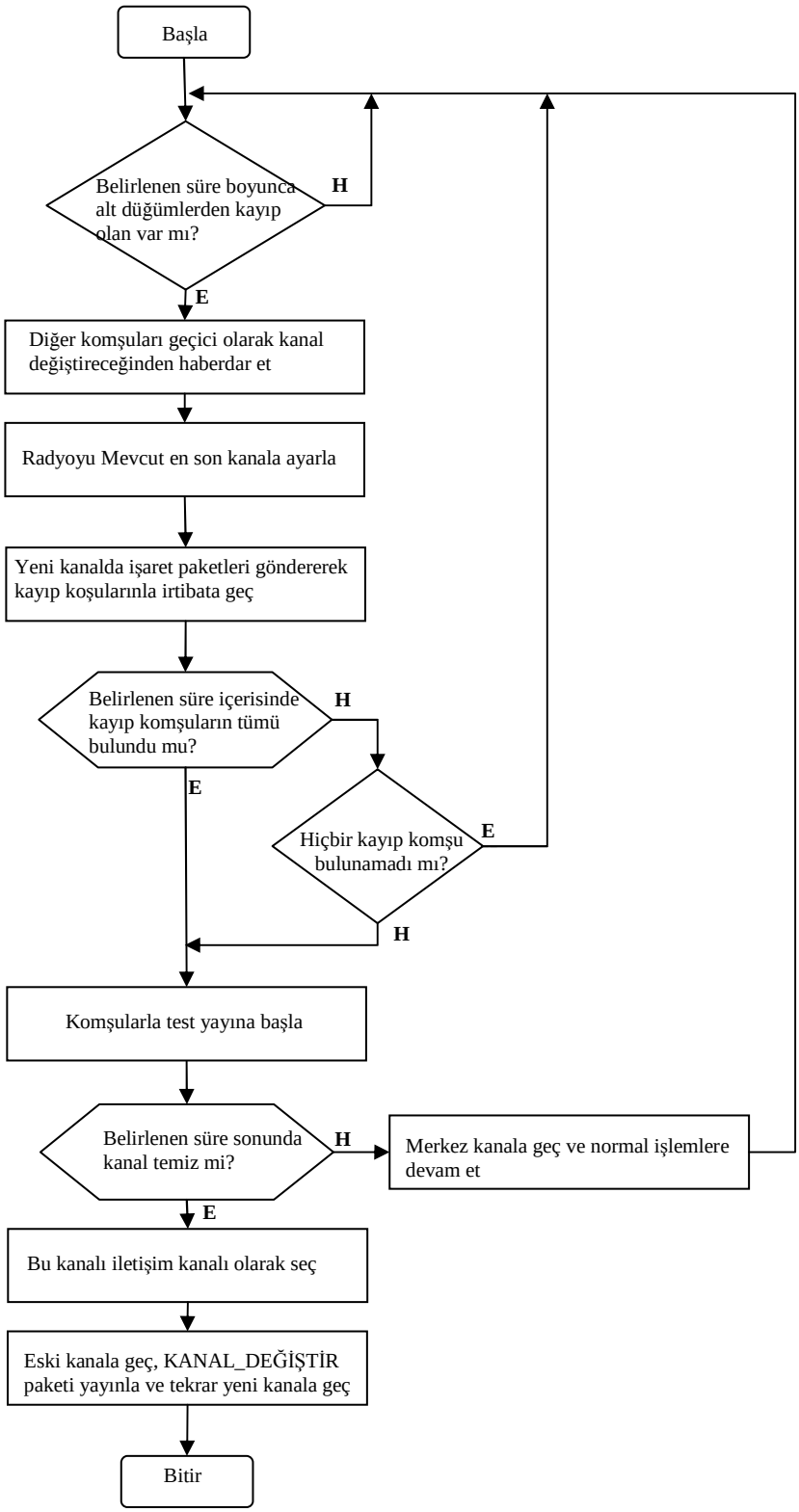
6.3.7. Dinamik kanal atlama yönteminin özeti

Belirli aşamalardan meydana gelen Dinamik Kanal Atlama yönteminin anlaşılmasını kolaylaştırmak için Şekil 6.7, 6.8 ve 6.9'da akış diyagramları verilmiştir. Şekil 6.7'de dinamik kanal atlama yönteminin genel akış şeması 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 uğramayacağını tespit etmektedir. Eğer kanalın bir saldırgan tarafından bozulduğu tespit edilirse Rasgele Kanal Atlama algoritması çalıştırılmakta aksi durumda ise yeni kanal iletişim kanalı olarak seçilmekte ve sınır düğümler tarafından seçilen bu kanal ağdaki tüm düğümlere duyurulmaktadır.

Şekil 6.8'de alt komşuları saldırıya uğramış olan düğümlerin DKA yöntemine dâhil olmasının akış şeması görülmektedir. Kendisi saldırı altında olmasa da alt düğümlerinden birisi ya da bir kaçı saldırıya maruz kalan düğümler alt komşularının kanal atlama durumundan haberdar olamazlar. DKA yönteminde bu sorun, Bölüm 6.3.2'de de belirtildiği gibi her düğümün alt komşularını takip etmesi sayesinde aşılmaktadır. Düğümler, kendisi saldırıya maruz kalmasa bile altındaki düğümleri sürekli olarak takip etmelidir. Belirli süre boyunca alt komşudan haber alınamaması durumunda, saldırı ihtimali düşünülerek mevcut en son kanala atlanmalı ve kayıp komşular aranmalıdır. Kayıp komşusunun yeni kanalda bulunması ile Şekil 6.7'deki duruma benzer olarak test işlemi gerçekleşmeli ve ardından eğer kanal temiz ise kanal değiştirme işleminden diğer düğümlerin de haberdar olabilmesi için KANAL_DEĞİŞTİR paketleri yayınlanmalıdır. Eğer düğümün atlanılan yeni kanalda yine alt düğümlerle olan irtibatı kesildiyse yani o kanalda saldırı başladıysa, düğüm merkez kanala geçmeli ve rasgele kanal atlama işlemine başlayan alt komşularının ona merkez kanalda paket göndermesini beklemelidir.

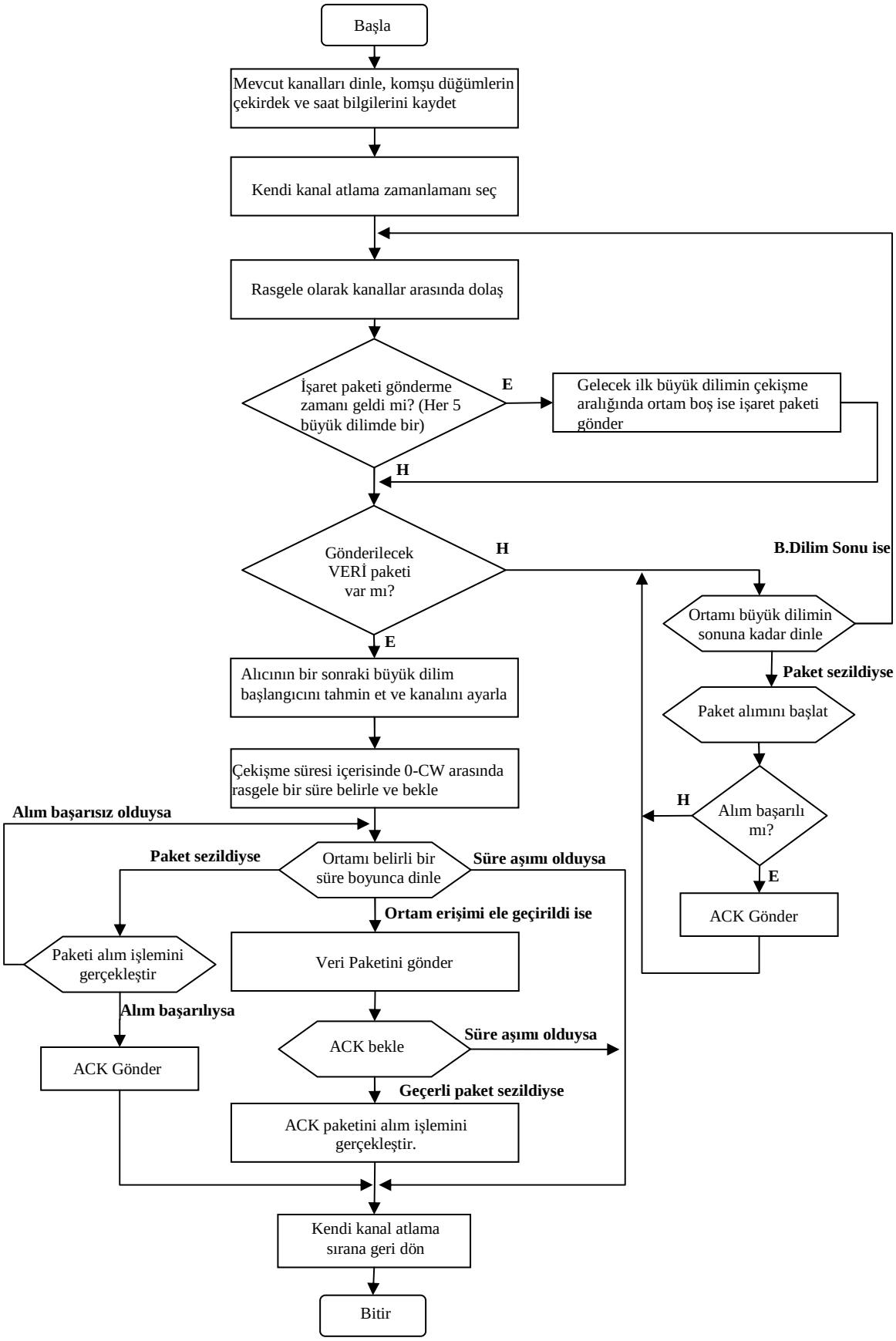


Şekil 6.7. DKA yönteminin genel akış şeması



Şekil 6.8. Alt komşuları saldırıya uğramış olan düğümlerin DKA yöntemine dâhil olması

Şekil 6.9’da ise DKA yönteminin bir alt metodu olan Rasgele Kanal Atlama algoritmasının akış şeması 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 süreler 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 kez 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.



Şekil 6.9. DKA yönteminin bir metodu olan RKA algoritmasının akış şeması

6.4. Geliştirilen dinamik kanal atlama yönteminin başarım analizi

Boğma saldırılarına karşı olarak geliştirilmiş olan Dinamik Kanal Atlama (DKA) 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 ve benzetimler, detayları EK.B'de verilen OMNET++ tabanlı benzetim yazılımı ile gerçekleştirilmiştir.

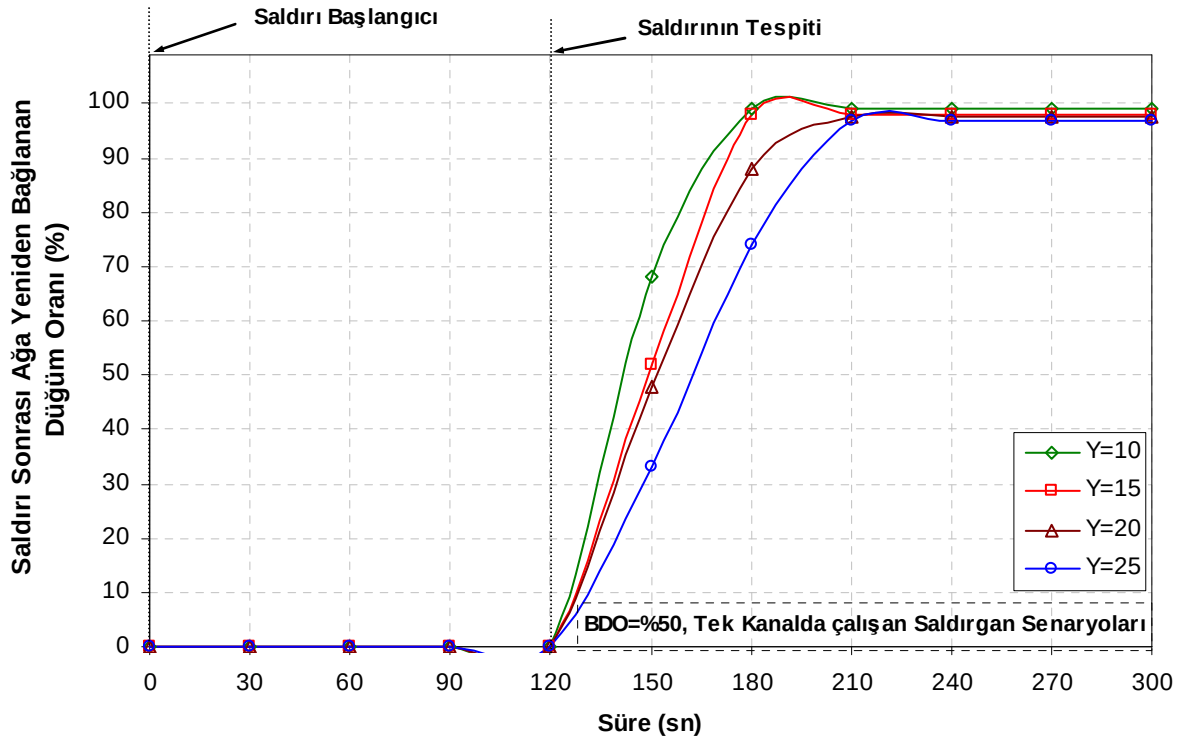
Tüm benzetim senaryolarında normal düğümler ile saldırgan düğümlerin güç kapasiteleri, güç tüketimleri, radyo iletim mesafeleri MICAz düğümüne uygun olarak seçilmiştir. Geliştirilen yöntemin farklı düğüm yoğunluklarındaki başarımını belirleyebilmek için iletişim mesafesi r olan N=100 adet normal düğüm, uzunluğu ℓ olan bir kare alana, Formül 6.2 yardımıyla istenilen düğüm yoğunluğuna (Y) göre [6] rasgele olarak dağıtılmıştır. Bir adet çıkış (sink) düğümü ise merkeze yerleştirilmiştir.

$$Y = \sqrt{\frac{N.\pi}{\ell} r} \tag{6.2}$$

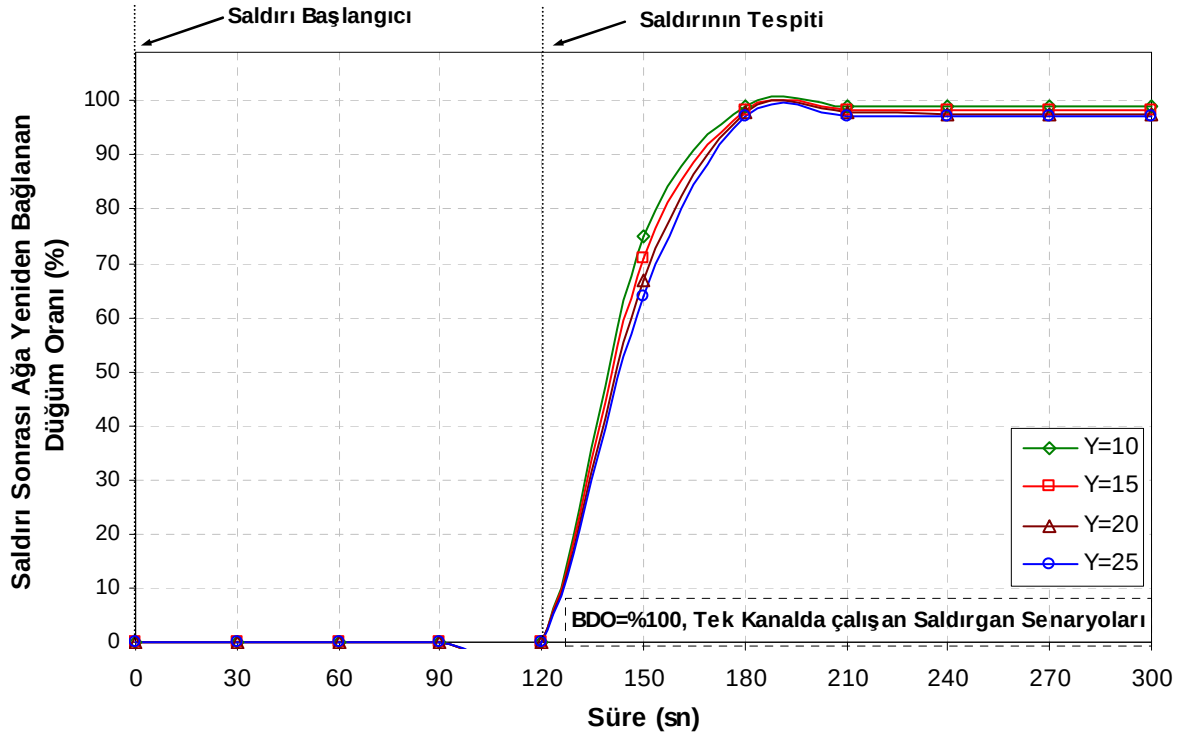
DKA yönteminin farklı saldırgan koşullarındaki başarımını ölçmek için ise toplam düğümlerin %50'sinin (Boğulmuş Düğüm Oranı=% 50) ve %100'nün (Boğulmuş Düğüm Oranı=% 100) saldırılara maruz kaldığı varsayılmıştır. Tarama saldırganın aslına uygun olarak bir kanalı 262 µSn'de tarayabildiği kabul edilmiştir.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

6.4.1. Cevap süresi

Şekil 6.10'da DKA yönteminin farklı ağ yoğunluklarında, %50 boğulmuş düğüm oranlarında, Şekil 6.11'de ise %100 boğulmuş düğüm oranlarında ve 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 saldırı tespit sisteminin SORGU/CEVAP işlemleri sebebiyle dört örnekleme periyodu sonunda yani saldırılar başladıktan 120 saniye sonra tespit işlemlerini bitirmesidir. Boğulmuş düğüm oranının %50 olduğu Şekil 6.10'da tüm ağın saldırı etkilerinden kurtulması yaklaşık olarak saldırılar başladıktan 210 saniye sonra yani yedi örnekleme periyodu sonunda gerçekleşmektedir. Bu üç örnekleme periyotluk süre kanal değiştirme, komşular ile irtibata geçme, test işlemi ve KANAL_DEĞİŞTİR komutunun ağa yayılması gibi işlemlerden kaynaklanmaktadır. Boğulmuş düğüm oranının %100 olduğu Şekil 6.11'de ise tüm ağın saldırı etkilerinden kurtulması yaklaşık olarak saldırılar başladıktan 180 saniye sonra yani altı örnekleme periyodu 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. 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 bu sebeple bazı düğümler ile irtibatın kurulmasında zorluk çekilmesidir.

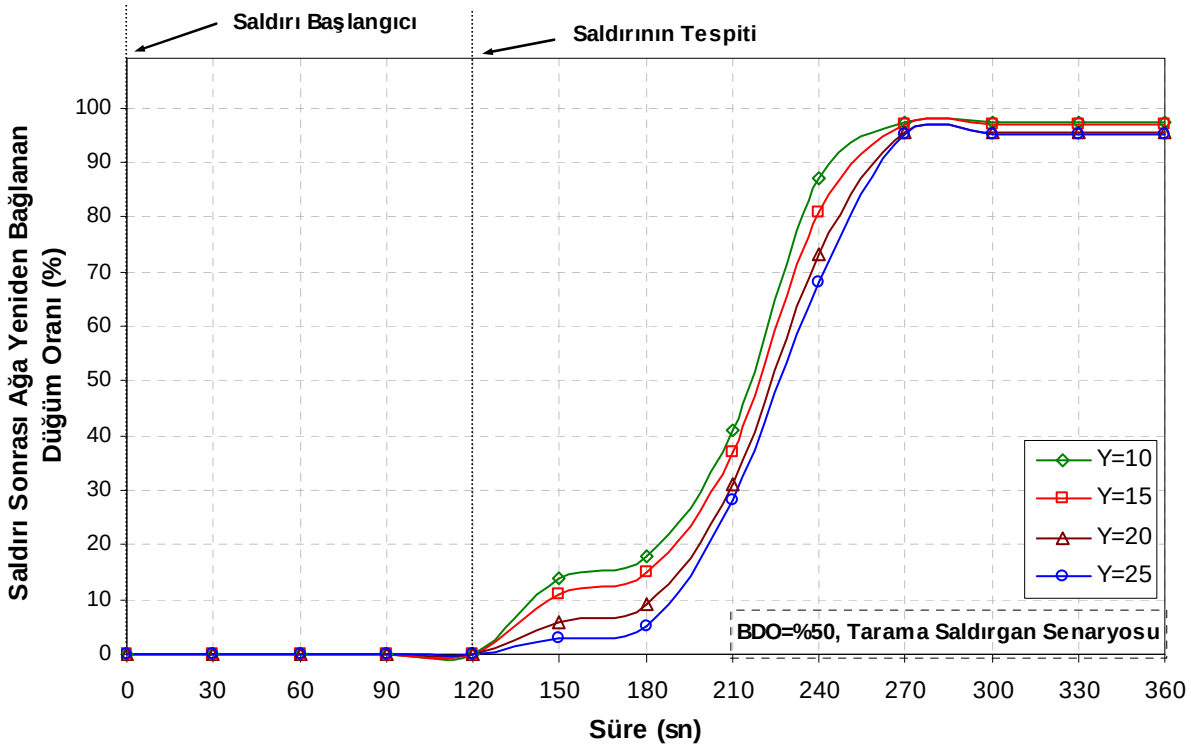


Şekil 6.10. Tek kanal frekansında çalışan saldırgan senaryoları için DKA yönteminin saldırılara verdiği cevap süresi (BDO=50)

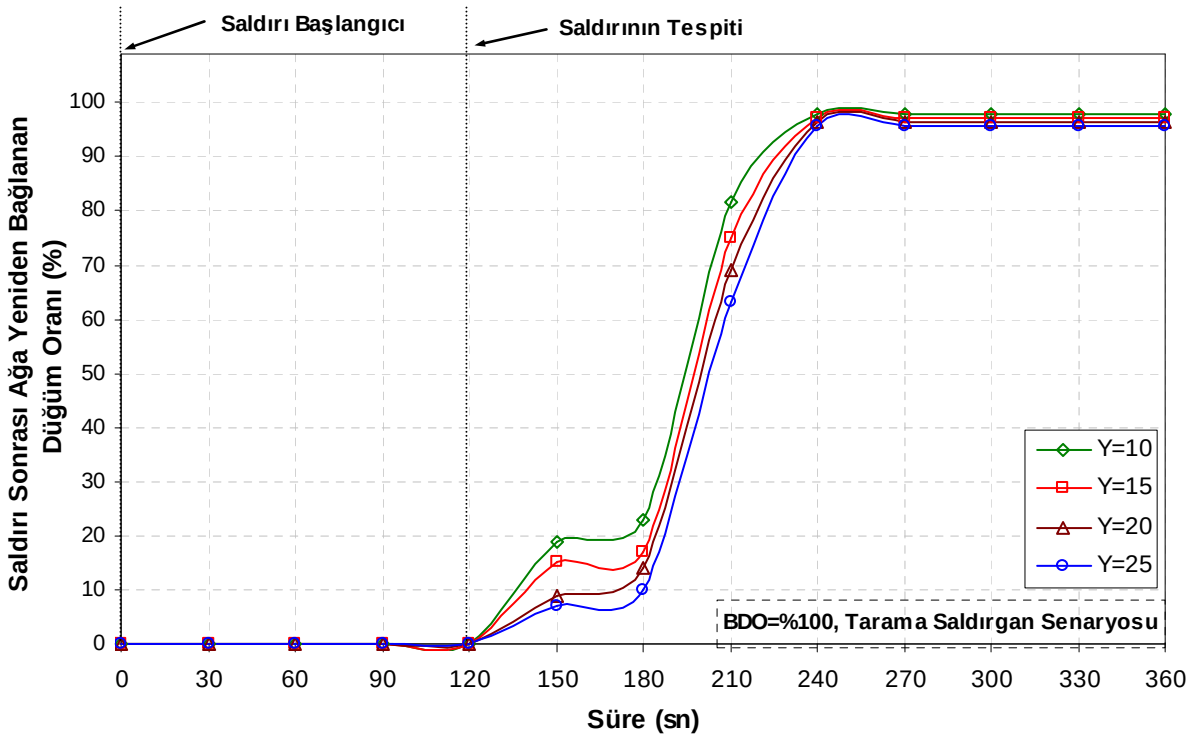


Şekil 6.11. Tek kanal frekansında çalışan saldırgan senaryoları için DKA yönteminin saldırılara verdiği cevap süresi (BDO=100)

Şekil 6.12'de DKA yönteminin farklı ağ yoğunluklarında, %50 boğulmuş düğüm oranlarında, Şekil 6.13'de ise %100 boğulmuş düğüm oranlarında ve tarama saldırgan türüne karşı verdiği cevap süreleri görülmektedir. Bu grafiklerde de Şekil 6.12 ve Şekilde 6.13'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 yaptığı test aşamasından sonra RKA metoduna başlamaları ve 1-atlama uzaklıktaki komşuları ile senkronize olmalarıdır.



Şekil 6.12. Kanallar arası çalışan saldırgan senaryosu için DKA yönteminin saldırılara verdiği cevap süresi (BDO=50)

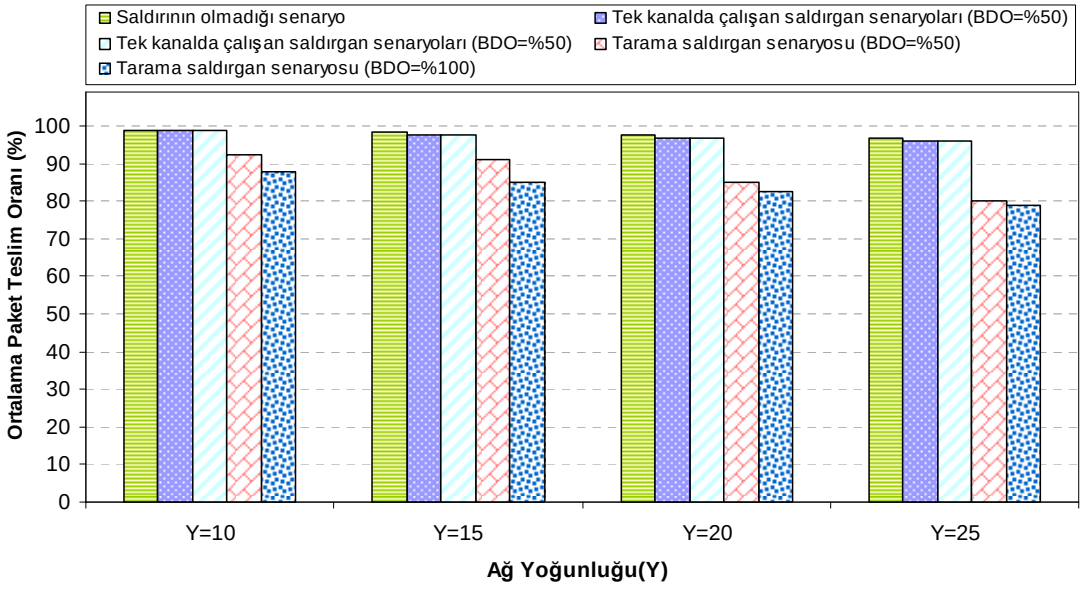


Şekil 6.13. Kanallar arası çalışan saldırgan senaryosu için DKA yönteminin saldırılara verdiği cevap süresi (BDO=100)

6.4.2. Başarım oranı

Şekil 6.14 ve Şekil 6.15'de 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 saldırganın bazı paketleri bozmasıdır. Şekillerdeki ikinci önemli nokta ise ağ yoğunluğunun artması ile DKA yönteminin tarama saldırgan senaryosundaki başarım oranın düşmesidir. Bunun sebebi, 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 6.14. Farklı ağ yoğunlukları ve boğulmuş düğüm oranlarındaki DKA yönteminin başarım oranı

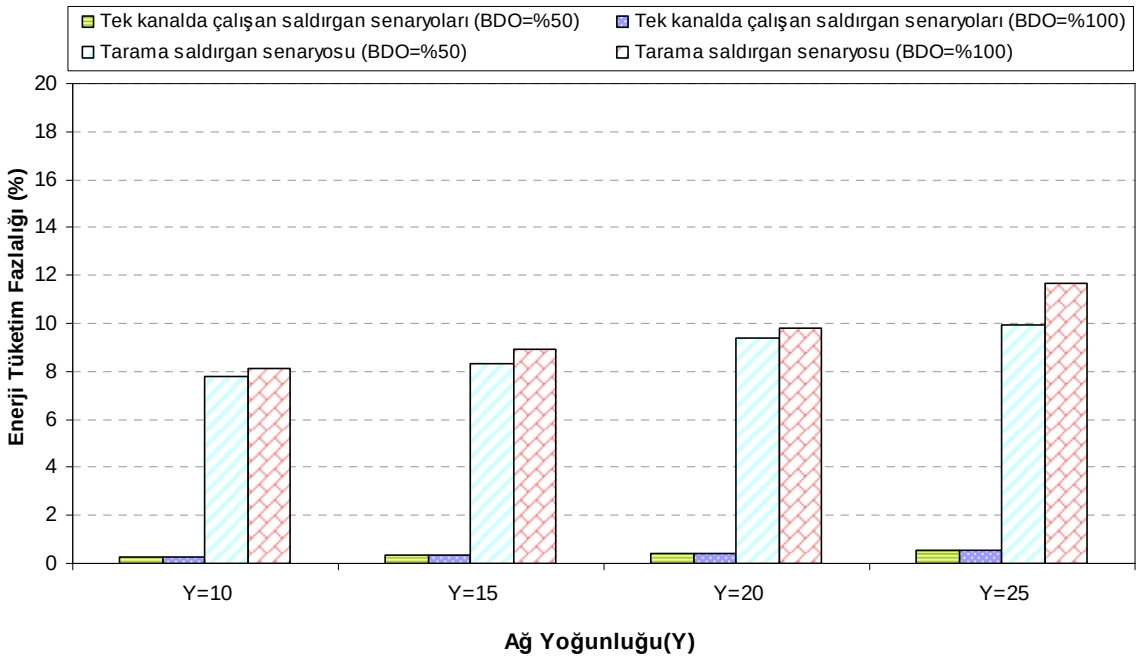
6.4.3. Enerji tüketim fazlalığı

Enerji tüketim fazlalığı, DKA yöntemi nedeniyle düğümlerin fazladan harcadığı enerji miktarını gösteren parametredir ve Formül 6.3 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.

$$Enerji\ Tüketim\ Fazlalığı = \frac{E_{Saldırı+DKA}}{E_{SaldırıYok}} \times 100 \qquad (6.3)$$

Şekil 6.15'de farklı senaryolarda bir düğümden elde edilen enerji tüketim fazlıkları görülmektedir. Şekilde dikkat edilecek 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 sebebi 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 6.15. Farklı ağ yoğunlukları ve boğulmuş düğüm oranlarındaki enerji tüketim fazlalıkları

6.5. Sonuçlar

Bu bölümde, boğma saldırılarının etkisini en az 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) metodunu kullanmaktadırlar. Geliştirilen DKA yöntemi yardımıyla düğümler oldukça kısa bir sürede (210–270 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.

BÖLÜM 7. SONUÇLAR VE DEĞERLENDİRMELER

7.1. Sonuçlar

Kaynakları kısıtlı olan kablosuz algılayıcı ağlar için *güvenlik* son derece önemli bir tasarım ölçütüdür ve güvenilir algılayıcı ağlar her türdeki saldırılara karşı dayanıklı olabilmeli, her şeye rağmen görevlerini idame ettirebilmedir. Bu çalışmada kablosuz algılayıcı ağlarının güvenliğini tehdit eden saldırılardan olan boğma saldırıları ele alınmış ve bu saldırılara karşı çözüm yöntemi geliştirilmiştir.

Tez çalışması kapsamında elde edilen sonuçların özetleri aşağıdaki gibi sıralanmıştır.

1. Literatürde var olan boğma saldırgan modellerinin etkinliklerini ve kablosuz algılayıcı ağına verdiği zararı tespit etmek için bir yöntem geliştirilmiştir.

Düşmana karşı etkin bir savunma yöntemi geliştirebilmenin ilk adımı O'nu çok iyi tanımaktan geçmektedir. Bu sebeple ilk olarak literatürdeki saldırgan modelleri benzetim metoduyla gerçeklenmiş ve bu saldırıların etkinlik süreleri ile kablosuz algılayıcı ağına verdikleri zararlar, Saldırgan Yaşam Oranı (SYO), Tüketme Oranı (TO), Paket Engelleme Oranı (PEO) ve Paket Bozma Oranı (PBO) olarak adlandırdığımız ölçütler yardımıyla ölçülmüştür. Elde edilen sayısal sonuçlara göre enerjisini en verimli kullanan saldırgan modelinin periyodik kontrol aralığı saldırganı (PKAS) olduğu anlaşılmış ve bu saldırganın normal düğümlerin yaşam süresinin %77'si (SYO=%177) oranında daha uzun yaşadığı tespit edilmiştir. Enerjisini en verimsiz kullanan saldırgan türünün ise tarama saldırganı olduğu ve bu saldırganın normal düğümlerin yaşam süresinin yaklaşık % 4.1 (SYO=%4.1) kadar yaşayabildiği belirlenmiştir. Düğümlerin enerjilerinin normal senaryolara göre ne kadar kısaldığını gösteren tüketme oranı sonuçlarına göre PKAS ve Periyodik Dinleme Aralığı Saldırganı'nın (PDAS) düğüm enerjilerinin en çabuk tükenmesine yol açan saldırgan

modelleri olduğu göze çarpmaktadır. Bu saldırganlar normal senaryolara göre düğümlerin yaşam sürelerinin yaklaşık %87 ve %85'lik oranlarında azalmasına yol açmaktadırlar. PEO ölçütlerine göre sürekli, aldatıcı ve periyodik dinleme aralığı saldırganlarının yaşadığı süre boyunca düğümlerin paket göndermelerini tamamen engellediği görülmüştür. Bununla birlikte PBO'ya göre ise reaktif, kesme, veri paketi ve küme saldırganlarının gönderilen tüm paketleri bozduğu tespit edilmiştir.

2. Literatürdeki boğma saldırgan modellerinin çeşitli doğal ağ koşullarından başarıyla ayrılmasını sağlayan yeni bir saldırı tespit sisteminin tasarımı gerçekleştirilmiştir.

Bu tez çalışmasında saldırı özelliklerinin ve etkilerinin belirlenmesinin ardından ikinci olarak saldırıların başarılı bir biçimde tespit edilmesine yönelik yöntem geliştirilmiştir. Paket Teslim Oranı (PTO), Hatalı Paket Oranı (HPO) ve Enerji Tüketim Miktarı (ETM) olarak adlandırılan parametreler yardımıyla anomali tabanlı boğma saldırı tespit sisteminin (ABSTS) tasarımı gerçekleştirilmiştir. ABSTS ile literatürdeki saldırgan modellerinin çoğu yüksek sezme oranları (>%98) ve düşük hatalı sezme oranları ile tespit edilebilmiştir (<%1). Aktivite, tarama ve darbe saldırgan senaryolarında daha düşük sezme oranları elde edilmiş olmasına rağmen bu saldırılar ağın performansında fazla bir kayba yol açmadığı için yüksek başarımla tespit edilmemeleri çok önem taşımamaktadır. Geliştirilen yöntemin bir diğer özelliği ise sisteme getirdiği ek yükün oldukça düşük olmasıdır. ABSTS'nin düğüm iletişimlerine getirdiği ek yük en fazla %12 civarındayken, enerji tüketimine getirdiği yük ise en fazla on binde 7 civarındadır.

3. Literatürdeki boğma saldırılarının çözümüne yönelik yeni bir yöntem tasarımı gerçekleştirilmiştir.

Farklı boğma saldırılarının etkisini en az indirmek ve saldırılara rağmen düğüm iletişimlerinin devam edebilmesine imkân tanımak için düğümlerin var olan kanal çeşitliliğinden faydalanmasını sağlayan Dinamik Kanal Atlama (DKA) metodu tasarlanmıştır. Geliştirilen yöntem ile 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 bu kanalda kalarak iletişimlerini devam ettirmektedir. Ancak, düğümler kanalları tarayarak saldıran bir saldırgan modeline karşı çok kısa aralıklar ile var olan kanallar arasında rasgele şekilde atlamayı öngören rasgele kanal atlama metodunu kullanmaktadır. Geliştirilen DKA yöntemi yardımıyla düğümler oldukça kısa bir süre içerisinde (210–270 sn) saldırı etkilerinden kurtulabilmektedir. Ayrıca düğümler, DKA yöntemi yardımıyla tek kanalda çalışan saldırgan senaryolarında %96 oranında, kanallar arası çalışan saldırgan senaryolarında ise %80 oranındaki bir başarımla iletişimlerini devam ettirebilmektedir. Buna ek olarak, DKA yönteminin sisteme getirdiği enerji yükü ise oldukça düşüktür. Tek kanal frekansında çalışan saldırgan durumlarında DKA yöntemi, düğümlerin enerji tüketimlerinin %0.5 oranında artmasına neden olmaktadır. Tarama saldırgan senaryosunda ise düğümlerin kanallar arasında gezmesi ve senkronizasyonun sağlanabilmesi için daha fazla paket gönderilmesi sebebiyle bu oran yaklaşık olarak %11 seviyesine kadar çıkabilmektedir. Ancak, DKA yöntemi ile düğümlerin enerji tüketimleri %11 oranında artarken ağdan beklenen görevler aksamamakta ve saldırılara rağmen düğümler iletişimlerini gerçekleştirebilmektedir.

4. Boğma saldırgan modellerinin, geliştirilen saldırı tespit sisteminin ve Dinamik Kanal Atlama metodunun gerçeklendiği OMNET++ tabanlı ücretsiz benzetim yazılımı tasarlanmıştır.

Kablosuz algılayıcı ağların tüm özellikleri içeren ve hazır modellerin bulunduğu bir ticari benzetim yazılımının henüz bulunmaması kendi benzetim yazılımımızı geliştirmemizi gerektirmiştir. OMNET++ tabanlı olan benzetim yazılımı grafiksel kullanıcı arabirim desteği ve modüler yapısı ile kablosuz algılayıcı ağlarının birçok fonksiyonun benzetilmesine olanak sağlamaktadır. Ayrıca literatürdeki boğma saldırgan modellerinin benzetim ortamında hazır olarak bulunması gelecekte bu konu üzerine çalışacak araştırmacıların işlerini oldukça kolaylaştıracaktır.

7.2. Tartışma ve Öneriler

Bu tez çalışmasında, boğma saldırılarının tespiti ve çözümüne yönelik yöntem tasarımı gerçekleştirilmiştir. Bu tezden elde edilen sonuçlar ve katkılar doğrultusunda gelecekte yapılabilecek çalışmalar şunlardır:

1. Tasarlanan saldırı tespit sisteminin ve dinamik kanal atlama metodunun performansını arttırmak için yapay zekâ tekniklerinden faydalanılabilir.

2. Geliştirdiğimiz saldırı tespit ve savunma yöntemi, hizmet engelleme saldırılarının bir alt konusu olan boğma saldırılarına yöneliktir. Gerçekleştirilen bu çalışma, boğma saldırıları da dâhil olmak üzere tüm katmanlardaki hizmet engelleme saldırılarının tespitini ve çözümünü kapsayacak şekilde genelleştirilebilir.

3. Geliştirdiğimiz saldırı tespit ve savunma yöntemi, günümüz algılayıcı düğümleri üzerinde ek bir donanıma ihtiyaç duymadan çalışabilir. Bu sebeple, benzetim yoluyla tasarlanan ABSTS ve DKA yöntemi fiziksel olarak, ticari algılayıcı düğümleri üzerinde gerçeklenebilir.

4. Şu ana kadar kablosuz algılayıcı ağlardaki boğma saldırılarına karşı geliştirilen çözüm yöntemlerinde saldırganların da normal düğümlerle aynı donanıma sahip olduğu ve aynı kısıtlamalarla karşı karşıya olduğu varsayılmaktadır. Bu tez çalışmasında da aynı kabuller söz konusudur. Literatürde henüz enerji ve donanımsal kaynak sıkıntısı olmayan boğma saldırılarına karşı bir yöntem geliştirilmemiştir. Günümüzde var olan yöntemlerin mevcut kanalları çok kısa sürede tarayan ya da aynı anda birçok kanalda yüksek güç ile yayın yapabilen saldırganlara karşı hiçbir faydası olmayacaktır. Bu sebeple güçlü boğma saldırıları ile başa çıkabilecek donanımlara sahip algılayıcı düğüm tasarımı gerçekleştirilebilir.

5. Bu tezde boğma saldırılarına karşı çözüm yöntemlerinin tasarlanması hedeflenmiştir. Ancak bu çalışmanın karşıtı bir çalışma gerçekleştirmek de mümkündür. Yani enerjisini günümüzdeki saldırgan modellerine oranla daha

verimli kullanan ve tespiti daha zor saldırgan modellerinin tasarımı gerçekleştirilebilir.

KAYNAKLAR

[1] AKYILDIZ I.F., SU W., SANKARASUBRAMANIAM Y., CAYIRCI E., Wireless Sensor Networks: A Survey, Computer Networks, Vol. 38, No. 4, pp. 393-422, March 2002.

[2] HARTUNG C., BALASALLE J., HAN R., 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] WOOD A.D., STANKOVIC J.A., Denial of service in sensor Networks, IEEE Computer, 35(10):54–62, Oct.2002

[4] KARLOF C, WAGNER D., Secure routing in wireless sensor networks attacks and countermeasures, Ad Hoc Networks 1(2-3): 293-315, 2003

[5] XU W., TRAPPE W, ZHANG Y., WOOD T., The feasibility of launching and detecting jamming attacks in wireless networks, In ACM MobiHoc ’05, page To appear. ACM Press, 2005.

[6] LAW Y., W., HARTEL P., HARTOG J., HAVINGA P., Link-layer jamming attacks on S-MAC, In 2nd European Workshop on Wireless Sensor Networks (EWSN 2005), IEEE, pages 217–225, 2005.

[7] LAW Y. W, LODEWIJK L., HOESEL V., DOUMEN J., HARTEL P, HAVINGA P., Energy-Efficient Link-Layer Jamming Attacks against Wireless Sensor Network MAC Protocols, SANS’05 Virginia, USA, November 7, 2005.

[8] WOOD A., STANKOVIC J., ZHOU G., DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks, SECON 2007, San Diego, California, USA, June 2007.

[9] WOOD A., STANKOVIC J., SON S., JAM: A jammed-area mapping service for sensor networks, In 24th IEEE Real-Time Systems Symposium, pages 286-297, 2003.

[10] XU W., WOOD T., TRAPPE W., ZHANG Y., Channel surfing and spatial retreats: defenses against wireless denial of service,” in Proceedings of the 2004 ACM workshop on Wireless security, pp. 80-89, 2004.

[11] XU W., TRAPPE W., ZHANG Y., Channel Surfing: Defending Wireless Sensor Networks from,” IPSN'07 Cambridge, Massachusetts, USA, 25-27 April 2007.

[12] CAGALJ M., CAPKUN S,. HUBAUX J.-P., Wormhole-Based Anti-Jamming Techniques in Sensor Networks, IEEE Transactions on Mobile Computing, May, 2006.

[13] www.tinyos.org, TinyOS işletim sistemi resmi web sayfası (Son ziyaret tarihi: ağustos 2008).

[14] CHONG C., KUMAR S.P., Sensor Networks: Evolution, Opportunities, and Challenges, in Proceedings of IEEE, vol.91, no.8, pp.1247-1256, 2003

[15] KOUBÂA A., ALVES M., TOVAR E., Lower Protocol Layers for Wireless Sensor Networks: A Survey, Teknik Rapor, 2005

[16] HEINZELMAN W., CHANDRAKASAN A., BALAKRISHNAN H.. Energy-efficient communication protocol for wireless microsensor networks, In Proc. 33rd Hawaii Intl. Conf. on System Sciences, January 2000.

[17] PEI G., CHIEN C., Low power TDMA in large wireless sensor networks, In Military Communications Conference (MILCOM 2001), volume 1, pages 347–351, Vienna, VA, October 2001.

[18] RAJENDRAN V., OBRACZKA K., GARCIA-LUNA-ACEVES J., Energy-efficient, collision-free medium access control for wireless sensor networks, In 1st ACM Conf. on Embedded Networked Sensor Systems (SenSys 2003), pages 181–192, Los Angeles, CA, November 2003.

[19] HOESEL L. VAN, HAVINGA P., A lightweight medium access protocol (LMAC) for wireless sensor networks, In 1st Int. Workshop on Networked Sensing Systems (INSS 2004), Tokyo, Japan, June 2004.

[20] LANGENDOEN K., HALKES G., Energy-Efficient Medium Access Control, Embedded Systems Handbook, CRC Press, 2005.

[21] DEMIRKOL I., ERSOY C., ALAGÖZ F, MAC Protocols for Wireless Sensor Networks: a Survey, IEEE Communications Magazine, vol.44, no.4, pp.115-121, April 2006.

[22] SOHRABI K., GAO J., AILAWADHI V., POTTIE G., Protocols for self-organization of a wireless sensor network, IEEE Personal Communications, 7(5):16–27, October 2000.

[23] GUO C., ZHONG L., RABAEY J., Low power distributed MAC for ad hoc sensor networks, In IEEE GlobeCom, San Antonio, AZ, November 2001.

[24] LIU B. HUA, NIRUPAMA B., PHAM H., JHA S., CSMAC: A Novel DS-CDMA Based MAC Protocol for Wireless Sensor Networks, GlobeCom, 2004

[25] KARN P., MACA-A new channel access method for packet radio, presented at the ARRL/CRRL Amateur Radio 9th Computer Networking Conf., 1990.

[26] BHARGHAVAN V., DEMERS A., SHENKER S., ZHANG L., MACAW: A media access protocol for wireless LANs, in Proc. ACM SIGCOMM Conf., vol. 24, , pp. 212–225, Aug. 1994

[27] WEI Y., HEIDEMANN J., ESTRIN D., An energy-efficient MAC protocol for wireless sensor networks, IEEE Infocom, pages 1567–1576, NY, June 2002.

[28] TIJS V. D., LANGENDOEN K, An adaptive energy-efficient MAC protocol for wireless sensor networks, In Proceedings of the First ACM Conference on Embedded Networked Sensor Systems, pages 171–180, Los Angeles, California, USA, November 2003.

[29] LU G., KRISHNAMACHARI B, RAGHAVENDRA C.S., An adaptive energy efficient and low-latency MAC for data gathering in wireless sensor networks, Proceedings of 18th International Parallel and Distributed Processing Symposium, Pages: 224, 26-30 April 2004.

[30] EL-HOIYDI A., DECOTIGNIE J. D., Wisemac: An ultra low power MAC protocol for multi-hop wireless sensor networks. In Algorithmic Aspects of Wireless Sensor Networks: First International Workshop, ALGOSENSORS 2004, Turku, Finland, July 16, 2004.

[31] POLSTRE J., HILL J., CULLER D., “Versatile low power media access for wireless sensor networks,” in ACM SENSYS 2004

[32] AL-KARAKI J. N., KAMAL A. E., Routing Techniques in Wireless Sensor Networks: A Survey, IEEE Wireless Communication, vol 11,no. 6, pp.6-28, Dec 2004.

[33] HEINZELMAN W., KULIK J., BALAKRISHNAN H., Adaptive Protocols for Information Dissemination in Wireless Sensor Networks, 5th ACM/IEEE Mobicom Conference (MobiCom '99), Seattle, WA, pp. 174-85, August, 1999.

[34] INTANAGONWIWAT C., GOVINDAN R., ESTRIN D., Directed Diffusion: a scalable and robust communication paradigm for sensor networks, Proceedings of ACM MobiCom'00, Boston, MA, pp. 56-67, 2000

[35] BRAGINSKY D., ESTRIN D., Rumor Routing Algorithm for Sensor Networks, in the Proceedings of the First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA, October 2002.

[36] SCHURGERS C., SRIVASTAVA M.B., Energy effcient routing in wireless sensor networks, in the MILCOM Proceedings on Communications for Network-Centric Operations: Creating the Information Force, McLean, VA, 2001.

[37] YE F., CHEN A., LIU S., ZHANG L., A scalable solution to minimum cost forwarding in large sensor networks, Proceedings of the tenth International Conference on Computer Communications and Networks (ICCCN), pp. 304-309, 2001

[38] CHU M., HAUSSECKER H., ZHAO F., Scalable Information-Driven Sensor Querying and Routing for ad hoc Heterogeneous Sensor Networks, The International Journal of High Performance Computing Applications, Vol. 16, No. 3, August 2002.

[39] YAO Y., GEHRKE J., The cougar approach to in-network query processing in sensor networks, in SIGMOD Record, Volume 31, Issue 3, September 2002.

[40] SADAGOPAN N. ET AL., The ACQUIRE mechanism for efficient querying in sensor networks, in the Proceedings of the First International Workshop on Sensor Network Protocol and Applications, Anchorage, Alaska, May 2003.

[41] SHAH R. C., RABAEY J., Energy Aware Routing for Low Energy Ad Hoc Sensor Networks", IEEE Wireless Communications and Networking Conference (WCNC), Orlando, FL., March 17-21, 2002.

[42] HEINZELMAN W., CHANDRAKASAN A., BALAKRISHNAN H., Energy-Efficient Communication Protocol for Wireless Microsensor Networks," Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS '00), January 2000.

[43] MANJESHWAR A., AGARWAL D. P., TEEN: a routing protocol for enhanced efficiency in wireless sensor networks, In 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, April 2001.

[44] MANJESHWAR A., AGARWAL D. P., APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks, Parallel and Distributed Processing Symposium, Proceedings International, pp. 195-202, IPDPS 2002.

[45] LINDSEY S., RAGHAVENDRA C., PEGASIS: Power-Efficient Gathering in Sensor Information Systems, IEEE Aerospace Conference Proceedings, Vol. 3, 9-16 pp. 1125-1130, 2002.

[46] RODOPLU V., MENG T. H., Minimum Energy Mobile Wireless Networks, IEEE Journal Selected Areas in Communications, vol. 17, no. 8, pp. 1333-1344, Aug. 1999.

[47] SUBRAMANIAN L., KATZ R. H., An Architecture for Building Self Configurable Systems, in the Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing, Boston, MA, August 2000.

[48] LI Q., ASLAM J., RUS D., Hierarchical Power-aware Routing in Sensor Networks", In Proceedings of the DIMACS Workshop on Pervasive Networking, May, 2001.

[49] FANG Q., ZHAO F., GUIBAS L., Lightweight Sensing and Communication Protocols for Target Enumeration and Aggregation, Proceedings of the 4th ACM international symposium on Mobile ad hoc networking and computing (MOBIHOC), pp. 165-176, 2003.

[50] JAMAL N., RAZA UL-MUSTAFA, KAMAL AHMED E., Data Aggregation in Wireless Sensor Networks-Exact and Approximate Algorithms, Proceedings of IEEE Workshop on High Performance Switching and Routing (HPSR), Phoenix, Arizona, USA, April 18-21, 2004.

[51] YE F., LUO H., CHENG J., LU S., ZHANG L., A Two-tier data dissemination model for large-scale wireless sensor networks, proceedings of ACM/IEEE MOBICOM, 2002.

[52] XU Y., HEIDEMANN J., ESTRIN D., Geography-informed Energy Conservation for Ad-hoc Routing," In Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking pp. 70-84, 2001.

[53] YU Y., ESTRIN D., GOVINDAN R., Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks", UCLA Computer Science Department Technical Report, UCLA-CSD TR-01-0023, May 2001.

[54] CHEN B., JAMIESON K., BALAKRISHNAN H., MORRIS R., SPAN: an energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks, Wireless Networks, Vol. 8, No. 5, Page(s): 481-494, September 2002.

[55] STOJMENOVIC I., LIN X.. GEDIR: Loop-Free Location Based Routing in Wireless Networks, In International Conference on Parallel and Distributed Computing and Systems, Boston, MA, USA, Nov. 3-6, 1999.

[56] KUHN F.,. WATTENHOFER R, ZOLLINGER A., Worst-Case optimal and average-case efficient geometric ad-hoc routing", Proceedings of the 4th ACM International Conference on Mobile Computing and Networking, Pages: 267-278, 2003.

[57] SOHRABI K., POTTIE J., Protocols for self-organization of a wireless sensor network, IEEE Personal Communications, Volume 7, Issue 5, pp 16-27, 2000.

[58] T. HE ET AL, SPEED: A stateless protocol for real-time communication in sensor networks", in the Proceedings of International Conference on Distributed Computing Systems, Providence, RI, May 2003.

[59] ROMER K., MATTERN F.. The design space of wireless sensor networks, In IEEE Wireless Communications, volume 11, pages 54 – 61. ETH Zurich, Switzerland, December 2004.

[60] R.C. JOHNSON., Sandia enlists MEMS for anti-terror systems." EE Times, March 2002. URL http://www.eet.com/at/

[61] http://www-rtsl.cs.uiuc.edu/muri, (Son ziyaret tarihi: Ağustos 2008)

[62] http://fiji.eecs.harvard.edu/CodeBlue, (Son ziyaret tarihi: Ağustos 2008)

[63] MAINWARING A., CULLER D., POLASTRE J., SZEWCZYK R., ANDERSON J., Wireless sensor networks for habitat monitoring, Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, p. 88–97. ACM Press, 2002. ISBN 1-58113-589-0.

[64] CERPA A., ELSON J., HAMILTON M., ZHAO J., Habitat monitoring: application driver for wireless communications technology, ACM SIGCOMM'2000, Costa Rica, April 2001.

[65] http://www.alertsystems.org, (Son ziyaret tarihi: Ağustos 2008)

[66] GEOFFREY W.A, WELSH M., JOHNSON J., RUIZ M., JONATHAN L., Monitoring volcanic eruptions with a wireless sensor network, Technical Report 27-04, Harvard University, 2004.

[67] KLOEPPEL DJ., Smart bricks could monitor buildings, save lives, News Bureau, University of Illinois at Urbana-Champaign, URL http://www.news.uiuc.edu/scitips/03/0612smartbricks.html (Son ziyaret tarihi: Ağustos 2008)

[68] RUPPE D., Nations to discuss using nuclear test sensors as tsunami warning system. Global Security Newswire, January 2005. URL http://www.nti.org/d_newswire/issues/print.asp?story_id=5FDDA53C-7385-41B0-A0D5-47652595F5CE

[69] RABAEY J., ARENS E., FEDERSPIEL C., GADGIL A., MESSERSCHMITT D., NAZAROFF W., PISTER K.,. OREN S, VARAIYA P., Smart energy distribution and consumption: Information technology as an enabling force, http://bwrc.eecs.berkeley.edu/Publications/2001/samrt_energy_dist_consump/SmartEnergy.pdf

[70] KNOTT T., Smart surrogates. Frontiers, 9, April 2004. URL http://www.bp.com/liveassets/bp_internet/globalbp/STAGING/global_assets/images/fr/downloads/Frontiers_magazine_issue_09_smart_surrogates.pdf

[71] CATLIN W., ECCLES L., MALCHODI L., Smart sensor project takes flight – boeing 'pressure belt' to measure airplane wing stress. InTech, May 2002, http://www.isa.org/Content/ContentGroups/InTech2/Features/20023/May6/20020531.pdf.

[72] WALTERS JOHN P., ZHENGQIANG L., WEISONG S, CHAUDHARY W, Wireless Sensor Network Security: A Survey, Security in Distributed, Grid, and Pervasive Computing, Auerbach Publications, CRC Press.2006

[73] WOOD A., STANKOVIC J., A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks, IEEE Computer, 35(10): 54-62, October 2002

[74] GANESAN D., GOVINDAN R., SHENKER S., ESTRIN D., Highly-resilient, energy-efficient multipath routing in wireless sensor networks, Mobile Computing and Communications Review, 4(5), October 2001

[75] YU B., XIAO B., Detecting selective forwarding attacks in wireless sensor networks, Proceedings of the Second International Workshop on Security in Systems and Networks (IPDPS 2006 Workshop), pp. 1-8., 2006,

[76] DOUCEUR J.R., The Sybil attack, In Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS), LNCS, pages 251-260, March 2002

[77] NEWSOME J., SHI E., SONG D., PERRIG A., The sybil attack in sensor networks: analysis & defenses, In Proceedings of the third international symposium on Information processing in sensor networks, pages 259–268. ACM Press, 2004.

[78] www.omnetpp.org, Ayrık olay tabanlı benzetim yazılımı resmi web sayfası. (Son ziyaret tarihi: Eylül 2008)

[79] http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/MICA2_Datasheet.pdf, MICA2 çalışma sayfası, (Son ziyaret tarihi: Eylül 2008)

[80] CHEBROLU S, ABRAHAM, THOMAS J., "Feature deduction and ensemble design of intrusion detection systems", Computers & Security, 24, 295-307, 2005

[81] LOO C. E., NG M. Y., LECKIE C, PALANISWAMI M., Intrusion detection for routing attacks in sensor networks, International Journal of Distributed Sensor Networks, Volume 2, Issue 4 December 2006

[82] ILKER O., MIRI ALI, Detection An Intrusion Detection System for Wireless Sensor Networks, in Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMOB), Montreal, Canada, Volume 3, pp. 253–259. August 2005,

[83] WENLIANG D., FANG L., NING P., LAD: Localization Anomaly Detection for Wireless Sensor Networks, in Proceedings of the 19th IEEE International Parallel & Distributed Processing Symposium (IPDPS '05), April 2005.

[84] ZHAO J., GOVINDAN R., Understanding packet delivery performance in dense wireless sensor networks, In Proceedings of the First ACM SenSys, Nov. 2003.

[85] CC1000, Düşük güçlü RF Alıcı/Verici Kullanım Kılavuzu, Chipcon. http://focus.ti.com/lit/ds/symlink/cc1000.pdf, (Son ziyaret tarihi: Eylül 2008)

[86] LIN EN-YI A., RABAEY JAN M., WOLISZ A., Power-Efficient Rendez-vous Schemes for Dense Wireless Sensor Networks, In Proceedings of ICC 2004, Paris, France

[87] SO H. W., NGUYEN G., WALRAND J., Practical synchronization techniques for multi-channel MAC, In MobiCom '06: Proceedings of the he Twelfth Annual International Conference on Mobile Computing and Networking, New York, ACM Press, 2006.

[88] SUN K., NING P., WANG C., TinySeRSync: secure and resilient time synchronization in wireless sensor networks," in Proc. of CCS, pp. 264–277, 2006.

[89] BAYILMIŞ C., IEEE 802.11b KLAN Kullanarak CAN Segmentleri Genişleten Arabağlaşım Birimi Tasarımı, Doktora Tezi, Kocaeli Üniversitesi Fen Bilimleri Enstitüsü, 2006.

[90] EKİZ H., Design, Implementation, and Performance Analysis of CAN/CAN and CAN/Ethernet Bridges", Doktora Tezi, University of Sussex, Brighton, İngiltere, 1997.

[91] ERTÜRK İ., Internetworking Between ATM LANs and Legacy LANs Over ATM Networks, Doktora Tezi, Sussex University, The School of Engineering and Information Technology, İngiltere, 2000.

[92] OPNET, OPNET Modeler 11.5 Documentation, OPNET Technologies, Release 11.5, 2006.

[93] SCALABLE NETWORKS, Qualnet user manual, http://www.scalable-networks.com, (Son ziyaret tarihi: Eylül 2008)

[94] THE NETWORK SIMULATOR, ns-2, http://www.isi.edu/nsnam/ns, (Son ziyaret tarihi: Eylül 2008)

[95] LEVIS P., LEE N., WELSH M., CULLER D., TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications, Proceedings of SenSys'03, First ACM Conference on Embedded Networked Sensor Systems, 2003.

[96] SOH. S. , WALRAND W, JEONGHOON J. MO, McMAC: A Parallel Rendezvous Multi-Channel MAC Protocol, IEEE Wireless Communications and Networking Conference, 2007,WCNC 2007, 11-15 March 2007

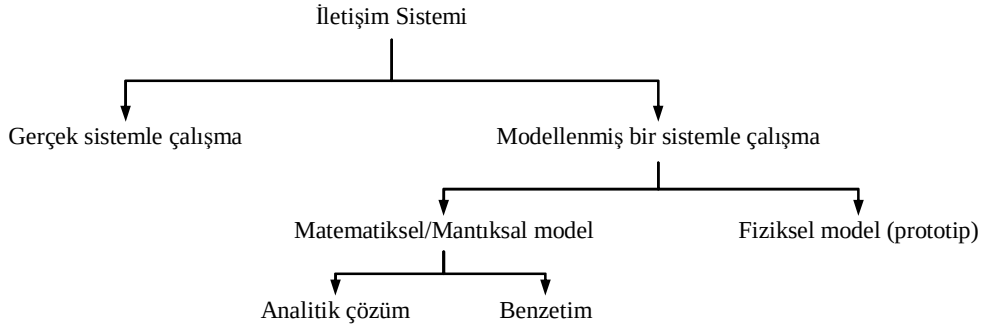
[97] POLASTRE J., A Unifying Link Abstraction for Wireless Sensor Networks, Doktora Tezi, University of California, Berkeley, A.B.D., 2005

EKLER

Ek A. Modelleme ve Benzetim Ortamının Tanıtımı

A.1. Giriş

Tasarımcılar ve araştırmacılar, bir sistemi gerçekleştirmeden önce daha ucuz yöntemlerle sistemin çalışırlığını ve yeterliliğini ortaya koyarlar. Karmaşık yapıya sahip iletişim sistemlerinde, başta kullanıcı davranışları, iletişim ortamının doğası ve toleranslar olmak üzere başarımı etkileyen pek çok sebep vardır. İletişim sistemlerinin başarım analizi, gerçek bir sistem ya da modellenmiş eşleniğinin kullanılması ile elde edilebilir (
Şekil **A.1**). Bir sistemi modellemek için üç farklı yöntem kullanılır. Bunlar; fiziksel model ya da prototip, analitik çözüm ve benzetim (simülasyon) yöntemleridir [90].



Şekil A.1. İletişim sistemleri geliştirmede kullanılan yöntemler

Fiziksel model yönteminde başarım, mevcut sistem ya da sistemin prototipi değişik koşullar altında incelenerek elde edilebilir. Fiziksel model, en güvenilir ve en doğru yöntem olmasına rağmen, özellikle karmaşık iletişim sistemleri için planlama ve tasarım aşamaları gibi çeşitli konfigürasyonların denenmesinin zorunlu olduğu birçok durumda gerçekleştirilmesi oldukça zordur. Prototip ya da gerçek bir sistemle çalışma pratik olmayan yüksek maliyet ve uzun zaman gerektiren bir yöntemdir.

Analitik model, diğer yöntemler arasında basitlik avantajına sahiptir ve genellikle basitleştirilmiş varsayımlar ve ideal kabuller üzerine kurulur. Bu yüzden kesin sonuçlar istendiğinde analitik modeli oluşturmak karmaşıklık ve zaman tüketimi açısından sistemin prototipini oluşturmak kadar zordur. Sistem modellemek için kullanılan bir diğer yöntem de benzetimdir. Benzetim somut anlamda belirli bir nesnenin modeli ya da temsilidir. Bir diğer ifadeyle benzetim, gerçek sistemin modelinin tasarımı ve bu model ile amacına yönelik olarak sistemin işletilmesi, sistemin davranışını anlayabilmek veya değişik stratejileri değerlendirebilmek için deneyler yürütülmesi sürecidir. Benzetimin sayısal ortamda bilgisayarla gerçekleştirilmesi ise bilgisayar benzetimi olarak adlandırılır. Bir sistemi modellemek için kullanılan yöntemler karşılaştırıldığında sayısal veri haberleşme ağlarının başarım analizinde olay tabanlı (event-driven) bilgisayar benzetimi en iyi çözüm olarak görülmektedir [91,92].

Bu tez çalışmasında kablosuz algılayıcı ağlarında boğma saldırılarına yönelik olarak geliştirilen saldırı tespit sistemi ve saldırı çözüm yöntemlerinin başarım analizi için bilgisayar destekli benzetim metodu kullanılmaktadır. Bu bölümde tasarlanan yöntemlerin bilgisayar tabanlı benzetimlerinin gerçekleştirilebilmesi için geliştirilen benzetim ortamının detayları hakkında bilgi verilmektedir.

A.2. Benzetim ortamının seçimi

Kablosuz algılayıcı ağlarda donanımsal ve yazılımsal olarak henüz bir standartlaşmanın gerçekleştirilmemesi popüler birçok benzetim yazılımının KAA'lara yönelik hazır model ve protokol desteği bulunmamasına sebep olmaktadır. Dolayısıyla kablosuz algılayıcı ağlar için geliştirilen protokol, yöntem ya da algoritmaların modellenmesi ve benzetimlerinin gerçekleştirilmesi oldukça güçtür.

Bu tez çalışmasında kablosuz algılayıcı ağlara yönelik olarak tasarlanan yöntemlerin başarım analizinin gerçekleştirilmesinde kullanılacak olan benzetim yazılımını belirleyebilmek için popüler benzetim yazılımları arasında bir araştırma gerçekleştirilmiş ve araştıramadan elde edilen sonuçlar Tablo A.1'de verilmiştir. OPNET [93] ve QUALNET [94] yazılımları, detaylı kütüphanelere sahip olması ve

kullanım kolaylığı sebebiyle kablosuz algılayıcı ağlarının modellenmesi ve benzetimi için oldukça uygundur. Ancak bu yazılımların yüksek maliyetlerinin olması en büyük dezavantajlarıdır. Network Simulator (NS) [95], akademik amaçlı olarak en yaygın kullanılan benzetim yazılımı olmasına karşın kullanımının zor ve ölçeklenebilirliğinin düşük olması sebebiyle bu tez çalışmasında tercih edilmemiştir. TOSSIM [96], diğerlerinden farklı olarak sadece kablosuz algılayıcı ağlarının benzetimine yönelik bir yazılımdır. Çok daha gerçekçi modelleme imkânı tanıyan TOSSIM yazılımında uygulama geliştirmek oldukça zor ve benzetim hızı diğer yazılımlara göre son derece düşüktür. OMNET++, son derece esnek yapısıyla modüler programlamaya olanak tanıması, gelişmiş kullanıcı arabirim desteğinin bulunması, zengin dokümantasyon kaynaklarına sahip olması ve ücretsiz olması gibi birçok nedenden dolayı bu tez çalışmasındaki önerilen yöntemlerin başarım analizinin gerçekleştirilmesinde kullanılan benzetim yazılımı olmuştur.

Tablo A.1. Yaygın olarak kullanılan benzetim yazılımları ve özellikleri

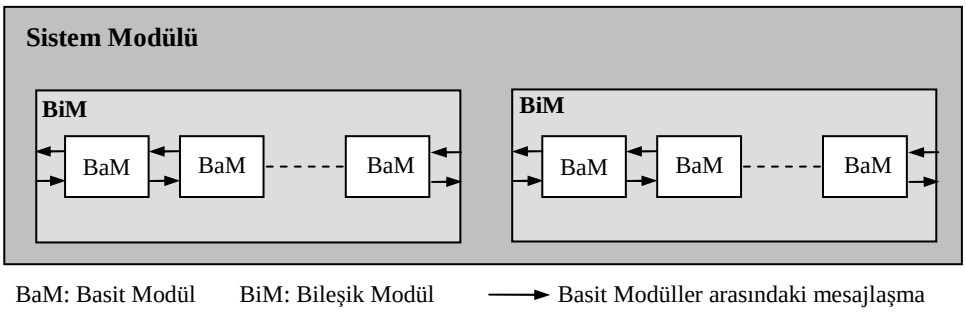
Özellik	**OPNET**	**QUALNET**	**NS**	**OMNET**	**TOSSIM**
Amaç	Genel amaçlı ağ benzeticisi	Genel amaçlı ağ benzeticisi	Genel amaçlı ağ benzeticisi	Genel amaçlı ağ benzeticisi	KAA Benzeticisi
Lisans	Ticari	Ticari	Ücretsiz	Ücretsiz	Ücretsiz
Kullanım Kolaylığı	Çok iyi	Çok iyi	Zor	İyi	Çok Zor
Esneklik	İyi	İyi	Orta	Çok İyi	Kötü
Kullanıcı Arabirimi	Güçlü GUI	Güçlü GUI	Yetersiz GUI	Güçlü GUI	Yok
Paralel Çalışabilme	Var	Var	Var (PDNS)	Var	Yok
Ölçeklenebilirlik	Orta	Çok İyi	Orta	İyi	Kötü
Programlama Dili	C++	C++	C++ ve OTcl	C++	NesC
Dokümantasyon	Çok İyi	İyi	İyi	İyi	Orta
Kütüphane	Çok İyi	Çok İyi	İyi	Orta	Orta
Hız	Kötü	Orta	Orta	İyi	Kötü

A.3. OMNET++ benzetim yazılımı

OMNET++ (Objective Modular Network Testbed in C++), nesneye-yönelik (object-oriented) modüler bir ayrık olay ağ benzeticisidir ve bu yazılım aşağıda maddeler halinde verilen süreçlerin benzetiminde kullanılabilmektedir.

- Haberleşme trafiğinin modellenmesi
- İletişim protokollerinin modellemesi
- Çok işlemcili ve diğer dağıtık donanım sistemlerini modelleme
- Donanım yapılarının incelemesi
- Karmaşık sistemlerin başarım analizlerinin değerlendirilmesi
- Ayrık olay yaklaşımının elverişli olduğu diğer sistemlerin modellemesi.

OMNeT++ yazılımda bir ağ modeli, Şekil A.2'de görüldüğü gibi iç içe geçmiş modüllerin birleşiminden meydana gelmektedir. En üst seviyedeki modül, sistem modülü ya da ağ olarak isimlendirilir. İç içe geçen modüllerin derinliği kullanıcıya bağlıdır ve bu sayede karmaşık sistemlerin modelleri kolaylıkla gerçekleştirilebilir. Modüller, basit ve bileşik olmak üzere iki kategoriye ayrılmaktadır. Bir basit modül, modellenmek istenen parçanın davranışlarını tanımlayan C++ dosyasıyla ilişkilendirilir ve bu dosya kullanıcı tarafından OMNET++ benzetim sınıf kütüphaneleri kullanılarak yazılmaktadır. Bileşik modüller ise basit modüllerin birleşiminden meydana gelmektedir ve doğrudan bir C++ dosyasıyla ilişkili değillerdir. Modüller kendi aralarından mesajlar yardımıyla haberleşmekte ve benzetim zamanı, bir modül kendisinden veya başka bir modülden mesaj aldığında ilerlemektedir. OMNET++, zamanlama işlemlerini "self message" adı verilen ve düğümün kendisine gönderdiği mesajlar yardımıyla gerçekleştirmektedir. Modüllerin yapısı ve arabirimleri, Ağ Tanımlama Dili (Network Description Languages – NED) ile oluşturulmakta ve benzetim parametreleri bir başlangıç dosyası (.ini) ile kolaylıkla ayarlanabilmektedir.



Şekil A.2. OMNET++ modül yapısı

C++ ve Tcl/Tk dili ile yazılmış olan OMNET++ benzetim yazılımının avantajları şunlardır;

- Taşınabilir kod üretimi: DOS, UNIX ve Windows üzerinde, oluşturulan kodlar platformdan bağımsız olarak çalışabilmektedir.
- Bazı görsel kullanıcı arabirim desteği ile kolay hata-ayıklamaya (debugging) ve değişkenlerin denetimine imkân verir.
- Benzetim sonuçlarının şekillerinin vektörel ve sayısal olarak çizilmesine olanak sağlayan grafik programları mevcuttur.
- Paralel yürütme ve çoklu işlemci ile çalışma desteği bulunmaktadır.
- Gelişmiş bir benzetim kütüphanesine sahiptir; Rasgele sayı üreteçleri, İstatistiksel fonksiyonlar, yoğunluk tahmin fonksiyonları, yönlendirme ve topoloji desteği v.b.
- Benzetimler "ini" uzantılı bir dosya kullanarak kolayca yapılandırılabilir.
- Bir benzetimin farklı parametreler ile çalıştırılabilmesini desteklemektedir. Toplu çalıştırma (batch executing) desteği sayesinde tek bir dosya ile arka arkaya birçok benzetimin gerçekleştirilebilmesine ve sonuçların toplanmasına olanak sağlar.
- Benzetilecek olan tüm nesneler (modüller, kapılar ve bağlantılar) statik ya da dinamik olarak oluşturulabilmektedir. Statik oluşumda nesneler yapılandırma dosyası yardımıyla benzetim başlangıcında meydana getirilirken, dinamik oluşturmada benzetim sırasında gerektiğinde meydana getirilmektedir.
- Ücretsiz bir yazılımdır ve zengin dokümantasyon desteği bulunmaktadır.

A.3.1. OMNET++ bileşenleri

OMNET++ benzetim yazılımı, benzetimlerin gerçekleştirilmesi, benzetimler sırasında meydana gelebilecek hataların ayıklaması ve elde edilen sonuçların analizi için aşağıda maddeler halinde listelenen arabirimlere/bileşenlere sahiptir.

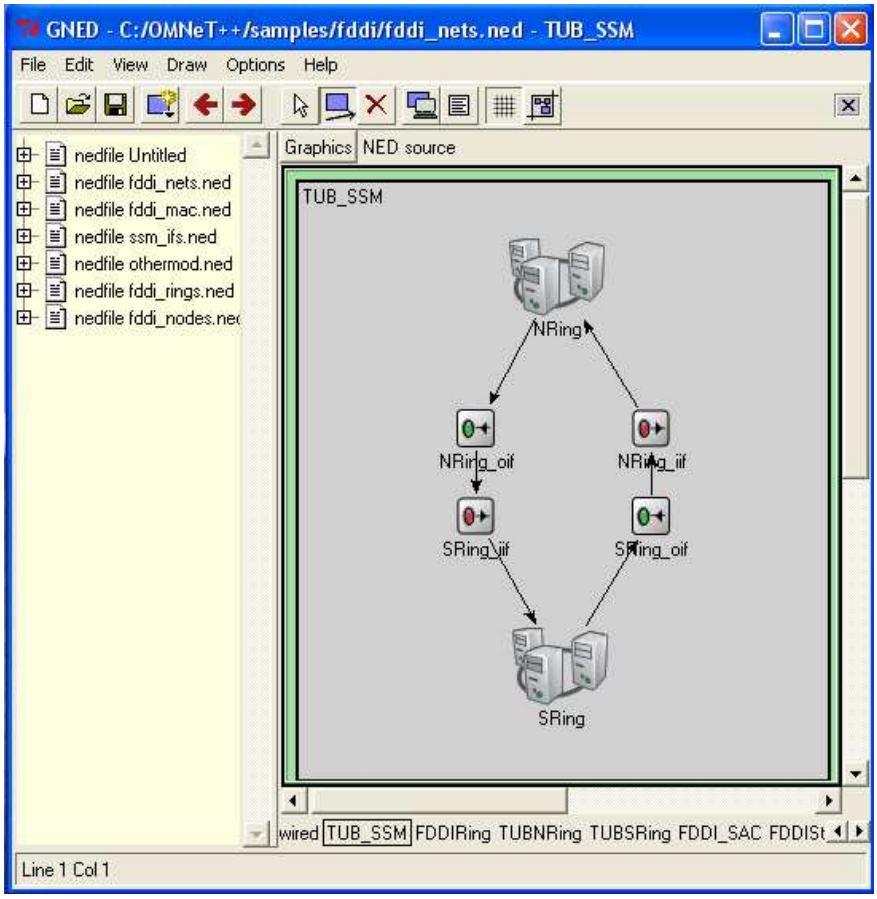
- Gelişmiş Benzetim Kütüphanesi
- Topoloji tanımlama dili (NED) için derleyici (nedc)
- Topoloji tanımlamaya yönelik grafiksel ağ editörü (GNED)

- Benzetimlerin çalıştırılması, hızlı veya yavaş koşturulması, benzetimlerdeki değişkenlerin ve parametrelerin izlenmesine olanak sağlayan kullanıcı arabirimi (Tkenv)
- Benzetimleri görsellik olmadan hızlı bir şekilde çalıştırmaya olanak sağlayan komut satırlı kullanıcı arabirimi (Cmdenv)
- Vektörel ve sayısal olarak saklanan benzetim çıktılarını grafiksel olarak göstermeye yarayan çizim araçları (Plove ve Scalar)
- Rasgele sayı üreteçlerinde kullanılan çekirdeklerin üretilmesine yönelik ve otomatik derleme dosyalarının oluşturulmasını sağlayan araçlar.
- Örnek benzetimler, detaylı kullanıcı el kitabı.
- Hazır benzetim modelleri

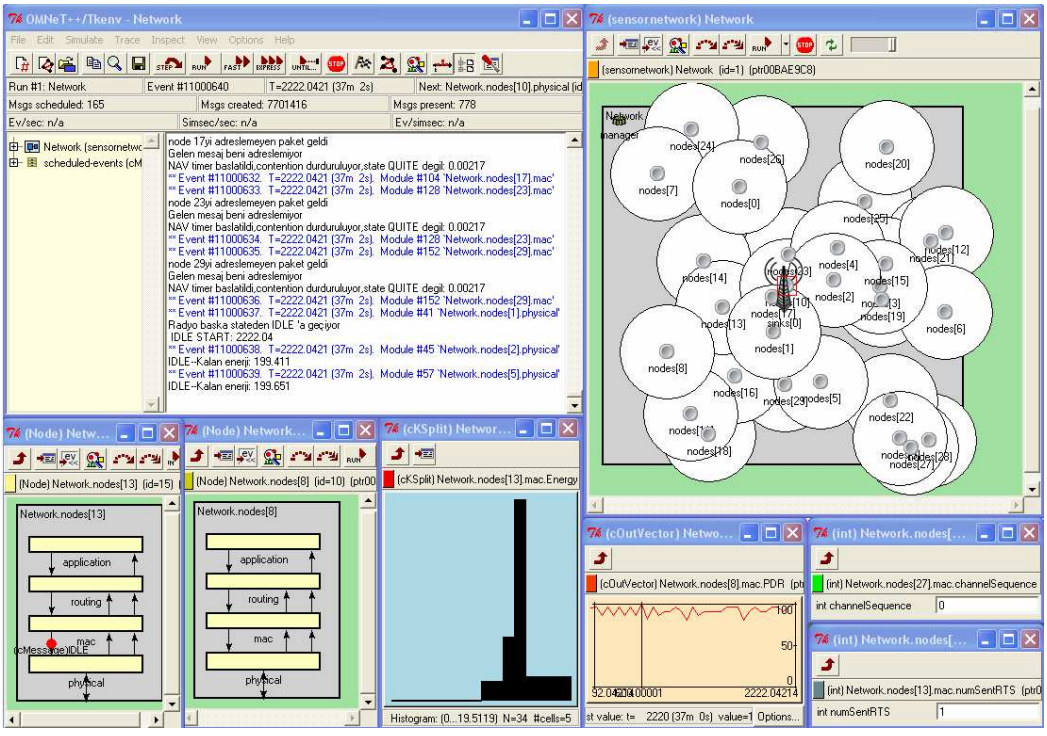
Gelişmiş Benzetim Kütüphanesi: OMNET++, mesajların gönderilmesi, alınması, zamanlamaların gerçekleştirilmesi, iletişim kanalının tanımlanması, paralel çalıştırma işlemlerinin yürütülmesi gibi işlemlerin gerçeklenmesini sağlayan çok çeşitli kütüphanelere sahiptir.

Topoloji Tanımlama Dili, Derleyicisi ve Grafik Arabirimi: NED (NEtwork Description- Ağ tanımlama), OMNET++ benzetim yazılımının topoloji tanımlama dilidir. Basit bir komut yapısı olmasına karşın oldukça güçlüdür. GNED ise Şekil A.3'de görüldüğü gibi ağ topolojisini görsel bir şekilde oluşturmayı sağlayan grafik arabirimidir. Bu grafik arabirim otomatik olarak topoloji tanımlama kodlarını oluşturmaktadır.

Görsel Kullanıcı Arabirimi (TkEnv): TkEnv, OMNET++ benzetim yazılımının taşınabilir ve görsel kullanıcı arabirimidir. Şekil A.4'de görüldüğü gibi benzetimlerdeki ağ topolojisinin, düğümlerin, paket animasyonlarının, modeller içerisindeki çeşitli değişkenlerin izlenebilmesine olanak sağlayan ve hata ayıklama işlemlerini kolaylaştıran etkileşimli bir arayüzdür.

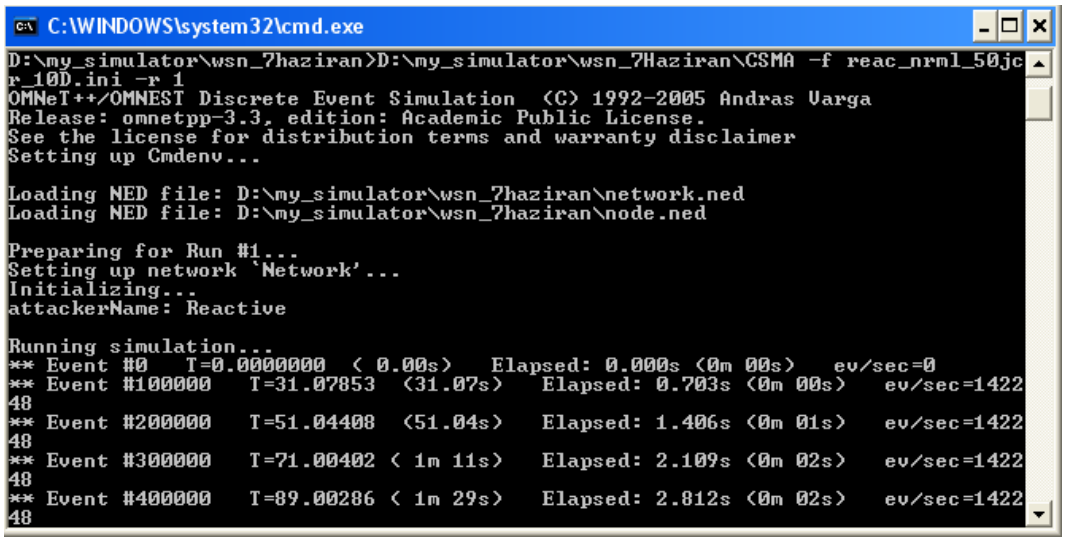


Şekil A.3. Ağ topolojisi oluşturmak için kullanılan grafik arabirimi (GNED)



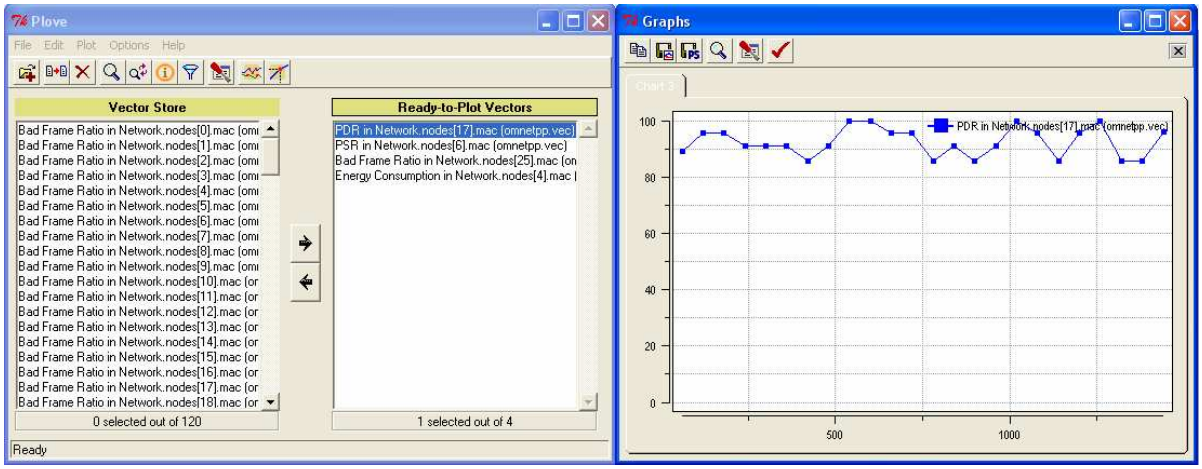
Şekil A.4. Grafiksel kullanıcı arabirimi (TkEnv)

Komut Satırlı Kullanıcı Arabirimi: CmdEnv, TkEnv'taki gibi grafiksel denetim ve izleme araçlarını içermeyen komut satırlı kullanıcı arabirimidir. Grafiksel öğeler ve animasyonlar olmadan benzetimin gerçekleştirmesine olanak sağladığı için çok daha hızlı benzetim imkânı tanımaktadır. Bir benzetim hem TkEnv ortamında hem de CmdEnv ortamında kolaylıkla çalıştırılabilmektedir ve bu seçim kullanıcının inisiyatifine bırakılmıştır. Şekil A.5'de bir CmdEnv ortamının örneği görülmektedir.

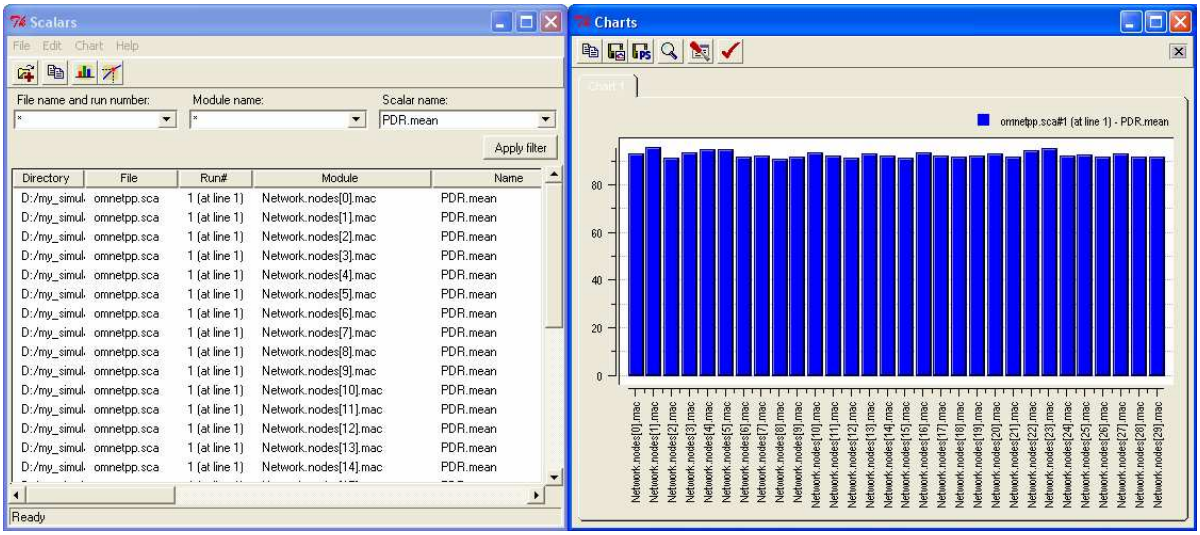


Şekil A.5. Komut Satırlı Kullanıcı Arabirimi (CmdEnv)

Vektörel ve Sayısal Çizim Araçları: OMNET++, benzetim sonuçlarını *.vec* ve *.sca* uzantılı dosyalarda saklar ve bu dosyalar *Plove* ve *Scalar* isimli araçlar sayesinden grafik haline çevrilebilir. Şekil A.6'da *Plove*, Şekil A.7'de ise *Scalar* çizim araçlarının bir ekran görüntüsü görülmektedir.



Şekil A.6. Vektörel çizim aracı (Plove)



Şekil A.7. Sayısal çizim aracı (Scalar)

Çeşitli Araçlar ve Dokümantasyon: OMNET++ kolaylıkla kullanılabilen rasgele sayı üreteçlerine sahiptir ve bu sayı üreteçlerinde kullanılan çekirdeklerin üretilmesini sağlayan çekirdek üretim aracı bulunmaktadır (seedtool). Buna ek olarak oluşturulan benzetim modellerinin otomatik olarak derlenmesine imkân tanıyan derleme araçları bulunmaktadır. OMNET++ bunların yanında güçlü bir dokümantasyon desteği sunmaktadır. Kapsamlı bir kullanıcı el kitabı, çeşitli örnek benzetimler ve forum sayfa desteği ile kullanıcılara büyük kolaylıklar sağlamaktadır.

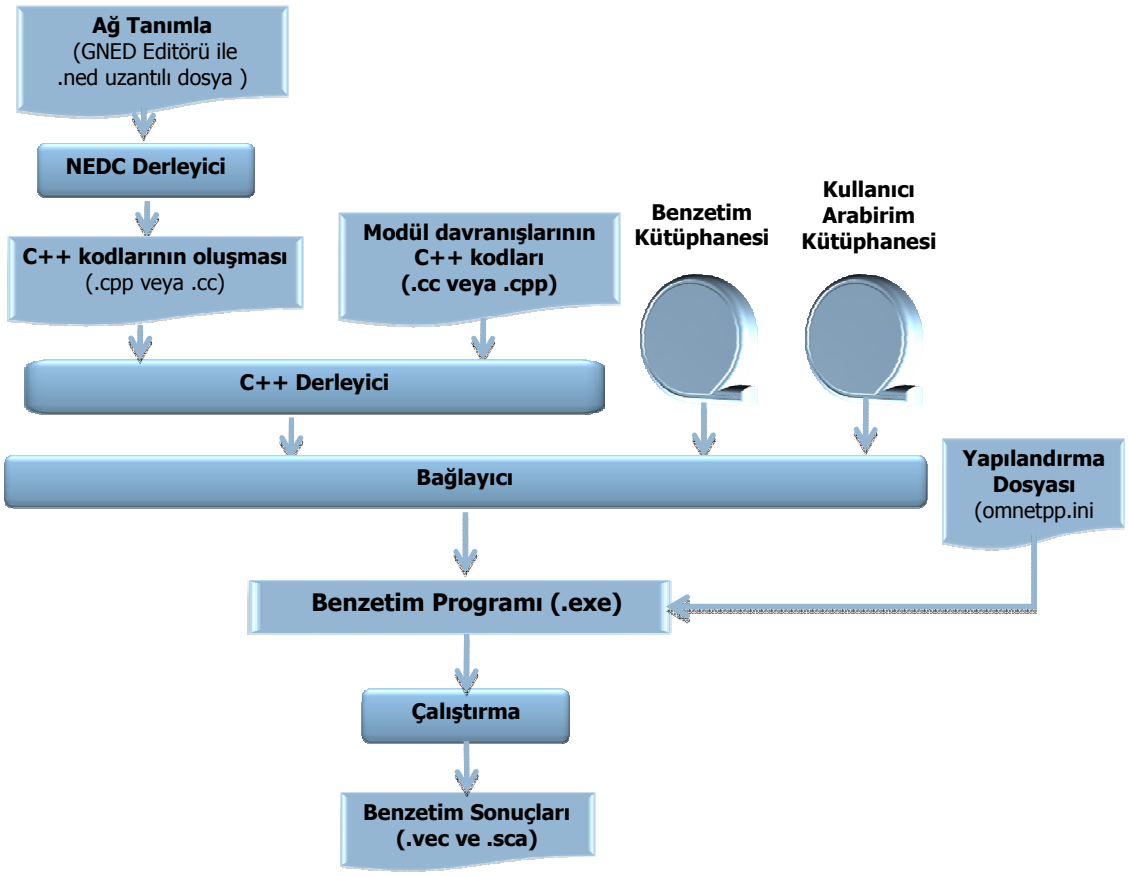
Hazır Benzetim Modelleri: Omnet++ yeni bir benzetim yazılımı olması sebebiyle birçok benzetim modeli son yıllarda geliştirilmiş ve geliştirilmeye devam etmektedir. Ücretsiz olması sebebiyle OMNET kullanan birçok araştırmacı yeni model ve protokoller geliştirerek başkalarının kullanımına sunmaktadır. OMNET++ benzetim yazılımında bulunan başlıca hazır modeller şunlardır:

- Ethernet: Ethernet, Hızlı Ethernet ve Gigabit Ethernet modelleri ile MAC, LLC, anahtarlama, hub ve veriyolu modellerinin bulunduğu benzetim paketi.
- IPv6Suite: IPv6 protokol ve ağlarının modellerini içeren benzetim paketi.
- Mobility Framework (MF): OMNET++ benzetim yazılımının kablosuz ve gezgin düğümlerin benzetimine olanak sağlaması üzerene geliştirilmiş model topluluğudur. 802.11 iletişim modellerini, kablosuz kanal ve çeşitli gezginlik modellerini bulundurmaktadır.

- INET Framework: INET, kablolu/kablosuz ve ad-hoc ağların benzetimine yönelik olarak geliştirilmiş bir pakettir. IP, UDP/TCP, 802.11, Ethernet, PPP, IPv6, OSPF, RIP, MPLS, RSVP-TE sinyalleşmesi ve diğer birçok protokolü destekler.
- OverSim: Bindirmeli ağ (Overlay Network) benzetimleri için geliştirilmiş model topluluğudur. Noktadan noktaya (Peer to Peer-P2P) haberleşme tekniklerine yönelik protokolleri desteklemektedir.
- SimSANs: Saklama Alan Ağlarına (Storage Area Networks-SAN) yönelik tasarım, modelleme ve benzetim aracıdır.
- MACSimulator: Kablosuz algılayıcı ağlarda birçok MAC protokolünün modellendiği ve benzetimine olanak sağladığı benzetim paketidir. .
- Castalia: Kablosuz algılayıcı ağlara yönelik olarak geliştirilmiş realistik benzetim yazılımıdır.
- CDNsim: İçerik Dağılım Ağları (Content Distribution Networks-CDNs), yönelik olarak geliştirilmiş benzetim yazılımıdır.
- WDM Simulator ve FieldBus Simulator: WDM ağlar ve FieldBus protokollerinin benzetimine olanak sağlayan benzetim yazılımlarıdır.

A.3.2. OMNET++ benzetim yazılımında modelleme ve benzetim Akışı

OMNET++ yazılımında bir modelleme ve benzetim akışı Şekil A.8'de görüldüğü gibi yürütülmektedir. Bir benzetim geliştirilirken ilk olarak ağı meydana getiren elemanların modelleri GNED grafik arayüzü ile tanımlanır. Daha sonra, tanımlanan bu modellerin davranışlarını belirleyen C++ kodları, bir C++ editörü kullanılarak oluşturulur. Oluşan .cpp veya .cc uzantılı dosyalar derlenir ve bağlayıcı tarafından benzetim kütüphaneleri kullanılarak çalıştırılabilir benzetim programı meydana gelir. Bir yapılandırma dosyası yardımıyla benzetimde kullanılacak olan parametre ayarları yapılabilir. Elde edilen benzetim sonuçları ise *Plove* veya *Scalar* gibi çizim araçları ile grafik haline dönüştürülebilir. Ayrıca farklı harici programlar yardımıyla *.vec* ve *.sca* uzantılı dosyalar işlenerek grafik haline çevrilebilir.



Şekil A.8. OMNET++ modelleme ve benzetim Akışı

A.4. Sonuçlar

Bu bölümde, ilk olarak modelleme ve benzetim kavramları üzerinde durulmuş ve sayısal haberleşme ağlarının başarım analizinizi için olay tabanlı (event-driven) bilgisayar benzetim metodunun en uygun çözüm olabileceği açıklanmıştır. Daha sonra günümüzde yaygın olarak kullanılan bilgisayar tabanlı benzetim yazılımlarının üstünlükleri ve zayıflıkları özetlenmiş ve bu yazılımlardan OMNET++ benzetim ortamının seçilme nedenleri sıralanmıştır. Son olarak da OMNET++ benzetim ortamının özellikleri, yapısı ve kullanım şekli kısaca anlatılmıştır.

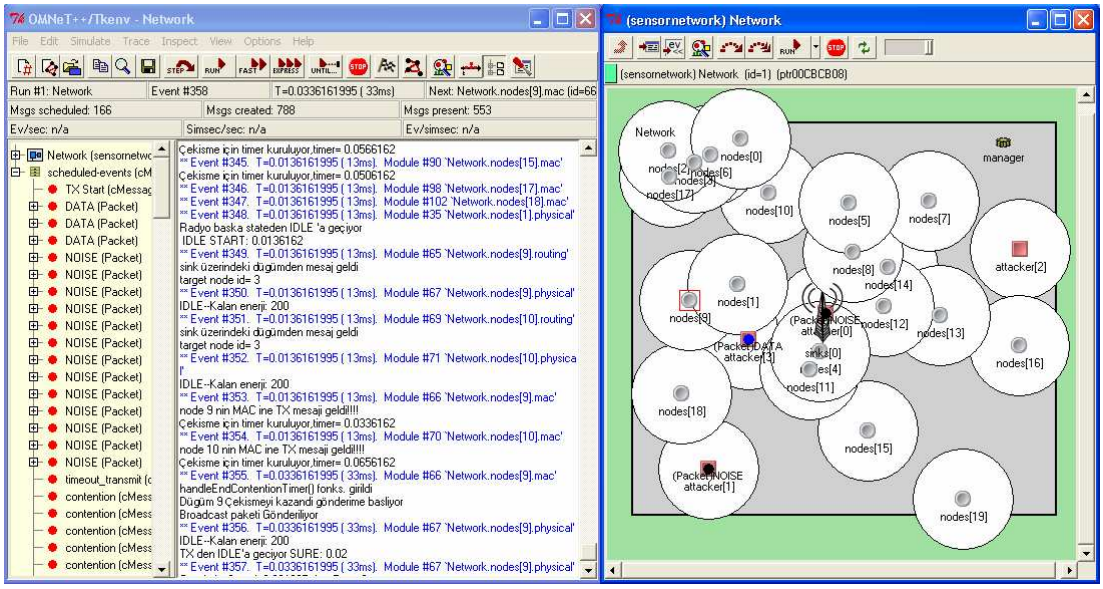
Ek B. Kablosuz Algılayıcı Ağlara Yönelik OMNET++ Tabanlı Benzetim Modelinin Tasarımı

B.1. Giriş

OPNET ve NS yazılımlarına oranla daha yeni bir benzetim ortamı olan OMNET++'ın hazır model yapıları son yıllarda gelişmeye başlamıştır. Günümüzde kablosuz algılayıcı ağları için tasarlanmış OMNET++ tabanlı çeşitli benzetim modelleri bulunmaktadır. Ancak bu tezin ilk yıllarında KAA'larına yönelik OMNET++ tabanlı modellerin henüz geliştirilmemiş veya deneme aşamasında olması yeni bir benzetim modelinin tasarımını zorunlu kılmıştır.

B.2. OMNET++ tabanlı benzetim modelinin genel özellikleri

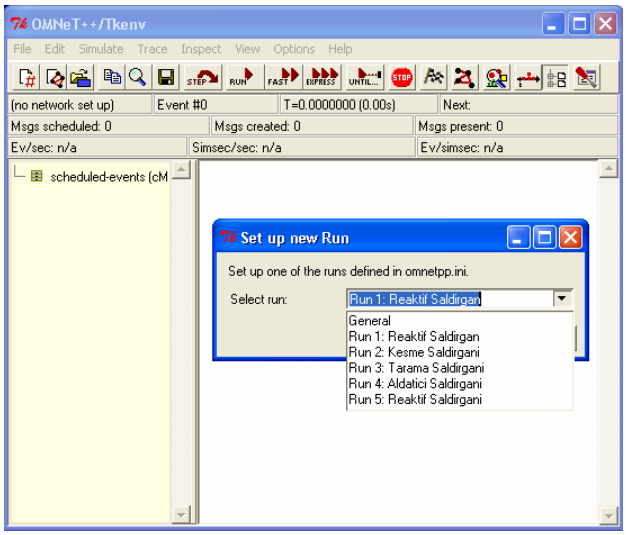
OMNET++ tabanlı kablosuz algılayıcı ağ benzetim modeli, Visual Studio 8.0 platformunda geliştirilmiştir. Tasarlanan model, Şekil B.1'de görüldüğü gibi görsel kullanıcı arayüzüne sahiptir ve bu arayüz yardımıyla benzetimler kolaylıkla gerçekleştirilebilir. Tasarlanan benzetim modelinde normal (node), çıkış (sink), saldırgan (attacker) ve yönetici (manager) olmak üzere dört farklı düğüm türü bulunmaktadır. Normal düğümler belirli zaman aralıklarında algıladıkları bilgileri komşuları üzerinden çıkış düğümüne iletmekle görevlidir. Çıkış düğümü (Sink), normal düğümlerden gelen bilgilerin toplanması ve işlenerek harici ağlara gönderilmesinden sorumludur. Saldırgan düğümler, çeşitli türdeki boğma saldırı modellerinin gerçeklendiği düğümlerdir. Yönetici düğümü ise gerçek bir düğüm değildir sadece normal, saldırgan ve çıkış düğümlerinin ağa yerleştirilmesi, komşuluklarının hesaplanması, rasgele hatalı düğümlerin belirlenmesi gibi görevlerin yürütülmesinden sorumludur.



Şekil B.1. OMNET++ tabanlı kablosuz algılayıcı ağ benzetim modelinin ekran görüntüsü

Benzetim modelindeki birçok parametre omnetpp.ini yapılandırma dosyasında tanımlandığı için herhangi bir kod yazmadan çok çeşitli benzetimler gerçekleştirmek mümkündür. Şekil B.2'de görüldüğü gibi benzetim alanının büyüklüğü, benzetimdeki düğüm sayıları, düğümlerin radyo alıcı/verici türü, radyo iletim mesafesi, saldırgan türü, MAC protokol türü gibi birçok parametre bu dosya yardımıyla ayarlanarak benzetimler kolaylıkla yapılandırılabilmektedir. Ayrıca sık şekilde çalıştırılan benzetimlerin parametreleri `[Run]` isimli kısımlarda tanımlanarak kullanıcının omnetpp.ini dosyasını yapılandırmadan benzetimleri değiştirebilmesi sağlar. Şekil B.3'de omnetpp.ini dosyasının `[Run]` kısmında tanımlanmış olan farklı ayarlarının, benzetim başlangıcında seçilmesi görülmektedir. Başlangıçta kullanıcı hangi `[Run]` sekmesini seçerse benzetim o kısımda olan parametrelere göre çalıştırılmaktadır.

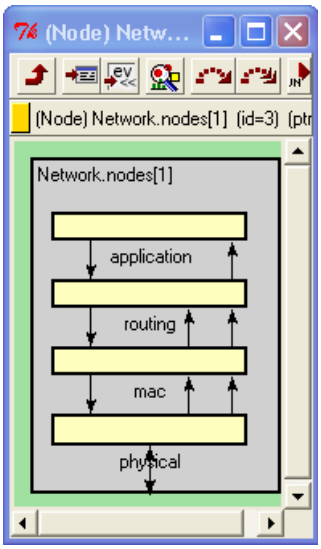
Şekil B.2. OMNET++ tabanlı benzetim modelinin yapılandırma dosyası (omnetpp.ini)



Şekil B.3. Farklı benzetim türlerinin benzetim başlangıcında arayüzden seçilmesi

B.3. Düğüm yapısı

Geliştirilen OMNET++ tabanlı benzetim modelinde kablosuz algılayıcı düğümleri, Şekil B.4'de görüldüğü gibi katmanlı ağ mimarisini destekleyecek şekilde tasarlanmıştır. Böylelikle istenildiğinde herhangi bir katmandaki protokolün değiştirilmesi diğer katmanlar açısından bir sorun teşkil etmeyecektir.



Şekil B.4. Katmanlı düğüm mimarisi

B.3.1. Fiziksel katman

Paket gönderimi, alımı ve kanal değiştirme gibi işlemlerden sorumlu olan fiziksel katman CC1000 ve CC2420 gibi popüler radyo alıcı/verici tüm devrelerini desteklemektedir. Yapılandırma dosyasından (omnetpp.ini) seçilen radyo modülü yardımıyla ilgili alıcı/verici devresinin veri iletim hızı, iletim frekansı, mevcut kanal sayısı, radyo modları gibi özellikleri otomatik olarak aktif hale getirilmiş olur. Ayrıca bir düğümün enerji tüketiminin çoğunu alıcı/verici birimi harcadığı için güç tüketim modellemeleri de fiziksel katmana entegre edilmiştir. Güç tüketimi, alıcı/vericinin mevcut radyo modlarında (aylak, gönderme, alma veya uyuma) kaldığı sürenin belirlenmesine göre hesaplanmaktadır. Alıcı/vericinin her bir radyo modunda harcadığı enerji miktarı bilindiğinden bir düğümün radyo modlarında kaldığı sürenin hesaplanmasıyla toplam enerji miktarı kolaylıkla bulunabilir.

B.3.2. MAC katmanı

MAC, kanal erişimi, çerçeve filtreleme ve radyo modlarının ayarlanmasından sorumlu katmandır. Tasarlanan benzetim programında MAC protokolü olarak CSMA/CA ve kablosuz algılayıcı ağlara yönelik olarak tasarlanmış ve en yaygın protokol olan S-MAC protokolünün modeli bulunmaktadır. MAC protokolü bu özelliklerin dışında Anomali tabanlı Boğma Saldırı Tespit Sistemi (ABSTS) ile Dinamik Kanal Atlama (DKA) yönteminin entegre edildiği katmandır. İstenilen MAC protokolünün türü ile saldırı tespit ve savunma yöntemlerinin ayarları, yapılandırma dosyasından gerçekleştirilebilmektedir. `Network.SaldiriTespit=true` yapılarak ABSTS, `Network.SaldiriSavunma=true` yapılarak ise DKA yöntemi aktif hale getirilmiş olur.

B.3.3. Yönlendirme katmanı

Yönlendirme katmanı, düğümlerin çok atlamalı yollar üzerinden çıkış düğümünü bulmasını sağlayan katmandır. Düğümler en kısa yol algoritmasını kullanarak çıkış düğümünü bulmaktadır. Bunun dışında farklı yönlendirme protokolleri kolaylıkla modellenerek sisteme entegre edilebilir.

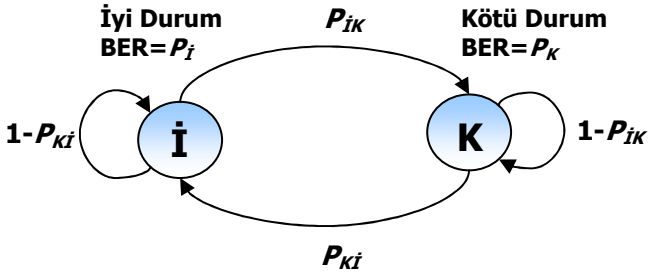
B.3.4. Uygulama katmanı

Düğümlerin hangi sıklıkla veya hangi aralıklarla algılama işlemlerini yürüteceğini belirleyen katmandır. OMNET++ tabanlı benzetim modelinde düğümlerin algılama işlemleri paket üreteci ile sağlanmaktadır. CBR (Constant Bit Rate-Sabit Bit Hızı), üstel (exponential), uniform gibi birçok paket dağılım üreteçleri yardımıyla trafik üretimi gerçekleştirilebilmektedir. Paket dağılım fonksiyonun türü ve sıklığı *omnetpp.ini* dosyasından ayarlanabilmektedir.

B.4. İletişim kanalı

İletişim kanalı düğümlerin kablosuz ortam üzerinden haberleşmesini sağlayan ortamdır. Kablosuz ağlarda düğümlerin birbirleri ile verimli olarak haberleşmesini engelleyen en önemli sorunlardan birisi de kötü iletişim ortamıdır.

Kablosuz algılayıcı düğümlerinde maliyeti ve güç tüketimini azaltmak için basit radyoların tercih edilmesi genellikle kablosuz iletim kanalının ya iyi ya da kötü olmasına sebep olmaktadır. Bu yüzden iletim kanalındaki kayıpları benzetebilmek için Şekil B.5'de görüldüğü gibi Gilbert-Elliot modeli olarak adlandırılan iki durumlu ayrık Markov zinciri kullanılmıştır.



Şekil B.5. İki durumlu Gilbert-Elliot kanal modeli

İki durumlu Gilbert-Elliot kanal modelinde, Bit Hata Oranı (Bit Error Rate – BER) $P_{bİ}$ olan İyi (İ) ve Bit Hata Oranı P_{bK} olan Kötü (K) durumları bulunmaktadır. Kanalın İ durumundan K durumuna geçme olasılığı $P_{İK}$ ve K durumundan İ durumuna geçme olasılığı ise $P_{Kİ}$ olduğunda, Markov zincirinin geçiş matrisi Formül B.1'deki gibi olur.

$$\begin{pmatrix} 1\text{-}P_{İK} & P_{İK} \\ P_{Kİ} & 1\text{-}P_{Kİ} \end{pmatrix} \tag{B.1}$$

Kanalın İ ve K durumlarında olma olasılığının ortalaması ise Formül A.2 yardımıyla hesaplanabilir.

$$\pi_İ = \frac{P_{Kİ}}{P_{İK} + P_{Kİ}} \quad \text{ve} \quad \pi_K = \frac{P_{İK}}{P_{İK} + P_{Kİ}} \tag{B.2}$$

Ortalama Bit Hata Oranı (BER) ise Formül B.3 yardımıyla bulunabilir.

$$P_{b,ort} = \pi_İ P_{bİ} + \pi_K P_{bK} \tag{B.3}$$

İletişim kanalının İ ve K durumlarda ortalama kalma zamanı ise Formül B.4 yardımıyla hesaplanabilir.

$$\frac{1}{P_{İK}} \quad \text{ve} \quad \frac{1}{P_{Kİ}} \tag{B.4}$$

Geliştirilen benzetim yazılımında istenilen özelliklerdeki kanal şeklini ayarlamak için omnetpp.ini dosyasındaki `Network.BER`, `Network.Pki` ve `Network.Pik` parametrelerinin değiştirilmesi yeterli olacaktır.

B.5. Hata durumlarının benzetimi

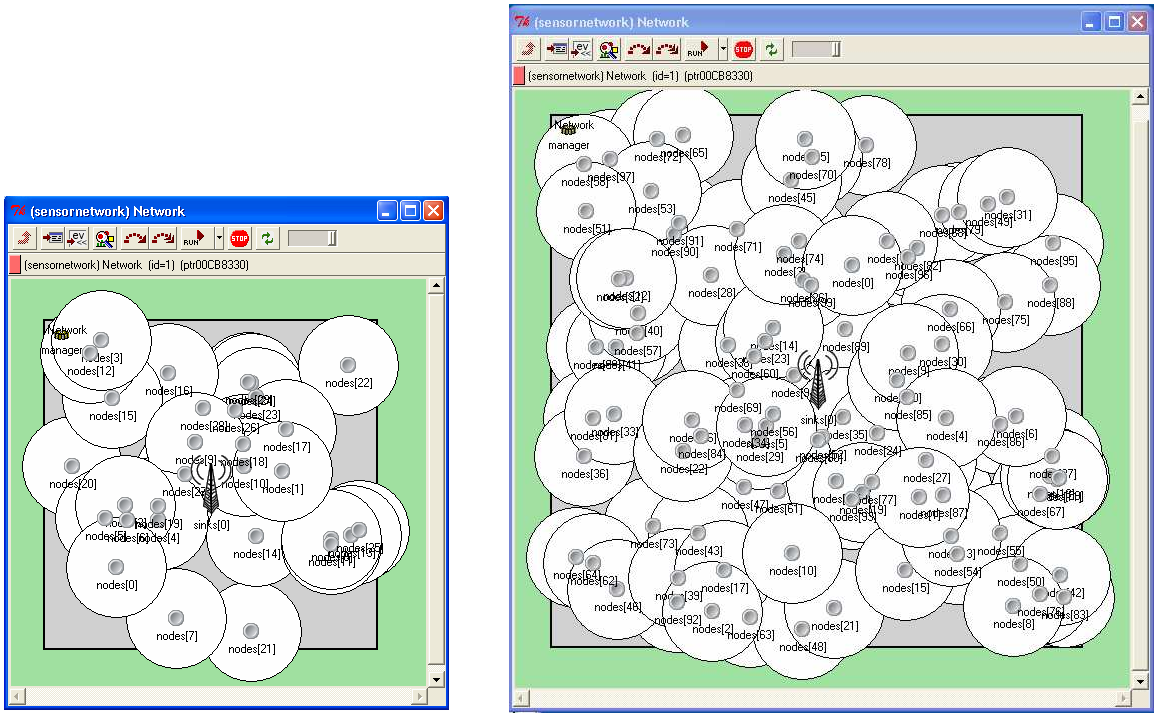
Kablosuz algılayıcı ağlarının doğası gereği donanımsal ve yazılımsal hatalara meyilli olması, tasarlanan benzetim ortamında hata senaryolarının benzetiminin gerçekleştirilebilmesini gerekli kılmıştır. Geliştirilen benzetim modelinde bir düğümün enerjisinin tükenmesi veya donanımsal olarak bozulması gibi hata durumlarının benzetimini gerçekleştirmek üzere ağdaki bazı düğümlerin rasgele zamanlarda iletişim yapamaz hale gelmesi sağlanmaktadır. Yapılandırma dosyasındaki (omnetpp.ini) `Network.Hata=true` parametresi sayesinde hata senaryolarının benzetimi aktif hale getirilmiş olur ayrıca `Network.HataliDügümOrani` parametresi ile ağ içerisindeki düğümlerin ne kadarının hata sebebiyle bozulacağı belirlenebilmektedir.

B.6. Saldırı senaryolarının benzetimi

OMNET++ tabanlı benzetim modelinde sürekli, aldatıcı, rasgele, reaktif, dinleme aralığı, kontrol aralığı, veri paketi, küme, kesme, aktivite, tarama ve darbe boğma saldırgan modelleri tanımlanmıştır. Yapılandırma dosyasındaki `Network.SaldirganTuru` isimli parametre yardımıyla istenilen saldırı durumunun benzetimi gerçekleştirilebilir. Saldırı durumlarının benzetiminin gerçekleştirilmesi istenmediğinde ise `Network.SaldirganSayisi` parametresine sıfır değeri atanarak saldırgansız bir ağ ortamının benzetimi sağlanabilir.

B.7. Düğümlerin konumlandırılması

OMNET++ tabanlı benzetim yazılımı, omnetpp.*ini* dosyasında belirtilen düğüm sayılarına ve benzetim alanının büyüklüğüne göre düğümlerin rasgele şekilde konumlandırabilmesine imkân tanımaktadır. Network.DugumSayisi, Network.SaldirganSayisi ve Network.SinkSayisi parametrelerinde belirtilen sayıdaki düğüm, Network.AREASIZEX ve Network.AREASIZEY parametrelerine atanan benzetim alan büyüklüğüne göre rasgele şekilde yerleştirilir. Bu parametreler sayesinde istenilen ölçekte ve yoğunlukta benzetim gerçekleştirmek mümkündür. Şekil B.6'de farklı büyüklükte ve farklı düğüm sayılarındaki topoloji örnekleri görülmektedir.



a) 300x300m^2 alan ve 30 düğüm b) 500x500 m^2 alan ve 100 düğüm

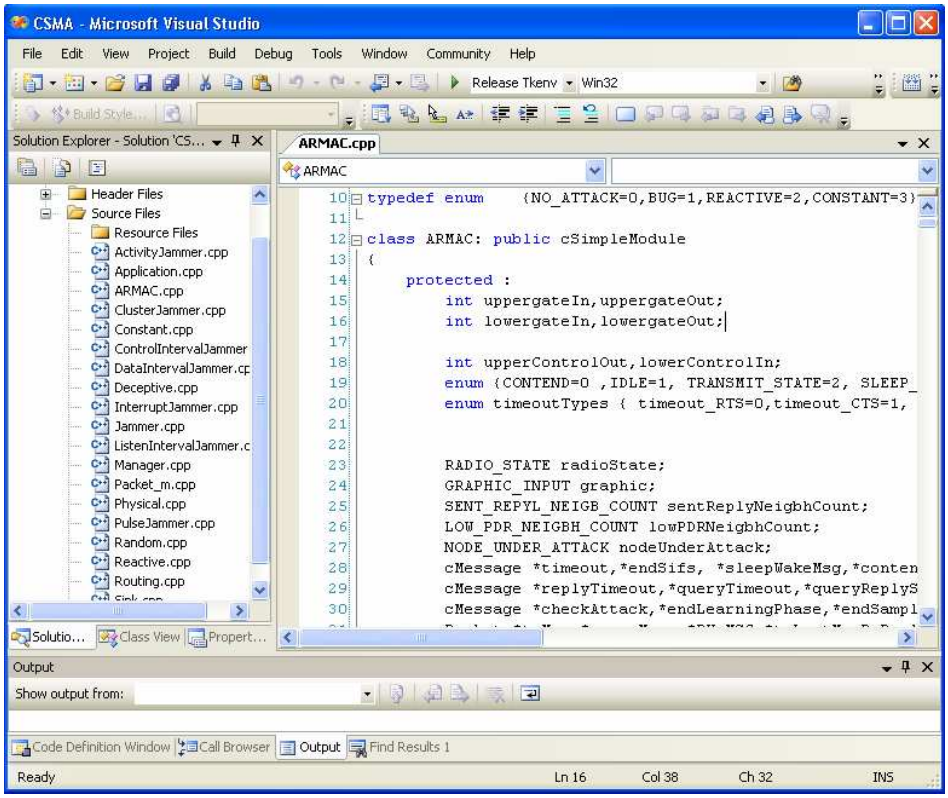
Şekil B.6. Düğüm topoloji örnekleri

B.8. Yeni bir benzetimin gerçekleştirilmesi

Tasarlanan OMNET++ tabanlı benzetim modeli, kablosuz algılayıcı ağların benzetimine yönelik olarak geliştirilmiş modüler ve kolay konfigüre edilebilir bir benzetim ortamıdır. Yapılandırma dosyasındaki parametreler değiştirilerek farklı

amaçlara yönelik birçok uygulamanın benzetimi kolaylıkla gerçekleştirilebilir. Ancak kullanıcının benzetim modelindeki bir özelliği değiştirmesi, yeni özellikler eklemesi veya yeni bir protokol tasarlaması gerekebilir. Bu durumda yapılması gereken adımlar şunlardır.

1. Örneğin yeni bir MAC protokolü oluşturulacaksa, MAC protokolünün davranışlarının tanımlandığı yeni bir C++ dosyası (.cpp), Şekil B.7'de ekran görüntüsü görülen OMNET++ proje dosyasına eklenmeli ve proje yeniden derlenmelidir ayrıca omnetpp.ini dosyasındaki `Network.MACTuru` isimli parametreye yeni tanımlanan MAC protokolünün ismi atanmalıdır.



Şekil B.7. OMNET++ tabanlı benzetim modelinin Visual Studio proje dosyası

2. Farklı bir saldırgan türünün benzetimi için OMNET++ proje dosyasına yeni saldırganın davranışlarını belirleyen C++ kodu eklenmeli ve proje yeniden derlenmelidir ayrıca omnetpp.ini dosyasındaki `Network.SaldirganTuru` isimli parametreye yeni tanımlanan saldırganın ismi atanmalıdır.

3. Eğer ağa farklı özelliklerde yeni bir düğüm türünün eklenmesi gerekirse düğümün kapı tanımlamaları ve varsa parametreleri GNED editörü kullanılarak tanımlanmalıdır. Ayrıca eklenen düğümün davranışını belirleyen C++ kodları OMNET++ proje dosyasına eklenmeli ve proje yeniden derlenmelidir.

4. Tüm düğümlerin yönetimini ilgilendiren uygulamaların modelleri manager (yönetici) düğümün davranışlarını belirleyen manager.cpp isimli dosyaya eklenmelidir. Örneğin düğümlerin gezginliğinin sağlanması için gerekli olan değişiklikler manager.cpp dosyasında yapılmalıdır.

B.9. Sonuçlar

Bu bölümde, OMNET++ tabanlı olarak geliştirilen kablosuz algılayıcı ağ benzetim modelinin tasarım detayları ve kullanımı açıklanmıştır. Geliştirilen yazılımda birçok ağ parametresinin modüler yapıda olması sayesinde benzetim ayarları kolaylıkla değiştirilebilmekte ve kullanıcı herhangi bir kod değişikliği yapmadan çeşitli algılayıcı ağ uygulamalarının benzetimini gerçekleştirilebilmektedir. Etkileşimli kullanıcı arabirimi sayesinde benzetimin hızlı ya da yavaş koşturulabilmesi, benzetim sırasındaki değişkenlerin izlenebilmesi ve çeşitli animasyonlar ile benzetimlerin zenginleştirilmesi mümkündür.

ÖZGEÇMİŞ

1979 İstanbul doğumludur. İlk ve orta öğrenimini İstanbul'da tamamlamıştır. 1997 yılında Sakarya Üniversitesi Teknik Eğitim Fakültesi Elektronik ve Bilgisayar Eğitimi, Elektronik Öğretmenliği Programına girerek 2001 yılında mezun olmuştur. Yüksek Lisans Eğitimini Sakarya Üniversitesi Fen Bilimleri Enstitüsü Elektronik ve Bilgisayar Eğitimi Bölümünde 2003 yılında tamamlamıştır. Devamında, aynı üniversitede Fen Bilimleri Enstitüsü Elektrik-Elektronik Mühendisliği Doktora programına başlamıştır. Sakarya Üniversitesi Teknik Eğitim Fakültesi Elektronik ve Bilgisayar Eğitimi Bölümü'nde halen araştırma görevlisi olarak görev yapmaktadır.