EN KRİTİK DÜĞÜMÜN BERTARAF EDİLMESİNİN KABLOSUZ ALGILAYICI AĞININ YAŞAM SÜRESİNE ETKİSİ

ANIL YÜKSEL

YÜKSEK LİSANS TEZİ

ELEKTRİK VE ELEKTRONİK MÜHENDİSLİĞİ

TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

MART 2015

ANKARA

Fen Bilimleri Enstitü onayı

_____

Prof. Dr. Osman EROĞUL
Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksinimlerini sağladığını onaylarım.

_____

Prof Dr. Dr. Murat ALANYALI
Anabilim Dalı Başkanı

ANIL YÜKSEL tarafından hazırlanan EN KRİTİK DÜĞÜMÜN BERTARAF EDİLMESİNİN KABLOSUZ ALGILAYICI AĞININ YAŞAM SÜRESİNE ETKİSİ adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

_____

Doç. Dr. Bülent TAVLI
Tez Danışmanı

Tez Jüri Üyeleri

Başkan : Doç. Dr. Tolga GİRİCİ _____

Üye : Doç. Dr. Bülent TAVLI _____

Üye : Dr. Ahmet TÜMAY _____

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

Anıl YÜKSEL

Üniversitesi	**:**	**TOBB Ekonomi ve Teknoloji Üniversitesi**
Enstitüsü	**:**	**Fen Bilimleri**
Anabilim Dalı	**:**	**Elektrik ve Elektronik Mühendisliği**
Tez Danışmanı	**:**	**Doç. Dr. Bülent TAVLI**
Tez Türü ve Tarihi	**:**	**Yüksek Lisans – Mart 2015**

Anıl YÜKSEL

EN KRİTİK DÜĞÜMÜN BERTARAF EDİLMESİNİN KABLOSUZ ALGILAYICI AĞININ YAŞAM SÜRESİNE ETKİSİ

ÖZET

Kablosuz Algılayıcı Ağları (KAA) paradigması, yaygın bilişimin (ubiquitous computing) ve Makineden-Makineye (Machine-to-Machine) haberleşmenin ayrılmaz bir parçasıdır. KAA'ların anayurt güvenliği, askeri uygulamalar, yeni nesil elektrik şebekeleri, kritik altyapı izleme sistemleri alanlarında yaygın olarak kullanılmasından dolayı saldırganlara ilgi çekici gelmektedir. Ayrıca zorlu topolojilerden kaynaklı doğa koşullarına karşı savunmasızdır. Servis dışı bırakma saldırılarının tek ve birden çok algılayıcı düğüme yapılmasına karşı çözümler oluşturulsa da KAA'lar daha karmaşık saldırılara karşı zayıf bir şekilde korunmaktadır. Müdahale ve yedek sistemlerin çalışma sürelerinin hesaplanması için saldırı altındaki algılayıcı ağın ayakta durma süresi büyük önem taşımaktadır. Bu çalışmada tek düğüm saldırılarının ağ yaşam süresine olan etkisinin modellenmesi ile ilgili bir doğrusal programlama yaklaşımı teklif edilmektedir. Doğrusal programlama modeli kullanılarak en önemli düğümün bertaraf edilmesinin KAA yaşam süresine etkisi ölçülmektedir.

Anahtar Kelimeler: kablosuz algilayici ağlar, matematiksel programlama, doğrusal programlama, enerji verimliliği, ağ yaşam süresi, tek düğüm saldırısı, servis dışı bırakma saldırısı, uyku engelleme saldırısı, fiziksel saldırı.

University	:	**TOBB University of Economics and Technology**
Institute	:	**Institute of Natural and Applied Sciences**
Science Programme	:	**Electrical and Electronics Engineering**
Supervisor	:	**Assoc. Prof. Bülent TAVLI**
Degree Awarded and Date	:	**M.Sc. – MARCH 2015**

Anıl YÜKSEL

THE IMPACT OF ELIMINATION OF THE MOST CRITICAL NODE ON WIRELESS SENSOR NETWORK LIFETIME

ABSTRACT

Wireless Sensor Network (WSN) paradigm is an integral component of ubiquitous computing and Machine- to-Machine communications. Since WSNs are widely used in homeland security, military applications, next generation power lines, critical infrastructure monitoring and smart spaces, they are naturally attractive to the adversaries and vulnerable to natural conditions because of their harsh topologies. Although, there are some solutions against Denial of Service (DoS) attacks conducted against single or multiple sensor nodes in WSNs, WSNs are, at best, weakly defended against more sophisticated attack types. Therefore, the period that the sensor network will stand out against such attacks has a crucial importance to calculate intervention or backup times for WSNs. In this study, we propose a linear programming (LP) approach for modelling the impact of single node attacks on network lifetime in WSNs. We explored the parameter space through the numerical evaluations of the LP model to quantify the impact of elimination of the most critical node on WSN lifetime.

Keywords: wireless sensor networks, mathematical programming, linear programming, energy efficiency, network lifetime, single node attack, denial of service attack, denial of sleep attack, physical attack.

TEŞEKKÜR

Yüksek Lisans eğitimim boyunca bana yol gösteren ve yardımlarını esirgemeyen, bilimsel katkıları ile bana yardımcı olan tez danışmanım ve hocam Sayın Doç. Dr. Bülent Tavlı'ya en içten teşekkür ve saygılarımı sunarım. Ayrıca Yüksek Lisans eğitimimi Araştırma Bursu ile yapmamı sağlayan TOBB Ekonomi ve Teknoloji Üniversitesi'ne teşekkür ederim.

Bu günlere gelmemde emeği geçen, maddi ve manevi her koşulda yanımda olan ve desteklerini esirgemeyen Çağlayan YÜKSEL, Derya YÜKSEL ve Yusuf Kaan YÜKSEL'e, desteği ve yardımlarından dolayı Fatma Nur BEREKET'e, tezin düzeltilmesi ve iyileştirmesi için vakit ayıran Rauf Kaan DENİZER ve Erkam UZUN'a teşekkürlerimi sunarım.

İçindekiler

Şekil Listesi

Tablo Listesi

Sembol Listesi

Bu çalışmada kullanılmış olan simgeler açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklamalar**
s_i	Düğüm-i'de üretilen veri miktarı *(bit)*
$G = (V, A)$	Ağ topolojisini ifade eden yönlü grafik
V	Baz istasyonu dahil edilen düğümler kümesi
W	Baz istasyonu hariç düğümler kümesi
A	Düğümlerin gönderdikleri bütün akılar
t	Ağ ömrü *(s)*
f_{ij}	Düğüm-i'den düğüm-j'ye iletilen veri miktarı *(bit)*
e_i	Her algılayıcıdaki pil enerjisi *(J)*
$E_{tx,ij}^{opt}$	Düğüm-i'den düğüm-j'ye bir bit verinin iletilmesi için gereken enerji miktarı *(J)*
E_{rx}	Bir bit veri alabilmek için gereken enerji miktarı *(J)*
l	Veri iletiminde kullanılan güç seviyesi
E_{tx}^{l}	Güç seviyesi l için enerji kaybı
R_{max}^{l}	Güç seviyesi l için maksimum iletim uzaklığı
d_{ij}	Düğüm-i ile düğüm-j arasındaki uzaklık *(m)*
E_{Elec}	Elektronik devrede harcanan enerji *(nJ)*

Kısaltmalar

Kısaltmalar	**Açıklama**
DP	Doğrusal Programlama
KAA	Kablosuz Algılayıcı Ağ
GAMS	General Algebraic Modeling System
SDB	Servis Dışı Bırakma
RTS	Gönderme istem kodu
SYN	Senkronizasyon paketi

1. GİRİŞ

Mikroelektromekanik sistemler, kablosuz haberleşme ve dijital elektronik alanlarındaki gelişmeler sayesinde, düşük maliyetli, düşük güç tüketimi yapan, çok fonksiyonlu ve küçük boyutlarda algılayıcı düğümler geliştirilmektedir. Algılayıcı düğümlerin bu özellikleri sayesinde Kablosuz Algılayıcı Ağlar aşağıdaki alanlarda yaygın olarak kullanılmaktadır [4]:

- Askeri Uygulamalar; dost birliklerin, malzemelerin ve cephanelerin izlenmesi, savaş alanlarının izlenmesi, hedef ve savaş hasarının belirlenmesi, nükleer, biyolojik ve kimyasal saldırıların tespit edilmesi,
- Ekolojik Sistemler; orman yangınlarının tespit edilmesi, sel tespiti, hassas tarım uygulamaları,
- Sağlık Sistemleri; insanların psikolojik verilerinin izlenmesi, hastane içerisindeki doktor ve hastaların takibi ve izlenmesi, hastanelerdeki ilaç kullanımının takibi,
- Bina ve Diğer Otomasyon Sistemleri; akıllı ev otomasyonları, iklimlendirme kontrolü, interaktif müzeler, depo kontrol sistemleri, araç takip ve algılama sistemleri.

Bu ve benzeri uygulamara ek olarak, kurulum ve işletme maliyetlerinin düşük olması, hata dayanaklılığının yüksek olması, ölçeklenebilir olması, yüksek algılama doğruluğu, gelişmiş kararlılığı ve geniş kapsama alanı sayesinde KAA'lar Akıllı şebekelerin müşteri, iletim, dağıtım ve üretim sistemlerinde önemli rol oynamaktadır [5]. Elektrik altyapılarının birçok ülkede eski olması akıllı şebekelerin hızla yaygınlaşmasını sağlamaktadır. Akıllı şebekeler, elektrik üretim, iletim ve dağıtım sistemlerini anlık verilerle izlemekte ve kapasite sıkıntıları, donanım arızaları, doğal afetler vb. durumlarda müdahaleyi hızlandırmaktadır. Kablolu haberleşme altyapılarında, kablolama ve bakım maliyetinin yüksek olması nedeniyle algılayıcı

ağların kullanımı Akıllı Şebekelerde hızla artmaktadır [6]. Algılayıcı ağların kolay uygulanabilir olması bu alanların bir çoğunda özgün ve yenilikçi teknolojik gelişmelerin ortaya çıkmasını sağlamaktadır.

KAA sistemlerinin verimli, kararlı ve güvenilir çalışabilmeleri için dikkat edilmesi ve üzerinde çalışılması gereken hata dayanıklılığı, ölçeklenebilirlik, üretim maliyeti, donanımsal kaynak kısıtları vb. tasarım başlıkları bulunmaktadır [4]. Bu tasarım başlıkları KAA sistemlerinin karakteristik özelliklerinden ortaya çıkmaktadır. Algılayıcı düğümlerin küçük boyutlarda olmasından dolayı az enerji ve kaynak bulundurması gerekmektedir. Ayrıca sistemlerin birçoğunda verilerin anlık ve kayıpsız iletilme gerekliliği nedeniyle hata dayanıklılığı ve gecikmelerin planlanması önemlidir [7]. Bunların yanında enerji verimliliği, birlikte çalışabilirlik, güvenlik, gecikme gereksinimleri, dayanıklılık, zorlu doğa koşulları vb. tasarım zorlukları bulunmaktadır [6, 7]. Bu tip zorluklardan kaynaklı olarak KAA sistemleri fiziksel katmandan uygulama katmanına kadar gerçekleştirilen farklı saldırı tiplerine karşı savunmasızdır.

KAA sistemlerinde güvenlik servislerinin amacı erişilebilirlik, gizlilik ve bütünlük gereksinimlerini karşılamaktır [8]. Gizlilik, istenmeyen kişilerin verilere erişmesini engellemekte ve bütünlük ise verinin değişmediğini garanti etmektedir. Erişilebilirlik, verilerin, servislerin ve diğer hizmetlerin sürekli erişilebilir olmasını sağlamaktadır. Servis dışı bırakma saldırıları güvenlik ilkelerinden erişilebilirliği hedef almaktadır [2]. Yapılan saldırılar bu güvenlik adımları kötü yönde kullanılarak gerçekleştirilebilmektedir [8–11].

Yönlendirme protokollerindeki yönlendirme bilgisi içeren paketleri ve bilgilendirme mesajlarını değiştirerek veya tekrarlayarak saldırgan sisteme zarar verebilmektedir [10]. Kopyalama, ortadaki adam, frekans bozma, hile karıştırma, solucan deliği vb. saldırı tipleri KAA sistemlerinin çalışmasını durdurabilir. Bu saldırıların genel olarak amaçları düğümlerden hassas bilgiyi ele geçirmek, ağ akılarını karıştırmak, ağa yanlış bilgi yerleştirmek, belirli düğümü diğerleri için çekici hale getirmek, ilgisiz paketler göndererek enerji tüketimini arttırmak veya düğümlerin uyku moduna geçmelerini engellemektir.

Enerji verimliliği KAA sistemlerinin zayıf bir noktası olduğu için servis dışı bırakma saldırılarının büyük bir kısmında enerji kullanımının arttırılması amaçlanmaktadır. Enerji kullanımının artmasıyla sistemde bulunan düğümler planlanandan önce servis dışı kalacaktır [1, 2]. Örneğin iki adet 3000 mAh pil bulunduran Crossbow Mica2 algılayıcı düğümü uyku modunda 4000 gün, aktif modda ise 10 gün çalışabilmektedir [2]. Algılayıcı düğümün yaşam süresinin uyku ve aktif mod arasında bu kadar farketmesi düğümün çok kısa zamanda servis dışı kalabileceğini göstermektedir. Çizelge 1.1, servis dışı bırakma saldırılarının tiplerini protokol katmanlarına göre göstermektedir. Servis dışı bırakma saldırıları en alt katmandan en üst katmana kadar birçok protokol ve algoritmayı hedef almaktadır. Donanımsal arızalar, yazılım hataları, kaynak tüketme, çevre koşulları vb. faktörler servis dışı bırakma saldırılarına izin verebilmektedir. KAA sistemleri için protokoller SDB saldırıları göz önünde bulundurularak geliştirilmelidir. Bazı protokoller tasarımlarından gelen zafiyetler nedeniyle SDB saldırılarına izin vermektedir [1].

Tablo 1.1. Protokol katmanlarına göre servis dışı bırakma saldırıları [1, 2]

Protokol Katmanı	Saldırı
Fiziksel	Frekans Karıştırma
	Düğümle oynama ve tahrip etme
Erişim	Uyku Engelleme
	Çok sayıda *RTS* paketi gönderme
	Çarpışma
Ağ	Yönlendirme kontrol paketlerini değiştirme ve tekrarlama
	Hello seli saldırısı
	Yanlış yönlendirme
	Karadelik
İletim	*SYN* seli saldırısı
	Desenkrenizasyon saldırısı
Uygulama	Sensörleri uyararak büyük veriler üretilmesini sağlamak
	Yol bazlı SDB

Servis dışı bırakma saldırısının özel bir tipi olan uyku engelleme saldırısı, düğümün veri işlemediği veya göndermediği zamanlarda uyku moduna geçmesini engellemeyi amaçlamaktadır. Bu saldırı sonucunda düğümler uyku moduna saldırı süresi boyunca geçemeyeceği için enerjileri planlanandan daha kısa sürede tükenecektir. Bir veya daha fazla algılayıcı düğümün enerjisinin tükenmesi bütün sistemin veya belirli bir bölgenin servis dışı kalmasına neden olabilmektedir. Uyku eksikliği, senkronizasyon, baraj saldırılarında kötü niyetli bir kişi doğru istekleri kullanarak algılayıcı düğümün enerji tüketimini artırabilir. Yapılan isteklerin meşru olmasından dolayı bu tür saldırıların tespit edilmesi çok zordur [12]. Uyku

engelleme saldırılarına karşı birçok güvenlik önlemi sunulmasına karşın tam anlamıyla ağın güvenli hale getirilmesi oldukça karmaşık ve zorlayıcıdır. Uygulanan güvenlik önlemleri uyku yoksunluğu, baraj, eşleme, tekrarlama, çakışma ve yayımlama saldırıları gibi karmaşık saldırıları engelleyememektedir [12–14].

Servis dışı bırakma, uyku engelleme vb. saldırılarının ötesinde, saldırganın amacı düğümü fiziksel olarak tahrip ederek çalışmaz hale getirmek olabilir. Her ne kadar tasarım sırasında bu tarz durumlar planlansa da kötü niyetli bir kişinin algılayıcı düğümlere fiziksel erişimi olduğu sürece istediği gibi düğümü ısıtabilir, soğutabilir veya yerini değiştirebilir. Örneğin çölde kurulan bir KAA topolojisinde algılayıcıların çöl sıcaklıklarına dirençli olması gerekmektedir.

Fiziksel saldırılar kolayca gerçekleştirilebilmesine rağmen, çok yıkıcı sonuçlara neden olabilmektedir. Basit fiziksel saldırıların aksine [15]'de belirtilen saldırı tipinde kötü niyetli kişi algılayıcı düğümleri tespit ederek saldırıyı gerçekleştirmektedir. Bu tip kasıtlı saldırıların dışında bazı topolojilerde ağaç devrilmesi, deprem, toprak kayması gibi doğal ve ekolojik riskler bazı düğümlerin tahrip olmasına ve çalışmamasına neden olabilir.

Algılayıcı düğümlerin enerjilerini dengeli bir şekilde kullanmaları bazı düğümlerin enerjilerinin erken bitmesini engellemektedir. Bu düğümlerin çalışmaması KAA sistemlerinin belirli bölgede bulunan servisi yerine getirememesine neden olabilmektedir. Ayrıca kablosuz sistemlerde kullanılan çok sekmeli iletişim yöntemi direk iletişim yöntemine göre daha verimlidir [16]. KAA'nın bütünlüğünde tek bir düğüm önemli bir faktör olduğundan, en kritik olan düğüm saldırı öncesi tespit edilerek saldırı daha etkin bir şekilde gerçekleştirilebilir [15, 17, 18]. Arama tabanlı saldırılarda her ne kadar düğümlerin yerleri tespit edilmeye çalışılsa da en kritik düğümlerin tespit edilmesi amaçlanmaktadır. Düğüm bazlı saldırılara karşı alınan güvenlik önlemleri bazı düğümlerin gözden çıkarılması üzerine geliştirilmektedir [19]. Burada yerel kapsama alanına saldırı yapılması sağlanarak ağın tüm kapsama alanının korunması amaçlanmaktadır. Kritik olmayan düğümlerin çalışmaması kapsama alanının azalmasının yanında topoloji bütünlüğünün bozulmasına ve buna bağlı olarak yaşam süresinin olumlu veya olumsuz etkilenmesine

neden olmaktadır.

[4] makalesinde algılayıcı düğüm konumlarının önceden belirlenmesine ihtiyaç olmadığı ve bunun sayesinde erişilemeyen arazilere veya afet bölgelerine rastgele kurulum yapılabilmesinden bahsedilmektedir. Bu çalışmanın aksine algılayıcı düğüm konumlarının yaşam süresi, kapsama alanı vb. gerekliliklerden dolayı belirlenmesi ile ilgili [20], [21], [22], [23] ve [24] makalelerinde çalışmalar yapılmıştır.

Bu çalışmada baz istasyonundan farklı, tek bir düğüme yapılacak herhangi bir saldırı tipinin KAA yaşam süresine olan etkisi incelenmektedir. Saldırı tipi önemli olmadığından ağ bütünlüğünü bozacak herhangi bir saldırının KAA'lara uygulandığı varsayılmaktadır. Ayrıca düğümlere yapılan saldırı ile ilgili herhangi bir planlama yapılmamıştır. Doğrusal programlama kullanılarak herhangi bir saldırı altında KAA yaşam süresinin hesaplanması amaçlanmıştır. Çalışma sonucunda hem düğüm konumlandırmalarının, hem de topoloji bütünlüğünün yaşam süresi üzerindeki etkisi ortaya çıkarılacaktır. Bunun yanında, bu yaklaşım sayesinde en önemli düğüme yapılan tek düğüm saldırısının ağ yaşam süresine olan etkisi tanımlanabilecektir [25].

2. SİSTEM MODELİ

Çalışmada oluşturulan ağ modelinde merkezde tek bir baz istasyonu bulunan daire şeklinde bir topoloji bulunmaktadır. Baz istasyonu, N adet algılayıcı düğümünden veri toplamaktadır. Algılayıcı düğümleri topolojide düzgün dağılım kullanılarak rastgele yerleştirilmiştir. Her düğüm-i aynı miktarda veri (s_i) üretmekte ve diğer algılayıcı düğümlerinin verilerini baz istasyonuna iletmektedir. Ağ topolojisi yönlü grafik olarak gösterilmektedir, $G = (V, A)$. V, topolojide bulunan baz istasyonu ve bütün algılayıcı düğümleri belirtmektedir. Ayrıca $W = V \setminus \{1\}$, baz istasyonu hariç bütün algılayıcı düğümlerini temsil etmektedir. $A = \{(i, j) : i \in W, j \in V - i\}$, düğümlerin gönderdikleri bütün akıları belirtmekte ve düğümlerin kendilerine veri göndermediğini garantilemektedir.

DP modelleri verilen kısıtlar ile en iyi sonuçları bulmak için kullanılmaktadır. Alternatifler, amaç fonksiyonu değerlerine bakılarak karşılaştırılmakta ve en iyi değere sahip olan ideal çözüm olarak seçilmektedir. Çalışmadaki amaç fonksiyonu, toplam üretilen verinin en yüksek değere çıkarılmasıdır. Bu da t değerini en yüksek değere çıkarılması ile sağlanabilir. Ağ yaşam süresi, diğer algılayıcı düğümlere kıyasla enerjisini daha hızlı bir şekilde tüketen düğüm tarafından belirlenir. Yaşam süresinin en yüksek olabilmesi için bütün algılayıcı düğümlerin enerjilerini dengeli şekilde harcaması sağlanmalıdır. Kullanılan doğrusal programlama modelinin sayısal analizleri GAMS ile yapılmıştır [26].

$$f_{ij} \geq 0 \ \forall (i,j) \in A \tag{2.1}$$

$$\sum_{j \in V} f_{ij} = \sum_{j \in W} f_{ji} + s_i t \ \forall i \in W \tag{2.2}$$

$$\sum_{j \in V} E^{opt}_{tx,ij} f_{ij} + E_{rx} \sum_{j \in W} f_{ji} \leq e_i \ \forall i \in W \tag{2.3}$$

Denklem (2.1), topolojide bulunan bütün akıların negatif değer almamasını sağlamaktadır. Denklem (2.2), baz istasyonu hariç bütün algılayıcı düğümlerdeki akıların dengeli olma kısıtıdır. Akıların dengeli olması bütün algılayıcı düğümlerin

aynı zamanda enerjilerini tüketmesini sağlamaktadır. Düğümden dışarı yönlü olan verinin, üretilen ve diğer düğümlerden alınan veriye eşit olduğunu göstermektedir. Denklem (2.3), her bir algılayıcı düğümün üzerinde bulunan pil enerjisinden daha fazla enerji harcamadığını garanti etmektedir. Baz istasyonu hariç bütün algılayıcı düğümlerin eşit miktarda enerjiye sahip olduğu kabul edilmektedir. Her algılayıcı düğümün enerji miktarı $e_i = 3J$ olarak belirlenmiştir.

Algılayıcı düğümlerin enerji tüketim modeli [3]'de sunulan ve CC1000 radyo kullanan Mica2 mote cihazının değerlerinden oluşmaktadır. İletim uzaklığı ve buna uygun enerji kaybı değerleri Çizelge 2.1'de gösterilmektedir. Güç seviyesi l için enerji kaybı E_{tx}^{l} ve bu seviye için en fazla iletim uzaklığı R_{max}^{l} ile ifade edilmektedir.

Düğüm-i ve düğüm-j arasındaki (d_{ij}) uzaklık maksimum olan 82.92m değerinden daha fazla olduğunda düğümler arasında herhangi veri alış verişi yapılmamaktadır. Bu değerden uzaktaki baz istasyonuna diğer düğümler ile işbirliği yapılarak veri gönderilmektedir. Her algılayıcı düğüm ideal iletim enerjisini dinamik olarak denklem 2.4'de belirtilen şekilde seçmektedir. Kaynak düğüm-i ve hedef düğüm-j arasında her bit için iletim enerjisi değişiklik göstermesine rağmen bir bit için alma enerjisi değişmemekte ve sabit kalmaktadır. Alma enerjisi olarak $E_{rx} = 0.923\ \mu J/bit$ kullanılmaktadır.

Tablo 2.1. Mica2 Motes, iletme enerjisi (μJ/bit) ve iletim uzaklığıyla (M) değişen güç seviyeleri ([3] makalesindeki verilerden hesaplanmıştır.)

l	E_{tx}^{l}	R_{max}^{l}	l	E_{tx}^{l}	R_{max}^{l}
1	0.672	19.30	14	0.844	41.19
2	0.688	20.46	15	0.867	43.67
3	0.703	21.69	16	1.078	46.29
4	0.706	22.69	17	1.133	49.07
5	0.711	24.38	18	1.135	52.01
6	0.724	25.84	19	1.180	55.13
7	0.727	27.39	20	1.234	58.44
8	0.742	29.03	21	1.313	61.95
9	0.758	30.78	22	1.344	65.67
10	0.773	32.62	23	1.445	69.61
11	0.789	34.58	24	1.500	73.79
12	0.813	36.66	25	1.664	78.22
13	0.828	38.86	26	1.984	82.92

$$E_{tx,ij}^{opt} = \left\{ \begin{array}{c} E_{tx}^{(l-1)} \; if \; d_{ij} \leq R_{max}^{(l-1)} \\ \\ \infty \; else \; if \; d_{ij} \geq R_{max}^{(l-26)} \\ \\ E_{tx}^{(l+1)} \; else \; if \; R_{max}^{l} < d_{ij} \leq R_{max}^{(l+1)} \end{array} \right\} \tag{2.4}$$

3. ANALİZLER

Bu bölümde, tek bir düğümün topolojiden çıkarılmasının KAA yaşam süresine olan etkisi incelenmiştir. Çalışmanın amacı, KAA sistemlerinin bir düğümü çalışmaz hale getirecek saldırılara karşı hassasiyet seviyesini incelemektir. Ayrıca topolojide bulunan en önemli algılayıcı düğümün servis dışı bırakılması durumunda yaşam süresinin nasıl değiştiği araştırılmaktadır. Algılayıcı düğüm sayısının, yapılan servis dışı bırakma saldırısına karşı verdiği cevabın incelenmesi için 75 ve 150 arasında değişen algılayıcı düğüm bulunan topolojiler oluşturulmuştur.

Çalışmalarda kullanılan ağ topolojileri 100m ve 200m arasında değişen çaplardaki dairesel sistemlerdir. Her senaryo farklı düğüm ve yarıçap için oluşturulmaktadır. Bir düğümün topolojiden çıkarılmasıyla ağ yaşam süresi hesaplanmakta ve bütün düğümlerin çalıştığı durum ile karşılaştırılmaktadır. Karşılaştırma sonucunda yaşam süresinin değişimi yüzde olarak hesaplanmaktadır. Her senaryo, 80-100 kere tekrar edilmiştir. Örneğin, 75 düğüm bulunan ve 100m çapa sahip bir topoloji için düğümler tekrar sayısı kadar rastgele konumlandırılmıştır. Çalışma sonucunda ağ yaşam süresine olan etkinin maksimum ve minimum olduğu değerler belirlenmiştir. Burada maksimum etkiye sahip düğümün en kritik düğüm olduğu varsayılmaktadır. Ayrıca aynı düğüm sayısına ve çapa sahip topolojiler için ortalama maksimum ve ortalama minimum yaşam süresi değişimleri hesaplanmıştır. Yaşam süresinde oluşan ortalama maksimum değeri ise en kritik düğümün yaşam süresine olan ortalama etkisini göstermektedir.

Şekil 3.1, 3.2, 3.3 ve 3.4 sırasıyla 75, 100, 125 ve 150 algılayıcı düğüm için tek düğüm saldırısından sonra ağ yaşam süresindeki değişikliğin maksimum, minimum, ortalama maksimum ve ortalama minimum olduğu değerleri göstermektedir. Ağ yaşam süresindeki negatif değerler, yaşam süresindeki artışı göstermektedir.

Tek düğümün servis dışı bırakılması yaşam süresini bazı durumlarda azaltmakta bazı durumlarda ise arttırmaktadır. Analizler, her topoloji için yaşam süresindeki

azalma değerlerinin artma değerlerine göre daha fazla olduğunu göstermektedir. Bu değişiklik miktarları boyut olarak daha büyük olan topolojilerde daha fazla olmaktadır. Örneğin, ağ yaşam süresindeki maksimum düşüş 75, 100, 125 ve 150 algılayıcı düğüm bulunduran topolojiler için sırasıyla 46.5%, 27.5%, 16.7% ve 7.8% olmaktadır. Yaşam süresindeki düşüşün aksine, artışı gösteren minimum değişim değerleri aynı sayıda algılayıcı düğüm bulunduran topolojiler için sırasıyla 16.1%, 13.9%, 4.5% ve 2.1% olmaktadır.

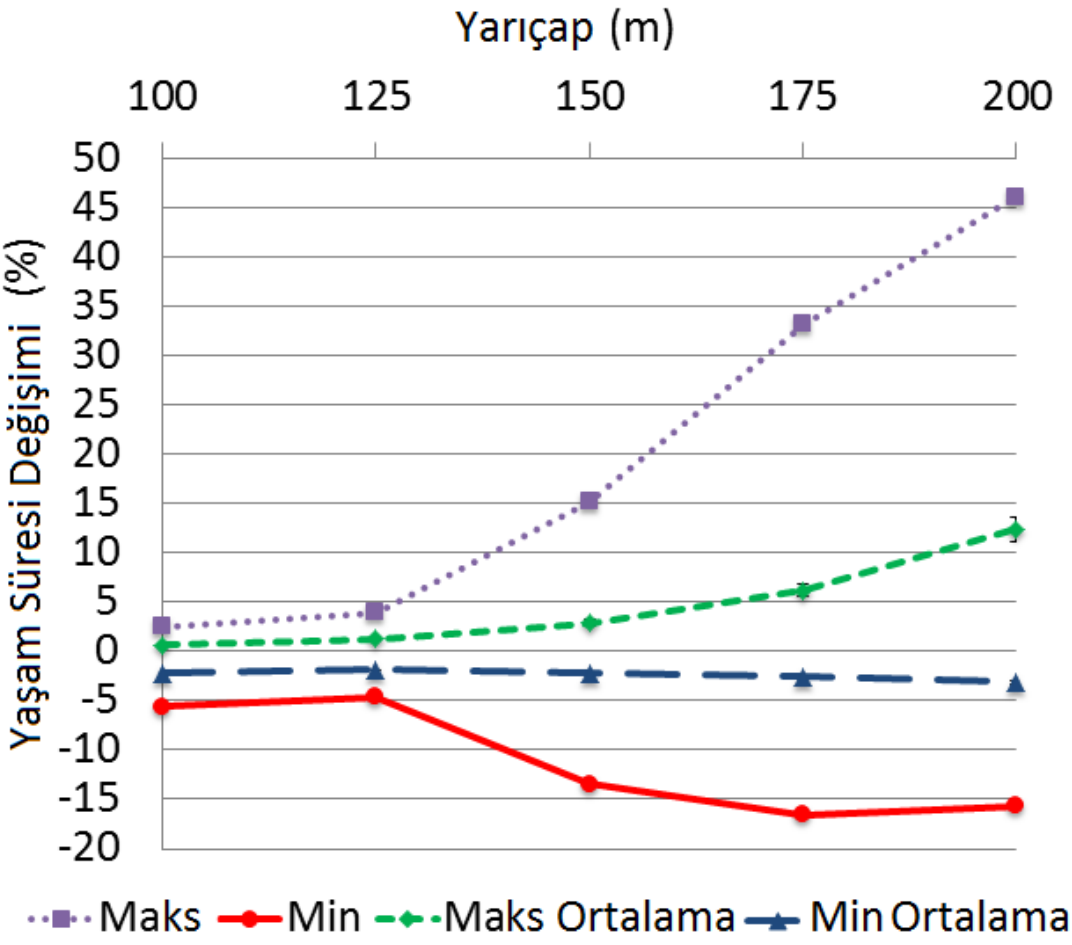
Yaşam süresindeki ortalama maksimum ve ortalama minimum değişimlerine bakıldığında tek düğüm saldırılarının ağ yaşam süresine etkisinin sınırlı olduğu görülmektedir. Ağ yaşam süresindeki ortalama maksimum düşüş 75, 100, 125 ve 150 algılayıcı düğüm bulunduran topolojiler için 12.5%, 5.0%, 2.6% ve 1.5% olmaktadır. Yaşam süresindeki düşüşün aksine, artışı gösteren ortalama minimum değişim değerleri aynı sayıda algılayıcı düğüm bulunduran topolojiler için sırasıyla 2.1%, 2.0%, 1.0% ve 0.9% olmaktadır.

KAA topolojisindeki en önemli düğüme yapılan saldırı, kritik olmayan düğüme yapılan saldırıya karşı yaşam süresinin daha fazla azalmasına neden olmaktadır. Örneğin, 3.1'de gösterilen 200m yarıçapa ve 75 algılayıcı düğüme sahip topolojide, maksimum yaşam süresindeki düşüş 46.5% olmaktadır. Ortalama düşüşün 12.5% değerinde kalması, tek düğüm saldırılarında yaşam süresinin kritik düğümler için daha fazla etkiye sahip olduğunu göstermektedir. Aynı durum farklı yarıçapa ve düğüm sayısına sahip topolojiler için geçerlidir.

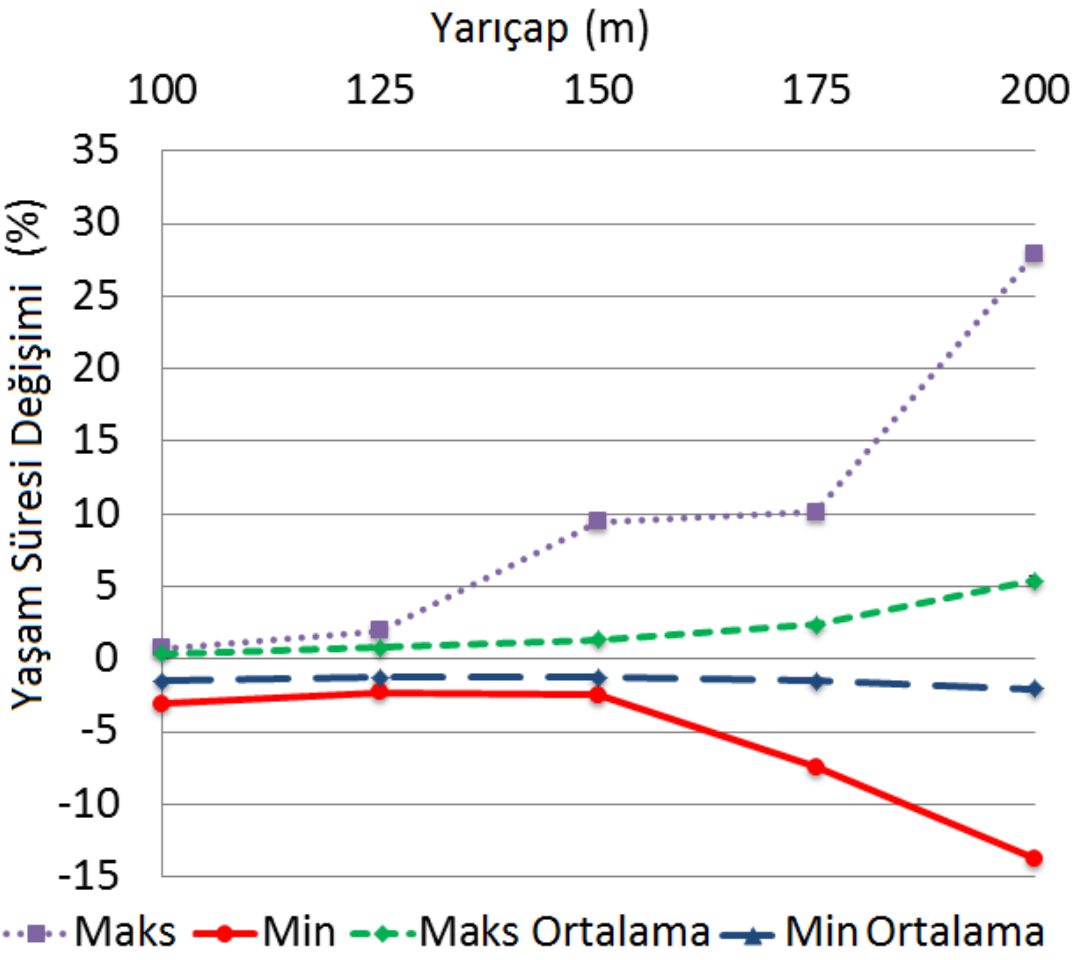
Elde edilen veriler, yaşam süresindeki değişimin algılayıcı düğüm yoğunluğuna büyük ölçüde bağlı olduğunu göstermektedir. Algılayıcı düğüm yoğunluğu fazla olan topolojilerde yaşam süresindeki azalma sınırlı olmaktadır. Bu çalışmada 150 algılayıcı düğüme sahip 100m yarıçapındaki topoloji en fazla yoğunluğa sahiptir ve 3.4'de görülen yaşam süresindeki maksimum düşüş 0.4% ve ortalama maksimum düşüş 0.2% değerinde kalmaktadır.

Düğüm yoğunluğunun düşmesi yaşam süresine olan etkiyi artırmaktadır. Bunun

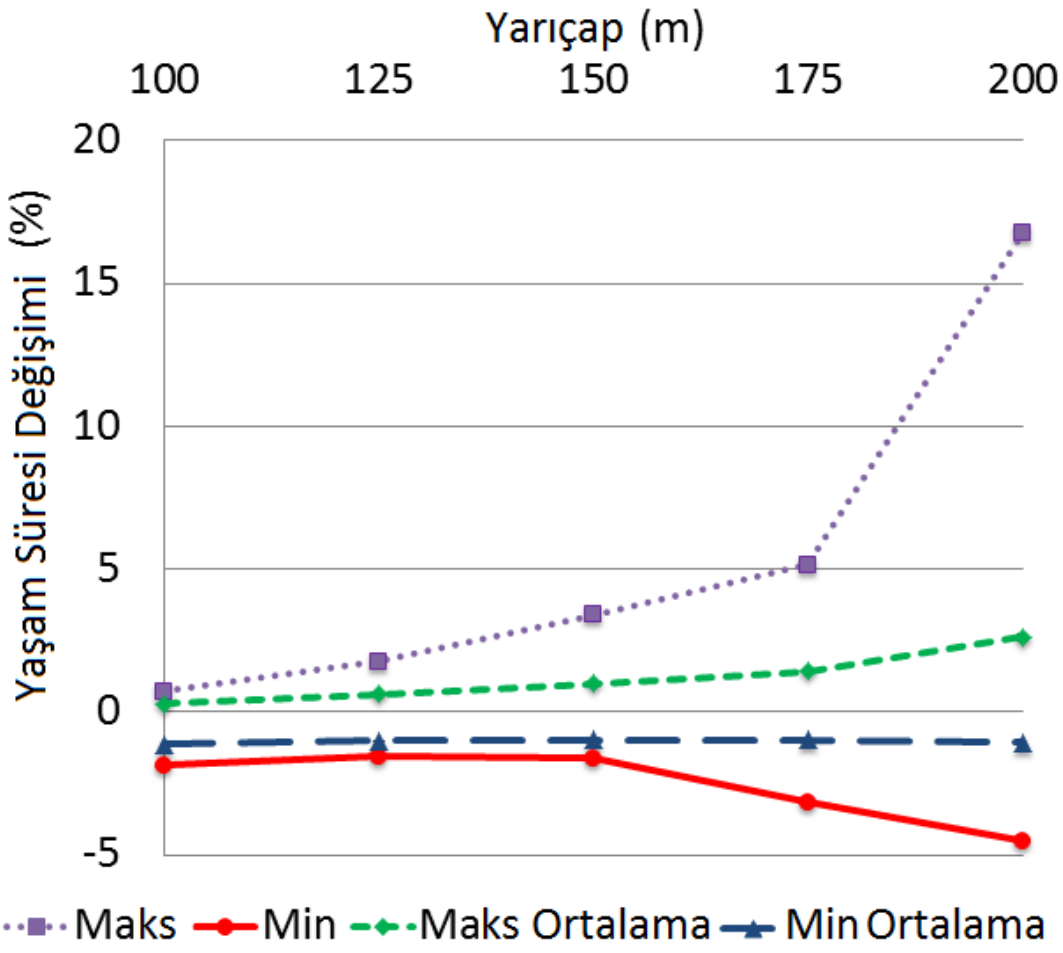
nedeni, düşük düğüm yoğunluğu bulunan ağlarda belirli düğümlerin enerji kaybını dengelemesi için az komşusunun bulunmasıdır. Böyle bir kritik düğümün devre dışı bırakılması durumunda belirli düğümlerin verilerini gönderecek başka bir düğüm bulamamasından dolayı yaşam süresi maksimum seviyede azalmaktadır. Daha fazla yoğunluğa sahip topolojilerde kritik düğümlerin bulunması daha zordur. Bunun nedeni ise düğümlerin daha fazla komşu ile veri gönderme şanslarının olmasıdır. Şekil 3.1, 3.2, 3.3 ve 3.4'de düğüm sayısının artmasıyla yaşam süresindeki maksimum düşüşün azaldığı görülmektedir. Yaşam süresindeki düşüşlerin 75, 100, 125 ve 150 algılayıcı düğüm barındıran topolojiler için 46.5%, 27.5%, 16.7% ve 7.8% değerlerinde olduğu gözlemlenmiştir.



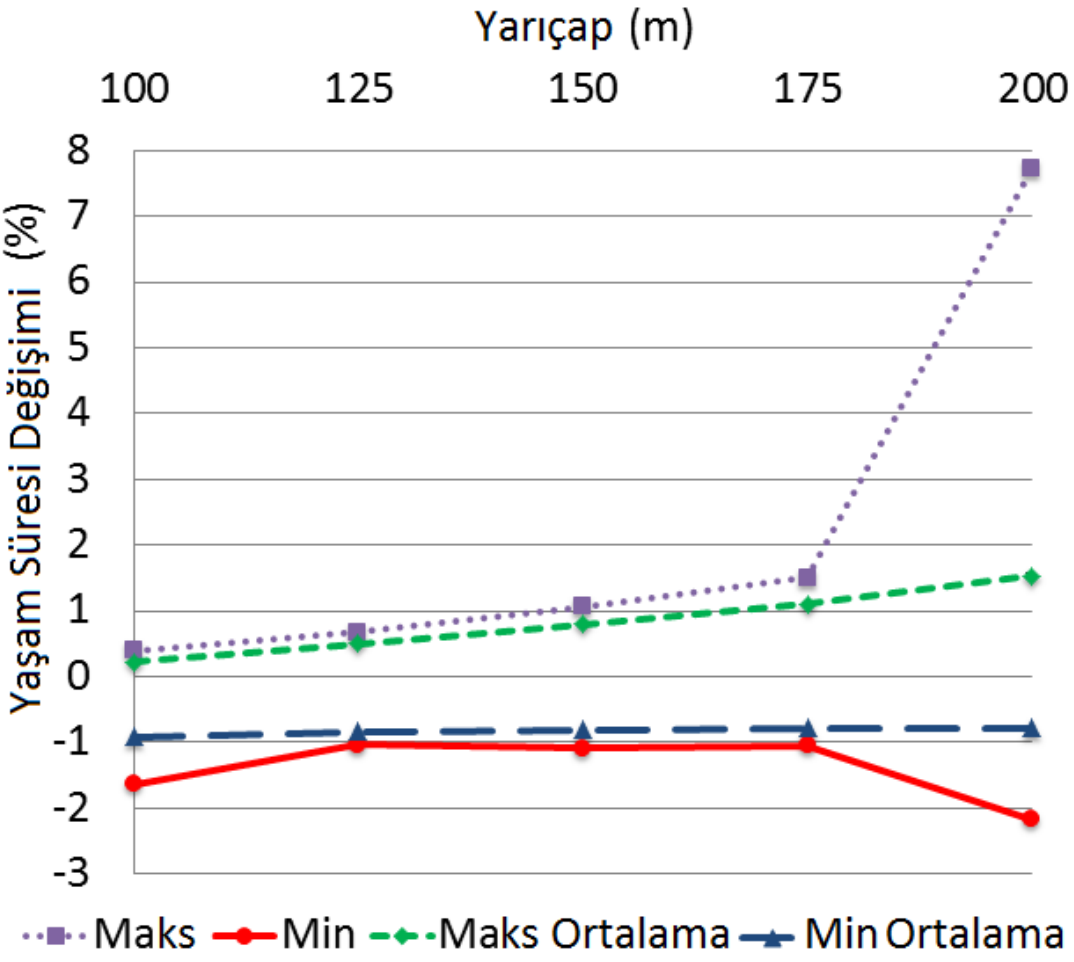
Şekil 3.1. 75 algılayıcı düğüm bulunan ve yarıçapı 100m ve 200m arasında değişen dairesel topoloji için maksimum, minimum, ortalama maksimum ve ortalama minimum yaşam süresi değişimi



Şekil 3.2. 100 algılayıcı düğüm bulunan ve yarıçapı 100m ve 200m arasında değişen dairesel topoloji için maksimum, minimum, ortalama maksimum ve ortalama minimum yaşam süresi değişimi



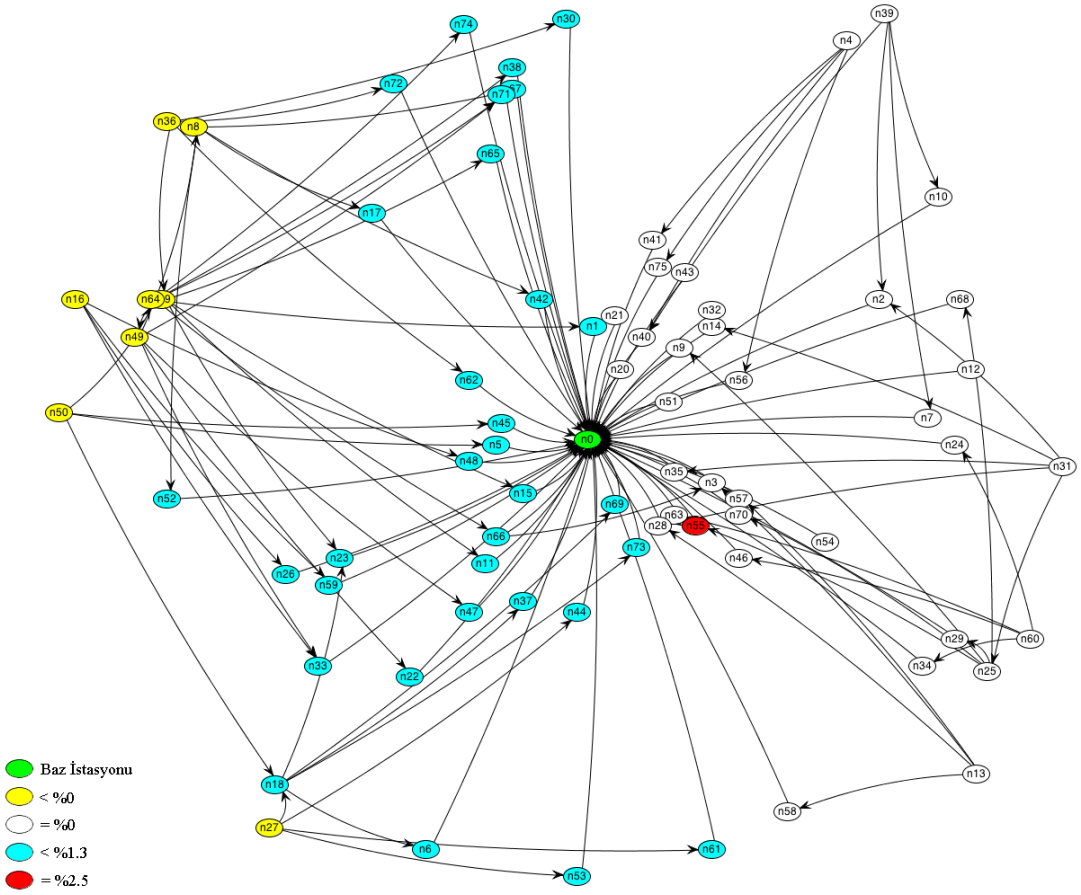
Şekil 3.3. 125 algılayıcı düğüm bulunan ve yarıçapı 100m ve 200m arasında değişen dairesel topoloji için maksimum, minimum, ortalama maksimum ve ortalama minimum yaşam süresi değişimi



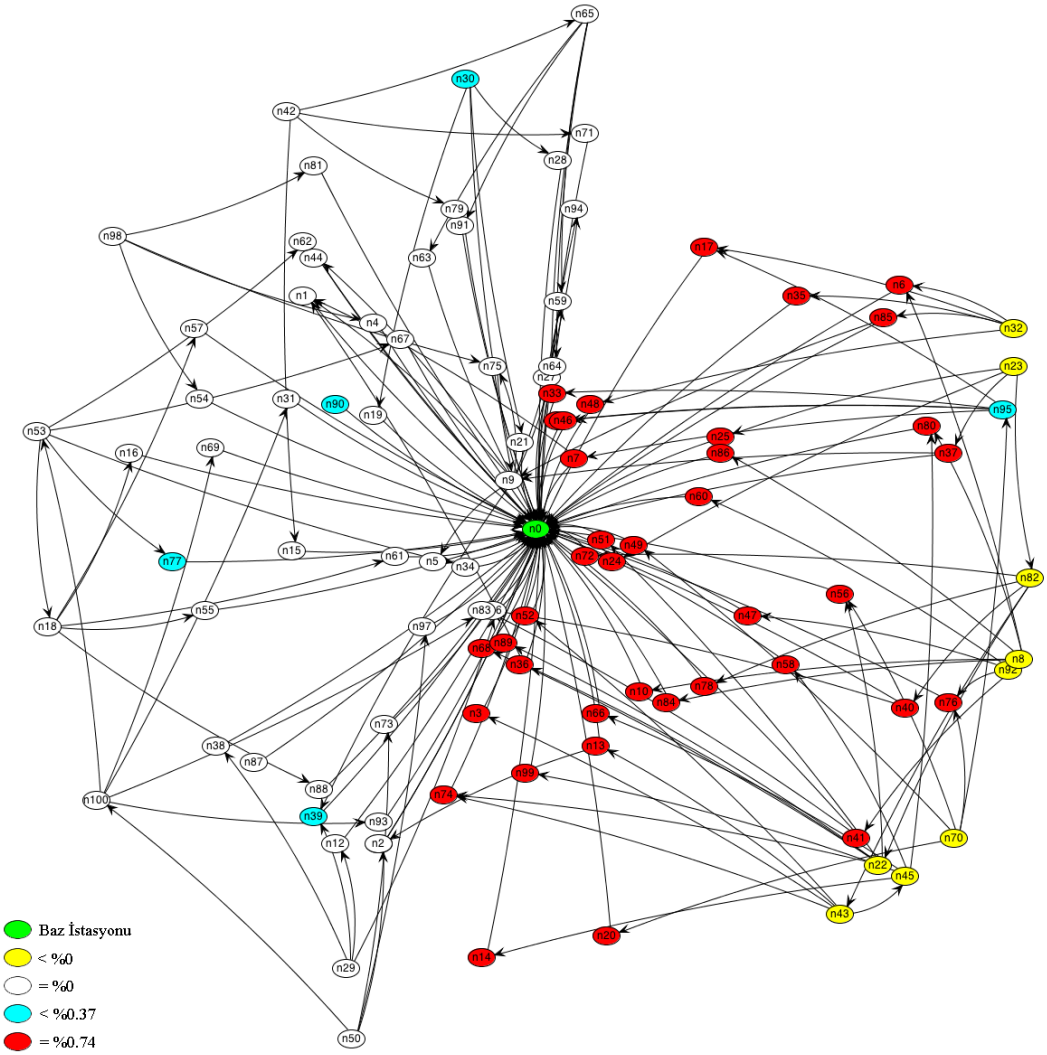
Şekil 3.4. 150 algılayıcı düğüm bulunan ve yarıçapı 100m ve 200m arasında değişen dairesel topoloji için maksimum, minimum, ortalama maksimum ve ortalama minimum yaşam süresi değişimi

Yaşam süresini azaltmasının aksine bazı düğümlerin bertaraf edilmesinin ağın yaşam süresini arttıracak bir etkisi bulunmaktadır. Şekil 3.5'de 75 düğüm bulunduran ve 100m yarıçapa sahip bir KAA topolojisinin yaşam süresi değişimleri ve bütün düğümler aktif olduğunda gerçekleşen akıları gösterilmektedir. Aynı şekilde Şekil 3.6, 3.7 ve 3.8'de yaşam süresindeki artış daha fazladır. Yaşam süresini artıran düğümlerin her birinin yaptığı etki, maksimum azaltan düğümün etkisinden daha fazla ve yaklaşık 3.5% civarındadır. Yaşam süresini artıran düğümler, baz istasyonuna veri gönderirken kullandıkları komşu düğümlerin daha fazla enerji tüketmesine neden olmaktadır.

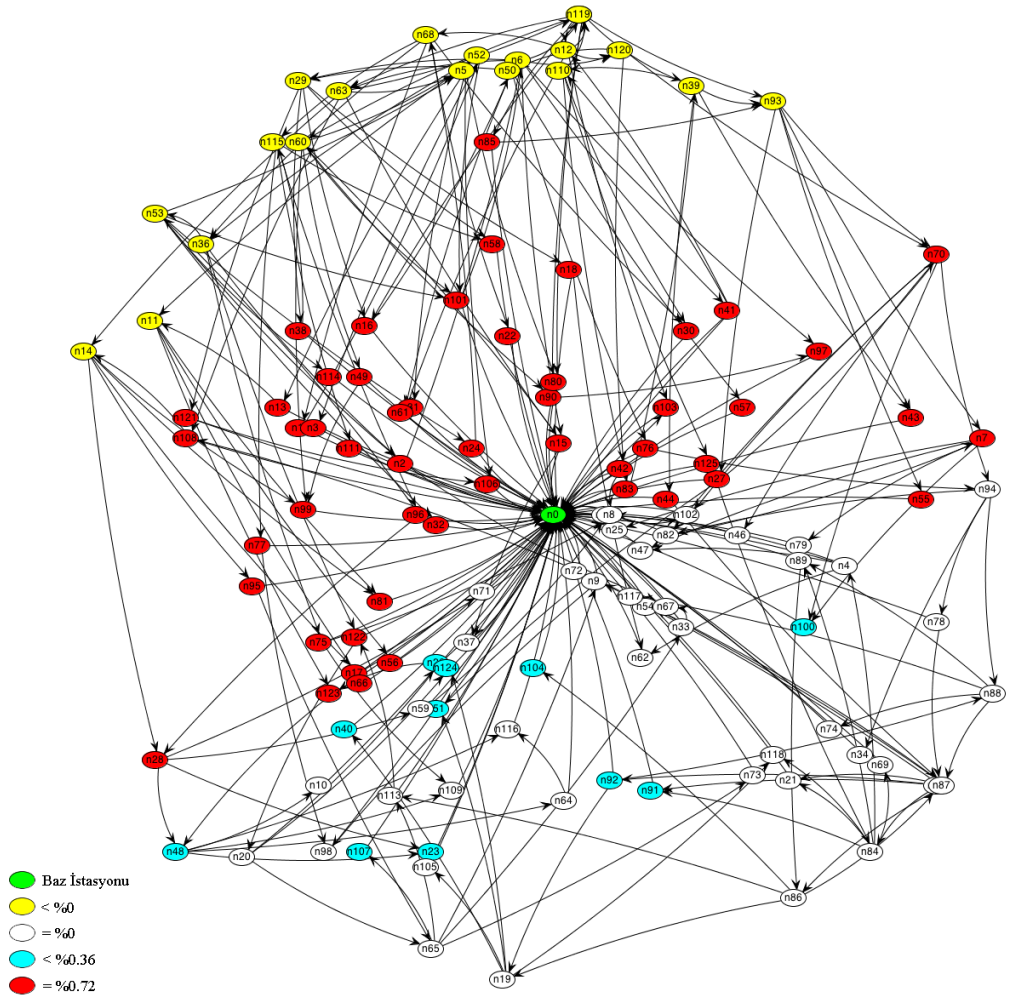
Şekil 3.1, 3.2, 3.3 ve 3.4'de yaşam süresindeki değişikliklerin düğüm sayısı ve yarıçapa göre değişimi gösterilmektedir. Her düğüm sayısı için yaşam süresindeki artışın miktarı belirli yarıçaptaki topolojilerde yaşam süresindeki düşüş miktarının üzerine çıkmaktadır. Örneğin 100m yarıçapındaki 75, 100, 125 ve 150 düğüm bulunduran topolojilerde maksimum artış sırasıyla 5%, 3%, 2% ve 1.5% değerindeyken, yaşam süresindeki düşüş 2.5%, 0.75%, 0.72% ve 0.4% değerindedir.



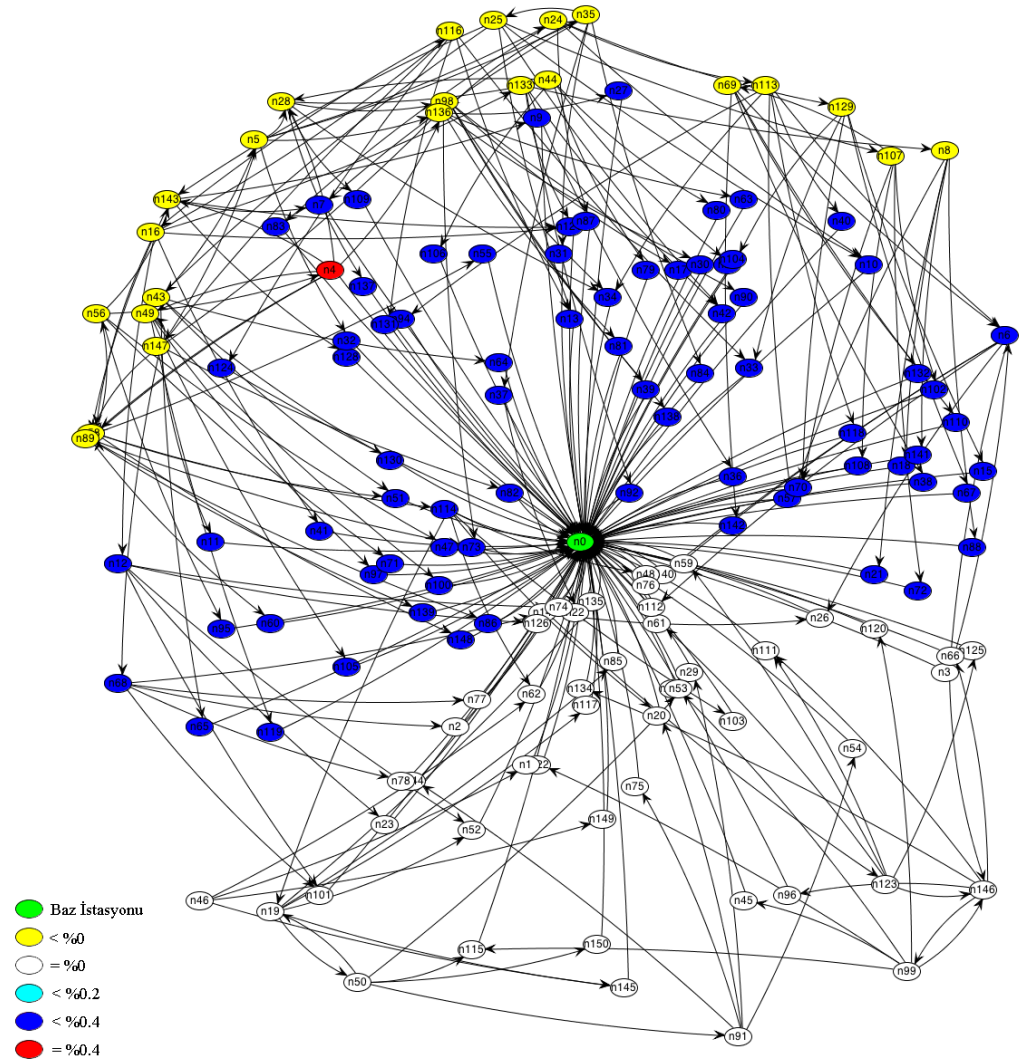
Şekil 3.5. 75 düğüm bulunan ve 100m yarıçapındaki KAA'nın yaşam süresi değişimi



Şekil 3.6. 100 düğüm bulunan ve 100m yarıçapındaki KAA'nın yaşam süresi değişimi

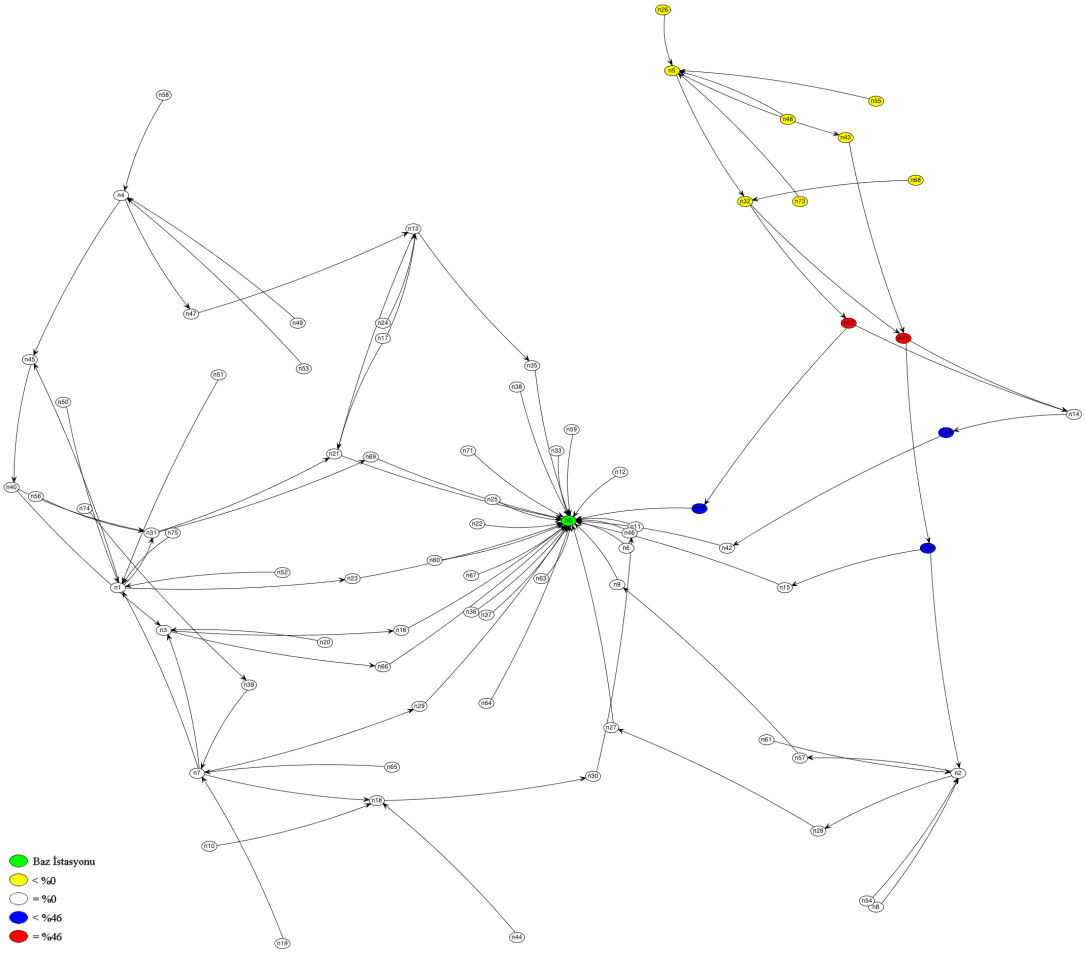


Şekil 3.7. 125 düğüm bulunan ve 100m yarıçapındaki KAA'nın yaşam süresi değişimi

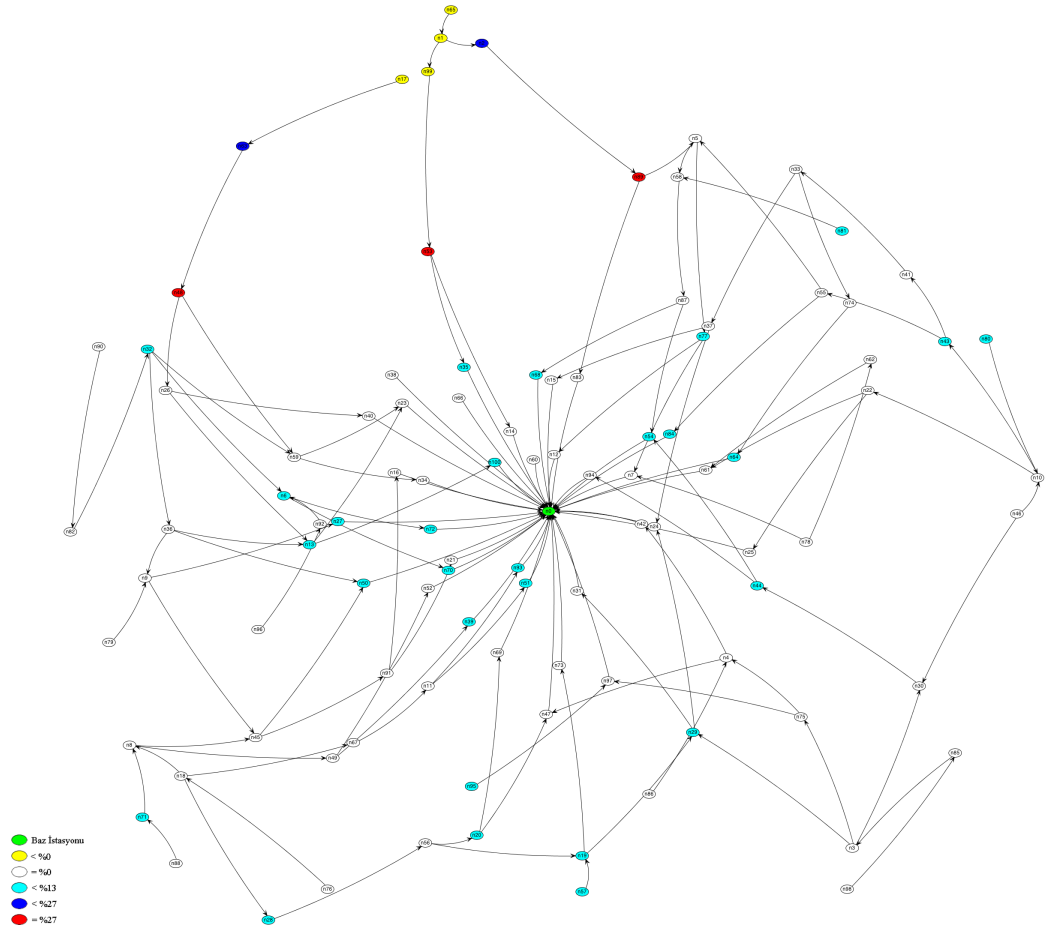


Şekil 3.8. 150 düğüm bulunan ve 100m yarıçapındaki KAA'nın yaşam süresi değişimi

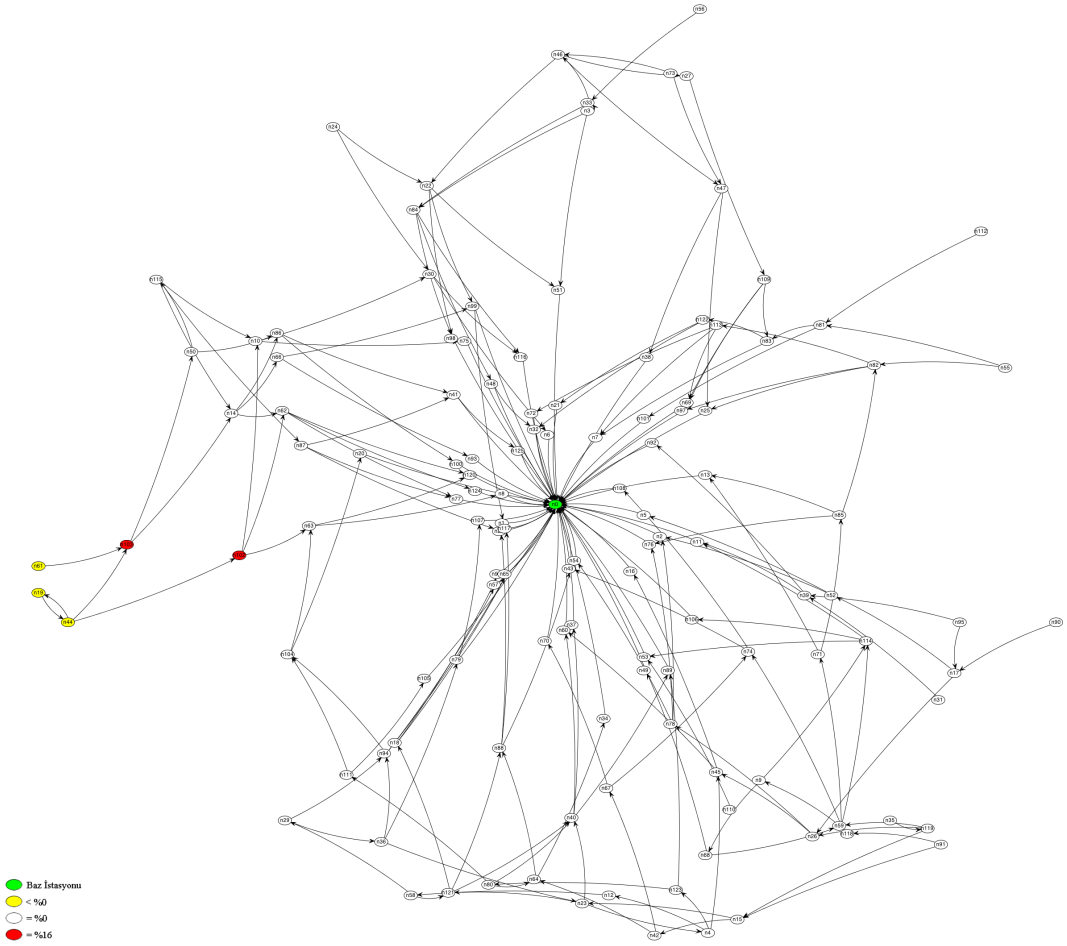
Şekil 3.9, 3.10, 3.11 ve 3.12'da bulunan KAA topolojisinde en fazla yaşam süresini düşüren düğümler, belirli bölgedeki düğümlerin baz istasyonuna ulaşması için kullanabileceği sınırlı sayıdaki alternatiflerden biridir. Topoloji bütünlüğü korunurken oluşan akılardan bu düğümlerin önemi görülmektedir.



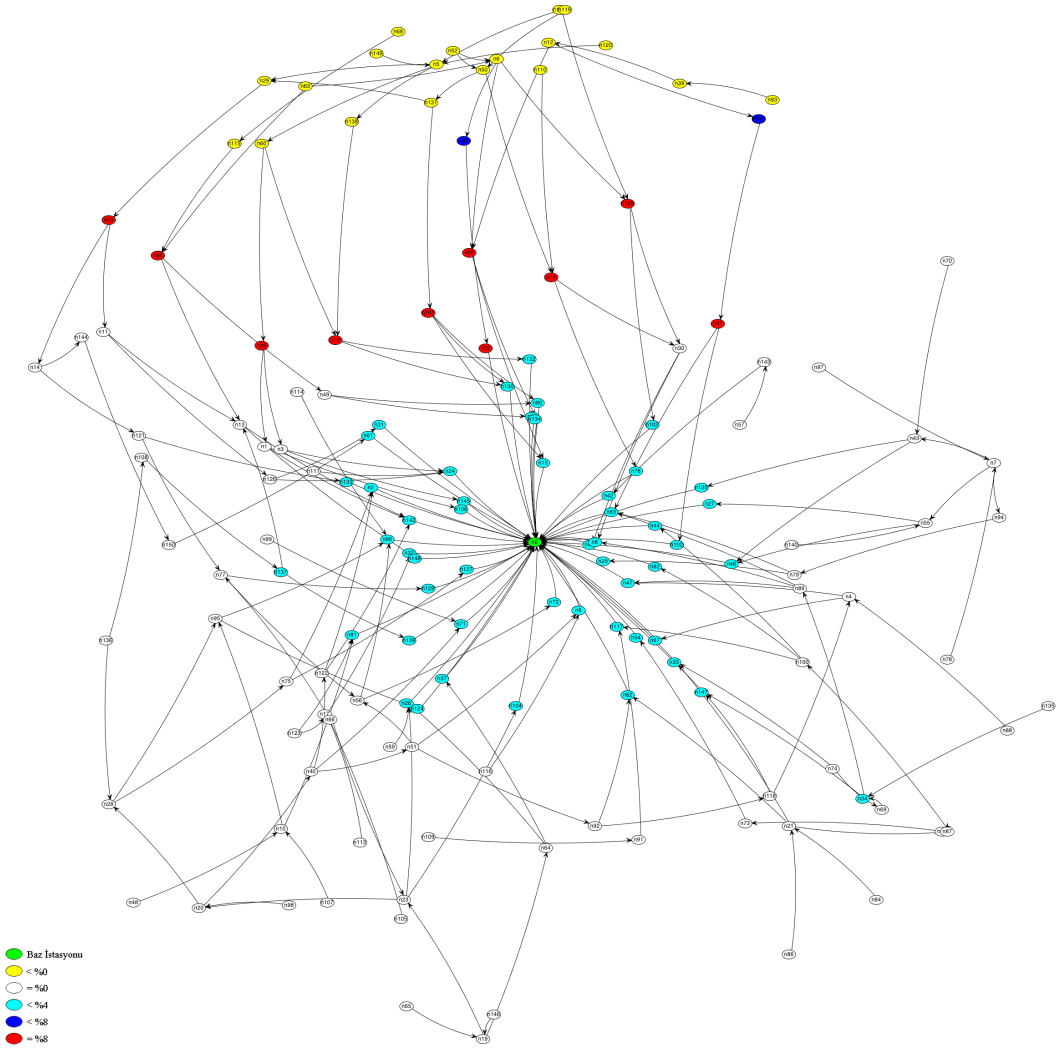
Şekil 3.9. 75 düğüm bulunan ve 200m yarıçapındaki KAA'nın yaşam süresi değişimi



Şekil 3.10. 100 düğüm bulunan ve 200m yarıçapındaki KAA'nın yaşam süresi değişimi



Şekil 3.11. 125 düğüm bulunan ve 200m yarıçapındaki KAA'nın yaşam süresi değişimi



Şekil 3.12. 150 düğüm bulunan ve 200m yarıçapındaki KAA'nın yaşam süresi değişimi

4. SONUÇ

KAA sistemleri anayurt güvenliği, medikal sistemler, askeri uygulamalar ve akıllı şebekeler gibi kritik öneme sahip sistemlerde sıkça kullanılmaktadır. Ayrıca teknolojik gelişmeler sayesinde yeni nesil sistemler için KAA entegrasyonu hızla artmaktadır. Yaygın ve askeri, sağlık vb. önemli alanlarda kullanılması, kötü niyetli kişiler tarafından yapılan saldırılara karşı bu sistemleri cazip hale getirmektedir. Saldırılar verilerin ele geçirilmesi, değiştirilmesi, düğümün veri göndermesinin engellenmesi veya servis dışı bırakılması vb. bir çok farklı amaç doğrultusunda yapılabilir.

Protokol ve algoritma tasarımlarında bulunan zafiyetler nedeniyle fiziksel katmandan uygulama katmanına birçok farklı saldırıya karşı savunmasızdır. KAA sistemlerinin daha güvenli hale gelmesi, veri kaybı ve sistem kesintilerinin yaşanmaması için saldırılara karşı güvenlik mekanizmaları oluşturulmaktadır. Güvenlik mekanizmaları bir veya birden fazla saldırıya karşı koruma veya dayanıklılık sağlasa da bütün saldırılara karşı koruma sağlamak oldukça zordur. Saldırılara karşı oluşturulan algoritmalarda yaşam süresinden, kapsama alanından veya donanım kaynaklarından fedakarlık yapılması gerekmektedir. Güvenlik ve bu tür tasarım gereklilikleri arasında kurulması gereken zor bir denge bulunmaktadır.

Fiziksel, SDB ve uyku engelleme saldırılarının etkisinin azaltılması için ağın dikkatli ve detaylı şekilde tasarlanması gerekmektedir. Yapılan çalışma ile algılayıcı düğümlerin sayısının ve konumlarının yaşam süresine olan etkisi ortaya çıkarılmıştır. Aynı boyutta ve sayıda düğüme sahip topolojilerde tek düğümün bertaraf edilmesi yaşam süresinde en fazla 46.5% ve ortalama 12.5% düşüş yaşanmaktadır. Ortalama ile maksimum arasındaki fark düğüm konumlarının bu tip saldırılardaki önemini göstermektedir. Az sayıda düğüm kullanılan topolojilerde yaşam süresinde önemli azalmalar yaşanmaktadır. 75 düğüm bulunduran ve 200m çapa sahip topolojide yaşam süresi 46.5% azalabilmektedir. Fakat aynı çapa sahip topolojide düğüm sayısı artırıldığı zaman yaşam süresine olan direnç belirgin derecede artmaktadır. Aynı şekilde düğüm konumlarının önemi yaşam süresindeki hem azalma hem de artma ile görülmektedir. Topolojide belirli bölgelere yerleştirilen

düğümlerin az olması o bölgeler için kritik düğümlerin artmasına neden olmaktadır.

KAA topolojilerinde bulunan tek bir düğüme yapılan saldırı her zaman aynı etkiyi yaratmamaktadır. Yaşam süresini düşüren düğümler arasında en fazla etkiye sahip düğümler bulunmaktadır. Bu düğümler topolojiler için en kritik düğüm olarak belirlenmiştir. Kritik düğümlere yapılan saldırılar algılayıcı düğüm sayısına ve topoloji boyutuna yani algılayıcı düğüm yoğunluğuna bağlı olarak farklı etkilere neden olmaktadır. Düğüm sayısının düşük olduğu büyük boyutlu topolojilerde yaşam süresi yaklaşık olarak yarı yarıya düşmektedir. Düğüm yoğunlunun artması, yaşam süresinin saldırılara karşı dayanıklı olmasını sağlamaktadır. Oluşturulan modeller içerisinde en fazla düğüm yoğunluğuna sahip topolojide yaşam süresindeki azalma 0.3% civarındadır.

Tek düğümün bertaraf edilmesi bazı durumlarda yaşam süresini artırmaktadır. Bu artış düğüm sayısı ve topoloji boyutuna bağlı olarak azalmadan daha fazla olmaktadır. KAA topolojilerinde düğüm konumlandırmasına dikkat edilmesi ile yaşam süresinde artış sağlanabilmektedir. Yaşam süresinin artmasındaki en büyük etken servis dışı bırakılan düğümün verilerinin iletilmesi için kullanılan enerjinin diğer düğüm tarafından veri üretiminde kullanılmasıdır.

Yaşam süresinin tek düğüm saldırıları sonucunda büyük oranda değişebileceği ortaya çıkarılmıştır. Yapılan çalışma ile düğüm konumlandırmasına, sayısına bağlı olarak tasarımların yapılmasının ne kadar önemli olduğu gösterilmektedir. Saldırıların, tek düğüm ile sınırlı kalmaması durumunda etkileri beklenenden fazla olabilir.

Kaynakca

[1] A. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[2] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," *Pervasive Computing, IEEE*, vol. 7, no. 1, pp. 74–81, 2008.

[3] J. Vales-Alonso, E. Egea-López, A. Martínez-Sala, P. Pavón-Mariño, M. Victoria Bueno-Delgado, and J. García-Haro, "Performance evaluation of mac transmission power control in wireless sensor networks," *Computer Networks*, vol. 51, no. 6, pp. 1483–1498, 2007.

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, no. 4, pp. 393–422, 2002.

[5] E. Hossain, Z. Han, and H. V. Poor, *Smart grid communications and networking*. Cambridge University Press, 2012.

[6] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *Industrial Electronics, IEEE Transactions on*, vol. 57, no. 10, pp. 3557–3564, 2010.

[7] K. Römer, O. Kasten, and F. Mattern, "Middleware challenges for wireless sensor networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 6, no. 4, pp. 59–61, 2002.

[8] R. Dubey, V. Jain, R. Thakur, and S. Choubey, "Attacks in wireless sensor networks," *International Journal of Scientific & Engineering Research*, vol. 3, no. 3, 2012.

[9] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," *Dependable and Secure Computing, IEEE Transactions on*, vol. 8, no. 5, pp. 685–698, 2011.

[10] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc networks*, vol. 1, no. 2, pp. 293–315, 2003.

[11] B. Prasannajit, S. Anupama, K. Vindhykumari, S. Subhashini, G. Vinitha, *et al.*, "An approach towards detection of wormhole attack in sensor networks," in *Integrated Intelligent Computing (ICIIC), 2010 First International Conference on*, pp. 283–289, IEEE, 2010.

[12] D. E. Boubiche and A. Bilami, "A defense strategy against energy exhausting attacks in wireless sensor networks," *Journal of Emerging Technologies in Web Intelligence*, vol. 5, no. 1, pp. 18–27, 2013.

[13] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network mac protocols," *Vehicular Technology, IEEE Transactions on*, vol. 58, no. 1, pp. 367–380, 2009.

[14] T. Bhattasali, R. Chaki, and S. Sanyal, "Sleep deprivation attack detection in wireless sensor network," *arXiv preprint arXiv:1203.0231*, 2012.

[15] X. Wang, S. Chellappan, W. Gu, W. Yu, and D. Xuan, "Search-based physical attacks in sensor networks," in *Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference on*, pp. 489–496, IEEE, 2005.

[16] Z. Cheng, M. Perillo, and W. B. Heinzelman, "General network lifetime and cost models for evaluating sensor network deployment strategies," *IEEE Transactions on Mobile Computing*, vol. 7, pp. 484–497, April 2008.

[17] Y. Shen, N. P. Nguyen, Y. Xuan, and M. T. Thai, "On the discovery of critical links and nodes for assessing network vulnerability," *IEEE/ACM Transactions on Networking (TON)*, vol. 21, no. 3, pp. 963–973, 2013.

[18] H. Liu, X. Cao, J. He, P. Cheng, J. Chen, and Y. Sun, "Distributed identification of the most critical node for average consensus," *The International Federation of Automatic Control*, 2014.

[19] W. Gu, *Defending Against Node-targeted Attacks in Wireless Networks*. PhD thesis, The Ohio State University, 2008.

[20] M. Younis and K. Akkaya, "Strategies and techniques for node placement in wireless sensor networks: A survey," *Ad Hoc Networks*, vol. 6, no. 4, pp. 621–655, 2008.

[21] P. Cheng, C. Chuah, and X. Liu, "Energy-aware node placement in wireless sensor networks," in *Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE*, vol. 5, pp. 3210–3214, 2004.

[22] K. Ssu, C. Ou, and H. C. Jiau, "Localization with mobile anchor points in wireless sensor networks," *Vehicular Technology, IEEE Transactions on*, vol. 34, no. 5, pp. 1187–1197, 2005.

[23] L. Nian-qiang and L. Ping, "A range-free localization scheme in wireless sensor networks," in *Knowledge Acquisition and Modeling Workshop, 2008. KAM Workshop 2008. IEEE International Symposium on*, pp. 525–528, 2008.

[24] E. L. Lloyd and G. Xue, "Relay node placement in wireless sensor networks," *Computers, IEEE Transactions on*, vol. 56, no. 1, pp. 134–138, 2007.

[25] H. Cotuk, K. Bicakci, B. Tavli, and E. Uzun, "The impact of transmission power control strategies on lifetime of wireless sensor networks," *IEEE Transactions on Computers*, 2014.

[26] *General Algebraic Modeling System (GAMS)*. http://www.gams.com/, 2013.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı	: YÜKSEL, Anıl
Uyruğu	: T.C.
Doğum Tarihi ve Yeri	: 25.09.1988, Ankara
Medeni Hali	: Bekar
Telefon	: 0507 943 40 75
E-mail	: anil.yuksel@etu.edu.tr

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Y. Lisans	TOBB ETÜ, Elektrik-Elektronik Müh.	2015
Lisans	TOBB ETÜ, Elektrik-Elektronik Müh.	2011

İş Deneyimi

Yıl	Yer	Görev
01.2014-Halen	Havelsan A.Ş.	Siber Güvenlik Mühendisi
05.2013-01.2014	Havelsan A.Ş.	Ağ Mühendisi
12.2011-04.2013	Tübitak YTE	Ağ Mühendisi

Yabancı Dil

İngilizce

Yayınlar

Anıl Yüksel, Erkam Uzun, Bülent Tavlı: The Impact Of Elminiation Of The Most Critical Node On Wireless Sensor Network Lifetime. IEEE Sensor Applications Symposium 2015