



**T.C.
MUSTAFA KEMAL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

**KÜMELEME TABANLI KABLOSUZ ALGILAYICI AĞLARDA
SINKHOLE SALDIRILARININ TESPİT EDİLMESİ**

Merve Nilay AYDIN

ENFORMATİK ANABİLİM DALI

YÜKSEK LİSANS TEZİ

**HATAY
EYLÜL-2015**



T.C.
MUSTAFA KEMAL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

**KÜMELEME TABANLI KABLOSUZ ALGILAYICI AĞLARDA
SINKHOLE SALDIRILARININ TESPİT EDİLMESİ**

Merve Nilay AYDIN

ENFORMATİK ANABİLİM DALI

YÜKSEK LİSANS TEZİ

**HATAY
EYLÜL-2015**

T.C.
MUSTAFA KEMAL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

**KÜMELEME TABANLI KABLOSUZ ALGILAYICI AĞLARDA SINKHOLE
SALDIRILARININ TESPİT EDİLMESİ**

MERVE NİLAY AYDIN

ENFORMATİK ANABİLİM DALI

YÜKSEK LİSANS TEZİ

Yrd. Doç. Dr. İpek ABASIKELEŞ TURGUT danışmanlığında hazırlanan bu tez
03/09/2015 tarihinde aşağıdaki jüri üyeleri tarafından **OYBİRLİĞİ** ile kabul edilmiştir.

Yrd. Doç. Dr. İpek ABASIKELEŞ TURGUT
Başkan

Yrd. Doç. Dr. Yakup KUTLU
Üye

Doç. Dr. Mutlu AVCI
Üye

Kod No: 859

Prof. Dr. Okan ŞENER
Enstitü Müdür V.

Not: Bu tezde kullanılan özgün ve başka kaynaktan yapılan bildirişlerin, çizelge, şekil ve fotoğrafların kaynak gösterilmeden kullanımı, 5846 sayılı Fikir ve Sanat Eserleri Kanunundaki hükümlere tabidir.

03/09/2015

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını ve tez üzerinde Yükseköğretim Kurulu tarafından hiçbir değişiklik yapılamayacağı için tezin bilgisayar ekranında görüntülendiğinde asıl nüsha ile aynı olması sorumluluğunun tarafıma ait olduğunu beyan ederim.

Merve Nilay AYDIN

ÖZET

KÜMELEME TABANLI KABLOSUZ ALGILAYICI AĞLARDA SINKHOLE SALDIRILARININ TESPİT EDİLMESİ

Kablosuz algılayıcı ağlar (KAA) küçük, düşük maliyetli, kablosuz iletişimi kullanan yüzlerce hatta binlerce algılayıcıdan oluşan ve birçok çevreye uyarlanabilen ağlardır. KAA' lar ile gerçekleştirilen uygulamaların çoğu dışarıdan gelebilecek saldırılara açıktır. Bu saldırılardan en tehlikeli olanlarından birisi de sinkhole saldırıdır. Sinkhole saldırılarının tespit edilebilmesi için öncelikle sistemin modellenmesi gerekmektedir. Bu çalışmada kümeleme mimarisine sahip KAA' larda sinkhole saldırıları üç farklı şekilde modellenmiş ve bu modellenen saldırılar içinden bir tanesi için kural tabanlı tespit çalışması yapılmıştır. Tespit çalışması, farklı kalan enerji eşik değerleri kullanılarak yapılmış ve sistem için hangi eşik değerinin en uygun olduğu bulunmaya çalışılmıştır.

2015, 51 sayfa

Anahtar Kelimeler: Kablosuz algılayıcı ağlar, güvenlik, sinkhole, LEACH

ABSTRACT

DETECTION OF SINKHOLE ATTACK ON CLUSTER BASED WIRELESS SENSOR NETWORKS

Wireless sensor networks (WSNs) is a small, low-cost, consisting of thousands of sensor networks using wireless communication and adaptable to many environments. Most of the applications implemented WSN 's are open to attack from outside. One of the most dangerous of these attacks are the sinkhole attack. In order to determine the sinkhole attack must first modeling the system. In this paper, sinkhole attack are modelled in three different ways on the WSN, which has a cluster-based architecture and rule based determinations are performed for one of the modelled attack. Determinations were made using different remaining energy thresholds and the threshold for the system was sought which is most suitable.

2015, 51 pages

Key Words: Wireless sensor network, security, sinkhole, LEACH

TEŞEKKÜR

Yüksek Lisans tez konusunun belirlenmesinde, araştırılması ve yazımı sırasında sahip olduğu bilgi birikimi ve tecrübesi ile çalışmayı yönlendiren ve her türlü yardımı esirgemeyen saygıdeğer danışman hocam Yar.Doç. Dr. İpek ABASIKELEŞ TURGUT' a sonsuz saygı ve teşekkürlerimi sunarım.

Çalışmalarım sırasında desteğini esirgemeyen Arş.Gör. Kadir TOHMA' ya ve her zaman yanımda olan aileme çok teşekkür ederim.

İÇİNDEKİLER

ÖZET	I
ABSTRACT	II
TEŞEKKÜR.....	III
İÇİNDEKİLER	IV
ÇİZELGELER DİZİNİ	V
ŞEKİLLER DİZİNİ.....	VI
1. GİRİŞ.....	1
2. ÖNCEKİ ÇALIŞMALAR.....	9
3. MATERYAL ve YÖNTEM.....	13
3.1. Materyal	13
3.2.Yöntem.....	14
3.2.1. Model 1	14
3.2.2. Model 2	14
3.2.3. Model 3	17
3.3. Sinkhole Saldırıların Tespit Edilmesi	18
3.4. Simülasyon Parametreleri	19
3.4.1. Sistemde Üretilen Mesajlar	19
3.4.2. Simülasyon Parametreleri	21
4. ARAŞTIRMA BULGULARI VE TARTIŞMA.....	22
4.1. Model Zarar Değerlendirmeleri	22
4.2. Tespit Çalışması Sonuçları.....	25
5. SONUÇ VE ÖNERİLER	47
KAYNAKLAR	49
ÖZGEÇMİŞ	51

ÇİZELGELER DİZİNİ

Çizelge 3.1.	Sistemde kullanılan yönlendirme protokolü mesajları	19
Çizelge 3.2.	Sistemde kötü niyetli düğümleri tespit etmek için kullanılan mesajlar.....	20
Çizelge 3.3.	Sistemde kullanılan paket içeriği.....	20
Çizelge 3.4.	Eşik değeri seçiminin farkları.....	21
Çizelge 3.5.	Simülasyon Parametreleri.....	21
Çizelge 4.1.	50 Düğüm için kötü niyetli düğüm yakalama oranı	28
Çizelge 4.2.	100 Düğüm için kötü niyetli düğüm yakalama oranı	31
Çizelge 4.3.	150 Düğüm için kötü niyetli düğüm yakalama oranı	33

ŞEKİLLER DİZİNİ

Şekil 1.1.	Algılayıcı ağların genel yapısı.	2
Şekil 1.2.	Algılayıcı ağların iç yapısı.....	2
Şekil 1.3.	Kümeleme tabanlı kablosuz algılayıcı ağların genel yapısı	4
Şekil 1.4.	Düz yönlendirme tabanlı sistemlerde sinkhole atağı.	7
Şekil 1.5.	Hiyerarşik yönlendirme tabanlı sistemlerde sinkhole atağı	8
Şekil 3.1.	OMNet++ simülasyon programı (https://omnetpp.org/).....	13
Şekil 3.2.	Kötü niyetli düğümün küme başı olma durumu	15
Şekil 3.3.	Kötü niyetli düğümün üye düğüm olma durumu.....	15
Şekil 3.4.	Kötü niyetli düğümün etki alanı içinde küme başı olma durumu.....	16
Şekil 3.5.	Kötü niyetli düğümün etki alanı içinde üye düğüm olma durumu	16
Şekil 3.6.	Kötü niyetli düğümün diğer düğümleri etki alanına alma durumu.....	17
Şekil 3.7.	Tespit mekanizması akış diyagramı.....	19
Şekil 4.1.	Baz istasyonuna ulaşan paket sayısı kıyası.	22
Şekil 4.2.	Sistemde tüketilen toplam enerji miktarı	23
Şekil 4.3.	Sistemde yaşayan düğüm sayıları	24
Şekil 4.4.	Sürekli saldırı modelinde farklı eşik değerleri için 50 düğümde tüketilen toplam enerji miktarının kıyaslanması.....	25
Şekil 4.5.	Sürekli saldırı modelinde farklı eşik değerleri için 50 düğümde gecikmelerin kıyaslanması.....	26
Şekil 4.6.	Sürekli saldırı modelinde farklı eşik değerleri için 50 düğümde yakalanan paket miktarının kıyaslanması	27
Şekil 4.7.	Sürekli saldırı modelinde farklı eşik değerleri için 100 düğümde tüketilen toplam enerji miktarının kıyaslanması.....	29
Şekil 4.8.	Sürekli saldırı modelinde farklı eşik değerleri için 100 düğümde gecikmelerin kıyaslanması.....	29
Şekil 4.9.	Sürekli saldırı modelinde farklı eşik değerleri için 100 düğümde yakalanan paket miktarının kıyaslanması	30
Şekil 4.10.	Sürekli saldırı modelinde farklı eşik değerleri için 150 düğümde tüketilen toplam enerji miktarının kıyaslanması.....	31
Şekil 4.11.	Sürekli saldırı modelinde farklı eşik değerleri için 150 düğümde gecikmelerin kıyaslanması.....	32
Şekil 4.12.	Sürekli saldırı modelinde farklı eşik değerleri için 150 düğümde yakalanan paket miktarının kıyaslanması	33
Şekil 4.13.	Sürekli saldırı modelinde farklı eşik değerleri için 200 düğümde tüketilen toplam enerji miktarının kıyaslanması.....	34
Şekil 4.14.	Sürekli saldırı modelinde farklı eşik değerleri için 200 düğümde gecikmelerin kıyaslanması.....	35
Şekil 4.15.	Sürekli saldırı modelinde farklı eşik değerleri için 200 düğümde yakalanan paket miktarının kıyaslanması	35
Şekil 4.16.	Tekil saldırı modelinde farklı eşik değerleri için 50 düğümde tüketilen toplam enerji miktarının kıyaslanması.....	37

Şekil 4.17.	Tekil saldırı modelinde farklı eşik değerleri için 50 düğümde gecikmelerin kıyaslanması.....	37
Şekil 4.18.	Tekil saldırı modelinde farklı eşik değerleri için 50 düğümde yakalanan paket miktarının kıyaslanması	38
Şekil 4.19.	Tekil saldırı modelinde farklı eşik değerleri için 100 düğümde tüketilen toplam enerji miktarının kıyaslanması.....	39
Şekil 4.20.	Tekil saldırı modelinde farklı eşik değerleri için 100 düğümde gecikmelerin kıyaslanması.....	40
Şekil 4.21.	Tekil saldırı modelinde farklı eşik değerleri için 100 düğümde yakalanan paket miktarının kıyaslanması	40
Şekil 4.22.	Tekil saldırı modelinde farklı eşik değerleri için 150 düğümde tüketilen toplam enerji miktarının kıyaslanması.....	41
Şekil 4.23.	Tekil saldırı modelinde farklı eşik değerleri için 150 düğümde gecikmelerin kıyaslanması.....	42
Şekil 4.24.	Tekil saldırı modelinde farklı eşik değerleri için 150 düğümde yakalanan paket miktarının kıyaslanması	43
Şekil 4.25.	Farklı eşik değerleri için 200 düğümde tüketilen toplam enerji miktarının kıyaslanması	44
Şekil 4.26.	Tekil saldırı modelinde farklı eşik değerleri için 200 düğümde gecikmelerin kıyaslanması.....	45
Şekil 4.27.	Tekil saldırı modelinde farklı eşik değerleri için 200 düğümde yakalanan paket miktarının kıyaslanması	45

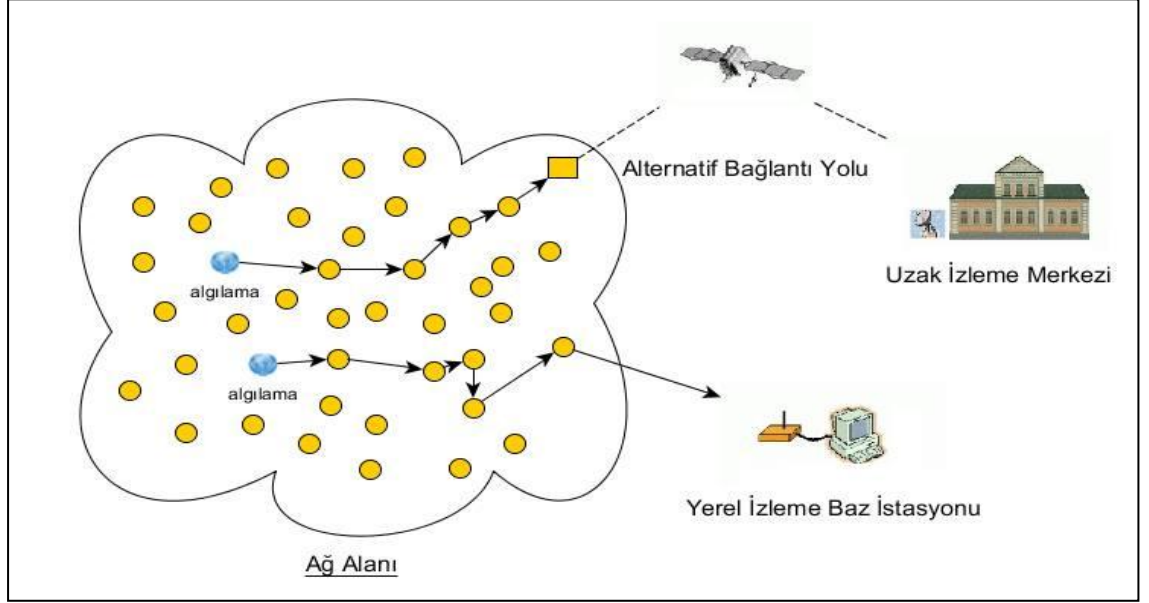
1. GİRİŞ

Mikro Elektro Mekanik Sistemler (MEMS), milimetrelerden mikrometrelere kadar olan boyutları sayesinde, büyük ölçekli sistemlere göre taşınabilirlik, düşük güç tüketimi, düşük maliyet ve yüksek performans gibi birçok avantaj sunarlar. Bu avantajlarla beraber ilerleyen mikro ve nano üretim teknolojileri sayesinde MEMS, algılama sistemleri, RF iletişim ve biyomedikal cihazlar gibi birçok alanda yaygın olarak kullanılmaktadır (Karasulu ve ark., 2009).

Gelişen MEMS teknolojisi ile birlikte, birçok uygulama için ağ yapısı oluşturmak önem kazanmıştır. Kablosuz algılayıcı ağlar (KAA) küçük, düşük maliyetli, kablosuz iletişimi kullanan yüzlerce hatta binlerce algılayıcıdan oluşan ve birçok çevreye uyarlanabilen ağlardır. KAA' lar, çevre ve doğa takibi, envanter izleme, tıbbi takip, askeri uygulamalar, sismik algılama, trafik kontrol gibi birçok alanda rahatlıkla izleme, takip ve karar destek sistemi için başarıyla kullanılmaktadır (Ceyhan ve Sağıroğlu, 2013).

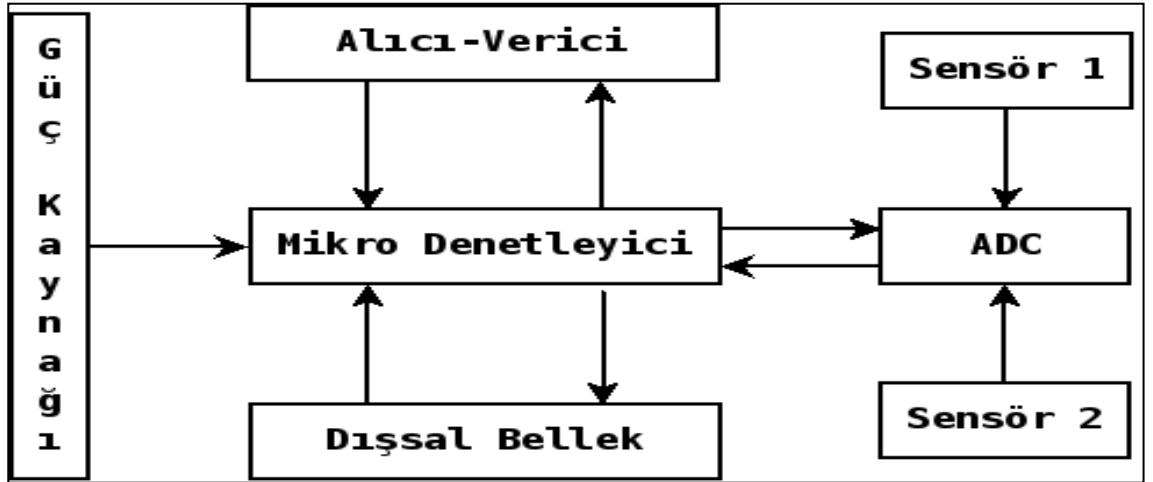
KAA' lar insan bakımına gereksinim duymayan fiziksel olarak ayrılmış pek çok düğüm içerebilir. Tek bir düğüm olarak bakıldığında etkisi küçük olarak düşünülse de yoğun olarak dağıtılmış düğümler eş zamanlı ve iş birliği içinde çalışabilirler. Ayrıca sensör düğümler yaşam tehlikesinin bulunduğu alanlara bırakılabilir ve her şartta işlem yapabilirler. Bu düğümlerin algılama görevlerini her an yürütebilmelerini, kablolu ağlarla kontrol edilemeyen yerlerde rahatlıkla kullanılmalarını sağlar (Ceyhan ve Sağıroğlu, 2013).

Bir algılayıcı ağın yapısında (Şekil 1.1.) genel olarak kendi aralarında haberleşebilen birçok algılayıcı düğüm ve bu düğümlerin haberleştikleri bir baz istasyonu bulunmaktadır. Algılayıcı düğümler yerleştirildikten sonra çevreyi gözetleme işlemine başlarlar. Bir olay meydana geldiğinde çevredeki algılayıcı düğümlerden biri bu olayı tespit eder, rapor oluşturur ve bu raporu baz istasyonuna kablosuz bağlantı aracılığıyla iletir. Baz istasyonu bu sonucu işler ve daha fazla işlem için dış dünyaya yüksek kaliteli kablolu veya kablosuz bağlantı aracılığı ile iletir. Ayrıca KAA uzmanları, hazırladıkları komut veya sorguları baz istasyonuna göndererek ağa yayılmasını sağlayabilir. Dolayısıyla baz istasyonu, KAA ve dış dünya arasında bir ağ geçidi gibi davranmaktadır (Ceyhan ve Sağıroğlu, 2013).



Şekil 1.1. Algılayıcı Ağların Genel Yapısı

Bir algılayıcı düğümün yapısında (Şekil 1.2.) mikro denetleyici, alıcı-verici, dışsal bellek, güç kaynağı ve bir veya daha fazla sensör bulunur (Kalaycı, 2009).



Şekil 1.2. Algılayıcı Ağların İçYapısı

Veri işleme görevini üstlenen mikro denetleyici, aynı zamanda sensör düğüm içerisindeki diğer bileşenlerin işlevselliğini de denetler. Alıcı-verici, radyo frekansını kullanarak ISM bandı üzerinden ağın iletişimini sağlar. Algılayıcı ağlar birbirleri ile haberleşmek ve verilerini baz istasyonuna iletmek için güç harcarlar. Bu harcadıkları gücü güç kaynağından temin ederler. Sensörler, sıcaklık, basınç gibi fiziksel durumlardaki değişimlere ölçülebilir tepkiler üretebilen donanım aygıtlarıdır. Dışsal

bellek, uygulamalar ile ilgili verileri saklamak için ve algılayıcının programlanması için kullanılır. ADC, çevreden analog olarak alınan verinin digital veriye dönüştürme işlemini yapar (Kalaycı, 2009).

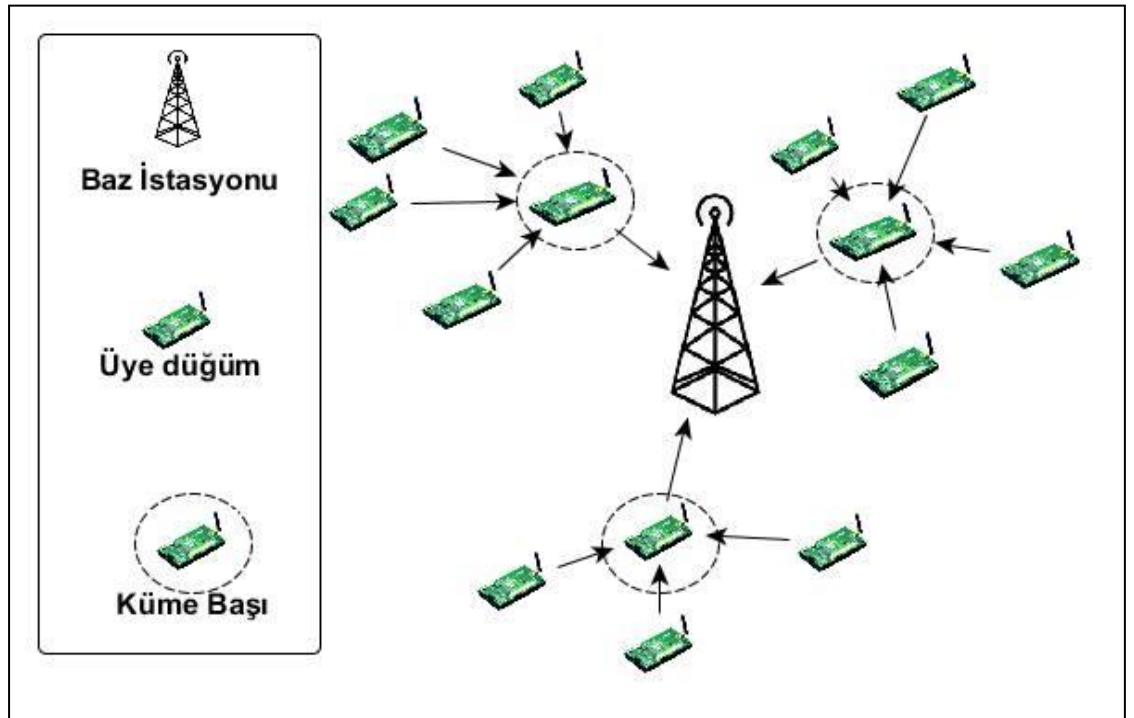
KAA' larda yönlendirmenin temel amaçlarının başında ağ ömrünün artırılması ve yoğun enerji yönetimi tekniklerinin kullanımıyla ortaya çıkan bağlantı hatalarının önlenmesi gelmektedir. KAA' ların enerji kaynakları sınırlıdır ve çoğu zaman değiştirilmesi mümkün olmamaktadır. Ayrıca, algılayıcı noktaların konumları genellikle önceden belirlenememekte ve bu düğümler zor coğrafya bölgelerine veya afet bölgelerine rastgele yerleştirilmektedir. Bu ise, algılayıcı noktaların herhangi bir düzenleme veya bakım yapılmaksızın, uzun süre algılama ve iletişim yapmak zorunda oldukları anlamına gelir. Bu nedenle, yüksek kalitede algılama ve hatasız çalışma için algılayıcı noktalar arasında önemli ölçüde dayanışma ve işbirliğinin gerçekleştirilmesi şarttır. Bir algılayıcı ağına, bu kısıtlamalardan dolayı klasik bir ağ protokolü uygulanamamaktadır. Bu nedenle KAA yapılarına özgü kriterleri dikkate alan ağ protokollerinin geliştirilmesi gerekmektedir (Ökdem ve Derviş, 2007).

Literatürde KAA' larda yönlendirme protokol çalışmaları geniş ölçüde yer almaktadır. KAA' larda yönlendirme genel olarak; düz, hiyerarşik ve adaptif olarak sınıflandırılabilir. Düz yönlendirmede, bütün düğümler eşit rollere sahipken, hiyerarşik yönlendirmede, düğümlere farklı roller verilmiştir. Adaptif yönlendirmede ise belirli sistem parametreleri ağın mevcut durumuna ve uygun enerji seviyesine göre kontrol edilmektedir. Küçük ölçekli ağlar için uygun olan düz ve adaptif yönlendirme tekniklerine kıyasla kümeleme tabanlı yönlendirme, enerji tüketiminin daha aza indirilmesi, yük dağılımının minimize edilmesi, güvenilirliğin daha fazla olması ve daha fazla ölçeklenebilirlik gibi özelliklerinden dolayı büyük ölçekli ağlar için daha uygundur (Ökdem ve Derviş, 2007).

Hiyerarşik veya cluster-based (küme-tabanlı) yönlendirme ilk olarak kablolu ağlarda önerilmiştir. Bu yönlendirme, sistem kapasitesini ayarlama ve verimli haberleşmeyi sağlama avantajlarına sahiptir. Şekilde kümeleme mimarisine göre tasarlanmış bir ağ yapısı görülmektedir (Şekil 1.3.). Kümeleme tabanlı KAA sisteminde üç ana eleman vardır. Bunlar baz istasyonu, küme başı ve üye düğümlerdir. Baz istasyonu, küme başının üye düğümlerden toplayıp yolladığı verileri değerlendirme işleminden sorumludur. Küme başı, kendisine bağlı üye düğümlerden veri toplama ve

bu verileri baz istasyonuna iletmekten sorumludur. Üye düğümler ise bağlı oldukları küme başına, bir durum algıladığı zaman veri yollamaktan sorumludur

Literatürde KAA' lar için, çok sayıda kümeleme tabanlı yönlendirme protokolü geliştirilmiştir. Bu çalışmaların çoğu kümeleme tabanlı ağ mimarilerinin temeli olarak kabul edilen LEACH (Heinzelman ve ark., 2000) protokolünü kullanmıştır. Heinzelman, algılayıcı ağları için düşük enerjili adaptif kümeleme hiyerarşisi (low energy adaptive clustering hierarchy-LEACH) isminde hiyerarşik kümeleme algoritmasını önermiştir. LEACH, her döngüde tamamen dağıtık yapıda küme oluşumu içeren kümeleme tabanlı bir protokoldür. Daha az enerji tüketimi için küme başları rastgele bir şekilde dönüşümlü olarak verilir ve enerji harcaması ağıdaki algılayıcılara paylaştırılır. LEACH, kapasite ayarlanabilirliği ve dinamik ağlardaki dayanıklılığı (robustness) sağlamak üzere yerel bir koordinasyon kullanır ve baz istasyonuna gönderilecek bilgi miktarını azaltmak üzere veri-birleştirmesini (data fusion) gerçekleştirir.



Şekil 1.3. Kümeleme Tabanlı Kablosuz Algılayıcı Ağların Genel Yapısı

KAA' ların kaynakları kısıtlıdır ve düşman alanlar gibi zorlu şartlar altında bile konumlandırılabilir. Dolayısıyla KAA' ların iletim kanalları ile algılayıcı düğümleri arasındaki düğüm iletişimi çeşitli saldırılara açıktır (Meghdadi ve ark., 2008). KAA' lar kullanılarak tasarlanan uygulamalar dışarıdan gelen saldırılara karşı güvenlik

önlemlerinin alınmasını gerektirir. Ağın güvenli ve stabil halde çalışır olması kadar, gizliliğin korunumu ilkesi de önemle ele alınmalıdır. Özellikle teröristler tarafından planlanan birçok felaket senaryosunda, yetkisiz erişimlerden ağı korumak zorunludur (Meghdadi ve ark., 2008).

Ayrıca, kimyasal, biyolojik veya diğer çevresel tehditlerin görüntülediği uygulamalarda ağın erişilebilirliğinin etkilenmemesi büyük önem taşır. Hatalı alarm oluşturan saldırılar, yanlış işlem yapılmasına ve ağ yapısının bozulmasına neden olabilir. Sağlık hizmetlerinde de gizliliğin korunması önemlidir. Sadece yetkilendirilmiş kişilerin ağa ulaşması ve görüntülemesi sağlanmalıdır (Ceyhan ve Sağiroğlu, 2013). KAA uygulamaları yaygınlaşıp karmaşıktıkça, sistemlerin yetkisiz kullanıcılara karşı korunmasının gerekliliğinin önemi daha da artacaktır. Bu nedenle KAA' larda güvenlik alanında kapsamlı çalışmalar yapılması önem arz etmektedir.

KAA' larda veri gizliliği, veri doğrulama, veri bütünlüğü, veri durumu gibi birincil güvenlik hedefleri istisnasız her uygulamada olması gereken standart güvenlik hedeflerdir (Padmavathi ve Shanmugapriya, 2009).

Veri Gizliliği, algılayıcı ağ üzerinde iletilen mesajların saldırgandan gizlenmesidir. Veri doğrulama, kaynağın kimliğinin belirlenerek mesajın güvenliğini sağlama işlemidir. Veri Bütünlüğü, verinin tahrip edilmiş yada değiştirilmiş olup olmadığını tespit etmek için kullanılır. Veri durumu ise herhangi bir düğümün kaynaklarını kullanıp kullanmadığını ve mesajların iletimi için ağın kullanılabilir olup olmadığını denetlemek için kullanılır (Padmavathi ve Shanmugapriya, 2009).

KAA ikincil güvenlik hedefleri uygulamanın kalitesini artırmak ve sistemin daha verimli çalışması için sisteme dahil edilen hedeflerdir. İkincil hedefler, verinin güncelliği, kendi kendini örgütlenme, zaman senkronizasyonu ve güvenli konumlandırma (Padmavathi ve Shanmugapriya, 2009).

KAA' larda verilerde gizlilik ve bütünlük sağlansa bile her mesajın güncelliğinden emin olunması gerekir. Veri güncelliği, mevcut verinin eski verilerin bir tekrarı olmadığından emin olunması durumudur. Kendi kendini örgütlenme, tüm algılayıcı düğümlerin kendi kendine örgütlenmesi için yeterince bağımsız ve esnek olduğunun garanti edilmesidir. Zaman senkronizasyonu, verilerin iki algılayıcı ağ arasında taşınırken belli bir senkron içinde olduğunun garanti edilmesi işlemidir. Güvenli konumlandırma ise algılayıcı ağın tam ve düzgün olarak konumlandırılmasını sağlama kabiliyetidir (Padmavathi ve Shanmugapriya, 2009).

Algılayıcı ağ saldırıları iç saldırılar (insider attacks) ve dış saldırılar (outsider attacks) olmak üzere ikiye ayrılırlar. Dış saldırılarda saldırgan, gizli anahtar bilgisine sahip olmadan kendi algılayıcı düğümleri ile hedefindeki algılayıcı ağın işlevini bozacak şekilde saldırılar düzenler (Meghdadi ve ark., 2008; Sedjelmaci ve ark., 2012; Xing ve ark., 2010). Yetkisiz saldırgan tarafından iletişim kanalının izlenmesi ve dinlenmesi dış saldırılara örnek olarak verilebilir. Dış saldırılar, anahtarlama, şifreleme, kimlik doğrulama gibi yöntemlerle tespit edilebilir (Gondwal,ve Diwaker, 2013). İç saldırılarda ise saldırgan, algılayıcı düğümleri ve gizli anahtarı ele geçirerek içten saldırır. Kötü niyetli bir düğüm tarafından ele geçirilen normal düğümler, bilgilerin dışarı aktarılmasına neden olarak tüm ağı tehlikeye sokabilir. İç saldırıların tespit edilmesi ve engellenmesi ağın güvenliği açısından oldukça önemlidir (Gondwal,ve Diwaker, 2013). İç saldırıların ağa verdiği zarar çok büyük olmakla birlikte bu saldırıların kimlik doğrulama ve yetkilendirme gibi geleneksel yöntemlerle tespiti çok zordur. Bu nedenle iç saldırıların tespit edilmesi için farklı güvenlik önlemlerinin alınması gereklidir (Sheela ve ark., 2012). İç saldırılara sinkhole saldırıları, blackhole saldırıları, sybil saldırıları, wormhole saldırıları örnek olarak verilebilir. İç saldırıların en tehlikeli olanlarından biriside sinkhole saldırılarıdır (Xing ve ark., 2010).

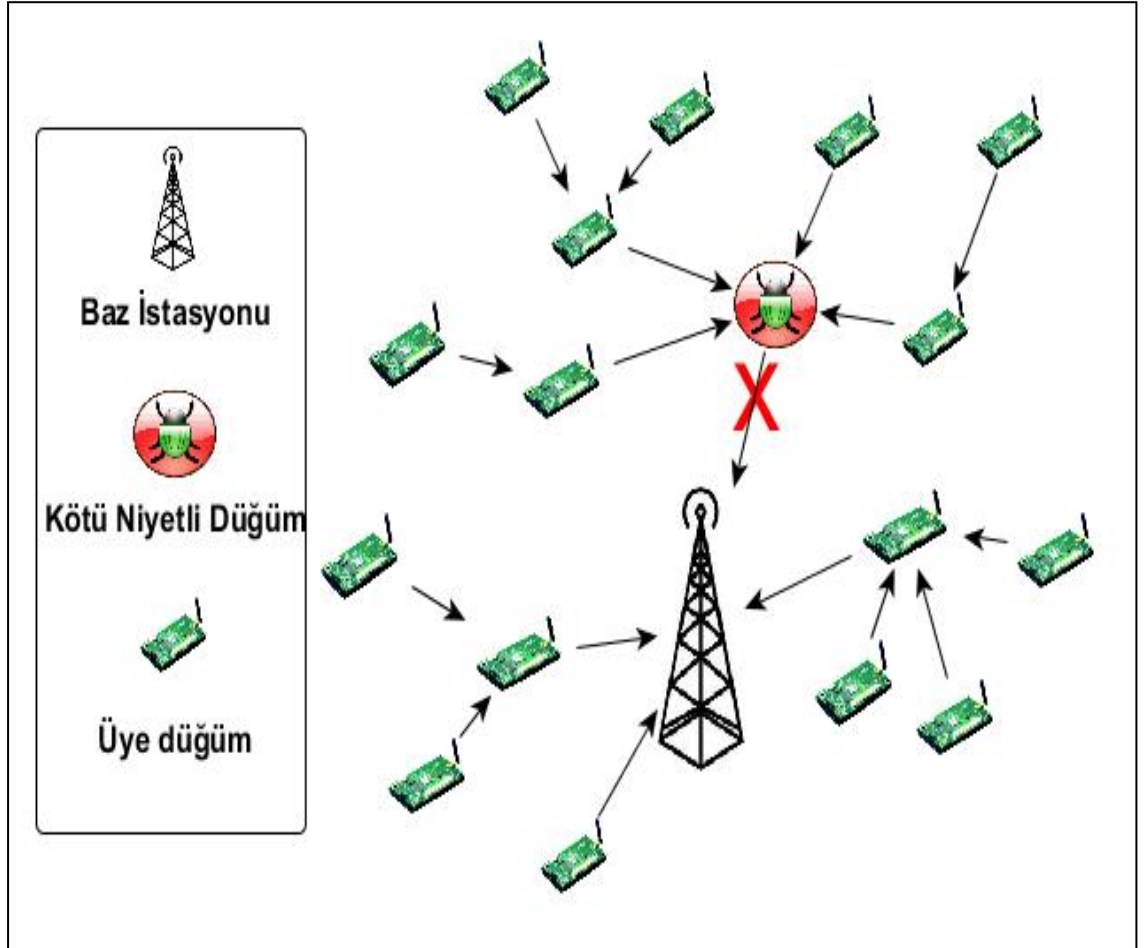
Sinkhole atağında, ağa sızmaya çalışan kötü niyetli bir düğüm, ya başka bir algılayıcı düğümü tehlikeye düşürür ya da ağın içine kötü niyetli bir düğüm sokarak onu bir saldırı başlatmak için kullanır.

Düz yönlendirme mimarisine dayalı bir ağ yapısı üzerinde modellenen Sinkhole atağında (Şekil 1.4.) tüm düğümler eşit role sahip olduklarından kötü niyetli düğüm yalnızca üye düğüm rolünde olarak sisteme zarar verebilir. Hiyerarşik yönlendirme mimarisine dayalı ağ yapısı üzerinde modellenen bir sinkhole atağında (Şekil 1.5.) ise kötü niyetli düğüm, hem küme başı hem de üye düğüm rolünde olarak sisteme zarar verebilir. Kötü niyetli bir düğüm, diğer düğümlerin yönlendirme protokolünü kullanarak elde ettikleri yönlendirme bilgilerinden oluşan tüm ağın trafik bilgisini elde etmeye çalışır. Bu amaçla sahte yönlendirme bilgileri kullanır. KAA' larda tüm düğümler verilerini tek bir baz istasyonuna yolladıkları için sinkhole ataklarına açıktır. İletişim akışına dayalı KAA' larda kötü niyetli düğüm diğer düğümleri hedef olarak görmez, sadece baz istasyonu ile yakın olmayı hedefler.

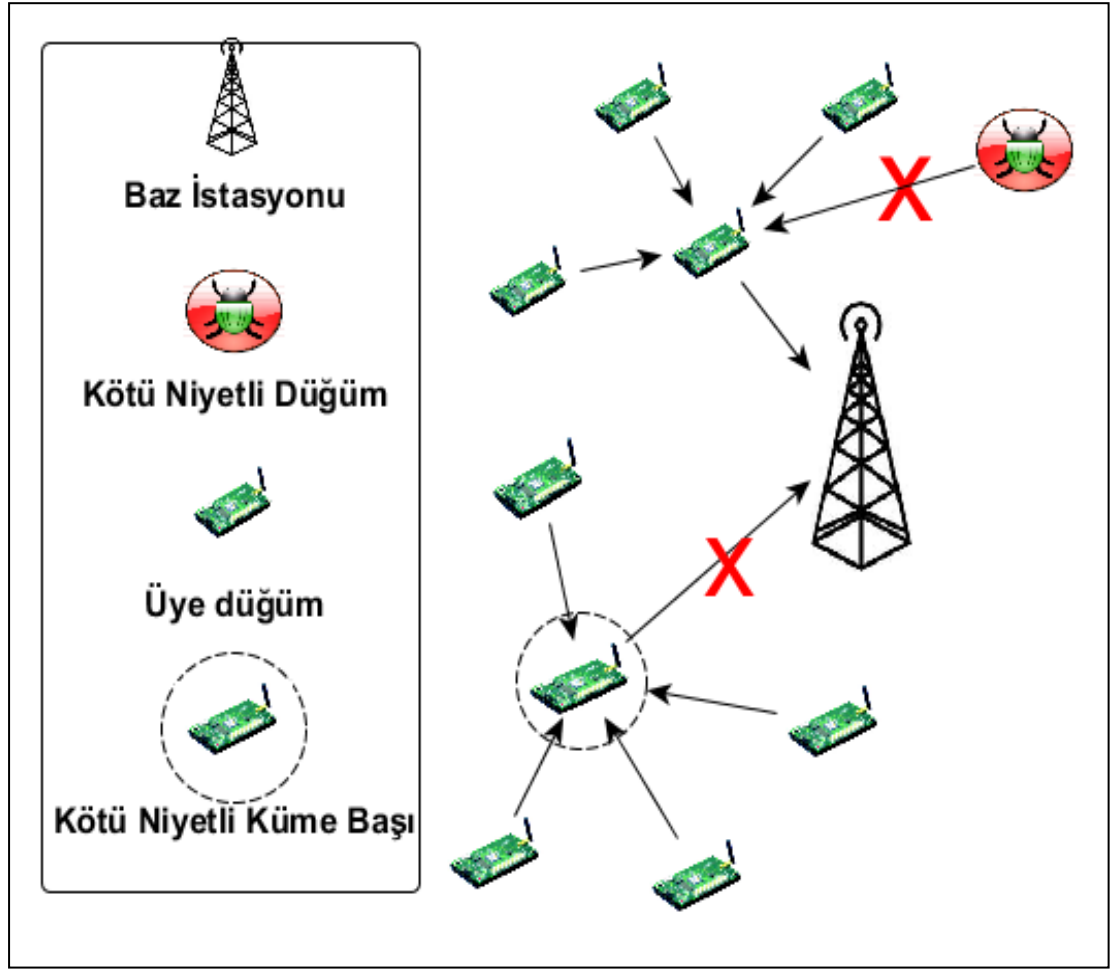
Sinkhole saldırıları için iki tip senaryo vardır. İlkinde kötü niyetli düğüm diğer düğümlerden daha fazla enerjiye sahiptir. İkinci senaryoda ise kötü niyetli düğüm ile

diğer düğümler aynı enerjiye sahiptir. İki senaryoda da kötü niyetli düğüm baz istasyonuna giden en kısa yolun kendinde olduğunu iddia ederek ağ trafiğini elde etmeye çalışır. KAA' larda baz istasyonuna giden en kısa yol yönlendirme bilgilerinden, temel hesaplama ile elde edilir (Chaudhry ve ark., 2013).

Kötü niyetli düğüm, ağ trafik bilgilerini ele geçirdikten sonra, ağın işlevini bozmak için üç çeşit saldırı ile paket iletimine zarar verebilir. Bunlar, paketi iletmeme, paketi kopyalama ve sürekli paket yollamadır. Paket iletmeme, kötü niyetli düğümün aldığı paketleri baz istasyonuna iletmeme durumudur. Paket kopyalama, kötü niyetli düğümün daha önceden iletilen paketleri tekrar baz istasyonuna iletmeme durumudur. Sürekli paket yollama ise kötü niyetli düğümün sürekli toplu paket yollayarak trafik yaratma durumudur (Heinzelman ve ark., 2000).



Şekil 1.4. Düz Yönlendirme Tabanlı Sistemde Sinkhole Atağı



Şekil 1.5. Hiyerarşik Yönlendirme Tabanlı Sistemde Sinkhole Atağı

Bu çalışmada hiyerarşik KAA' larda sinkhole saldırılarının kural tabanlı tespiti için algoritmalar önerilmiştir. Çalışmada öncelikle kümeleme mimarisine sahip KAA' larda sinkhole saldırılarının farklı şekillerde modellenmesi yapılmıştır. Modeller incelendikten ve çeşitli parametreler üzerinden ayrıntılı şekilde test edildikten sonra tespiti için yeni algoritmalar önerilmiştir. Bu çalışmanın hedefi, sistemi saldırılardan mümkün olan en optimum sürede, minimum zarar ile kurtarmaktır. Bu nedenle sinkhole saldırılarının uygun bir şekilde modellenmesi, saldırı tespitinin kısa bir süre içinde yapılması ve iyileştirmenin enerji efektif algoritmalarla uygulanması çalışmanın birincil amacıdır. Tespit çalışması yapılırken, enerji tabanlı saldırı tespit mekanizması kullanılmıştır. Bu amaçla tespit işlemleri baz istasyonu tarafından yapılmıştır. Bunun nedeni baz istasyonunun tamamen güvenilir bir kaynak olduğunun ve enerji kısıtlamasının bulunmadığının kabulüdür.

2. ÖNCEKİ ÇALIŞMALAR

Ngai ve arkadaşlarının yaptıkları düz yönlendirme tabanlı çalışmada (Ngai ve ark., 2007) sinkhole saldırıları baz istasyonu üzerinden tespit edilmeye çalışılmıştır. Baz istasyonu içerisinde etkilenen düğümlerin kimliklerini içeren bir istek mesajı yollar. Etkilenen düğümler baz istasyonundan gelen mesajı aldıktan sonra, baz istasyonuna yanıt mesajı yollar. Bu mesajın içerisinde düğümün kimlik bilgisi, bağlı olduğu bir sonraki düğümün kimlik bilgisi ve bunlara ilişkin maliyet bilgileri yer alır. Alınan bu bilgiler baz istasyonu tarafından sinkhole saldırılarını tespit etmek için kullanılır.

Papadimitriou ve arkadaşları yaptıkları şifreleme tabanlı çalışmada (Papadimitriou ve ark., 2009) RESIST-0 ve RESIST-1 adında iki güvenlik algoritması önermişlerdir. Bu protokollerde, tüm kimlik doğrulama ve veri mesajlarının belirlenmesi işlemi ağ kurulmadan önce, önceden hazırlanmış özel ve gizli anahtarların kullanılması ile yapılır. Bu anahtarlar kullanılarak sinkhole saldırıları tespit edilmeye çalışılır.

Chen ve arkadaşlarının yaptıkları hiyerarşik yönlendirme tabanlı çalışmada (Chen ve ark., 2010) sinkhole saldırılarını tespit etmek için GRSh (Girshick-Rubin-Shyriaev) algoritmasını önermişlerdir. Bu çalışmada sinkhole saldırılarını tespit etmek için baz istasyonu kullanılmıştır. Toplam düğüm sayısının %5' i kadar kötü niyetli düğüm sisteme yerleştirilmiştir. Her düğüm kendi CPU kullanım miktarını tutar ve baz istasyonuna periyodik olarak rapor eder. Düğümlerin CPU kullanım oranlarının genellikle %80' in altında olduğu belirlenmiştir. Düğümlerin CPU kullanım oranları bu değerin üzerinde olursa sistemde atak olduğu baz istasyonu tarafında belirlenir.

Sharmila ve arkadaşlarının yaptıkları şifreleme tabanlı çalışmada (Sharmila ve Umamaheswari, 2011) sinkhole düğüm bir kimlik doğrulama anahtarı kullanılarak tespit edilir. Bir düğüm yeni yol bilgisini yaydığı zaman, bu bilgiyi alan düğüm, mesajın bir özetini oluşturup hem orijinal yola hem de şüpheli düğümün bulunduğu yola iletir. Eğer yeni düğüm mesajı onaylamazsa kötü niyetli düğüm olarak düğüm olarak etiketlenir.

Singh ve arkadaşlarının yaptıkları hiyerarşik yönlendirme tabanlı çalışmada (Singh ve ark., 2011) mac adres tabanlı kötü niyetli düğüm algılaması yapılması amaçlanmıştır. Sistem oluştuktan sonra, her düğüm mac adresini baz istasyonuna gönderir. Böylece baz istasyonu ağdaki tüm düğümlerin mac adres bilgisine sahip olur. Daha sonra, baz istasyonu kendisine paket yollayan düğümlerin mac adreslerini kontrol

ederek kötü niyetli düğümleri tespit etmeye çalışır. Kötü niyetli düğümleri tespit etme işlevi baz istasyonuna verilerek enerji verimliliği sağlanması amaçlanmıştır.

Bahekmat ve arkadaşlarının yaptıkları şifreleme tabanlı çalışmada (Bahekmat ve ark., 2012) bir sensör düğüm baz istasyonuna veri göndermek istediğinde, ilk olarak baz istasyonuna doğrudan bir kontrol paketi yollar. Baz istasyonundan yanıt paketi aldıktan sonra ise çok sekmeli yönlendirme(multihop routing) aracılığı ile baz istasyonuna veri paketini yollar. Veri paketi baz istasyonuna ulaştığında veri paketindeki kontrol alanları orijinal kontrol paketi ile kıyaslanır. Bu kontrol paketinde herhangi bir değişiklik algılanırsa, sistemde şüpheli düğümlerin olduğu anlaşılır. Kötü niyetli düğümleri tespit etmek amacıyla veri iletimi, yönlendirme yolları ve yollar üzerinde bulunan düğümler kontrol edilir. Paketlerde herhangi bir hata algılanırsa, baz istasyonu bellekte saklanan mevcut düğümle yeni yoldaki diğer düğümleri karşılaştırır ve ardından benzer düğümleri saklarken kalan düğümler siler.

Patil.ve arkadaşlarının yaptıkları hiyerarşik yönlendirme tabanlı çalışmada (Patil ve ark., 2012) baz istasyonu port no, mac adresi, ip adresi gibi parametrelere bakarak kötü niyetli düğümü tespit etmeye çalışır. Tüm düğümler paketlerini küme başı aracılığı ile baz istasyonuna iletir, eğer üye düğümlerde bir değişiklik olursa bu durum baz istasyonu tarafından izlenir. Baz istasyonu kötü niyetli bir düğüm tespit ederse bunu diğer üye düğümlere bildirir.

Hichem Sedjelmaci ve arkadaşlarının yaptığı hiyerarşik yönlendirme tabanlı çalışmada (Sedjelmaci ve ark., 2012) anormallik tespiti SVM(Support Vektor Machine) kullanılarak yapılır. SWM eğitimi için dağıtılmış öğrenme algoritmalarını kullanır. Bu sayede normal ve anormal faaliyetler arasında ayırım sağlanmaya çalışılır.

Razzaque ve arkadaşlarının yaptıkları düz yönlendirme tabanlı çalışmada (Razzaque ve ark., 2013) AODV protokolü üzerinden sinkhole ataklarını tespit etmeye çalışılmıştır. Önerilen algoritmada ilk olarak şüpheli düğümlerin listesi oluşturulur. Şüpheli düğümler baz istasyonu tarafından, mesajların tutarlı olup olmamasına bakarak belirlenir. Bu şüpheli düğümler arasındaki sinkhole düğümler ise ağdaki veri akışı kontrol edilerek sağlanmaya çalışılır.

Rajkumar ve arkadaşlarının yaptıkları hiyerarşik yönlendirme tabanlı çalışmada (Rajkumar ve Vayanaperumal, 2013) sinkhole ataklardan kaçınmak ve sinkhole atakları tespit etmek için lider bazlı saldırı tespit sistemi(LBIDS) önerilmiştir. Bu yaklaşımda ağdaki tüm düğüm grupları içinden bir lider seçilerek akıllı bir bölge yaratılır. Bu bölge

içinde düğümlerin olması gereken davranışları hesaplanarak, bu davranışların dışında hareket eden düğümler tespit edilir. Ağdaki herhangi bir düğüm başka bir düğümü kötü niyetli olarak algıladığı zaman, KAA içindeki liderleri bu durumla ilgili bilgilendirir. Böylece ağ içindeki tüm liderler kötü niyetli düğüm bilgisini alırlar ve o düğümle olan iletişimlerini keserler.

Sahraoui arkadaşlarının yaptıkları hiyerarşik yönlendirme tabanlı çalışmada (Sahraoui ve Bouam, 2013) her küme içerisinde bir adet izleyici düğüm bulunur. Üye düğümler ve küme başları karşılıklı olarak birbirlerini izlerler. Her üye düğümün kendine ait bir kötü niyetli listesi bulunur. Küme başları üye düğümlerden aldıkları verileri izlemci düğüme iletirler. İzlemci düğüm küme başından gelen mesajda bir farklılık görürse bu düğümü saldırgan olarak kabul eder. İzlemci düğüm kötü niyetli düğümün kimlik bilgisini baz istasyonuna ve komşularına iletir. Uyarı mesajını alan düğümler kötü niyetli listelerine o düğümün kimlik bilgisini eklerler. Baz istasyonu kendisine gelen paketleri kontrol ederek kötü niyetli düğüm listesini günceller. Kötü niyetli olarak belirlenen düğümler bir daha küme başı olamazlar ve sistemden izole edilirler.

Guangjie Han ve arkadaşlarının yaptığı düz yönlendirme tabanlı çalışmada (Han ve ark., 2014) sinkhole saldırılarına karşı, komşu bilgilerine dayanan saldırı tespit algoritması(IDASA) sunulmuştur. IDASA sensör düğümlerin komşuluk bilgilerinden yararlanarak sinkhole saldırılarını tespit eder. Bu çalışma kötü niyetli düğümlerin doğru tespiti ,paket kayıp oranı ve enerji tüketimi açısından değerlendirilmiştir.

Radhikabaskar ve arkadaşlarının yaptıkları çalışmada (Radhikabaskar ve ark., 2014) şüpheli düğüm tespiti baz istasyonuna yollanan paket sayısına göre yapılır. Şüpheli düğüm tespiti yapıldıktan sonra trafik akışına göre kötü niyetli düğüm tespiti yapılmaktadır. Bu çalışmada hiyerarşik KAA' larda sinkhole saldırılarının anormallik tabanlı tespiti için algoritmalar önerilmiştir. Çalışmada öncelikle kümeleme mimarisine sahip KAA' larda sinkhole saldırılarının farklı şekillerde modellenmesi yapılmıştır. Modeller incelendikten ve çeşitli parametreler üzerinden ayrıntılı şekilde test edildikten sonra tespiti için yeni algoritmalar önerilmiştir. Bu çalışmanın hedefi, sistemi saldırılardan mümkün olan en optimum sürede, minimum zarar ile kurtarmaktır. Bu nedenle sinkhole saldırılarının uygun bir şekilde modellenmesi, saldırı tespitinin kısa bir süre içinde yapılması ve iyileştirmenin enerji efektif algoritmalarla uygulanması çalışmanın birincil amacıdır. Tespit çalışması yapılırken, enerji tabanlı saldırı tespit

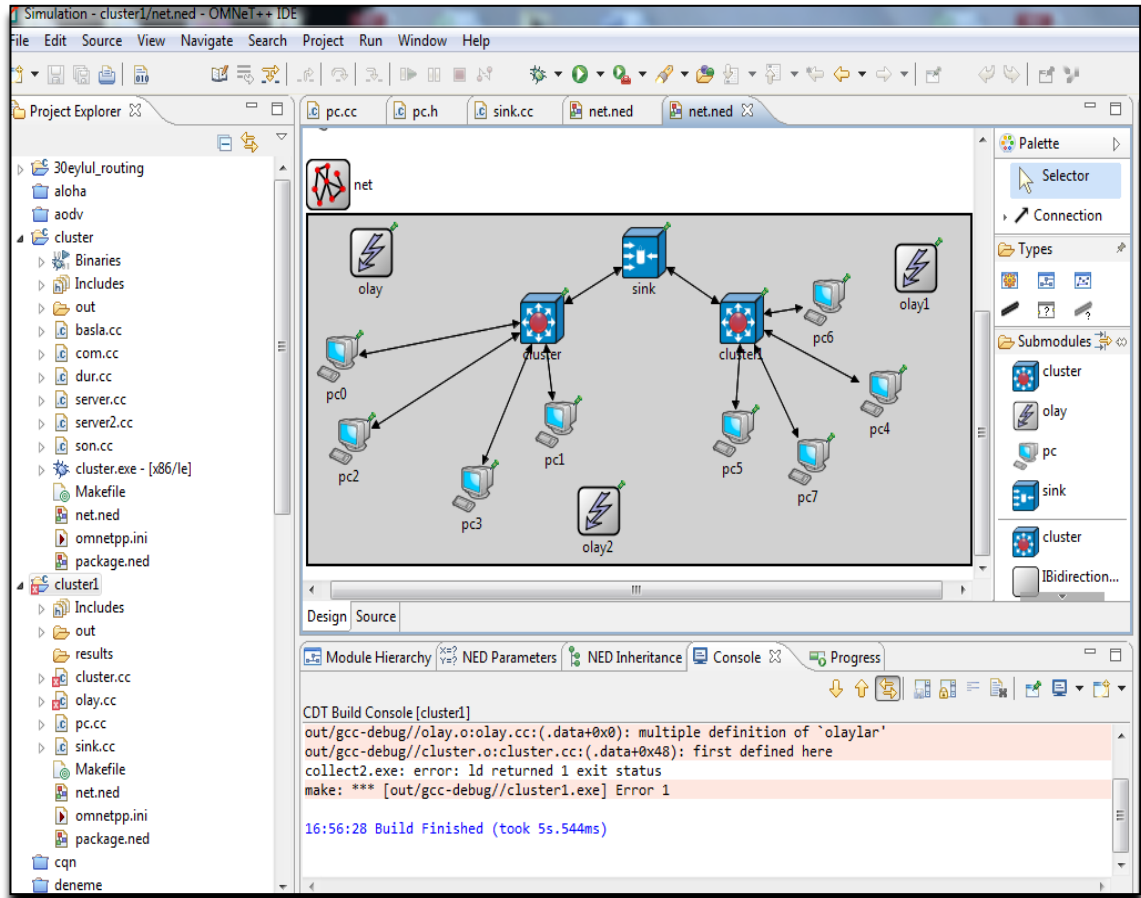
mekanizması kullanılmıştır. Bu amaçla tespit işlemleri baz istasyonu tarafından yapılmıştır. Bunun nedeni baz istasyonunun tamamen güvenilir bir kaynak olduğunun ve enerji kısıtlamasının bulunmadığının kabulüdür.

3. MATERİYAL VE YÖNTEM

Bu çalışmada KAA' larda kümeleme tabanlı yönlendirme çatısı üzerinde sinkhole saldırıları simülasyon yöntemi kullanılarak modellenmiş ve modellenen saldırıları tespit edecek algoritmalar önerilmiştir.

3.1. Materyal

Bu çalışma, OMNeT++ simülasyon programı üzerinde gerçekleştirilmiştir. OMNeT++ (Şekil 3.1.) nesneye yönelik ve modüler yapıda ayrık olay ağ benzetim programıdır. Birçok çalışmanın modellenmesi için kullanılabilir haberleşme ağlarını içermektedir. Buna ek olarak kullanıcının kendi modüllerini gerçekleyebilmesi için temel modüller sağlar. Bu yapı sayesinde bir programcı, hareketlik iskeletine yönelik kendi iletişim kurallarını, gerekli arabirim ve malzemelerin birlikte çalışılabilirliği ile uğraşmaksızın, kolaylıkla geliştirebilir (Anonim, 2015).



Şekil 3.1. OMNeT++ simülasyon programı

3.2. Yöntem

Bu çalışmada ilk olarak kümeleme tabanlı bir KAA sistemi tasarlanmıştır. Ardından sisteme sinkhole saldırıları üç farklı şekilde eklenmiş ve her bir döngüde baza ulaşan paket sayısı, sistemde tüketilen ortalama enerji miktarı ve yaşayan düğüm sayısı parametreleri izlenmiştir. Sistemin aldığı zarar belirlendikten sonra saldırının tespiti ve tespit edilen bu saldırıdan kurtulmak amacıyla sisteme verilecek uyarı için çeşitli algoritmalar oluşturulmuştur. Sistem kurtarıldıktan sonra yine çeşitli parametreler üzerinden performans değerlendirmesi yapılmıştır.

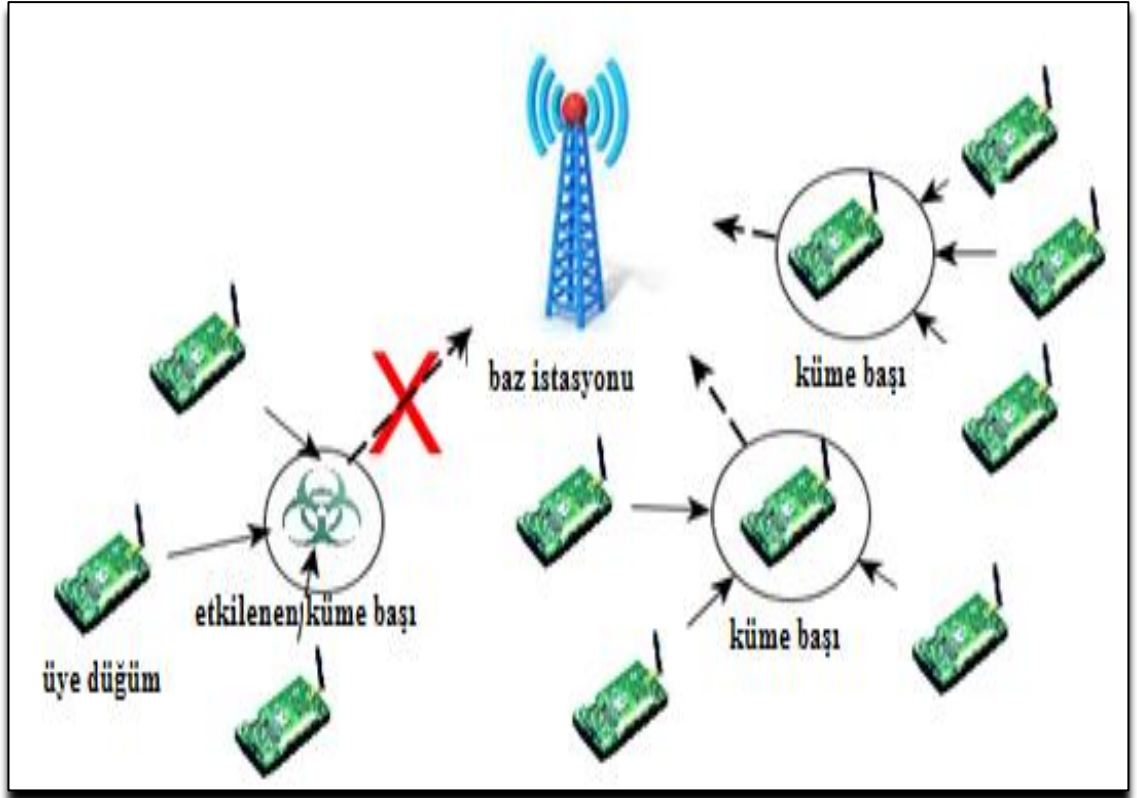
Sinkhole atağında ağa sızmaya çalışan kötü niyetli bir düğüm, ya başka bir algılayıcı düğümü tehlikeye düşürür ya da ağın içine kötü niyetli bir düğüm sokarak onu bir saldırı başlatmak için kullanır (Xing, Srinivasan, Jose ve Cheng, 2010). Bu tanıma bağlı olarak sinkhole saldırıları farklı şekillerde modellenenabilir. Sinkhole saldırılarının nasıl modellendiği sistemin performansı açısından oldukça önemlidir. Bu çalışmada sinkhole saldırıları üç farklı şekilde modellenmiş ve modellenen saldırıların ağa verdiği zararlar değerlendirildikten sonra tespit çalışmaları yapılmıştır.

3.2.1. Model 1

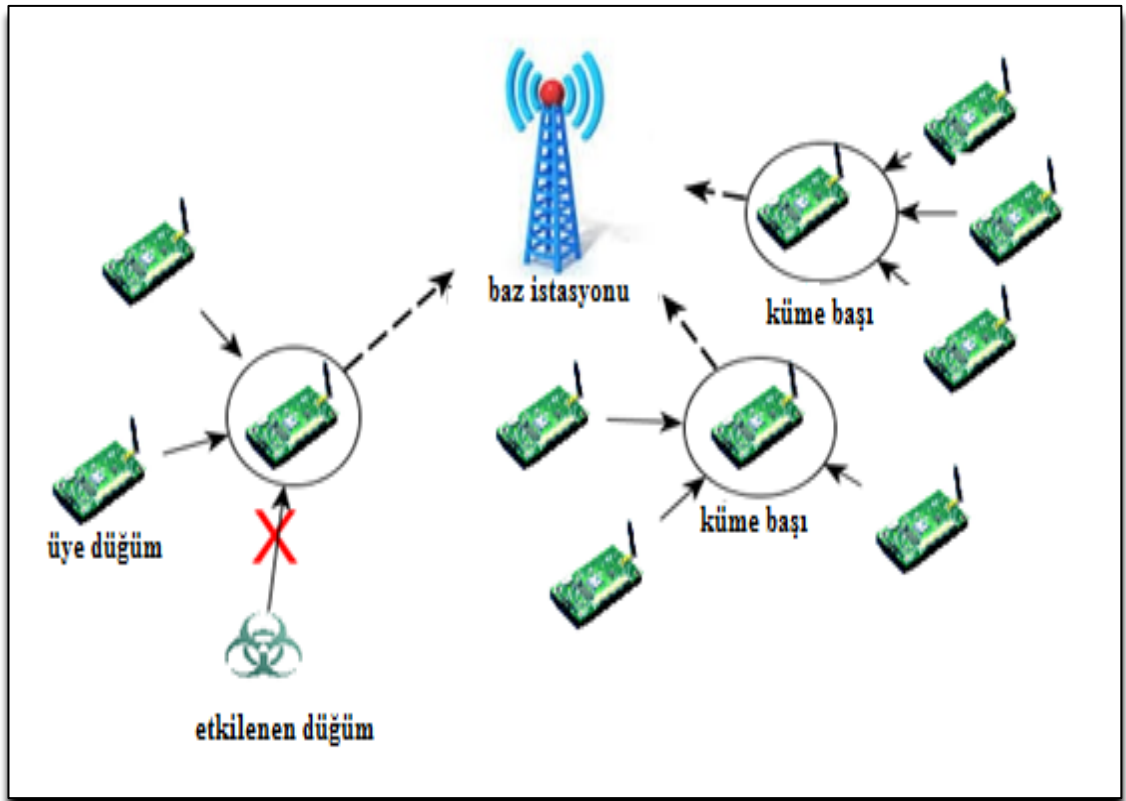
İlk modelde ağdaki toplam düğüm sayısının %10 u kadar kötü niyetli düğüm ağa yerleştirilmiş ve bu kötü niyetli düğümlerin verilerini iletmeyerek ağa verdikleri zarar incelenmiştir. Eğer kötü niyetli düğüm ağda küme başı rolünde olursa (Şekil 3.2.) üye düğümlerden topladığı verileri baz istasyonuna iletmeyerek; üye düğüm rolünde olursa (Şekil 3.3.) verilerini küme başına iletmeyerek ağa zarar vermektedir.

3.2.2. Model 2

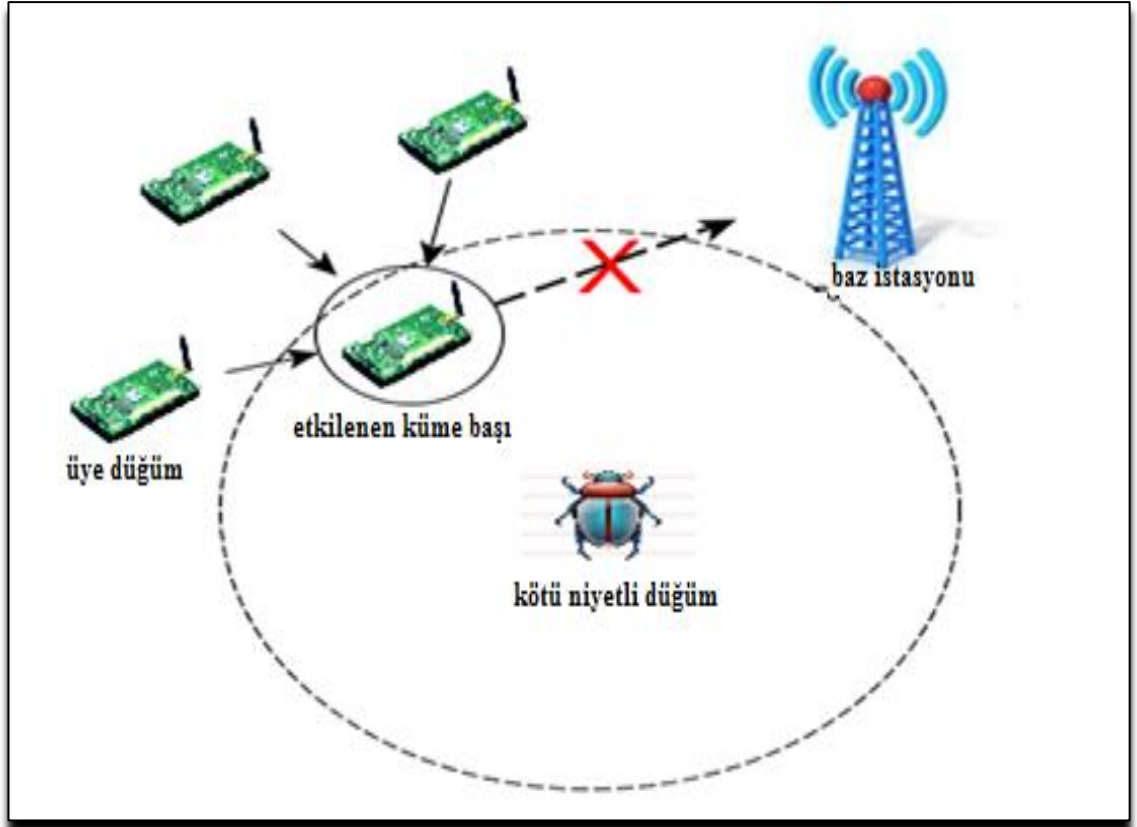
İkinci modelde kötü niyetli düğüm belirli bir kapsama alanı içinde yer alan düğümleri etkilemeye çalışmıştır. Eğer etki alanı içerisinde bir küme başı bulunursa (Şekil 3.4.), kötü niyetli düğüm küme başını etkileyerek verilerini baz istasyonuna iletmesini engeller. Eğer etki alanı içerisinde bir üye düğüm bulunursa (Şekil 3.5.), kötü niyetli düğüm, üye düğümü etkileyerek verisini küme başına iletmesini engeller.



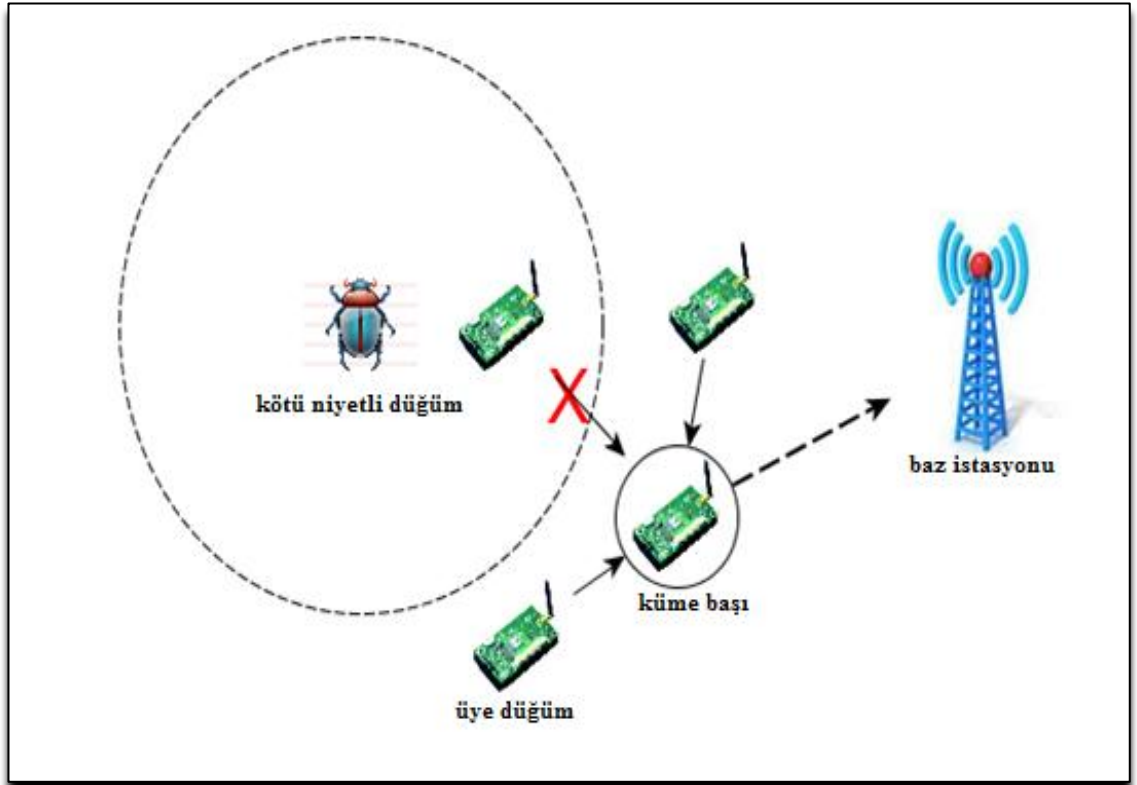
Şekil 3.2. Model 1 kötü niyetli düğüm küme başı olma durumu



Şekil 3.3. Model 1 kötü niyetli düğüm üye düğüm olma durumu



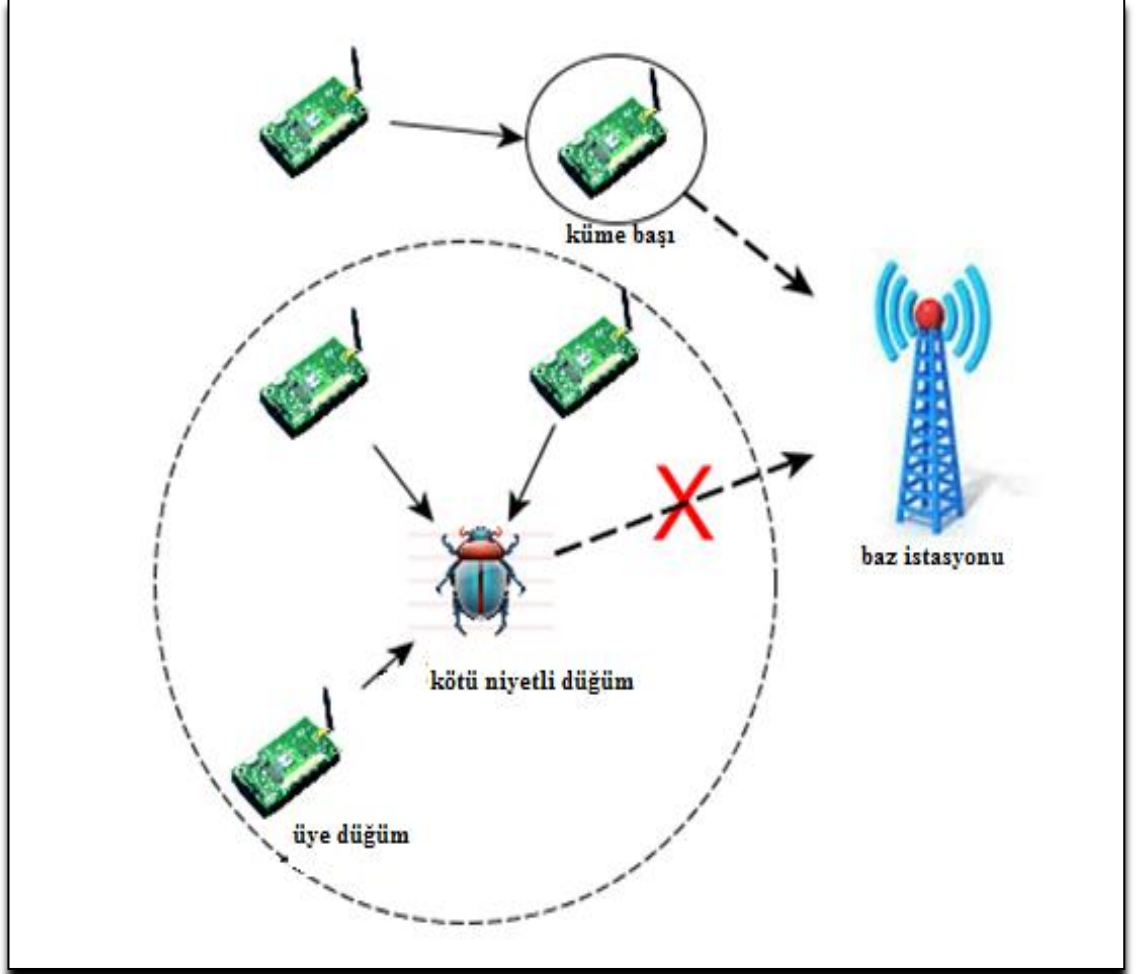
Şekil 3.4. Model 2 kötü niyetli düğümün etki alanı içinde küme başı olma durumu



Şekil 3.5. Model 2 kötü niyetli düğümün etki alanı içinde üye düğüm olma durumu

3.2.3. Model 3

Üçüncü modelde ise ağda rastgele bir düğümün kötü niyetli olarak etiketlendiği varsayılmıştır. Şekil 3.6.'da görüldüğü gibi seçilen kötü niyetli düğüm yanlış ağ trafik mesajı yollayarak küme başıymış gibi davranır ve ağdaki üye düğümleri kendi üzerine çekmeye çalışır. Ardından, üye düğümlerden aldığı verileri baz istasyonuna iletmeyerek ağa zarar verir.



Şekil 3.6. Model 3 kötü niyetli düğümün diğer düğümleri etki alanına alma durumu

Kötü niyetli düğümün ağa verdiği zarar, baz istasyonuna ulaşan paket sayısı, sistemde tüketilen ortalama enerji miktarı ve ağda yaşayan düğüm sayısı parametreleri üzerinden ölçülmüştür. Modeller test edilirken düğüm sayılarının farklı değer aralıkları hesaba katılmıştır. Ayrıca eşit şartlarda değerlendirme yapmak amacıyla modeller 185 döngü boyunca çalıştırılmıştır.

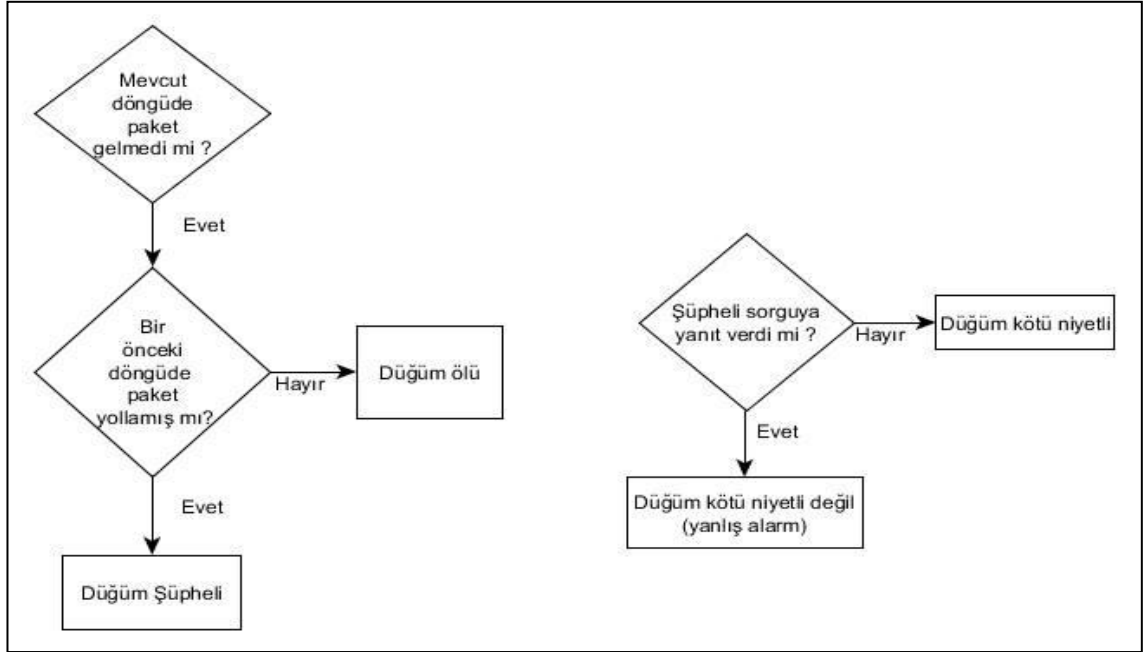
3.3. Sinkhole Saldırılarının Tespit Edilmesi

Sinkhole saldırılarının tespiti için literatürde çeşitli yöntemler kullanılmıştır. Bu çalışmalarda saldırı tespiti için düğümlerin CPU kullanımlarının (Chen), MAC adreslerinin (Shio Kumar Sing) port numaralarının ve ip adreslerinin (Shilpa S.) takibi gibi yöntemler kullanılmıştır.

Tasarlanan kural tabanlı tespit mekanizması temelde iki aşamadan oluşur. Birinci aşama şüpheli listesinin oluşturulması, ikinci aşama ise bu listedeki düğümlerin saldırgan olup olmadığının belirlenmesidir. İlk aşamada baz istasyonu bir önceki döngüde kendisine gelen paketler ile mevcut döngüde kendisine gelen paketleri karşılaştırarak paket göndermeyen düğümleri şüpheli (kötü niyetli olma ihtimali olan) düğümler listesine ekler. İkinci aşamada şüpheli düğümlerin bir önceki döngüdeki enerjisini kontrol eder. Bu enerji değeri belirli bir eşik seviyesinin altında ise, baz istasyonu bu düğümü ölü olarak kabul eder ve herhangi bir işlem yapmaz. Eğer bu enerji değeri belirli bir eşik seviyesinin üzerinde ise baz istasyonu şüpheli düğüme sorgu mesajı yollar ve düğümden bu sorguya karşılık bir yanıt mesajının gelmesini bekler. Eğer düğüm bu sorguya yanıt vermez ise baz istasyonu bu düğümü kötü niyetli olarak etiketler.

Eşik değerinin seçimi sistem performansı açısından oldukça önemlidir. Eğer eşik değeri çok küçük bir değer seçilirse baz istasyonu daha fazla sayıda şüpheliye sorgu mesajı yollar ve buna bağlı olarak sistemde ekstra enerji harcanır. Eğer eşik değeri çok büyük bir değer seçilir ise daha az sayıda şüpheliye sorgu mesajı yollanacağı için, kötü niyetli düğümleri tespit etmek zorlaşır. Bu nedenle eşik değeri için optimum değer seçilmesi oldukça önemlidir. Eğer baz istasyonu herhangi bir döngüde sistemde kötü niyetli bir düğüm olduğunu algılasa, ağdaki diğer düğümlere bu kötü niyetli düğüm yada düğümlerin kimlik bilgilerini içeren bir ALARM mesajı yollar. Ağdaki düğümler aldıkları ALARM mesajının içerisindeki kimlik bilgilerine bakarak, kötü niyetli düğümleri algılar ve bu düğümlerle bağlantılarını koparırlar. Eğer baz istasyonu herhangi bir döngüde sistemde kötü niyetli bir düğüm algılamazsa, ağdaki düğümlere DEVAM mesajı yollar ve düğümlerin sorunsuz bir şekilde bir sonraki döngüye başlamasını sağlar. Ağdaki düğümler döngü sonlarında baz istasyonundan gelen mesaj tipine göre bir sonraki adımda ne yapacaklarına karar verirler. Bu kural tabanlı saldırı tespit mekanizmasının başarılı bir şekilde çalışması için sistemde bazı varsayımlar yapılması gerekmektedir. Bunlardan ilki, ilk döngüde sistemde kötü niyetli bir düğümün

olmadığının kabulüdür. Diğeri ise baz istasyonunun tamamen güvenilir ve enerji kısıtlaması olmayan bir kaynak olduğunun kabulüdür.



Şekil 3.7. Tespit mekanizması akış diyagramı

3.4. Simülasyon Parametreleri

3.4.1. Sistemde Üretilen Mesajlar

Sistemde üretilen mesajlar iki çeşittir. İlki kümeleme tabanlı yönlendirme protokolü içinde var olan mesajlardır. İkincisi ise sistemdeki kötü niyetli düğümleri tespit etmek için kullanılan mesajlardır.

Çizelge 3.1. Sistemde Kullanılan Yönlendirme Protokolü Mesajları

Mesaj Adı	Mesaj Adı	Mesaj İşlevi	Mesaj Boyutu
REKLAM	Reklam Mesajı	Küme Başlarından üye düğümlere gider. Küme oluşumunu başlatmak için kullanılır.	X
R_YANIT	Reklama Yanıt Mesajı	Üye düğümlerden küme başlarına gider. Üye düğümlerin hangi küme başlarına bağlandığını belirlemek için kullanılır	X
VERİ_UYE	Veri Mesajı	Üye Düğümlerin algıladıkları olayları küme başlarına iletmek için kullanılır.	4X
VERİ_KB	Veri Mesajı	Küme başlarından baz istasyonuna gider ve üye düğümlerden topladıkları verileri iletmek için kullanılır.	4X

Çizelge 3.1.'de sistemde kullanılan, kümeleme protokolü içinde var olan mesajlar, bu mesajların işlevleri ve boyutları görülmektedir. REKLAM mesajı, küme başlarının kendine en yakın düğümleri bulup kümelerini oluşturmak için yolladıkları mesajdır. R_YANIT mesajı sayesinde küme başları, hangi üye düğümün kendi kümesinin içinde olduğunu belirler. Kümeler oluşuktan sonra, üye düğümler verilerini baz istasyonuna iletmek üzere VERİ_UYE mesajı içerisinde küme başlarına yollarlar. Küme başları da bu mesajları baz istasyonuna VERİ_KB mesajı ile iletirler.

Çizelge 3.2. Sistemde Kötü Niyetli Düğümleri Tespit Etmek İçin Kullanılan Mesajlar

Mesaj Adı	Mesaj Adı	Mesaj İşlevi	Mesaj Boyutu
SORGU	Sorgu Mesajı	Şüpheli düğümlerin, kötü niyetli olup olmadıklarını tespit etmek için kullanılır.	X
S_YANIT	Sorguya Yanıt Mesajı	Üye düğümler tarafından baz istasyonuna SORGU mesajına cevap olarak kullanılır.	X
ALARM/D EVAM	Alarm/Devam Mesajı	Sistemin nasıl devam edeceğine karar vermesi için baz İstasyonundan Üye düğümlere Gider	X

Çizelge 3.3. Sistemde Kullanılan Paket İçeriği

Paket İçeriği
HEDEF ID
KAYNAK ID
MESAJ İÇERİĞİ
KALAN ENERJİ MİKTARI
X KOORDİNATI
Y KOORDİNATI

Çizelge 3.2.'de kötü niyetli düğümü tespit etmek için sistemde üretilen yeni mesajlar görülmektedir. Baz istasyonu şüpheli bir düğüm algıarsa, bu düğüme SORGU mesajı yollar ve yanıt gelmesini bekler. Üye düğüm kötü niyetli değil ise, baz istasyonuna S_YANIT mesajı yollar. Baz istasyonuna mesaj yolladığı üye düğümden sorguya yanıt mesajı gelmez ise, bu düğümlerin kimlik bilgilerini ağa ALARM mesajı ile bildirir. Eğer baz istasyonu sistemde herhangi bir kötü niyetli düğüm algılamaz ise, ağa DEVAM mesajı yollar. Ağdaki düğümler baz istasyonundan gelen mesaj tipine göre bir sonraki adımda ne yapacağına karar verirler.

3.4.2. Simülasyon Parametreleri

Çizelge 3.3.'de simülasyon parametreleri görülmektedir. Çizelgede görüldüğü üzere baz istasyonunun konumu, 1000m x 1000m ' lik network alanının merkezidir. Modelleme yaparken 50, 100, 150 ve 200 adet düğüm ağı rastgele olarak dağıtılmıştır. Sistemin test aşamasında da aynı düğüm sayıları kullanılmıştır. Sistemdeki kötü niyetli düğüm oranı %10' dur. Sistemdeki düğümlerin başlangıç enerjileri 4j olmakla beraber, kötü niyetli düğümlerin başlangıç enerjileri 8j' dür. Kullanılan enerji modeli LEACH protokolü ile aynıdır. Sinkhole saldırıları için gerçekleştirilen Model 1 üzerinden, tekil saldırı ve sürekli saldırı olmak üzere iki farklı saldırı tasarlanmış ve bu tasarımlar için ayrı ayrı kural tabanlı tespit çalışmaları yapılmıştır. Tekil saldırı tasarımında kötü niyetli düğümler ikinci döngüde sisteme dahil edilmiş ve bu düğümlerin tespiti yapıldıktan sonra tekrar sisteme eklenmemiştir. Sürekli saldırı tasarımında ise kötü niyetli düğümler 10 döngüde bir sisteme dahil edilmiştir. Buda, kötü niyetli düğümlerin yakalansalar dahi 10 döngüde bir tekrar sistemde görülmeleri anlamına gelmektedir. Kural tabanlı tespit çalışması farklı kalan enerji eşik değerleri kullanılarak yapılmış ve sistem için hangi eşik değerinin en uygun olduğu bulunmaya çalışılmıştır. İlk eşik değeri olarak 0.0001 seçilmiştir. İkinci eşik değeri olarak 0,17 seçilmiştir. Üçüncü eşik değeri ise bir önceki döngüde tüketilen ortalama enerji miktarı olarak belirlenmiştir.

Çizelge 3.4. Eşik Değeri Seçiminin Farkları

Eşik Değeri	Tüketilen Enerji	Paket Ulaşım Oranı	Kötü niyetli düğüm yakalama oranı
KÜÇÜK	Yüksek	Yüksek	Yüksek
ORTALAMA	Ortalama	Yüksek	Yüksek
YÜKSEK	Düşük	Düşük	Yüksek

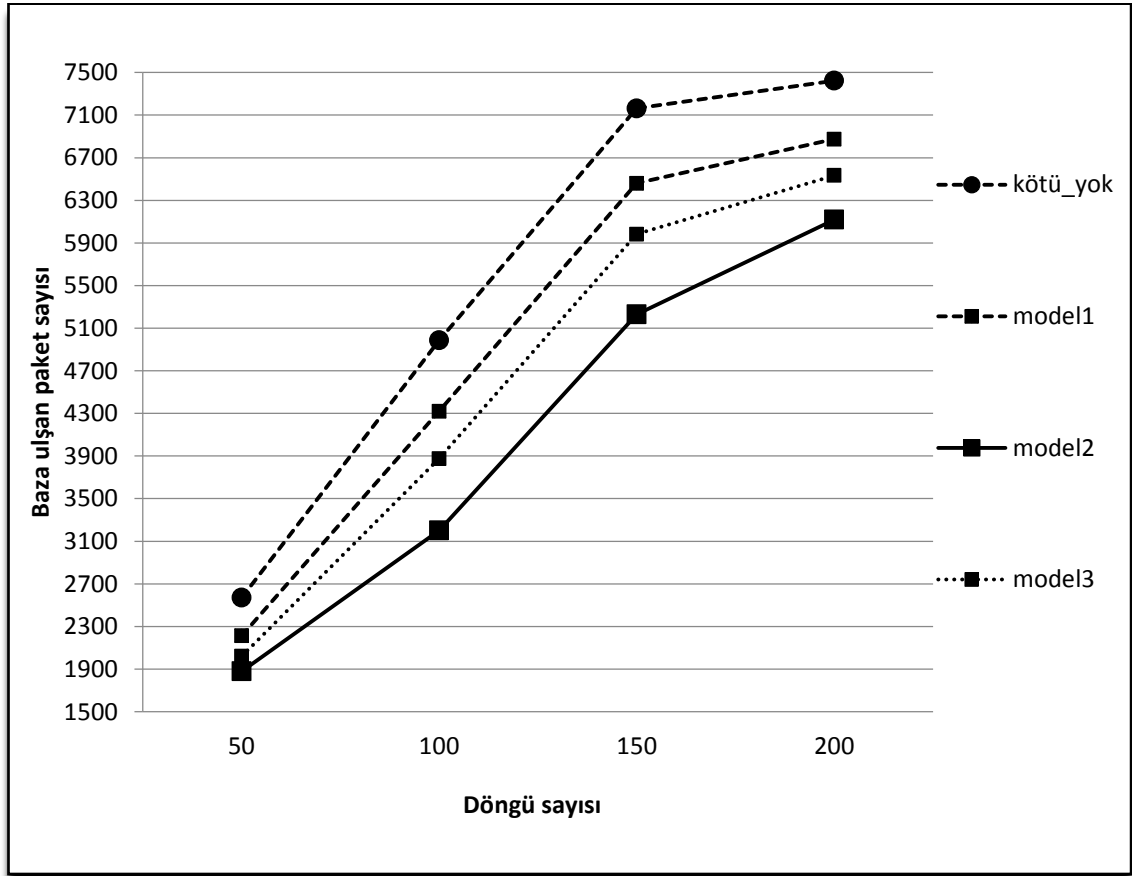
Çizelge 3.5. Simülasyon Parametreleri

Parametreler	Değerler
Ağ Alanı	1000m x 1000m
Düğüm Sayısı(modelleme ve test)	50 100 150 200
Baz İstasyonu Konumu	(500,500)
Düğüm Başlangıç Enerjileri	4J
Kötü Niyetli Düğüm Başlangıç Enerjileri	8J
Düğüm Dağılımı	Rastgele
Paket Boyutu (X)	2000 bit
Kötü Niyetli Düğüm Oranı	%10
Sinkhole Modeli	Model 1
Tasarım Şekli	Tekil, Sürekli
Eşik Değerleri	0.0001, Bir önceki döngüde tüketilen ortalama enerji miktarı, 0,17

4. ARAŞTIRMA BULGULARI VE TARTIŞMA

4.1. Model Zarar Değerlendirmeleri

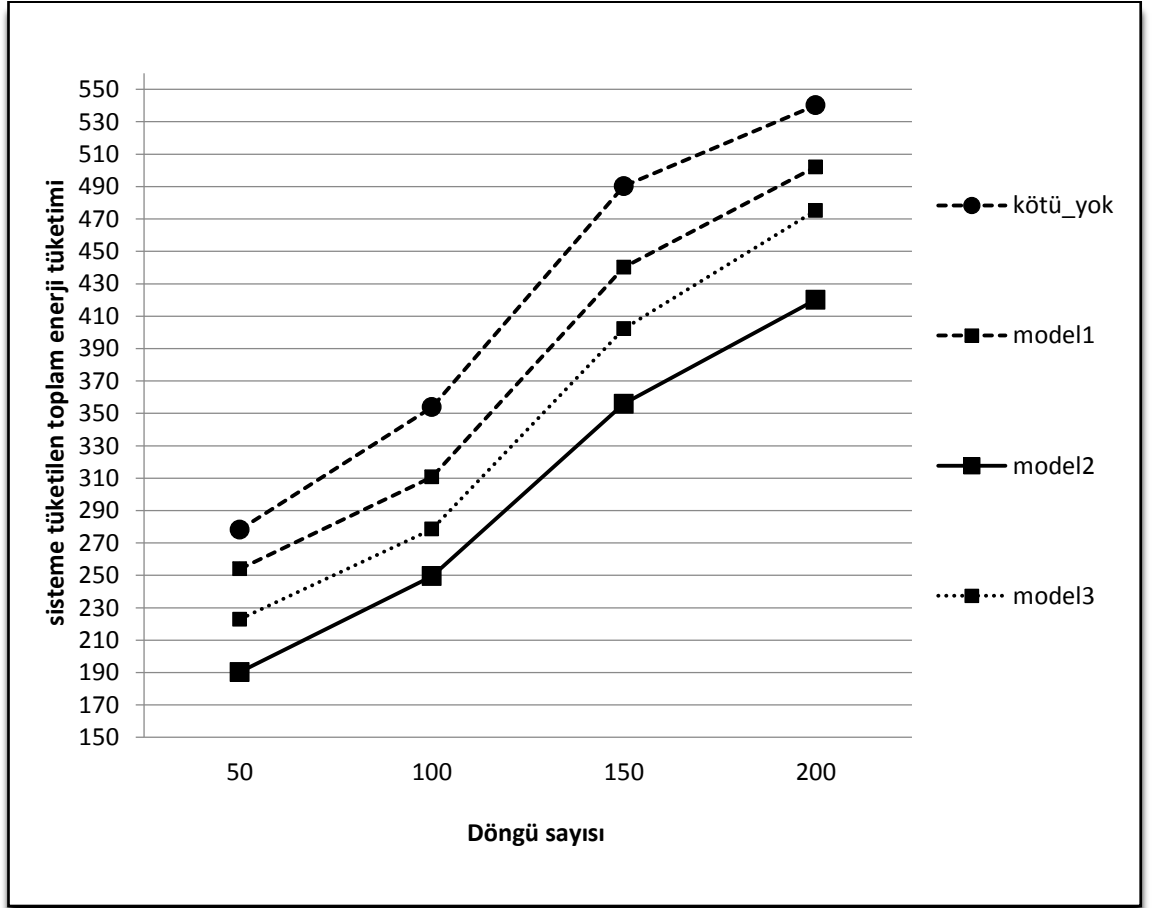
Bu çalışmada tasarlanan modeller için zarar değerlendirmesi, baz istasyonuna ulaşan paket sayısı, sistemde tüketilen ortalama enerji miktarı ve ağda yaşayan düğüm sayısı parametreleri üzerinden yapılmıştır.



Şekil 4.1. Baz istasyonuna ulaşan Paket sayısı kıyası

Şekil 4.1.'de kötü niyetli bir düğümün olmadığı durum ile birlikte, sinkhole saldırısı için tasarlanan üç modelin farklı düğüm sayılarında baz istasyonuna ulaşan toplam paket sayıları görülmektedir. Kötü niyetli düğümlerin doğrudan ya da dolaylı olarak paketlerin baz istasyonuna ulaşmasını engellemesi nedeniyle, tasarlanan her üç modelde de paket kayıpları yaşanmaktadır. Düğüm sayısı arttıkça her üç model içinde baza ulaşan paket kayıp oranlarında artış meydana gelmiştir. Bunun nedeni düğüm sayısının artmasıyla doğru orantılı olarak kötü niyetli düğümlerin etki ettiği düğümlerin sayısının da artmasıdır. Baza ulaşan paket sayısındaki azalma miktarı düğüm sayısından

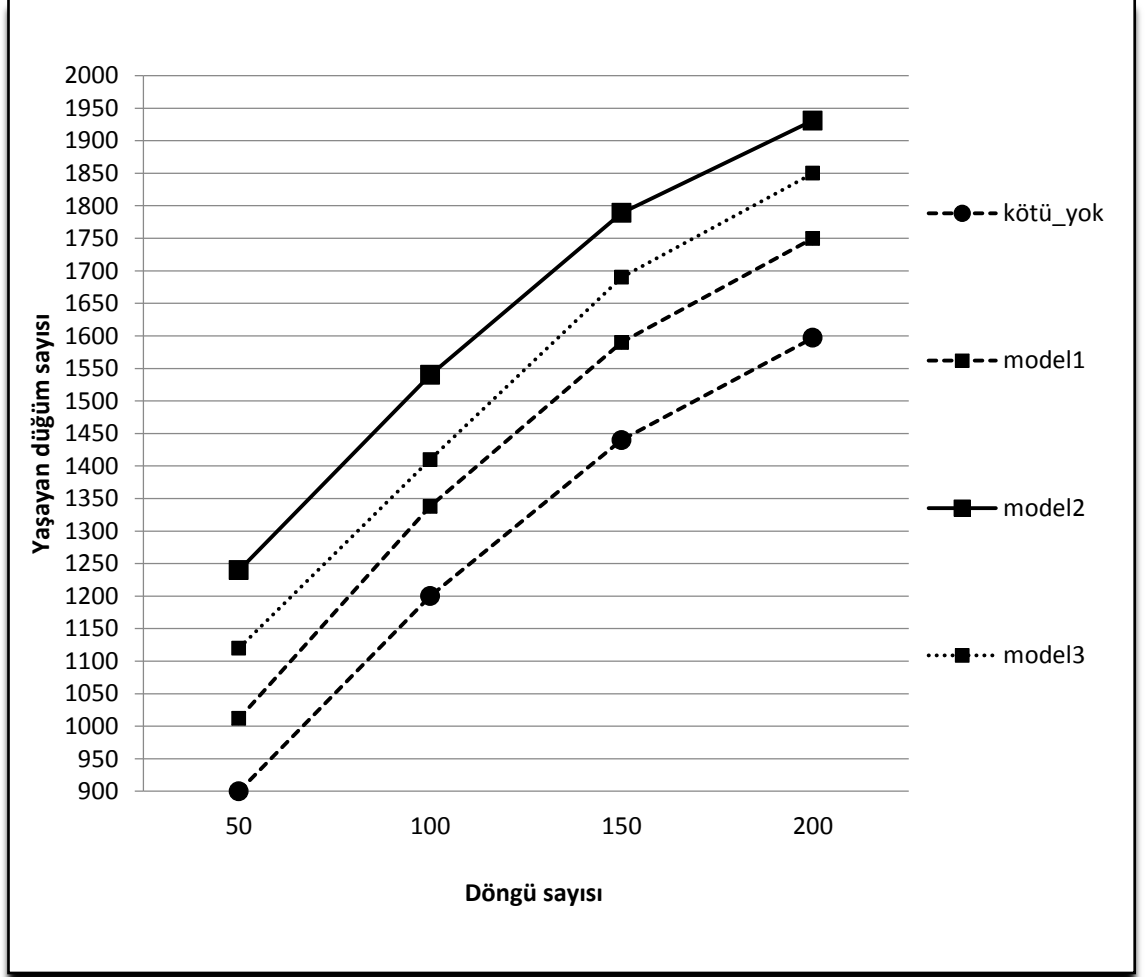
bağımsız olarak en fazla Model 2 ‘ de en az ise Model 1’ de gözlemlenmiştir. Bunun nedeni Model 2’ nin Model 1 ve Model 3’ e göre daha fazla düğümü etkisi altına almasıdır. Model 1’ de toplam düğüm sayısının %10’ u kadar düğüm kötü niyetli olmakla beraber Model 2’ de kötü niyetli düğümün etkisi altına aldığı düğümler kötü niyetli olmaktadır. Model 2’ nin daha fazla düğümü etkisi altına alma şansı olduğu için daha fazla paket kaybına neden olmuştur.



Şekil 4.2. Sistemde tüketilen toplam enerji miktarı

Şekil 4.2.’de kötü niyetli bir düğümün olmadığı durum ile birlikte, sinkhole saldırısı için tasarlanan üç modelin farklı düğüm sayılarında sistemde tüketilen toplam enerji miktarı görülmektedir. Düğüm sayısından bağımsız olarak, kötü niyetli düğümün olduğu durumlarda harcanan toplam enerji miktarı, kötü niyetli düğüm olmadığı duruma göre daha azdır. Bu değerlere göre her ne kadar kötü niyetli düğüm ağına daha uzun süre yaşamasına katkı sağlıyor gibi görünse de, gerçekte nedeni ağına performansının artması değil, kötü niyetli düğümün baz istasyonuna paket iletimini engellediği için düğümlerin

boşta olmasıdır. Şekil 4.3.'te görüldüğü gibi sinkhole saldırısı için tasarlanan üç modelde de boşta olan düğümler verilerini yollamak için enerji harcamadığından dolayı daha uzun süre hayatta kalmaktadır.



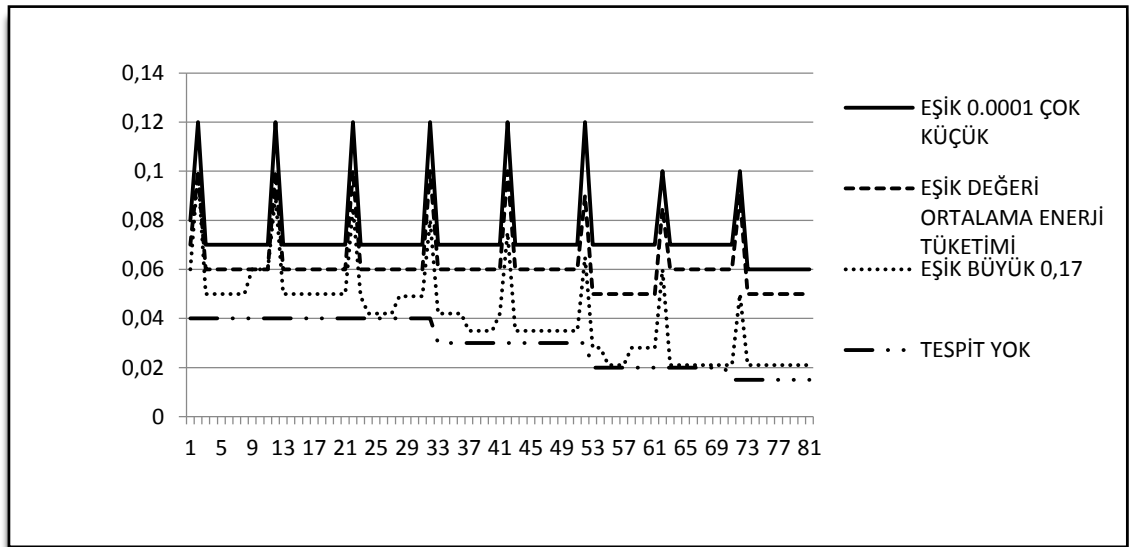
Şekil 4.3. Sistemde yaşayan düğüm sayıları

Sinkhole saldırılarının farklı şekillerde modellenmesi ve test edilip değerlendirilmesi işlemlerinin ardından tespit çalışmaları yapılmıştır. Saldırı tespiti, bu çalışmada Model 1 üzerinde gerçekleştirilmiştir. Bunun nedeni Model 2 ve Model 3 için literatürde çeşitli tespit çalışmalarının bulunmasıdır (Sharmilla,2011; Papadimitriou, 2009; Bahekmata, 2012; Han,2014; Razzaque,2013; Ngai,2007; Rajkumar,2013; Sahraoui,2013; Chen,2010; Hichem,2012; Radhikabaskar,2014; Shio, 2011; Shilpa, 2012)

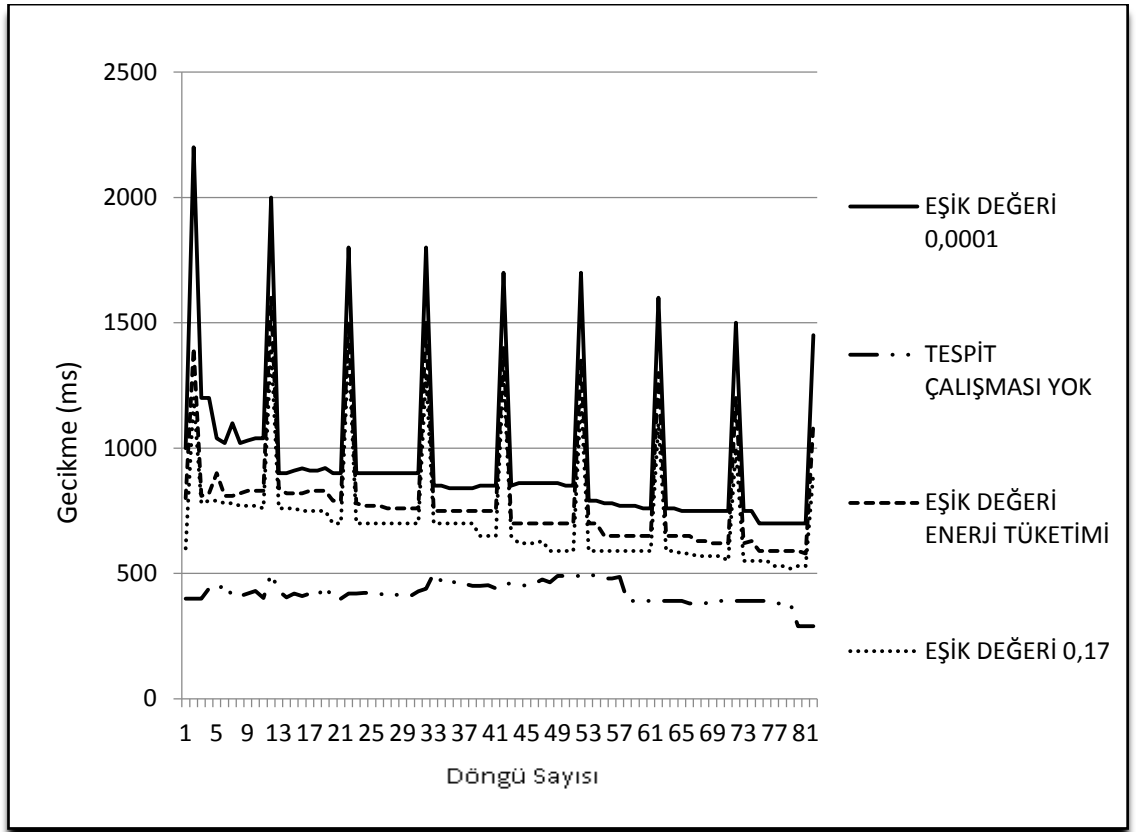
4.2. Tespit Çalışması Sonuçları

Bu çalışmada kötü niyetli çıkma durumu tasarlanan Model 1 üzerinden, tekil saldırı ve sürekli saldırı olmak üzere iki farklı şekilde modellenmiş ve bu modellemeler için ayrı ayrı tespit çalışması yapılmıştır. Tekil saldırı modelinde kötü niyetli düğümler ikinci döngüde sisteme dahil edilmiştir. Kötü niyetli düğümlerin tespiti yapıldıktan sonra tekrar sisteme dahil edilmemiştir. Sürekli saldırı modelinde ise kötü niyetli düğümler 10 döngüde bir sisteme dahil edilmiştir. Kötü niyetli düğümler yakalansa bile 10 döngüde bir tekrar sisteme dahil edilmiştir. Kural tabanlı tespit çalışması farklı eşik değerleri kullanılarak yapılmış ve sistem için hangi eşik değerinin daha uygun olduğu bulunmaya çalışılmıştır. Eşik değerleri belirlendikten sonra tespit çalışması yapılmıştır. İlk eşik değeri olarak çok küçük bir değer belirlenmiş ve 0.0001 seçilmiştir. İkinci eşik değeri olarak çok büyük bir değer olarak belirlenmiş ve 0,17 seçilmiştir. Üçüncü eşik değeri ise ortalama bir değer belirlenmiş ve bir önceki döngüde tüketilen ortalama enerji miktarı olarak seçilmiştir. Bu eşik değerlerine göre sistem için performans değerlendirmesi, sistemde tüketilen ortalama enerji miktarı, baz istasyonuna ulaşan paket sayısı ve sistemdeki gecikme parametreleri üzerinden yapılmıştır.

Sürekli saldırı modeli için, sistemde tüketilen toplam enerji miktarının farklı düğüm sayıları ve farklı eşik değerleri üzerinden değerlendirilmesi;



Şekil 4.4. Sürekli Saldırı Modelinde farklı eşik değerleri için 50 düğümde tüketilen toplam enerji miktarının kıyaslanması

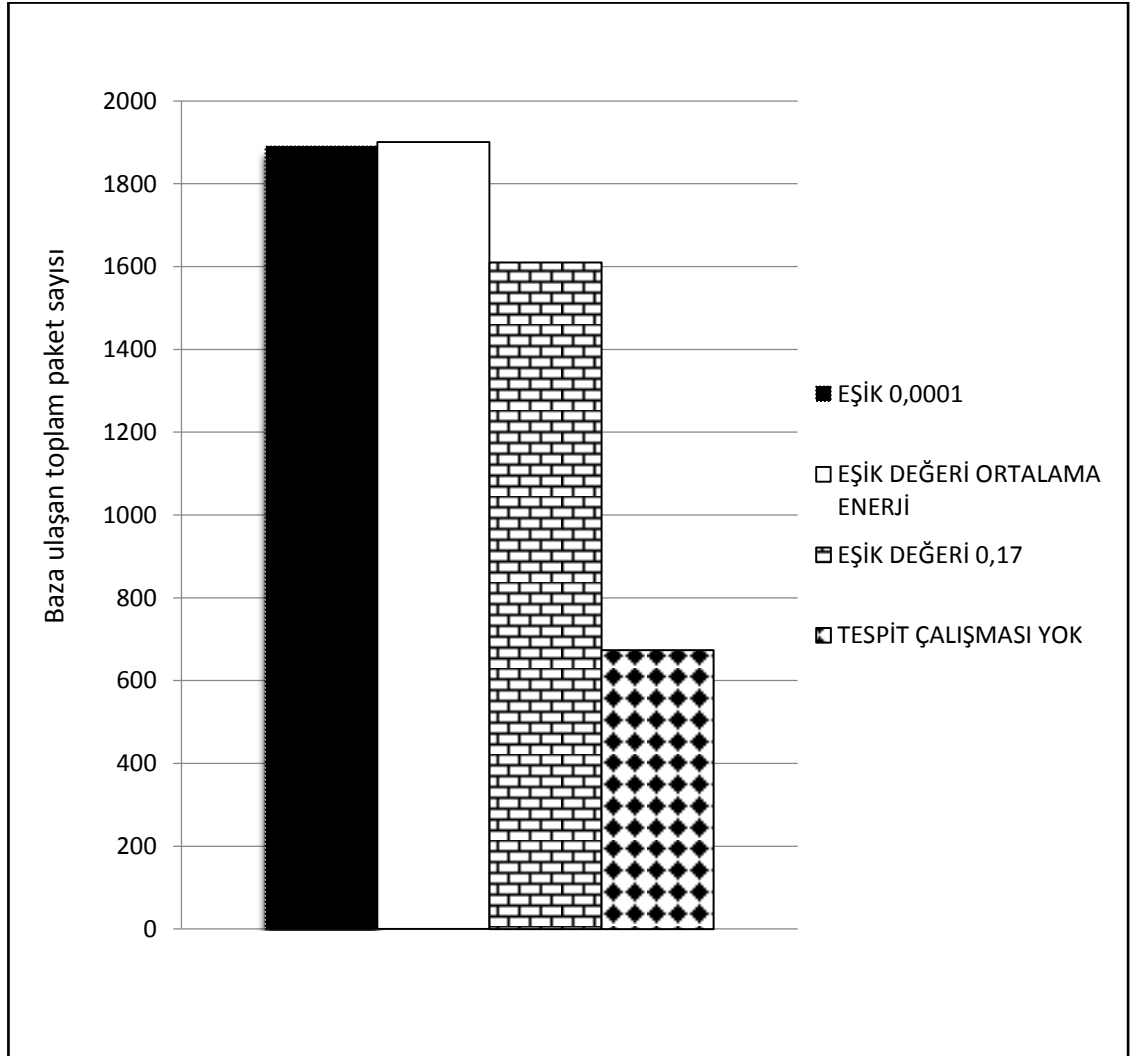


Şekil 4.5. Sürekli Saldırı Modelinde farklı eşik değerleri için 50 düğümde gecikmelerin kıyaslanması

Şekil 4.4.'te 50 düğüm için her döngüdeki tüketilen toplam enerji miktarının sürekli saldırı modelinde farklı eşik değerleri üzerinden kıyaslanması görülmektedir. Sistemde tespit çalışması yapılmadığı durumda, farklı eşik değerlerinde tespit çalışması yapıldığı duruma göre daha az enerji harcadığı görülmektedir. Bunun nedeni sistemin kötü niyetli düğümü tespit etmek için ekstra enerji harcamasıdır. Sürekli saldırı modelinde kötü niyetli düğümler 10 döngüde bir sisteme dahil edildiği için, bu döngülerde baz istasyonu kötü niyetli düğümleri tespit etmek için sorgu mesajları yollamış ve sistemde maksimum oranda enerji harcanmıştır. Sistemde tüketilen enerji miktarı en fazla eşik değerinin 0,0001 seçildiği durumda meydana gelmiştir. Bunun nedeni baz istasyonu küçük eşik değerinde, şüpheli düğümlere daha fazla sorgu mesajı yollaması, buna bağlı olarak fazladan enerji harcamasıdır. Aynı şekilde sistemde tüketilen enerji miktarı en az eşik değerinin 0,17 seçildiği durumda meydana gelmiştir. Bunun nedeni bir önceki durumla benzer olup, baz istasyonunun büyük eşik değerinde şüpheli düğümlere daha az sorgu mesajı yollaması, buna bağlı olarak daha az enerji harcamasıdır. Eşik değerinin ortalama enerji miktarı seçildiği durumda ise bu iki

değerin arasında ortalama bir enerji harcanmıştır. Eşik değeri 0,0001 seçildiği durumda tespit çalışması yapılmadığı duruma göre %59 daha fazla enerji, eşik değeri bir önceki döngüde tüketilen ortalama enerji miktarı seçildiği durumda tespit çalışması yapılmadığı duruma göre %46 daha fazla enerji, eşik değeri 0,17 seçildiği durumda tespit çalışması yapılmadığı duruma göre % 27 daha fazla enerji harcanmıştır. Sistemde meydana gelen gecikmeler enerji tüketimi ile paralellik göstermektedir (Şekil 4.5.).

Her ne kadar eşik değerinin büyük seçilmesi sistemde tüketilen toplam enerji miktarı ve gecikme için faydalı gibi görünse de, bu eşik değerinde paket yakalama oranı ve kötü niyetli düğüm yakalama oranı diğer eşik değerlerine göre daha kötü sonuç vermektedir.



Şekil 4.6. Sürekli Saldırı Modelinde farklı eşik değerleri için 50 düğümde yakalanan paket miktarının kıyaslanması

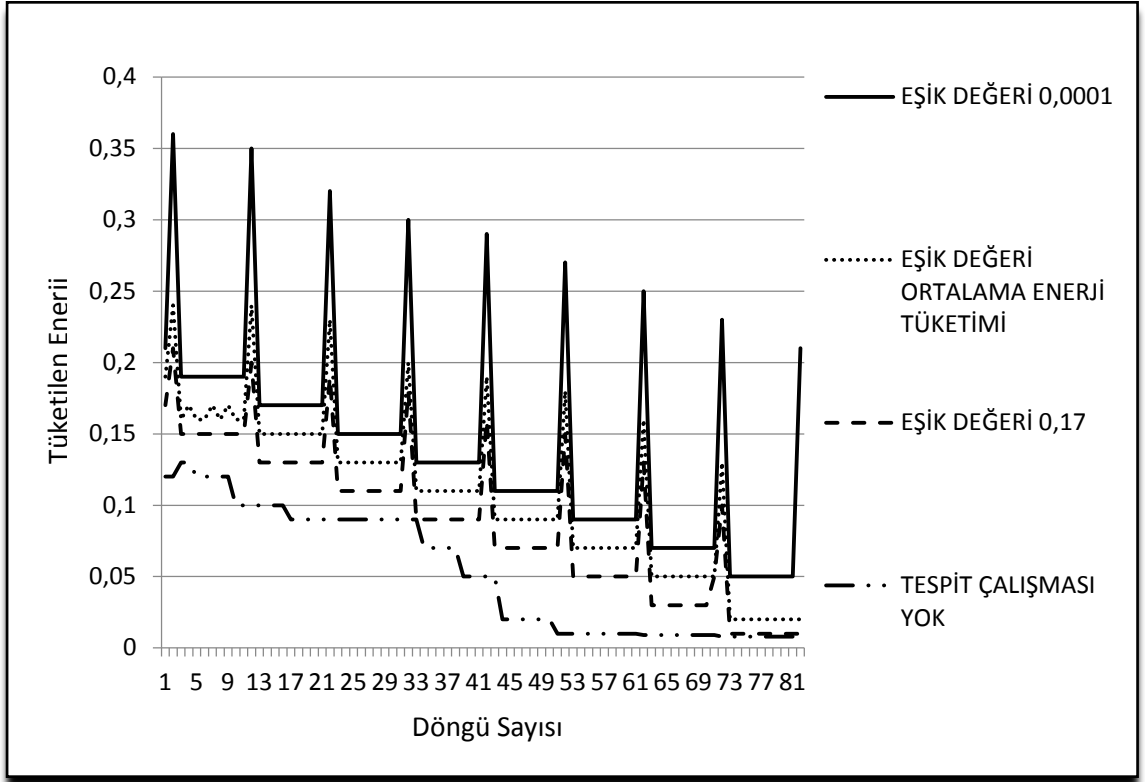
Şekil 4.6.'da 50 düğüm için sisteme yakalanan paket miktarının sürekli saldırı modelinde farklı eşik değerleri üzerinden kıyaslanması görülmektedir. Tespit çalışması yapılmadığı durumda, farklı eşik değerlerine göre tespit çalışması yapıldığı durumlara göre daha az paket yakalanmıştır. Eşik değerinin 0,17 seçildiği durumda diğer eşik değerlerine göre daha az paket yakalanmıştır. Bunun nedeni büyük eşik değerinde baz istasyonunun kötü niyetli düğümlerin tamamını tespit edememesi, buna bağlı olarak kötü niyetli düğümlerin baz istasyonuna paket yollamamasıdır. Eşik değeri 0,17 seçildiği durumda diğer eşik değerlerine göre ortalama %15 daha az paket yakalanmıştır.

Çizelge 4.1.'de görüldüğü gibi eşik değeri 0,17 seçildiği durumda kötü niyetli yakalama oranı %90' dır. Diğer eşik değerlerinde ise bu oran %100' dür.

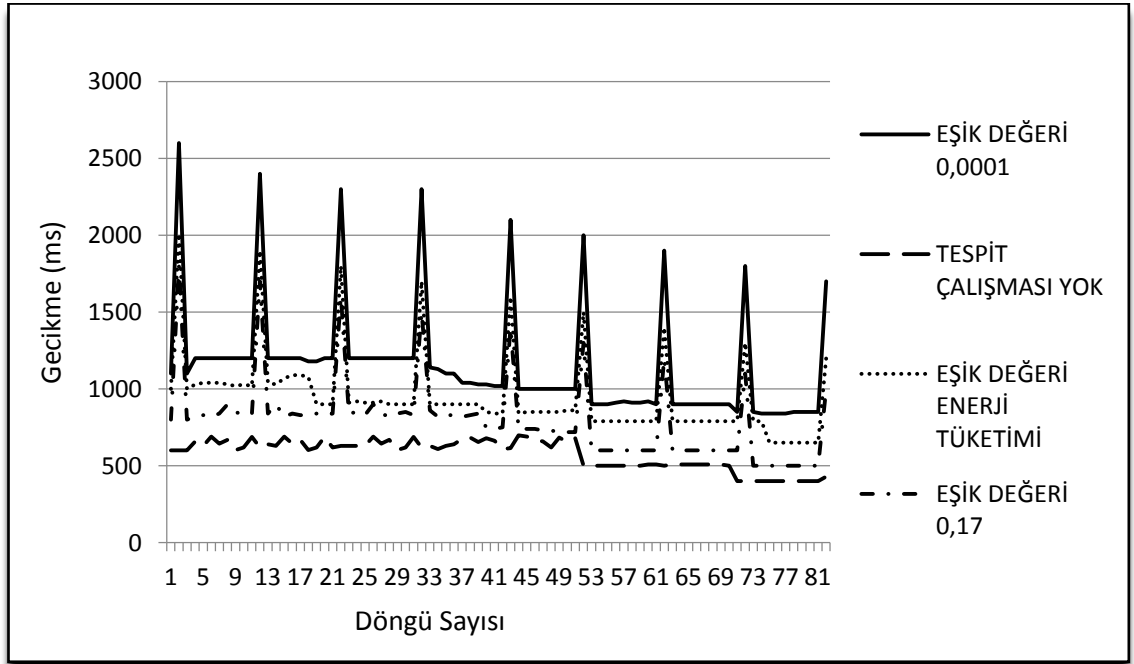
Çizelge 4.1. 50 Düğüm için kötü niyetli düğüm yakalama oranı

Sistemde Çıkan Kötü Niyetli Düğüm Yüzdesi	Eşik Değeri 0,0001 İken Yakalanan Kötü Niyetli Düğüm Yüzdesi	Eşik Değeri Ortalama Enerji Tüketimi İken Yakalanan Kötü Niyetli Düğüm Yüzdesi	Eşik Değeri 0,17 İken Yakalanan Kötü Niyetli Düğüm Yüzdesi
%100	%100	%100	%90

Şekil 4.7.'de 100 düğüm için her döngüdeki tüketilen toplam enerji miktarının sürekli saldırı modelinde farklı eşik değerleri üzerinden kıyaslanması görülmektedir. Sistemde tespit çalışması yapılmadığı durumda, farklı eşik değerlerinde tespit çalışması yapıldığı duruma göre daha az enerji harcandığı görülmektedir. Bunun nedeni sistemin kötü niyetli düğümü tespit etmek için ekstra enerji harcamasıdır. Eşik değeri 0,0001 seçildiği durumda tespit çalışması yapılmadığı duruma göre %62 daha fazla enerji, eşik değeri bir önceki döngüde tüketilen ortalama enerji miktarı seçildiği durumda tespit çalışması yapılmadığı duruma göre %51 daha fazla enerji, eşik değeri 0,17 seçildiği durumda tespit çalışması yapılmadığı duruma göre % 41 daha fazla enerji harcanmıştır. Sistemde meydana gelen gecikmeler enerji tüketimi ile paralellik göstermektedir (Şekil 4.8.).



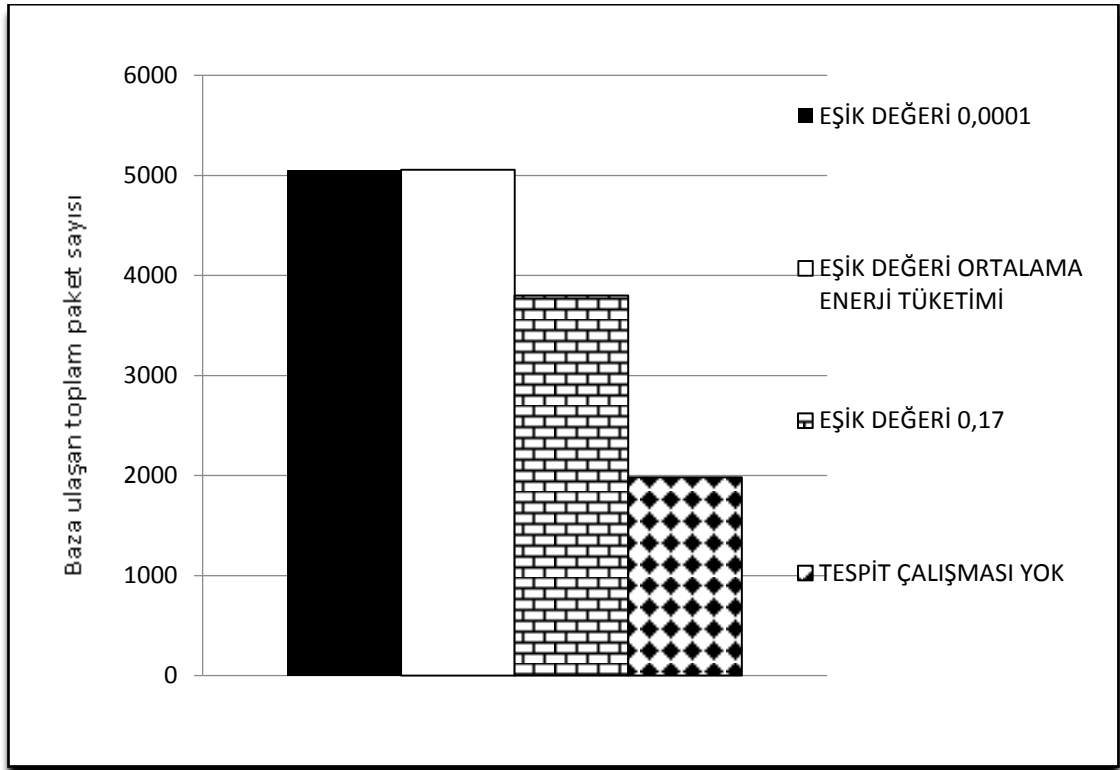
Şekil 4.7. Sürekli Saldırı Modelinde farklı eşik değerleri için 100 düğümde tüketilen toplam enerji miktarının kıyaslanması



Şekil 4.8. Sürekli Saldırı Modelinde farklı eşik değerleri için 100 düğümde gecikmelerin kıyaslanması

Her ne kadar eşik değerinin büyük seçilmesi sistemde tüketilen toplam enerji miktarı ve gecikme için faydalı gibi görünse de, bu eşik değerinde paket yakalama

oranı ve kötü niyetli düğüm yakalama oranı diğer eşik değerlerine göre daha kötü sonuç vermektedir.



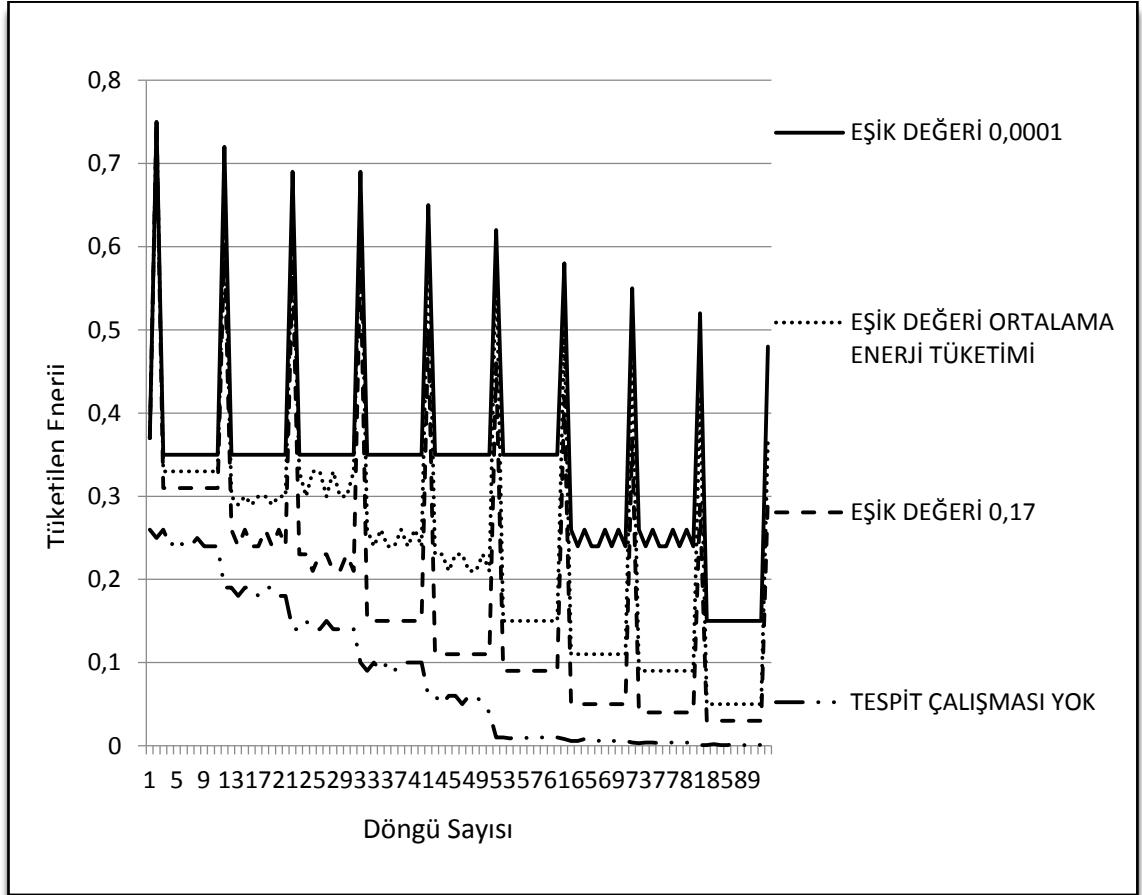
Şekil 4.9. Sürekli Saldırı Modelinde farklı eşik değerleri için 100 düğümde yakalanan paket miktarının kıyaslanması

Şekil 4.9.'da 100 düğüm için sisteme yakalanan paket miktarının sürekli saldırı modelinde farklı eşik değerleri üzerinden kıyaslanması görülmektedir. Tespit çalışması yapılmadığı durumda, farklı eşik değerlerine göre tespit çalışması yapıldığı durumlara göre daha az paket yakalanmıştır. Eşik değerinin 0,17 seçildiği durumda diğer eşik değerlerine göre daha az paket yakalanmıştır. Bunun nedeni büyük eşik değerinde baz istasyonunun kötü niyetli düğümlerin tamamını tespit edememesi, buna bağlı olarak kötü niyetli düğümlerin baz istasyonuna paket yollamamasıdır. Eşik değeri 0,17 seçildiği durumda diğer eşik değerlerine göre ortalama %25 daha az paket yakalanmıştır.

Çizelge 4.2.'de görüldüğü üzere eşik değeri 0,17 seçildiği durumda kötü niyetli yakalama oranı %65' dir. Diğer eşik değerlerinde ise bu oran %100' dür.

Çizelge 4.2. 100 Döğüm için kötü niyetli döğüm yakalama oranı

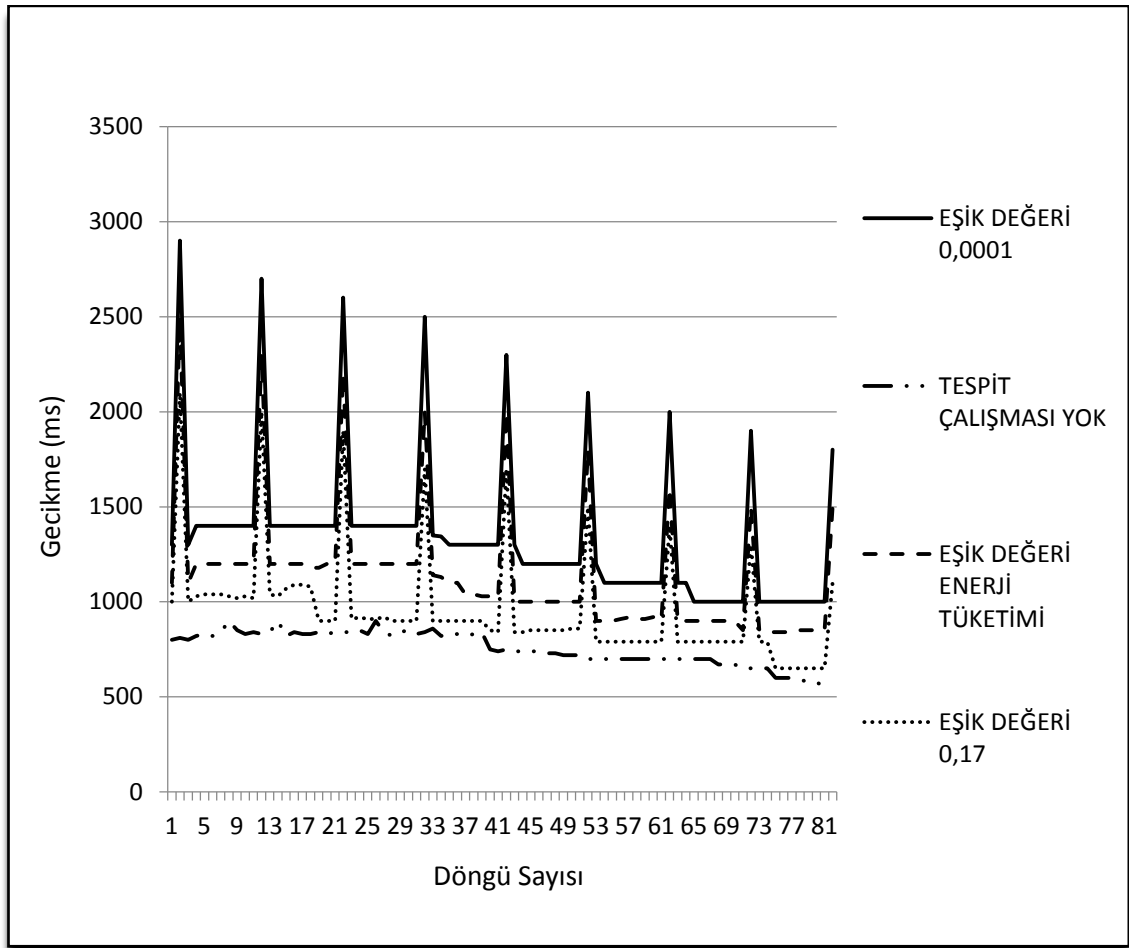
Sistemde Çıkan Kötü Niyetli Döğüm Yüzdesi	Eşik Değeri 0,0001 İken Yakalanan Kötü Niyetli Döğüm Yüzdesi	Eşik Değeri Ortalama Enerji Tüketimi İken Yakalanan Kötü Niyetli Döğüm Yüzdesi	Eşik Değeri 0,17 İken Yakalanan Kötü Niyetli Döğüm Yüzdesi
%100	%100	%100	%65



Şekil 4.10. Sürekli Saldırı Modelinde farklı eşik değerleri için 150 döğümde tüketilen toplam enerji miktarının kıyaslanması

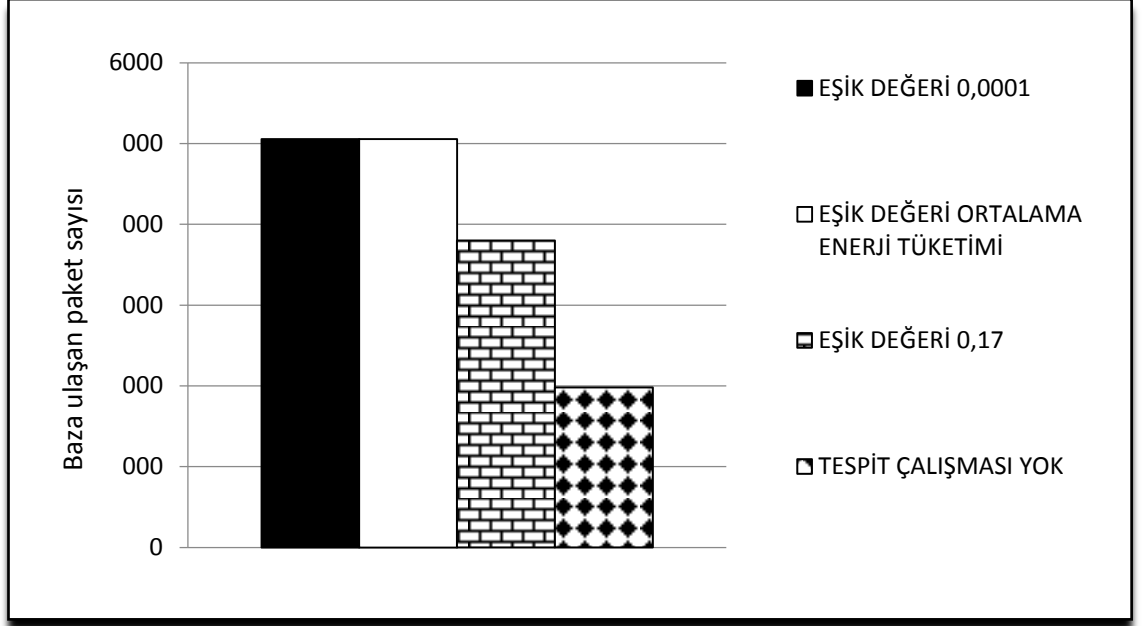
Şekil 4.10.'da 150 döğüm için her döğümdeki tüketilen toplam enerji miktarının sürekli saldırı modelinde farklı eşik değerleri üzerinden kıyaslanması görülmektedir. Sistemde tespit çalışması yapılmadığı durumda, farklı eşik değerlerinde tespit çalışması yapıldığı duruma göre daha az enerji harcandığı görülmektedir. Bunun nedeni sistemin kötü niyetli döğümü tespit etmek için ekstra enerji harcamasıdır. Eşik değeri 0,0001 seçildiği durumda tespit çalışması yapılmadığı duruma göre %66 daha fazla enerji, eşik değeri bir önceki döğümde tüketilen ortalama enerji miktarı seçildiği durumda tespit

çalışması yapılmadığı duruma göre %64 daha fazla enerji, eşik değeri 0,17 seçildiği durumda tespit çalışması yapılmadığı duruma göre % 54 daha fazla enerji harcanmıştır. Her ne kadar eşik değerinin büyük seçilmesi sistemde tüketilen toplam enerji miktarı için faydalı gibi görünse de, bu eşik değerinde paket yakalama oranı ve kötü niyetli düğüm yakalama oranı diğer eşik değerlerine göre daha kötü sonuç vermektedir. Sistemde meydana gelen gecikmeler enerji tüketimi ile paralellik göstermektedir.(Şekil 4.11.)



Şekil 4.11. Sürekli Saldırı Modelinde farklı eşik değerleri için 150 düğümde gecikmelerin kıyaslanması

Her ne kadar eşik değerinin büyük seçilmesi sistemde tüketilen toplam enerji miktarı ve gecikme için faydalı gibi görünse de, bu eşik değerinde paket yakalama oranı ve kötü niyetli düğüm yakalama oranı diğer eşik değerlerine göre daha kötü sonuç vermektedir.



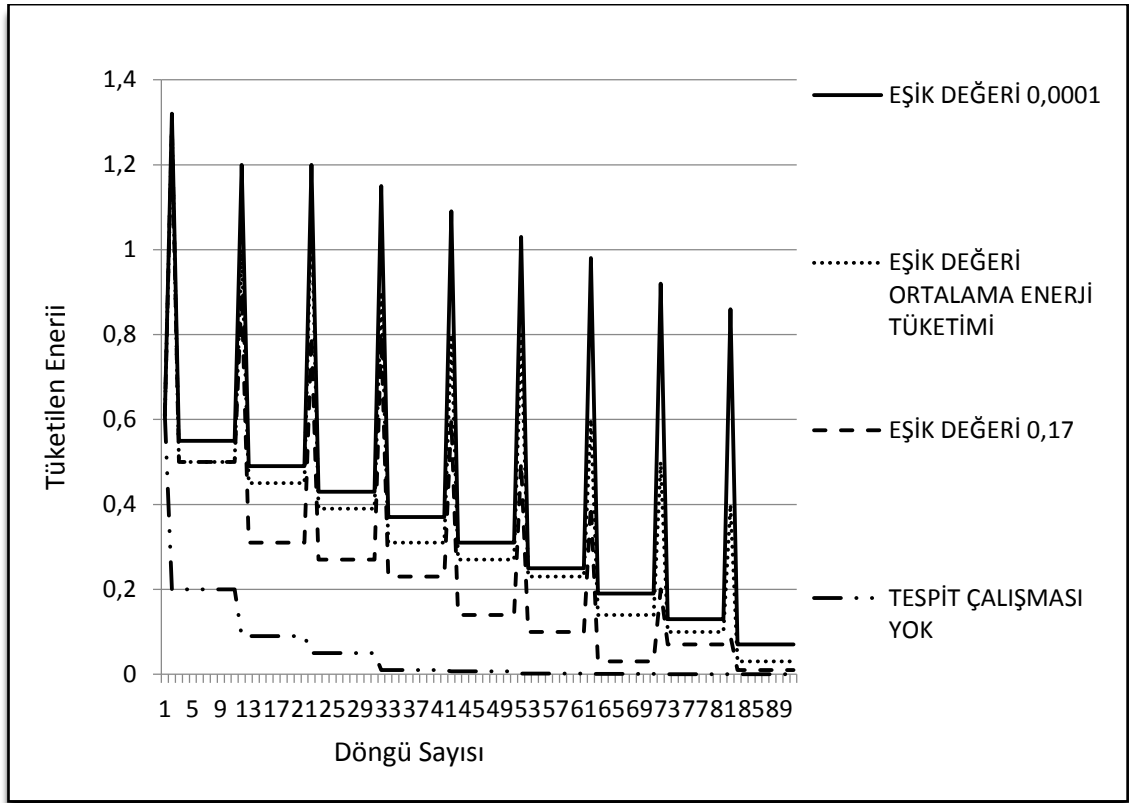
Şekil 4.12. Sürekli Saldırı Modelinde farklı eşik değerleri için 150 düğümde yakalanan paket miktarının kıyaslanması

Şekil 4.12.'de 150 düğüm için sisteme yakalanan paket miktarının sürekli saldırı modelinde farklı eşik değerleri üzerinden kıyaslanması görülmektedir. Tespit çalışması yapılmadığı durumda, farklı eşik değerlerine göre tespit çalışması yapıldığı durumlara göre daha az paket yakalanmıştır. Eşik değerinin 0,17 seçildiği durumda diğer eşik değerlerine göre daha az paket yakalanmıştır. Bunun nedeni büyük eşik değerinde baz istasyonunun kötü niyetli düğümlerin tamamını tespit edememesi, buna bağlı olarak kötü niyetli düğümlerin baz istasyonuna paket yollamamasıdır. Eşik değeri 0,17 seçildiği durumda diğer eşik değerlerine göre ortalama %24 daha az paket yakalanmıştır.

Çizelge 4.3.'de görüldüğü üzere eşik değeri 0,17 seçildiği durumda kötü niyetli yakalama oranı %60' dır. Diğer eşik değerlerinde ise bu oran %100' dür.

Çizelge 4.3. 150 Düğüm için kötü niyetli düğüm yakalama oranı

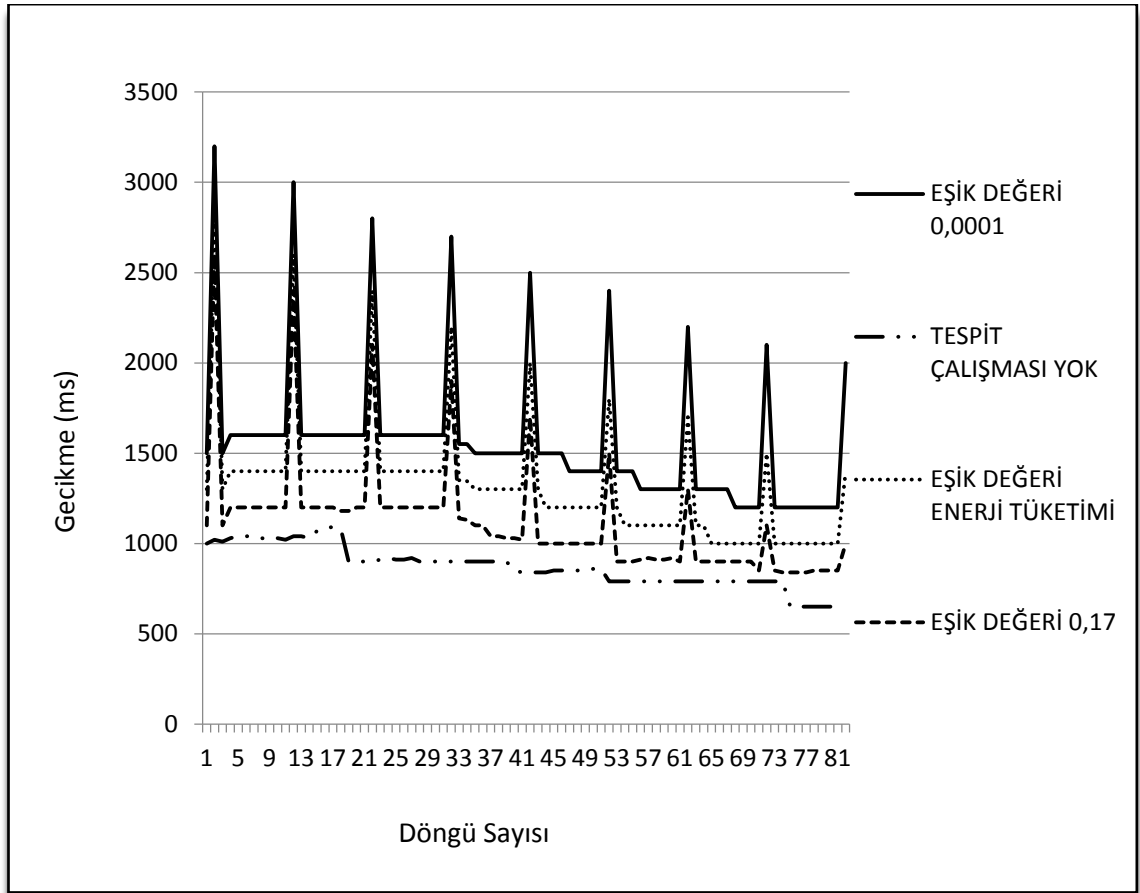
Sistemde Çıkan Kötü Niyetli Düğüm Yüzdesi	Eşik Değeri 0,0001 İken Yakalanan Kötü Niyetli Düğüm Yüzdesi	Eşik Değeri Ortalama Enerji Tüketimi İken Yakalanan Kötü Niyetli Düğüm Yüzdesi	Eşik Değeri 0,17 iken Yakalanan Kötü Niyetli Düğüm Yüzdesi
%100	%100	%100	%60



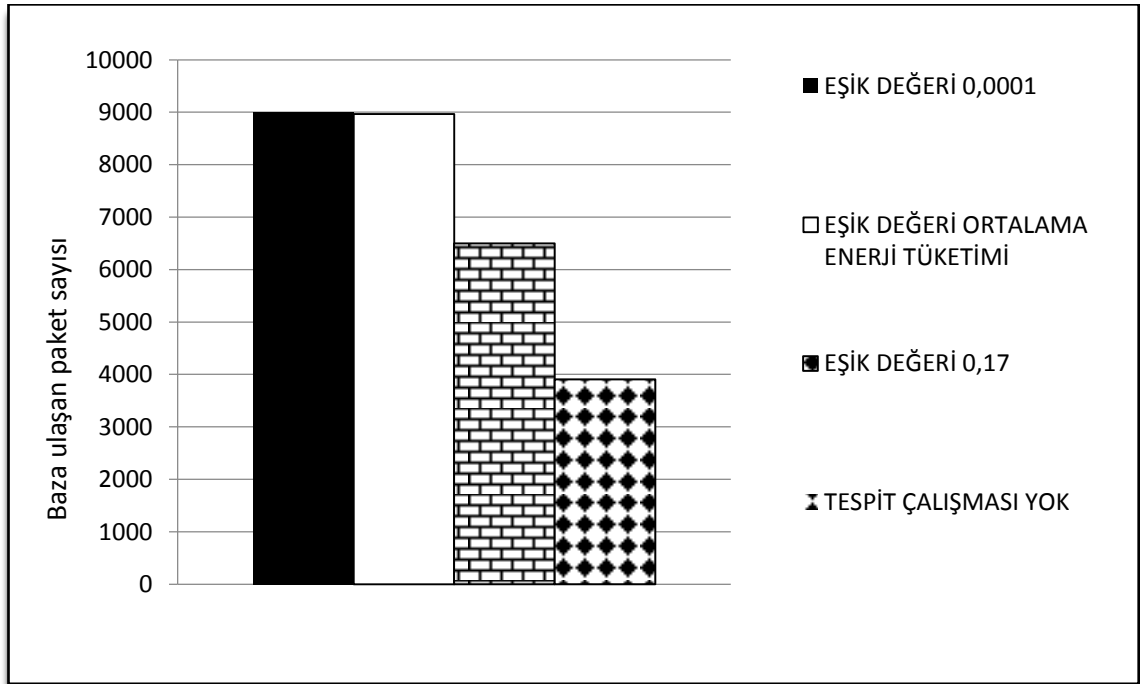
Şekil 4.13. Sürekli Saldırı Modelinde farklı eşik değerleri için 200 düğümde tüketilen toplam enerji miktarının kıyaslanması

Şekil 4.13.'te 200 düğüm için her döngüdeki tüketilen toplam enerji miktarının sürekli saldırı modelinde farklı eşik değerleri üzerinden kıyaslanması görülmektedir. Sistemde tespit çalışması yapılmadığı durumda, farklı eşik değerlerinde tespit çalışması yapıldığı duruma göre daha az enerji harcadığı görülmektedir. Bunun nedeni sistemin kötü niyetli düğümü tespit etmek için ekstra enerji harcamasıdır. Eşik değeri 0,0001 seçildiği durumda tespit çalışması yapılmadığı duruma göre %80 daha fazla enerji, eşik değeri bir önceki döngüde tüketilen ortalama enerji miktarı seçildiği durumda tespit çalışması yapılmadığı duruma göre %75 daha fazla enerji, eşik değeri 0,17 seçildiği durumda tespit çalışması yapılmadığı duruma göre % 70 daha fazla enerji harcanmıştır. Her ne kadar eşik değerinin büyük seçilmesi sistemde tüketilen toplam enerji miktarı için faydalı gibi görünse de, bu eşik değerinde paket yakalama oranı ve kötü niyetli düğüm yakalama oranı diğer eşik değerlerine göre daha kötü sonuç vermektedir.

Düğüm sayısı arttıkça tüm eşik değerlerinde kötü niyetli düğümü bulmak için daha fazla enerji harcanmaktadır. Sistem performansı açısından, yüksek düğüm sayılarında optimum eşik değerini bulmanın önemi artmaktadır. Sistemde meydana gelen gecikmeler enerji tüketimi ile paralellik göstermektedir (Şekil 4.14.).



Şekil 4.14. Sürekli Saldırı Modelinde farklı eşik değerleri için 150 düğümde gecikmelerin kıyaslanması



Şekil 4.15. Sürekli Saldırı Modelinde farklı eşik değerleri için 200 düğümde yakalanan paket miktarının kıyaslanması

Her ne kadar eşik değerinin büyük seçilmesi sistemde tüketilen toplam enerji miktarı ve gecikme için faydalı gibi görünse de, bu eşik değerinde paket yakalama oranı ve kötü niyetli düğüm yakalama oranı diğer eşik değerlerine göre daha kötü sonuç vermektedir.

Şekil 4.15.'de 200 düğüm için sisteme yakalanan paket miktarının sürekli saldırı modelinde farklı eşik değerleri üzerinden kıyaslanması görülmektedir. Tespit çalışması yapılmadığı durumda, farklı eşik değerlerine göre tespit çalışması yapıldığı durumlara göre daha az paket yakalanmıştır. Eşik değerinin 0,17 seçildiği durumda diğer eşik değerlerine göre daha az paket yakalanmıştır. Bunun nedeni büyük eşik değerinde baz istasyonunun kötü niyetli düğümlerin tamamını tespit edememesi, buna bağlı olarak kötü niyetli düğümlerin baz istasyonuna paket yollamamasıdır. Eşik değeri 0,17 seçildiği durumda diğer eşik değerlerine göre ortalama %29 daha az paket yakalanmıştır.

Çizelge 4.4.'de görüldüğü üzere eşik değeri 0,17 seçildiği durumda kötü niyetli yakalama oranı %55' dir. Diğer eşik değerlerinde ise bu oran %100' dür.

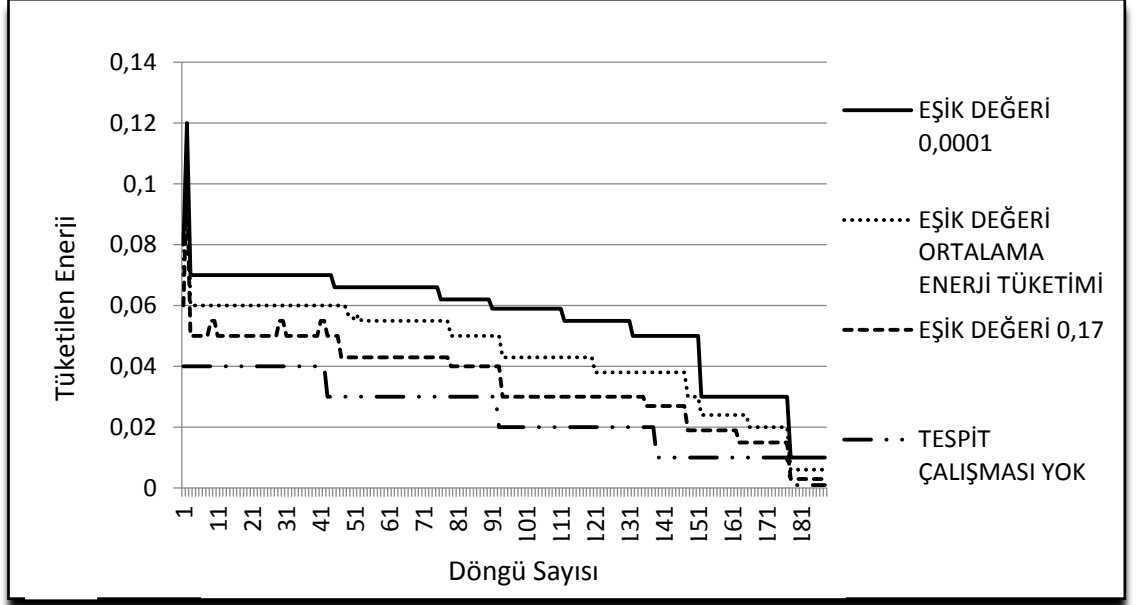
Çizelge 4.4. 200 Düğüm için kötü niyetli düğüm yakalama oranı

Sistemde Çıkan Kötü Niyetli Düğüm Yüzdesi	Eşik Değeri 0,0001 İken Yakalanan Kötü Niyetli Düğüm Yüzdesi	Eşik Değeri Ortalama Enerji Tüketimi İken Yakalanan Kötü Niyetli Düğüm Yüzdesi	Eşik Değeri 0,17 iken Yakalanan Kötü Niyetli Düğüm Yüzdesi
%100	%100	%100	%55

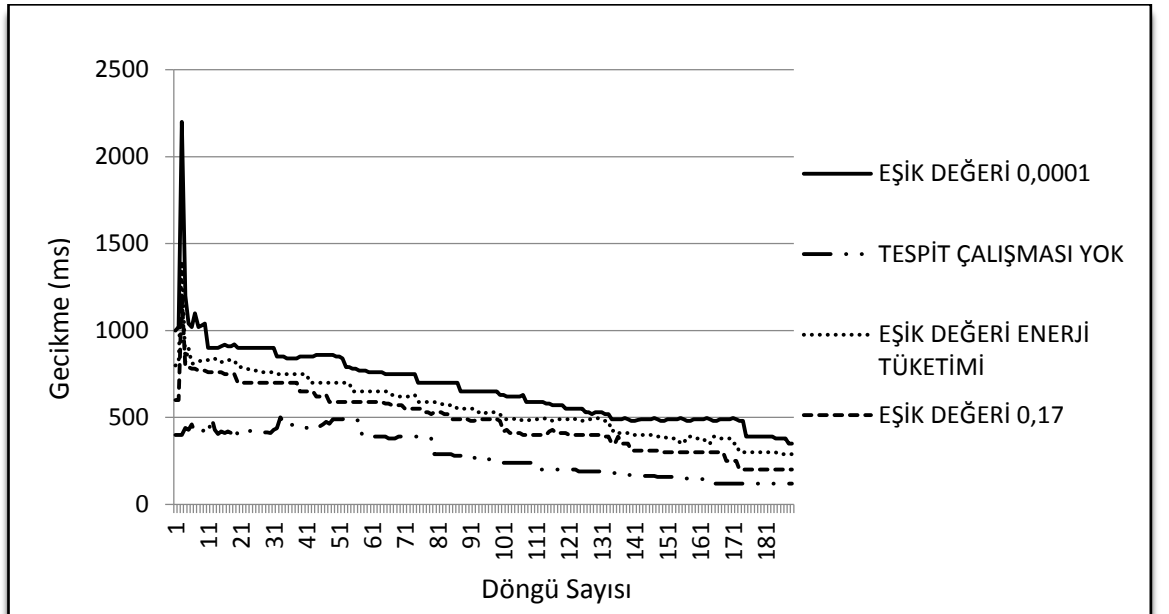
Tekil saldırı modeli için, sistemde tüketilen toplam enerji miktarının farklı düğüm sayıları ve farklı eşik değerleri üzerinden değerlendirilmesi;

Şekil 4.16.'da 50 düğüm için her döngüdeki tüketilen toplam enerji miktarının tekil saldırı modelinde farklı eşik değerleri üzerinden kıyaslanması görülmektedir. Sistemde tespit çalışması yapılmadığı durumda, farklı eşik değerlerinde tespit çalışması yapıldığı duruma göre daha az enerji harcandığı görülmektedir. Bunun nedeni sürekli saldırı modelinde olduğu gibi, sistemin kötü niyetli düğümü tespit etmek için ekstra enerji harcamasıdır. Eşik değeri 0,0001 seçildiği durumda tespit çalışması yapılmadığı duruma göre %58 daha fazla enerji, eşik değeri bir önceki döngüde tüketilen ortalama enerji miktarı seçildiği durumda tespit çalışması yapılmadığı duruma göre %46 daha fazla enerji, eşik değeri 0,17 seçildiği durumda tespit çalışması yapılmadığı duruma göre %31 daha fazla enerji harcanmıştır. Sistemde enerji tüketimi en fazla eşik

değerinin 0,0001 seçildiği durumda meydana gelmiştir. Bunun nedeni baz istasyonunun bataryası az olduğu için paket yollayamayan üye düğümleri şüpheli olarak algılayıp, sorgu mesajı yollamasındandır. Sistemde sorgu mesajının fazla olması ekstra gecikmeye neden olmuştur (Şekil 4.17.).

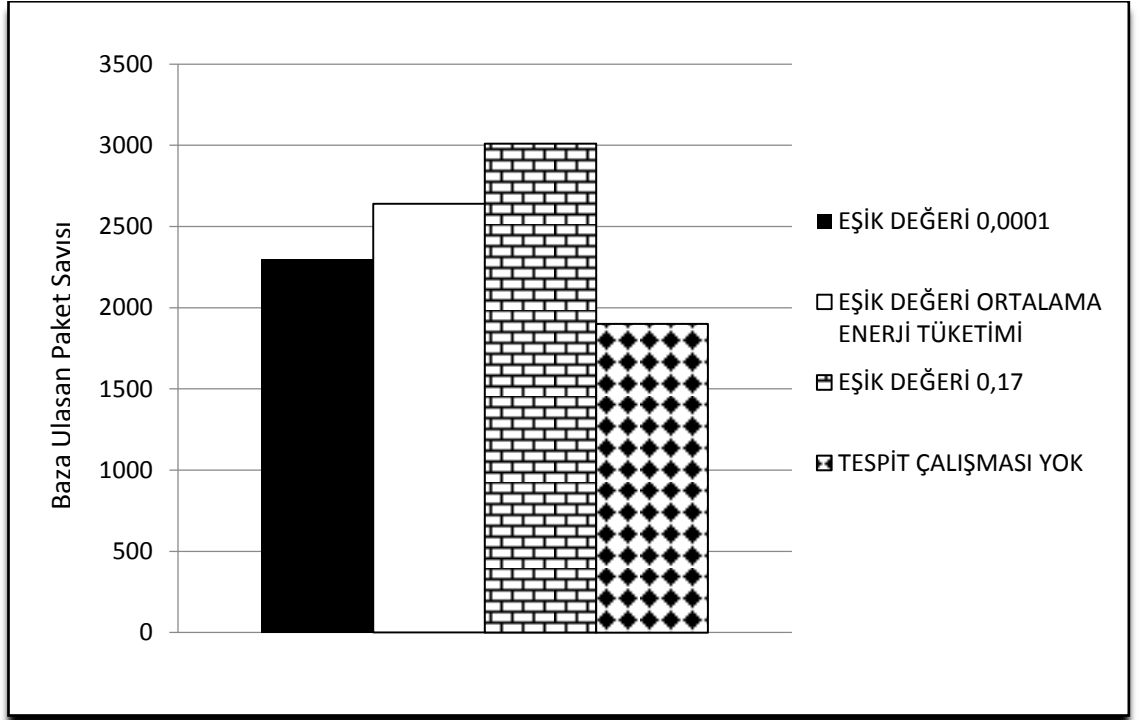


Şekil 4.16. Tekil saldırı modelinde farklı eşik değerleri için 50 düğümde tüketilen toplam enerji miktarının kıyaslanması



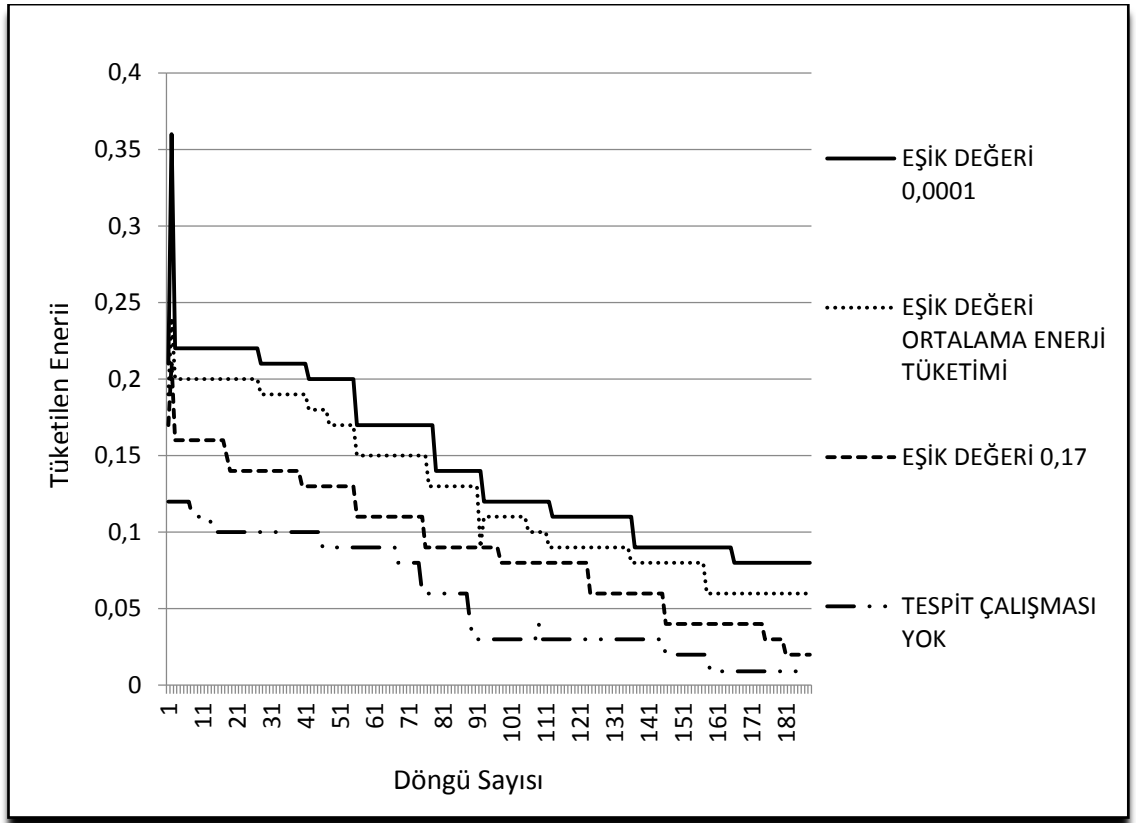
Şekil 4.17. Tekil saldırı modelinde farklı eşik değerleri için 50 düğümde gecikme miktarının kıyaslanması

Tekil saldırı modelinde, sürekli saldırı modeline benzer olarak, eşik değerinin büyük seçilmesi sistemdeki enerji tüketimi ve gecikme bakımından daha iyi sonuç vermektedir. Fakat tekil saldırı modelinde, sürekli saldırı modelinden farklı olarak paket yakalama oranı, büyük eşikte daha iyi sonuç vermektedir.



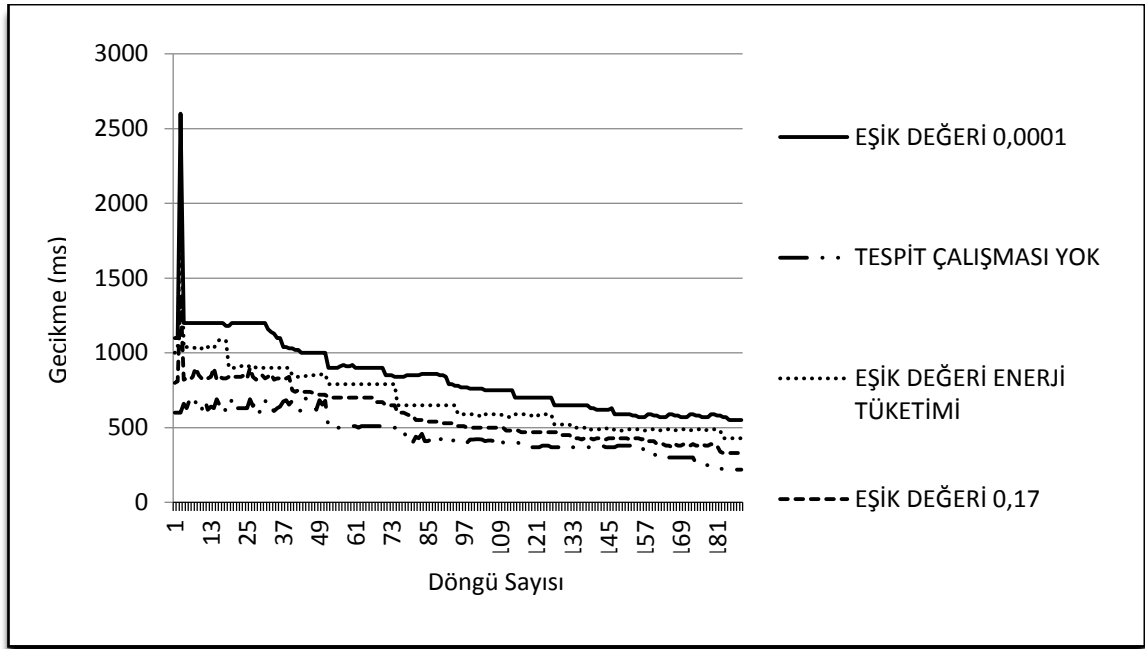
Şekil 4.18. Tekil saldırı modelinde farklı eşik değerleri için 50 düğümde yakalanan paket miktarının kıyaslanması

Şekil 4.18.'de 50 düğüm için sisteme yakalanan paket miktarının tekil saldırı modelinde farklı eşik değerleri üzerinden kıyaslanması görülmektedir. Tespit çalışması yapılmadığı durumda, farklı eşik değerlerine göre tespit çalışması yapıldığı durumlara göre daha az paket yakalanmıştır. Bunun nedeni tespit edilemeyen kötü niyetli düğümlerin sisteme zarar vermeye devam etmesidir. Eşik değerinin 0,0001 seçildiği durumda diğer eşik değerlerine göre daha az paket yakalanmıştır. Bunun nedeni daha çok enerji harcayan düğümlerin bataryalarının daha erken bitmesi ve paketlerini baz istasyonuna ulaştıramamasıdır. Eşik değerinin 0,0001 seçildiği durumda diğer eşik değerlerine göre ortalama %28 daha az paket yakalanmıştır.



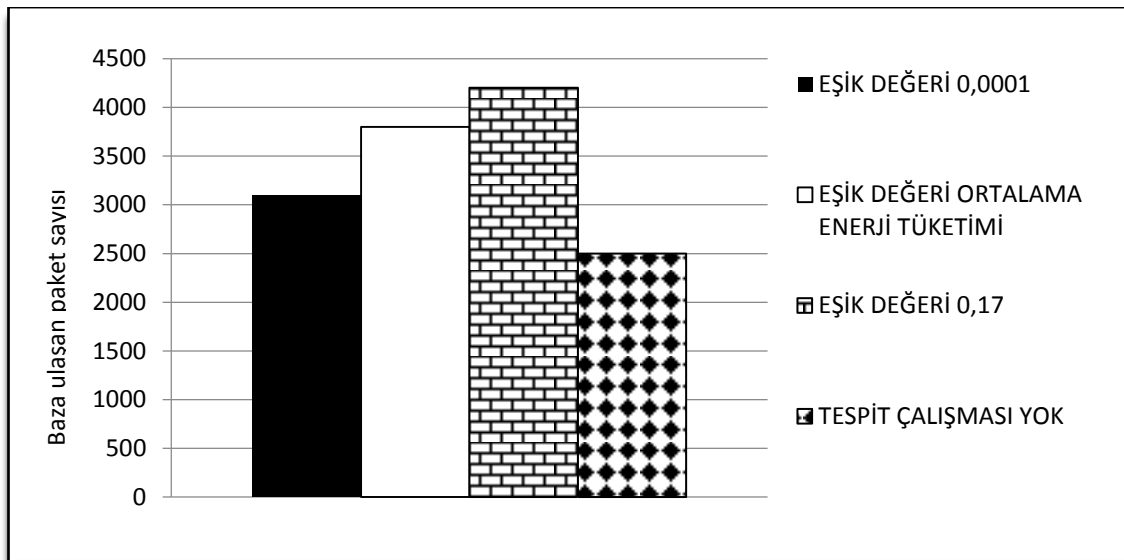
Şekil 4.19. Tekil saldırı modelinde farklı eşik değerleri için 100 düğümde tüketilen toplam enerji miktarının kıyaslanması

Şekil 4.19.'da 100 düğüm için her döngüdeki tüketilen toplam enerji miktarının tekil saldırı modelinde farklı eşik değerleri üzerinden kıyaslanması görülmektedir. Sistemde tespit çalışması yapılmadığı durumda, farklı eşik değerlerinde tespit çalışması yapıldığı duruma göre daha az enerji harcandığı görülmektedir. Bunun nedeni sürekli saldırı modelinde olduğu gibi, sistemin kötü niyetli düğümü tespit etmek için ekstra enerji harcamasıdır. Eşik değeri 0,0001 seçildiği durumda tespit çalışması yapılmadığı duruma göre %59 daha fazla enerji, eşik değeri bir önceki döngüde tüketilen ortalama enerji miktarı seçildiği durumda tespit çalışması yapılmadığı duruma göre %48 daha fazla enerji, eşik değeri 0,17 seçildiği durumda tespit çalışması yapılmadığı duruma göre %32 daha fazla enerji harcanmıştır. Sistemde enerji tüketimi en fazla eşik değerinin 0,0001 seçildiği durumda meydana gelmiştir. Bunun nedeni baz istasyonunun bataryası az olduğu için paket yollayamayan üye düğümleri şüpheli olarak algılayıp, sorgu mesajı yollamasındandır. Sistemde sorgu mesajının fazla olması ekstra gecikmeye neden olmuştur (Şekil 4.20.).



Şekil 4.20. Tekil saldırı modelinde farklı eşik değerleri için 100 düğümde gecikme miktarının kıyaslanması

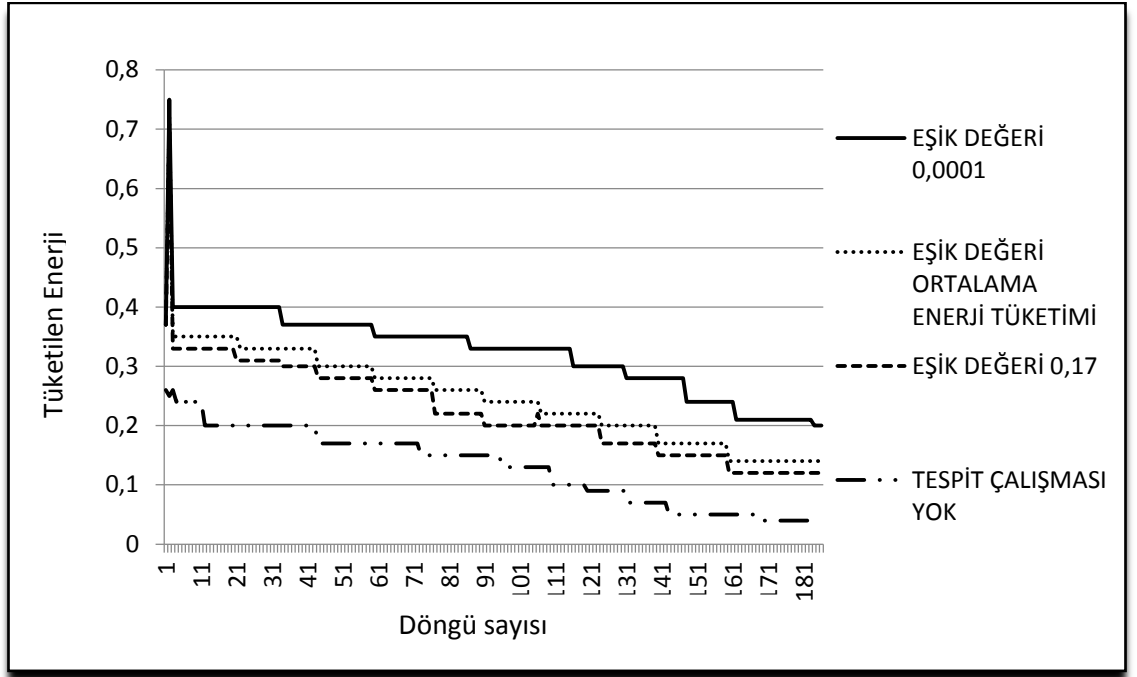
Tekil saldırı modelinde, sürekli saldırı modelinden farklı olarak, eşik değerinin büyük seçilmesi sistemdeki enerji tüketimi ve gecikme bakımından daha iyi sonuç vermektedir.



Şekil 4.21. Tekil saldırı modelinde farklı eşik değerleri için 100 düğümde yakalanan paket miktarının kıyaslanması

Şekil 4.21.'de 100 düğüm için sisteme yakalanan paket miktarının tekil saldırı modelinde farklı eşik değerleri üzerinden kıyaslanması görülmektedir. Tespit çalışması

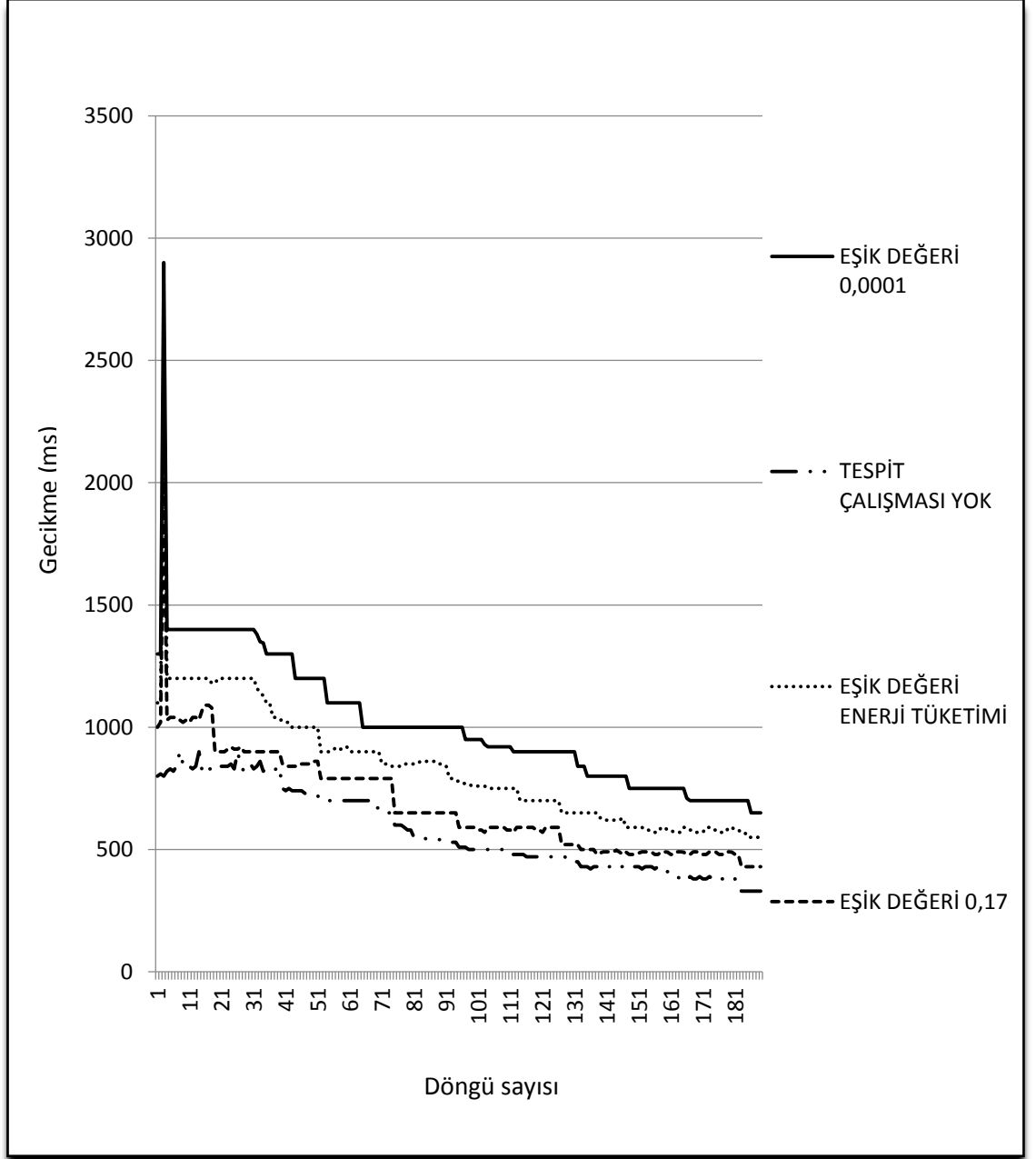
yapılmadığı durumda, farklı eşik değerlerine göre tespit çalışması yapıldığı durumlara göre daha az paket yakalanmıştır. Bunun nedeni tespit edilemeyen kötü niyetli düğümlerin sisteme zarar vermeye devam etmesidir. Eşik değerinin 0,0001 seçildiği durumda diğer eşik değerlerine göre daha az paket yakalanmıştır. Bunun nedeni daha çok enerji harcayan düğümlerin bataryalarının daha erken bitmesi ve paketlerini baz istasyonuna ulaştıramamasıdır. Eşik değerinin 0,0001 seçildiği durumda diğer eşik değerlerine göre ortalama %20 daha az paket yakalanmıştır.



Şekil 4.22. Tekil saldırı modelinde farklı eşik değerleri için 150 düğümde tüketilen toplam enerji miktarının kıyaslanması

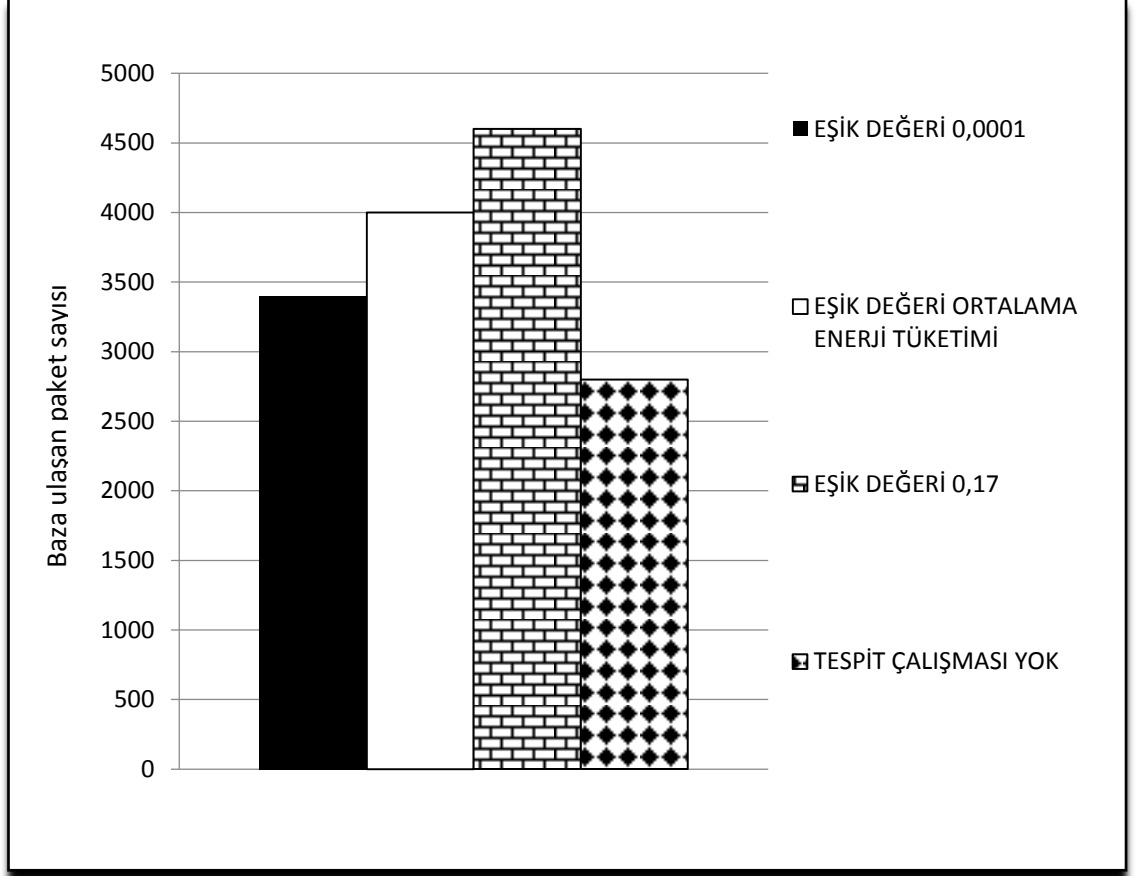
Şekil 4.22.'de 150 düğüm için her döngüdeki tüketilen toplam enerji miktarının tekil saldırı modelinde farklı eşik değerleri üzerinden kıyaslanması görülmektedir. Sistemde tespit çalışması yapılmadığı durumda, farklı eşik değerlerinde tespit çalışması yapıldığı duruma göre daha az enerji harcandığı görülmektedir. Bunun nedeni sürekli saldırı modelinde olduğu gibi, sistemin kötü niyetli düğümü tespit etmek için ekstra enerji harcamasıdır. Eşik değeri 0,0001 seçildiği durumda tespit çalışması yapılmadığı duruma göre %60 daha fazla enerji, eşik değeri bir önceki döngüde tüketilen ortalama enerji miktarı seçildiği durumda tespit çalışması yapılmadığı duruma göre %49 daha fazla enerji, eşik değeri 0,17 seçildiği durumda tespit çalışması yapılmadığı duruma göre %33 daha fazla enerji harcanmıştır. Sistemde enerji tüketimi en fazla eşik

değerinin 0,0001 seçildiği durumda meydana gelmiştir. Bunun nedeni baz istasyonunun bataryası az olduğu için paket yollayamayan üye düğümleri şüpheli olarak algılayıp, sorgu mesajı yollamasındandır. Sistemde sorgu mesajının fazla olması ekstra gecikmeye neden olmuştur (Şekil 4.23.).



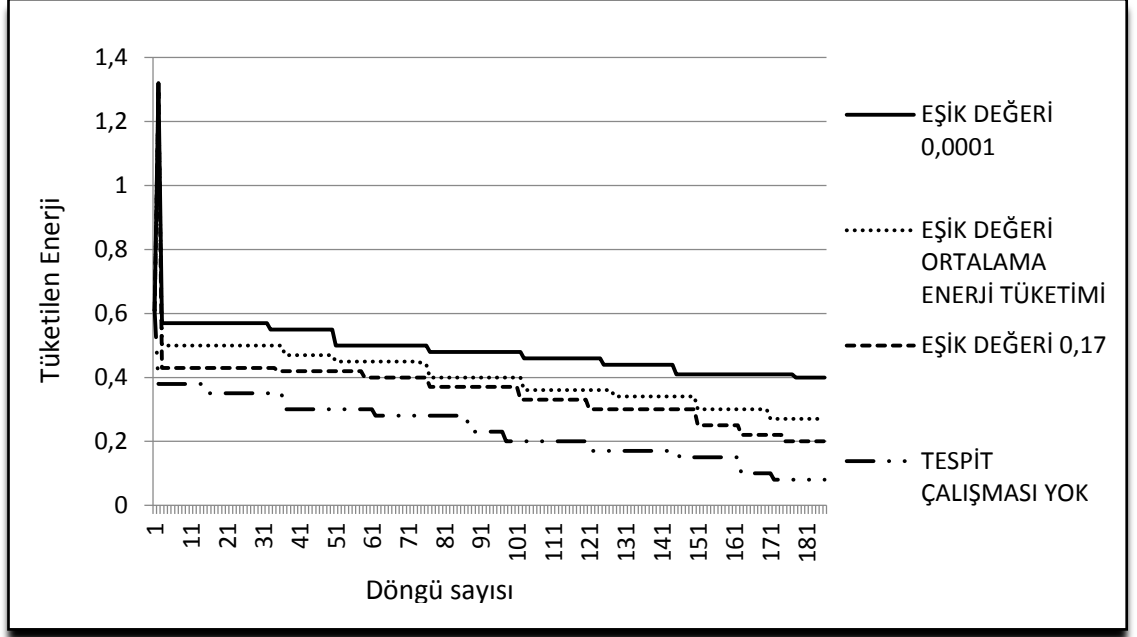
Şekil 4.23. Tekil saldırı modelinde farklı eşik değerleri için 150 düğümde gecikme miktarının kıyaslanması

Tekil saldırı modelinde, sürekli saldırı modelinden farklı olarak, eşik değerinin büyük seçilmesi sistemdeki enerji tüketimi ve gecikme bakımından daha iyi sonuç vermektedir.



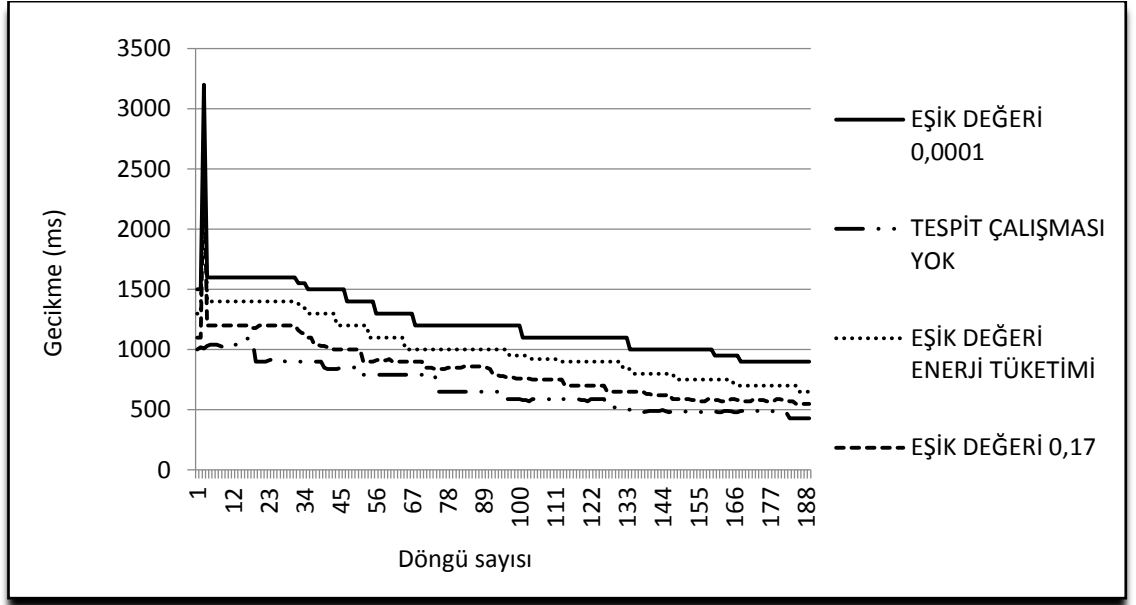
Şekil 4.24. Tekil saldırı modelinde farklı eşik değerleri için 150 düğümde yakalanan paket miktarının kıyaslanması

Şekil 4.24.'te 150 düğüm için sisteme yakalanan paket miktarının tekil saldırı modelinde farklı eşik değerleri üzerinden kıyaslanması görülmektedir. Tespit çalışması yapılmadığı durumda, farklı eşik değerlerine göre tespit çalışması yapıldığı durumlara göre daha az paket yakalanmıştır. Bunun nedeni tespit edilemeyen kötü niyetli düğümlerin sisteme zarar vermeye devam etmesidir. Eşik değerinin 0,0001 seçildiği durumda diğer eşik değerlerine göre daha az paket yakalanmıştır. Bunun nedeni daha çok enerji harcayan düğümlerin bataryalarının daha erken bitmesi ve paketlerini baz istasyonuna ulaştırılamamasıdır. Eşik değerinin 0,0001 seçildiği durumda diğer eşik değerlerine göre ortalama %18 daha az paket yakalanmıştır.



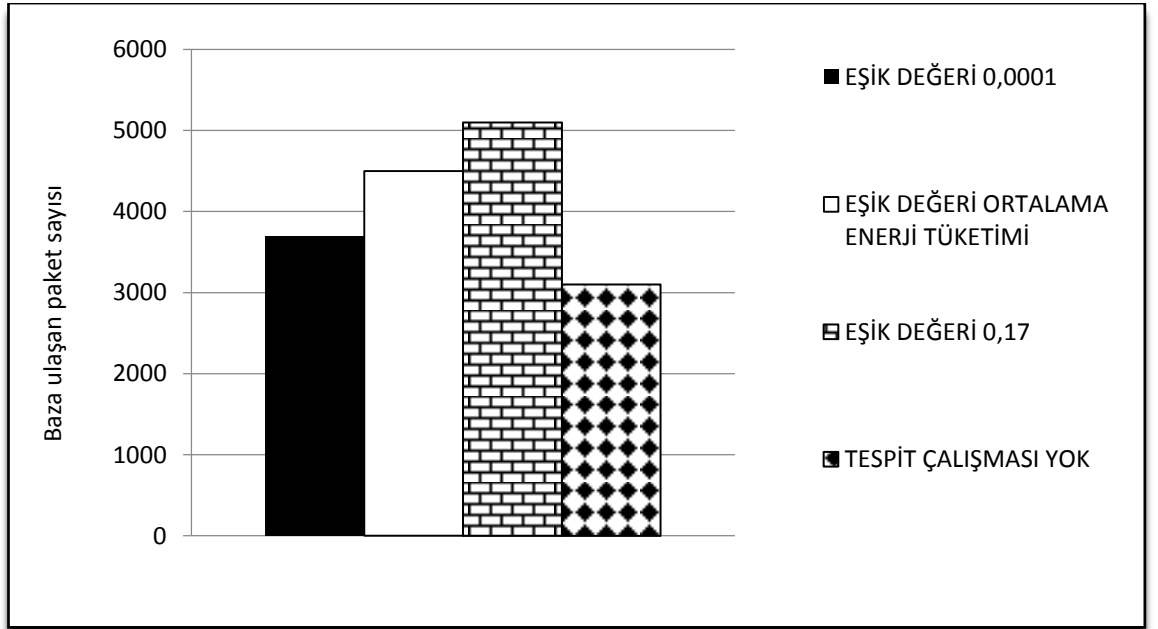
Şekil 4.25. Tekil saldırı modelinde farklı eşik değerleri için 200 düğümde tüketilen toplam enerji miktarının kıyaslanması

Şekil 4.25.'te 200 düğüm için her döngüdeki tüketilen toplam enerji miktarının tekil saldırı modelinde farklı eşik değerleri üzerinden kıyaslanması görülmektedir. Sistemde tespit çalışması yapılmadığı durumda, farklı eşik değerlerinde tespit çalışması yapıldığı duruma göre daha az enerji harcandığı görülmektedir. Bunun nedeni sürekli saldırı modelinde olduğu gibi, sistemin kötü niyetli düğümü tespit etmek için ekstra enerji harcamasıdır. Eşik değeri 0,0001 seçildiği durumda tespit çalışması yapılmadığı duruma göre %61 daha fazla enerji, eşik değeri bir önceki döngüde tüketilen ortalama enerji miktarı seçildiği durumda tespit çalışması yapılmadığı duruma göre %51 daha fazla enerji, eşik değeri 0,17 seçildiği durumda tespit çalışması yapılmadığı duruma göre %35 daha fazla enerji harcanmıştır. Sistemde enerji tüketimi en fazla eşik değerinin 0,0001 seçildiği durumda meydana gelmiştir. Bunun nedeni baz istasyonunun bataryası az olduğu için paket yollayamayan üye düğümleri şüpheli olarak algılayıp, sorgu mesajı yollamasındandır. Sistemde sorgu mesajının fazla olması ekstra gecikmeye neden olmuştur (Şekil 4.26.).



Şekil 4.26. Tekil saldırı modelinde farklı eşik değerleri için 200 düğümde gecikme miktarının kıyaslanması

Tekil saldırı modelinde, sürekli saldırı modelinden farklı olarak, eşik değerinin büyük seçilmesi sistemdeki enerji tüketimi ve gecikme bakımından daha iyi sonuç vermektedir.



Şekil 4.27. Tekil saldırı modelinde farklı eşik değerleri için 200 düğümde yakalanan paket miktarının kıyaslanması

Şekil 4.27.'de 200 düğüm için sisteme yakalanan paket miktarının tekil saldırı modelinde farklı eşik değerleri üzerinden kıyaslanması görülmektedir. Tespit çalışması yapılmadığı durumda, farklı eşik değerlerine göre tespit çalışması yapıldığı durumlara göre daha az paket yakalanmıştır. Bunun nedeni tespit edilemeyen kötü niyetli düğümlerin sisteme zarar vermeye devam etmesidir. Eşik değerinin 0,0001 seçildiği durumda diğer eşik değerlerine göre daha az paket yakalanmıştır. Bunun nedeni daha çok enerji harcayan düğümlerin bataryalarının daha erken bitmesi ve paketlerini baz istasyonuna ulaştıramamasıdır. Eşik değerinin 0,0001 seçildiği durumda diğer eşik değerlerine göre ortalama %17 daha az paket yakalanmıştır.

5. SONUÇLAR VE ÖNERİLER

KAA' lar sınırlı kaynaklara sahiptir ve çok zor şartlar altında dahi konumlandırılabilirler. Bu nedenle KAA' lar hem çevreden hem de içerden gelebilecek saldırılara açıktır. Algılayıcı ağ saldırıları iç saldırılar ve dış saldırılar olmak üzere ikiye ayrılırlar. Dış saldırılarda saldırgan, gizli anahtar bilgisine sahip olmadan kendi algılayıcı düğümleri ile hedefindeki algılayıcı ağın işlevini bozacak şekilde saldırılar düzenler. Dış saldırılar, anahtarlama, şifreleme, kimlik doğrulama gibi yöntemlerle tespit edilebilir. İç saldırılarda ise saldırgan, algılayıcı düğümleri ve gizli anahtarı ele geçirerek içten saldırır. İç saldırıların ağa verdiği zarar çok büyük olmakla birlikte bu saldırıların kimlik doğrulama ve yetkilendirme gibi geleneksel yöntemlerle tespiti çok zordur. Bu nedenle iç saldırıların tespit edilmesi için farklı güvenlik önlemlerinin alınması gereklidir. İç saldırıların en tehlikeli olanlarından birisi de sinkhole saldırılarıdır.

Bu çalışmada sinkhole saldırıları önce modellenmiş, daha sonra modellenen saldırı üzerinden tespit çalışması yapılmıştır. Sinkhole saldırıları üç farklı şekilde modellenmiştir. İlk modelde ağdaki toplam düğüm sayısının %10 u kadar kötü niyetli düğüm ağa yerleştirilmiş ve bu kötü niyetli düğümlerin verilerini iletmeyerek ağa verdikleri zarar incelenmiştir. İkinci modelde kötü niyetli düğüm belirli bir kapsama alanı içinde yer alan düğümleri etkilemeye çalışmıştır. Üçüncü modelde ise ağda rastgele bir düğümün kötü niyetli olarak etiketlendiği varsayılmıştır. Bu üç modelin ağar verdiği zararlar çeşitli parametreler üzerinden değerlendirilmiştir. Literatürde Model2 ve Model3 üzerinden tespit yapan birçok çalışma bulunduğu için bu çalışmada Model1 üzerinden tespit çalışması yapılmıştır. Model1 üzerinden tekil saldırı ve sürekli saldırı olmak üzere iki farklı tasarım yapılmıştır. Tekil saldırı tasarımında kötü niyetli düğümler ikinci döngüde sisteme dahil edilmiş ve bu düğümlerin tespiti yapıldıktan sonra tekrar sisteme eklenmemiştir. Sürekli saldırı tasarımında ise kötü niyetli düğümler 10 döngüde bir sisteme dahil edilmiştir. Buda, kötü niyetli düğümlerin yakalansalar dahi 10 döngüde bir tekrar sistemde görülmeleri anlamına gelmektedir. Tespit çalışması farklı kalan enerji eşik değerleri kullanılarak yapılmış ve sistem için hangi eşik değerinin en uygun olduğu bulunmaya çalışılmıştır. Aynı zamanda farklı düğüm sayıları üzerinden test çalışmaları yapılarak düğüm sayısının tespit sistemi üzerindeki etkisi bulunmaya çalışılmıştır. Tespit çalışması yapılırken sistemde tüketilen toplam enerji

miktarı, sistemdeki toplam gecikme miktarı ve sistemde yakalanan paketler ile sisteme dahil edilen kötü niyetli düğümünün kaç tanesinin yakalandığı farklı eşik değerleri üzerinden kıyaslanmıştır. Hangi eşik değerinin optimum sonuç verdiği bulunmaya çalışılmıştır. Tekil saldırı tasarımı yüksek eşik değeri daha iyi sonuç verirken sürekli saldırı modelinde ortalama eşik değeri daha iyi sonuç vermiştir. Düğüm sayısı arttıkça sistemde tüketilen toplam enerji miktarı artış gösterirken, kötü niyetli düğüm yakalama oranı düşüş göstermiştir.

KAYNAKLAR

- Anonim, 2015. Cells. <http://www.omnetpp.com/intro>. Erişim tarihi: 12.08.2015
- Bahekmatt, M., Yaghmaee, M. H., Yazdi, A. S. H. and Sadeghi, S. 2012. A Novel Algorithm for Detecting Sinkhole Attacks in WSNs. **International Journal of Computer Theory and Engineering**, 4(3), 418-421.
- Ceyhan, E. B. ve Sağıroğlu, Ş. 2013. Kablosuz Algılayıcı Ağlarda Güvenlik Sorunları ve Alınabilecek Önlemler. **Gazi Üniversitesi Politeknik Dergisi**, 16(4).
- Chaudhry, J. A., Tariq, U., Amin, M. A. and Rittenhouse, R. G. 2013. Dealing with Sinkhole Attacks in Wireless Sensor Networks. **Advanced Science and Technology Letters**, 29, 7-12.
- Chen, C., Song, M. and Hsieh, G. 2010. Intrusion detection of sinkhole attacks in large-scale wireless sensor networks. **In Wireless Communications, Networking and Information Security (WCNIS)**, (pp. 711-716).
- Coppolino, L., D' Antonio, S., Romano, L. and Spagnuolo, G. 2010. An intrusion detection system for critical information infrastructures using wireless sensor network technologies. **In Critical Infrastructure (CRIS), International Conference on** (pp. 1-8).
- Gondwal, N. and Diwaker, C. 2013. Detecting Blackhole Attack In Wsn By Check Agent Using Multiple Base Stations. **AIJRSTEM**, 3(2), 149-152.
- Han, G., Li, X., Jiang, J., Shu, L. and Lloret, J. 2014. Intrusion Detection Algorithm Based on Neighbor Information Against Sinkhole Attack in Wireless Sensor Networks. **The Computer Journal**, bxu036.
- Heinzelman, W. R., Chandrakasan, A. and Balakrishnan, H. 2000. Energy-efficient communication protocol for wireless microsensor networks. **In System sciences. Proceedings of the 33rd annual Hawaii international conference on** (pp. 10-pp).
- Kalaycı, T. E. 2009. Kablosuz Sensör Ağlar ve Uygulamaları. **Akademik Bilişim**.
- Karasulu, B., Toker, L. and Korukoğlu, S. 2009. ZigBee-IEEE 802.15. 4 standardı temelli kablosuz algılayıcı ağları. **XIV. Türkiye' de İnternet Konferansı-Inet-tr**.
- Meghdadi, M., Özdemir, S. and Güler, I. 2008. Kablosuz Algılayıcı Ağlarında Güvenlik: Sorunlar ve Çözümler. **International Journal of InformaticsTechnologies**, 1(1).
- Ngai, E. C., Liu, J. and Lyu, M. R. 2007. An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. **Computer Communications**, 30(11), 2353-2364.
- Ökdem, S., and Derviş, K. 2007. Kablosuz Algılayıcı Ağlarında Yönlendirme Teknikleri. **Akademik Bilişim**.
- Padmavathi, D. G. and Shanmugapriya, M. 2009. A survey of attacks, security mechanisms and challenges in wireless sensor networks. **arXiv preprint arXiv:0909.0576**.
- Papadimitriou, A., Le Fessant, F., Viana, A. C. and Sengul, C. 2009. Cryptographic protocols to fight sinkhole attacks on tree-based routing in wireless sensor networks. **In Secure Network Protocols, 2009. NPSec 2009. 5th IEEE Workshop on** (pp. 43-48).

- Patil, S. S. and Khanagoudar, P. S. 2012. Intrusion Detection Based Security Solution for Cluster Based WSN. **International Journal of Advanced Research in Computer Engineering and Technology (IJARCET)**, 1(4), pp-331.
- Radhikabaskar, D. P., Komara, S. and Paul, V. 2014 Sinkhole Attack Detection In Hierarchical Sensor Networks. **International Journal of Scientific and Engineering Research**, Volume 5, Issue 9,
- Rajkumar, D. U. S. and Vayanaperumal, R. 2013. A Leader Based Monitoring Approach For Sinkhole Attack in Wireless Sensor Network. **Journal of Computer Science**, 9(9), 1106.
- Razzaque, M. A., Salehi, A. and Cheraghi, S. M. 2013. Security and privacy in vehicular Ad-Hoc networks: survey and the road ahead. **In Wireless Networks and Security** (pp. 107-132). Springer Berlin Heidelberg.
- Sahraoui, S. and Bouam, S. 2013. Secure routing optimization in hierarchical cluster-based wireless sensor networks. **International Journal of Communication Networks and Information Security (IJCNIS)**, 5(3).
- Sedjelmaci, H., Senouci, S. M. and Feham, M. 2012. Intrusion detection framework of cluster-based wireless sensor network. **In Computers and Communications (ISCC), 2012 IEEE Symposium on** (pp. 000857-000861).
- Sharmila, S. and Umamaheswari, G. 2011. Detection of sinkhole attack in wireless sensor networks using message digest algorithms. **In Process Automation, Control and Computing (PACC), International Conference on**(pp. 1-6).
- Sheela.D, Srividhya.V.R, Asma Begam, Anjali ve Chidanand G.M. 2012. Detecting Blackhole Attacks in Wireless Sensor Networks using Mobil Agent. **International Conference on Artificial Intelligence and Embedded Systems** Singapore
- Singh, S. K., Singh, M. P. and Singh, D. K. 2011. A survey on network security and attack defense mechanism for wireless sensor networks. **Int. J. Comput.Trends Tech**, 5-6.
- Singh, S. K., Singh, M. P., and Singh, D. K. 2011. Intrusion detection based security solution for cluster-based wireless sensor networks. **International Journal of Advanced Science and Technology**, 30(83).
- Xing, K., Srinivasan, S. S. R., Jose, M., Li, J. and Cheng, X. 2010. Attacks and countermeasures in sensor networks: a survey. **In Network security** (pp. 251-272). Springer US

ÖZGEÇMİŞ

Yazar 1989 yılında Osmaniye’de doğdu. İlköğretimini Cebeli Bereket İlköğretim okulunda tamamladı. Lise eğitimi için Atatürk Lisesine gitti. 2011 yılında Fırat Üniversitesi Bilgisayar Mühendisliği bölümünde üniversite eğitimi tamamladı. 2013 yılından bu yana Mustafa Kemal Üniversitesinde Enformatik Bölümünde Yüksek Lisans çalışmasını yapmakta ve araştırma görevlisi olarak çalışmaktadır. Yazarın çalışma alanları ağlar ve kablosuz algılayıcı ağları konularıdır.