Cansu CANBOLAT

İSKENDERUN TEKNİK
ÜNİVERSİTESİ
MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ

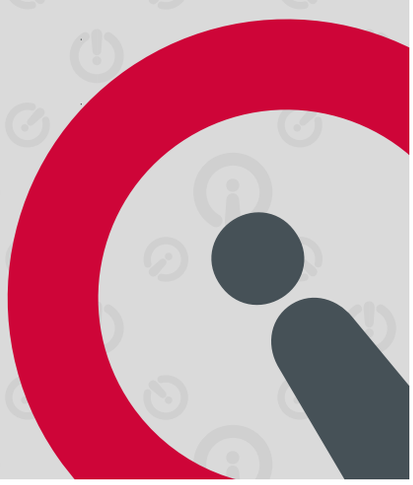
YÜKSEK LİSANS TEZİ

KÜME TABANLI KABLOSUZ ALGILAYICI AĞLARDA GÜVEN TABANLI YÖNLENDİRME PROTOKOLÜ TASARIMI

Cansu CANBOLAT

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

OCAK 2020



BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

OCAK 2020

KÜME TABANLI KABLOSUZ ALGILAYICI AĞLARDA GÜVEN TABANLI YÖNLENDİRME PROTOKOLÜ TASARIMI

Cansu CANBOLAT

YÜKSEK LİSANS

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

İSKENDERUN TEKNİK ÜNİVERSİTESİ

MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ

OCAK 2020

CANSU CANBOLAT tarafından hazırlanan" KÜME TABANLI KABLOSUZ ALGILAYICI AĞLARDA GÜVEN TABANLI YÖNLENDİRME PROTOKOLÜ TASARIMI" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ / OY ÇOKLUĞU ile İskenderun Teknik Üniversitesi Bilgisayar Mühendisliği Anabilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Dr. Öğr. Üyesi İpek ABASIKELEŞ TURGUT .....

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum.

Başkan: Dr. Öğr. Üyesi Ahmet AYDIN .....

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum.

Üye: Dr. Öğr. Üyesi Ahmet GÖKÇEN .....

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum.

Tez Savunma Tarihi 10/01/2020

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

.....

Prof. Dr. Tolga DEPCİ

Mühendislik ve Fen Bilimleri Enstitüsü Müdürü

ETİK BEYAN

İskenderun Teknik Üniversitesi Mühendislik ve Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- ☑ Tez üzerinde Yükseköğretim Kurulu tarafından hiçbir değişiklik yapılamayacağı için tezin bilgisayar ekranında görüntülendiğinde asıl nüsha ile aynı olması sorumluluğunun tarafıma ait olduğunu,
- ☑ Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- ☑ Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- ☑ Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- ☑ Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- ☑ Bu tezde sunduğum çalışmanın özgün olduğunu, bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

İmza

Cansu CANBOLAT

10./01./2020

KÜME TABANLI KABLOSUZ ALGILAYICI AĞLARDA GÜVEN TABANLI YÖNLENDİRME PROTOKOLÜ TASARIMI

(Yüksek Lisans Tezi)

Cansu CANBOLAT

İSKENDERUN TEKNİK ÜNİVERSİTESİ
MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ

Ocak 2020

ÖZET

Bir Kablosuz Algılayıcı Ağ (KAA), fiziksel dünyadan algıladığı verinin uygulama doğrultusunda talep edilen lokasyona kablosuz ortam aracılığı ile aktarılmasını sağlayan binlerce algılayıcı düğümden oluşmaktadır. Algılayıcıların düşük maliyet, küçük boyut ve kolay yerleşim avantajlarının yanında sınırlı enerji, kısıtlı iletişim kapasitesi ve değiştirilemeyen batarya sorunu gibi birçok dezavantajı da bulunmaktadır. Tehlikeli iç saldırılar grubuna dahil olan yönlendirme saldırıları, ağ sistemini bloke ederek, veri iletimine büyük ölçüde zarar vermektedir. Güven tabanlı sistemlerde amaç, saldırı tespit sistemlerdeki gibi saldırıyı yakalamak değil, paket için güvenilir bir yol oluşturularak, hedef düğüme başarıyla ulaşmasını sağlamaktır. Bu tezde, kümeleme tabanlı bir KAA için tutarlılık faktörü, paket iletim oranı ve bencillik parametrelerinden oluşan güven değerine ve kalan enerji seviyesine bağlı olarak küme başı seçim yöntemi ve güvenli yönlendirme protokolü olan GüYöM önerilmiştir. Simülasyon yöntemi ile yapılan değerlendirmelerde, GüYöM, LEACH ve TLES yönlendirme protokolleri, ağ alanı, düğüm sayısı, saldırgan oranı gibi KAA'ların çeşitli ağ parametrelerinin farklı değerleri için kıyaslanmıştır. Performans kriterleri olarak da paket kayıp oranları, yaşayan düğüm sayısı ve düğümler tarafından harcanan enerji kullanılmıştır. Her iki saldırı modeli için de GüYöM'ün, LEACH ve TLES protokollerine kıyasla daha uzun ağ yaşam süresi, daha az harcanan enerji ve paket kayıp oranlarını ise azalttığı tespit edilmiştir.

Anahtar Kelimeler : Kablosuz Algılayıcı Ağ, Güven Tabanlı Yönlendirme, Küme Başı
Sayfa Adedi : 69
Danışman : Dr. Öğr. Üyesi İpek ABASIKELEŞ TURGUT

TRUST-BASED ROUTING PROTOCOL DESIGN IN WIRELESS BASED WIRELESS SENSOR NETWORKS

(M. Sc. Thesis)

Cansu CANBOLAT

ISKENDERUN TECHNICAL UNIVERSITY
ENGINEERING AND SCIENCE INSTITUTE

January 2020

ABSTRACT

A Wireless Sensor Network (WSN) is composed of thousands of sensor nodes that enable the transmission of perceived data from the physical world to the requested location via wireless media. Besides the advantages of low cost, small size and easy deployment of the sensor nodes, there are many disadvantages such as limited energy, limited communication capacity and non-replaceable battery problem. In trust-based systems, the goal is not to capture the attack as in intrusion detection systems, but to create a reliable path for the package to ensure that it reaches the target node successfully. In this thesis, a cluster selection method and a secure routing protocol, GüYöM, is proposed for a cluster-based WSN based on the trust value consisting of consistency factor, packet transmission rate and selfishness parameters and the remaining energy level. In the evaluations made by simulation method, GüYöM, LEACH and TLES routing protocols are compared for different values of various network parameters such as the network area, the number of the nodes, and the attacker rate. As performance criteria, packet loss rates, the number of living nodes and energy consumed by the nodes are used. For both attack models, GüYöM has been found to provide longer network life, less consumed energy and reduced packet loss rates compared to LEACH and TLES protocols.

Key Words : Wireless Sensor Networks, Trust-based Routing, Cluster Head
Page Number : 69
Supervisor : Assist. Prof. Dr. İpek ABASIKELEŞ TURGUT

TEŞEKKÜR

Yüksek Lisans tez konusunun belirlenmesinde, araştırılması ve yazımı sırasında sahip olduğu bilgi birikimi ve tecrübesi ile çalışmayı yönlendiren ve her türlü yardımı esirgemeyen saygı değer danışman hocam Dr. Öğr. Üyesi İpek ABASIKELEŞ TURGUT' a ve bu süreçte her konuda yanımda olan aileme ve arkadaşlarıma sonsuz saygı ve teşekkürlerimi sunarım.

İÇİNDEKİLER

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	**Açıklamalar**
j/J	Joule

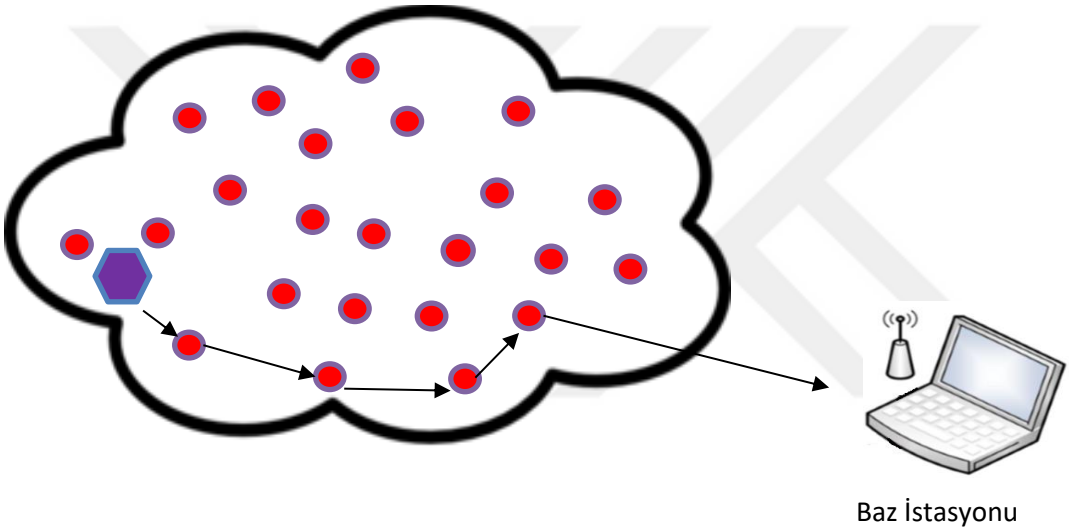
1. GİRİŞ

Bir Kablosuz Algılayıcı Ağ (KAA), fiziksel dünya ile iletişimde bulunmak amacıyla ortama yerleştirilmiş olan çok sayıda boyutu küçük, kapasiteli kısıtlı, kısa mesafede iletişim kurabilen, düşük güç tüketimine sahip ve maliyet efektif algılayıcı düğümden oluşmaktadır. (Rawat, Singh, Chaouchi ve Bonnin, 2014). Günümüzde KAA'lar, önemli bir IoT (Internet of Things, Nesnelerin Interneti) altyapısı olarak birçok farklı alanda tercih edilmektedirler. Bu alanlara örnek olarak sağlık sektöründeki uygulamalar, endüstriyel sistemler, askeri izleme sistemleri, doğa takip sistemleri ve hatta spor müsabakaları verilebilir. Bazı KAA uygulamalarında algılayıcı düğümler üzerlerine yerleştirildikleri yapıların, insanların ve rotaların bilgilerini toplayarak; bu bilgileri gerekli bölgelere, aygıtlara veya kişilere güvenli bir şekilde iletmektedirler (Perrig, Szewczyk, Tygar, Wen ve Culler, 2002).

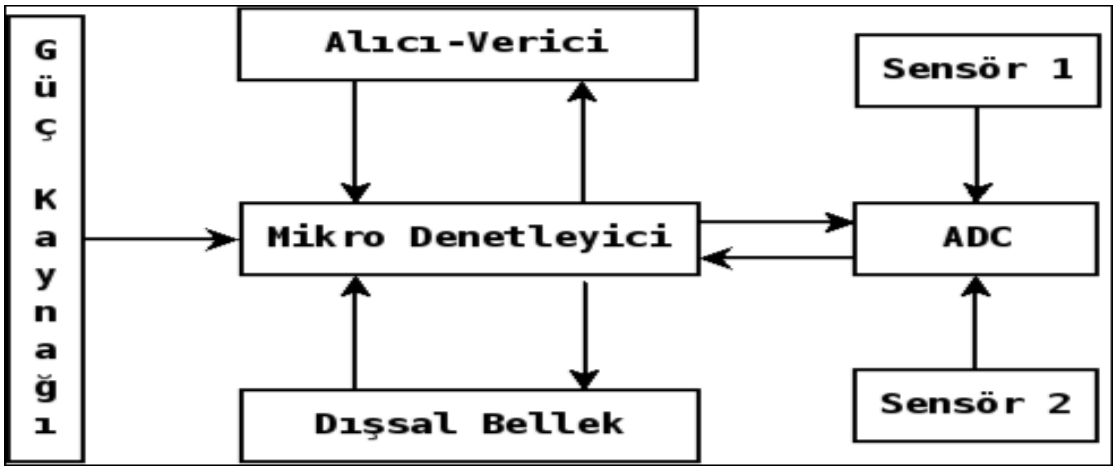
Bir KAA sisteminde (Şekil 1.1.) birbirleri ile haberleşebilen birden fazla algılayıcı düğüm ve elde edilen veri üzerinde gerekli işlemlerin yapılmasını sağlayan ve merkezi bir yönetim aygıtı olan baz istasyonu bulunur. Bir algılayıcı düğümün yapısında (Şekil 1.2.) işlem gücü kısıtlı bir mikro denetleyici, kısa mesafeli bir alıcı verici, sınırlı kapasiteli bir bellek, kısıtlı bir batarya ve amaca yönelik olarak bir veya daha fazla sayıda algılayıcı yer alır (Kalaycı, 2009). KAA' lar sistem üzerinde hareketli olabilseler de çoğu uygulamada genellikle durağandırlar. Algılayıcı düğümler, yerleştirildikleri ortamı algılama, elde ettikleri verileri uygun bir şekilde işleme ve bu veriyi baz istasyonuna gönderilmesi amacıyla diğer düğümlere iletme işlerini yaparlar (Ceyhan ve Sağıroğlu,2013). Algılayıcı düğümler, ağ alanına yerleştirildikten sonra çevreyi gözetlemeye başlamaktadırlar. Ağ sisteminde bir olay olduğu zaman, algılayıcı düğümler bu olayı tespit ederek, bir rapor oluşturur ve bu raporu baz istasyonuna iletirler. Gerçekleşen olayı birden fazla algılayıcı düğüm tespit ederse, algılayıcı düğümler arasında önce iş birliği yapılmakta; daha sonra baz istasyonuna rapor gönderilmektedir. Baz istasyonu ağ sistemi ile fiziksel dünya arasında bir köprü görevi üstlenmektedir.

Her ne kadar KAA'ların avantajları birçok kritik uygulamalarda geniş kullanım alanı imkânı doğursa da bu ağların genellikle korunmasız ortamlarda konumlandırılması, saldırganların ilgisini çekmektedir. Algılayıcı düğümlerin küçük boyutlarda olması, düşük maliyete sahip olması ve az güç tüketmesi gibi avantajlarının yanında; güvenlik, kısıtlı enerjinin verimli bir şekilde kullanılması, düğümlerin lokalizasyonu vb. birçok problemin çözülmesi gerekmektedir. (Sharma, R. Bansal, S. Bansal 2013). Özellikle kritik görevler için öngörülen

bir KAA ' ın boyutu arttıkça, güvenlik en önemli konulardan biri haline gelir (Z. Chen, He, Liang, K. Chen, 2015). Askeri bir uygulamadaki güvenlik açığı düşmanların elini güçlendirecek ve bölgesel çatışma veya savaşın kaybedilmesine neden olabilecektir. Benzer şekilde, gizli bir hasta sağlığı kaydı, bir sağlık bakımı uygulamasında yetkisiz kullanımlardan korunmalıdır (Butun, Morgera ve Sankar, 2014). Bununla birlikte KAA'ların işlemci ve radyo kapasitelerinin düşük olması geleneksel güvenlik protokollerinin bu ağlarda uygulanmasına olanak tanımaz. Bu nedenle güvenlik alanında KAA'lara özel kapsamlı çalışmalar yapılması gerekmektedir (Jan, 2016). KAA'ların ihtiyaç çeşidine, kullanım alanına göre tasarlanarak kurulum yapılması, KAA sisteminin başarımı açısından büyük önem taşımaktadır.



Şekil 1.1. KAA yapısı



Şekil 1.2. Bir algılayıcı düğümün yapısı

KAA'lara yapılan saldırılar iç ve dış saldırılar olmak üzere iki temel grupta toplanabilir. Dış saldırıların tespiti için kriptolojik çözümler ve yetkilendirme protokolleri başarılı sonuçlar vermektedir. İç saldırılarda ise saldırgan, algılayıcı düğümleri ele geçirerek ağ sistemine içeriden saldırı yapmaktadırlar. Saldırgan tarafından ele geçirilen düğümler, bilgilerin yetkisiz kişilere aktarılmasına neden olarak tüm ağ sistemini tehlikeye atabilir. Bu nedenle iç saldırıların tespit edilmesi ve ağın bu saldırılardan kurtarılması sistemin güvenliği açısından oldukça önem arz etmektedir (Gondwal,ve Diwaker, 2013). Dışarıdan gelen saldırılara karşı etkili bir yöntem olarak kullanılan kimlik doğrulama ve yetkilendirme gibi geleneksel kriptolojik yöntemlerin iç saldırılar üzerinde etkili olmaması, iç saldırılara özel olarak farklı güvenlik önlemlerinin alınması gerekliliğini doğurur (Sheele, Srividhya, Asma ve Chidanand, 2012).

KAA'larda ağ katmanının işleyişini durdurmayı veya aksatmayı hedef alan en tehlikeli iç saldırı gruplarından birisi de yönlendirme protokolüne yapılan saldırılarıdır. Bu saldırılara; sinkhole (Obruk), blackhole (kara delik), gray hole (gri delik), selective forwarding (seçici yönlendirme) ve wormhole (solucan deliği) örnek olarak verilebilir. Bu saldırı gruplarında saldırgan düğüm tarafından ele geçirilen algılayıcı düğümler, bilginin ağın dışındaki yetkisiz şahıslara aktarılmasına, hedefe hiç aktarılmamasına veya eksik aktarılmasına neden olarak tüm ağ sistemini tehlikeye atabilir (Sedjelmaci, Senouci ve Feham, 2012). Bu saldırıların tespit edilmesi ve önlenebilmesi için atakların davranışlarının doğru bir şekilde analiz edilmesi gerekmektedir. Literatürde yönlendirme saldırıları üzerine yapılan çalışmalar, temelde iki grupta toplanır. Bunlardan ilki izinsiz giriş tespit sistemleri (intrusion detection systems- IDS), diğeri ise güvene dayalı sistemler (trust based systems – TBS) olarak adlandırılır. Bir IDS, periyodik olarak ağın veya belirli bir hedef düğüm grubunun davranışını izleyerek, analiz eder. Şüpheli bir faaliyet yakaladığında ise ağı uyarmak amacıyla bir alarm tetikler (Sedjelmaci ve diğerleri, 2012). Alarm tetikleme sürecinin ardından sistemin saldırıdan temizlenmesi amacıyla izinsiz giriş yanıtlama sistemi (intrusion response systems- IRS) devreye girer ve IRS, gerekli eylem planlarını uygulayarak sistemin kontrolünün yeniden ele alınmasını sağlar. Bununla birlikte TBS'de amaç, saldırıyı veya saldırganı yakalamak değil; kaynak düğümden hedef düğüme verinin iletilmesi amacıyla ağda güvenli bir rota kurmaktır. Böylece sistem, saldırının tespit edilmesi veya uzaklaştırılması için gerekli olan yükten arındırılmış olur. Bu da kaynakları kısıtlı olan KAA'lar için TBS'nin enerji verimli bir çözüm olmasını sağlar.

Bu tezde, kümeleme tabanlı hiyerarşik mimariye sahip KAA'larda, TBS protokolü tasarlanmıştır. Kümeleme mimarisinde küme içindeki algılayıcı düğümlerden gelen verinin toplanarak işlenmesini ve baz istasyonuna iletilmesini sağlayan düğüme küme başı adı verilir. Algılayıcı düğüm ve baz istasyonu arasında kurulacak olan güvenli rotada, saldırgan tarafından ele geçirilmemiş küme başlarının seçilmesi, verini başarılı bir şekilde hedefe iletilmesini sağlayacaktır. Bu nedenle bu tezde küme başı seçiminde düğümün tutarlılık faktörü, paket iletim oranı ve bencillik olmak üzere üç farklı güven parametresine bağlı olarak küme başı seçimi sağlanır. KAA'ların kaynak kısıtları göz önüne alındığında küme başlarının fazla enerji harcayarak daha erken ölmesini engellemek amacıyla ağda küme başı seçiminde güven ile birlikte enerji parametresi de hesaba katılır. Buna bağlı olarak ağda hem güven değeri yüksek hem de enerjisi yüksek düğümlerin küme başı olarak seçilmesi sağlanarak ağda verinin hem başarılı bir şekilde hedefe ulaştırılması hem de bunun enerji verimli bir şekilde yapılması sağlanır. Önerilen yönlendirme mimarisi, literatürde kümeleme mimarisinin temeli olarak kabul edilen LEACH (Heinzelman, Chadrakasan ve Balakrishnan) protokolü ve kümeleme tabanlı ağlarda güven tabanlı CH seçimini öneren TLES (Z. Chen ve diğerleri, 2014) protokolü ile ağdaki ortalama paket kayıp oranı, ağda harcanan toplam enerji ve ağ yaşam süresi parametreleri üzerinden simülasyon yöntemi kullanılarak kıyaslanmıştır.

Bölüm 2'de literatürde konuyla ilgili yapılan çalışmalar incelenmiş; Bölüm 3'te küme tabanlı KAA sistemi detaylandırılmıştır. Bölüm 4'te önerilen güven tabanlı yönlendirme mimarisi ve Bölüm 5'te oluşturulan simülasyon çatısı açıklanmıştır. Bölüm 6'da ise elde edilen sonuçlar üzerinden önerilen protokolün performans değerlendirilmesi yapılmıştır. Son olarak Bölüm 7'de ise çalışmanın özeti verilerek tez sonuçlandırılmıştır.

2. LİTERATÜRDEKİ ÇALIŞMALAR

Bu tezin konusuna olan benzerliği dikkate alınarak literatürde yer alan kümeleme tabanlı KAA mimarileri için önerilen IDS ve TBS çalışmaları ile birlikte yönlendirme saldırılarının modellenmesine odaklanan çalışmalar incelenmiştir.

2.1. Yönlendirme Saldırılarının Modellenmesi ve IDS Tabanlı Çözümler

Patil ve Khanagoudar (2012) yaptıkları çalışmada, kümeleme tabanlı heterojen bir KAA sistemi için baz istasyonu tarafından gerçekleştirilen merkezi bir IDS önermişlerdir. Ağda hem tekli hem de çoklu saldırılar için algılama sistemi tasarlamışlardır. KAA üzerinde saldırganı tespit etmek için, düğümlerin port numaraları, IP adresleri, MAC adresleri bilgileri kullanılmıştır. Sistemde yer alan baz istasyonunun tüm bilgilere sahip olduğu varsayılmıştır. Bir düğüm, kullanılan parametreler ile doğrulanamıyorsa, baz istasyonu tarafından kötü niyetli düğüm olarak etiketlenir ve sistem alarmı devreye girer. Önerilen sistemin, saldırıların tespiti ve önlenmesi için verimli olduğu ifade edilmiştir.

Mahajan, Reddy ve Rajput (2016), kümeleme tabanlı heterojen bir KAA sistemi için önerdikleri merkezi IDS'de yüksek enerjiye sahip saldırgan düğümleri tespit etmeye çalışmışlardır. Küme başı seçimi LEACH (Heinzelman, Chadrakasan ve Balakrishnan, 2000) protokolüne göre yapılmıştır. Seçilen küme başı düğümler, ağ sisteminde yer alan tüm düğümlere kendi konum bilgisini gönderir. Konum bilgisi yayım mesajından sonra üye düğümler ile küme başı düğümleri arasındaki mesafe hesaplanır ve ağ sisteminde kümeler oluşturulur. Radyo aralığına ve mesafe değerine göre RTresh değeri belirlenir. RTresh değerine göre, bir düğümün şüpheli düğüm olup olmadığı baz istasyonu tarafından değerlendirilir. Şüpheli düğümler baz istasyonu tarafından sistemden izole edilir. Önerilen sistemde, hello flood saldırıları modellenmiştir.

Zhang, Zhai,Yang ve Cui (2014) tarafından heterojen KAA'lar için tasarlanan IDS sistemi, rota talebi, rota cevaplama ve rota kurulumu olmak üzere üç aşamadan oluşmaktadır. Sistemde iki düğüm arasında rota kurulumu sayesinde düğümlerin baz istasyonu yolunda verisini iletecekleri bir sonraki düğümün adresleri saklanır. Baz istasyonu, ağdaki tüm düğümlerin koordinat bilgisine sahiptir. Şüpheli düğümlere çoklu mesaj gönderilerek, fazlalık mekanizması yöntemi uygulanmıştır. Çoklu yol seçimi temel alınarak, obruk saldırıları tespit edilmiştir.

Tripathi, Gaur ve Laxmi (2013) yaptıkları çalışmada, LEACH protokolü üzerinde kara delik ve gri delik saldırılarını yüksek enerji eşiği kavramı ile modellemişlerdir. Küme tabanlı homojen bir KAA sisteminde çalışılmıştır. Küme başı seçimi LEACH protokolü ile gerçekleşmiştir. Ağ sistemi baz istasyonu tarafından yönetilmektedir. Deneyler farklı büyüklükteki ağlar için test edilmiştir. Baz istasyonu tarafından elde edilen simülasyon sonuçlarına göre gri delik saldırısındaki kayıp oranının, kara delik saldırısından daha az olduğu sonucu elde edilmiştir.

Bir diğer yönlendirme saldırısı modelleme çalışması ise Abasıkeleş-Turgut, Aydın ve Tohma (2016) tarafından önerilmiştir. Bu çalışmada kümeleme tabanlı bir bir KAA'da obruk ve kara delik saldırıları modellenmiştir. Saldırgan düğümün hem üye düğüm hem de küme başı olma olasılıkları ayrı ayrı ele alınmış, benzetimi yapılan farklı saldırı modellerinin ağ yaşam süresi, baz istasyonuna ulaşan paket sayısı ve enerji tüketimleri ölçülmüştür.

Wazid, Katal, Sachan , Goudar ve Singh (2013) yaptıkları çalışmada, kara delik saldırısının tespiti ve önlenmesi üzerine bir protokol önermişlerdir. Ağ sisteminde kümeler oluştuktan sonra, her küme için bir küme koordinatörü seçilmiştir. Her kümedeki üye düğümler, kümenin koordinatörüne bağlıdır. Kara delik saldırısında saldırgan düğüm paketin tamamını göndermemektedir. Yakalanan saldırgan düğüm, kara listeye alınıp sistemden izole edilir.

Dongare ve Mangrulkar (2016) yaptıkları çalışmada, optimal rota seçiminde enerji verimliliği tekniği ile kara delik ve gri delik saldırılarına karşı bir IDS önermişlerdir. Ağ sisteminde yönlendirme AODV protokolüne göre yapılmıştır. Yönlendirme işlemi, yönlendirme tablosuna göre yapılır. Önerilen enerji verimli tekniğin temel amacı, tehlikeye atılmış düğümü tespit etmek ve ağ iletişiminin bir parçası olmasını önlemeye çalışmaktır. Modellenen her iki saldırının da kötü niyetli düğümü önemli ölçüde tespit ettiği ve bu saldırılardaki etkilerini azalttığı iddia edilmiştir.

Bahekmat, Yaghmaee, Yazdi ve Sadeghi (2012) tasarladıkları IDS'de ağdaki kötü niyetli düğümleri tespit etmek için veri iletim yollarının kontrol edilmesini önermişlerdir. Bu kontrol, sistemde baz istasyonu tarafından gerçekleştirilir. Paketlerde hata yakalayan baz istasyonu, saldırgan olduğunu belirlediği düğümleri sistemden izole eder. Tüm düğümlerin lokasyon bilgileri baz istasyonu tarafından bilinir. Bu çalışmada obruk saldırıları modellenmiştir.

Radhikabaskar, Raja, Komara ve Paul'un (2014) önerdikleri IDS sisteminde baz istasyonu, küme başlarının ID numarasına göre ağı izler. Sistemdeki küme başı düğümler baz

istasyonu tarafından atanır ve her birine eşsiz bir ID numarası verilir. Küme başı, kapsama alanına bağlı olarak kendi kümesini oluşturur. Paket iletme algoritmasında, düğümler arasında paket iletimi sırasında en yüksek enerjiyi kaybeden düğüm saldırgan olarak algılanır. Yapılan simülasyonlar obruk saldırılarını tespit etmeyi hedeflemiştir.

Sedmelmaci ve diğerleri (2012) yaptıkları çalışmada, hiyerarşik bir mimari üzerinde anormallik ve imza tabanlı yaklaşımları birleştirmişlerdir. Bu çalışmada hiyerarşik mimariden kaynaklanan rol dağılımlarının dışında IDS ajanı adı verilen ek bir düğüm tipi bulunmaktadır. Bu ajanlar komşularını izleyerek bir rapor oluştururlar. Bu ajanların içerisinde bulunan anormallik tabanlı tespit için kullanılan SVM, dağıtık öğrenme algoritmalarını kullanarak sistemdeki anormal davranışları normal olanlardan ayırır. Ayrıca ataklara ait imzalarla bağlantılı sabit bazı kurallar da ajanlarda saklanmaktadır. IDS ajanları kendi kümeleri içerisindeki diğer ajanlarla doğrudan haberleşirken; başka kümelerde yer alan ajanlarla haberleşmek için küme başlarını kullanırlar. Böylece sistemde enerji tasarrufu sağlanmış olur. Haberleşme sonucunda her IDS ajanı düğümlere anormal veya normal etiketi verir. Eğer anormal davranış, daha önce tanımlanmış bir imzaya uyuyorsa bu durumda şüpheli düğümün kötü niyetli olduğuna karar verilir ve kümeden izole edilir. Aksi durumda oylama mekanizması devreye girer. IDS ajanı ilgili küme başına şüpheli düğüm ve özelliklerini içeren bir mesaj yollar. Bu mesaja göre küme başı oylama mekanizmasını devreye sokarak oyların yarısından fazlasını alan düğümleri kötü niyetli olarak etiketleyip kümeden atar.

Sahraoui ve Bouam (2013) yaptıkları çalışmada, hiyerarşik bir KAA üzerinde saldırıları tespit etmek amacıyla gözlemci düğümler kullanır. Her küme içerisinde belirli bir miktarda bulunmak zorunda olan gözlemci düğümler, küme başlarını izleyerek anormal davranışları tespit eder. Sistemde üye düğümlerin verilerini ilettikleri andan itibaren gözlemci düğümler, küme başlarını izlemeye başlar. Eğer küme başında hiçbir veri iletimi olmuyorsa, küme başı saldırgan olarak etiketlenir; kara listeye alınır ve komşu düğümler için yerel bir uyarı mesajı yayımlanır. Bu uyarı mesajını alan düğümler kara listelerine saldırganı eklerler. Düğümlerin kara listelerinde bulunan saldırganlar asla küme başı seçilemezler. Bu sayede gelecekteki obruk atakları da önlenmiş olur. Bununla birlikte, kötü niyetli düğümlerin tüm sistemden izole edilmesi için genel alarm mesajının da üretilmesi gerekmektedir. Ancak her seferinde üretilecek bir genel alarm sistemde çok fazla enerji harcayacağı için sadece belirli bir eşik değerinin üzerinde saldırgan kara listeye girerse genel alarm mesajı üretilir.

2.2. Güven Tabanlı Çözümler

Bao, Chen, Chang ve Cho (2012) yaptıkları çalışmada, güven tabanlı bir yönetim protokolü önermişlerdir. Küme tabanlı KAA sisteminde, küme başı seçiminde HEED (Younis ve Fahmy, 2004) algoritması kullanılmıştır. Sistemde güven mekanizması için önceki çalışmalardan farklı olarak sosyal güven ve servis kalitesi güveni olmak üzere iki farklı güven başlığı altında güven değeri hesaplanmıştır. Düğümün gerçek zamanlı durum değerlendirmesinden elde edilen nesnel güvene karşı, çalışma zamanı protokol yürütmesi sonucu ortaya çıkan öznel güven karşılaştırılması sistemin doğruluğunu ispatlamak için kullanılmıştır. Önerilen dinamik güven yönetim protokolünde sosyal güven bileşenleri, yakınlık (intimacy) ve dürüstlük (honesty); servis kalitesi güven bileşenleri ise enerji ve cömertlik (unselfishness)'tir. Yakınlık güven parametresi, düğümler arasındaki etkileşim deneyimleridir. Dürüstlük güven parametresi, düğümlerin kötü amaçlı olup olmadığının değerlendirmesidir. Enerji güven parametresi, düğümlerin yeterliliğini ölçmek içindir. Son olarak cömertlik güven parametresi ise düğümün sistemin refah düzeyini yükselme eğilimidir. Güven yönetim protokolü iki üye düğüm veya iki küme başı arasında periyodik olarak uçtan uca yöntemi kullanılarak yürütülmektedir. Önerilen hiyerarşik güven yönetim protokolünün performansını izlemek amacıyla, güvene dayalı coğrafi yönlendirme ve güvene dayalı izinsiz giriş saptama sisteminde olmak üzere iki farklı sistem üzerinde kullanmışlardır. Elde edilen sonuçlar, güvene dayalı coğrafi yönlendirmenin mesaj gönderim oranının, önemli bir mesaj ek yüküne neden olmadan, taşma tabanlı yönlendirmeyle elde edilebilecek ideal performans düzeyine ve mesaj gecikmesine yaklaştığını göstermektedir. Çalışmada, güvene dayalı izinsiz giriş tespiti için yanlış pozitifleri ve yanlış negatifleri en aza indirecek en uygun güven eşiği tespit edilmiştir. Ayrıca, güvene dayalı izinsiz giriş tespiti hem saptama olasılığı hem de yanlış pozitif olasılığı için geleneksel anomali tabanlı saldırı tespit yaklaşımlarını geride bırakmaktadır.
Z.Chen ve diğerleri (2015) yaptıkları çalışmada, TLES olarak adlandırılan, güvene duyarlı ve düşük enerji tüketimi olan güvenli bir topoloji protokolü önermişlerdir. TLES algoritması iki aşamadan oluşmaktadır. İlk aşama güven değeri hesaplanması ve küme başı seçimidir. Daha sonra güvenilir ve enerji tasarrufu sağlayan bir ağ elde etmek için ikinci aşama olarak ağ topolojisi oluşturulur. Sistemde gönderme oranı, tutarlılık faktörü, paket kayıp oranı olmak üzere üç farklı güven bileşeni vardır. Güven yönetim protokolünde, düğümün kendi değerlendirmesiyle oluşan sonuçla, diğer düğümlerden elde ettiği sonuçlar kıyaslanır.

Önerilen protokol literatürdeki çeşitli yönlendirme protokolleri ile karşılaştırılmıştır. Simülasyonlar sonucunda ağdaki saldırgan düğümlerin etkin bir şekilde izole edildiği, tüm ağın enerji tüketiminin azaltıldığı gözlemlenmiştir. Önerilen protokolün, karşılaştırılan diğer protokollere göre enerji tüketimin daha az olduğu ve ağ ömrünün daha uzun olduğu raporlanmıştır.

Dhakne ve Chatur (2017) yaptıkları çalışmada, HTBID olarak adlandırılan hiyerarşik güven tabanlı saldırı tespit sistemi ve HTEP olarak adlandırılan hiyerarşik güven yönetim protokolü önermişlerdir. Küme tabanlı KAA sisteminde, küme başı seçiminde HEED algoritması kullanılmıştır. Çalışmada yakınlık, dürüstlük, enerji ve cömertlik olmak üzere toplam dört adet güven bileşeni kullanılmaktadır. Yakınlık güven parametresi, düğümler arasındaki etkileşim deneyimleridir. Dürüstlük güven parametresi, düğümlerin kötü amaçlı olup olmadığının değerlendirmesidir. Enerji güven parametresi, düğümlerin yeterliliğini ölçmek içindir. Cömertlik güven parametresi ise düğümün sistemin refah düzeyini yükselme eğilimidir. Güven yönetim protokolü iki normal düğüm veya iki küme başı düğümü arasında periyodik olarak uçtan uca yöntemi kullanılarak yürütülmektedir. Çalışma saldırı tespit sistemi üzerinde test edilmiştir. Çalışmada kara delik, seçici yönlendirme ve aç-kapa saldırıları modellenerek sonuçlar kıyaslanmıştır. Önerilen yöntemin yanlış pozitif oranları düşük; saldırıları algılama oranı ve paket teslim oranının ise eşdeğerlerinden daha başarılı olduğu bildirilmiştir.

Salehi ve Karimian (2017) yaptıkları çalışmada, hiyerarşik güven yönetim protokolü önermişlerdir. Çalışmada ilk kümelenme LEACH bezneri bir kümeleme protokolüne göre yapılır. Çalışmada her düğüm, komşularının güven değerini hesaplar, hesaplanan değerlere göre veri alışverişi yapılır. Güven değeri belirlenen eşik değerinden büyük olan her düğüm küme başı olmaya aday olabilmektedir. Çalışmada güven değeri hesaplama, pozitif iletim oranı ve negatif iletim oranı olmak üzere iki adet güven parametresine bağlıdır. Pozitif iletim oranı her bir komşudan alınan başarılı iletim oranıdır. Negatif iletim oranı her bir komşudan alınan başarısız iletim oranıdır. Çalışma saldırı tespit sistemi üzerinde test edilmiştir. Aç-kapa, reputation squeeze, re-entry, unfair rating, collusion ve sybil saldırıları üzerinde analiz edilmiştir. Simülasyon sonuçları ağda güvenilmeyen düğümlerin küme başı olmasının engellediğini göstermiştir.

Fei ve Jian (2008) yaptıkları çalışmada, güven tabanlı bir yönlendirme protokolü önermişlerdir. Çalışmada dolaylı güven yönetimi kullanılmıştır. Tüm algılayıcılar birbirlerini izleyerek komşu algılayıcılara ait bir güven kaydı tutmaktadır. Elde edilen güven

değerleri bir güven tablosunda saklanmaktadır. Sistemde ağ iletimi güven değeri yüksek algılayıcılar üzerinden yapılmaktadır.

Juliana ve Maheswari (2016) yaptıkları çalışmada, küme tabanlı bir KAA sisteminde yapay arı kolonisi algoritması kullanılarak, güven tabanlı bir küme başı seçim protokolü önermişlerdir. Önerilen sistem kara delik ve servisi engelleme saldırıları için modellenmiştir. Sistemde paket teslimi ve enerji olmak üzere iki farklı parametre kullanılmıştır. Paket teslim parametresi ile enerji parametresi değerlerinin toplamı 1'e eşittir. Kullanılan performans ölçütleri oluşturulan küme sayısı, ortalama uçtan uca gecikme, ortalama paket teslim oranı, ağ ömrü ve kalan enerji tüketimidir. Simülasyon sonuçlarına dayanarak önerilen protokolün verimli olduğu bildirilmiştir.

Wazid ve diğerleri (2009) yaptıkları çalışmada, güven tabanlı bir yönlendirme protokolü önermişlerdir. Önerilen protokol LEACH protokolü ile kıyaslanmıştır. Çalışmada önerilen protokol, LEACH'in eksiklerini önlemek amacıyla tasarlanmış LEACH-TM protokolüdür. LEACH-TM protokolü güven tabanlı bir sistemdir. Elde edilen güven değerlerine göre algılayıcılar bir sonraki adımını seçerek paket iletimini gerçekleştirirler. Bu sistem algılayıcıların en iyi yolu kullanmaya ve uygun ağ kaynaklarını kullanmaya uygundur. Elde edilen güven değeri belirlenen eşik değerinden düşükse kaynak kullanımına izin verilmemektedir. Simülasyon sonuçlarında LEACH-TM protokolünün LEACH protokolüne göre daha başarılı olduğu görülmüştür.

Wang, Du ve Xu (2009) yaptıkları çalışmada, ağ sistemindeki normal düğümler, küme başı düğümleri izlemektedir. Düğümlerin itibarını korumak ve güvenilirliklerini değerlendirmek için bekçi mekanizması kullanılır. Algılayıcıların güven değeri, belirlenen eşik değerinden düşük ise küme başı düğümü tarafından sistemden izole edilir. Düğümlerin güven değeri hesaplanırken, beta dağılımı kullanılmıştır.

Zhiyuan, ZhiGang, SongSong, YeQing ve Jing (2009) yaptıkları çalışmada, küme tabanlı KAA'larda Bayes Teoremine dayanan TMBBT protokolünü önermişlerdir. TMBBT protokolü doğrudan ve dolaylı iletişimi, iletişim güvenini ve veri güvenini ayırt etmiştir. Veri ve iletişimsel güven ilişkisini ele almak için Bayes Teoremini kullanmıştır. Ayrıca, güven oluşturmak, sürdürmek ve güncellemek için kullanılan enerjiyi de azaltmıştır.

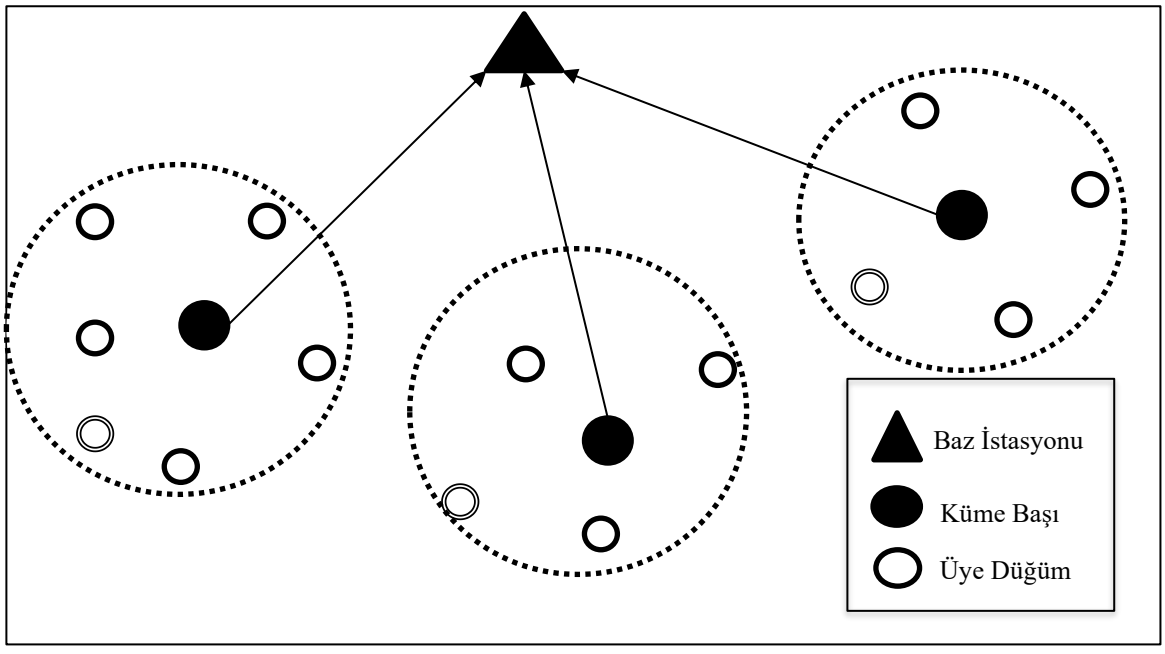
2.3. Tez Çalışmasının Literatüre Katkısı

Bu tezde, kümeleme tabanlı hiyerarşik mimariye sahip KAA'lar için güven tabanlı yönlendirme mimarisi (GüYöM) tasarlanmıştır. Tasarlanan protokolde temel amaç, saldırgan tarafından ele geçirilmemiş düğümlerin küme başı olarak seçilmesini sağlayarak, ağ verisini güvenli bir rota üzerinden enerji verimli bir şekilde baz istasyonuna ulaştırmaktır. Bu amaçla küme başı seçiminde literatürde de kullanılmış olan tutarlılık faktörü ve paket iletim oranı parametreleri kullanılmıştır. Literatürdeki çalışmalardan farklı olarak bencillik parametresi de küme başı seçimine dahil edilmiştir. Ayrıca KAA'ların enerji kısıtları dikkate alındığında küme başı seçiminde enerjisi yüksek düğümlerin seçilmesi, küme başlarının daha uzun süre yaşamasına ve buna bağlı olarak ağın ömrünün uzamasına katkıda bulunacaktır. Bu amaçla küme başı seçiminde düğümlerin kalan enerjileri de dikkate alınmıştır. Bununla birlikte sadece yüksek enerjiye sahip düğümlerin seçilmesi ağda saldırganların küme başı olmasına neden olabileceği için, enerji parametresi güven parametresi ile birlikte kullanılmıştır. Böylece hem güvenilir düğümlerin küme başı olarak seçilerek ağdaki saldırıdan korunma; hem de enerjisi yüksek düğümlerin seçimi ile ağ yaşam süresinin uzatılması sağlanmıştır. Önerilen GüYöM protokolü, literatürde kümeleme mimarisinin temeli olarak kabul edilen LEACH algoritması ve kümeleme mimarileri üzerinde güven tabanlı yol kurmayı öneren TLES algoritması ile çeşitli ağ parametreleri üzerinden simülasyon yöntemi kullanılarak kıyaslanmıştır. Yapılan simülasyonlardan elde edilen sonuçlar, GüYöM' ün her iki protokole göre de daha uzun ağ yaşam süresi, daha az harcanan enerji ve ortalama paket kayıp oranlarını ise azalttığını göstermiştir.

- Tez çalışmasında; tutarlılık faktörü, paket iletim oranı ve bencillik olmak 3 farklı güven parametresi kullanıldı.
- Düğümün güven değeri belirlenen eşikten yüksek ise kümebaşı düğüm olmasına izin verildi.
- Kümebaşı seçiminde güven değeri ile birlikte kalan enerji değeri de hesaba eklenerek, hem yüksek güven değerine hem de yüksek enerji değerine sahip olan düğümün kümebaşı düğüm olması sağlandı.
- Bazdaki paket kayıp oranı, ağdaki yaşayan düğüm sayısı ve ağda harcanan enerji parametreleri üzerinden, LEACH ve TLES protokolleri ile kıyaslanmıştır.
- Kıyaslamalar sonucunda, ağ yaşam süresi parametresinde uzama, harcanan enerji parametresinde azalma ve ortalama paket kayıp oranı parametresinde ise azalma görülmüştür.

3. KÜME TABANLI KABLOSUZ ALGILAYICI AĞ YAPISI

Büyük ölçekli KAA' lar, binlerce algılayıcı düğümün bir araya gelmesiyle oluşur. Bu ağlarda ölçeklenebilirlik problemi için kümeleme tabanlı hiyerarşik yönlendirme protokollerinin kullanılması etkili bir çözüm yöntemidir (Singh ve diğerleri ,2015). Kümeleme yapısında birbirine yakın konumdaki komşu düğümler ve bunların arasından seçilen bir küme başı düğüm bir küme oluşturmak üzere gruplandırılır. Küme başı düğüm (cluster head- CH) seçimi önceden belirlenen bir protokole göre uygulanır. Kümeleme tabanlı KAA'lar, Şekil 3.1'te görüldüğü gibi küme başı, üye düğümler ve baz istasyonu olmak üzere üç ana bileşenden oluşur. Baz istasyonu, küme başının, üye düğümlerden toplayıp kendisine gönderdiği veriyi değerlendirirken; küme başı düğümler kendisine bağlı olan üye düğümlerden topladığı veriye önce birleştirme işlemi, ardından da birleştirilen veriyi baz istasyonuna iletme işlemini gerçekleştirir. Üye düğümler ise yerleştirildikleri ortamda bir olay algıladıkları zaman bağlı oldukları küme başına algıladıkları olayları bildirmekten sorumludur. Kümeleme yapısı sayesinde algılayıcı düğümler, düşük enerji tüketimi ile kapsamlı bir algılama; aralarındaki iş birliği ile sağlam bir ağ yapısı oluştururlar (Tohma, Aydın ve Turgut, 2015).



Şekil 3.1. Küme tabanlı KAA yapısı

3.1. Küme Tabanlı Kablosuz Algılayıcı Ağlarda Yönlendirme Saldırıları

Yönlendirme saldırıları, KAA'ların ağ katmanında paket iletimini engellemeye yönelik olarak gerçekleştirilen saldırılardır. Obruk (sinkhole), kara delik (blackhole), gri delik (gray hole), solucan deliği (wormhole), seçici yönlendirme (selective forwarding) gibi çeşitli saldırılar yönlendirme saldırıları başlığı altında toplanır (Kalita ve Kar,2009). Solucan deliği saldırısında, iki kötücül düğüm birbirleri arasında yüksek iletişim kalitesine sahip bir kanal oluştururlar. Daha sonra yönlendirme için bu kanalın reklamını yaparak çevredeki algılayıcılardan baz istasyonuna gönderilmek üzere veri toplarlar (Meghdadi, Özdemir ve Güler,2008). Obruk saldırısında ise, ağa sızmaya saldırgan düğüm, bir algılayıcı düğümü tehlikeye düşürerek veya ağın içine saldırgan düğüm sokarak ağ sistemini tehlikeye sokmaya çalışmaktadır.

Kara delik saldırısında saldırgan düğüm, kendisine ulaşan paketlerin tamamını bloke ederek hedefe iletimini engellerken, gri delik saldırısında saldırgan düğüm, kendisine ulaşan paketlerin yarısını bloke ederek hedefe iletimini engeller. Seçici yönlendirme saldırısında paketlerin bir kısmını bloke edip, bir kısmını hedefe düğüme yönlendirir (Roosta, Shieh ve Sastry,2006). Bütün saldırı çeşitleri, baz istasyonunda veri kaybına neden olup, ağdan sağlıklı bir bilgi toplanamaması sonucuna sebep olur.

Yönlendirme saldırılarına karşı literatürde çok sayıda çözüm önerisi sunulmuştur (S.Singh,M.Singh ve D.Singh ,2011). Bu saldırılara karşı alınacak önlemleri tasarlamadan önce saldırıların davranışlarının ve ağa verdiği zararların belirlenmesi, ağın başarı oranı üzerinde çok büyük önem taşımaktadır.

4. GüYöM: GÜVEN TABANLI YÖNLENDİRME MİMARİSİ

4.1. Yönlendirme Çatısı

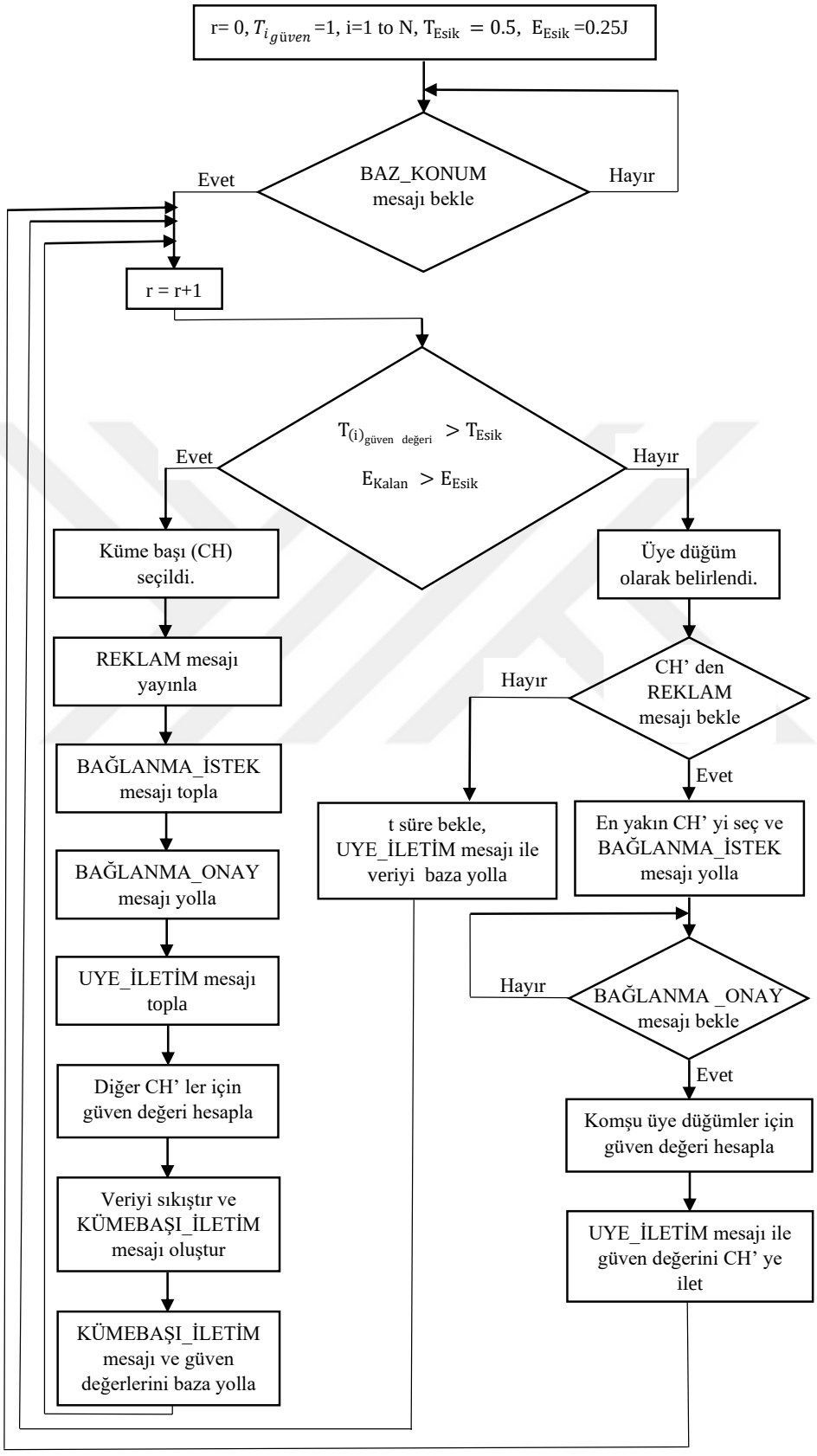
Önerilen GüYöM protokolünün yönlendirme altyapısı, LEACH protokolü temel alınarak tasarlanmıştır. Ağ sistemi ardışık döngülerden oluşmaktadır. Her döngü, sırasıyla küme başlarının seçilmesi, etrafında kümelerin oluşturulması ve veri iletimi aşamalarından oluşur. Düğümlerin enerjilerini tüketip ölerek sistemden çıkmaları sonucunda ağ süresi içinde gittikçe daha az düğüm bu prosese dahil olur. Tüm düğümlerin ölüp, ağdan verinin toplanamadığı ilk döngü, ağ yaşam süresi olarak adlandırılır. Sistemin çalışması, baz istasyonunun kendi konum bilgisini, BAZ_KONUM mesajı yoluyla ağa yayım yaparak tüm düğümlere iletmesi ile başlar. Bu işlem sadece 1 kez, ilk döngünün başında gerçekleştirilir. Diğer döngülerin başlatılması baz istasyonu tarafından gönderilen DÖNGÜ_BAŞLAT mesajı ile gerçekleştirilmektedir. Çizelge 4.1. 'de sistemdeki mesajlar görülmektedir.

Çizelge 4.1. Küme tabanlı KAA sisteminde kullanılan mesajlar ve işlevleri

Mesajın Adı	**Mesajın İşlevi**
DÖNGÜ_BAŞLAT	Yeni döngünün başlatılması
BAZ_KONUM	İlk döngünün başlatılması
REKLAM	Küme başı düğümün varlığını diğer düğümlere haber vermesi
BAGLANMA_İSTEK	Kümeye katılma isteği
BAGLANMA_ONAY	Kümeye katılma onayı
UYE_İLETİM	Üye düğümlerden küme başlarına veri iletimi
KÜMEBAŞI_İLETİM	Küme başı düğümlerden baz istasyonuna veri iletimi

Döngünün başlatılmasının ardından düğümler küme başı seçim yarışına girerler. Merkezi bir denetim ve kontrol olmaksızın dağıtık bir şekilde düğümler tarafından belirli bir algoritmaya göre verilen küme başı olma kararının ardından, küme başı olarak seçilen düğümler etraflarına REKLAM mesajı yayımlayarak küme başı olduklarını diğer düğümlere duyururlar. Bu mesajı alan ve küme başı olarak seçilmeyen düğümler, kendilerine en yakın küme başını seçerek onun kümesine dahil olmak için BAGLANMA_İSTEK mesajı yollar. İstek mesajlarını toplayan küme başı düğümler, üye düğümlerin veri iletim zamanları için bir çizelge oluşturur ve hem bağlanma isteklerine onay vermek, hem de zaman aralıklarını bildirmek için tüm üye düğümlere ulaştırılmak üzere ağa BAGLANMA_ONAY mesajı

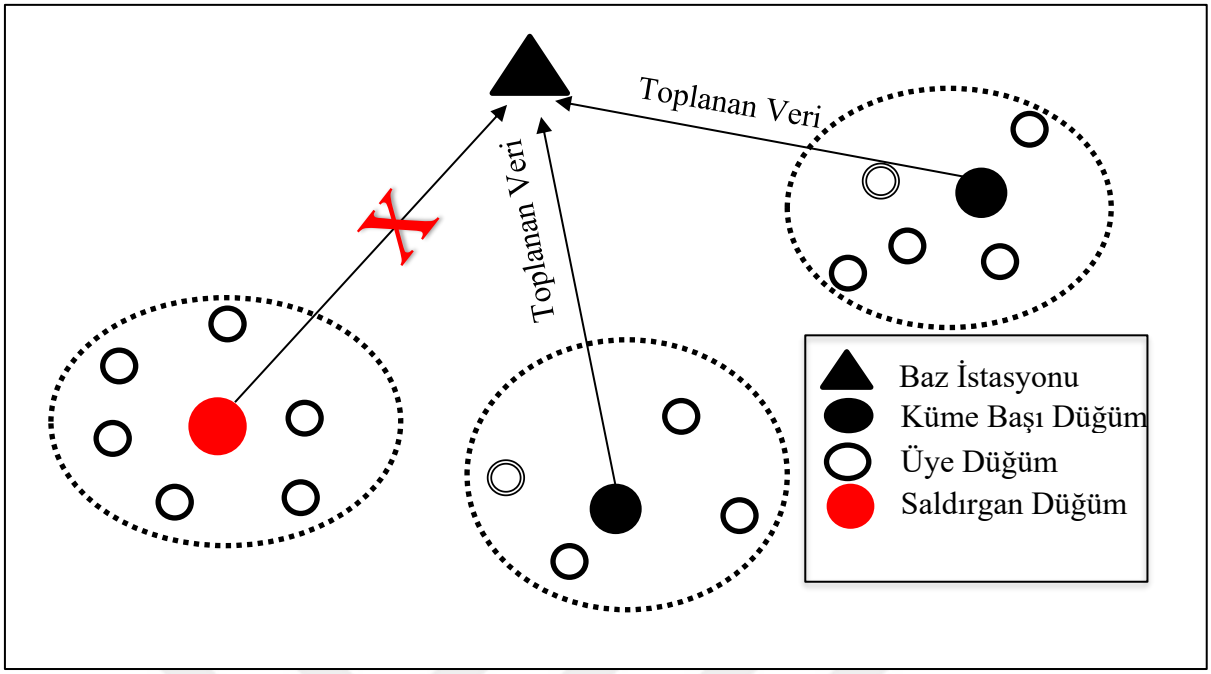
yollar. BAGLANMA_ONAY mesajı yollama işleminden sonra, üye düğümler kendi kümesindeki diğer üyelerin hepsi için bir güven değeri belirler. Bu aşamadan sonra veri iletim aşamasına geçilir. Veri iletim aşamasında, üyeler etraftan topladıkları veriyi ve BAGLANMA_ONAY mesajı sırasında hesaplanan üye düğümlerin güven değerlerini UYE_İLETİM mesajı ile birlikte küme başına gönderilmektedir. UYE_İLETİM mesajları, küme başına iletildikten sonra küme başı, ağdaki diğer küme başlarının hepsi için bir güven değeri belirler. Güven değeri belirleme işleminden sonra, küme başı topladıkları veriye, kendi verisini de dahil edip birleştirme işlemi uygular ve baz istasyonuna birleştirilmiş veri ile belirlenen güven değerleri KÜMEBAŞI_İLETİM mesajı içinde gönderir. Baz istasyonuna tüm küme başlarının verisinin gelmesinin ardından döngü tamamlanır ve yeniden bir döngü başlatılması amacıyla baz istasyonu ağa DÖNGÜ_BAŞLAT mesajını yayımlar. Sistemde veri ve kontrol olmak üzere iki tip paket vardır. Sistemde yer alan paket türlerinden UYE_İLETİM ve KÜMEBAŞI_İLETİM veri içermekle birlikte diğer paketler sadece kontrol amacıyla kullanıldığı için veri içermemektedir. Kontrol paketleri içerisinde sadece BAGLANMA_İSTEK mesajı yayım yoluyla iletilmediği için hedef adres içermektedir. Bununla birlikte tüm paketlerde gönderici düğümün ID bilgisi yer alır. REKLAM mesajında küme başı düğümün konum bilgisi; BAZ_KONUM mesajında baz istasyonunun konum bilgisi; veri ileten paketlerde ise düğümlerin o döngü harcamış olduğu enerji bilgileri diğer paket türlerinden farklı olarak yer alır. Son olarak BAGLANMA_ONAY mesajı içerisinde üye düğümlerin zaman çizelgesi de bulunmaktadır. Önerilen protokolde kodlanan, yazılımın akış diyagramı Şekil 4.1.' de gösterilmiştir. Kodlamada kullanılan kısaltmalarda, N: düğüm sayısını, r: döngü sayısını, $T_{(i)_{\text{güven değeri}}}$: i düğümüne duyulan güven değerini, T_{Esik} : güven eşik değerini, E_{Kalan}: düğümün kalan enerjisini, E_{Esik}: enerji parametresinin eşik değerini temsil etmektedir. Akış diyagramında görüldüğü gibi, yönlendirme alt yapısı kodlandıktan sonra, yaşayan tüm düğümler için hesaplanan güven değeri ve kalan enerji değeri belirlenen eşik değerinden yüksek ise düğüm küme başı düğüm olarak seçilmektedir. Düğümün kalan enerji değeri, enerji eşik değerinden yüksek ancak güven değeri eşik değerinden düşük ise düğüm küme başı düğüm olamamaktadır. Bu durum enerjisi yüksek olan saldırganların, küme başı seçilmesini engellemektedir. Düğümün küme başı olarak seçilebilmesi için hem yüksek güven değerine hem de yüksek enerji değerine sahip olması gereklidir.



Şekil 4.1. Yazılım sisteminin akış diyagramı

4.2. Saldırıların Modellenmesi

Bu tezde, kümeleme tabanlı KAA için kara delik saldırıları modellenmiş; ardından bu saldırıların olduğu ağda algılayıcı düğümlerden toplanan verinin güvenli bir yol üzerinden baz istasyonuna ulaşması sağlanmıştır. Baz istasyonu rolündeki düğümün, enerji kısıtı olmayan ve tamamen güvenilir bir kaynak olduğu varsayılmıştır. Kümeleme tabanlı bir ağda küme başı ve algılayıcı düğüm olmak üzere iki farklı role sahip düğüm yer almaktadır. Algılayıcı düğümün ağdaki tek görevi, çevresindeki olayı algıladıktan sonra oluşturduğu raporu küme başına yollamaktır. Küme başı düğüm ise tüm kümesindeki algılayıcı düğümlerin verisini baz istasyonuna iletmekten sorumludur. Kara delik gibi verinin iletilmesini engelleyen saldırı türlerinin ağa zarar verebilmesi ve yaşanan paket kayıplarının belirgin bir şekilde analiz edilebilmesi için bu ağlarda saldırganın küme başı rolündeki düğümü ele geçirmesi gerekmektedir. Bu nedenle bu tezde saldırılar modellenirken, küme başı düğümlerin kötü niyetli olduğu varsayılmıştır. Saldırgan düğümlerin ağda erken ölmesini engellemek ve önerilen güvenli rotanın başarımını test edebilmek için saldırgan düğümlerin başlangıç enerjileri sıradan algılayıcı düğümlerin 4 katı olarak belirlenmiştir. Böylece saldırganların ağda daha uzun süre yaşayarak rotayı bozması amaçlanmıştır. Saldırganlar ağda periyodik olarak, her döngü saldırı gerçekleştirmektedir. Kara delik saldırısında, saldırgan düğümler üyelerden topladığı veri paketlerinin tamamını bloke ederek baz istasyonuna ulaşmasını engeller. Şekil 4.2. ’de modellenen yönlendirme saldırıları görülmektedir.



Şekil 4.2. Modellenen yönlendirme saldırıları

4.3. Güven Değeri Hesaplaması

Bu tezde küme başlarının seçiminde güven ve enerji parametreleri hesaba katılmıştır. Güven parametresinin kullanılmasının sebebi, verinin saldırgan tarafından ele geçirilmemiş güvenilir düğümler üzerinden baz istasyonuna başarılı bir şekilde ulaştırılmasıdır. Enerji parametresinin kullanılma nedeni ise küme başlarının erken ölmelerinin engellenerek ağ yaşam süresinin uzatılmasıdır. Bu tez kapsamında küme başı seçiminde kullanılan güven parametresi 3 farklı alt bileşenden oluşur: tutarlılık faktörü, paket iletim oranı ve bencilliktir. Güven alt bileşenlerinin hesaplanmasında üye düğümlerin birbirlerini izlemesi, baz istasyonunun da küme başlarını izlemesi temel alınır. Bir küme içinde yer alan üye düğümler diğerlerine gelen-giden paketleri izleyerek tüm komşuları için bir güven değeri belirler. Bir düğümün güven değeri, komşuları tarafından belirlenen değerin ortalamasıdır. Her üye düğüm elde ettiği güven değerini küme başına iletir. Küme başlarının güven değeri ise baz istasyonu tarafından takip edilir. Test edilen sistemde üye düğümlerin saldırgan olmadıkları varsayıldığı için elde edilen sonuçlarda üye düğümlerin güven değerleri yüksek olmakla birlikte, modellenen sistem tüm düğümlerin saldırgan olabilme durumunu hesaba katmıştır. Güven parametrelerinin alt bileşenlerinin hesaplaması Eş. 4.1, Eş. 4.2 ve Eş. 4.3'te görülmektedir. $T_{i,j}^{tutarlılık\ faktörü}$, bir i düğümünün, j düğümü için belirlediği tutarlılık

faktörü değeridir. Bu değerin hesaplanmasına küme içinde yer alan düğüm sayısı ve j düğümünün döngü boyunca aldığı paket sayısı kullanılır. Küme içindeki üye düğüm sayısı, bir düğümün duyması gereken/alması gereken paket sayısını, aldığı paket sayısı ise gerçekte o döngü boyunca almış olduğu paket sayısını gösterir. Beklenen değer, düğümün duyması gereken tüm paketleri aldığı durum için 1'dir. Benzer şekilde paket iletim oranı, düğümün aldığı paketlerin ne kadarını ilettiğine göre belirlenir. Beklenen değer, düğümün aldığı tüm paketleri başarılı bir iletmesi olduğu için 1'dir. Bencillik parametresi ise düğümün enerji tasarrufu sağlamak için bencil olup olmadığını gösteren bir parametredir. Düğümün harcadığı enerji ile birlikte etrafında kendisi gibi bencil olan komşularının sayısına da bağlıdır. Beklenen durum, düğümün etrafında bencil komşularının bulunmaması ve harcadığı enerjinin o döngü için beklenen seviyenin üzerinde olmasıdır. μ değeri ağırlık katsayıdır ve değeri 0,5'tir. Bu durumda bencillik parametresi için beklenen değer 1 olmaktadır.

$$T_{i,j}^{tutarlılık\ faktörü} = \text{Alınan Paket Sayısı} \div \text{Küme Üye Sayısı} \quad \text{(Eş.4.1)}$$

$$T_{i,j}^{iletim\ oranı} = \text{Çıkan Paket Sayısı} \div \text{Giren Paket Sayısı} \quad \text{(Eş. 4.2)}$$

$$T_{i,j}^{bencillik} = \mu \times (Harcanan\ Enerji \div Beklenen\ Harcama\ Enerjisi) + (1-\mu) \times Bencil\ Olmayan\ Komşu\ Sayısı \div Tüm\ Komşu\ Sayısı \quad \text{(Eş. 4.3)}$$

Güven parametresinin alt bileşenleri, Eş.4.4' te görüldüğü şekilde birleştirilerek düğüme verilen güven değeri $T_{(i,j)_{güven\ değeri}}$ hesaplanır. Tüm alt bileşenlerin 1 olması durumunda düğümün tamamen güvenilir olduğu söylenebilir. Bununla birlikte güven eşik değeri 0.5'tir. Eşik değeri düğümün güvenilmez olduğunun belirlenmesinde kullanılır. Güven değeri yüzde ellinin altında olan düğüm güvenilmez olarak etiketlenir.

$$T_{(i,j)_{güven\ değeri}} = (T_{i,j}^{tutarlılık\ faktörü} + T_{i,j}^{iletim\ oranı} + T_{i,j}^{bencillik}) \div 3 \quad \text{(Eş. 4.4)}$$

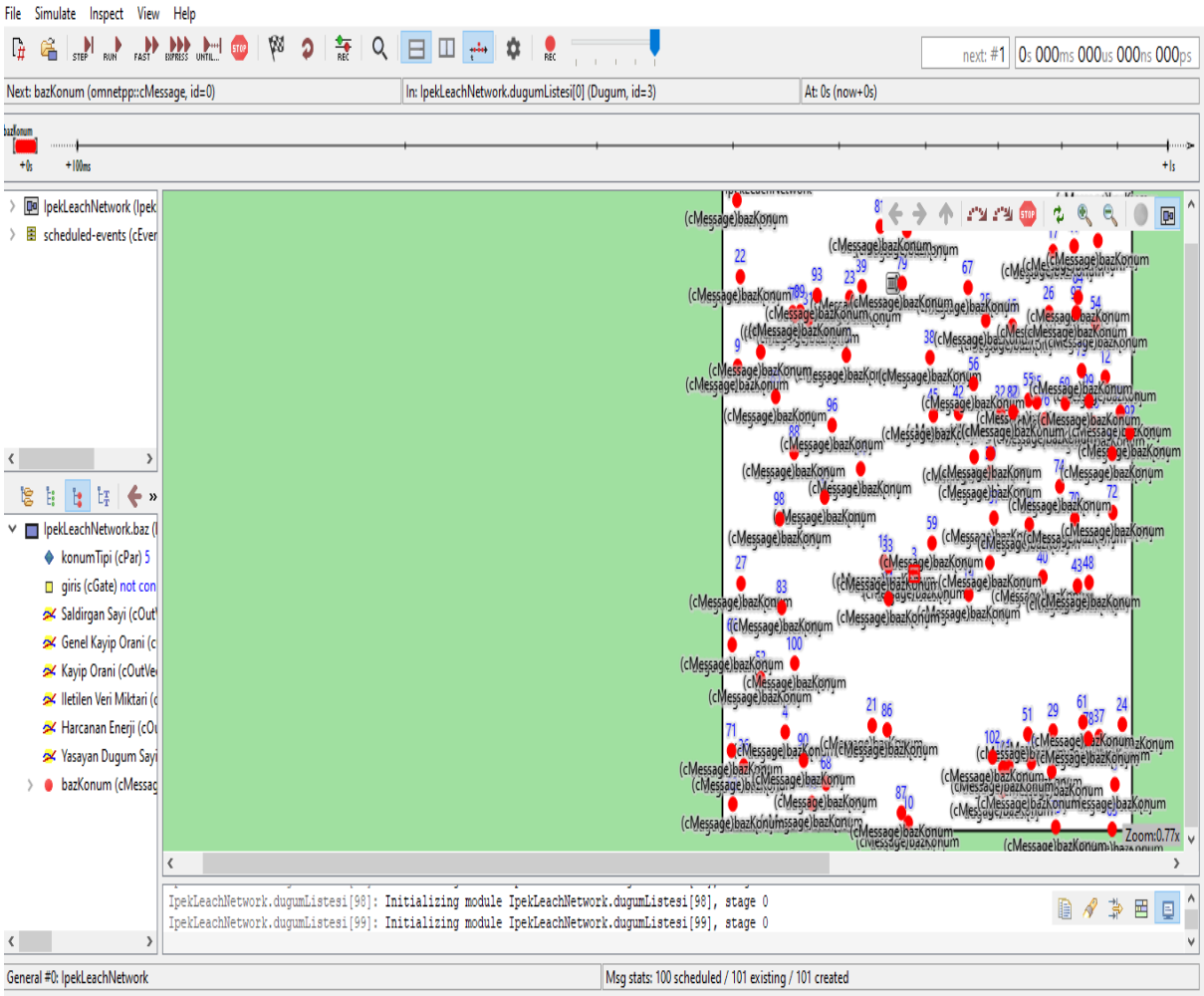
4.4. Küme Başı Seçim Yöntemi

Küme başı seçiminde güven parametresi ile birlikte düğümün enerjisi de hesaba katılır. Küme başlarını seçerken yüksek enerjili düğümlerin seçilmesi sağlanarak ağ ömrünün uzatılması amaçlanır. Bununla birlikte saldırgan düğümlerin enerjisinin yüksek olması

nedeniyle saldırganların küme başı seçiminden ağın korunmasının da sağlanması gerekmektedir. Bu nedenle küme başı seçiminde enerji parametresi ancak güven değeri hesaba katıldıktan sonra kullanılır. Bir düğüm ancak güvenilir ise (güven değeri yüzde 50'nin üzerinde ise) küme başı seçimine enerji parametresi dahil edilerek, daha yüksek enerjili düğümlerin küme başı seçilmesi sağlanır.

5.SİMÜLASYON ÇATISI

Bu tez, OMNeT++ simülasyon programı üzerinde gerçekleşmiştir. OMNeT++ (Şekil 5.1.) nesneye yönelik ve modüler yapıda ayrık olay ağ simülasyon programıdır. Birçok çalışmanın modellenmesi için kullanılabilir haberleşme ağlarını içermektedir. Buna ek olarak kullanıcıların kendi bileşenlerini simule edebilmeleri için birçok temel modül sağlamaktadır. Bu yapı sayesinde kullanıcı, hareketlik iskeletine yönelik kendi iletişim kurallarını, gerekli arabirim ve malzemelerin birlikte çalışılabilirliği ile uğraşmaksızın, kolaylıkla ağ sistemi geliştirebilmektedirler (Varga ve Hornig,2008).



Şekil 5.1. Omnet++ ağ simülasyon programı

5.1. Simülasyon Parametreleri

Sistemin performansının test edilmesi amacıyla çeşitli ağ parametrelerinin farklı değerleri için çok sayıda simülasyon çalıştırılmıştır. Her bir simülasyon, farklı bir model numarası ile adlandırılır. Tüm modellerde ortak olarak simülasyon parametreleri Çizelge 5.1'de görülmektedir. Heterojen bir ağda düğümlerin ilk enerjileri 0,75 J ile 1,25 J arasında değişmektedir. Kötü niyetli düğümlerin ise başlangıç enerjileri 4J'dir. Düğümler düzenli dağılım ile rasgele bir şekilde ağ alanına dağıtılmıştır. Veri paketleri 2000 bittir. Bir düğümün güvenilir olduğunun söylenebilmesi için en az %50'lik bir güven değerine sahip olması beklenir. Bununla birlikte Çizelge 5.2 'den Çizelge 5.19'a kadar görüldüğü üzere her modelde değişen ağ parametreleri ağ alanı, düğüm sayısı ve kötü niyetli düğümlerin yüzdesidir.

Çizelge 5.1. Tüm modellerde ortak olan simülasyon parametreleri

Parametreler	**Değerler**
Düğüm Başlangıç Enerjileri	0,75J – 1,25J arası
Kötü Niyetli Düğüm Başlangıç Enerjileri	4j
Düğüm Dağılımı	Rastgele
Paket Boyutu (X)	2000bit
Güven Eşik Değeri	0,5

Çizelge 5.2. Model 1 ağ simülasyon parametreleri

Parametreler	**Değerler**
Ağ Alanı	400x400
Düğüm Sayısı	100 Düğüm
Kötü Niyetli Düğüm Oranı	%10

Çizelge 5.3. Model 2 ağ simülasyon parametreleri

Parametreler	**Değerler**
Ağ Alanı	400x400
Düğüm Sayısı	100 Düğüm
Kötü Niyetli Düğüm Oranı	%20

Çizelge 5.4. Model 3 ağ simülasyon parametreleri

Parametreler	**Değerler**
Ağ Alanı	400x400
Düğüm Sayısı	100 Düğüm
Kötü Niyetli Düğüm Oranı	%30

Çizelge 5.5. Model 4 ağ simülasyon parametreleri

Parametreler	**Değerler**
Ağ Alanı	400x400
Düğüm Sayısı	200 Düğüm
Kötü Niyetli Düğüm Oranı	%10

Çizelge 5.6. Model 5 ağ simülasyon parametreleri

Parametreler	**Değerler**
Ağ Alanı	400x400
Düğüm Sayısı	200 Düğüm
Kötü Niyetli Düğüm Oranı	%20

Çizelge 5.7. Model 6 ağ simülasyon parametreleri

Parametreler	**Değerler**
Ağ Alanı	400x400
Düğüm Sayısı	200 Düğüm
Kötü Niyetli Düğüm Oranı	%30

Çizelge 5.8. Model 7 ağ simülasyon parametreleri

Parametreler	**Değerler**
Ağ Alanı	400x400
Düğüm Sayısı	300 Düğüm
Kötü Niyetli Düğüm Oranı	%10

Çizelge 5.9. Model 8 ağ simülasyon parametreleri

Parametreler	**Değerler**
Ağ Alanı	400x400
Düğüm Sayısı	300 Düğüm
Kötü Niyetli Düğüm Oranı	%20

Çizelge 5.10. Model 9 ağ simülasyon parametreleri

Parametreler	**Değerler**
Ağ Alanı	400x400
Düğüm Sayısı	300 Düğüm
Kötü Niyetli Düğüm Oranı	%30

Çizelge 5.11. Model 10 ağ simülasyon parametreleri

Parametreler	**Değerler**
Ağ Alanı	600x600
Düğüm Sayısı	100 Düğüm
Kötü Niyetli Düğüm Oranı	%10

Çizelge 5.12. Model 11 ağ simülasyon parametreleri

Parametreler	**Değerler**
Ağ Alanı	600x600
Düğüm Sayısı	100 Düğüm
Kötü Niyetli Düğüm Oranı	%20

Çizelge 5.13. Model 12 ağ simülasyon parametreleri

Parametreler	**Değerler**
Ağ Alanı	600x600
Düğüm Sayısı	100 Düğüm
Kötü Niyetli Düğüm Oranı	%30

Çizelge 5.14. Model 13 ağ simülasyon parametreleri

Parametreler	**Değerler**
Ağ Alanı	600x600
Düğüm Sayısı	200 Düğüm
Kötü Niyetli Düğüm Oranı	%10

Çizelge 5.15. Model 14 ağ simülasyon parametreleri

Parametreler	**Değerler**
Ağ Alanı	600x600
Düğüm Sayısı	200 Düğüm
Kötü Niyetli Düğüm Oranı	%20

Çizelge 5.16. Model 15 ağ simülasyon parametreleri

Parametreler	**Değerler**
Ağ Alanı	600x600
Düğüm Sayısı	200 Düğüm
Kötü Niyetli Düğüm Oranı	%30

Çizelge 5.17. Model 16 ağ simülasyon parametreleri

Parametreler	**Değerler**
Ağ Alanı	600x600
Düğüm Sayısı	300 Düğüm
Kötü Niyetli Düğüm Oranı	%10

Çizelge 5.18. Model 17 ağ simülasyon parametreleri

Parametreler	**Değerler**
Ağ Alanı	600x600
Düğüm Sayısı	300 Düğüm
Kötü Niyetli Düğüm Oranı	%20

Çizelge 5.19. Model 18 ağ simülasyon parametreleri

Parametreler	**Değerler**
Ağ Alanı	600x600
Düğüm Sayısı	300 Düğüm
Kötü Niyetli Düğüm Oranı	%30

5.2. Performans Ölçütleri

5.2.1. Yaşayan düğüm sayısı

Yapılan tez çalışmasında, sistem baz istasyonu tarafından yönetilmektedir. Her döngü sonunda baz istasyonu, enerji azalarak enerji eşik değerinin altına düşen düğümleri sistemden izole eder. Sistemden izole edilen düğümler bir sonraki döngüye katılamazlar. Her döngü sonunda enerji değeri, eşik değerinden yüksek olan düğümlerin sayısı yaşayan düğüm sayısı parametresi ile gösterilir.

5.2.2. Paket kayıp oranı

Her döngü sonunda baz istasyonu tarafından kontrol edilerek, saldırgan düğümlerin paketleri bloke etmesinden dolayı, baz istasyonuna ulaşamayan paketlerin yüzdelik kayıp miktarı, paket kayıp oranı olarak nitelendirilir.

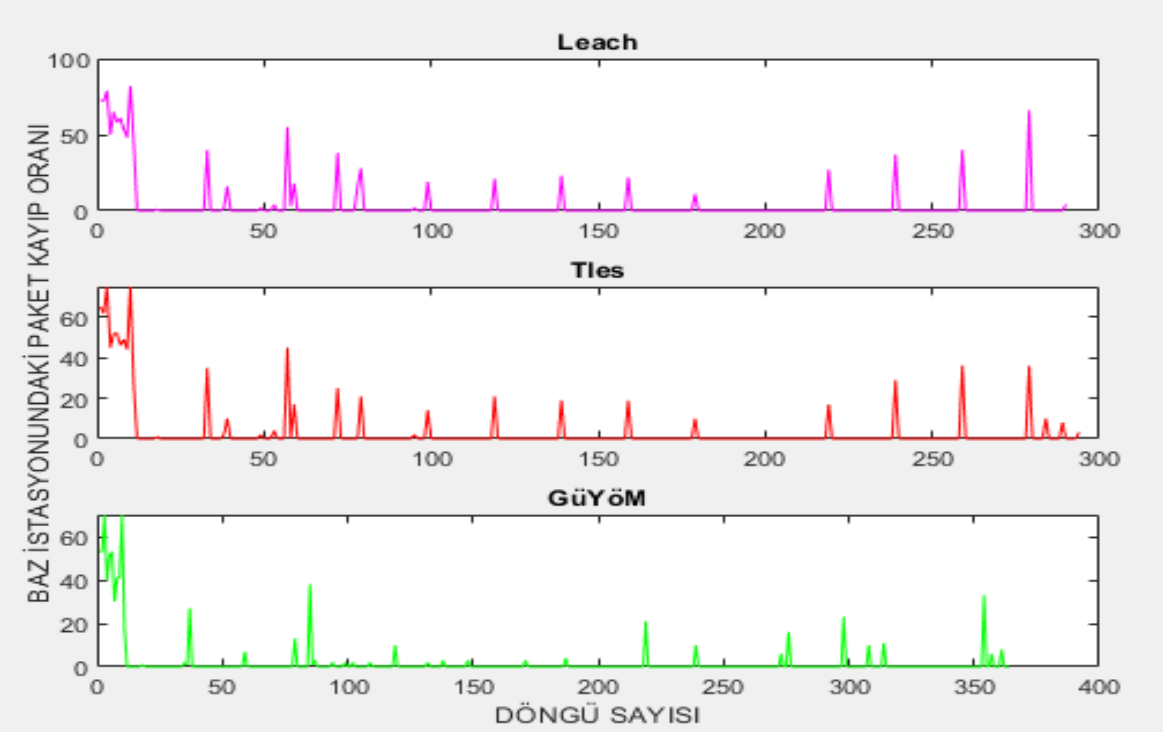
5.2.3. Harcanan enerji

Her döngü sonunda baz istasyonu tarafından kontrol edilerek, düğümlerin harcadığı toplam enerji miktarını göstermektedir.

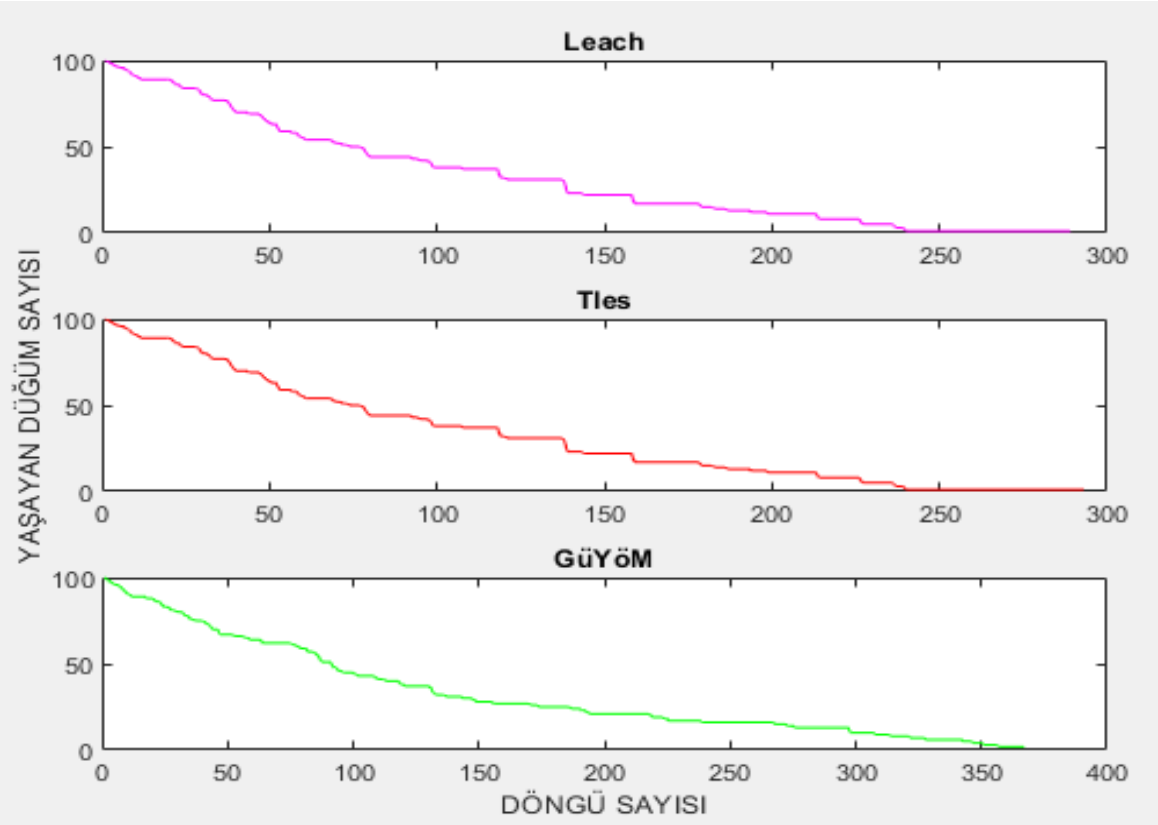
6. PERFORMANS DEĞERLENDİRMESİ

6.1. Model 1'in Performans Değerlendirmesi

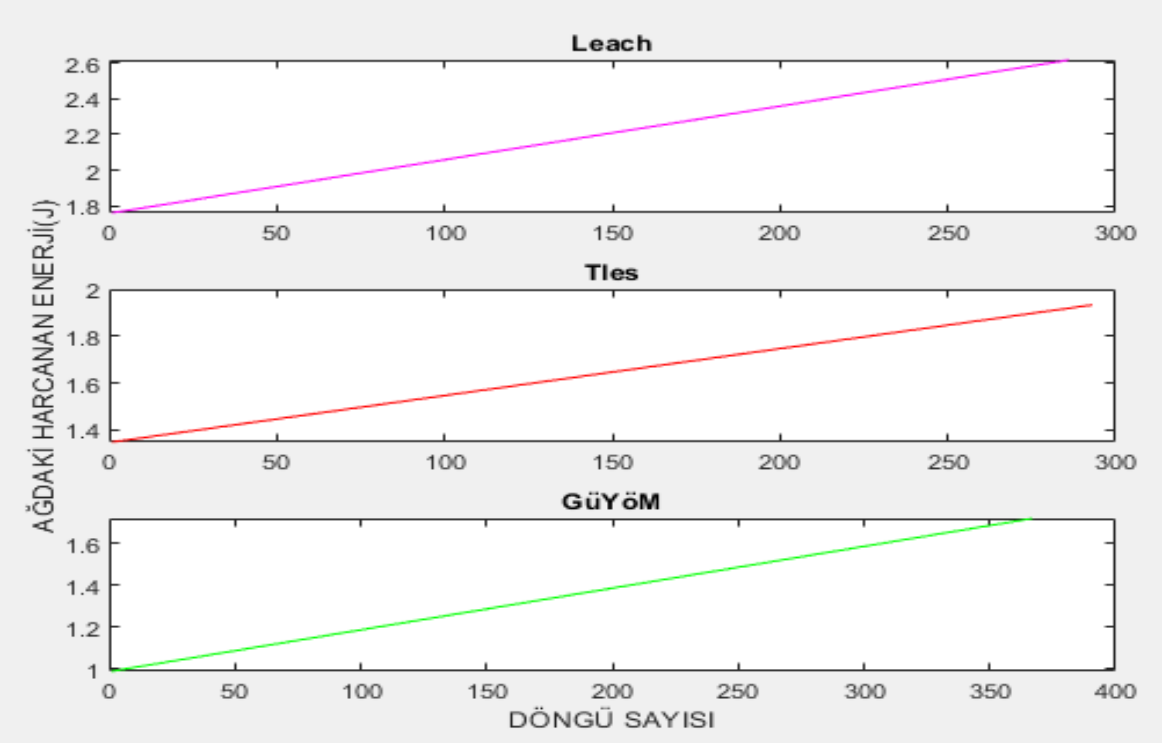
400x400'lük bir ağ alanı üzerinde modellenen KAA sisteminde 100 düğüm bulunmaktadır. Düğüm sayısının %10'u saldırgan düğüm olarak modellenmiş ve sonuçlar LEACH ve TLES algoritmaları ile kıyaslanmıştır. Performans ölçütü olarak ağda harcanan enerji, baz istasyonundaki paket kayıp oranı ve her döngü yaşayan düğüm sayısı olmak üzere 3 farklı parametre kullanılmıştır. Yapılan ölçümlerde LEACH protokolünde %4,01; TLES protokolünde %3,91; önerilen protokolde olan GüYöM'de ise %2,47 oranında paket kayıpları tespit edilmiştir (Şekil 6.1.). LEACH protokolünün ağ yaşam süresi 289 döngü iken, bu değer TLES protokolünde 293, GüYöM'de ise 367 döngüdür (Şekil 6.2.). Sonuçlardan da görüldüğü üzere GüYöM, güvenli yol üzerinden paketleri baz istasyonuna ulaştırmada diğer protokollere göre daha başarılı olurken, bunu enerji verimli bir şekilde yaptığı için ağ yaşam süresini de uzatmıştır. Bunun nedeni düğümlerin enerjilerinin verimli kullanmasını sağlamasıdır. Şekil 6.3.'te verilen harcanan enerji kıyaslamasında LEACH'in en fazla, GüYöM'ün ise en az enerji harcadığı tespit edilmiştir.



Şekil 6.1. Model 1 için her döngü baz istasyonunda gözlemlenen paket kayıp oranı



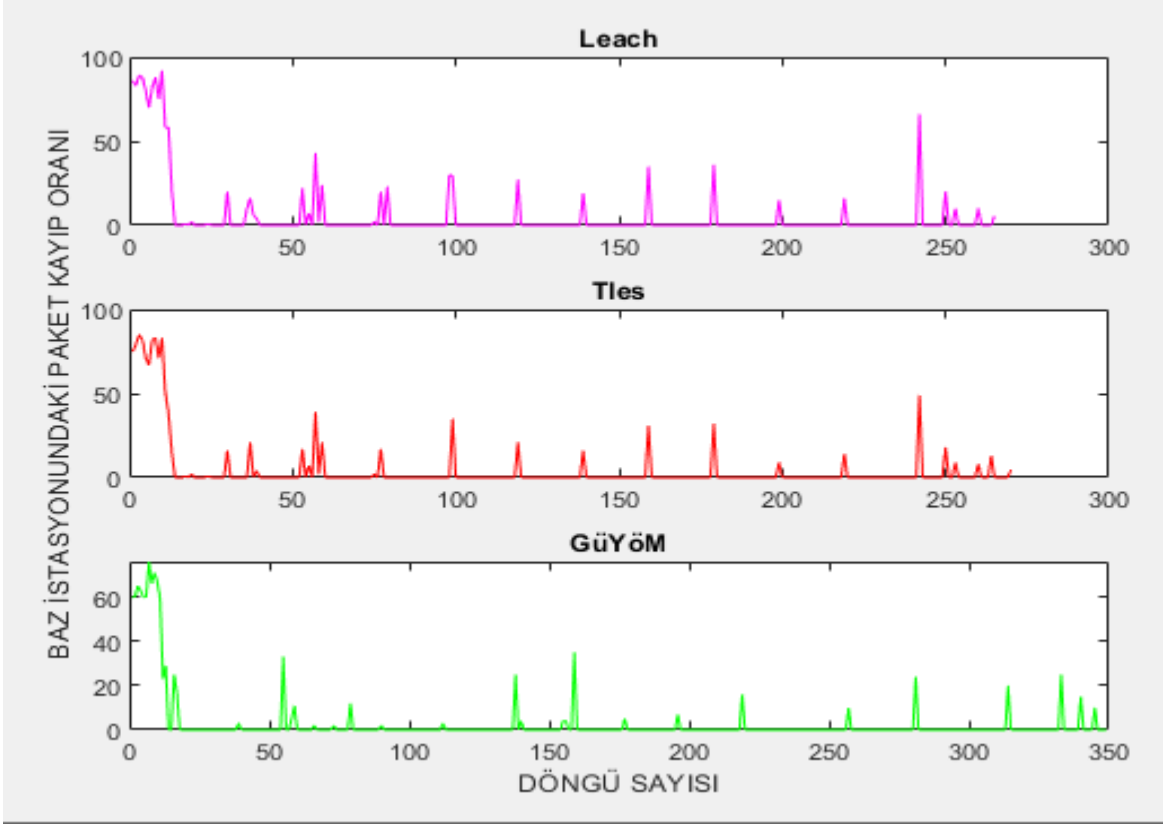
Şekil 6.2. Model 1 için her döngü yaşayan düğüm sayısı



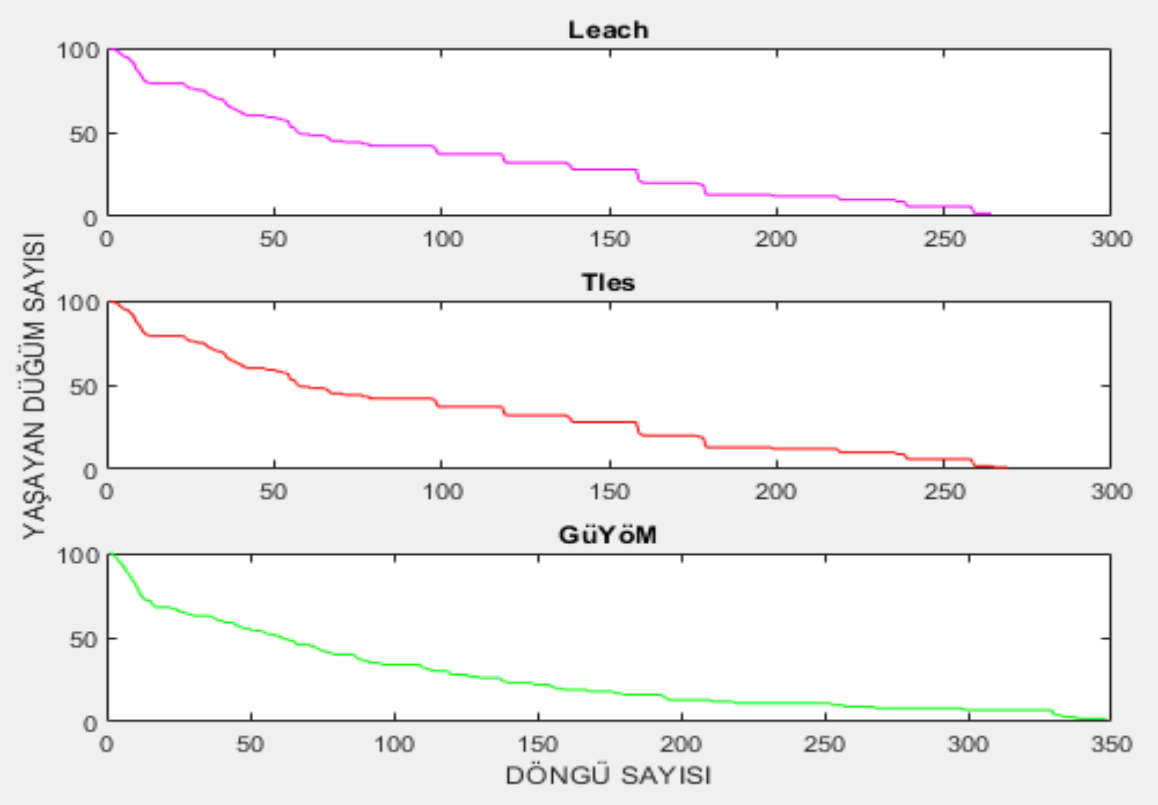
Şekil 6.3. Model 1 için her döngü ağda harcanan toplam enerji

6.2. Model 2'nin Performans Değerlendirmesi

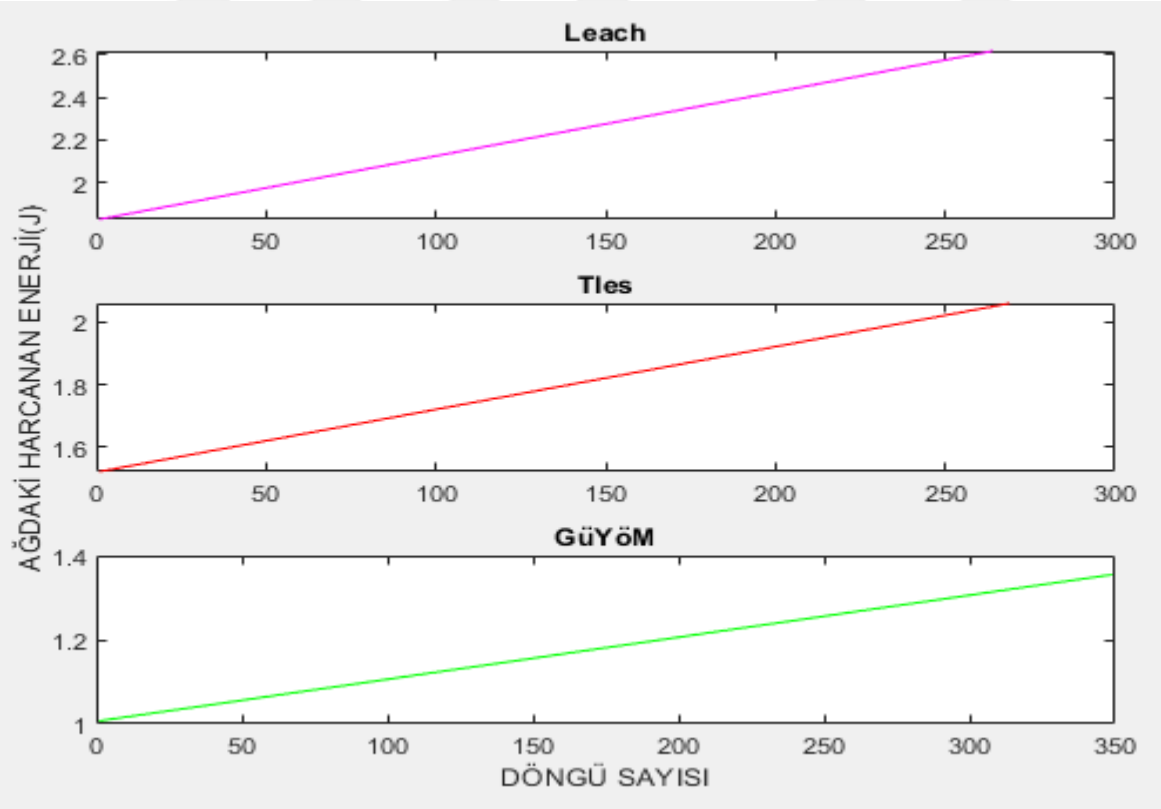
Bir önceki modelden farklı olarak saldırgan sayısı %20'ye çıkarılmıştır. Saldırgan sayısının artması ile tüm protokollerde baz istasyonuna ulaşan paket kayıp oranları artarken ağ yaşam süresi kısalmıştır. Yapılan ölçümlerde LEACH protokolünde %5,62; TLES protokolünde %5,57; önerilen protokolde olan GüYöM'de ise %3,08 oranında paket kayıpları tespit edilmiştir (Şekil 6.4.). LEACH protokolünün ağ yaşam süresi 264 döngü iken, bu değer TLES protokolünde 269, GüYöM'de ise 349 döngüdür (Şekil 6.5.). Sonuçlardan da görüldüğü üzere GüYöM, güvenli yol üzerinden paketleri baz istasyonuna ulaştırmada diğer protokollere göre daha başarılı olurken, bunu enerji verimli bir şekilde yaptığı için ağ yaşam süresini de uzatmıştır. Bunun nedeni düğümlerin enerjilerinin verimli kullanmasını sağlamasıdır. Şekil 6.6'da verilen harcanan enerji kıyaslamasında LEACH'in en fazla, GüYöM'ün ise en az enerji harcadığı tespit edilmiştir.



Şekil 6.4. Model 2 için her döngü baz istasyonunda gözlemlenen paket kayıp oranı



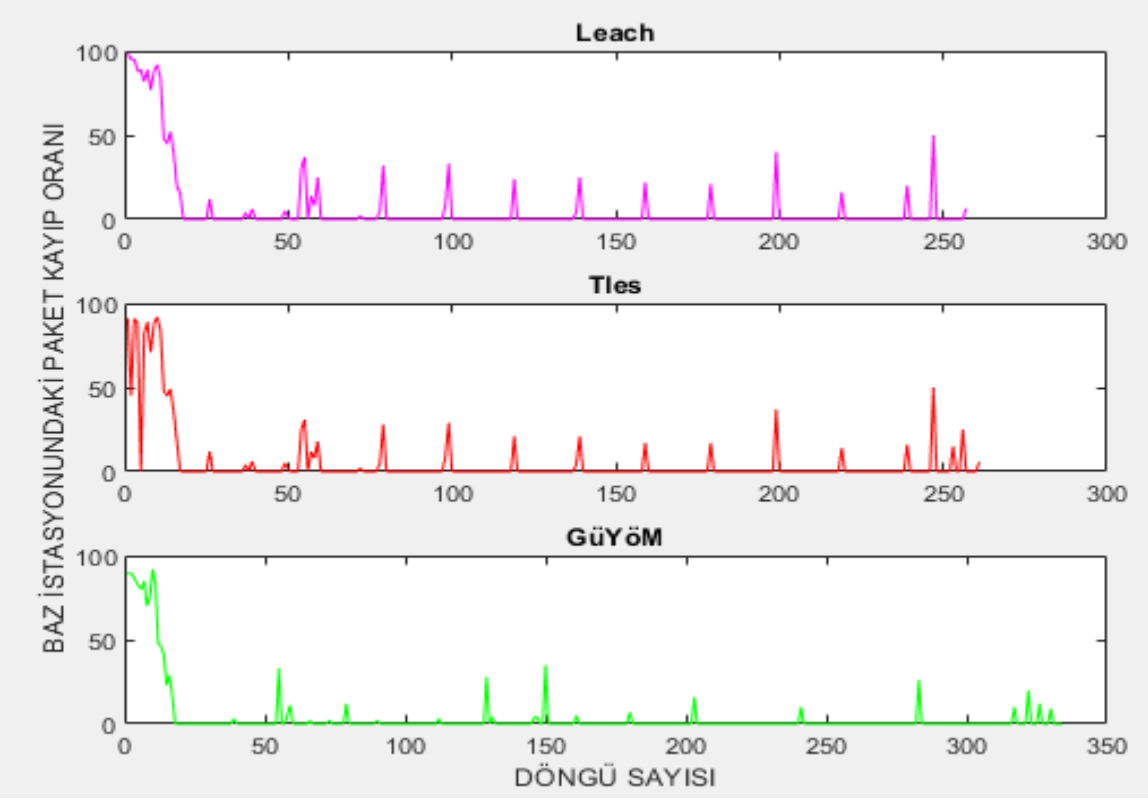
Şekil 6.5. Model 2 için her döngü yaşayan düğüm sayısı



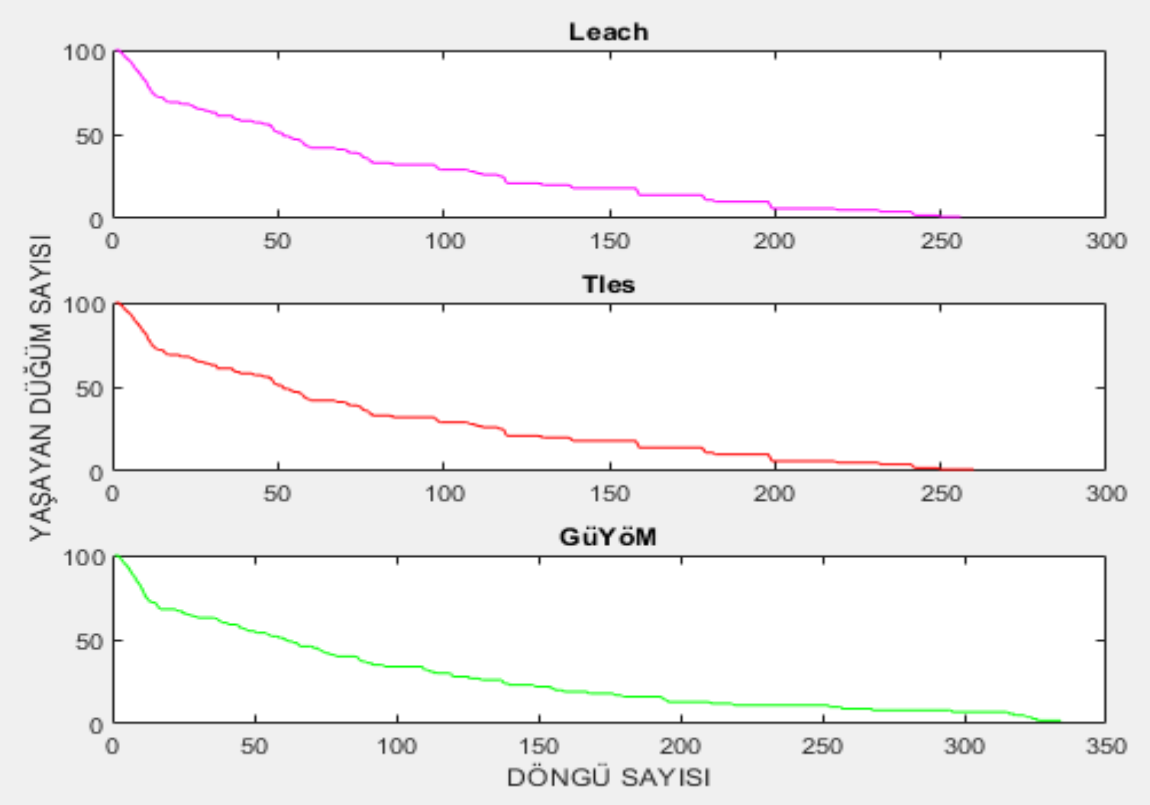
Şekil 6.6. Model 2 için her döngü ağda harcanan toplam enerji

6.3. Model 3'ün Performans Değerlendirmesi

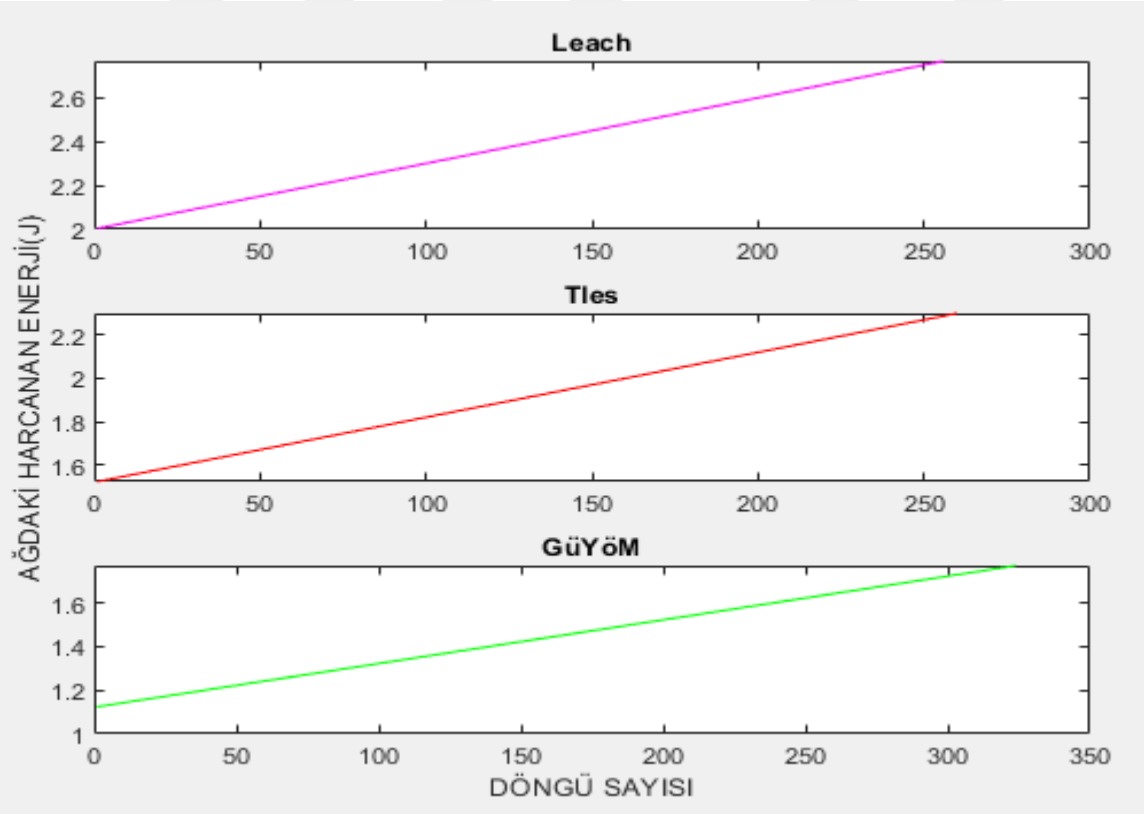
Model 1 ve Model 2'den farklı olarak saldırgan sayısı %30'ye çıkarılmıştır. Saldırgan sayısının artması ile tüm protokollerde baz istasyonuna ulaşan paket kayıp oranları artarken ağ yaşam süresi kısalmıştır. Yapılan ölçümlerde LEACH protokolünde %6,42; TLES protokolünde %5,94; önerilen protokolde olan GüYöM'de ise %4,15 oranında paket kayıpları tespit edilmiştir (Şekil 6.7.). LEACH protokolünün ağ yaşam süresi 255 döngü iken, bu değer TLES protokolünde 260, GüYöM'de ise 334 döngüdür (Şekil 6.8.). Sonuçlardan da görüldüğü üzere GüYöM, güvenli yol üzerinden paketleri baz istasyonuna ulaştırmada diğer protokollere göre daha başarılı olurken, bunu enerji verimli bir şekilde yaptığı için ağ yaşam süresini de uzatmıştır. Bunun nedeni düğümlerin enerjilerinin verimli kullanmasını sağlamasıdır. Şekil 6.9.'da verilen harcanan enerji kıyaslamasında LEACH'in en fazla, GüYöM'ün ise en az enerji harcadığı tespit edilmiştir.



Şekil 6.7. Model 3 için her döngü baz istasyonunda gözlemlenen paket kayıp oranı



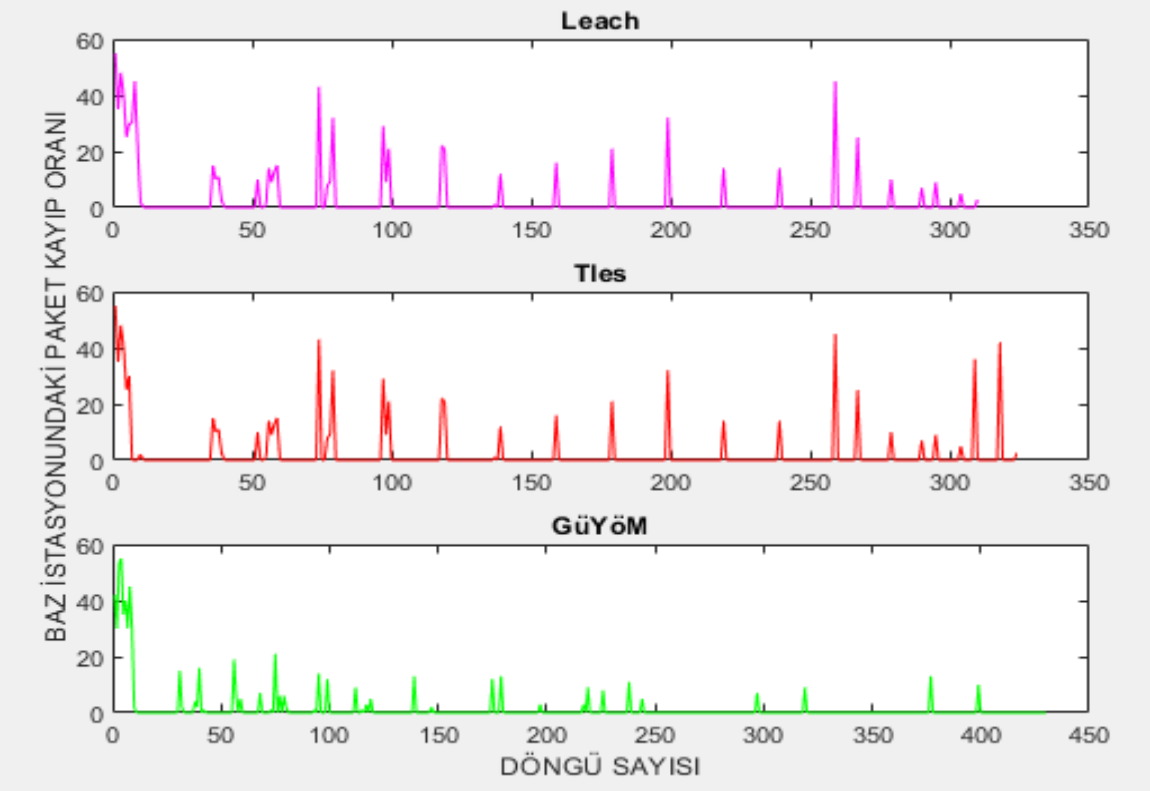
Şekil 6.8. Model 3 için her döngü yaşayan düğüm sayısı



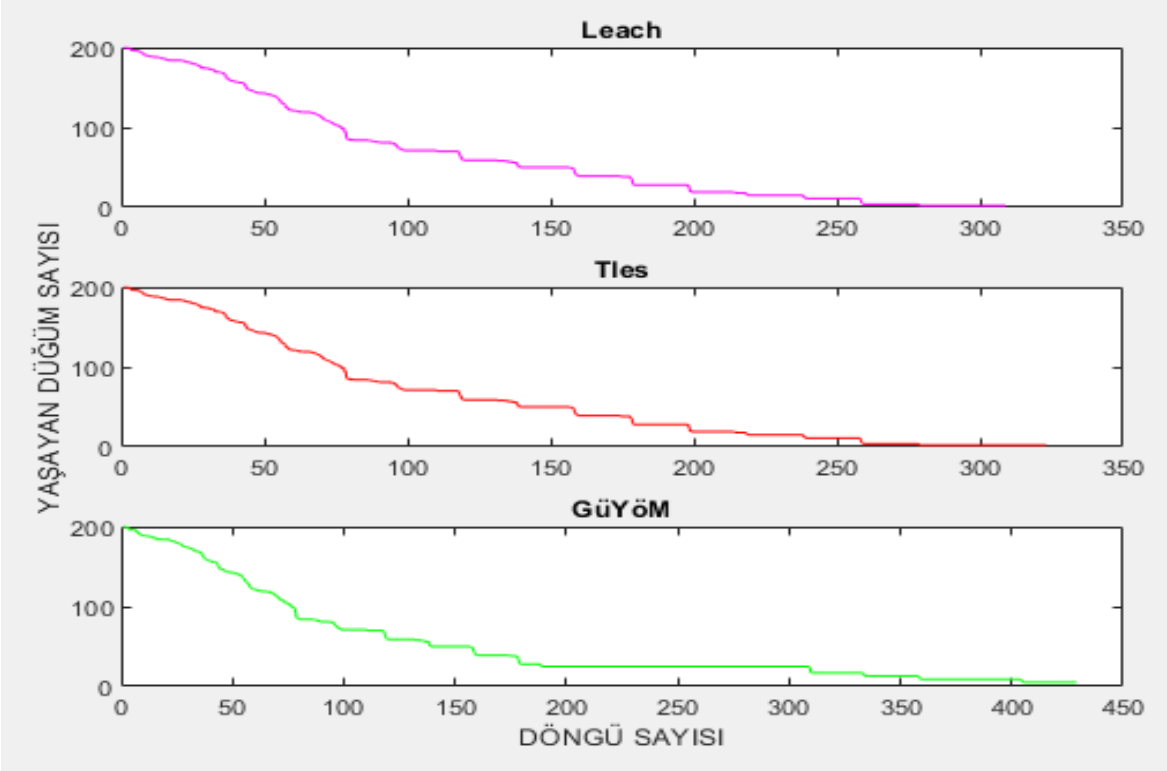
Şekil 6.9. Model 3 için her döngü ağda harcanan toplam enerji

6.4. Model 4'ün Performans Değerlendirmesi

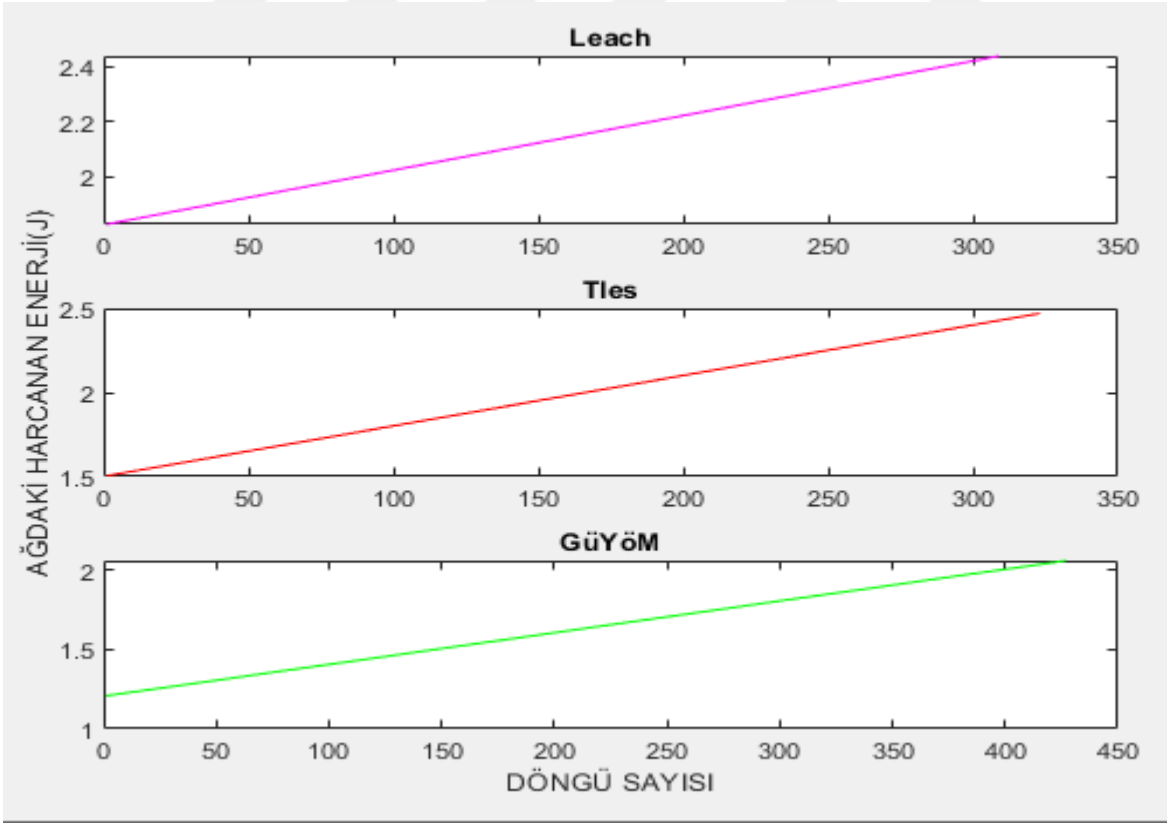
Daha önceki modellerden farklı olarak düğüm sayısı 2 katına çıkarılarak 200 düğüm yapılmıştır. Düğüm sayısının %10'u saldırgan düğüm olarak modellenmiş ve sonuçlar LEACH ve TLES algoritmaları ile kıyaslanmıştır. Aynı oranda saldırgan ve 100 düğüme sahip olan Model 1 ile kıyaslarsak, paket kayıp oranının azaldığı ve ağ yaşam süresinin uzadığı gözlemlenmiştir. Yapılan ölçümlerde LEACH protokolünde %2,71; TLES protokolünde %2,53; önerilen protokolde olan GüYöM' de ise %1,48 oranında paket kayıpları tespit edilmiştir (Şekil 6.10.). LEACH protokolünün ağ yaşam süresi 309 döngü iken, bu değer TLES protokolünde 323, GüYöM'de ise 431 döngüdür (Şekil 6.11.). Sonuçlardan da görüldüğü üzere GüYöM, güvenli yol üzerinden paketleri baz istasyonuna ulaştırmada diğer protokollere göre daha başarılı olurken, bunu enerji verimli bir şekilde yaptığı için ağ yaşam süresini de uzatmıştır. Bunun durumun nedeni düğümlerin enerjilerinin verimli kullanmasını sağlamasıdır. Şekil 6.12'de verilen harcanan enerji kıyaslamasında LEACH'in en fazla, GüYöM'ün ise en az enerji harcadığı tespit edilmiştir.



Şekil 6.10. Model 4 için her döngü baz istasyonunda gözlemlenen paket kayıp oranı



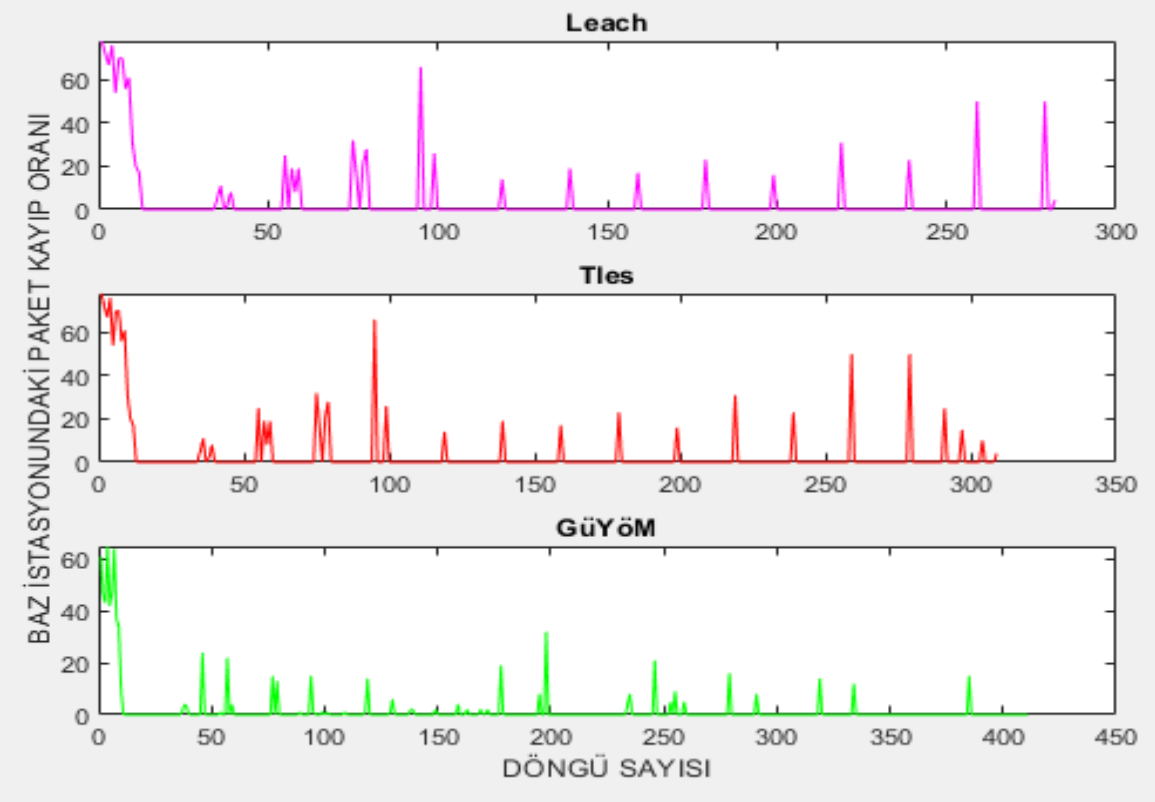
Şekil 6.11. Model 4 için her döngü yaşayan düğüm sayısı



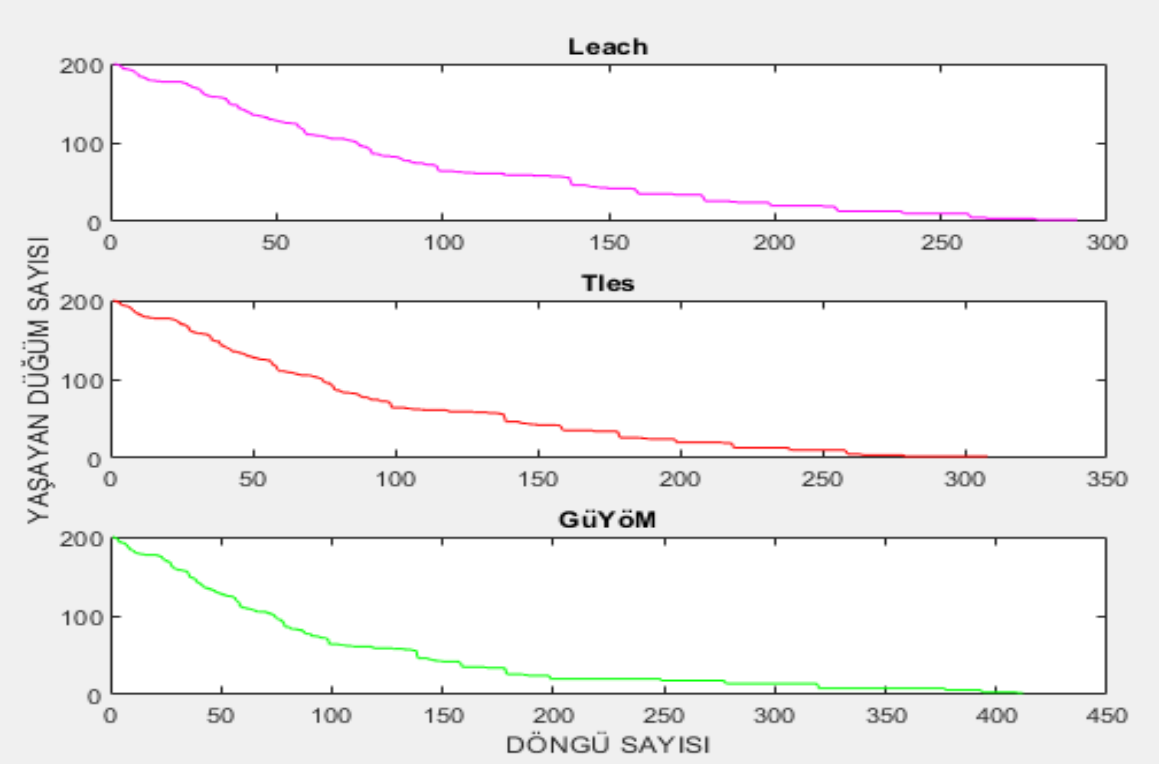
Şekil 6.12. Model 4 için her döngü ağda harcanan toplam enerji

6.5. Model 5'in Performans Değerlendirmesi

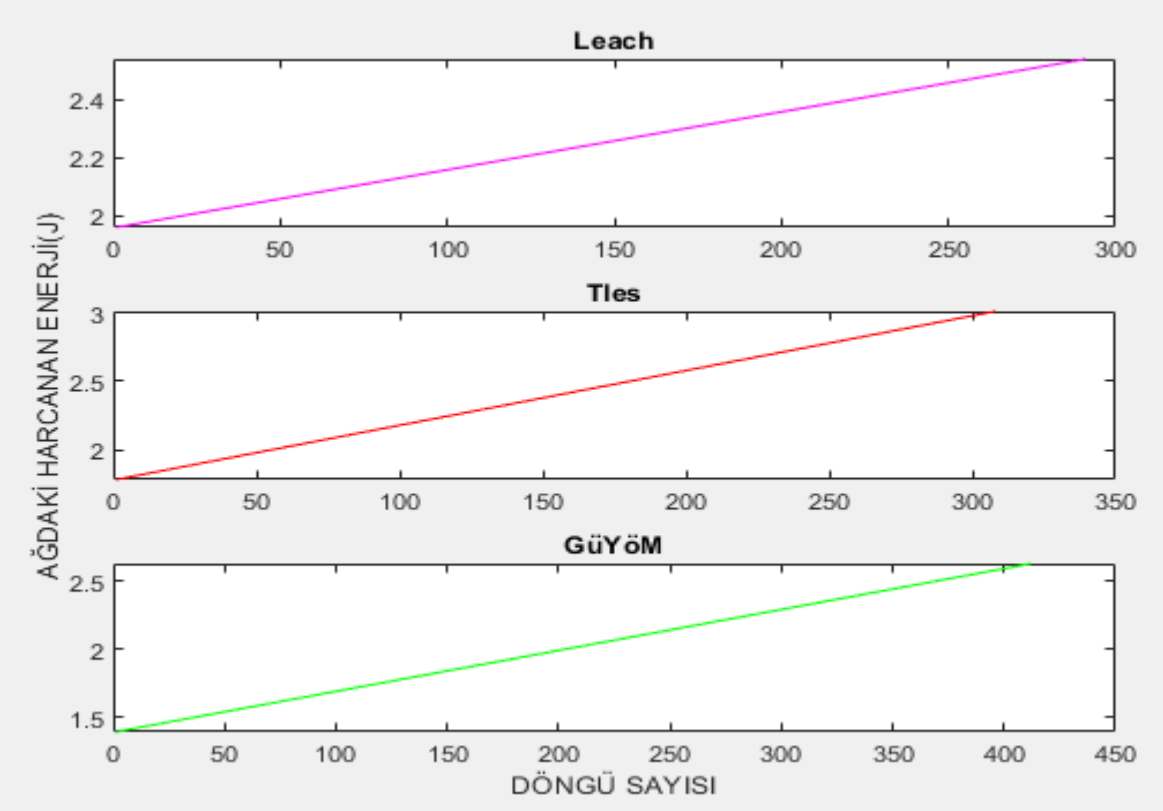
Bir önceki modelden farklı olarak saldırgan sayısı %20'ye çıkarılmıştır. Saldırgan sayısının artması ile tüm protokollerde baz istasyonuna ulaşan paket kayıp oranları artarken ağ yaşam süresi kısalmıştır. Aynı saldırgan oranı ve 100 düğüm ile modellenen Model 2 ile kıyasladığımızda, paket kayıp oranının azaldığı ve ağ yaşam süresinin arttığı gözlemlenmiştir. Yapılan ölçümlerde LEACH protokolünde %4,27; TLES protokolünde %4,06; önerilen protokolde olan GüYöM'de ise %1,87 oranında paket kayıpları tespit edilmiştir (Şekil 6.13.). LEACH protokolünün ağ yaşam süresi 291 döngü iken, bu değer TLES protokolünde 308, GüYöM'de ise 412 döngüdür (Şekil 6.14.). Sonuçlardan da görüldüğü üzere GüYöM, güvenli yol üzerinden paketleri baz istasyonuna ulaştırmada diğer protokollere göre daha başarılı olurken, bunu enerji verimli bir şekilde yaptığı için ağ yaşam süresini de uzatmıştır. Bunun nedeni düğümlerin enerjilerinin verimli kullanmasını sağlamasıdır. Şekil 6.15.'te verilen harcanan enerji kıyaslamasında LEACH'in en fazla, GüYöM'ün ise en az enerji harcadığı tespit edilmiştir.



Şekil 6.13. Model 5 için her döngü baz istasyonunda gözlemlenen paket kayıp oranı



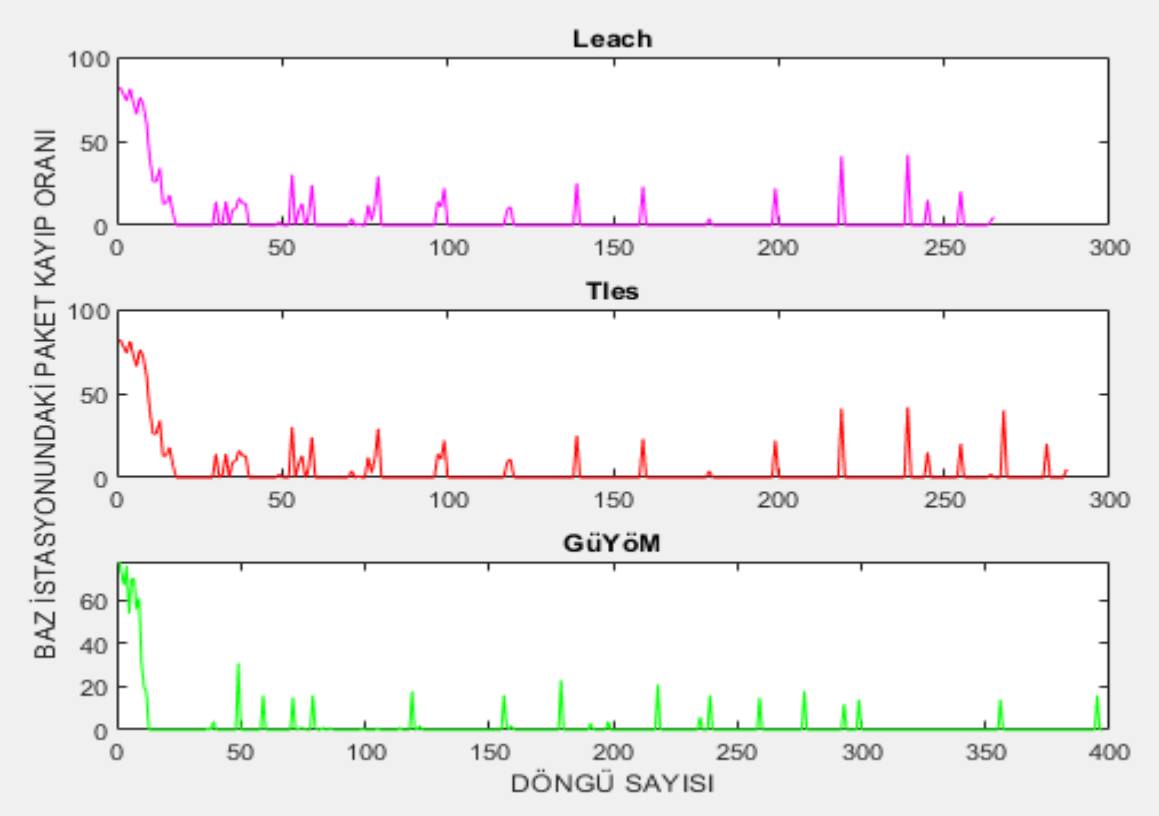
Şekil 6.14. Model 5 için her döngü yaşayan düğüm sayısı



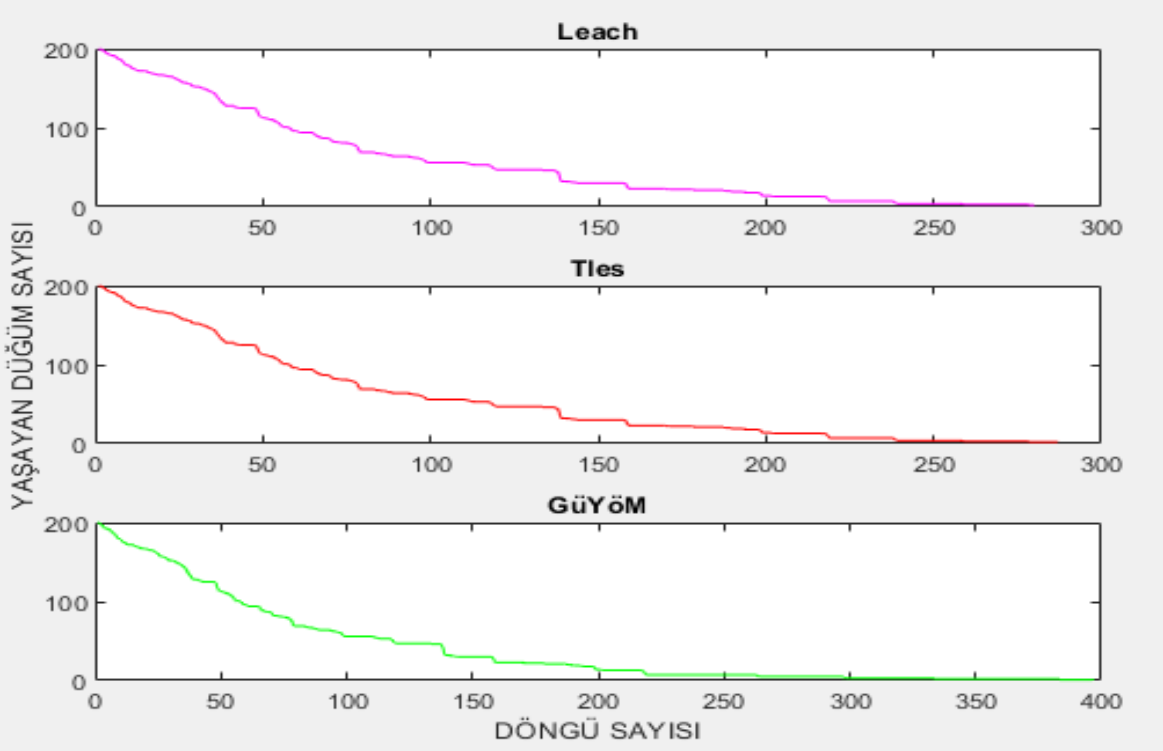
Şekil 6.15. Model 5 için her döngü ağda harcanan toplam enerji

6.6. Model 6'nın Performans Değerlendirmesi

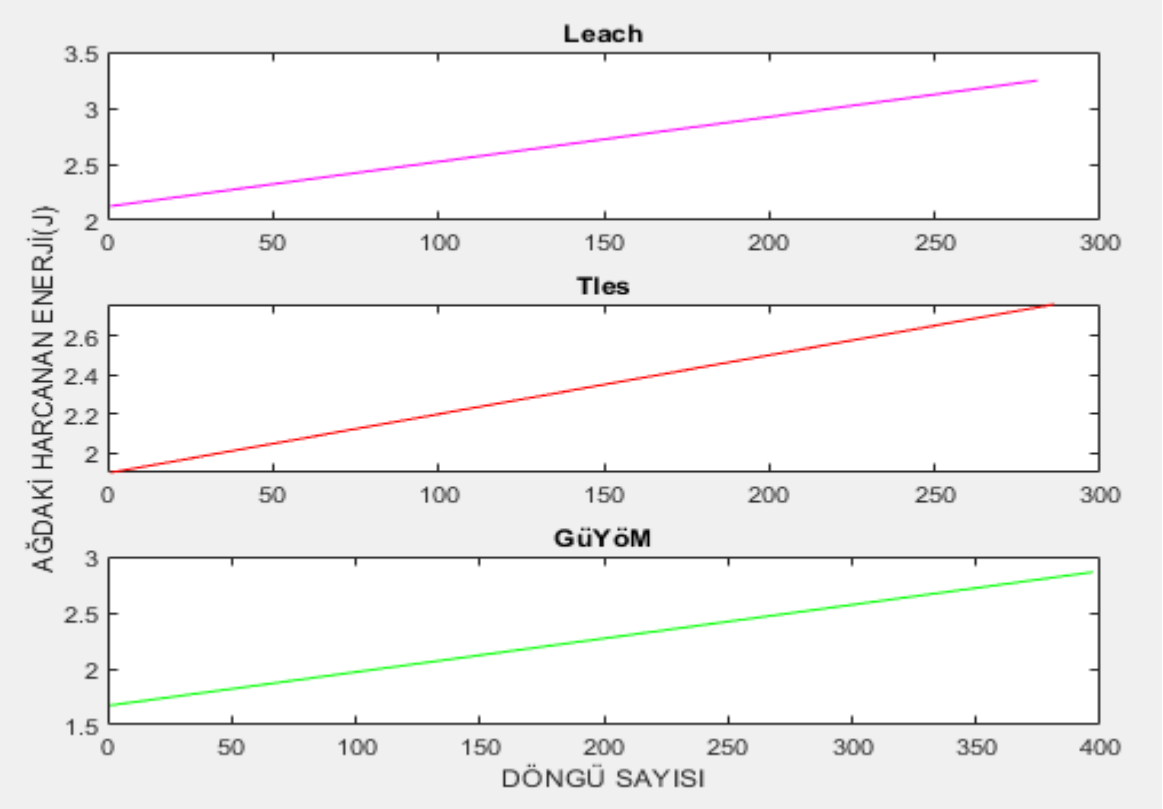
Model 4 ve model 5'ten farklı olarak saldırgan sayısı %30'ye çıkarılmıştır. Saldırgan sayısının artması ile tüm protokollerde baz istasyonuna ulaşan paket kayıp oranları artarken ağ yaşam süresi kısalmıştır. Yapılan ölçümlerde LEACH protokolünde %5,05; TLES protokolünde %4,87; önerilen protokolde olan GüYöM'de ise %2,43 oranında paket kayıpları tespit edilmiştir (Şekil 6.7.). LEACH protokolünün ağ yaşam süresi 280 döngü iken, bu değer TLES protokolünde 287, GüYöM'de ise 397 döngüdür (Şekil 6.8.). Sonuçlardan da görüldüğü üzere GüYöM, güvenli yol üzerinden paketleri baz istasyonuna ulaştırmada diğer protokollere göre daha başarılı olurken, bunu enerji verimli bir şekilde yaptığı için ağ yaşam süresini de uzatmıştır. Bunun nedeni düğümlerin enerjilerinin verimli kullanmasını sağlamasıdır. Şekil 6.9.'da verilen harcanan enerji kıyaslamasında LEACH'in en fazla, GüYöM'ün ise en az enerji harcadığı tespit edilmiştir.



Şekil 6.16. Model 6 için her döngü baz istasyonunda gözlemlenen paket kayıp oranı



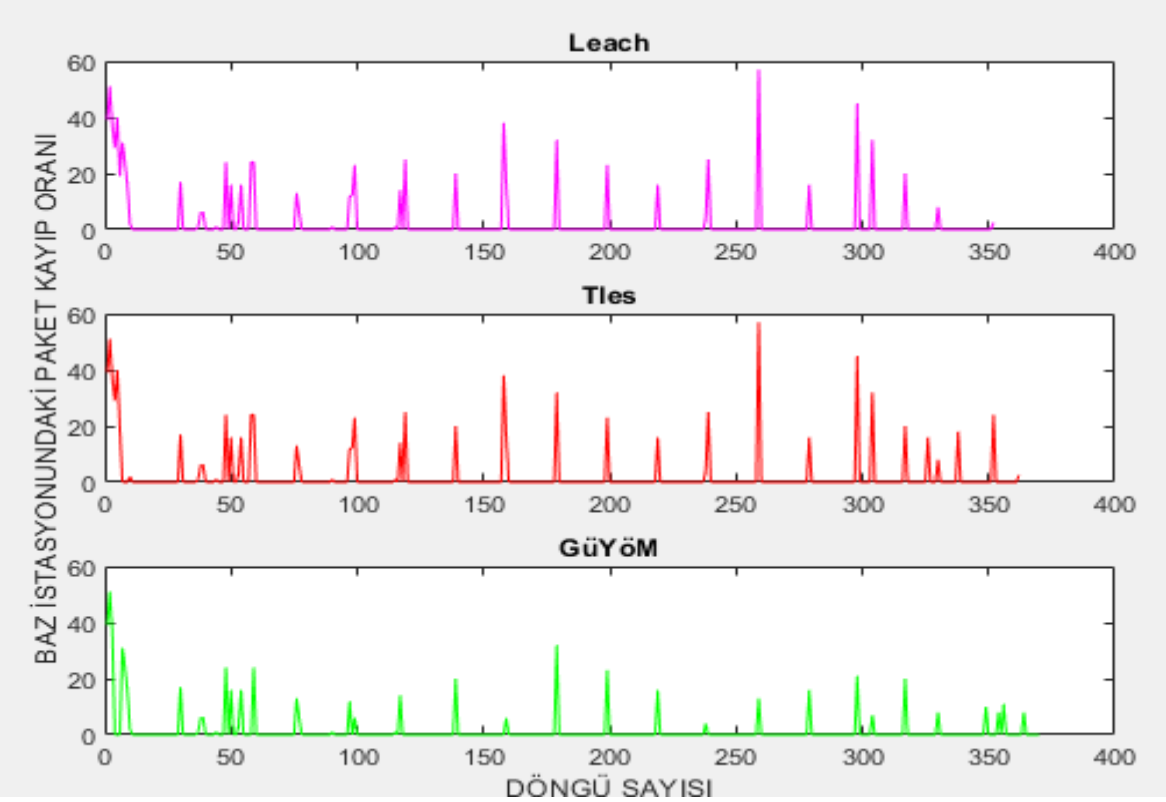
Şekil 6.17. Model 6 için her döngü yaşayan düğüm sayısı



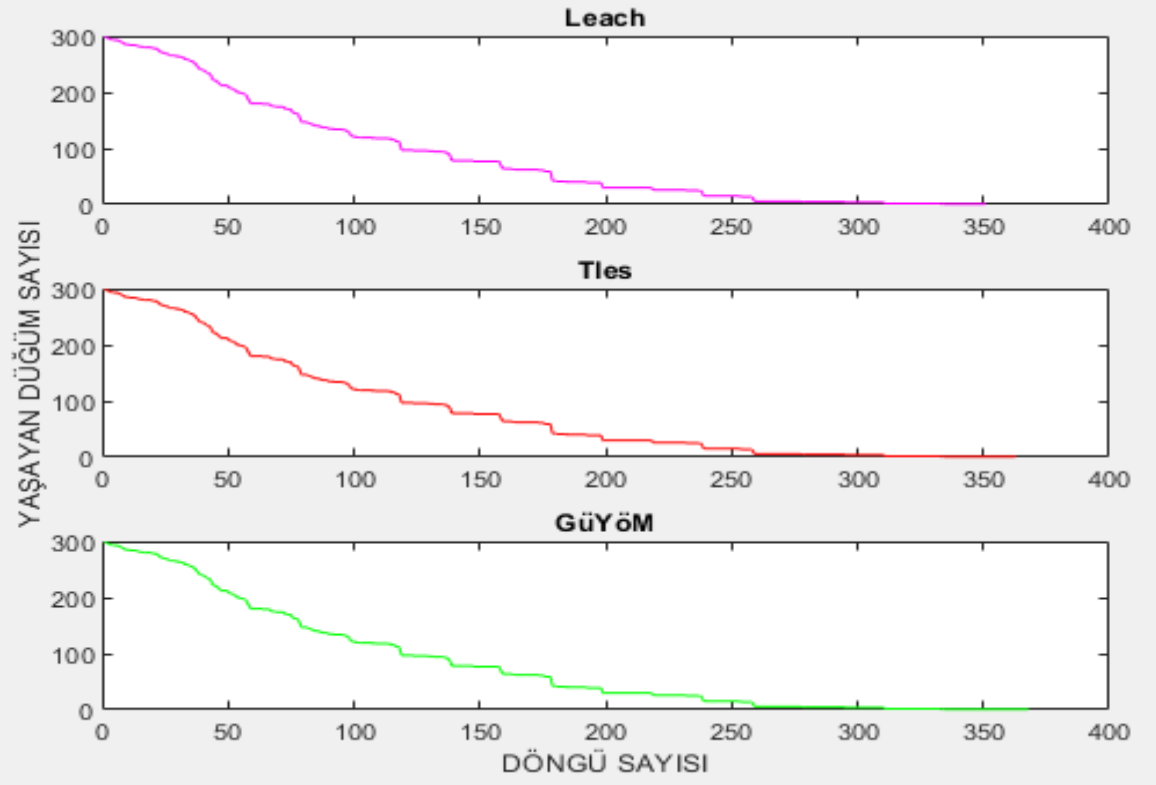
Şekil 6.18. Model 6 için her döngü ağda harcanan toplam enerji

6.7. Model 7'nin Performans Değerlendirmesi

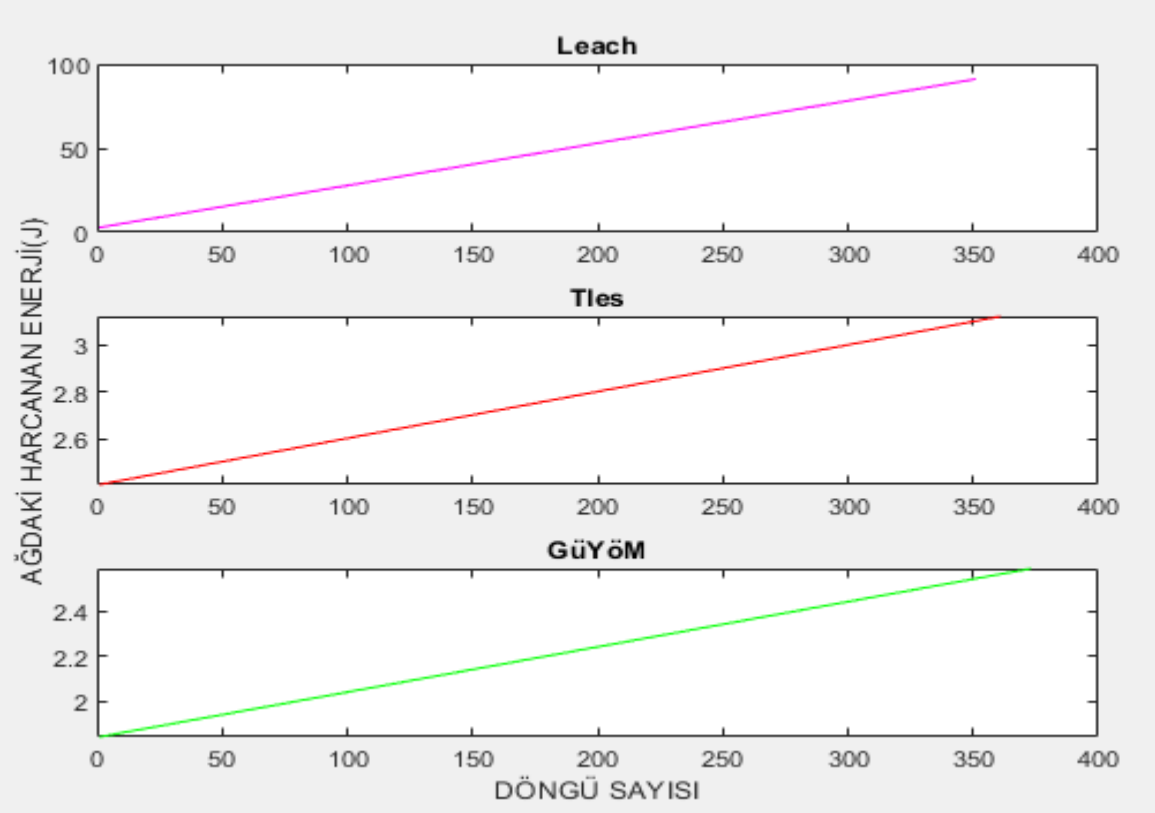
Daha önceki modellerimizden farklı olarak düğüm sayısı 300 düğüm yapılmıştır. Düğüm sayısının %10'u saldırgan düğüm olarak modellenmiş ve sonuçlar LEACH ve TLES algoritmaları ile kıyaslanmıştır. Performans ölçütü olarak ağda harcanan enerji, baz istasyonundaki paket kayıp oranı ve her döngü yaşayan düğüm sayısı olmak üzere 3 farklı parametre kullanılmıştır. Yapılan ölçümlerde LEACH protokolünde %2,52; TLES protokolünde %2,41; önerilen protokolde olan GüYöM'de ise %1,58 oranında paket kayıpları tespit edilmiştir (Şekil 6.19.). LEACH protokolünün ağ yaşam süresi 351 döngü iken, bu değer TLES protokolünde 363, GüYöM'de ise 371 döngüdür (Şekil 6.20.). Sonuçlardan da görüldüğü üzere GüYöM, güvenli yol üzerinden paketleri baz istasyonuna ulaştırmada diğer protokollere göre daha başarılı olurken, bunu enerji verimli bir şekilde yaptığı için ağ yaşam süresini de uzatmıştır. Bu durumun nedeni düğümlerin enerjilerinin verimli kullanmasını sağlamasıdır. Şekil 6.21.'de verilen harcanan enerji kıyaslamasında LEACH'in en fazla, GüYöM'ün ise en az enerji harcadığı tespit edilmiştir.



Şekil 6.19. Model 7 için her döngü baz istasyonunda gözlemlenen paket kayıp oranı



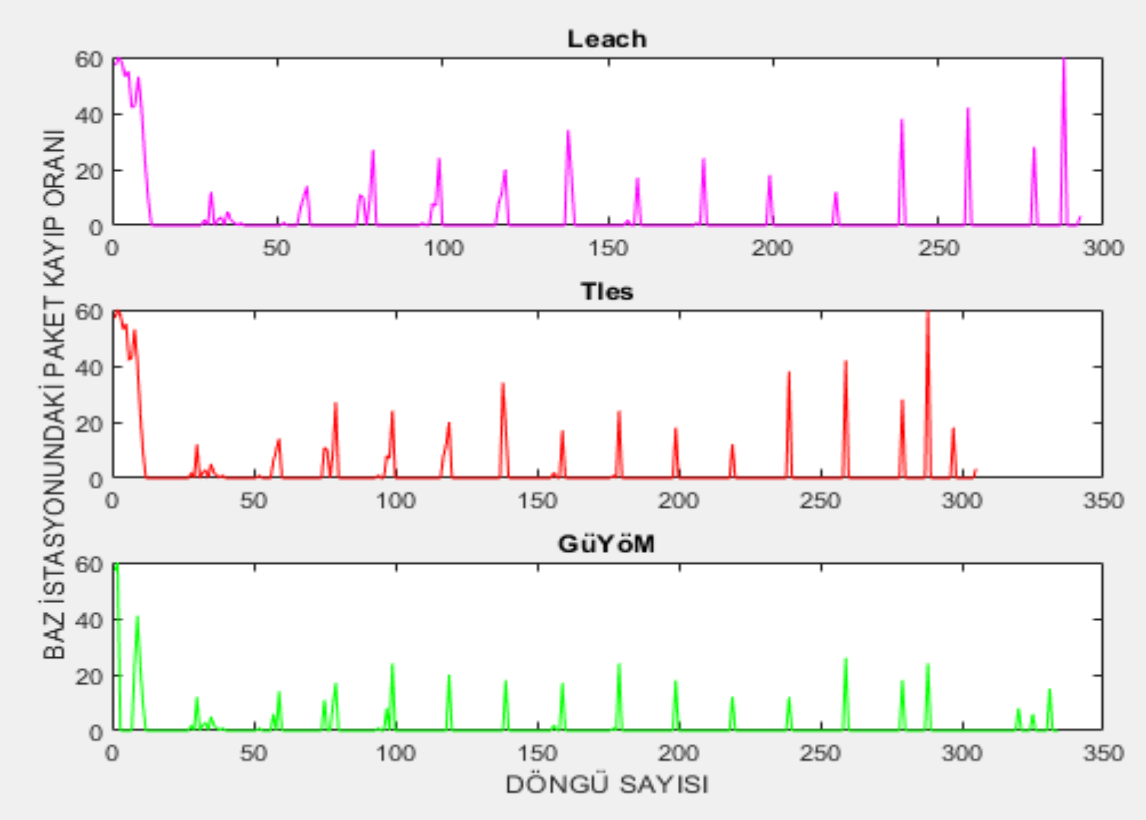
Şekil 6.20. Model 7 için her döngü yaşayan düğüm sayısı



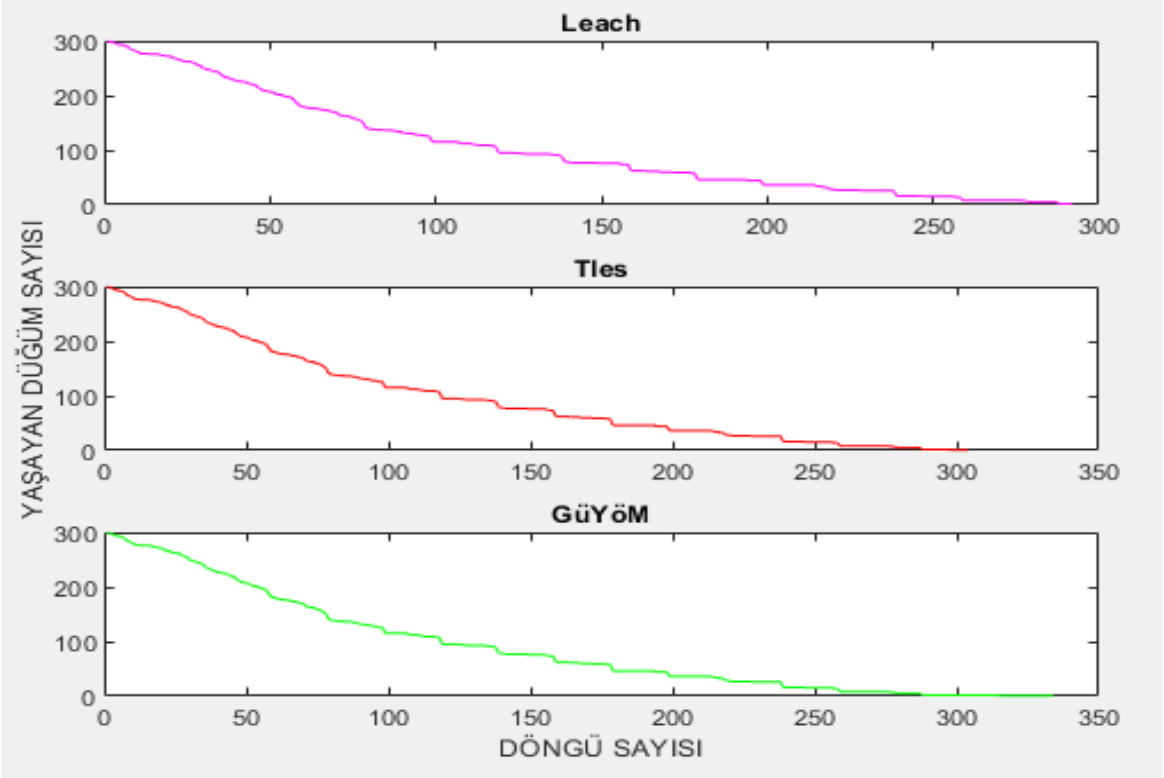
Şekil 6.21. Model 7 için her döngü ağda harcanan toplam enerji

6.8. Model 8’ in Performans Değerlendirmesi

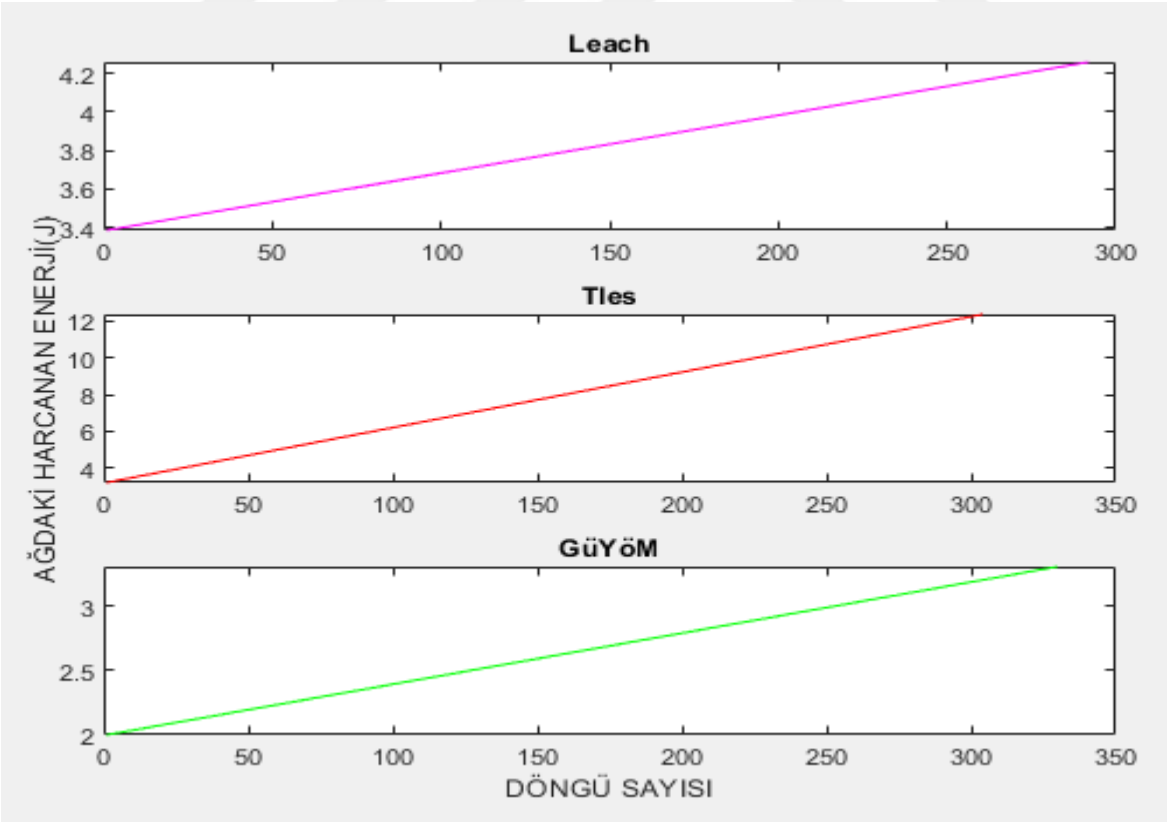
Bir önceki modelden farklı olarak saldırgan sayısı %20’ye çıkarılmıştır. Saldırgan sayısının artması ile tüm protokollerde baz istasyonuna ulaşan paket kayıp oranları artarken ağ yaşam süresi kısalmıştır. Aynı oranda saldırgana sahip ancak düğüm sayıları sırasıyla 100 düğüm ve 200 düğüm olan Model 2 ve Model 5 ile kıyasladığımızda, paket kayıp oranının azaldığı, ağ yaşam süresinin arttığı gözlemlenmiştir. Yapılan ölçümlerde LEACH protokolünde %3,36; TLES protokolünde %3,29; önerilen protokolde olan GüYöM’ de ise %1,65 oranında paket kayıpları tespit edilmiştir (Şekil 6.22.). LEACH protokolünün ağ yaşam süresi 292 döngü iken, bu değer TLES protokolünde 304, GüYöM’ de ise 334 döngüdür (Şekil 6.23.). Sonuçlardan da görüldüğü üzere GüYöM, güvenli yol üzerinden paketleri baz istasyonuna ulaştırmada diğer protokollere göre daha başarılı olurken, bunu enerji verimli bir şekilde yaptığı için ağ yaşam süresini de uzatmıştır. Bu durumun nedeni düğümlerin enerjilerinin verimli kullanmasını sağlamasıdır. Şekil 6.24.’de verilen harcanan enerji kıyaslamasında LEACH’in en fazla, GüYöM’ün ise en az enerji harcadığı tespit edilmiştir.



Şekil 6.22. Model 8 için her döngü baz istasyonunda gözlemlenen paket kayıp oranı



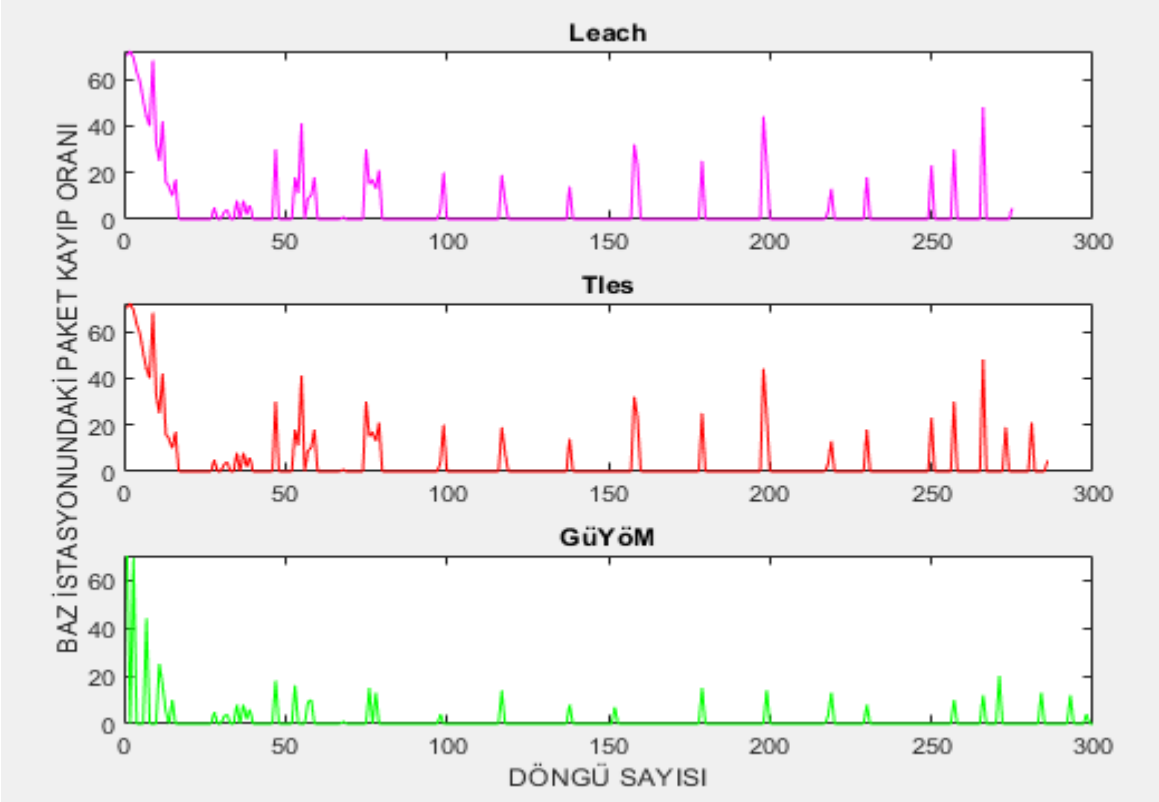
Şekil 6.23. Model 8 için her döngü yaşayan düğüm sayısı



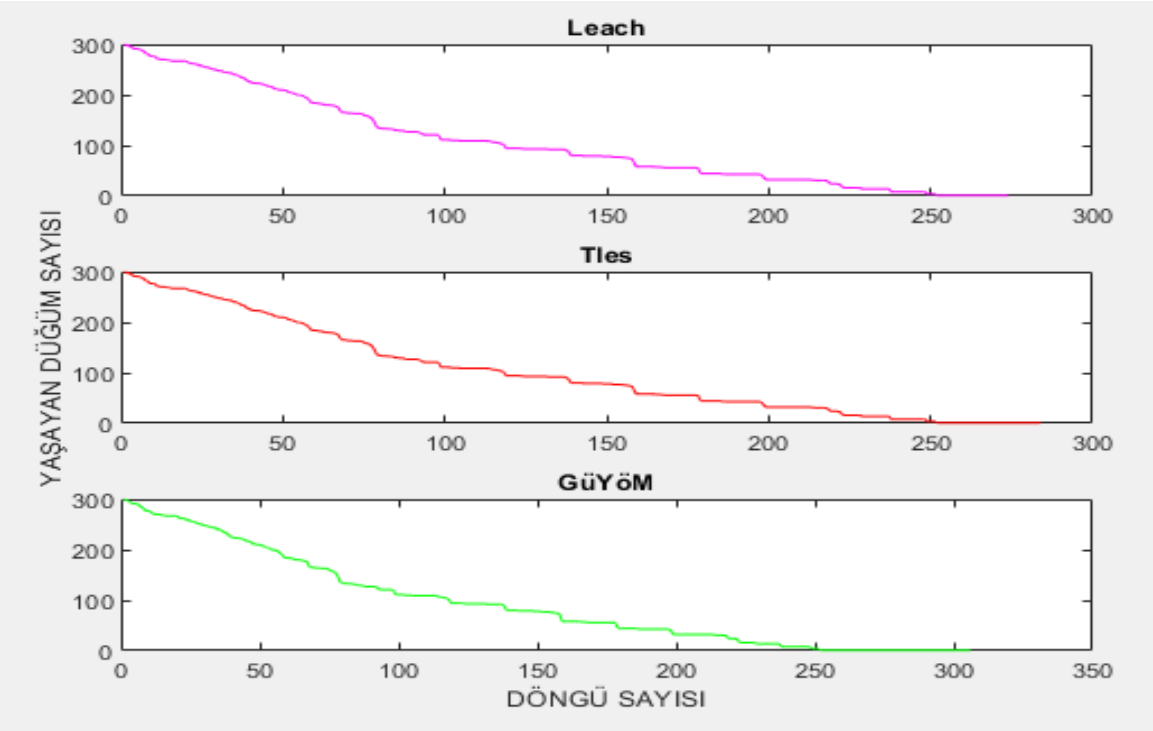
Şekil 6.24. Model 8 için her döngü ağda harcanan toplam enerji

6.9. Model 9’ un Performans Değerlendirmesi

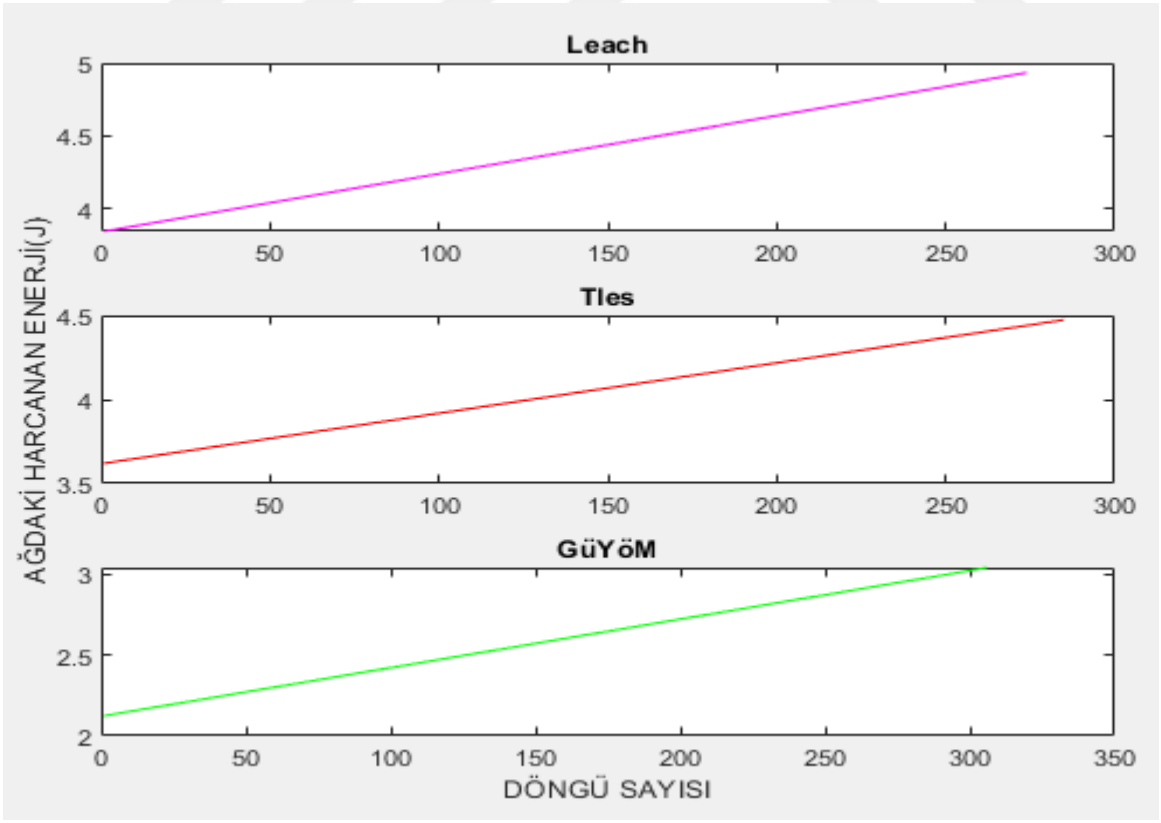
Model 7 ve Model 8’den farklı olarak saldırgan sayısı %30’a çıkarılmıştır. Saldırgan sayısının artması ile tüm protokollerde baz istasyonuna ulaşan paket kayıp oranları artarken ağ yaşam süresi kısalmıştır. Aynı oranda saldırgana sahip ancak düğüm sayıları sırasıyla 100 düğüm ve 200 düğüm olan Model 3 ve Model 6 ile kıyasladığımızda, paket kayıp oranının azaldığı, ağ yaşam süresinin arttığı gözlemlenmiştir. Yapılan ölçümlerde LEACH protokolünde %4,78; TLES protokolünde %4,65; önerilen protokolde olan GüYöM’de ise %1,71 oranında paket kayıpları tespit edilmiştir (Şekil 6.25.). LEACH protokolünün ağ yaşam süresi 274 döngü iken, bu değer TLES protokolünde 284, GüYöM’de ise 306 döngüdür (Şekil 6.26.). Sonuçlardan da görüldüğü üzere GüYöM, güvenli yol üzerinden paketleri baz istasyonuna ulaştırmada diğer protokollere göre daha başarılı olurken, bunu enerji verimli bir şekilde yaptığı için ağ yaşam süresini de uzatmıştır. Bunun nedeni düğümlerin enerjilerinin verimli kullanmasını sağlamasıdır. Şekil 6.27’de verilen harcanan enerji kıyaslamasında LEACH’in en fazla, GüYöM’ün ise en az enerji harcadığı tespit edilmiştir.



Şekil 6.25. Model 9 için her döngü baz istasyonunda gözlemlenen paket kayıp oranı



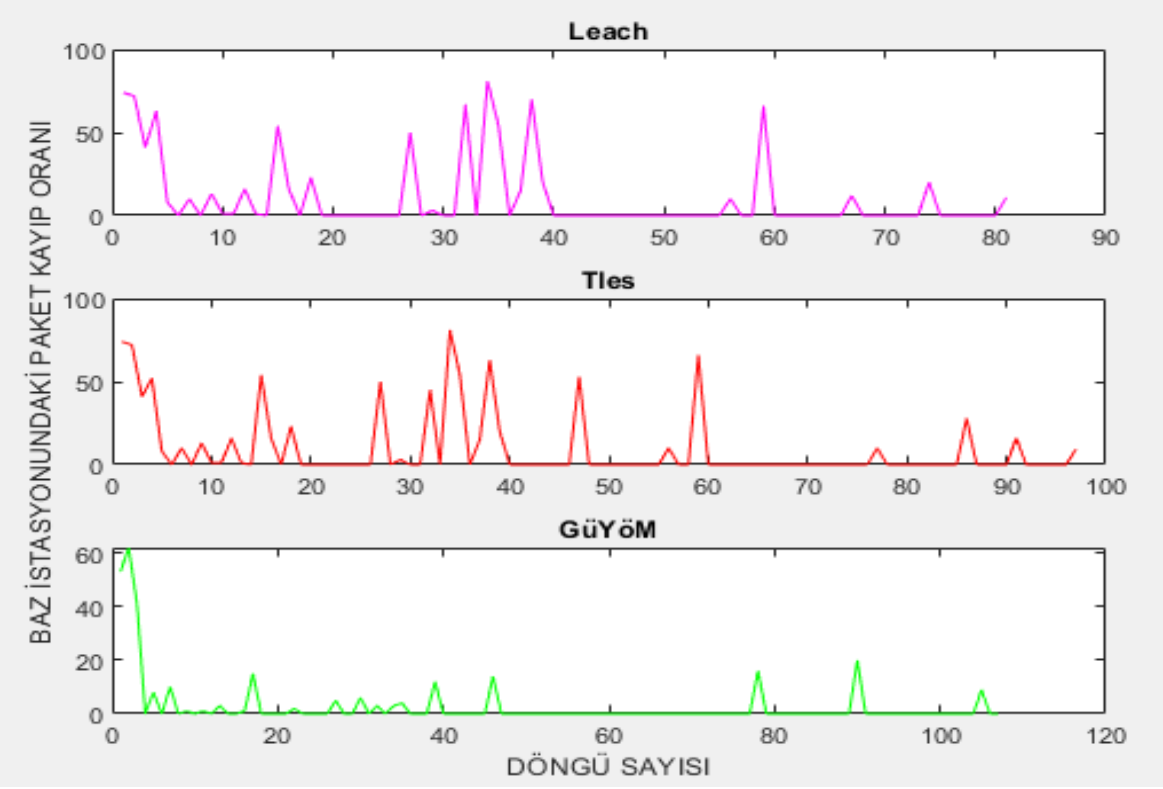
Şekil 6.26. Model 9 için her döngü yaşayan düğüm sayısı



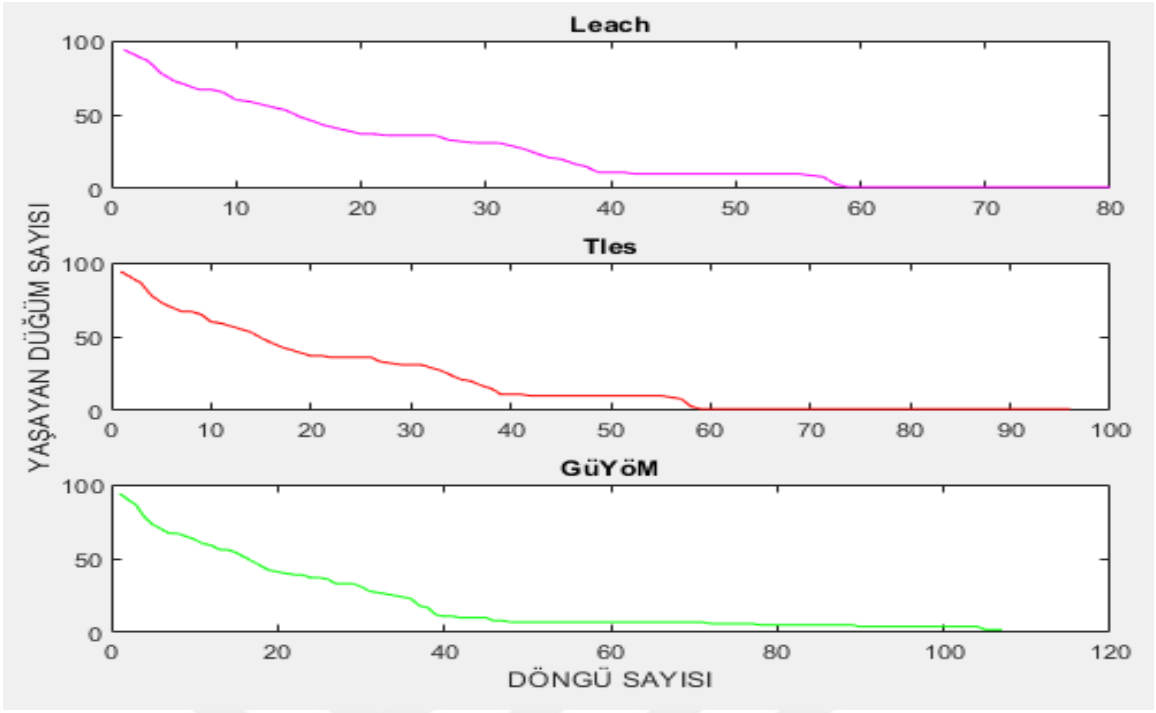
Şekil 6.27. Model 9 için her döngü ağda harcanan toplam enerji

6.10. Model 10’ un Performans Değerlendirmesi

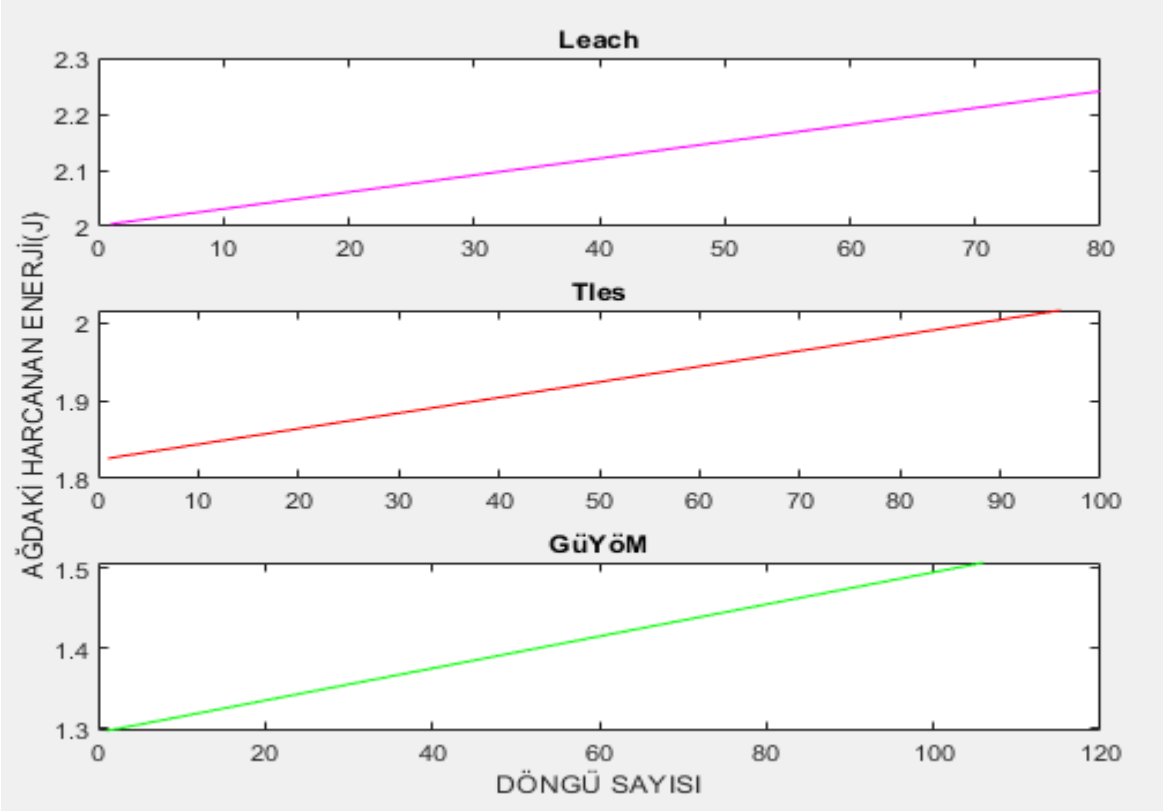
Daha önceki modellerden farklı olarak; ağ alanı 400x400’lük bir alandan, 600x600’ lük bir alan olacak şekilde arttırılmıştır. Modellenen KAA sisteminde 100 düğüm bulunmaktadır. Düğüm sayısının %10’u saldırgan düğüm olarak modellenmiş ve sonuçlar LEACH ve TLES algoritmaları ile kıyaslanmıştır. Yapılan ölçümlerde LEACH protokolünde %10,76; TLES protokolünde %9,33; önerilen protokolde olan GüYöM’de ise %2,67 oranında paket kayıpları tespit edilmiştir (Şekil 6.28.). LEACH protokolünün ağ yaşam süresi 80 döngü iken, bu değer TLES protokolünde 96, GüYöM’de ise 108 döngüdür (Şekil 6.29). Daha önceki modellerle kıyaslandığında, farklı olarak ağ alanının artması nedeniyle, yaşayan düğüm sayısında genel bir azalma gözlemlenmiştir. Bunun nedeni düğümlerin daha uzak mesafede iletişim kurmak zorunda olmaları ve buna bağlı olarak enerjilerini daha çabuk tüketmeleridir. Sonuçlardan da görüldüğü üzere GüYöM, güvenli yol üzerinden paketleri baz istasyonuna ulaştırmada diğer protokollere göre daha başarılı olurken, bunu enerji verimli bir şekilde yaptığı için ağ yaşam süresini de uzatmıştır. Şekil 6.30’da verilen harcanan enerji kıyaslamasında LEACH’in en fazla, GüYöM’ün ise en az enerji harcadığı tespit edilmiştir.



Şekil 6.28. Model 10 için her döngü baz istasyonunda gözlemlenen paket kayıp oranı



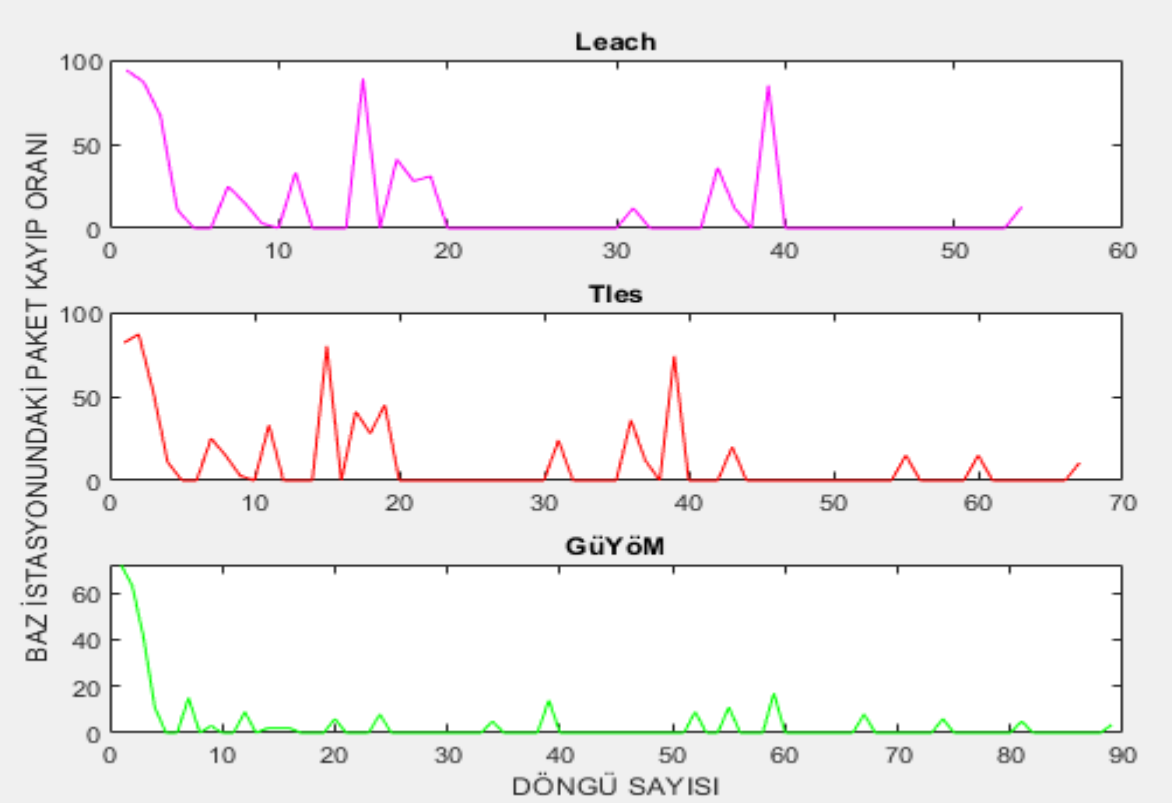
Şekil 6.29. Model 10 için her döngü yaşayan düğüm sayısı



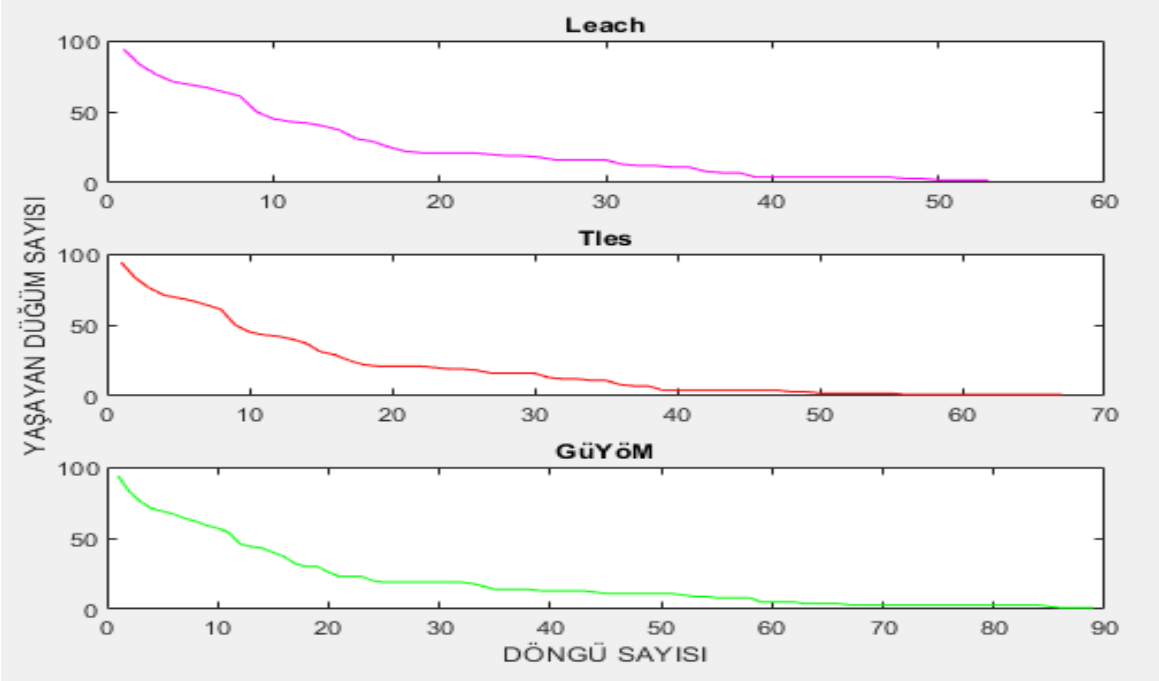
Şekil 6.30. Model 10 için her döngü ağda harcanan toplam enerji

6.11. Model 11' in Performans Değerlendirmesi

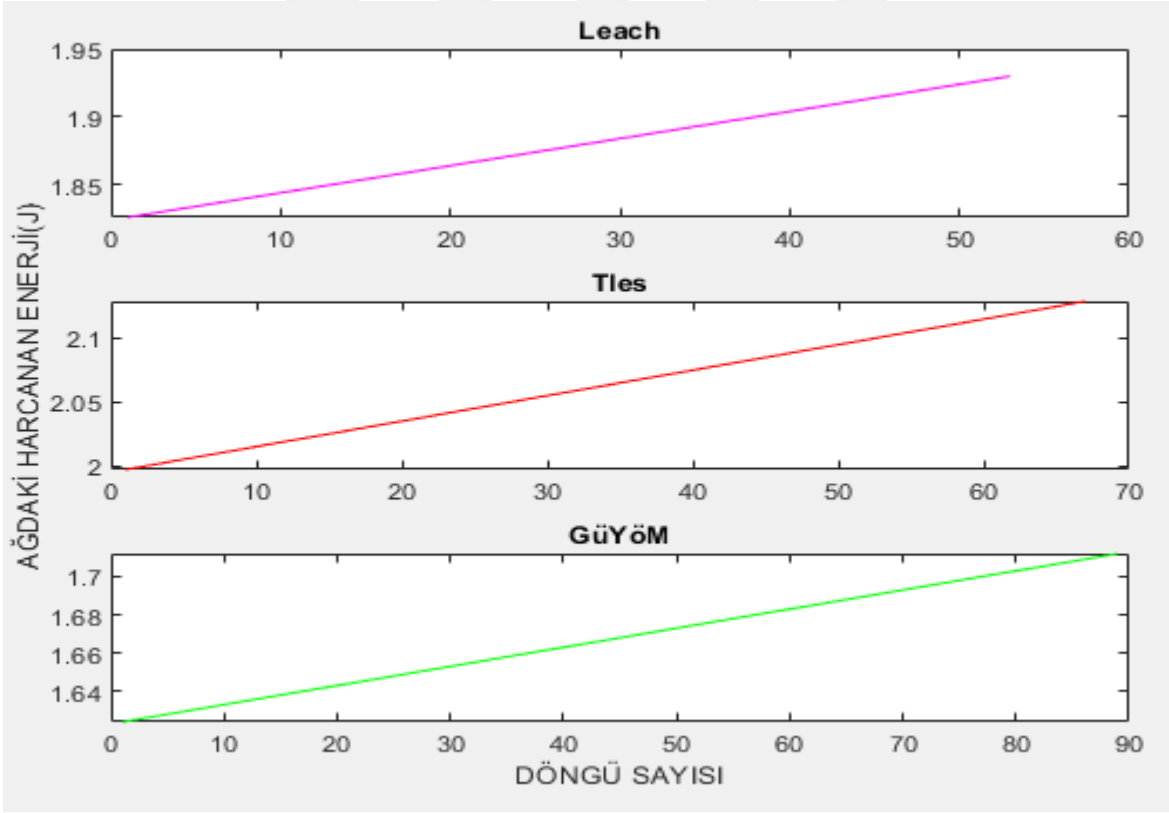
Bir önceki modelden farklı olarak saldırgan sayısı %20'ye çıkarılmıştır. Saldırgan sayısının artması ile tüm protokollerde baz istasyonuna ulaşan paket kayıp oranları artarken ağ yaşam süresi kısalmıştır. Yapılan ölçümlerde LEACH protokolünde %12,62; TLES protokolünde %10,59; önerilen protokolde olan GüYöM' de ise %3,51 oranında paket kayıpları tespit edilmiştir (Şekil 6.31). LEACH protokolünün ağ yaşam süresi 53 döngü iken, bu değer TLES protokolünde 67, GüYöM' de ise 89 döngüdür (Şekil 6.32). Sonuçlardan da görüldüğü üzere GüYöM, güvenli yol üzerinden paketleri baz istasyonuna ulaştırmada diğer protokollere göre daha başarılı olurken, bunu enerji verimli bir şekilde yaptığı için ağ yaşam süresini de uzatmıştır. Şekil 6.33'de verilen harcanan enerji kıyaslamasında LEACH'in en fazla, GüYöM'ün ise en az enerji harcadığı tespit edilmiştir.



Şekil 6.31. Model 11 için her döngü baz istasyonunda gözlemlenen paket kayıp oranı



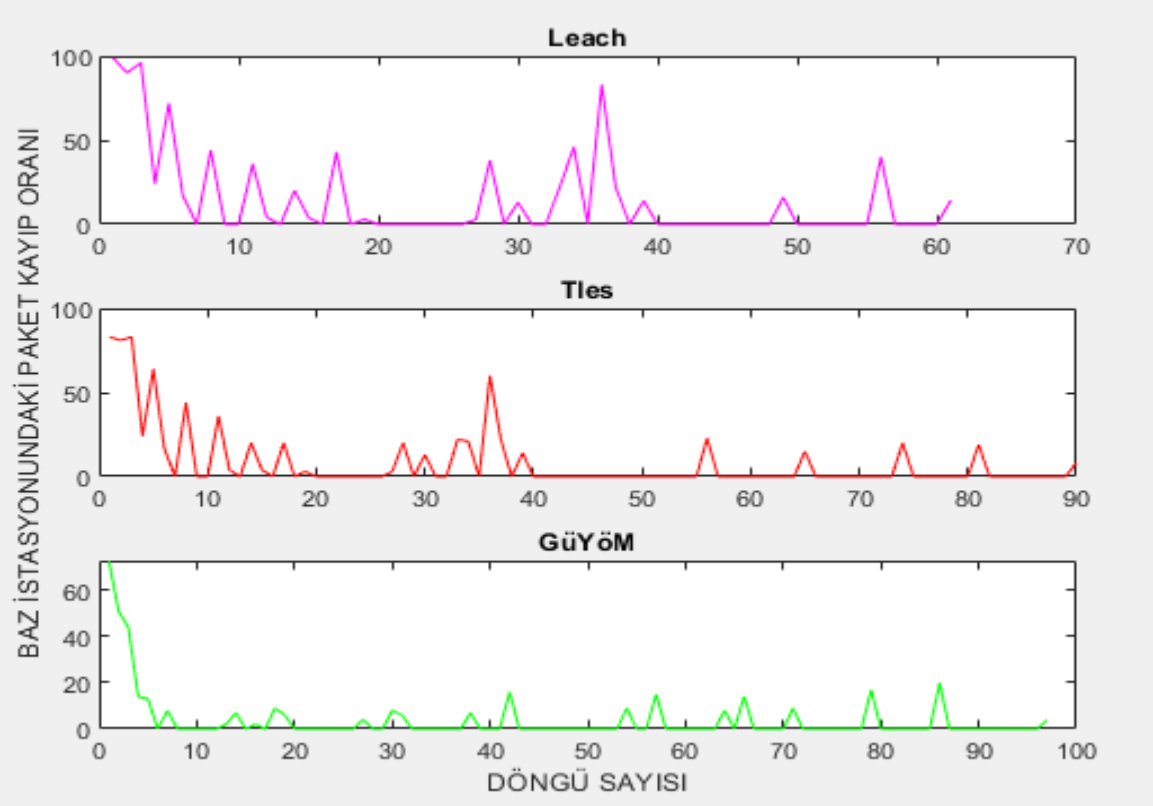
Şekil 6.32. Model 11 için her döngü yaşayan düğüm sayısı



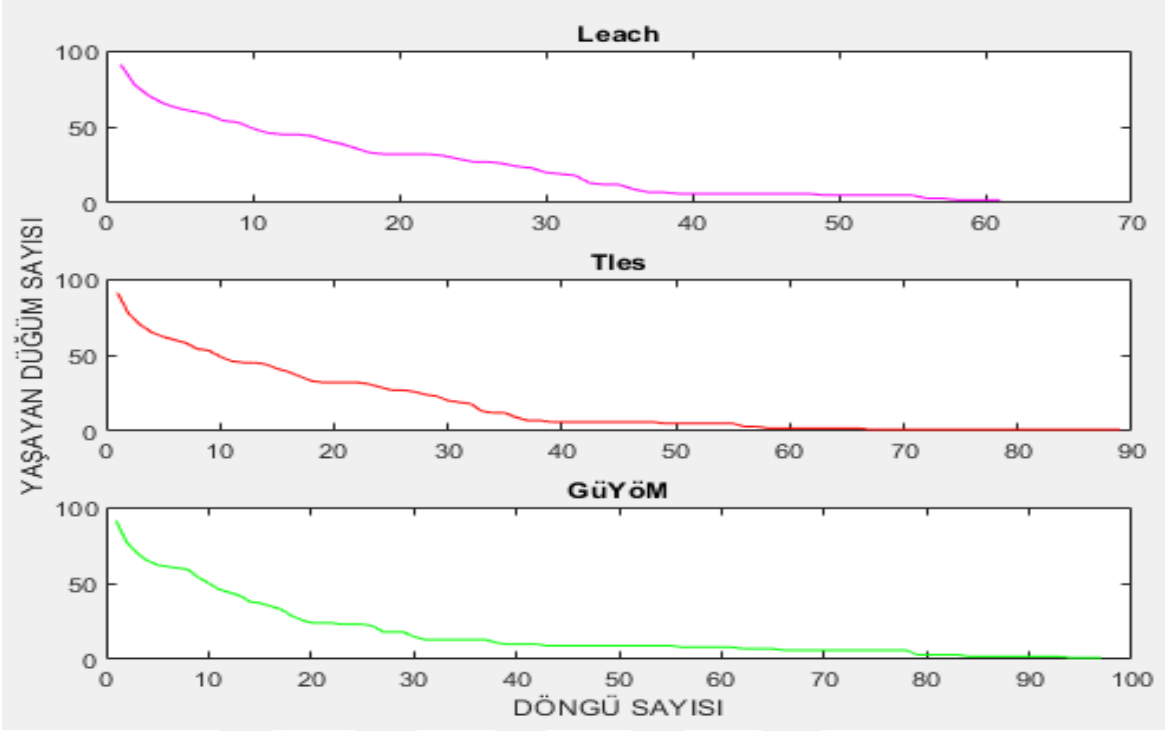
Şekil 6.33. Model 11 için her döngü ağda harcanan toplam enerji

6.12. Model 12' nin Performans Değerlendirmesi

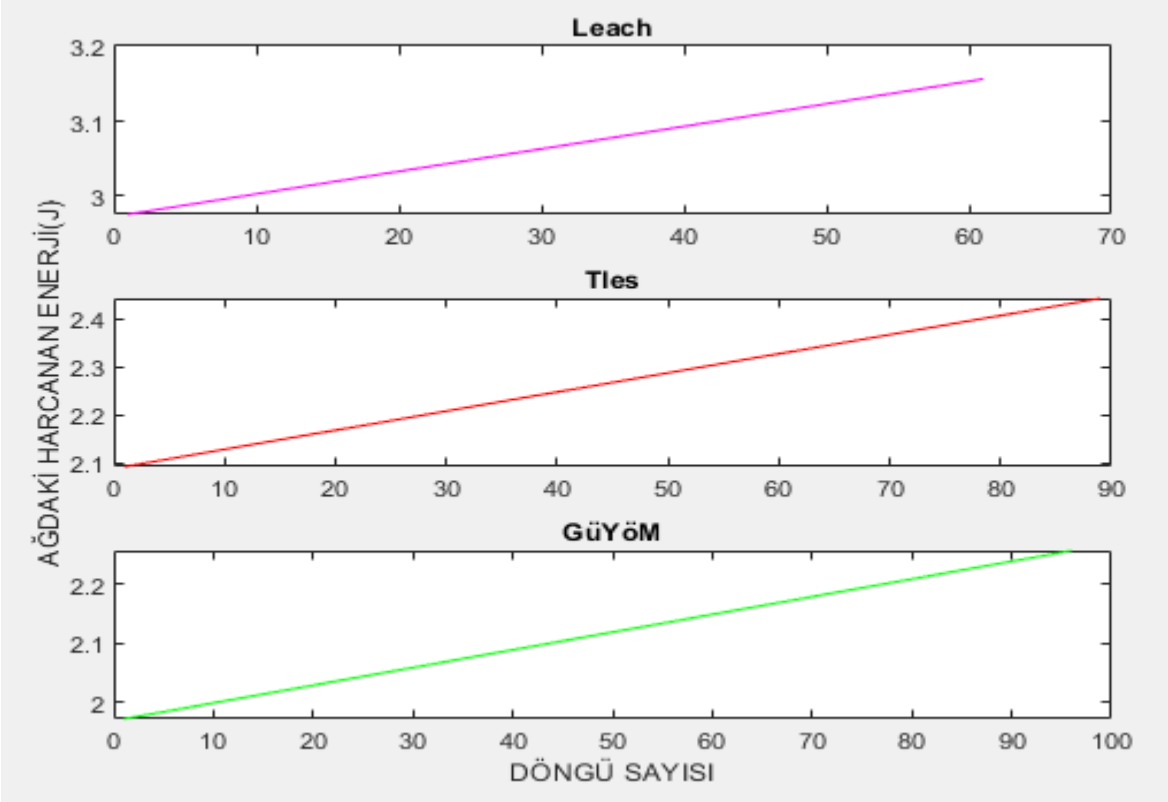
Model 10 ve Model 11'den farklı olarak saldırgan sayısı %30'a çıkarılmıştır. Saldırgan sayısının artması ile tüm protokollerde baz istasyonuna ulaşan paket kayıp oranları artarken ağ yaşam süresi kısalmıştır. Yapılan ölçümlerde LEACH protokolünde %14,15; TLES protokolünde %11,97; önerilen protokolde olan GüYöM' de ise %3,77 oranında paket kayıpları tespit edilmiştir (Şekil 6.34). LEACH protokolünün ağ yaşam süresi 61 döngü iken, bu değer TLES protokolünde 88, GüYöM' de ise 96 döngüdür (Şekil 6.35). Sonuçlardan da görüldüğü üzere GüYöM, güvenli yol üzerinden paketleri baz istasyonuna ulaştırmada diğer protokollere göre daha başarılı olurken, bunu enerji verimli bir şekilde yaptığı için ağ yaşam süresini de uzatmıştır. Şekil 6.36'da verilen harcanan enerji kıyaslamasında LEACH'in en fazla, GüYöM'ün ise en az enerji harcadığı tespit edilmiştir.



Şekil 6.34. Model 12 için her döngü baz istasyonunda gözlemlenen paket kayıp oranı



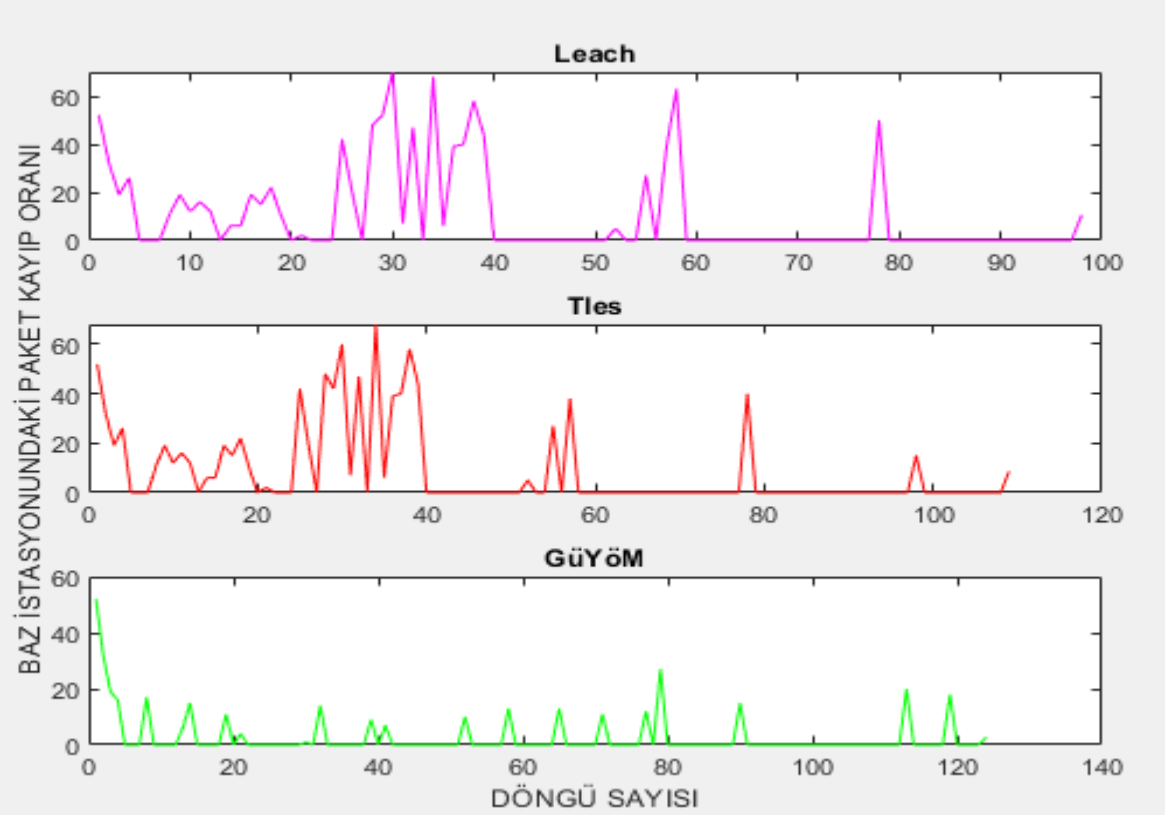
Şekil 6.35. Model 12 için her döngü yaşayan düğüm sayısı



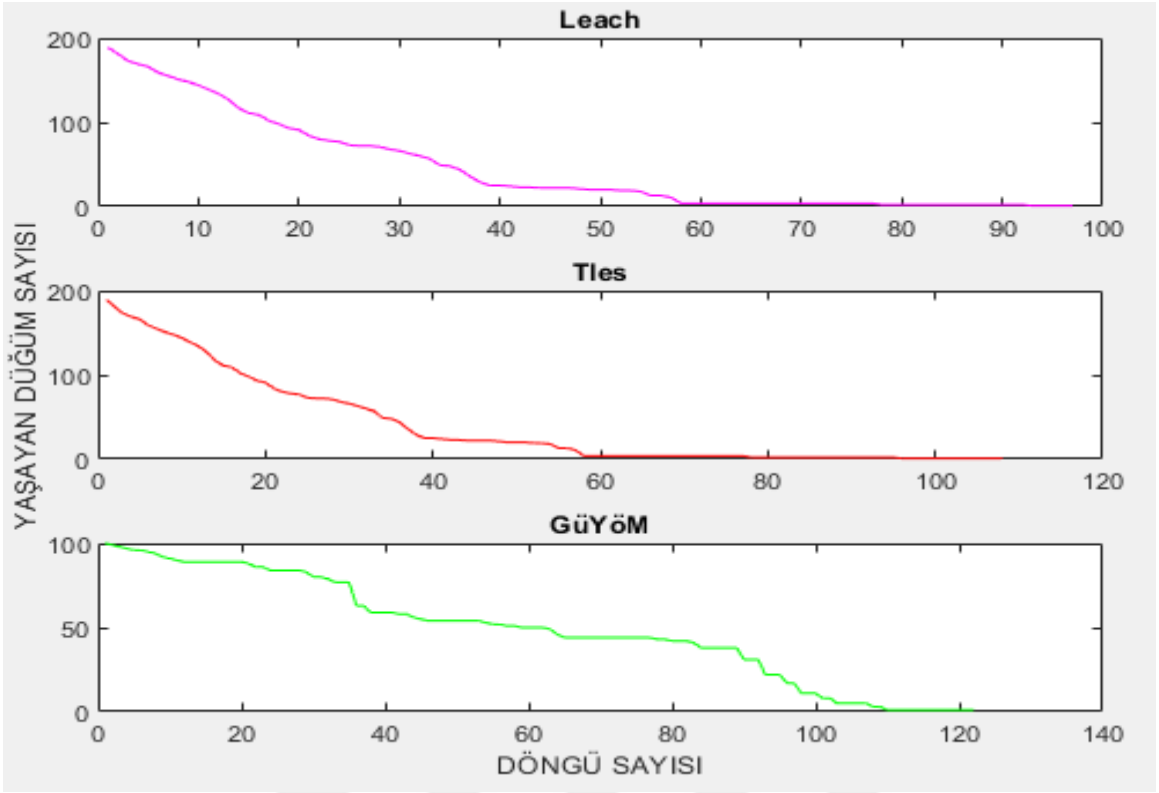
Şekil 6.36. Model 12 için her döngü ağda harcanan toplam enerji

6.13. Model 13' ün Performans Değerlendirmesi

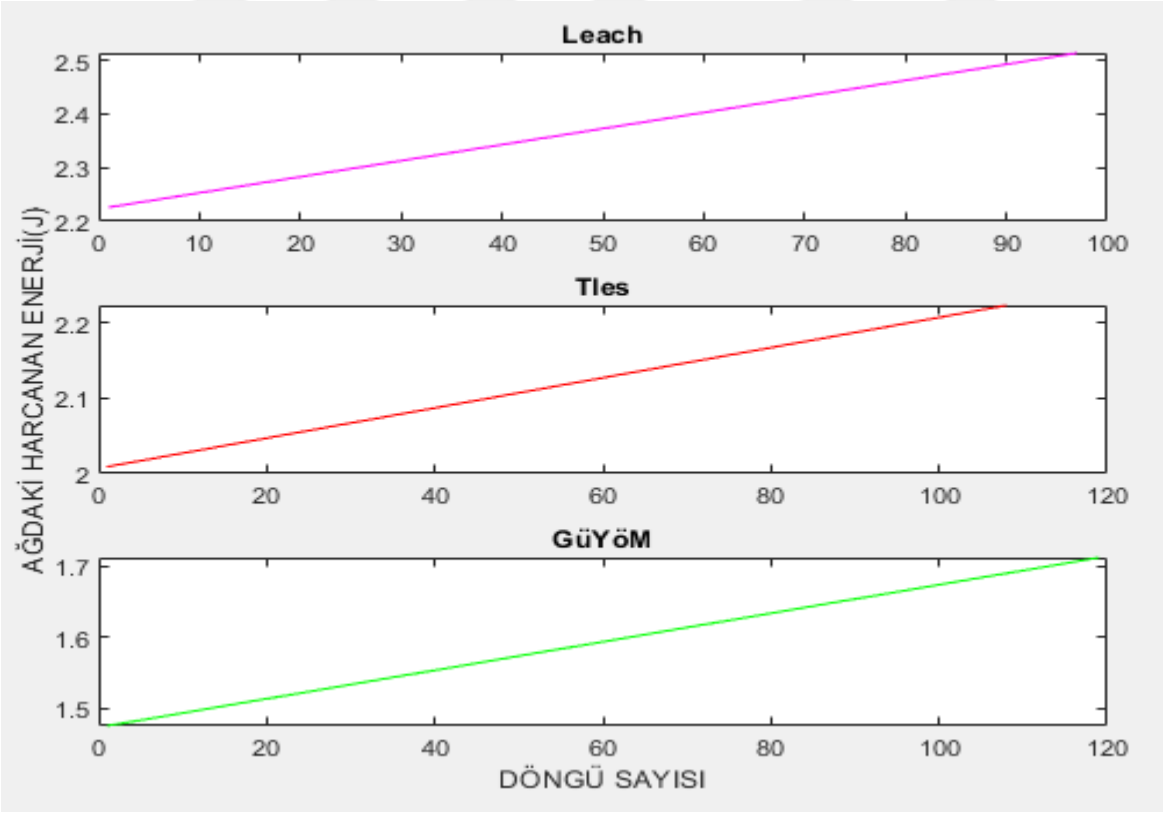
Modellenen 600x600'lük KAA sisteminde 200 düğüm bulunmaktadır. Düğüm sayısının %10'u saldırgan düğüm olarak modellenmiş ve sonuçlar LEACH ve TLES algoritmaları ile kıyaslanmıştır. Aynı oranda saldırgana sahip ancak düğüm sayısı 100 düğüm olan Model 10 ile kıyaslarsak, paket kayıp oranının azaldığı ve ağ yaşam süresinin arttığı tespit edilmiştir. Yapılan ölçümlerde LEACH protokolünde %10,34; TLES protokolünde %8,56; önerilen protokolde olan GüYöM' de ise %2,48 oranında paket kayıpları tespit edilmiştir (Şekil 6.37.). LEACH protokolünün ağ yaşam süresi 97 döngü iken, bu değer TLES protokolünde 108, GüYöM' de ise 123 döngüdür (Şekil 6.38.). Sonuçlardan da görüldüğü üzere GüYöM, güvenli yol üzerinden paketleri baz istasyonuna ulaştırmada diğer protokollere göre daha başarılı olurken, bunu enerji verimli bir şekilde yaptığı için ağ yaşam süresini de uzatmıştır. Şekil 6.39'da verilen harcanan enerji kıyaslamasında LEACH'in en fazla, GüYöM'ün ise en az enerji harcadığı tespit edilmiştir.



Şekil 6.37. Model 13 için her döngü baz istasyonunda gözlemlenen paket kayıp oranı



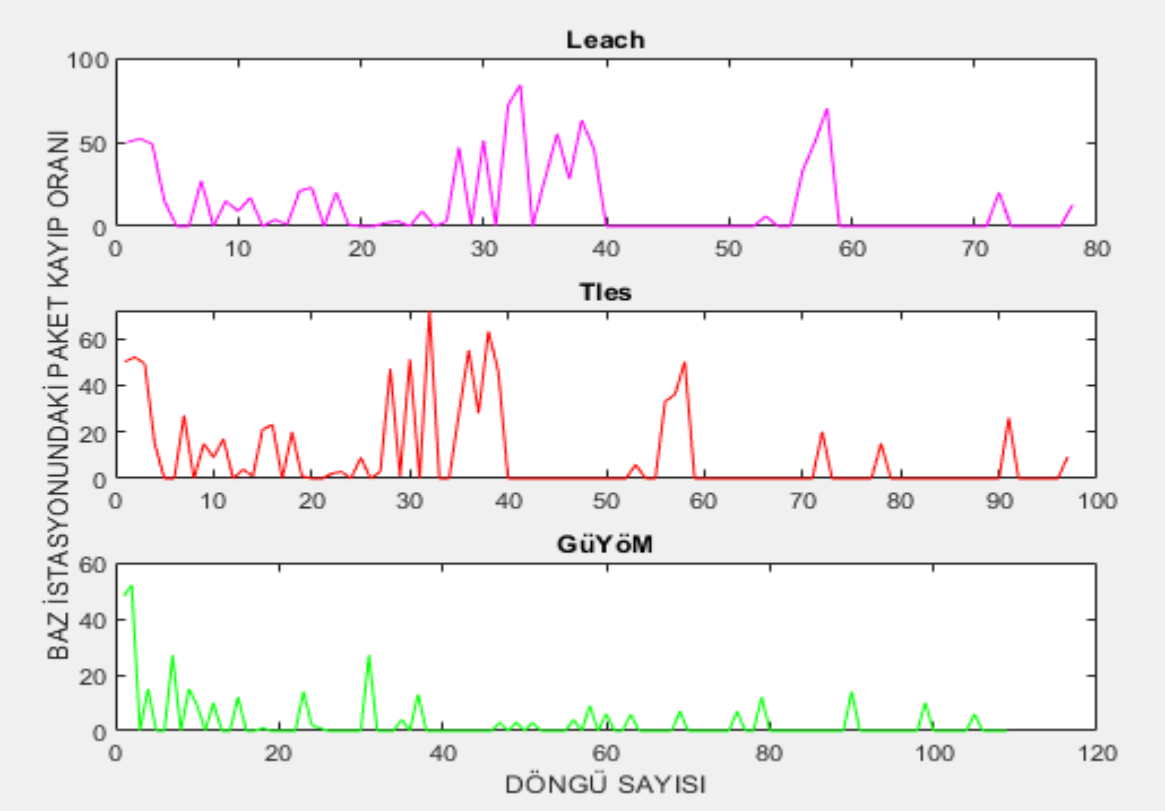
Şekil 6.38. Model 13 için her döngü yaşayan düğüm sayısı



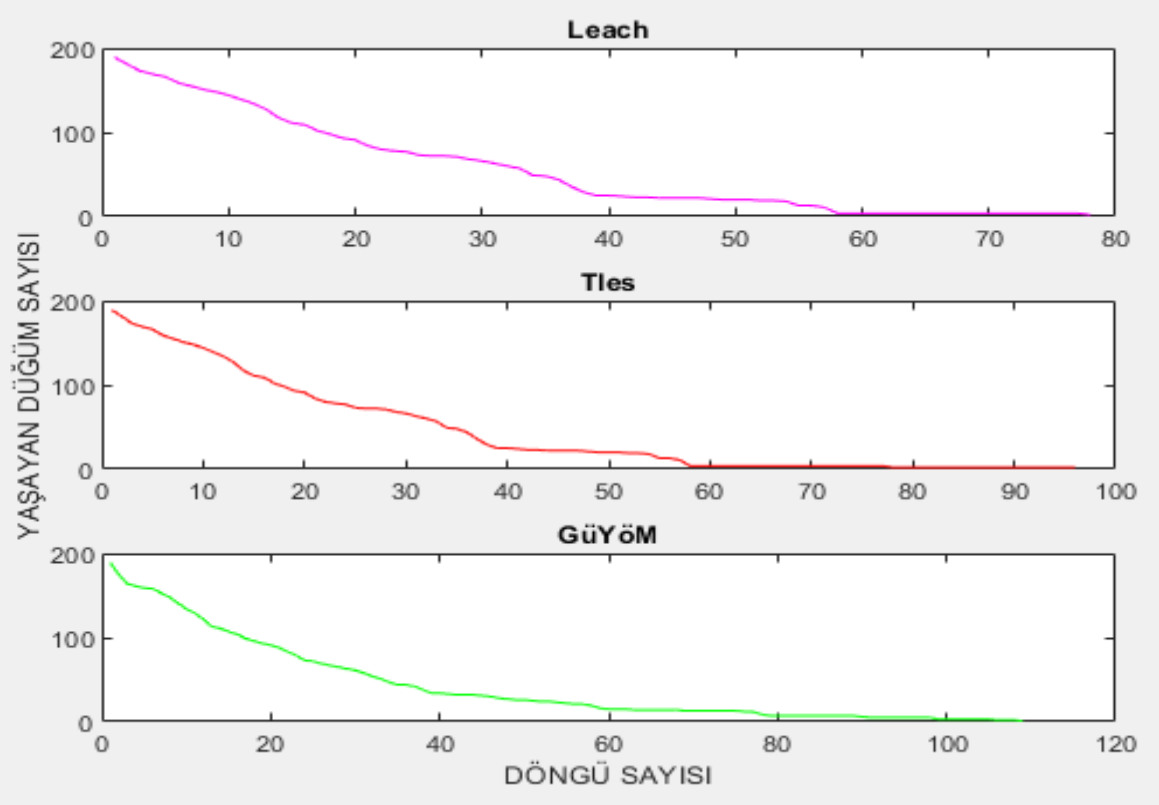
Şekil 6.39. Model 13 için her döngü ağda harcanan toplam enerji

6.14. Model 14' ün Performans Değerlendirmesi

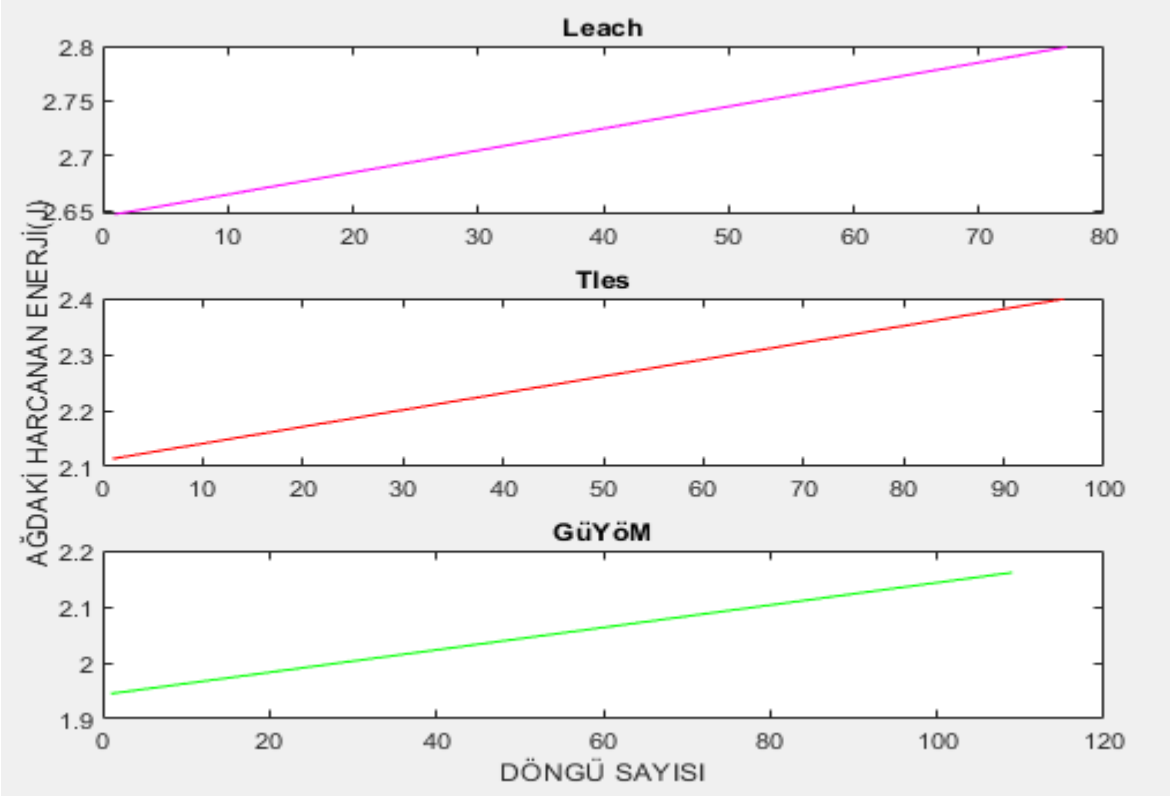
Bir önceki modelden farklı olarak saldırgan sayısı %20'ye çıkarılmıştır. Saldırgan sayısının artması ile tüm protokollerde baz istasyonuna ulaşan paket kayıp oranları artarken ağ yaşam süresi kısalmıştır. Aynı oranda saldırgana sahip ancak düğüm sayısı 100 düğüm olan Model 11 ile kıyaslarsak, paket kayıp oranının azaldığı ve ağ yaşam süresinin arttığı tespit edilmiştir. Yapılan ölçümlerde LEACH protokolünde %11,66; TLES protokolünde %9,35; önerilen protokolde olan GüYöM'de ise %3,11 oranında paket kayıpları tespit edilmiştir (Şekil 6.40.). LEACH protokolünün ağ yaşam süresi 78 döngü iken, bu değer TLES protokolünde 96, GüYöM'de ise 109 döngüdür (Şekil 6.41). Sonuçlardan da görüldüğü üzere GüYöM, güvenli yol üzerinden paketleri baz istasyonuna ulaştırmada diğer protokollere göre daha başarılı olurken, bunu enerji verimli bir şekilde yaptığı için ağ yaşam süresini de uzatmıştır. Şekil 6.42'de verilen harcanan enerji kıyaslamasında LEACH'in en fazla, GüYöM'ün ise en az enerji harcadığı tespit edilmiştir.



Şekil 6.40. Model 14 için her döngü baz istasyonunda gözlemlenen paket kayıp oranı



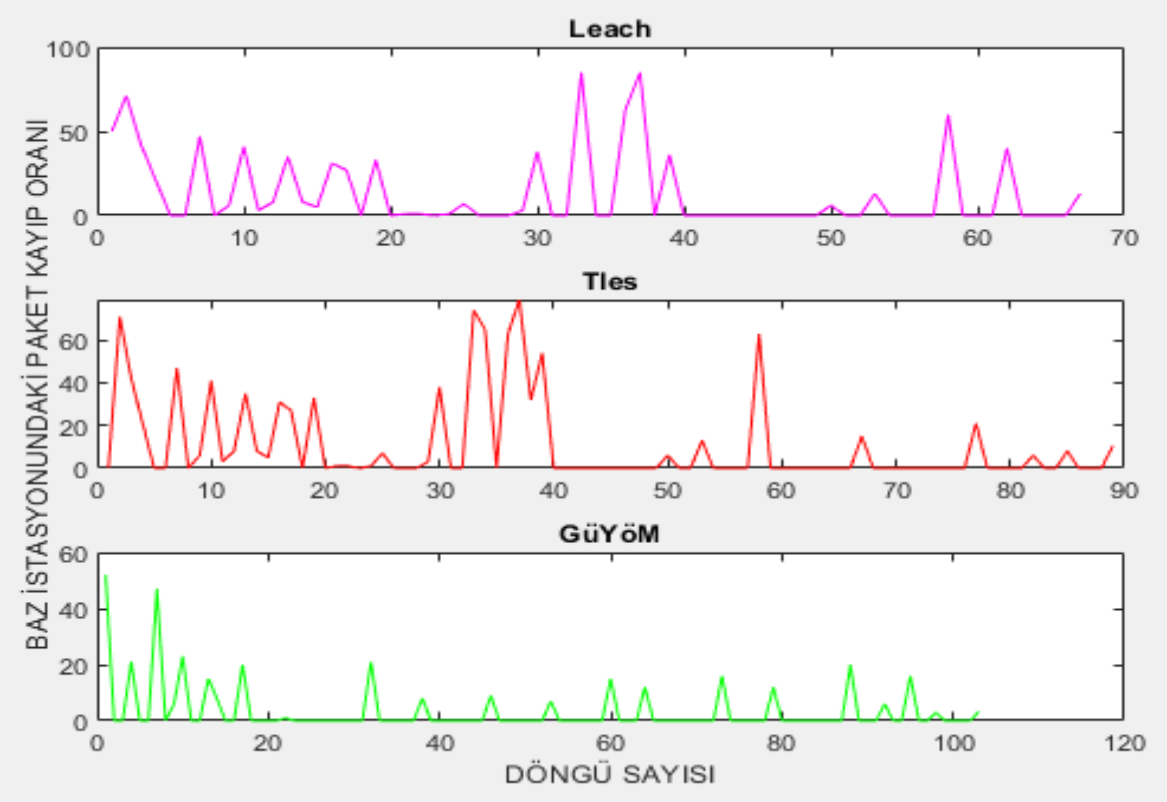
Şekil 6.41. Model 14 için her döngü yaşayan düğüm sayısı



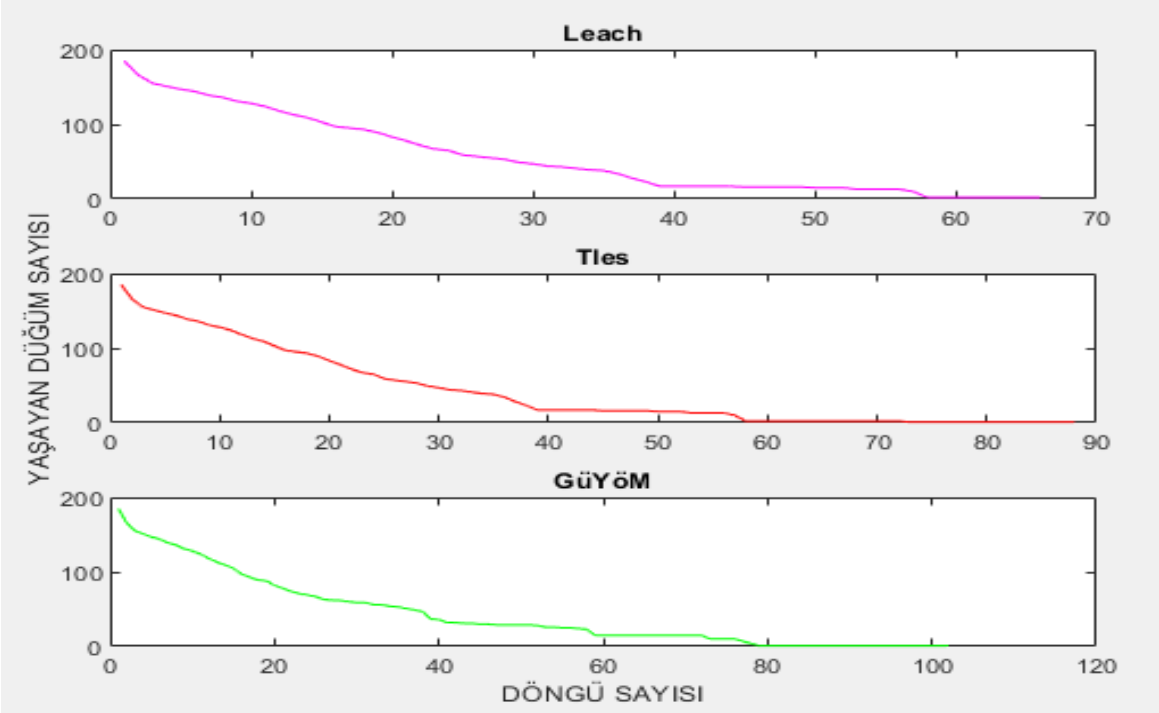
Şekil 6.42. Model 14 için her döngü ağda harcanan toplam enerji

6.15. Model 15' in Performans Değerlendirmesi

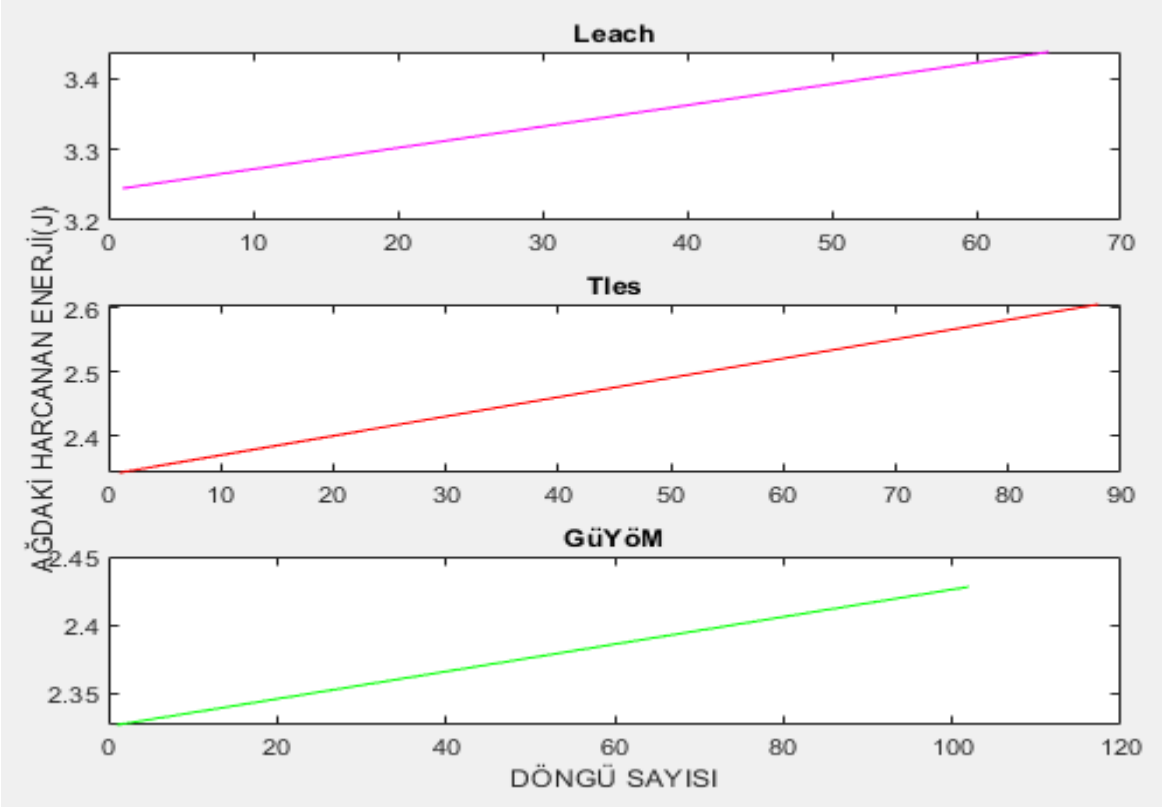
Model 13 ve Model 14'ten farklı olarak saldırgan sayısı %30'a çıkarılmıştır. Saldırgan sayısının artması ile tüm protokollerde baz istasyonuna ulaşan paket kayıp oranları artarken ağ yaşam süresi kısalmıştır. Aynı oranda saldırgana sahip ancak düğüm sayısı 100 düğüm olan Model 12 ile kıyaslarsak, paket kayıp oranının azaldığı ve ağ yaşam süresinin arttığı tespit edilmiştir. Yapılan ölçümlerde LEACH protokolünde %13,3; TLES protokolünde %10,54; önerilen protokolde olan GüYöM'de ise %3,31 oranında paket kayıpları tespit edilmiştir (Şekil 6.43). LEACH protokolünün ağ yaşam süresi 66 döngü iken, bu değer TLES protokolünde 88, GüYöM'de ise 102 döngüdür (Şekil 6.44). Sonuçlardan da görüldüğü üzere GüYöM, güvenli yol üzerinden paketleri baz istasyonuna ulaştırmada diğer protokollere göre daha başarılı olurken, bunu enerji verimli bir şekilde yaptığı için ağ yaşam süresini de uzatmıştır. Bunun nedeni düğümlerin enerjilerinin verimli kullanmasını sağlamasıdır. Şekil 6.45'te verilen harcanan enerji kıyaslamasında LEACH'in en fazla, GüYöM'ün ise en az enerji harcadığı tespit edilmiştir.



Şekil 6.43. Model 15 için her döngü baz istasyonunda gözlemlenen paket kayıp oranı



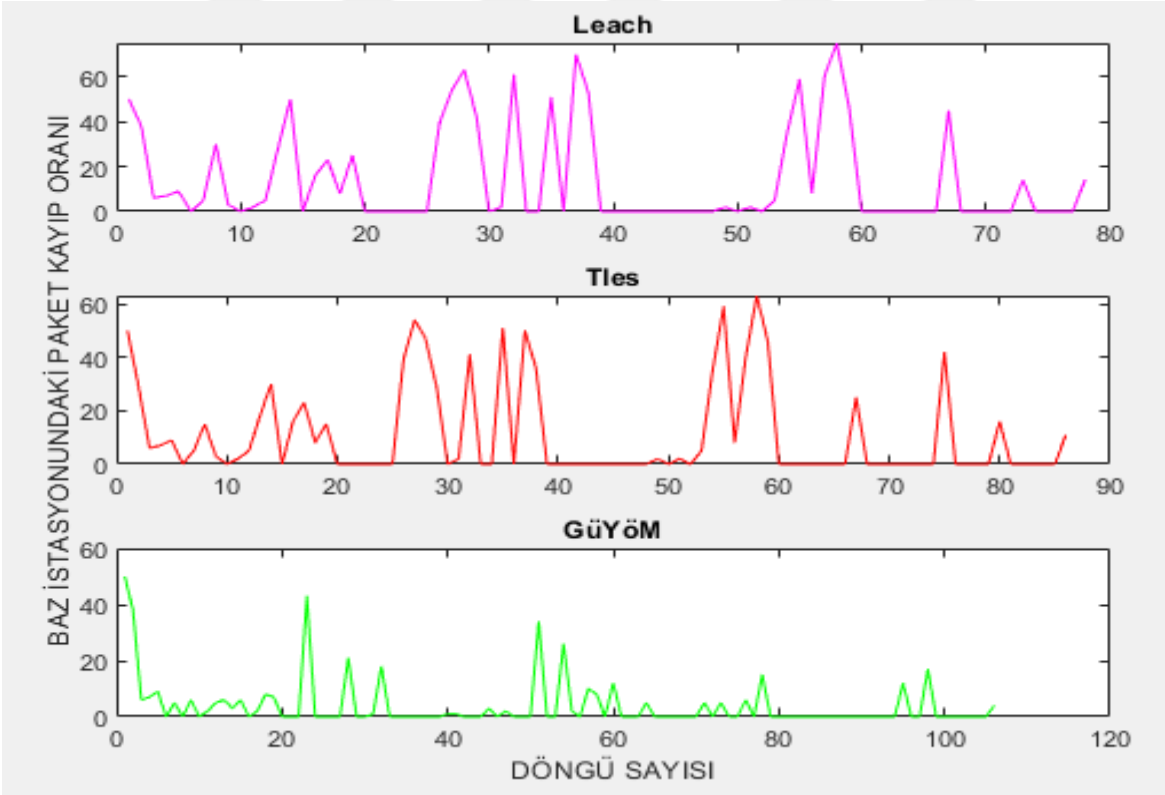
Şekil 6.44. Model 15 için her döngü yaşayan düğüm sayısı



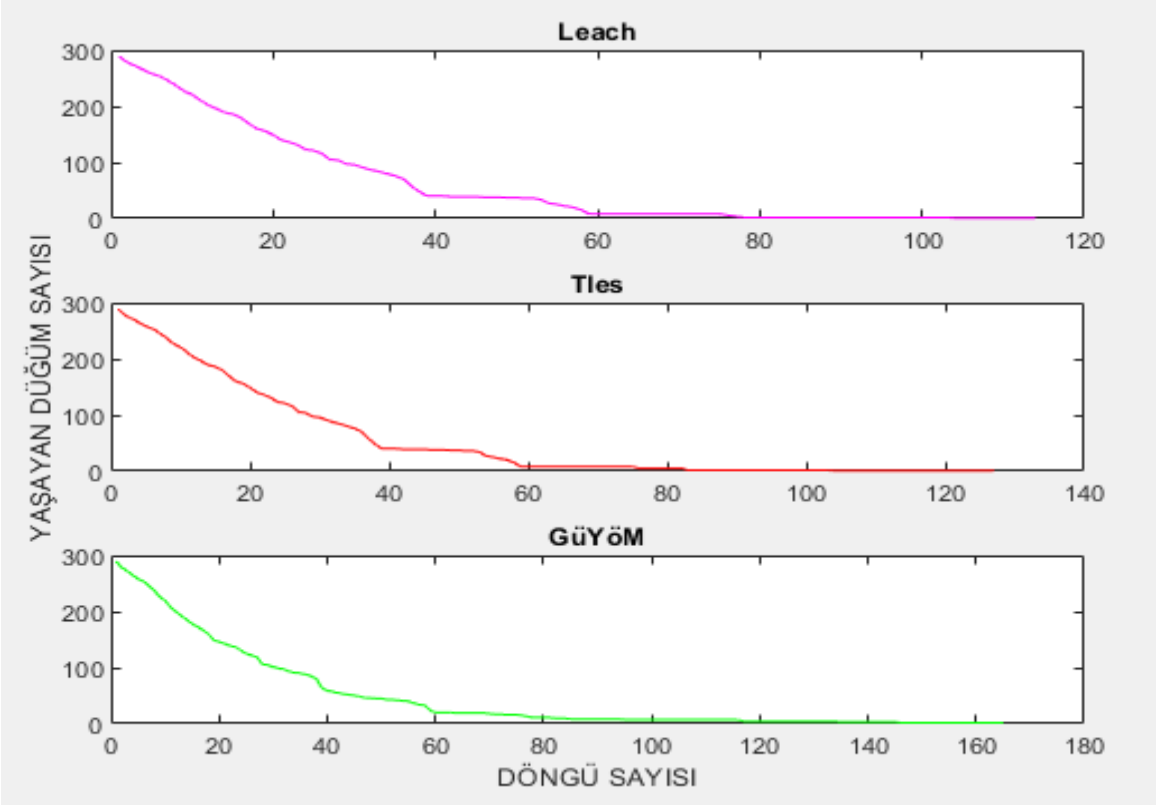
Şekil 6.45. Model 15 için her döngü ağda harcanan toplam enerji

6.16. Model 16' nın Performans Değerlendirmesi

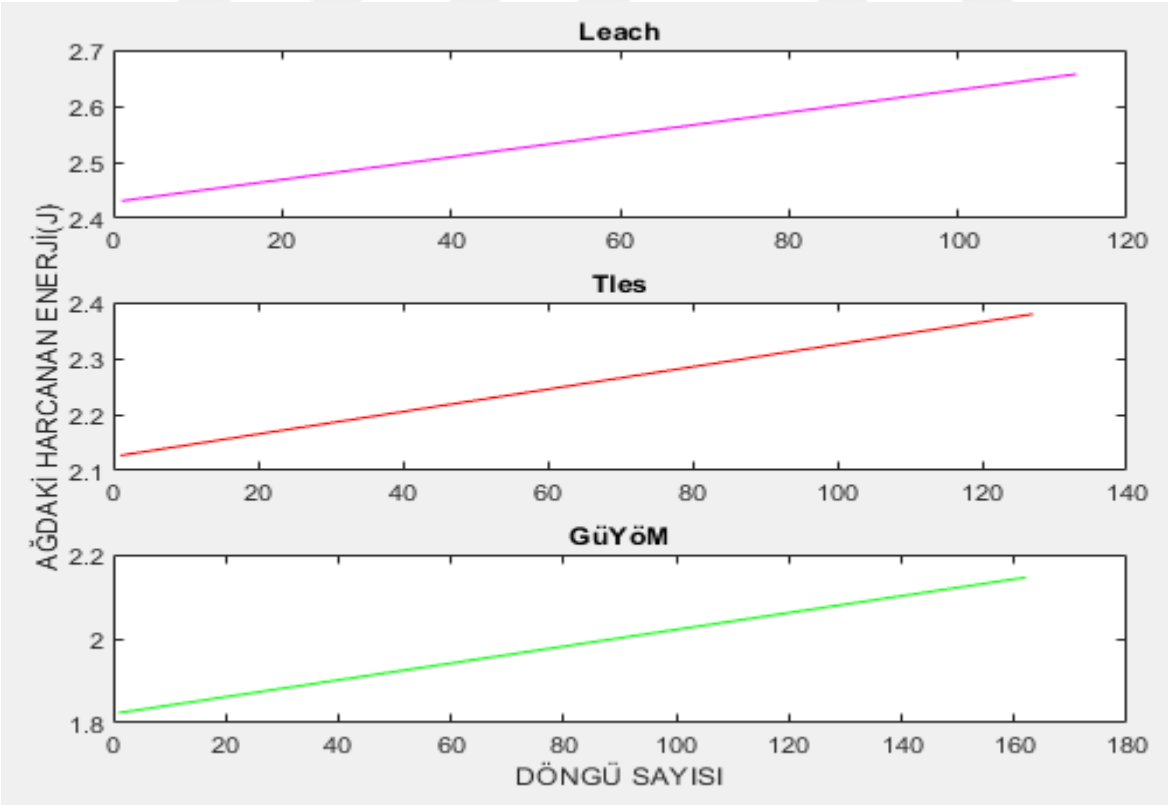
Bir önceki modelden farklı olarak saldırgan sayısı düğüm sayısı arttırılarak 300 düğüme çıkarılmıştır. Düğüm sayısının %10'u saldırgan düğüm olarak modellenmiş ve sonuçlar LEACH ve TLES algoritmaları ile kıyaslanmıştır. Aynı oranda saldırgana sahip ancak düğüm sayıları sırasıyla 100 düğüm ve 200 düğüm olan Model 10 ve Model 13 ile kıyasladığımızda, paket kayıp oranının azaldığı, ağ yaşam süresinin arttığı gözlemlenmiştir Yapılan ölçümlerde LEACH protokolünde %9,76; TLES protokolünde %7,45; önerilen protokolde olan GüYöM'de ise %2,32 oranında paket kayıpları tespit edilmiştir (Şekil 6.46.). LEACH protokolünün ağ yaşam süresi 114 döngü iken, bu değer TLES protokolünde 127, GüYöM'de ise 166 döngüdür (Şekil 6.47.). Sonuçlardan da görüldüğü üzere GüYöM, güvenli yol üzerinden paketleri baz istasyonuna ulaştırmada diğer protokollere göre daha başarılı olurken, bunu enerji verimli bir şekilde yaptığı için ağ yaşam süresini de uzatmıştır. Şekil 6.48.'de verilen harcanan enerji kıyaslamasında LEACH'in en fazla, GüYöM'ün ise en az enerji harcadığı tespit edilmiştir.



Şekil 6.46. Model 16 için her döngü baz istasyonunda gözlemlenen paket kayıp oranı



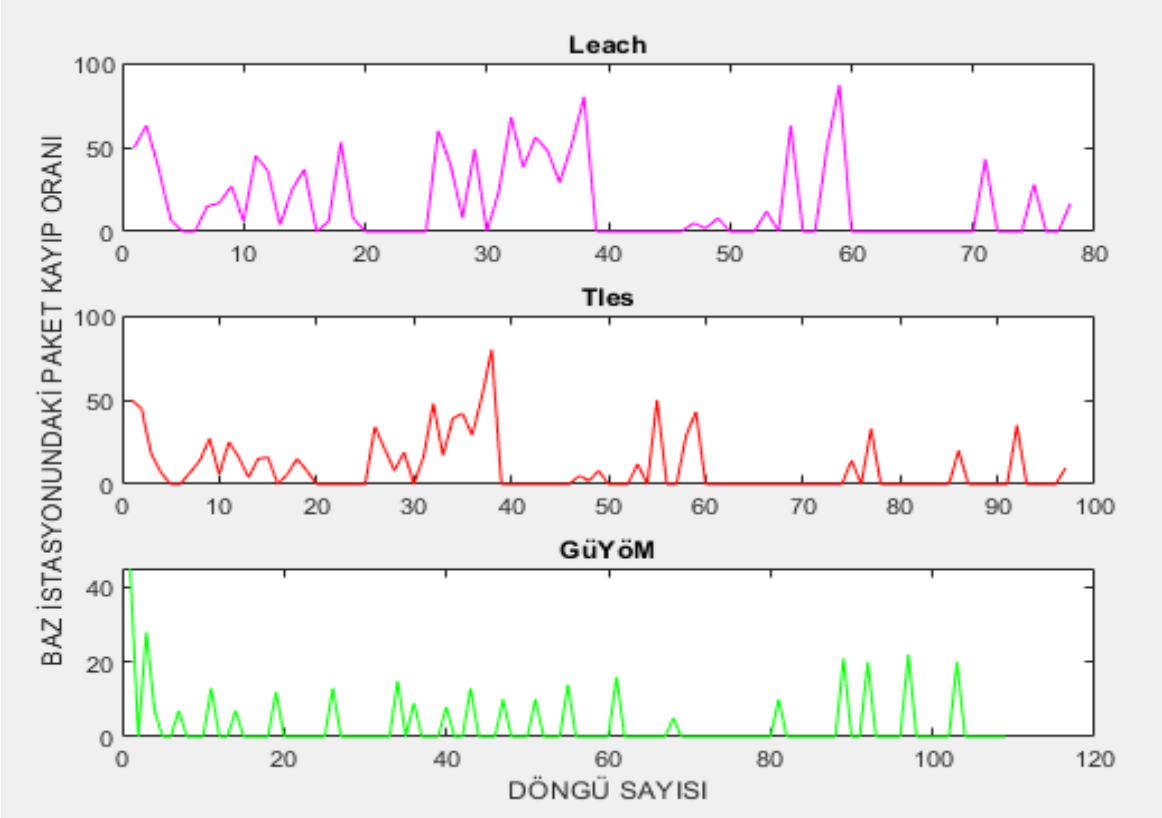
Şekil 6.47. Model 16 için her döngü yaşayan düğüm sayısı



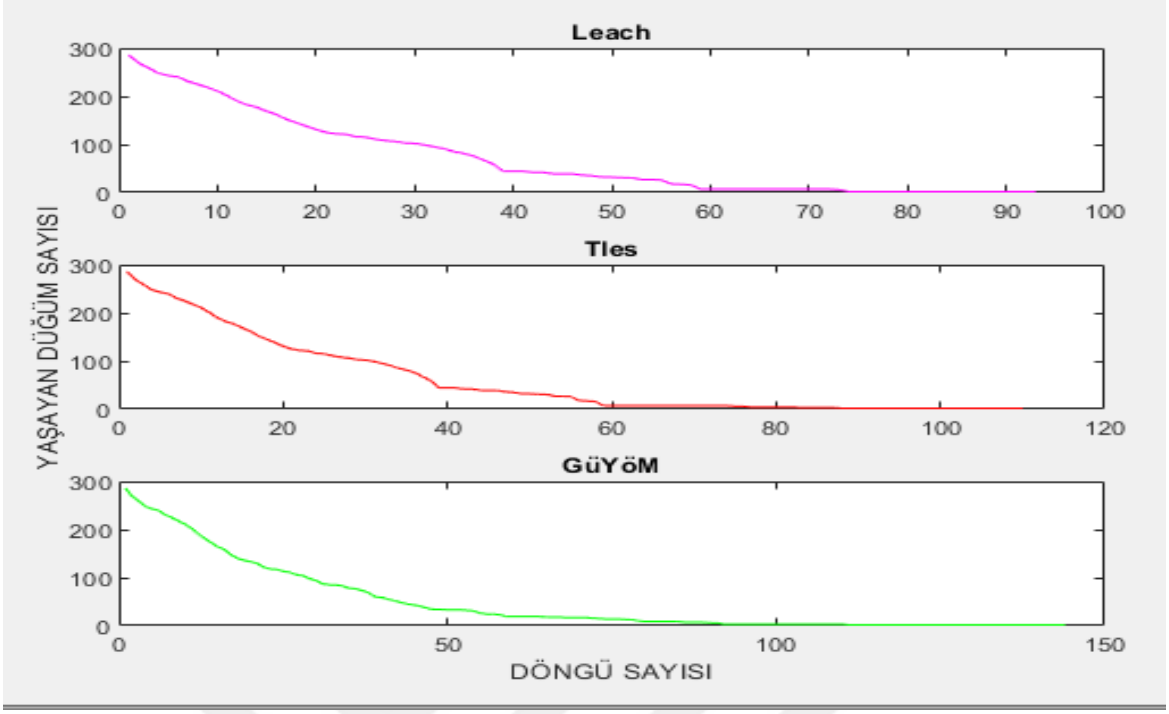
Şekil 6.48. Model 16 için her döngü ağda harcanan toplam enerji

6.17. Model 17' nin Performans Değerlendirmesi

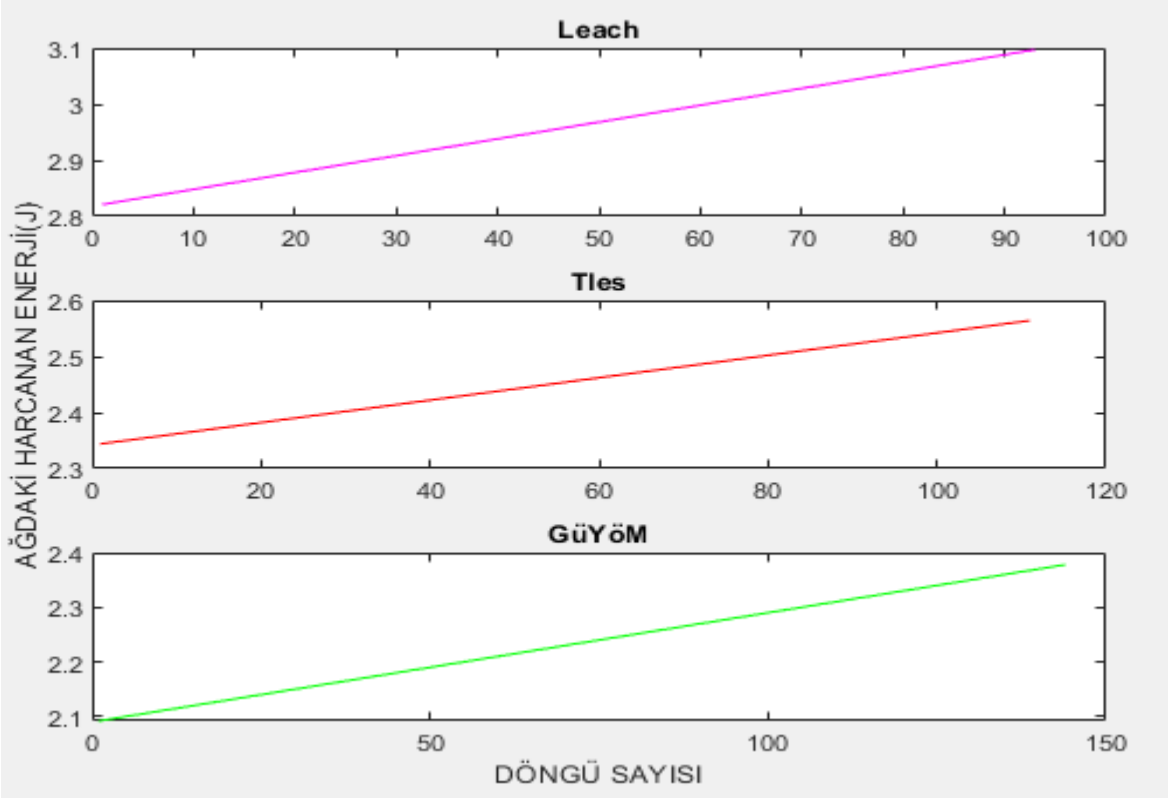
Bir önceki modelden farklı olarak saldırgan sayısı %20'ye çıkarılmıştır. Saldırgan sayısının artması ile tüm protokollerde baz istasyonuna ulaşan paket kayıp oranları artarken ağ yaşam süresi kısalmıştır. Aynı oranda saldırgana sahip ancak düğüm sayıları sırasıyla 100 düğüm ve 200 düğüm olan Model 11 ve Model 14 ile kıyasladığımızda, paket kayıp oranının azaldığı, ağ yaşam süresinin arttığı gözlemlenmiştir. Yapılan ölçümlerde LEACH protokolünde %10,83; TLES protokolünde %8,49; önerilen protokolde olan GüYöM'de ise %2,96 oranında paket kayıpları tespit edilmiştir (Şekil 6.49). LEACH protokolünün ağ yaşam süresi 93 döngü iken, bu değer TLES protokolünde 109, GüYöM' de ise 144 döngüdür (Şekil 6.50). Sonuçlardan da görüldüğü üzere GüYöM, güvenli yol üzerinden paketleri baz istasyonuna ulaştırmada diğer protokollere göre daha başarılı olurken, bunu enerji verimli bir şekilde yaptığı için ağ yaşam süresini de uzatmıştır. Şekil 6.51'de verilen harcanan enerji kıyaslamasında LEACH'in en fazla, GüYöM'ün ise en az enerji harcadığı tespit edilmiştir.



Şekil 6.49. Model 17 için her döngü baz istasyonunda gözlemlenen paket kayıp oranı



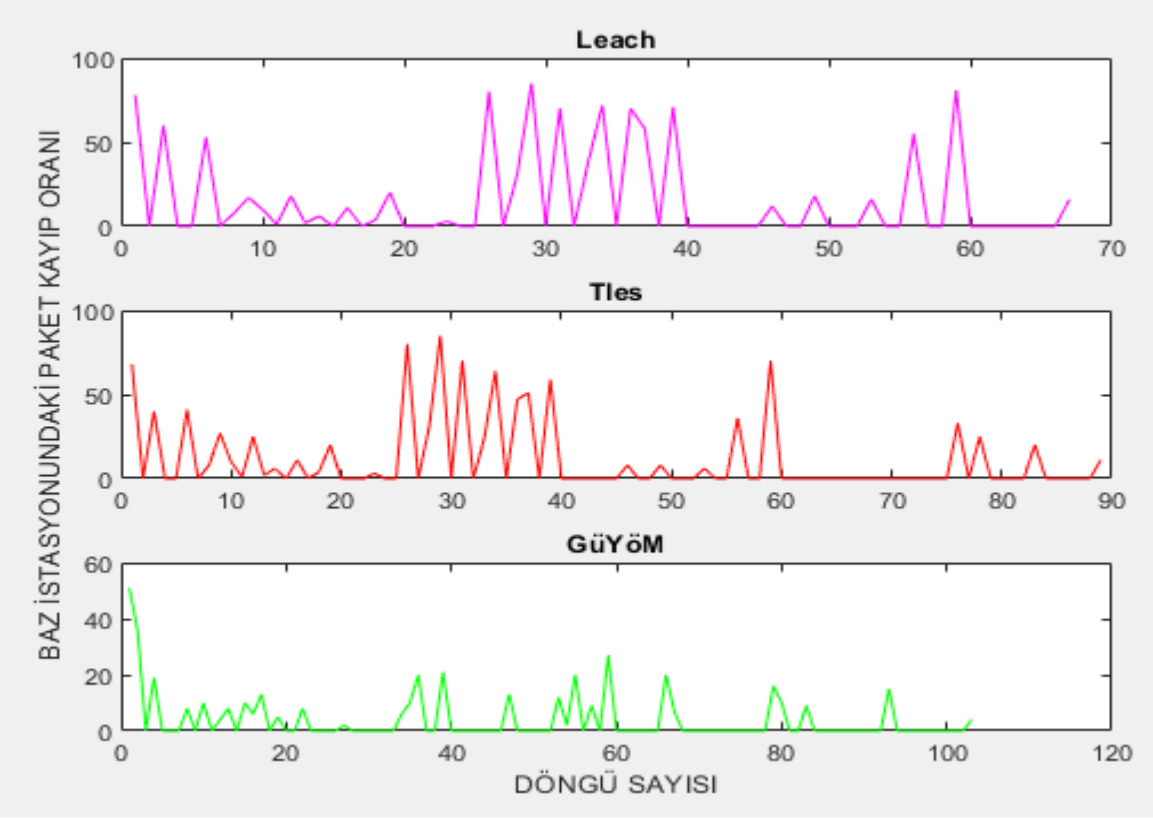
Şekil 6.50. Model 17 için her döngü yaşayan düğüm sayısı



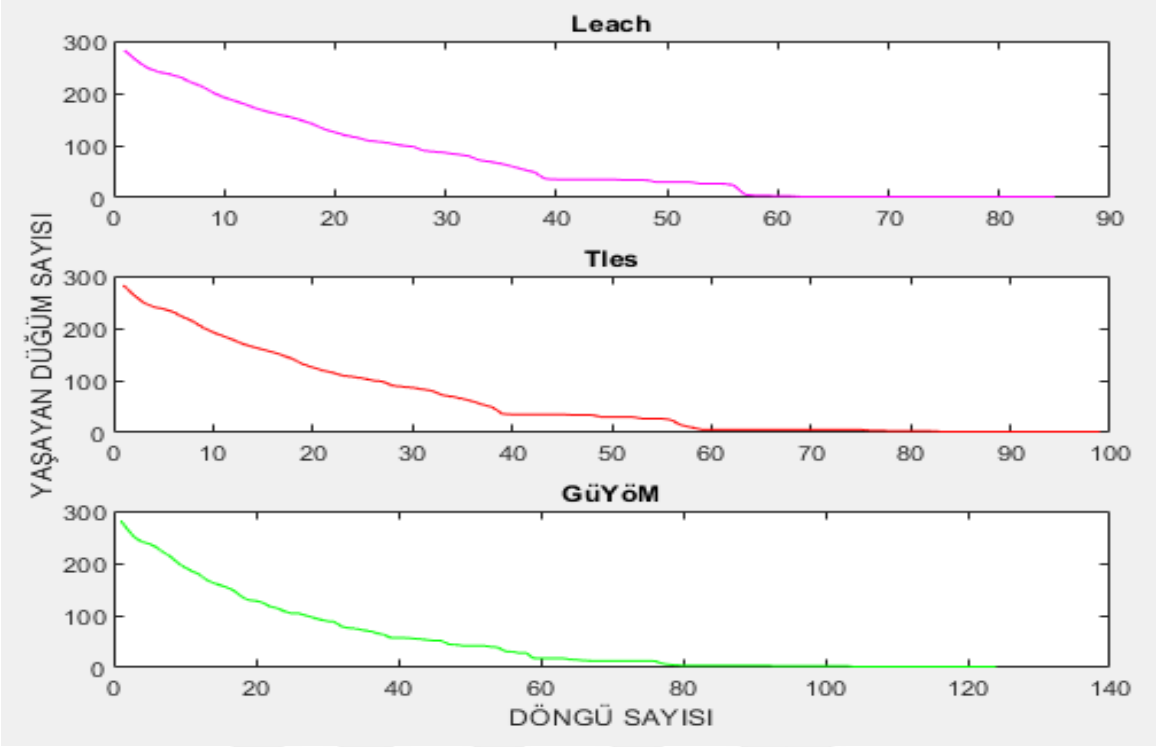
Şekil 6.51. Model 17 için her döngü ağda harcanan toplam enerji

6.18. Model 18' in Performans Değerlendirmesi

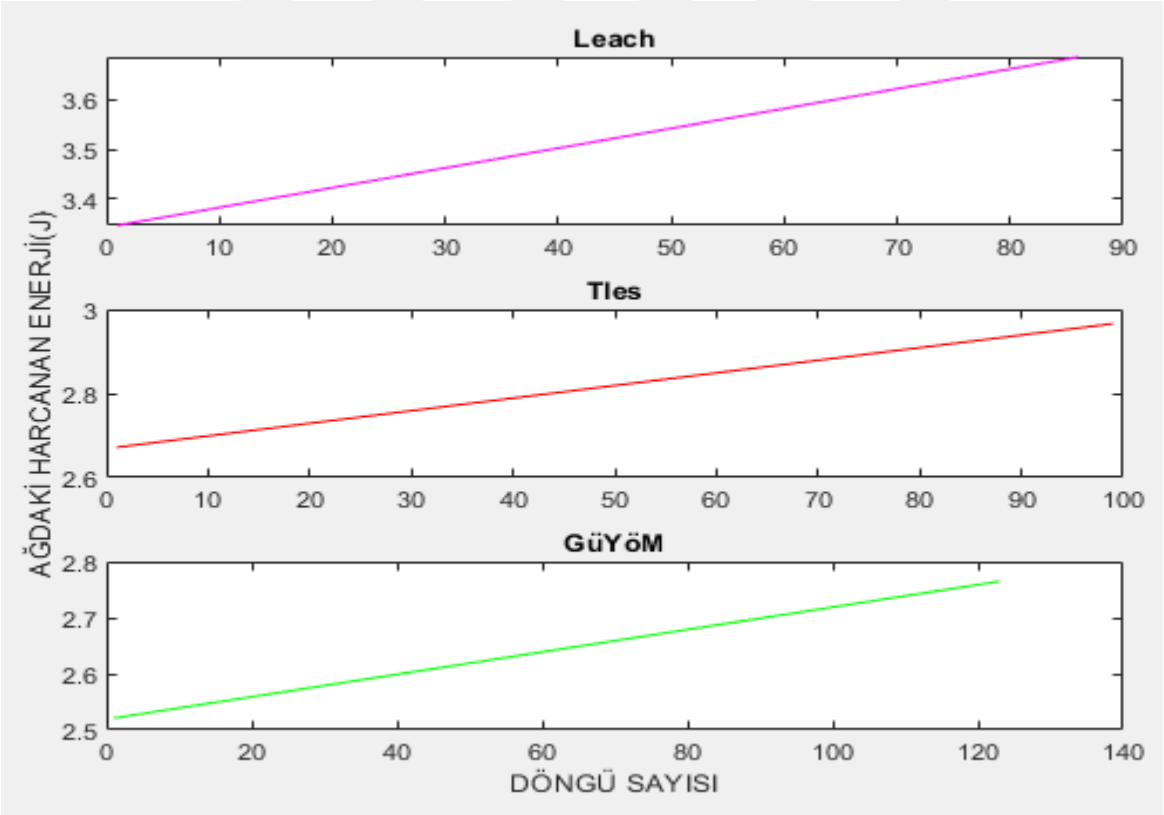
Model 6 ve Model 17'den farklı olarak saldırgan sayısı %30'a çıkarılmıştır. Saldırgan sayısının artması ile tüm protokollerde baz istasyonuna ulaşan paket kayıp oranları artarken ağ yaşam süresi kısalmıştır. Aynı oranda saldırgana sahip ancak düğüm sayıları sırasıyla 100 düğüm ve 200 düğüm olan Model 12 ve Model 15 ile kıyasladığımızda, paket kayıp oranının azaldığı, ağ yaşam süresinin arttığı gözlemlenmiştir. Yapılan ölçümlerde LEACH protokolünde %12,83; TLES protokolünde %9,73; önerilen protokolde olan GüYöM' de ise %3,09 oranında paket kayıpları tespit edilmiştir (Şekil 6.52). LEACH protokolünün ağ yaşam süresi 81 döngü iken, bu değer TLES protokolünde 96, GüYöM'de ise 123 döngüdür (Şekil 6.53). Sonuçlardan da görüldüğü üzere GüYöM, güvenli yol üzerinden paketleri baz istasyonuna ulaştırmada diğer protokollere göre daha başarılı olurken, bunu enerji verimli bir şekilde yaptığı için ağ yaşam süresini de uzatmıştır. Şekil 6.54'de verilen harcanan enerji kıyaslamasında LEACH'in en fazla, GüYöM'ün ise en az enerji harcadığı tespit edilmiştir.



Şekil 6.52. Model 18 için her döngü baz istasyonunda gözlemlenen paket kayıp oranı



Şekil 6.53. Model 18 için her döngü yaşayan düğüm sayısı



Şekil 6.54. Model 18 için her döngü ağda harcanan toplam enerji

Elde edilen sonuçlar, ağın farklı parametreleri altında da önerilen protokolün diğer yaklaşımlara göre enerjiyi kullanma açısından verimli olduğunu ve saldırıları yakalamada daha yüksek başarım elde ettiğini göstermektedir.

7. SONUÇLAR

Günümüzde KAA'lar, maliyet efektif bir şekilde izleme ve algılama sistemlerinin kurulması ve kablosuz ortam vasıtasıyla verinin iletilmesi imkanını sunması nedeniyle oldukça geniş kullanım alanı bulmaktadır. Sunduğu birçok avantajın yanında, güvenlik problemi KAA'larda çözülmesi gereken önemli bir sorun olarak karşımıza çıkmaktadır. Özellikle verinin başarılı bir şekilde iletilmesine engel olan yönlendirme atakları, ağdan bilginin verimli bir şekilde toplanmasını engelleyerek KAA'ların başarımlarını düşürmektedir. Bu nedenle yönlendirme saldırılarının yakalanmasını veya bu saldırıların etrafından dolanarak verinin güvenli bir şekilde iletilmesini amaçlayan çok sayıda çalışma literatürde yer almaktadır.

Bu tezde, paket kayıplarına sebep olan yönlendirme saldırılarına karşı güven tabanlı bir rota kurulum protokolü geliştirilmiştir. Kümeleme tabanlı KAA'lar üzerinde modellenen sistemde, paket iletim oranı, tutarlılık ve bencillik parametrelerine bağlı olarak küme başı düğüm adayları için bir güven değeri belirlenmiş ve güven değeri düşük olan düğümlerin küme başı olmaları engellenmiştir. Bununla birlikte küme başı düğümlerin çok fazla enerji harcadıkları düşünüldüğünde erken ölmelerinin ve ağ döngüsünden çıkmalarının ertelenmesi amacıyla hem güven değeri hem de enerjisi yüksek düğümlerin küme başı olarak seçilmesi sağlanmıştır. Önerilen güven tabanlı yönlendirme mimarisi GüYöM, literatürde yer alan LEACH ve TLES algoritmaları ile yaşayan düğüm sayısı, harcanan enerji ve baz istasyonunda toplanan paket kayıp oranları üzerinden farklı ağ büyüklükleri, farklı saldırgan oranları ve farklı düğüm sayıları altında kıyaslanmıştır. Yapılan simülasyonlar sonucunda GüYöM' ün her iki protokole göre de her durumda daha iyi performans sergilediği (daha uzun ağ yaşam süresi, daha az enerji harcamam, daha yüksek oranda paket iletimi) izlenmiştir.

KAYNAKLAR

Abasikeleş-Turgut, I., Aydin, M. N., & Tohma, K. (2016). A realistic modelling of the sinkhole and the black hole attacks in cluster-based WSNs. International Journal of Electronics and Electrical Engineering, 4(1), 74-78.

Bahekmat, M., Yaghmaee, M. H., Yazdi, A. S. H., & Sadeghi, S. (2012). A novel algorithm for detecting sinkhole attacks in WSNs. International Journal of Computer Theory and Engineering, 4(3), 418.

Bao, F., Chen, R., Chang, M., & Cho, J. H. (2012). Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE transactions on network and service management, 9(2), 169-183.

Butun, I., Morgera, S. D., & Sankar, R. (2014). A survey of intrusion detection systems in wireless sensor networks. IEEE communications surveys & tutorials, 16(1), 266-282.

Ceyhan, E. B., & Sağiroğlu, Ş. (2013). Kablosuz algilayici ağlarda güvenlik sorunlari ve alinabilecek önlemler. Politeknik Dergisi, 16(4), 155-163.

Chen, Z., He, M., Liang, W., & Chen, K. (2015). Trust-aware and low energy consumption security topology protocol of wireless sensor network. Journal of Sensors, 2015.

Dhakne, A. R., & Chatur, P. N. (2017). Design of Hierarchical Trust based Intrusion Detection System for Wireless Sensor Network [HTBID]. International Journal of Applied Engineering Research, 12(8), 1772-1778.

Dongare, S. P., & Mangrulkar, R. S. (2016). Optimal cluster head selection based energy efficient technique for defending against gray hole and black hole attacks in wireless sensor networks. Procedia Computer Science, 78, 423-430.

Fei, X., & Jian, X. Q. (2008, December). Active trust transmission mechanism for wireless sensor network. In 2008 Second International Symposium on Intelligent Information Technology Application (Vol. 1, pp. 626-632). IEEE.

Feng, R., Xu, X., Zhou, X., & Wan, J. (2011). A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory. Sensors, 11(2), 1345-1360.

Gondwal, N., & Diwaker, C. (2013). Detecting blackhole attack in WSN by check agent using multiple base stations. American International Journal of Research in Science, Technology, Engineering & Mathematics, 3(2), 149-152.

Heinzelman, W., Chandrakasan, A., & Balakrishnan, H. (2000, January). Energy-efficient communication protocol for wireless sensor networks [C]. In Proceeding of the Hawaii International Conference System Sciences, Hawaii.

Jan, M. A. (2016). Energy-efficient routing and secure communication in wireless sensor networks (Doctoral dissertation

Juliana, R., & Maheswari, P. U. (2016). An energy efficient cluster head selection technique using network trust and swarm intelligence. Wireless Personal Communications, 89(2), 351-364.

Kalita, H. K., & Kar, A. (2009). Wireless sensor network security analysis. International Journal of Next-Generation Networks (IJNGN), 1(1), 1-10.

Mahajan, M., Reddy, K. T. V., & Rajput, M. (2016). Design and simulation of a blacklisting technique for detection of hello flood attack on LEACH protocol. Procedia Computer Science, 79, 675-682.

Meghdadi, M., Özdemir, S., & Güler, İ. (2008). Kablosuz Algılayıcı Ağlarında Güvenlik: Sorunlar ve Çözümler. Bilişim Teknolojileri Dergisi, 1(1).networks and countermeasures. In The first IEEE international conference on system integration and

reliability improvements (Vol. 25, p. 94).
Patil, S. S., & Khanagoudar, P. S. (2012). Intrusion Detection Based Security Solution for Cluster Based WSN. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 1(4), 331-340.
Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., Culler, D. E. "SPINS: Security Protocols for Sensor Networks", ACM Journal of Wireless Networks, 8 (5), 521-534 (2002)
Radhikabaskar, D. P., Komara, S., & Paul, V. (2014). Sinkhole Attack Detection In Hierarchical Sensor Networks. International Journal of Scientific & Engineering Research, 5(9).
Rawat, P., Singh, K. D., Chaouchi, H., & Bonnin, J. M. (2014). Wireless sensor networks: a survey on recent developments and potential synergies. The Journal of supercomputing, 68(1), 1-48.
Roosta, T., Shieh, S., & Sastry, S. (2006, December). Taxonomy of security attacks in sensor redundancy mechanism in wireless sensor networks. Procedia Computer Science, 31, 711-720.
Sahraoui, S., & Bouam, S. (2013). Secure routing optimization in hierarchical cluster-based wireless sensor networks. International Journal of Communication Networks and Information Security, 5(3), 178-185.
Salehi, M., & Karimian, J. (2017). A trust-based security approach in hierarchical wireless sensor networks. Ad Hoc Netw., 7(6), 58-67.
Sedjelmaci, H., Senouci, S. M., & Feham, M. (2012, July). Intrusion detection framework of cluster-based wireless sensor network. In Computers and Communications (ISCC), 2012 IEEE Symposium on (pp. 000857-000861
Sharma, S., Bansal, R. K., & Bansal, S. (2013, December). Issues and challenges in wireless sensor networks. In Machine Intelligence and Research Advancement (ICMIRA), 2013 International Conference on (pp. 58-62). IEEE.
Sheela, D., Srividhya, V. R., Asma, B. A., & Chidanand, G. M. (2012, July). Detecting black hole attacks in wireless sensor networks using mobile agent. In International Conference on Artificial Intelligence and Embedded Systems (ICAIES'2012).
Singh, S. K., Singh, M. P., & Singh, D. K. (2011). A survey on network security and attack defense mechanism for wireless sensor networks. International Journal of Computer Trends and Technology, 1(2), 9-17.
Tohma, K., Aydın, M. N., & Turgut, İ. A. (2015, May). Improving the LEACH protocol on wireless sensor network. In Signal Processing and Communications Applications Conference (SIU), 2015 23th (pp. 240-243). IEEE.
Tripathi, M., Gaur, M. S., & Laxmi, V. (2013). Comparing the impact of black hole and gray hole attack on LEACH in WSN. Procedia Computer Science, 19, 1101-1107.
Varga, A., & Hornig, R. (2008, March). An overview of the OMNeT++ simulation environment. In Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops (p. 60). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
W. Heinzelman, A. Chadrakasan, H. Balakrishnan, "Energy-eficient Communication Protocol for Wireless Sensor Networks", Proceeding of the Hawaii International Conference on System Sciences, January 2000
Wang, W., Du, F., & Xu, Q. (2009, September). An improvement of LEACH routing protocol based on trust for wireless sensor networks. In 2009 5th international conference on wireless communications, networking and mobile computing (pp. 1-4). IEEE.
Wazid, M., Katal, A., Sachan, R. S., Goudar, R. H., & Singh, D. P. (2013, April). Detection

and prevention mechanism for blackhole attack in wireless sensor network. In 2013 International Conference on Communication and Signal Processing (pp. 576-581). IEEE.

Younis, O., & Fahmy, S. (2004). HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Transactions on mobile computing, (4), 366-379.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : CANBOLAT, Cansu
Uyruğu : T.C.
Doğum tarihi ve yeri : 04.10.1993, Gaziantep
Medeni hali : Bekar
Telefon : 0 (539) 331 43 32
E-mail : cansucanbolat165@gmail.com

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Yüksek Lisans	İskenderun Teknik Üniversitesi / Bilgisayar Mühendisliği	2020
Lisans	İskenderun Teknik Üniversitesi / Bilgisayar Mühendisliği	2016
Lise	Ahmet Cevdet Paşa Anadolu Lisesi/Osmaniye	2012

İş Deneyimi

Yıl	Yer	Görev
2019 Eylül -Halen	Belen Halk Eğitim Merkezi	Bilişim Tek. Öğrt.
2018 Ocak-2019 Haziran	İSTE Dörtyol MYO	Yarı Z. Öğr. Gör.
2017 Eylül-2018 Ocak	İsk. BİLSEM	Bilişim Tek. Öğrt.

Yabancı Dil

İngilizce

Yayınlar

Uluslararası hakemli dergilerde yayımlanan makaleler:

1- Turgut, İpek Abasıkeleş, and Cansu Canbolat. "Analysis of packet loss under black hole and selective forwarding attacks for cluster-based wireless sensor networks." Artıbilim: Adana Bilim ve Teknoloji Üniversitesi Fen Bilimleri Dergisi 1.1: 18-24.

2- Abasıkeleş Turgut İpek, Canbolat Cansu; Review of Trust Parameters in Secure Wireless Sensor Networks

Uluslararası bilimsel toplantılarda sunulan ve bildiri kitaplarında (proceedings) basılan bildiriler:

1-Abasıkeleş Turgut İpek, Canbolat Cansu, Daşdemir Yaşar; Data Loss Rate of Cluster Based WSNs under Routing Attacks; International Congress on Engineering and Life Science

2-Abasıkeleş Turgut İpek, Canbolat Cansu, Daşdemir Yaşar; Recent Trust-Based Security Solutions for Cluster-Based WSNs; International Congress on Engineering and Life Science

3-Abasıkeleş Turgut İpek, Canbolat Cansu; Trust Based Cluster Head Selection in Wireless Sensor Networks

4. Abasıkeleş Turgut İpek, Canbolat Cansu; Kablosuz Algılayıcı Ağlarda Güven Temelli Küme Başı Seçimi

TEKNOVERSİTE

İSKENDERUN TEKNİK ÜNİVERSİTESİ

teknoversite AYRICALIĞINDASINIZ

İSTE