T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KABLOSUZ ALGILAMA AĞLARINDA GÜVEN MODELLERİ

KÖKSAL AVİNCAN

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ PROGRAMI

DANIŞMAN
YRD. DOÇ. DR. GÜLÜSTAN DOĞAN

İSTANBUL, 2015

T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

KABLOSUZ ALGILAMA AĞLARINDA GÜVEN MODELLERİ

Köksal AVİNCAN tarafından hazırlanan tez çalışması 16.06.2015 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Bilgisayar Mühendisliği Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Yrd. Doç. Dr. Gülüstan DOĞAN

Yıldız Teknik Üniversitesi

Jüri Üyeleri

Yrd. Doç. Dr. Gülüstan DOĞAN

Yıldız Teknik Üniversitesi _____

Yrd. Doç. Dr. M. Amaç GÜVENSAN

Yıldız Teknik Üniversitesi _____

Doç. Dr. Hacı Ali MANTAR

Gebze Teknik Üniversitesi _____

ÖNSÖZ

Zamanla kablosuz algılayıcı ağlara olan ilgi ciddi bir şekilde artmıştır. Algılayıcı düğümler, genel olarak pille çalışan cihazlarla benzerlik göstermektedirler. Bu sistemlerde ağın ömrü enerji miktarı ile paralellik gösterdiğinden dolayı enerji tüketiminin optimize edilmesi önemli bir yer teşkil etmektedir. Ayrıca kısıtlı enerji ve sınırlı hesaplama problemlerinden dolayı bu ağlarda güvenliği klasik kriptografik algoritmalarla sağlamak oldukça güçtür.

Bu çalışmayla birlikte güvenliği sağlayan bir güven modeli ve bu güven modelinin enerji tüketimi hesaplanılmaya ve optimize edilmeye çalışılmıştır.

Bu çalışmanın her anında bilgisi, tecrübesi, sabrı ve yol göstericiliği ile bana destek olan hocam Yrd. Doç. Dr. Gülüstan DOĞAN'a teşekkür ederim.

Hayatım boyunca benden desteğini esirgemeyen sevgili annem Necife AVİNCAN, babam Yılmaz AVİNCAN ve kardeşlerime çok teşekkür ederim.

Haziran, 2015

Köksal AVİNCAN

İÇİNDEKİLER

Sayfa

SİMGE LİSTESİ

k	Zaman aralıkları
x_k	Tahmin değeri
x_{k-1}	Önceki tahmin değeri
u_k:	Kontrol değeri
w_{k-1}	Önceki işlemin gürültüsü
z_k	Ölçülen değer
v_k	Ölçüm gürültüsü
A	Durum geçiş matrisi
B	Kontrol matrisi
H	Gözlem matrisi
$\overline{x}_k$	k anındaki tahmin değeri
$\overline{x}_{k-1}$	Tahmin sonrası, ölçümden önceki değer
$\overline{P}_k$	Ölçüm öncesi kovaryans
Q	Tahmini işlem hata kovaryansı
R	Ölçüm hata kovaryansı
$\overline{d}$	Tüm düğümlerden toplanan ortalama veri değeri
d_i	Tekil anahtar değeri i olan her bir yaprak düğümden toplanan veri değeri
t_i	Her bir düğüme ait güven değeri
k_c	Küme sayısı
α	Radyo frekans güç yükselticinin verimliliği
N_f	Alıcı gürültü miktarı
σ^2	AWGN(additive white Gaussian noise) iletim güç yoğunluğu
P_b	Faz kaydırmalı anahtarlama kullanırken elde edilen bit hata oranı
G_1	Kazanç faktörü
M_1	Kazanç marjı
B	Bant genişliği
P_{ct}	Verici devresinin güç tüketimi
P_{cr}	Alıcı devresin güç tüketimi
F_n	Bir çerçeve içindeki simgelerin sayısı
P	Her bir düğümün gönderme olasılığı
s	Paket boyutu

R_{bt}	Yönlendirme bilgi alışverişi için gerekli olan süre
R_{ts}	Yönlendirme tablosu boyutu
G_t	İleten anten kazancı
G_r	Alıcı anten kazancı
λ	İletim dalga boyu
agg	Toplama faktörü
$f(x)$	Olasılık yoğunluk fonksiyonu
μ	Verilerin ortalaması
σ	Varyans değeri
T_{data}	Düğümün güven değeri
v_d	Algılayıcının ölçtüğü değer
x	v_d veri öğesinin özniteliği

KISALTMA LİSTESİ

CMOS	Complimentary metal-oxide semiconductor
DRBTS	Distributed reputation-based beacon trust system
EDTM	Effficient Distributed Trust Model
GAF	Geographic adaptive fidelity
GPS	Global positioning system
KAA	Kablosuz algılayıcı ağlar
LED	Light emitting diode
MANET	Mobil ad hoc networks
MIMO	Multi-input and multi-output
OPM	Open provenance model
P2P	Peer to peer
RFSN	Reputation-based Framework for high integrity sensor networks

ŞEKİL LİSTESİ

Sayfa

ÇİZELGE LİSTESİ

Sayfa

ÖZET

KABLOSUZ ALGILAMA AĞLARINDA GÜVEN MODELLERİ

Köksal AVİNCAN

Bilgisayar Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Tez Danışmanı: Yrd. Doç. Dr. Gülüstan DOĞAN

Güven, kablosuz algılama ağlarında üretilen verilerin doğruluğunu ölçme konusunda önemli bir yer teşkil etmektedir. Kablosuz algılama ağlarının, düşük hesaplama yeteneğine ve enerji kısıtlamalarına sahip olmasından dolayı bu sistemlerde, enerji verimliliğini etkilemeyecek bir şekilde güvenliği sağlamak oldukça güçtür. Bu problemi çözmek amacıyla daha önce geliştirilmiş olunan ProTru adındaki mimari, birden çok atlamalı bir yapı şeklinde güncellenmiş olup ve MultiProTru adında yeni bir mimari geliştirilmiştir. ProTru'dan farklı olarak, baş düğümlerin derecelendirilmesine ve baş düğümlerin güven değerlerinin karşılaştırılmasına dayalı bir yönlendirme mekanizmasına sahip birden çok atlamalı bir mimari inşa edilmiştir. Bununla birlikte güven değerlerini hesaplamada Kalman Filtrelemesi kullanılmıştır. Yeni geliştirilen mimari, özellikle düğümlerden gelen verilerin doğruluk derecesinin kritik bir öneme sahip olduğu kablosuz algılama ağları sistemlerinde, ağın güven değerini ölçerek, verinin güvenilirliği hakkında daha açık bir bilgi edinmemizi sağlayacaktır.

Anahtar Kelimeler: Kablosuz algılama ağları, güven, enerji verimliliği, Kalman filtresi, güven modelleri

ABSTRACT

TRUST MODELS IN WIRELESS SENSOR NETWORKS

Köksal AVİNCAN

Computer Engineering

MSc. Thesis

Adviser: Ass. Prof. Dr.Gülüstan DOĞAN

Trust is an important factor in Wireless Sensor Networks in order to assess the believability of the produced data. Due to the limited computational power and energy resources of the wireless sensor networks, it is a challenge to maintain trust while using the energy efficiently. Previously we developed a trust enhancing architecture called ProTru. In order to use energy more efficiently, we developed a multi-hop version of our previous architecture called MultiProTru. In this architecture routing is done based on the trust values of the cluster heads. In MultiProTru in order to find untrusted data we used Kalman filtering approach. This new architecture will assist mission critical sensor networks in assessing the trust value of the data by calculating the network's trustworthiness.

Keywords: Wireless sensor networks, trust, energy efficiency, Kalman filter, trust models

BÖLÜM 1

GİRİŞ

Mikro elektromekanik sistemlerin yaygınlaşması ile birlikte kablosuz algılayıcı ağlarda (KAA) kullanılan akıllı algılayıcıların gelişimi hız kazanmış ve bu ağların kullanımı giderek artmıştır [1]. Algılayıcılar, sınırlı işlem yapabilme ve sınırlı hesaplama kaynaklarına sahip küçük cihazlardır ve geleneksel algılayıcılara kıyasla maliyetleri daha azdır. Algılayıcı düğümleri ölçme, hissedebilme, çevreden bilgi toplama ve topladıkları bilgiyi kullanıcılara aktarabilme yeteneklerine sahiptirler.

Akıllı algılayıcı düğümleri bir işlemci, bir bellek, bir güç kaynağı, bir telsiz, bir aktivatör ve bir veya daha fazla algılayıcı ile donatılmış düşük güç cihazlarından meydana gelmektedirler. Mekanik, termal, biyolojik, kimyasal, optik ve manyetik algılayıcılar çeşitli ortamların özelliklerini ölçmek için algılayıcı düğüme bağlanmış olabilirler. Algılayıcı düğümler, sınırlı hafızaya sahip olmalarından ve genellikle erişimin zor olduğu yerlere dağıtılmalarından dolayı bir baz istasyonuna veri aktarmaları için bir telsiz ile donatılmışlardır.

Pil, bir algılayıcı düğümün ana güç kaynağıdır. Çevreden güç toplayan güneş panelleri gibi güç kaynakları da algılayıcının konuşlandırıldığı alanın şartlarına göre sisteme enerji aktarması için kullanılabilir. Uygulamanın ve kullanılan algılayıcıların tipine bağlı olarak, aktüatörler de algılayıcılara dâhil edilebilir.

Bir kablosuz algılama ağının sahip olduğu ağ altyapısı ya az bir seviyededir ya da hiç yoktur. Bu ağlar, çevre ile ilgili verileri elde etmek ve bir bölgeyi izlemek için birlikte çalışan binlerce algılayıcı düğümden oluşurlar. Kablosuz algılama ağlarının iki tipi vardır:

- Yapılandırılmış kablosuz algılama ağları
- Yapılandırılmamış kablosuz algılama ağları

Yapılandırılmamış kablosuz algılama ağları, yoğun algılayıcı düğümlerinin bir araya gelmesiyle oluşur. Algılayıcı düğümleri, alana rastgele bir şekilde dağıtılabilir. Dağıtım işleminden sonra ağ, izleme ve raporlama işlevlerini gerçekleştirmek için gözetimsiz bırakılır. Bir yapılandırılmamış kablosuz algılama ağında çok sayıda düğüm olduğundan dolayı bağlantı yönetme ve arızaları tespit gibi şebeke bakım işlemlerini yapmak oldukça güçtür.

Yapılandırılmış bir kablosuz algılama ağında ise algılayıcı düğümlerin bazıları veya hepsi önceden planlanmış bir şekilde bilgi toplayacakları alana dağıtılır. Yapılandırılmış bir ağın temel avantajı, az düğümlerin düşük bir şebeke bakımı ve yönetim maliyeti ile dağıtılabilmesidir.

Kablosuz algılama ağları askeri hedef izleme ve gözetim [2], [3] doğal afet yardımı [4], biyomedikal sağlık izleme [5], [6] tehlikeli çevreleri keşif ve sismik algılama [7] gibi birçok senaryoda uygulama alanına sahiptir. Askeri hedef izleme ve gözetiminde kullanılan bir kablosuz algılama ağ sistemi, saldırı tespit ve tanımlanma işlemlerinde katkı sunabilir. Doğal afetlerde ise algılayıcı düğümler, afetler meydana gelmeden önce bu afetleri algılayabilir. Biyomedikal uygulamalarda ise algılayıcılar hastanın sağlığını izleme noktasında fayda sağlayabilir. Son olarak sismik algılama içinse volkanik alana rastgele bir şekilde dağıtılmış algılayıcılar, deprem ve patlamalar gibi gelişmeleri algılayabilir.

Geleneksel ağlardan farklı olarak kablosuz algılama ağlarının tasarım ve kaynak kısıtları gibi problemleri vardır. Kaynak kısıtlamalarını sınırlı enerji miktarı, kısa iletişim aralığı, düşük bant genişliği ve sınırlı işleme ve depolama şeklinde tanımlayabiliriz. Tasarım kısıtlamaları uygulamaya bağlıdır ve izlenen ortama göre değişebilmektedir. Çevre ağının büyüklüğü, dağıtım şeması ve ağ topolojisinin belirlenmesinde önemli bir rol oynar. Ağın büyüklüğü izlenen ortama göre değişir. Kapalı ortamlarda, sınırlı bir alanda ağ oluşturmak için daha az düğüme ihtiyaç duyulurken, açık ortamlarda daha geniş bir alan olacağından dolayı daha fazla düğüme ihtiyaç duyulabilir. Çevrenin insanlar tarafından erişilemez olduğu veya ağdaki düğüm sayısının çok fazla olduğu durumlarda

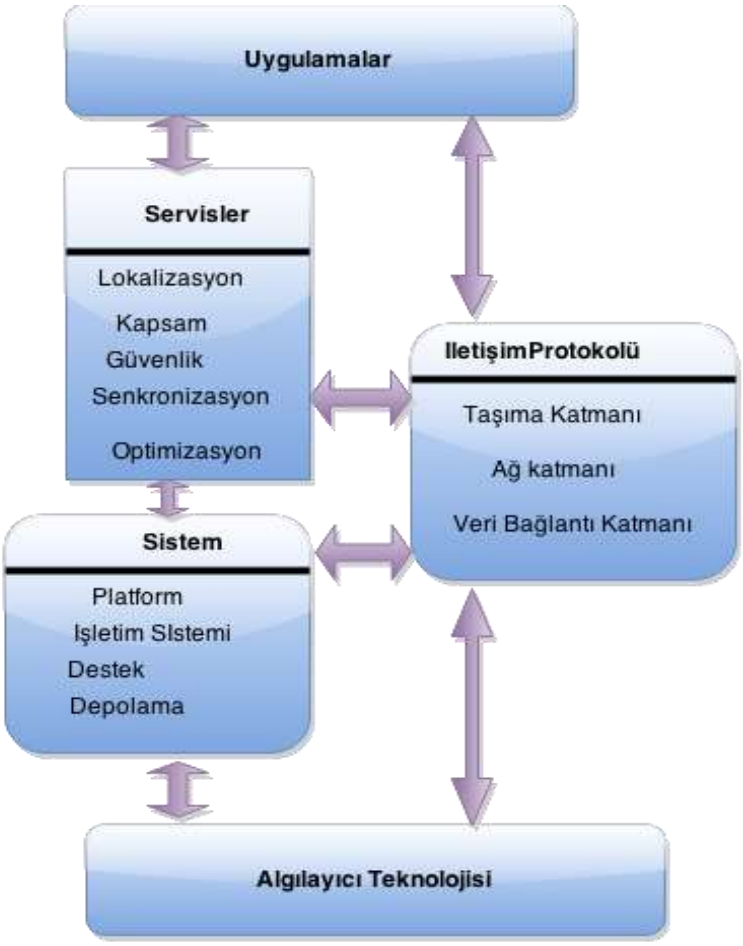
ad-hoc dağıtım tercih edilebilir. Ortamdaki engeller de düğümler arasındaki iletişimi engelleyebilir.

1.1 Literatür Özeti

Algılayıcı teknolojisi, kablosuz algılayıcı uygulamalarını geliştirmek ve tasarlamak için çözüm sağlar. Piyasadaki algılayıcılar, genel (çok amaçlı) düğümleri ve ağ geçidi(köprü) düğümlerini içerir. Bir genel algılayıcı düğümünün görevi, izlenen ortamdaki ölçümleri almaktır. Bu düğümler ışık, sıcaklık, nem, basınç, hız, ivme ve manyetik alan gibi çeşitli fiziksel özellikleri ölçebilen çeşitli cihazlar ile donatılmış olabilirler. Ağ geçidi (köprü) düğümleri ise genel algılayıcılardan gelen verileri toplar ve bu verilerin baz istasyonuna iletimini sağlarlar. Ağ geçidi düğümleri daha yüksek işleme yeteneği, pil gücü ve iletim aralığına sahiptirler. Genel ve ağ geçidi düğüm birleşimi, tipik bir kablosuz algılama ağı oluşturmak için dağıtılır.

Algılayıcı teknolojilerini kullanarak kablosuz algılayıcı uygulamalarını etkinleştirmek için, görev sınıfları Şekil 1.1'de gösterildiği üzere 3 temel sınıfa ayrılır. Birinci grup, sistemdir. Her algılayıcı düğümü bağımsız bir sistemdir. Bir algılayıcı sistemindeki farklı uygulama yazılımlarının desteklenmesi amacıyla yeni platformlar, işletim sistemleri ve depolama programlarının geliştirilmesi gereklidir. İkinci grupta ise uygulama ile algılayıcılar arasındaki iletişimi sağlayan haberleşme protokolleri vardır. Bu protokoller de algılayıcı düğümleri arasındaki iletişimi sağlarlar. Son grupta ise uygulamayı güçlendirmek, sistem performansı ve ağ verimliliğini artırmak için geliştirilen servisler vardır.

Uygulama gereksinimleri ve ağ yönetim perspektifinden dolayı algılayıcı düğümlerinin kendi kendilerine organize olabilme yeteneğine sahip olmaları önemlidir. Algılayıcı düğümlerin güç, işlemci kapasitesi ve depolama miktarları sınırlı olduğundan yeni iletişim protokolleri ve yönetim hizmetlerinin öz organizasyonunu yerine getirmeleri için bazı gereksinimlere ihtiyaçları vardır.



Şekil 1. 1 Kablosuz algılama ağlarının farklı konularda sınıflandırılması

İletişim protokolü paket anahtarlama için beş standart protokol katmandan oluşur:

- Uygulama Katmanı
- Ulaşım Katmanı
- Ağ Katmanı
- Veri Bağlantı Katmanı
- Fiziksel Katman

Protokol yığınındaki farklı katmanlarda protokollerin uygulanması enerji tüketimini, uçtan uca gecikme ve sistem verimliliğini önemli ölçüde etkileyebilir. Bu iletişimi optimize etmek ve enerji kullanımını en aza indirmek için önemlidir. Geleneksel ağ protokolleri kablosuz algılama ağlarının gereksinimlerini karşılamak için tasarlanmadığından dolayı bu ağ protokolleri kablosuz algılama ağları için pek uygun değildir. Bu nedenle, protokol yığınındaki her katman için yeni enerji tasarruflu

protokoller önerilmiştir. Bu protokoller, protokol katmanları arasındaki etkileşimi destekleyerek çapraz katmanlı optimizasyonu kullanır. Özellikle belli bir katmanda protokol durum bilgisi, kablosuz algılama ağlarının özel gereksinimlerini karşılamak için tüm katmanlar arasında paylaşılır.

Enerji toplama, bir düğümün bir enerji kaynağından enerji ikmali yapma işlemidir. Potansiyel enerji kaynakları güneş hücreleri [8], [9] titreşim [10], akaryakıt hücreleri, akustik gürültü ve mobil tedarikçi [11] olarak düşünülebilir. Çevreden enerji toplama bakımından [12], ışıktan enerji toplayan güneş pilinin en güncel teknik olduğu söylenebilir. Ayrıca enerjiyi güncellemek noktasında robot teknolojisi de kullanılabilir.

1.1.1 Kablosuz Algılama Ağları Türleri

Şu anki kablosuz algılama ağları kara, yeraltı ve su altı gibi alanlar üzerine kurulmaktadır. Ortama bağlı olarak, bir algılayıcı ağı farklı zorluklar ve kısıtlamalar ile karşı karşıya kalabilir. Bu zorluklar temel alınarak kablosuz algılama ağları 5 sınıfa ayrılabilir.

- Karasal kablosuz algılama ağları
- Yeraltı kablosuz algılama ağları
- Su altı kablosuz algılama ağları
- Multi-medya kablosuz algılama ağları
- Mobil kablosuz algılama ağları

Karasal kablosuz algılama ağları [13], ad-hoc veya önceden belirlenmiş bir alana dağıtılan binlerce ucuz kablosuz algılayıcı düğümlerinden oluşur. Ad-hoc dağıtımında, algılayıcı düğümler rastgele hedef alana yerleştirilir. Önceden planlanmış dağıtımda ise grid yerleştirme, en uygun yerleştirmedir [14]. 2-d ve 3-d yerleştirme [15], [16] gibi modeller de vardır.

Bir karasal kablosuz algılama ağında, yoğun bir ortamdaki güvenilir iletişim çok önemlidir. Karasal algılayıcı düğümlerinin baz istasyonuyla etkili veri iletişimi kurabilmesi gerekir. Pil gücünün sınırlı olduğu veya şarj edilebilir durumda olmadığı zaman karasal algılayıcılar ancak güneş hücreleri gibi ikincil bir güç kaynağı ile

donatılabilir. Her durumda, algılayıcı düğümlerinin enerji tasarrufu önemlidir. Ağ verilerini toplama, veri fazlalığını ortadan kaldırmada, gecikmeleri en aza indirmede enerji birden çok atlamalı optimal ve kısa iletim menzili ile muhafaza edilebilir.

Yeraltı kablosuz algılama ağları [17], [18] yeraltında gömülü olan veya bir mağarada madeni yeraltı koşullarını izlemek için kullanılan algılayıcı düğümlerinin bir araya gelmesiyle oluşur. Ek alıcı düğümleri, algılayıcı düğümlerden baz istasyonuna bilgi geçişinin sağlandığı yerde bulunmaktadır. Bir yeraltı kablosuz algılama ağının donanımları, dağıtım ve bakım açısından bir karasal kablosuz algılama ağından daha pahalıdır çünkü toprak, kaya, su ve diğer mineral içerikleri ile güvenli iletişim sağlamak için uygun donanım parçalarının seçilmesi gerekmektedir. Yeraltı çevrelerindeki kablosuz iletişimde sinyal kayıpları veya sinyalin yüksek düzeyde zayıflaması gibi sorunlarla karşılaşılma ihtimali fazladır. Karasal kablosuz algılama ağlarının aksine, yeraltı kablosuz algılama ağlarının dağıtımı daha dikkatli planlama, enerji ve maliyet analizleri gerektirir. Enerji, yeraltı kablosuz algılama ağları için önemli bir hususdur. Karasal kablosuz algılama ağları gibi, yeraltı algılayıcı düğümleri de sınırlı pil gücü ile donatılmışlardır ve bu algılayıcı düğümleri toprağa yerleştirildikten sonra bu düğümlerin bataryasını değiştirmek oldukça zordur. Daha önce de olduğu gibi önemli bir amacı, etkin iletişim protokolünü uygulayarak, ağ ömrünü artırmak için enerji tasarrufu sağlamaktır.

Su altı kablosuz algılama ağları [19], [20] su altına dağıtılan algılayıcı düğümlerinden ve araçlarından oluşur. Karasal kablosuz algılama ağlarının aksine, su altı kablosuz algılama ağları daha pahalıdır ve bilgi toplayacağı alana daha az sayıda dağıtılırlar. Bağımsız su altı araçları, algılayıcı düğümlerinden veri toplama veya arama için kullanılır. Bir karasal kablosuz algılama ağındaki algılayıcı düğümlerinin yoğun bir dağıtım ile karşılaştırıldığında, su altındaki düğümlerin daha seyrek dağıtıldığı görülecektir. Tipik su altı kablosuz iletişimler, ses dalgaların iletimi yoluyla kurulmuştur. Su altı ses dalgalarının en temel sorunları olarak sınırlı bant genişliği, uzun yayılım gecikmesi ve sinyallerin düşmesi gösterilebilir. Başka bir sorunsa, çevre koşullarına bağlı olarak algılayıcı düğümlerinin başarısız olmasıdır. Su altı algılayıcı düğümleri, sert okyanus ortamına uyum sağlamak ve kendini yapılandırabilmek zorundadırlar. Su altı algılayıcı düğümleri değiştirilemez veya şarj edilemez sınırlı bir batarya ile

donatılmıştır. Su altı kablosuz algılama ağlarında enerji tasarrufu sorunu çözmek için verimli su altı iletişim ve ağ tekniklerinin geliştirilmesi gerekmektedir.

Multimedya kablosuz algılama ağları video, ses ve görüntüleme gibi olayların izlenmesinde kullanılmaktadır. Multimedya kablosuz algılama ağları, kameralar ve mikrofonlarla donatılmış düşük maliyetli algılayıcı düğümlerinin bir araya gelmesiyle oluşmaktadır. Algılayıcı düğümleri veri alma, veri işleme, korelasyon ve veri sıkıştırma için kablosuz bağlantı üzerinden birbirleri ile bağlantı kurmaktadırlar. Multimedya algılayıcı düğümleri, kapsama alanını garanti altına almak için ortama önceden planlanmış bir şekilde dağıtılırlar. Multimedya kablosuz algılama ağlarında karşılaşılan zorluklara yüksek bant genişliği talebi, yüksek enerji tüketimi, servis kalitesi, veri işleme ve sıkıştırma teknikleri örnek verilebilir. Video akışı gibi bir multimedya içeriğinin teslim edilebilmesi için yüksek bant genişliği gerekir. Bunun bir sonucu olarak yüksek veri oranı yüksek enerji tüketimine yol açar. Bu nedenle yüksek bant genişliği ve düşük enerji tüketimini destekleyen iletim tekniklerinin geliştirilmesi gerekmektedir. Bir multimedya kablosuz algılama ağı içinde kaliteli servis sağlama, değişken gecikme ve değişken kanal kapasitesi nedeniyle zor bir iştir. Servis kalitesinin, güvenilir içerik teslimatı için belirli bir seviyede olması önemlidir. Ağdaki işleme, filtreleme ve sıkıştırma işlemleri filtreleme açısından ağ performansını artırmak ve gereksiz bilgileri ayıklamak ve içeriğini birleştirmek adına çok önemlidir.

Mobil kablosuz algılama ağları, kendi başlarına hareket edebilen ve fiziksel çevreyle etkileşim içerisinde olan algılayıcı düğümlerin bir araya gelmesiyle oluşmaktadır. Mobil düğümler algılama, hesaplama ve statik düğümlerle iletişim gibi yeteneklere sahiptirler. Mobil düğümlerin en önemli farkları ise ağda kendilerini organize edebilme ve konumlandırma yeteneklerinin olmasıdır. Bir mobil kablosuz algılama ağı ön bir dağıtım ile başlar ve daha sonra düğümler bilgi toplamak amacıyla yayılırlar. Birbirlerinin hâkim oldukları alanlar içerisinde olunduğunda, bir mobil düğüm tarafından toplanan bilgiler, başka bir mobil düğüme iletilebilir. Bir başka önemli fark ise veri dağıtım işlemidir. Bir statik kablosuz algılama ağında, veri sabit yönlendirme kullanılarak dağıtılabilir ama bir mobil kablosuz algılama ağında veri dinamik yönlendirme kullanılarak dağıtılabilir. Mobil kablosuz algılama ağlarında karşılaşılan

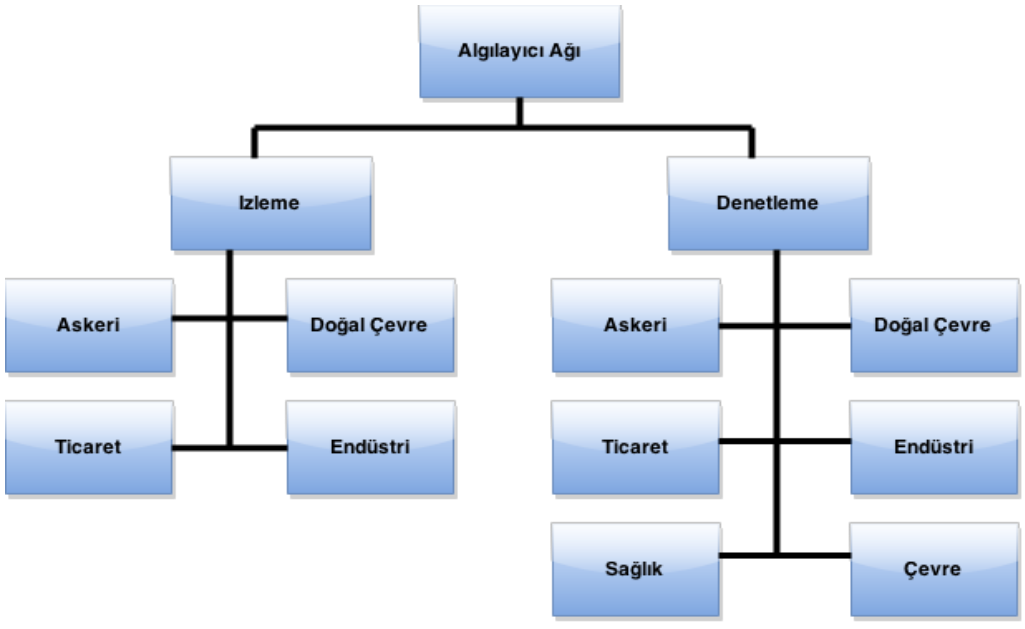
zorluklara dağıtım, lokalizasyon, öz-örgütlenme, navigasyon ve kontrol, kapsama alanı, enerji, bakım ve veri işleme sayılabilir.

Mobil kablosuz algılama ağ uygulamaları çevre izleme, hedef izleme, arama, kurtarma ve tehlikeli maddeleri gerçek zamanlı izleme ile sınırlı değildir. Afet bölgelerinde çevresel izleme için, elle dağıtım mümkün olmayabilir. Mobil algılayıcı düğümlerinin yerleri, gerekli kapsama sağlamak için dağıtımdan sonra olayların oldukları yere doğru değiştirilebilir. Askeri gözetim ve izlemede de, mobil algılayıcı düğümleriyle iş birliği yapabilir ve hedefe dayalı kararlar alınabilir. Mobil düğümler statik düğümlerle karşılaştırıldığı zaman mobil düğümlerin daha yüksek seviyede bir kapsama alanı ve bağlantı oluşturduğu görülecektir. Alanda engellerin bulunması durumunda, mobil algılayıcı düğümler ileriye dönük plan yapabilir ve hedefe maruz kalabileceği alanlardan daha uygun alanlara doğru hareket edebilir.

1.1.2 Kablosuz Algılama Ağlarının Uygulama Alanları

Kablosuz algılama ağ uygulamaları iki kategoriye ayrılabilir (Şekil 1.2) :

- İzleme
- Takip



Şekil 1. 2 Algılayıcı uygulamalarına genel bakış

İzleme uygulamaları açık -kapalı çevre izleme, sağlık ve sağlıklı yaşam izleme, enerji izleme, stok yeri izleme, fabrika ve işlem otomasyonu ve sismik ve yapısal izlemeyi içerir.

Takip uygulamaları ise nesneleri, hayvanları, insanları ve araçları takibi içerir. Birçok farklı uygulamalar olmakla birlikte, aşağıda gerçek ortamda dağıtılan ve sınanmış bir kaç örnek uygulama gösterilmiştir.

PinPtr [2], atıcıları algılamak ve bulmak için geliştirilmiş bir deneysel, karşıt keskin nişancı sistemidir. Namlu patlamasının varış zamanını ve merminin çarpma dalgasını ölçmek ve algılamak için algılayıcılar yoğun bir şekilde alana dağıtılır. Daha sonra algılayıcılar, atıcının yerini hesaplamak için kendi ölçümlerini bir baz istasyonuna yönlendirirler.

Macroscope of redwood [21], Sonoma ve Kaliforniya kızılağaçlarını kaydeden ve izleyen bir kablosuz algılama ağı çalışmasıdır. Her algılayıcı düğümü hava sıcaklığı, bağıl nem ve aktif güneş radyasyon bilgilerini ölçer. Algılayıcı düğümleri ağacının farklı yüksekliklerine yerleştirilir. Bu çalışmada bitki biyologları, bir sekoya ağacının etrafındaki mikro iklimin mekânsal geçişlerindeki değişiklikleri izlemeye çalışmış ve kendi biyolojik teorilerini doğrulamaya çalışmışlardır.

Su altı izleme çalışmasında [22], mercan kayalıkları ve su ürünlerinin uzun vadeli izlenmesi için algılayıcı ağlarının kullanıldığı bir platform geliştirilmiştir. Algılayıcı ağı, statik ve mobil su altı algılayıcı düğümlerinden oluşmaktadır. Düğümler, yüksek hızlı optik iletişimi kullanarak noktadan noktaya linkler aracılığı ile iletişim kurar. Düğümler, TinyOS protokol yığınına entegre olan bir ses protokolünü kullanarak yayın yaparlar. Bu platformda sıcaklık ve basınç algılama cihazları ve kameralar gibi farklı algılama cihazları kullanılmıştır. Mobil düğümler, yeniden konumlandırma ve kurtarma ve ağ bakım işlevlerini yerine getirmek için statik düğümler üzerinden hareket edebilirler. Bu çalışma, bir su altı ortamına algılayıcıları dağıtma noktasında karşılaşılan zorlukları ve sorunları anlama noktasında katkı sağlamıştır.

MAX [23], fiziksel dünyada insan merkezli arama için tasarlanmış bir sistemdir. MAX, ihtiyaç duyulduğunda kişilerin fiziksel nesneleri aramasını ve bulmasını sağlar.

Tanımlanabilir konumdan ziyade kesin koordinata dayalı bir konum bilgisi sağlar. MAX gizlilik, hedefleme, etiketlenmiş nesneyi etkin arama ve insan merkezli çalışma düşünülerek tasarlanmıştır.

CenWits [24], Berkeley Mica2 algılayıcısı kullanılarak uygulanan, tasarlanan ve değerlendirilen bir arama kurtarma sistemidir. Sistem, birkaç küçük radyo frekans tabanlı algılayıcıyı ve az sayıda depolama ve işleme mekanizmalarını kullanır. CenWits, sürekli ağa bağlı bir sistem değildir. Aralıklı ağ bağlantısı için tasarlanmıştır. Bu sistem deneklere(insanlara) giydirilen mobil algılayıcılar aracılığıyla, bazı diğer algılayıcılardan ve GPS alıcılardan bilgi toplar ve algılayıcılara konum bilgisi gönderir. Bir denek, konumunu belirlemek için GPS alıcıları ve konum noktalarını kullanır. Bu sistemde kullanılan bir diğer önemli kavram ise bir deneğin hareketini iletmek ve dış dünyaya konum bilgisi göndermek için tanıkların kullanılmasıdır. CenWits'in amacı küçük bir alandaki arama kurtarma çalışmalarına katkı sağlamaktır.

Cyclops [25], küçük bir kamera cihazı tarafından kısıtlı hesaplama yeteneğine sahip algılayıcı düğümleri ile metal oksit yarı iletken (CMOS) kameralar arasında köprü kuran bir sistemdir. Bu çalışma algılayıcı teknolojisi ile CMOS(complimentary metal-oxide semiconductor) görüntülemeyi sağlar. Cyclops, bir kamera modülü ve bir hafif algılayıcı düğüm arasındaki arayüzle çalışır. Cyclops, yüksek hızlı veri aktarımı ile programlanabilir mantık ve hafıza devreleri ve dış dünya ile arayüz oluşturan bir mikro-denetleyici içerir. Cyclops'un yüksek hızda işlem ve yüksek çözünürlüklü görüntüler gerektiren birçok uygulamada yarar sağladığı görülecektir.

Bir petrol tesisinde [26] kablosuz algılama ağları, maliyeti azaltır ve verimliliği artırır. Bu ağın tasarımında, veri hızına ve tesisin gecikme gereksinimine odaklanılmıştır. Ağ, dört algılayıcı düğümü ve bir aktüatör düğümü içerir.

Volkanik olaylarda [7] kablosuz algılama ağlarının kullanılması dağıtım, kurulum ve bakım işlemelerini hızlandırma noktasında fayda sağlar. Kablosuz algılama ağ donanımları küçük, hafif ve daha az güç tüketirler. Volkanik olaylarda kablosuz algılama ağları veri toplama evresinde güvenilir olay algılama, verimli veri toplama, yüksek veri hızları ve düğümlerin seyrek dağıtımı gibi zorluklarla karşılaşılabilir. Bu zorluklar göz önüne alınarak, Kuzey Ekvador Volcán Reventador üzerine 16 algılayıcı düğümden

oluşan bir ağ konuşlandırılmıştır. Her algılayıcı düğüm birçok yönlü anten, bir sismograf, bir mikrofon ve özel bir donanım arayüz kartı ile donatılmıştır.

Sağlık izleme uygulamalarında [27] kablosuz algılama ağlarının kullanımı, mevcut sağlık ve hasta izleme hizmetlerinin gelişmesine katkı sunmaktadır. Bebek izleme, sağır uyarıcı, kan basıncı gözetim ve izleme uygulamaları için prototipler geliştirilmiştir. İki tip prototipi vardır. Bunlar T-mote sky devices and SHIMMER (Intel Digital Health Group's Sensing Health with Intelligence, Modularity, Mobility, and Experimental Re-usability)'dir.

Fireline, kablosuz kalp atış hızı algılama sistemidir. Bir itfaiyecinin, herhangi bir anormallik ve stres anında gerçek zamanlı olarak kalp atışlarının izlenmesi için kullanılır. FireLine, özel yapım bir kalp hızı algılayıcısından ve 3 adet yeniden kullanılabilir elektrottan oluşur. Tüm bu bileşenler, itfaiyecinin giyineceği koruyucu elbisesinin içerisine gömülür. İtfaiyecinin kalp hızı çok yükselirse, bir uyarı mesajı gönderilir.

Heart@Home kablosuz tansiyon izleme sistemidir. Bir kullanıcının, kan basıncı ve kalp atış hızı Osilometrik yöntem kullanılarak hesaplanmıştır. SHIMMER okunan değerleri kaydeder ve kullanıcının bilgisayarına bilgi gönderir.

LISTSENse, işitme engellilerinin kendi ortamındaki seslerden haberdar olmasını sağlar. Bir kullanıcı onu T mote baz istasyonuna taşır. T-mote baz istasyonu, bir vibratör ve ledlerden oluşmaktadır. İletici mote yakınındaki nesneleri (örneğin, duman alarmı ve kapı zili) duyabilir. İletici motelar çok yönlü bir kondansatör mikrofondan oluşmaktadır. Bu iletici motelar düzenli olarak 20 Hz hızında mikrofon sinyalini gönderirler. Sinyalin referans sinyalinden büyük olması durumunda, şifrelenmiş bir aktivasyon mesajı kullanıcıya gönderilir. Mesajı alan T-Mote baz istasyonu, kullanıcıyı uyarmak için vibratör ve LED ışıklarını etkinleştirir. Kullanıcının alarmı devre dışı bırakması için onaylama butonuna basması gerekir.

ZebraNet [9] sistemi, hayvan geçişlerini izlemek için kullanılan bir mobil telsiz algılayıcı ağıdır. ZebraNet, zebraların yakasına yerleştirilen algılayıcı düğümlerinden oluşur. Düğümler 16-bitlik bir TI mikro denetleyiciden, 4 Mbit'lik off-chip flaş bellekten, 900 MHz radyo ve bir GPS ünitesinden oluşur. Zebraların konum bilgileri, GPS kullanılarak

alınır ve baz istasyonuna zebraların konum bilgileri birden çok atlamalı bir şekilde gönderilir. Bu sistemin temel amacı zebraların konum bilgilerini doğru bir şekilde tutmak ve bu verileri kullanmaktır.

1.1.3 Kablosuz Algılama Ağlarının Amacı ve Kapsamı

Bir kablosuz algılama ağı, kendi kendine organize olabilen düğümlerin geçici olarak oluşturduğu ağların bir araya gelmesiyle oluşmaktadır. Bu yapılarda merkezi ağ yönetimi veya ağ altyapısı önceden tanımlı değildir. Bu düğümler birbirleriyle, radyo sinyalleri aracılığıyla iletişime geçerler. Radyo sinyallerinin iletim aralığı sınırlıdır. Bu yüzden birbirinden uzak düğümler, birden çok atlamalı stratejisiyle iletişim kurarlar. Her bir düğüm, bir yönlendirici ve bir host gibi hareket eder [28]. Düğümler arasında çok düşük bir veri iletim kapasitesi ve bant genişliği vardır. Kablosuz algılayıcı ağların bir diğer özelliği ise sınırlı güce sahip olmaları ve enerjilerinin kolayca bitmesidir. Düğümler bir ağa herhangi bir zaman aralığında katılabilir veya bu ağdan herhangi bir zaman dilimi içerisinde ayrılabilirler. Ayrıca düğümler dinamik ağ topolojisinin sonucu olarak konumlarını değiştirebilme özelliğine de sahiptirler. Düğümler bir MANET'in sahip olduğu zorluklarla da karşılaşabilirler. MANET'tekine benzer karşılaşılan sorunlara ek olarak kablosuz algılayıcı ağların altyapının olmaması, hareketlilik, bağlantı eksikliği ve kablosuz algılayıcı ağlarının kısıtlı hesaplama kapasitelerinin olması sayılabilir. Kablosuz algılayıcı ağları için güven modellerinin geliştirilmesindeki temel etmen bu problemlere çözüm üretebilmektir [28].

Bir algılayıcı düğümü 4 alt sistemden oluşur. Bunlar:

- **Bilgisayar Alt Sistemi (İşlemci ve Bellek) :** Bu yapı algılayıcıları kontrol eder ve iletişim protokollerini yürütür.
- **Haberleşme Alt Yapısı (Alıcı-Verici) :** Bu yapı komşu düğümlerle iletişimi sağlar.
- **Algılama Alt Sistemi (Algılayıcı) :** Düğümün dış dünyaya bağlanmasını sağlar.
- **Güç Kaynağı Alt Sistemi(Batarya veya Pil) :** Bu yapı ise düğümün çalışması için gerekli olan enerjiyi tutar ve gerektiği zaman düğümün bu enerjiyi kullanması için servis işlemi görür.

Küçük ve maliyetlerinin düşük olması sebebiyle, askeri alanlar gibi gözetimi zor bölgelerde dahi kullanılmaktadır. Küçük ve düşük maliyetli bu algılayıcılar hâkim oldukları bölgelerden veri bilgisini toplar ve bu verileri işlemek için genel merkeze gönderirler [13].

Bazı algılayıcı ağlarının, klasik veri tabanı yapılarının sahip olduğu, veri üzerinde kontrol yapabilme mekanizmaları yoktur. Algılayıcı ağlar kontrol edilemez bir yapıya sahip olduğundan dolayı verinin, sistemi kuran kullanıcının haberi olmadan kopyalanabilmesi, taşınabilmesi, oluşturulabilmesi, güncellenebilmesi ve silinebilmesi gibi problemlerle karşılaşabilir. İşte tam bu noktada provenans verinin güvenirliği, doğruluğu ve doğrulunabilirliğinin ölçülmesinde büyük rol oynar. Kablosuz algılayıcı ağlarında hata toleransı, sorun giderme, sonuç üretme ve performans optimizasyonu gibi daha sonra kullanılmak üzere elde edilen sonuçların nasıl bir anlama geldiğini yorumlamak için provenans yönetimi geliştirilirken daha dikkatli olunmalıdır.

1.2 Tezin Amacı

Günümüzde kablosuz algılama ağları teknolojisinin günlük hayatta kullanımı oldukça artmıştır. Özellikle algılayıcı üretim fiyatının düşmesiyle birlikte bu kullanım pozitif noktada bir ivme kazanmıştır. Bu kullanımın artmasıyla beraber kablosuz algılama ağlarında karşılaşılan sorunlar daha da ilgi çekici hale gelmiştir. Bu problemlerin en göze çarpanları güvenlik ve enerji sorunlarıdır. Kablosuz algılama ağlarının kısıtlı düzeyde işlem yapabilme kapasitesine ve sınırlı miktarda enerjiye sahip olmalarından dolayı bu ağlarda güvenliği klasik kriptografik algoritmalarla gerçekleştirmek oldukça güçtür. Klasik kriptografik algoritmaların zaman ve bellek karmaşıklıklarının büyük olması bunun en temel nedenidir.

Yukarıda tanımlanan problemler doğrultusunda daha önce geliştirilen ProTru[29] adındaki mimari birden çok atlamalı bir yapı şeklinde genişletilmiş ve MultiProTru mimarisi geliştirilmiştir. Birden çok atlamalı mimari geliştirilirken de enerji ve güvenlik paralel olarak optimize edilmeye çalışılmıştır.

ProTru mimarisinde güvenliği sağlamak adına kullanılan veri benzerliğine dayalı yaklaşımın eksik noktaları tespit edilmiş ve eksiklik Kalman filtresi kullanılarak giderilmeye çalışılmıştır.

Enerji noktasında da verim alabilmek için iletim esnasında kullanılan veri miktarı en az seviyeye çekilmeye çalışılmıştır.

1.3 Hipotez

Algılayıcı düğümlerinin sınırlı pil gücüyle çalışmasından dolayı enerji kullanımı kablosuz algılama ağları için çok önemli bir husustur. Bundan dolayı enerji tüketiminin minimize edilmesi ve enerjinin toplanması hep ilgi çeken bir konu olmuştur. Bir algılayıcı düğümün enerjisinin tükenmesi, algılayıcının kullanılmaz hale gelmesi ve bağlantının kopması gibi uygulamanın performansını etkileyecek durumlara sebebiyet verebilir. Algılayıcının ağ ömrü, ağdaki aktif düğümlere ve bağlantı sayısına bağlıdır. Bu yüzden ağ ömrünün uzaması için enerjinin verimli kullanılması gerekir.

Bu çalışma kapsamında daha önce geliştirilmiş olunan ProTru mimarisi birden çok atlamalı bir şekilde güncellenmiştir. Güncellenen yeni mimariye MultiProTru ismi verilmiştir. ProTru mimarisinde sadece yaprak düğümlerden baş düğümlere doğru bir veri akışı vardır. Bu veri akış modeli de baz istasyonuna uzak olan baş düğümlerin enerji verimliliğini olumsuz yönde etkilemektedir. ProTru mimarisinin bu sorununu çözmek adına baz istasyonuna uzak olan baş düğümlerin veri iletiminde baz istasyonuna daha yakın olan bir diğer baş düğümü kullanmaları amaçlanmıştır. Bu sayede baş düğümlerin enerji verimlilik oranı artırılmaya çalışmıştır.

ProTru mimarisinde güvenliği sağlamak adına veri benzerliğine dayalı bir algoritma kullanılmıştır. Bu tez kapsamında veri benzerliğine dayalı yaklaşımın eksik noktaları saptanmıştır ve bu eksiklik çözmek adına Kalman filtresi yöntemi kullanılmıştır ve yeni geliştirilen mimariye MultiProTru adı verilmiştir. Literatürde kablosuz algılama ağlarının güven değerlendirilmesinde Kalman filtresi yönteminin kullanıldığı herhangi bir çalışmaya rastlanılmamıştır.

BÖLÜM 2

KABLOSUZ ALGILAMA AĞLARINDA GÜVEN

Güven, kablosuz algılama ağları gibi kendi kendini yönetebilen ve yapılandırabilen sistemler için oldukça önemli bir kavramdır. Kablosuz algılama ağları, sınırlı hesaplama yeteneğine ve enerji noktasında kısıtlı imkânlara sahip olmaları ve ağ saldırılarına maruz kalabilme ihtimalleri dolayısıyla çok hassas bir yapıya sahiptirler. Buna ek olarak bir kablosuz algılama ağının dışarıdaki fiziksel saldırılara da açık olması ayrı bir sorun teşkil etmektedir. Bir kablosuz algılama ağında güven yönetim modeli, bir düğüm arızası veya aksaklığı meydana geldiği zaman, bu hataları ve aksaklıkları tolere edebilir bir noktaya çekmek için karar verme sürecinde etkili bir rol alır. Örneğin, bir düğüm başka bir düğümle bu güven modelini temel alarak iş birliği yapmaya karar verebilir. Güven konusunda yapılan çalışma sayısının az olduğu göz önüne alındığında bu araştırma konusunun yeni olduğu çıkarımı yapılabilir [30], [31]. Daha çok P2P ağlar ve Ad-hoc ile ilgili çalışmalarda güven kullanılmıştır. Bu ağ tiplerinin birbirine çok benzer olmasına rağmen kablosuz algılama ağlarının sınırlı işlem yapabilme kapasitesine sahip olmaları ve enerji noktasındaki kısıtlarının olması nedeniyle hala yeni güven yönetim modelleri geliştirilmeye çalışılmaktadır.

Veri toplama işlemi, güven yönetim modeli tasarımı sürecinde oldukça önemlidir. Bu bağlamda daha önceki sistem geçmişi bilinmeli ve geçmiş davranışları göz önüne alınmalıdır [32]. Bizim sistemimiz de geçmişteki davranışları hesaplama ve analiz etme noktası düşünülerek tasarlanmıştır. Ayrıca her düğüm geçmiş zaman aralıklarında oluşturulan verilerin hata payını göz önüne alarak, bu hata paylarıyla ilgili istatistiki bilgi tutabilme yeteneğine sahiptir. Yalnız, bu istatistiki bilgilerin güven modeline büyük

bir yük getirmesi en büyük kısıtlayıcı etkenlerden birisidir. Bu yüzden güven modellerinin sisteme büyük bir yük getirmemesi önemlidir [32].

Güven modellerini girdi olarak kullanabilecek birçok veri vardır. Örneğin bir düğümün uzun süre hayatta olmaması veya bir düğümün rastgele görünmesi ve kaybolması güvenli olamayabilir. İletişim katmanında eksik bilgi veren bir düğüm güvenilir olmayacaktır. Örnek olarak bir yangın alarm algılayıcısının düşük güven değerinde aktif duruma geçmesi verilebilir [32].

2.1 Tanımlar: Güven, Dürüstlük, Risk ve İtibar

Josang vd. [33], güven ve dürüstlüğü tanımlarken Gambetta'nın tanımlamalarını temel alırlar [34]. Solhaug vd. güvenilirliği güvenilen belirli bir eylemi güvenilen kişinin çıkarlarına bağlı objektif bir olasılık olarak tanımlarlar [35]. Güven ise 0 (tam güvensizlik) ve 1 (tam güven) arasında değişen subjektif bir olasılıktır [33].

Güven ve güvenilirlik arasındaki temel fark ise şudur. Güven düşünülen olasılık değeri, güvenirlik ise gerçek olasılık değeridir. Bu fark ortaya risk faktörünü çıkarır [36]. Güvenin yanlış konumlandırılması risk faktörünü artırır.

Güvenle ilişkili olduğundan dolayı itibar da önemli bir kavramdır. Bazen itibar ve güven aynı bağlamda kullanılabiliyor olsa da ikisi farklı anlamlara sahiptir. İtibar bir birimin diğer bir birimin hakkındaki görüşünü temsil eder. Ancak güven ise bir birimin itibarının türevidir.

2.1.1 Bilgi Güveni

Güven kavramının sosyal güven, zihinsel güven ve haberleşme güveni gibi birçok farklı türü vardır [29]. Bu çalışmada veri elemanları ve algılama düğümleri arasındaki bilgi güveni değerlendirilmiştir. Bilgi güveni veya veri güveni nesneler veya işlemler ile üretilen verilerin güven bölgesini ifade eder. Bir ağdaki bilgi güveni, ağda biriken hatalı verileri önleyebildiği için önemlidir. Bir ağdaki bir düğüm veri oluşturabilir, veriyi bir füzyon gibi işleyebilir ve veriyi aktarabilir.

2.1.2 Güvenin Özellikleri

Cho vd. yaptıkları survey çalışmasında güveninin özelliklerini şu şekilde sıralamışlardır [36].

- **Dinamiklik:** Düğümlerdeki hata ve hareketlilik dolayısıyla algılama ağları yüksek bir dinamikliğe sahiptir, bu nedenle güven de dinamik olmalıdır.
- **Öznellik:** Ağ dinamik olduğu için düğümler aynı düğümdeki güven seviyelerini farklı düzey seviyesine yerleştirmeye karar verebilirler [37].
- **Geçişlik:** Güvenin kesin olarak geçişli olduğu söylenemez. Geçişlik için iki tip güvene ihtiyaç duyarız. Birincisi Trustee içerisinde güven, ikincisi Trustee'nin önerilerindeki güven.
- **Asimetri:** Bir düğüm diğer bir düğüme güvenebilir ama trustee trustor'a güvenmeyebilir.
- **İçerik-bağımlılık:** Güven, içerik-bağımlıdır [38]. Örneğin bir düğüm diğer bir düğümden gelen görüntü verilerine güvenebilir ama bir düğüm aynı düğümden gelen ses verilerine güvenmiyor olabilir.

2.2 Farklı Alanlarda Güven ve İtibar

Momani ve Challa'nın çalışmasında güvenin sosyal bilimler, e-ticaret, dağıtık sistemler ve ad-hoc ağlarındaki tanımları verilmiştir [28].

2.2.1 Sosyal Bilimler ve E-Ticarette Güven

Güven insan yaşamının bir parçası olduğundan, sosyal bilimlerle ilişkisi oldukça fazladır [39]. Güven arkadaşlık etme, sırlarını paylaşma, satış ve satın alma işlemlerinde ve birlikte çalışma gibi insan ilişkilerinde büyük bir etkiye sahiptir. Güven karar alma işlemlerinde, delegasyon, belgelendirme ve kaynak erişimindeki yardımlarıyla günlük yaşantımızı kolaylaştırır [40].

Güven araştırmalarındaki motivasyon alanlarından biri de e ticarettir. İnternette alıcılar ve satıcılar arasında bir güven ilişkisi vardır. Alıcılar güvendikleri satıcılardan ürün alırlar. Güven, satıcılarının itibarı üzerine kuruludur. Satıcı geçmişte yaptığı

davranışlarıyla itibar kazanır. Bay [41], Yahoo[41] ve Keynote [42], [43]gibi bazı e ticaret sistemleri, itibar ve güven değerlerini sürdürmek için bir merkezi güven yetkisi sağlarlar.

Abdul-Rahman ve Hailes güvenin özelliklerine dayalı sosyolojik bir güven modeli tasarlamışlardır [44]. Modellerinde, kuruluşlara kendi itibarlarına ve doğrudan deneyimlerine bağlı olarak bir güven değeri verilir.

Josang ve Ismail elektronik marketler için bir itibar sistemi geliştirmiştir [45]. Çoğu itibar sistemi sezgisel ve geçicidir fakat onlar itibar sistemlerini istatistikteki beta yoğunluk fonksiyonu üzerine inşa etmişlerdir. Bu beta dağılımı durumların gerçekliği noktasında bir fikir sunar.

2.2.2 Dağıtık ve Peer to Peer Sistemlerde Güven

Dağıtık sistemlerde, varlıkların güveni değerlendirmek için merkezi bir sistemleri yoktur. Bu nedenle varlıklar kendi eşleriyle ile bilgi alışverişinde bulunarak kendi güven görüşlerini oluştururlar. Genellikle oyun teorisi [46] ve Bayes ağ [47] metotları, dağıtık sistemlerin güvenini hesaplamak için kullanılır.

Aberer ve Despotovis, P2P sistemleri için bir itibar yönetimi sistemi öneren ilk araştırmacılardır [48]. Bu sistemde, bir merkezi yetkiden bilgi gerektirmeyen algoritmalar ve veri yapıları kullanılmıştır. Güven modelleri, düğümler arasındaki geçmiş etkileşimlere dayanmaktadır. Tasarladıkları sistemlerinin dezavantajı ise sadece olumsuz geri bildirimlerin kabul edilmesi ve sistemin sadece peer aksaklıklara duyarlı olmasıdır.

Peer-to-peer sistemleri için başka güven modelleri de vardır. Bu çalışmada algılama ağlarındaki güven modelleriyle ilgilenildiğinden ayrıntıya girilmemiştir. Momani ve Challa [28] tarafından incelenen diğer güven mekanizmaları Bayesian Network Model [47], SECURE [49], UniTec [50], BambooTrust [51], B-trust model [52] modelleridir.

2.2.3 Ad-Hoc Ağlarda Güven

Geçici ağlarda düğümler çok sık yer değiştiren ağlara katılırlar. Ağın işlevselliğini destekleyen hiçbir düğüm yoktur. Düğümler arasındaki ilişki, ağda sürekli meydana gelen değişim gibi dinamiktir [53].

Geçici ağlarda güven mekanizmaların çoğunluğu oyun teorisi ve Bayes ağ yaklaşımlarını kullanır. CONFIDANT [54] ve CORE [55] bu sistemlere örnek verilebilir.

2.3 Kablosuz Algılama Ağlarında Güven

Kablosuz algılama ağlarında güvenle ilgili daha önce yapılan çeşitli çalışmalar vardır [30], [56]. Kablosuz algılama ağları gizlice dinlenme, uydurma, sızma, paketlerin değiştirilmesi gibi farklı saldırı senaryolarıyla karşılaşabilirler [28]. Bu tarz saldırılar gizlilik, hesap verebilirlik, veri bütünlüğü, veri kimlik doğrulaması ve veri tazeliği gibi konuları gündeme getirmektedir. Momani ve Challa tarafından kablosuz algılama ağların güvenliğiyle alakalı bazı çalışmalar yapılmıştır [53], [57], [58], [59], [60], [61] ,[62]. Kriptografik mekanizmalar bu sorunları tamamen çözememiştir. Kötü niyetli düğümler tarafından meydana gelebilecek sistem hataları, hatalı veri ve kötü yönlendirme ağın arızalanmasına sebep olabilir. Kriptografik yaklaşımlar istatistik, e-ticaret, sosyal bilimler gibi alanlarda araçları ile birlikte entegre edilmelidir. Bazı düğümler kötü niyetli davranabilir. Bu yüzden güven mimarilerinin, kötü düğümleri keşfetmesi ve bu düğümleri saf dışı bırakması gerekir. Bu bağlamda araştırmacılar tarafından benimsenen farklı yaklaşımlar mevcuttur [53]. Bunlar:

- Bir alt ağdaki tüm düğümler için bir güven ve itibar tablosu sağlamak
- Düğümlerin davranışlarını izlemek için bir izleme mekanizması kullanmak
- Hatalı düğümleri keşfedip onları ağdan uzaklaştırmak
- Protokol kurallarına uyacak olan düğümleri ödüllendirmek
- Verilerin bütünlüğünü korumak için düşük maliyetli kriptografi kullanmak

Güven konusu uzun bir süre için araştırılmıştır [63]. Bu konu sosyal bilimler [64], ekonomi [65] gibi birçok disiplinler tarafından incelenmiştir. Ancak güvenin resmi bir tanımının olduğunu söyleyemeyiz. Düğümler arasında güven kurulması kablosuz

algılama ağlarında etkili bir güvenlik yaklaşımıdır. Düğümlerin iş birliği içerisinde çalışmasıyla, düğümler arasındaki güven ilişkisi kablosuz algılama ağlarının güvenliğini artırır.

Güven ve güvenlik birbirleriyle ilişikli kavramlardır ve bazen birbirlerinin yerine kullanılabilir [66]. Ancak güvenlik güvenden farklıdır. Güvenlik, güvenden daha kapsamlı bir kavramdır ve güvenlikteki yük, güvenden daha fazladır.

2.3.1 Kablosuz Algılama Ağları İçin Geliştirilen En İyi Güven Uygulamaları

Lopez vd. kendi [67] ve diğer çalışmalara dayanarak kablosuz algılama ağlarındaki güven yönetiminin en iyi uygulamalarını tanımlamışlardır [32], [68], [69].

İlk olarak Ganeriwal ve Srivastava algılayıcı ağlar için RFSN (Reputation-based Framework for High Integrity Sensor Networks) güven modelini geliştirmişlerdir [30]. Güven ve itibar değerlerini güncellemek ve belirlemek için istatistiki bir yöntem olan beta dağılımını kullanmışlardır. Güven kavramlarını ise iş birliği olan ve iş birliği olmayan eylemler olarak iki temel sınıfa ayırmışlardır. Düğümler güvenirliği hesaplamada ikinci el bilgileri dolaylı olarak kullanmışlardır. Güvenilir düğümden elden edilen ikinci el bilgilere daha fazla ağırlık verilir. Beklenen itibar değeri düğümlerin güven değerini temsil eder. Eğer güven değeri eşik değerin altından çıkarsa bu düğüm iş birliği yapmayan düğüm olarak belirlenir. Yazarlar çalışmalarında sadece pozitif bildirim aldıkları düğümleri kullanarak gelebilecek saldırıları bertaraf etmeye çalışmışlardır.

Bir algılayıcının yerini belirlemek hayati bir önem taşıdığından bu görevi yapacak DRBTS (Distributed Reputation-based Beacon Trust System) adında bir sistem modellenmiştir [70]. Bu sistem yer bilgisini eksik bildiren düğümler için işaret düğümü kullanır. Her işaret düğümü beklenmeyen bir durum sergileyen düğümler için 1-hop komşu izleme ekranı dağıtılmış ve komşu itibar tablosunda eksik raporlama yapan düğümlerin itibar değerleri tutulup ve güncellenmiştir. Algılayıcı düğümler bilgi aldığı bir düğümün güvenirliğini tartmak için komşu itibar tablosunu kullanır.

Bundan önce yapılan başka bir çalışmada ise hem verilerin hem de veri benzerliği, yol benzerliği, veri çatışması ve veri kesilmesi gibi değişik faktörlere dayalı veri

kaynaklarının güven düzeyini tahmin etme fikrine dayalı bir anlayış benimsenmiştir [71]. Dai dört faktöre dayalı güven puanları hesaplamıştır [71] :

- **Yol benzerliği**
- **Veri benzerliği**
- **Veri çatışması**
- **Veri kesintisi**

Veri benzerliği için iki sayısal değer arasındaki mesafeyi hesaplanmıştır. Bunlar iki kategorik değer arasındaki mesafe ve iki dize(string) arasındaki mesafe değerleridir. Fakat bu teknik, rapor edilen duruma farklı ve birden fazla düğüm tarafından rapor edilmesi durumunda yüksek güvenilirlik atfeder ve gizli saldırıyı fark edemez.

Lim vd. akış verilerinin güven puanlarını provenansa dayalı olarak değerlendirmişlerdir [72], [73]**.** Akış ortamlarının güven hesaplanmasında provenanstan faydalanmaları bizim yaklaşımımızla paralellik göstermektedir. Lim vd. güven değerlerini hesaplamak için fiziksel provenansı kullanmışlardır. Provenans verilerini bir veri tabanında saklamış ve merkezi bir şekilde güven değerlendirmesi yapmışlardır. Buna karşın bizim önerdiğimiz modelde ise güven hesaplamaları dağıtık bir şekilde yapılacaktır.

IBM T.J. Watson merkezinde çevrimiçi sağlık analizi için biyomedikal veri akışı sistemine dayalı bir çalışma mevcuttur. Century adı verilen sistemlerinde bir olaya veri ve işlem noktasında destek sağlamak için tanımlanan ve provenans bilgileri depolayan tıbbi algılayıcılar mevcuttur [74], [75]**.**

Öte yandan TIBFIT tarafından güven endeks tabanlı, hataya dayanıklı bir sistem inşa edilmiştir. Güven endeks değerinin, önceki olay raporlarının aslına uygunluğunu nicel bir ölçü olarak tutmuşlardır [76]. Onların bu yaklaşımı, düğümlerin geçmiş doğruluğunu tutmak anlamında bizim mimarimizle benzerlik göstermektedir. Ancak bizim çalışmamızda, güvenin sadece bir hata oranından ibaret olmadığı fikri üzerine durulmuştur. Ve bizim hata oranımız, itibar ve kaynak vektörlerinde saklanan birçok değer kullanılarak hesaplanan geniş bir metriktir.

Bayes ağı [47], [77]ve oyun teorisi [46] teknikleri de, ağlarda güven oluşturmak için kullanılabilir Bizim sistemimizde ise güven değerlendirmesi için provenanstan destek

alan, dizin tabanlı güven modeli kullanılmıştır. Bu bağlamda bizim modelimizin yukarıdaki modellerden farklıdır.

Algılayıcı ağların en önemli güvenlik açığı, küme başlarının kötü olma ihtimalidir. Garth vd. [78] güvenilir küme başlarının seçimi için dağıtık güven tabanlı bir araç önermişlerdir. Bu yaklaşımda, güvenilir düğümlerden gelen doğrudan ve dolaylı bilgileri kullanmışlardır. Güven, paket düşürme oranı, veri paketleri ve kontrol paketlerinin ağırlıklı hesaplanmasına göre ölçülür. Bununla beraber her bir düğüm, kendi etrafındaki düğümlerin güven tablosunu tutup bunu istek üzerine küme başına raporlar.

Hur vd. algılayıcı verilerinin güvenilirliğini ölçmek ve kötü düğümlerden gelen bilgiyi silmek için bir güven modeli önermişlerdir [79]. Geliştirilen bu model bizim çalışmamızla benzerlik göstermektedir**.** Fakat onların önerdikleri model geçmiş verileri kullanmaz. Her bir düğüm komşusunun güvenirliğini, komşusunun gereksiz bilgi verilerini kendi sonuçlarıyla karşılaştırarak değerlendirir. Kötü düğümlerden gelen bilgi göz ardı edilerek daha kesin sonuçlar elde edilir.

Chen vd. [80] olasılık, istatistik ve matematik analizden araçlar kullanan itibar tabanlı bir güven modeli önerirler. Kablosuz algılayıcı ağlarında bir güven alanı ve itibar alanı oluştururlar ve itibar alanından güven alanına bir dönüşüm tanımlarlar. Son olarak kablosuz algılayıcı ağlarındaki önemli özellikleri ele alırlar ve kablosuz algılayıcı ağlarındaki itibar sistemleriyle alakalı açık problemlere dikkat çekerler.

Xiao vd. SensorRank adı verilen sistemlerinde Trust Voting algoritmasını kullanırlar. Algılayıcı düğümler, okudukları verilerin doğru olup olmadığını doğrulamak için komşularına danışırlar [81]**.** Hatalı düğümler Voting algoritmasına dâhil olmazlar.

Tanachaiwiwat vd. algılayıcı ağları için bir güven yönlendirme modeli(TRANS) geliştirmişlerdir [82]. Modellerinde, düğümler komşularına inceleme mesajları gönderir ve ACK mesajları beklerler. Mesajı istenmeyen yere yönlendiren veya mesajın ulaşmasını engelleyen düğümler baş düğüm tarafından kara listeye alınırlar. Mesaj akışı baş düğüm aracılığıyla yapılır.

Beta itibar sistemini kullanan modellerden birisi de Srinivasan vd. [83] tasarladığı CDS tabanlı itibar izleme sistemidir. Düğümler diğer düğümlerden direk olarak bilgi elde eder ve beta dağıtım parametrelerinin değişken gruplarını depolar.

Momani vd.[84] kablosuz algılayıcı ağları için Gauss itibar sistemini geliştirmişlerdir. Her düğümün rapor edilen verisi komşu düğümler tarafından değerlendirilir. Momani vd. direk olarak gözlenen bilgiyle, komşu düğümlerden elde edilen bilgileri füzyon etmek için Bayes' in olasılıksal yaklaşımını kullanmışlardır.

GTMS[85], Shaikh vd. tarafından geliştirilen grup tabanlı güven yönetim modelidir. Shaikh vd. bu çalışmada merkezi ve dağıtık yaklaşımları bir araya getirmişlerdir. Bu çalışmanın bizim yaklaşımımızla birçok benzerlik gösterdiği gözlemlenmiştir. Fakat bu model kötü düğümler tarafından bildirilen hatalı bilgiyi dikkate almaz. Her grubun, baz istasyonundaki küçük bir veri tabanında tutulan bir güven değeri vardır.

ATRM'de [86] düğümler güven ve itibar bilgilerini yerel olarak depolarlar[69].Ağ modeli kümelenmiş kablosuz algılama ağına dayanmaktadır.

Güven ihmal düğümleri, kümeleri birleştirme ve düğümleri ekleme gibi kablosuz algılama ağlarının yeniden inşa edilmesinde kullanılır. Kablosuz algılama ağları, düğümlerin güveni ve iş birliği yapısı özelliğini temel aldığı için güvenin kurulması bir zorunluluktur. Kablosuz algılama ağlarının sınırlı kaynaklara sahip olması nedeniyle, bu ağlarda geleneksel kriptografik yaklaşımlar kullanmak mümkün değildir [87]. Bu yüzden kablosuz algılama ağları için farklı güven mekanizmaları gereklidir. Kablosuz algılama ağlarında güven hala açık ve zorlu bir alandır.

Kablosuz algılama ağlarında geliştirilen diğer güven uygulamaları için bu çalışmalara da bakılabilir [88], [89], [90], [91], [92], [93].

2.3.2 Güven ve İtibar

Kablosuz algılama ağlarında güven ve itibar aynı kavramlar olarak düşünülmemelidir. İtibar zamanla oluşan bir kavramdır. Doğru bir karar vermek için güven, itibara dayalı olarak hesaplanmalıdır. İtibar olmadan güven, anlık davranışlara dayalı bir değere sahip olacaktır. Örneğin belli bir zaman aralığında kötü amaçlı davranmış bir düğüm, o anda iyi davranabilir ve bu da bizim aldanmamıza neden olabilir. Ancak kötü davranış geçmişini tutan bir itibar değeri olduğu zaman son eylemden aldanılma gibi bir durum meydana gelemeyecektir.

2.3.3 İlk Elden Bilgi Toplama

Bir algılama ağında güveni hesaplamak için kullanılan donanım hataları, enerji sorunları, düğüm yer değişimleri ve algılama okuma sapmaları gibi birçok etmen mevcuttur. Bunlar ilk elden bilgi olarak kabul edilir ve bu etmenler ihtiyaç duyulduğu zaman dikkate alınır. Bir güven yönetim sistemi, bilginin birçok kaynaktan sağlanması sayesinde daha güçlü olacaktır.

2.3.4 İkinci Elden Bilgi Toplama

Algılama ağları, iş birliği içerisinde çalıştığı düğümlerden meydana gelmektedir. İkinci el bilgi, güven yönetimi için düşünülmelidir. Bir düğüm yerel zekâya sahip olabilir. Bu düğümlerin kendisi, bir dereceye kadar anormal faaliyetleri tespit edebilir ve bunu komşu düğümlerine rapor edebilir. Aynı zamanda bir düğüm bir komşusunun kötü davranışını, bir diğer komşusuna rapor edebilir. Ancak ikinci elden bilgi alındığı zaman mouthing saldırılarına uğrama ihtimali göz ardı edilmemelidir. Kablosuz algılama ağlarında kötü mouthing saldırıları olduğu zaman, bir düğüm iyi bir düğüm hakkında kötü rapor verebilir veya bir düğüm kötü bir düğüm hakkında iyi rapor verebilir. Bu da güven hesaplama noktasında yanılmamıza sebep olacaktır.

2.3.5 İlk Değerler

Ağdaki düğümlere dağıtım sırasında ilk güven değerleri verilmelidir. İlgili çalışmada, bir ağ yöneticisinin düğümleri yapılandırdığı, test ettiği varsayılmıştır. Bununla birlikte başlangıçta her düğüme eşit güven değeri verilmiştir. Ancak sistem, ağa eklenen düğümlerin dağıtımı sonrasında şüpheli olmalıdır. Burada bir düğüm yeni bir kimlik oluşturarak kötü itibara sahip olabilir ve white-washer saldırasının bir parçası olabilir.

2.3.6 Tanesellik

Bir kablosuz algılama ağındaki düğümlerin algılama, yönlendirme gibi farklı eylemleri olabilir. Farklı güven değerleri için, bir algılama düğümüne farklı görevler verilmelidir.

2.3.7 Güven Değeri Güncellemesi

Güven yapılandırılması uzun zaman almaktadır. Bir düğümün güven değeri güncellendiği zaman, geçmiş güven değerleri üzerine yazılmamalıdır. Ağın önceki güven değeri unutulmamalıdır ve kaydı tutulmalıdır. Eğer geçmişteki kötü davranışlar unutulursa, ağ on-off saldırılarına karşı savunmasız olacaktır [94].

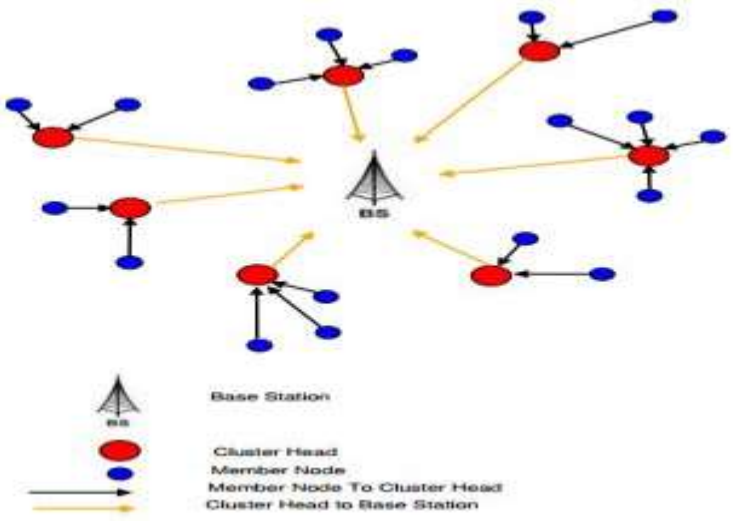
BÖLÜM 3

AĞ MODELİ ve MİMARİ YAPI

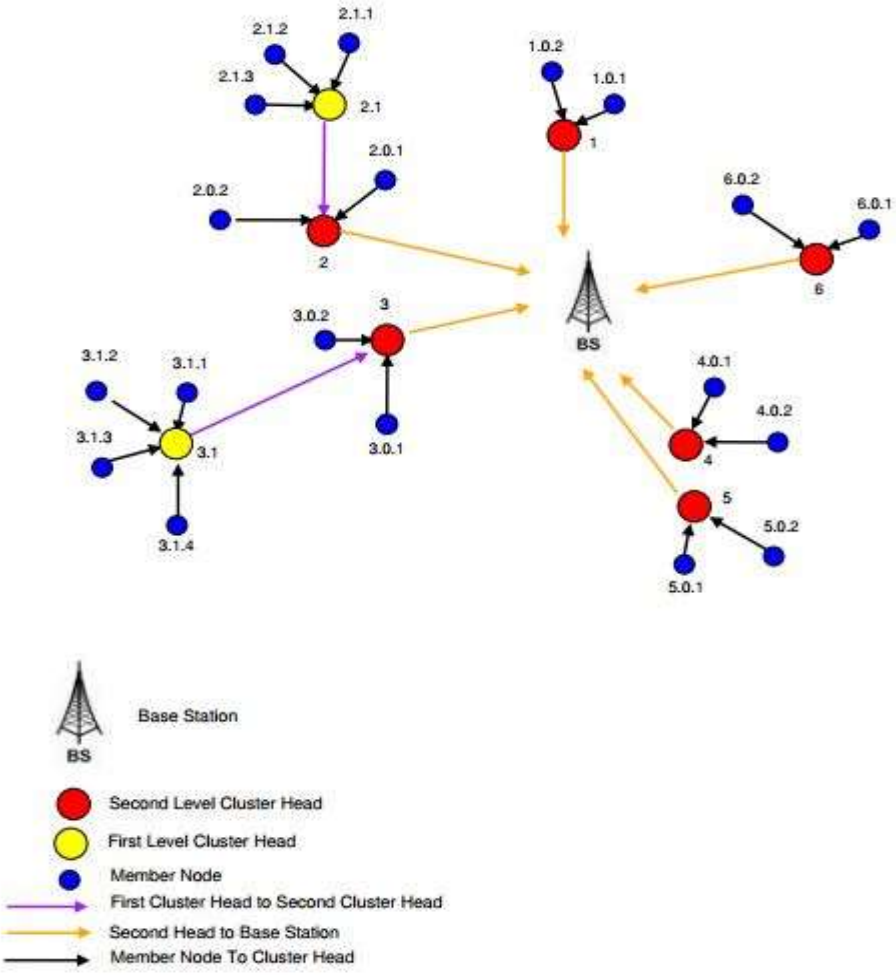
3.1 Ağ Mimarisi

Bu bölümde Şekil 3.1'de de gösterilen yeni mimari anlatılacaktır. Yeni mimarinin ProTru'dan [29] temel farkı, farklı bir yönlendirme mekanizmasının kullanılması ve güven değerinin hesaplanılmasında Kalman Filtreleme yönteminin tercih edilmesidir.

ProTru mimarisinin birden çok atlamalı bir şekilde güncellenmesinin ana nedeni algılayıcıların bir veriyi gönderebilecekleri mesafenin kısıtlı olması ve algılayıcının veriyi göndereceği mesafeyle harcadığı enerji arasında üssel olarak bir ilişkinin bulunmasıdır. ProTru mimarisinin birden çok atlamalı şekilde güncellenmesiyle tasarlanan MultiProTru sayesinde bu iki problem optimize edilmiştir.



Şekil 3. 1 ProTru mimarisi



Şekil 3. 2 MultiProTru mimari

3.1.1 Yaprak Düğümler (Member Nodes)

Yaprak düğümler, tekil (unique) bir anahtarla tanımlanmış olan kaynak düğümleridir. Yaprak düğümler, önce bilgiyi toplar; daha sonra bu bilgiyi yayarlar ama diğer düğümlerden bilgi alamazlar. Yaprak düğümler belli bir alana rastgele dağıtıldıktan sonra kümeleme algoritmasını kullanarak bir baş düğüm seçerler ve elde ettikleri verileri bu baş düğüm vasıtasıyla merkez düğüme iletirler.

3.1.2 Birinci Seviye Baş Düğümler (First Level Cluster Head)

Birinci seviye baş düğümler, mimaride kullanılan yeni kavramlardan bir tanesidir. ProTru mimarisinde sadece baş düğümler vardır ve tüm baş düğümler aynı seviyeye sahiptir. Yeni mimaride ise baş düğümler, merkez düğüme olan mesafelerine göre

derecelendirilir. Merkez düğüme uzak olan baş düğümler birinci seviye baş düğümler, yakın olanları ise ikinci seviye baş düğümler olarak adlandırılır. Bu derecelendirmenin yapılmasındaki ana hedef, merkez düğüme uzak olan baş düğümlerin, merkez düğüme daha yakın olan bir diğer baş düğümü kullanarak, enerji verimliliğini ve veri iletiminde kullandığı yolun güven değerini artırmasıdır. Bu düğümler, diğer bir ikinci seviye baş düğüm yardımıyla veri iletimi yapıp yapmayacaklarına, ikinci seviyedeki düğümün güven değerine bakarak karar verirler. Eğer ikinci seviyedeki düğümün güven değeri kendi güven değerinden büyükse, ikinci seviyedeki baş düğüm aracılığıyla veri iletimini gerçekleştirirler. Bu sayede veri iletiminde kullanılan yolun güven değeri artmış olur. Aynı zamanda bu düğümler, aşağıda anlattığımız ikinci seviye baş düğümlerin sahip olduğu güçlü hesaplama yeteneği ve diğer düğümlerden aldıkları bilgileri birleştirme özellikleriyle de paralellik göstermektedirler. Bu düğümleri, ikinci seviye baş düğümlerden ayıran temel özellik ise merkez düğüme uzak olmaları ve veri iletiminde merkez düğümle doğrudan iletişime geçememeleridir.

3.1.3 İkinci Seviye Baş Düğümler (Second Level Cluster Head)

İkinci seviye baş düğümler, hesaplama yeteneği noktasında güçlüdürler. Bir grup düğümden bilgi alırlar ve aldıkları bilgileri birleştirme ve ileri grup için bilgi aktarım gibi çeşitli hesaplamalar yaparlar. İkinci seviye baş düğümler, tekil bir kimlik ile tanımlanırlar ve yaprakların grup liderleri olurlar. Birinci seviye baş düğümlerden temel farkları ise merkez düğüme yakın olmaları ve veri iletimini kendi başlarına yapmalarıdır. Özetle yaprak düğümlerden topladıkları bilgileri, birleştirerek merkez düğüme doğrudan iletirler.

3.1.4 Merkez Düğüm (Base Station)

Yaprak düğümlerden gönderilen verileri, baş düğümler vasıtasıyla alan merkezi düğümler(base station), mimarinin en yüksek hiyerarşisini temsil eder ve final değerini hesaplarlar. Baş düğümler birleştirilen verileri, gelen güven değerlerini ve merkez düğüme nakil olan düğüm sayılarını hesaplayıp gönderecektir. Geliştirilen mimari dağıtık doğası nedeniyle, merkezi düğüme gelen güven ve verilerin ağırlıklı ortalamasını

hesaplayarak nihai sonuca ulaşır. Ayrıca gelen sonucu ve merkezi provenans veri akış grafiğini saklar.

3.2 Kümeleme Algoritması

Kablosuz iletişimde kullanılan algılayıcı düğümleri, alıcı-verici ve bekleme durumunda eşit enerji tüketirler [95].Bu nedenle veri yönlendirme ve veri iletimi için bölgesel ağlar kurmak adına bazı baş düğümlerin seçilmesi gerekir. İletişim modülünde, enerji tüketiminde tasarruf sağlamak için baş olmayan düğümlerin kapatılması kümeleme algoritmalarının ilk fikridir. Küme başlarının, küme içindeki düğümlerin çalışmalarını koordine etmesi ve veri toplanmasını ve iletimini gerçekleştirmesi gerekir. Bu nedenle küme başlarının enerjisi hızlı tükenir ve kümeleme algoritmasının, enerji tüketimini dengelemek ve yaşam döngüsünü uzatmak için ağ düğümlerinden periyodik olarak bir küme başı seçmesi gerekir. Kümeleme topolojisi, büyük ölçekli ağların dağıtımını yapmak için kullanılan dağıtık algoritmaların uygulanmasına katkıda bulunur. Bu bağlamda geliştirilen mimariye en uygun olabilecek kümeleme algoritmasının Geographic Adaptive Fidelity (GAF) olacağına karar verilmiştir.

3.2.1 Geographic Adaptive Fidelity (GAF)

GAF, konum tabanlı düğüm kümeleme algoritmasının bir türü [96] veya konum tabanlı bir enerji tasarruf protokolü olarak da tanımlanabilir [97]. Bu protokolde izlenen alan, sanal hücrelere bölünür ve her düğüm, periyodik olarak bulunduğu hücrenin konum bilgisi doğrultusunda bir küme başı düğümü seçer. Diğer düğümler, enerji tüketimini azaltmak için uyku durumuna geçebilirken; küme baş düğümleri her zaman aktif kalır. GAF, ilk olarak Ad-Hoc ağları için bir yönlendirme algoritması olarak önerilmiştir. Daha sonra hücrelerin sanal olarak bölünme yöntemiyle birlikte bu protokol kablosuz algılama ağları için de kullanılmaya başlanmıştır.

GAF'ın implementasyon süreci temel olarak iki aşamadan oluşmaktadır. Bunların ilki, izleme alanının sanal hücrelere bölünme evresidir. Bu aşamada, düğümün konumu ve iletişim mesafesine göre, tüm ağ sanal hücrelere bölünür. Bu bölünme işlemi sona erdikten sonra sanal hücrelerin küme baş düğümleri seçilir ve düğümler periyodik olarak keşif, uyku ve çalışma durumuna geçerler. Ağ başlatılırken, tüm düğümler keşif

durumundadır ve bir mesaj aracılığıyla konum ve kimlik bilgilerini bildirirler. Bu işlem sayesinde, tüm düğümler kendileri ile aynı hücrede bulunan diğer düğümlerin bilgisine sahip olurlar. Daha sonra, her düğüme T1 değerine sahip rastgele olarak ayarlanmış bir zamanlayıcı atanır. Herhangi bir zamanlayıcının ilk molasını vermesi, o zamanlayıcıya sahip olan düğümün, kendini küme baş düğüm ilan etme durumunda olduğunu gösterir. Eğer bu düğüm, T1 zamanlayıcısından önce aynı hücrede küme başı olan bir diğer düğümden bilgi alırsa; bu düğüm küme başı rekabetini kaybeder ve uyku durumuna geçer. Küme başı düğümü belli olduktan sonra küme başı olan düğüme T2 zamanlayıcısı set edilir. Zamanlayıcı mola vermeden önce; düzenli yayın paketleri, kendini küme başı olarak ilan eden düğüme gönderilir ve diğer düğümlerin küme başı düğüm olması engellenir. T2 sona erdiği zamanda küme baş düğüm durumunu tekrardan belirlemek üzere eski haline geri döner ve tekrardan küme başı olmak için rekabet eder. Uyku durumundaki bir düğüme T3 zamanlayıcısı atanır ve T3 zamanı dolduğundan uyku durumundaki düğüm durumunu tekrardan gözden geçirmek üzere eski durumuna geri döner.

GAF protokolünün temel fikri, enerji tüketimini azaltmak için mümkün olduğunca düğümleri uyku durumunda tutmaktır. Algılayıcı düğümlerinin kaynakları sınırlıdır ve coğrafi konumu dayalı bu alt küme algoritmasında algılayıcı düğümleri için düğümde kalan enerji sorunlarını göz ardı etmek zor bir durumdur. Bu yüzden enerjinin erken tükenmesi, düğümün yok olmasına yol açar ve ağ topolojisi kararsız kalır.

BÖLÜM 4

GÜVEN MODELİ

4.1 Yönlendirme Algoritması

Daha önce geliştirilen ProTru mimarisinde, düğümler belli bir alana dağıtıldıktan sonra her düğüm, bir baş düğüm seçmektedir. Daha sonra bu düğümler elde ettikleri verileri, baş düğüm üzerinden merkez düğüme göndermektedir. Özetle, iletişim mekanizması Şekil 3.1'de gösterilen Yaprak Düğüm (Member Node) →Baş Düğüm (Cluster Head)→Merkez Düğüm (Base Station)şeklinde organize olmaktaydı.

Geliştirilen yeni birden çok atlamalı mimarinin, bir önceki mimariden temel farkı şudur; ProTru mimarisinde her baş düğüm, yaprak düğümlerden elde ettiği bilgiyi merkez düğüme kendisi iletmektedir. Yani baş düğümler arasında bir ilişki söz konusu değildir. Bu yaklaşımın temel dezavantajı ise merkez düğüme çok uzak olan bir baş düğümün, topladığı bilgiyi merkez düğüme gönderdikten sonra enerji verimliliğinin düşmesidir. Bu çalışmadaki temel motivasyon ise merkez düğüme uzak olan baş düğümün, baz istasyonuna daha yakın olan bir baş düğümü kullanarak veri iletimini gerçekleştirmesidir. Geliştirilen yeni birden çok atlamalı mimaride, veri iletiminde iki yol seçeneği mevcuttur:

- Yaprak Düğüm →Baş Düğüm →Merkez Düğüm
- Yaprak Düğüm →Birinci Seviye Baş Düğüm →İkinci Seviye Baş Düğüm→Merkez Düğüm

Baş düğümün, merkez düğüme yakın olması durumunda Yaprak Düğüm →Baş Düğüm →Merkez Düğüm yolunu tercih etmektedir. Birden çok atlamalı mimaride ise baş düğümün merkez düğüme uzak bir mesafede olması durumunda Yaprak Düğüm →Birinci Seviye Baş Düğüm →İkinci Seviye Baş Düğüm→Merkez Düğüm yolunu kullanıp kullanmayacağına Birinci Seviye Baş Düğüm'ün ve İkinci Seviye Baş Düğüm 'ün güven değerlerine bakılarak karar verilir. Özetle, bir baş düğüm veri iletimi sırasında diğer bir baş düğümü kullanıp kullanmayacağına güven değerlerini esas alarak karar vermektedir. Bu bağlamda birden çok atlamalı modelin akış diyagramı Şekil 4.1'de gösterilmiş ve karar verme mekanizması aşağıda iki maddeyle açıklanmıştır.

- Birinci seviye baş düğümünün güven değeri, ikinci seviye baş düğümün güven değerinden daha düşük bir değere sahip olması durumunda, veriyi gönderen birinci seviye baş düğümümün Yaprak Düğüm →Birinci Seviye Baş Düğüm →İkinci Seviye Baş Düğüm→Merkez Düğüm yolunu kullanmasına izin verilir. Bu seçeneği kullanması durumunda hem tercih ettiği yolun ortalama güven değeri, hem de veriyi gönderen birinci seviye baş düğümün enerji verimliliği artacaktır.
- Birinci seviye baş düğümünün güven değeri, ikinci seviye baş düğümün güven değerinden daha büyük bir değere sahip olması durumunda ise, birinci seviye baş düğüm, ikinci seviye baş düğüm olarak güncellenmekte ve merkez düğümle Yaprak Düğüm →Baş Düğüm →Merkez Düğüm yolunu kullanarak direk olarak iletişime geçmektedir. Birinci seviye baş düğümünün güven değerinin, ikinci seviye baş düğümün güven değerinden daha düşük bir değere sahip olmasına rağmen bu yolun seçilmesi durumunda veri iletiminde kullanılan yolun ortalama güven değeri azalacaktır.

Bu birden çok atlamalı modelde birinci seviye baş düğümünün güven değerinin, ikinci seviye baş düğümün güven değerinden daha düşük bir değere sahip olması durumunda enerji verimliliğinden ziyade veri iletim yolunun ortalama güven değerinin yüksek tutulması amaçlanmıştır. Bu sayede veri tutarlığının çok önemli olduğu kablosuz algılama ağları sistemlerinde veri iletiminde kullanılan yolun ortalama güven değeri artırılmıştır. Birinci seviye baş düğümünün güven değerinin, ikinci seviye baş düğümün

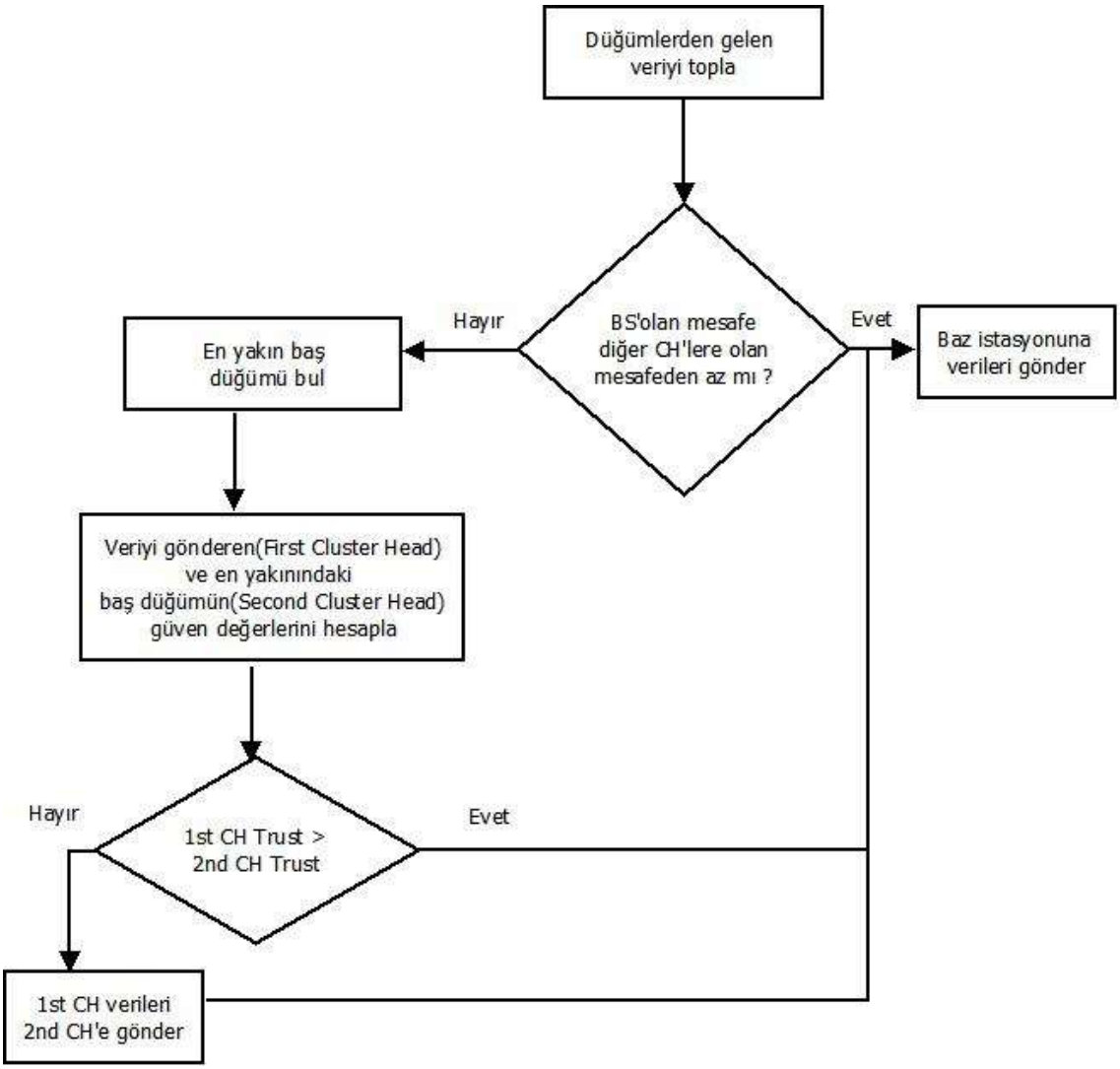
güven değerinden daha düşük bir değere sahip olması durumunda ise hem enerji hem de veri iletiminde kullanılan yolun ortalama güven değeri artırılır.

Şekil 3.2 incelendiği zaman 1, 2, 3, 4, 5, 6 nolu kırmızı düğümlerin ikinci seviye baş düğümler, 2.1 ve 3.1 nolu sarı düğümlerin birinci seviye baş düğümler ve diğer kalan 1.0.1, 1.0.2 gibi üç haneli mavi düğümlerin de yaprak düğümler olduğu görülecektir. 2.1 ve 3.1 nolu düğümlerin birinci seviye baş düğüm olarak tanımlanmalarının iki temel sebebi vardır. Bu iki şartı da aşağıda sıralandığı şekilde sağlamaları durumunda birinci seviye düğüm olarak tanımlanırlar. İlgili şartlar:

- Birinci seviye baş düğümlerin merkez düğüme olan mesafelerinin, diğer baş düğümlere olan mesafelerden daha fazla olması gerekmektedir.
- Bir diğer koşul ise birinci seviye baş düğüme en yakın olan ikinci seviye baş düğümün sahip olduğu güven değerinin, birinci seviye baş düğümün güven değerinden fazla olmasıdır.

Özetle, Şekil 3.2'deki 2 ve 3 numaralı ikinci seviye baş düğümlerin sahip olduğu güven değerlerinin, 2.1 ve 3.1 nolu birinci seviye baş düğümlerin güven değerlerinden büyük olması sebebiyle bu baş düğümler, birinci seviye baş düğüm olarak ilan edilmişlerdir.

Şekil 3.2'de görülen 5 numaralı ikinci seviye baş düğümün, baz istasyonuna uzak olduğu ve direk kendisinin baz istasyonuyla iletişime geçmesi yerine 4 numaralı ikinci seviye baş düğüm aracılığıyla veri iletimi gerçekleştirmesi gerekirken bu yolu tercih etmediği görülecektir. Bunun ana sebebi ise 4 numaralı ikinci seviye düğümün sahip olduğu güven değerinin 5 numaralı baş düğümün güven değerinden küçük olmasıdır. 5 numaralı baş düğümün bu yolu tercih etmesi durumunda tercih ettiği yolun güven değeri azalacaktır. Bu durum ise veri güvenliği tehlikeye sokacaktır.



Şekil 4. 1 Yönlendirme akış diyagramı

4.2 Kalman Filtrelemesi Yöntemiyle Güven Değerinin Hesaplanması

Kalman filtrelemesi, 1960 yılında Rudolf Kalman tarafından ortaya atılan bir teoridir. Özellikle meteoroloji olaylarının tahmininde kullanılan, istatistik tabanlı olan bu model, algılayıcı ve veri füzyonu gibi birçok alanda kullanılır. Kalman filtrelemesi, mevcut ve önceki verilere dayalı olarak sistemin durumu hakkında çeşitli tahminlerde bulunur. Bu bağlamda bu yöntemin öz yinelemeli (recursive) bir yapıya sahip olduğunu söylenebilir. Kalman, sistemin geçmişte ürettiği değerleri kullanarak sistemin gelecekte üretebileceği değeri tahmin edebilme yeteneğine sahiptir. Örneğin, A ve B yolları arasında seyahat eden bir gemi olduğunu ve bu geminin istikametini GPS yardımıyla bulduğunu varsayalım. Yolculuk esnasında GPS'in bozulması durumunda bu gemi

rotasını bulamayacaktır. İşte tam bu noktada Kalman filtrelemesi devreye girecek ve geminin geçmişte kullandığı rota bilgileriyle çeşitli hesaplamalar yaparak geminin rotasını bulmasına yardım edecektir. Geliştirilen sistemde de, baş düğümün hesapladığı ortalama değerden yaprak düğümün gönderdiği bilginin değeri çıkarılarak farka dayalı bir model tasarlanmış ve ardından bu fark değerlerin Kalman filtrelemesinden geçirilerek ideale daha yakın bir güven değeri hesaplanmıştır.

4.2.1 Kalman Filtresi Formülleri

Bu kısımda Kalman filtresinde kullanılan formüller açıklanacaktır [98]. Kalman filtrelemesi incelendiği zaman öncelikle şu iki formülün kullanıldığı görülecektir.

$$x_k = A.x_{k-1} + B.u_k + w_{k-1} \quad (4.1)$$

$$Z_k = H.x_k + v_k \quad (4.2)$$

- k: Zaman aralıklarını gösterir.
- x_k: Tahmin değeridir.
- x_{k-1} : Önceki tahmin değeridir.
- u_k: Kontrol değeridir.
- w_{k-1}: Önceki işlemin gürültüsüdür.
- z_k: Ölçülen değerdir
- v_k: Ölçüm gürültüsüdür.
- A: Durum geçiş matrisidir.
- B: Kontrol matrisidir.
- H: Gözlem matrisidir.

Tahmin aşamasında ise şu iki formül kullanılmaktadır.

$$\bar{x}_k = A.\bar{x}_{k-1} + B.u_{k-1} \quad (4.3)$$

$$\bar{P}_k = A.P_{k-1}A^T + Q \quad (4.4)$$

- $\bar{x}_k$: k anındaki tahmin değeridir.
- $\bar{x}_{k-1}$: Tahmin sonrası, ölçümden önceki değerdir.
- $\bar{P}_k$: Ölçüm öncesi kovaryansı gösterir.
- Q : Tahmini işlem hata kovaryansıdır

Ölçüm güncelleme evresinde şu formüller kullanılır.

$$x_k = \bar{x}_k + K_k(z_k - H.\bar{x}_k) \quad (4.5)$$

Burada ($z_k - H.\bar{x}_k$) ile tahmin ile gerçek karşılaştırılıp inovasyon değeri bulunur ve Kalman kazancı hesaplanır.

$$K_k = \bar{P}_k\ H^T(H\bar{P}_k\ H^T + R)^{-1} \quad (4.6)$$

Burada R ölçüm hata kovaryansıdır.

$$P_k\ = (I - K_k H)\bar{P}_k \quad (4.7)$$

ile de kovaryans güncellemesi yapılır.

4.2.2 Yaprak Düğümlerin Güven Değerinin Hesaplanması

Güven değeri hesaplanırken, başlangıçta her yaprak düğüme e güven değeri atanır ve her bir yaprak düğüm bağlı olduğu baş düğüme aynı anda veri gönderir. Bununla beraber, her yaprak düğüme atanan bir tekil anahtar mevcuttur. Daha sonra verilerin gönderildiği bu baş düğüm, (4.8) eşitliğini kullanarak ortalama bir değer elde eder ve her k anında elde ettiği ortalama değeri, her bir düğümün göndermiş olduğu veri değerinden çıkararak bu fark değerlerini Kalman filtresinden geçirilmek üzere her bir düğüme gönderir.

$$\bar{d} = \frac{\sum_{i=1}^{n} d_i t_i}{\sum_{i=1}^{n} t_i} \tag{4.8}$$

- $\bar{d}$ tüm düğümlerden toplanan ortalama veri değeri
- d_i tekil anahtar değeri i olan her bir yaprak düğümden toplanan veri değeri
- $t_i = e^{\lambda.KalmanFarki_i^{-1}}$ t_i her bir düğüme ait güven değeri

k anında her bir düğüme başlangıçta e güven değeri atandıktan sonra yaprak düğümlerin $k+1$ anındaki güven değerleri aşağıdaki gibi hesaplanır.

- k anında her bir yaprak düğüm (d_i , t_i) bilgilerini baş düğüme gönderir ve baş düğüm de gönderilen bu değerleri kullanarak $\bar{d}$ değerini hesaplar.
- Daha sonra k anında hesaplanan $\bar{d}$ değerinden her bir yaprak düğümün gönderdiği d_i değerinin mutlak değeri alınarak bir fark değeri hesaplanır.
- Bir sonraki adımda ise her bir yaprak düğüm bu fark değerlerini her k anı için Kalman filtrelemesinden geçirir ve tahmini bir fark değeri elde eder ve genelde bu değer ideale yakın bir değerdir.
- Kalman'ın hesapladığı bu tahmini fark değeri kullanılarak her bir düğümün $k+1$ anındaki güven değerini aşağıdaki formül kullanılarak hesaplanır. Burada kullanılan λ ise kullanıcı tarafından seçilir ve değeri [0-1] aralığındadır.

$$t_i = e^{\lambda.KalmanFarki_i^{-1}} \tag{4.9}$$

4.2.3 Baş Düğümlerin Güven Değerinin Hesaplanması

Baş düğümlerin güven değeri, kendisine bilgi gönderen tüm yaprak düğümlerin güven değerlerinin aritmetik ortalaması alınarak hesaplanmıştır. Yaprak düğümler, baş düğümlere bilgi gönderdikten hemen sonra baş düğümlerin güven değeri güncellenmektedir.

BÖLÜM 5

PROVENANS

Provenans, kablosuz algılama ağlarında önemli bir rol oynar [99]. Kablosuz algılayıcı ağ teknolojisinin, hızla büyüyen bir kavram olduğu bilinmektedir. Küçük ve ucuz düğümler orman ve göller gibi zor ortamlarda veri toplamak gibi birçok amaç doğrultusunda rahatlıkla kullanılabilir [13].

Kablosuz algılama ağlarının birçoğunda geleneksel veri tabanı sistemlerinde gördüğümüz verileri toplama üzerinde merkezi bir kontrol olanağı mevcut değildir. Bu yüzden veriler kontrol edilemez bir şekilde silinebilir, taşınabilir, güncellenebilir ve kopyalanabilir. Provenans, algılama ağlarında veri gelişimini takip ederek daha net bir veri akış resmi görmemize olanak sağlar. Aynı zamanda provenans, verinin güvenilirliği, doğruluğu ve doğrulanabilirliği gibi niteliklerin belirlenmesinde aktif ve önemli bir rol oynar. Provenans hatalı durumların nedenini öğrenmek, ağ bağlantısını belirlemek ve verilerin güvenliğini geliştirmek için kullanılabilir. Provenans güven değerlendirmesi, hata toleransı, sorun giderme, sonuç çoğaltma ve performans optimizasyonu gibi daha sonra kullanılacak olan sonuçları nasıl anlamamız ve yorumlamamız gerektiği konusunda kullanıcıya destek sağlar. Bu nedenle provenans kablosuz algılama ağlarında ilgi duyulan bir konu olmaya başlamıştır.

Kablosuz algılama ağları, sınırlı hesaplama yeteneği ve sınırlı enerjiye sahip olmasından dolayı çok zayıf ortamlardır. Ayrıca kablosuz algılama ağları, herhangi bir alanda yürüyen bir insan tarafından kolayca devre dışı bırakılma gibi fiziksel dünya etkilerine de açıktırlar. Güven, kablosuz algılama ağları gibi kendi kendini yönetebilen ve yapılandırabilen sistemler için oldukça önemli bir kavramdır [32]. Bir kablosuz algılama ağı, doğruca verilere bağımlıdır. Bu nedenle, güncel bir veri öğesini mümkün olduğu

kadar güvende tutmak açık bir sorun teşkil etmektedir ve buna ek olarak güven değerlendirmesi de ayrı bir problemdir. Ağ güvenliği verilerin iletim yolu, kaynağın güvenirliği ve iletimden sonra geçen zaman gibi birçok etmene bağlıdır. Güven değerinin artırılması, olayların nedensellik zincirini anlamaya bağlıdır ve veri akışı odaklı provenans modeli, verinin geçiş fazlarında sağlam bir referans olur [100]. Bu model kaynak ve hedef düğüm bilgilerini ve onların durumunu tutarak, daha net bir veri akışı resmi görmemize olanak sağlar.

Bir güven yönetim şeması, kablosuz algılama ağlarının karar verme sürecine yardım ederek bir düğüm hatasını tolere edebilir. Örneğin, bir düğüm bu güven modelinden aldığı yorumlara dayanarak bir başka düğümle iş birliği yapmaya karar verebilir. Kablosuz algılama ağlarında güven araştırması yeni bir konudur ve birkaç sistem bunu göz önüne alır [30],[31]. Ama Ad-hoc ve P2P ağlarında daha önce yapılmış birçok çalışma mevcuttur. Bu ağ tipleri kablosuz algılama ağları ile birçok benzerlik göstermesine rağmen, kablosuz algılama ağlarının kısıtlı hesaplama yeteneği ve kısıtlı enerji probleminden dolayı yeni güven modellerinin geliştirilme ihtiyacı devam etmektedir. Örneğin, ad-hoc ağları için güven modellerin bazıları, ağın güvenliğini denetleyen bir itibar yöneticisine ihtiyaç duyar [101]. Bu yaklaşımın, enerji ve ölçeklendirme sorunları nedeniyle kablosuz algılama ağlarında kullanılması pek uygun ve mümkün değildir. Bu çalışmanın en büyük katkısı provenanstan yararlanılarak güvenin sağlanması ve sürdürülmesi için ağın yeniden yapılandırılması işlemidir. Daha önceki hiçbir çalışmada güven, provenans ve kablosuz algılama ağları bir arada kullanılmamıştır. Kablosuz algılama ağlarının güven değerlendirmesinde provenans kullanmak bize birçok imkân ve ayrıcalık tanıdı. Açık ve daha önce ele alınan bir konu olmadığı için bizlere açık bir araştırma alanı sundu.

eScience community'de yapılan provenans çalışmalarında algılayıcı veri erişimi, analizi [102], kaynak tabanlı hata tolerans mekanizmaları [103],[104] kaynak-tabanlı güven değerlendirmesi gibi farklı etki ve uygulama çalışmaları eklenmiştir [105]. Ayrıca veri tabanı topluluğu da provenans konusunu ele almış ve hala da provenans boyunca verilerin doğruluk yönetimi konusunda çalışmalar yapılmaktadır [106].

Veri tabanı ve e-bilim topluluğu içinde yapılan araştırma çok geniş olmasa da, algılayıcı ağları topluluğunda provenans ile ilgili yapılan araştırmalar da olmuştur. Ama bu alandaki araştırmaların hala incelenmeyen birçok yönü vardır. Algılayıcı ağlar, uygun özelliklerine göre tüm bilim alanlarına katkıda bulunmasına rağmen, provenans yönetiminde sonuçların nasıl elde edildiğine dair endişeler de mevcuttur. Bu nedenle provenansın algılayıcı ağlar topluluğu tarafından daha derin bir şekilde incelenmesi ihtiyacı doğmuştur. Bazı araştırmalar sorun giderme, hata bulma [107],[108] hata kurtarma ve başarı doğrulama [109] konusunda yaptıkları çalışmalar ile provenansı desteklemişlerdir. Bazı araştırmalar da, algılayıcı verileri ile ilişkili provenans bilgileri, etki alanına özgü karmaşık sorguların cevaplanılmasında kullanılmıştır [110].

Shebaro vd. algılayıcı verilerinin provenansa bilgi aktarımı için verimli ve güvenli bir yaklaşım sunmuşlardır [111]. Tasarladıkları provenans yaklaşımı, ara algılayıcı düğümler üzerinden geçecek algılayıcı veri olarak kodlanmış ve çözümlenmiş ve baz istasyonunda doğrulanmış hafif ağırlıklı Bloom paket filtreleri kullanır. Onlar düğümlerin arızalanma ve düzgün çalışmama gibi sakıncalarından korunmak için iletim rotasını değiştirirler.

Lim vd. saldırılara karşı algılayıcı düğümlerini korumak ve algılanan veriler için yüksek seviyede bir güvenlik sağlamak için teorik oyun savunma stratejisi geliştirmişlerdir. Çalışmalarında, saldırı-savunma etkileşimli Stackelberg adında bir oyun geliştirmişlerdir [112].

Sultana vd. paket içi zamanlama alanı içine provenans gömerek, güvenli veri akışı için güvenli provenans iletimine dayalı yeni bir yaklaşım önermişlerdir [113]. Çalışmalarında provenansı paket içi gecikmelerden ziyade algılayıcı veri ağlarının içine gömmüşlerdir. Provenans, veri alıcı tarafından optimal eşik-tabanlı mekanizmasını kullanarak, provenans çözümleme hata olasılığını en aza indirir [112].

Algılayıcı ağlardaki provenans niteliği, e-bilim ve veri tabanı topluluğundaki tanımlamalardan farklıdır [114] ve algılayıcı ağları için sağlam provenans sistemleri geliştirmek adına daha kapsamlı provenans araştırmaları yapılması gerekmektedir.

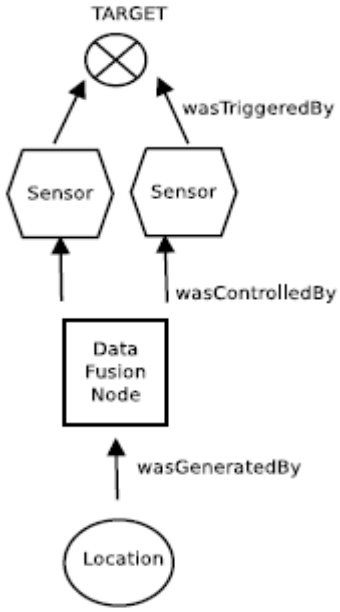
5.1 Provenans Model

Provenans model, ağın zaman aralıklarındaki anlık görüntülerini almak için kullanılmıştır [29]. Düğüm ve düğümün ait olduğu grup numaraları tutularak ağdaki veri akışı izlenebilmiştir. Ağda yeniden yapılandırma yaparken, ilgili zaman aralığındaki ağ görüntüsünü bilmek çok yararlı olmuştur. Örneğin, eğer grubun güven değeri belirli bir eşik değerinin altına düştüyse ara düğüm, grubunu güvenilir bir grupla birleştirme veya yüksek güven değeri olan bir düğümü grubuna ekleme kararı alabilir. Hangi düğümün ekleneceğine karar vermek için, ilgili zamandaki ağ görüntüsünü analiz eder ve kendisine en yakın gruptaki en güvenilir düğümü bulur.

Ağdaki veri akış provenansını modellemek için 'Open Provenance Model' kullanılmıştır. Bu model, provenans ile birlikte çalışabilirliği kolaylaştırmak için bir standart olarak geliştirilmiştir. Modelde; düğümler nesneleri, kenarlar ise kaynak nesneden (ancestor) hedef nesne arasındaki bilgi akışını temsil etmektedir (Şekil 5.1). Modelin tanımlı 5 tane nedensellik ilişkisi vardır: kullanma(used), tarafından oluşturulma (wasGeneratedBy), tarafından tetiklenme (wasTriggeredBy), -den türetilme (wasDerivedFrom), tarafından kontrol edilme (wasControlledBy). Ağdaki kenarlar bu ilişki türlerinden biriyle etiketlenir.

Şekil 5.2' de itibar ve provenans mekanizmasının işlevselliği gösterilmiştir.

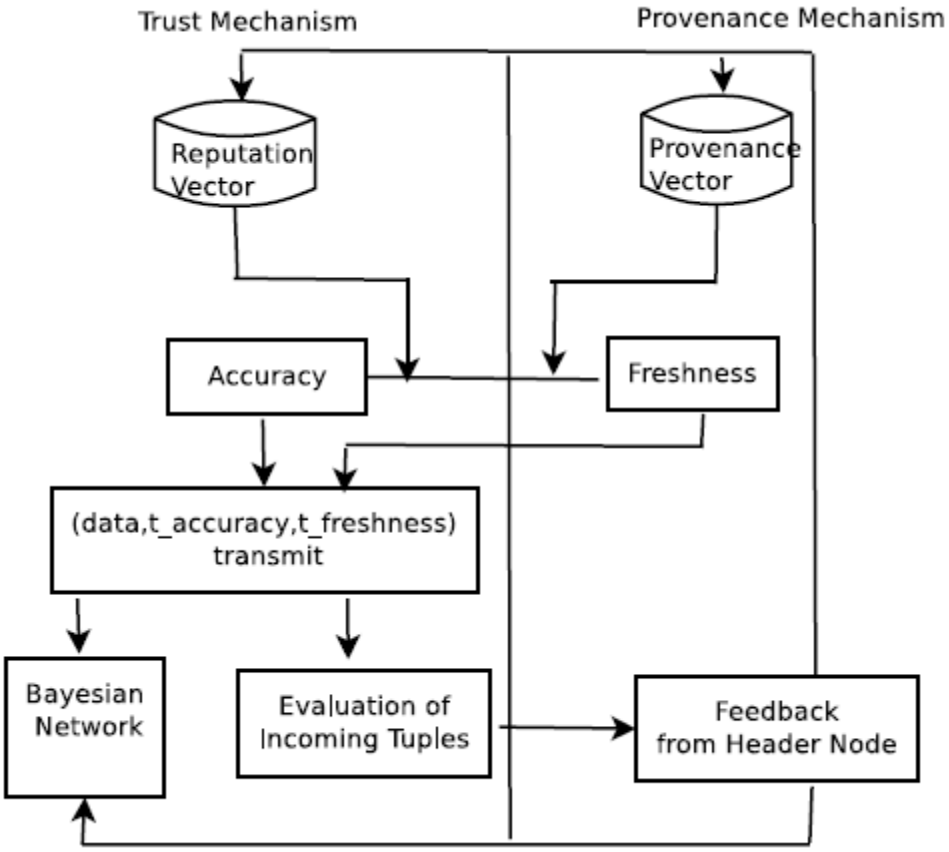
'Verinin bağlı olduğu yaprak düğümü verileri (On which leaf nodes does data depend)' ifadesi verinin bağımlılığını ifade eder [103]. Geliştirilen modelde, değer bağımlılıkları ağın anlık görüntülerini yakalamak için saklanır. Şekil 5.3'te 'C ara düğümü, A ve B düğümünden gelen veriye bağlıdır' değer bağımlılığı gösterilmektedir. Şekil 5.3'te provenans vektördeki düğüm ve grup kimliği bilgisi veri bağımlılığını oluşturur.



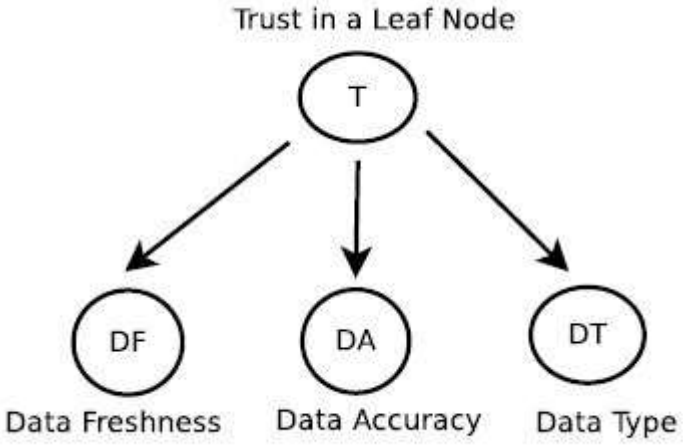
Şekil 5. 1 Provenans çizgesi [29]

Yaprak düğümdeki provenans vektör aşağıdaki değerleri tutar:

- **Node id:** Her yaprak düğümün bir düğüm kimliği(id) vardır.
- **Group id:** Her ara düğümün (intermediate node) bir kimliği vardır.
- **Message id:** Her bir mesajın bir kimliği vardır.
- **State of the node**: Yaprak düğümün durumu, uykuda (sleeping), uyanık (awake), iletiyor (transmitting) gibi
- **Creation time:** Verinin oluşturulma zamanı.
- **Left energy:** Düğümde kalan enerji.
- **Node loc x:** Düğümün x koordinatının değeri.
- **Node loc y:** Düğümün y koordinatının değeri.
- **Average error:** Geçmiş verideki ortalama hata. İlk adımda bu değer 0'dır çünkü ağ henüz gerçek değerinin farkında değildir, ilk iterasyondan sonra değer güncellenir.
- **Mean:** Geçmiş verinin ortalaması. İlk zaman aralığından sonra, iletilen veri değeri bu vektöre kopyalanır, veri algılandığında değer güncellenir.



Şekil 5. 2 İtibar ve provenans mekanizmasının işlevselliği [29]

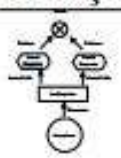


Şekil 5. 3 Güven bağımlılık modeli [29]

5.1.1 Provenans Modelin Geliştirilmesi

Bu çalışmada ProTru mimarisi, Sekil 5.4'te görülen merkezi provenans veri akış grafikleri deposu eklenerek genişletilmiştir. Daha önceki bir çalışmamızda provenans grafikleri üzerindeki sorunları gidermek maksadıyla madencilik işlevi gören DustDoctor adında bir sistem tasarlanmıştır [115]. Bu mimaride de kablosuz algılayıcı ağı sorunlarını gidermek ve güvenilmeyen düğümleri bulmak için DustDoctor'la aynı yaklaşım kullanılmıştır. DustDoctor, provenans grafikleri üzerinde madencilik yaparak GUI aracılığıyla hatalı düğümleri bildirir. Bu çalışmada önerilen modül DustDoctor'un sonuçlarına göre kablosuz algılama ağlarını yeniden şekillendirir ve ProTru'ya göre kendisini onarma açısından daha yeteneklidir.

Bu modül sonucunda elde edilen çizge verilerinin kullanılması ve test edilmesi için PopMine [116] adındaki çizge madencilik aracı kullanılmaktadır. Provenans çizgeleri Open Provenance Model(OPM) diye adlandırılan modele göre oluşturulacaktır [90].

ProvenansÇizgesi	Zaman	GüvenDeğeri
	2015-01-19 03:14:07	λ
.....	.....	.....

Şekil 5. 4 Merkezi provenans veri akış grafikleri deposu

5.2 Saldırı Modeli

Bilgi küme başına iletildiğinde, bazı saldırganlar kötü amaçlı düğüm tespitinden kurtulmak ve aynı zamanda karar vermede önemli hasar oluşturmak için kendi verilerine kendi güven değerlerini eklemeyi reddedebilir [29].

Veriye güven değeri iliştirildiğinde, her bir düğümün özel anahtarı ve <veri, güven> değer çifti ile imzalandığı varsayılır. Diğer düğüm bilgi aldığında, meta veriyi okuyabilir ve düğüm kimliğinde kimin gönderdiğini bulabilir. Böylece diğer düğüm bir önceki düğümün ilgili genel anahtarını kullanan imzayı doğrulayarak metanın bütünlüğünü doğrulayabilir. Burada düğüm, kendinden önceki düğümün güven değerini veya meta verisini değiştiremez. Çünkü meta veriyi değiştirirse, meta veriyi onun özel anahtarı ile

imzalamak zorundadır. Dolayısıyla provenansın bütünlüğü sağlanmış olur. Ayrıca düğümler hiçbir zaman sahte provenans olamaz. Kriptografiye göre, eğer herhangi bir düğüm, yetkisiz bir yolla provenansı değiştirirse veya kendi provenansı içinde sahte bir kimlik sağlarsa alıcı tarafından fark edilir.

Bunlar dikkate alınarak, aşağıda saldırı modeli listelenmiştir:

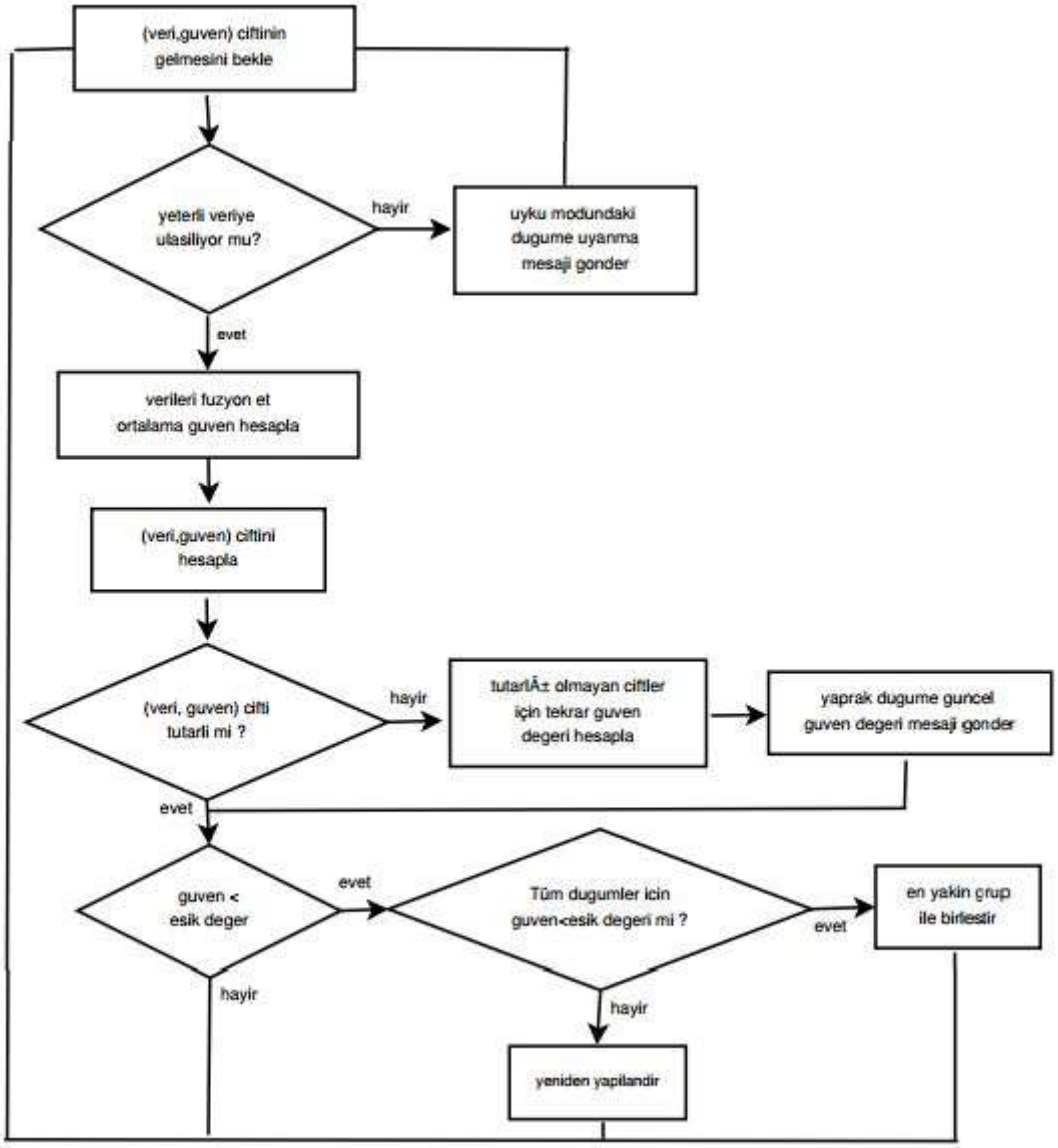
- **On-off saldırısı (attack):** Sahtekâr düğümler bundan yararlanabilir ve iyi ve kötü seçenek olarak davranır.
- **Yeni gelen saldırısı(New commer attack):** Bir düğüm yeni bir kimlik oluşturarak kendi kötü itibarından kurtulabilir.

Geliştirilen sistem, geçmişteki doğrulamadan faydalandığı için on-off saldırılara karşı esnektir. İtibar puanı sistemde zamanla oluşturulur. Geçmişte iyi davranmış olan iyi bir güven değerine sahip sahtekâr bir düğüm, hatalı veri gönderdiğinde 'Findsimilar algoritması' tarafından yakalanır, güven değeri düşürülür ve verisinin ağırlığı azaltılarak genel sonucu daha az etkilemesi sağlanır.

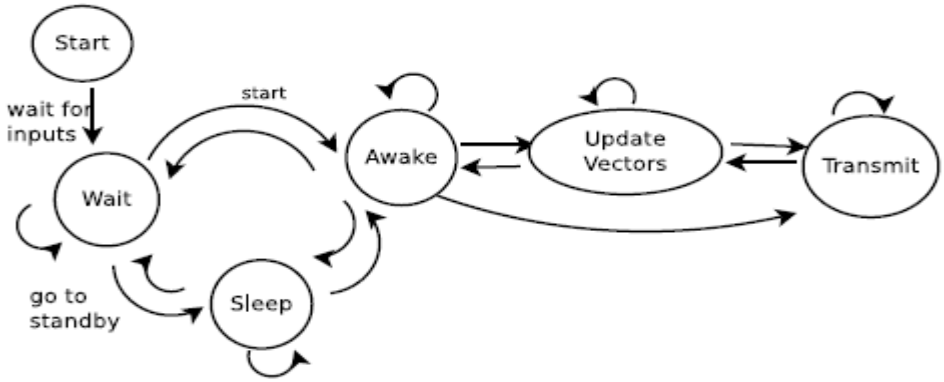
Sistem aynı zamanda kendisini yeni gelen saldırısına (new commer attack) karşıda koruyacaktır. Dağıtım sırasında genel ve özel anahtarlar merkez istasyon tarafından düğümlere atanır. Kriptografi merkezden yürütüldüğü için, kötü niyetli bir kimlik oluşturulduğunda, ağ bu düğümü fark eder.

5.2.1 Saldırı Modelindeki Sınırlamalar

Araştırmadaki sınırlamalar söyle sıralanabilir. Ağın karşılaşabileceği saldırılarla ilgili sınırlamalar olacaktır. Bir ağda yanlış veri enjeksiyonu (false data injection), sahte veri atağı (data forgery), ve gizli dinleme atağı (eavesdropping) gibi birçok saldırı olabilir. Bu çalışmada sadece yaprak düğümlere olabilecek çalışıp-çalışmayan saldırısı (on-off attack), yeni gelen saldırısı (new comer attack) saldırılarını göz önünde alınmıştır. Ana düğümlerin ise saldırılara kapalı olduğu varsayılmıştır.



Şekil 5. 5 Ara düğümde yer alan sonlu durum makinesi



Şekil 5. 6 Yaprak düğümde yer alan sonlu durum makinesi [29]

BÖLÜM 6

KABLOSUZ ALGILAMA AĞLARINDA ENERJİ

Kablosuz algılayıcı ağlara olan ilgili ciddi bir şekilde artmıştır. Algılayıcı düğümler genel olarak pille çalışan cihazlara benzerler. Ağın ömrü enerji miktarı ile paralellik gösterdiğinden dolayı bu ağlarda enerji tüketiminin optimize edilmesi önemlidir.

6.1 Kablosuz Algılama Ağlarında Enerji Tasarrufu

Bir kablosuz algılayıcı ağı sıcaklık, nem, titreşim, sismik olaylar gibi fiziksel olayları izlemek için bir coğrafi alana dağıtılan algılayıcı düğümlerden oluşur [13]. Tipik olarak, bir algılayıcı düğümü üç temel bileşen içeren küçük bir cihazdır. Fiziksel çevreden veri toplayan bir algılama sisteminden, yerel olarak veri işleyen ve depolayan bir alt sistemden ve veri iletimi için bir kablosuz iletişim alt sisteminden meydana gelmektedir. Buna ek olarak, bir güç kaynağı programlanmış görevi gerçekleştirmek için cihaz tarafından gerekli enerjiyi sağlar. Bu güç kaynağı, genellikle sınırlı bir enerjiye sahip bir pilden oluşur. Buna ek olarak bir pilin şarj edilmesi imkânsız veya çok zahmetli olabilir çünkü düğümler düşman veya kullanışsız bir ortama konuşlanmış olabilir. Öte yandan, algılayıcı ağlarının uygulama gereksinimlerini karşılaması için yeterince uzun bir ömre sahip olmaları gerekmektedir. Birçok durumda, birkaç ay veya birkaç yıla kadar bir kullanım süresi gerekli olabilir. Bu sebeplerden dolayı bu ağlardaki temel sorulardan bir tanesi ağ ömrünün nasıl uzatılacağıdır.

Bazı durumlarda, dış ortamdan enerji toplamak mümkündür [117]. Ancak, harici güç kaynağı kaynakları genellikle kesintili davranışlar gösterebilir bundan dolayı bazen bir güç tamponuna ihtiyaç duyulabilir. Her durumda enerji çok kritik bir kaynaktır ve çok az

miktarda kullanılmalıdır. Bu nedenle enerji tasarrufu, kablosuz algılayıcı ağlarına dayalı sistemlerin tasarımında önemli bir konudur.

Deneysel ölçümlerde, veri işleme işleminde daha az enerji tüketildiği görülürken, genellikle veri iletimi sırasında enerji tüketiminin daha fazla olduğu gözlemlenmiştir [118]. Normal algılayıcı düğümlerde yaklaşık olarak bir bit bilgiyi iletme maliyetinin, bin bitlik veriyi işleme maliyetine denk olduğu görülmüştür [119]. Algılama alt sisteminin enerji tüketimi, özel algılayıcıların tipine de bağlıdır. Birçok durumda verilerin işlenme süreci tüketilen enerji noktasında ihmal edilebilir. Diğer durumlarda veriyi algılamak için tüketilen enerji, veri iletimi için gerekli olan enerjiden fazla olabilir. Genel olarak, enerji tasarrufu teknikleri iki alt sisteme odaklanmıştır:

- Ağ alt sistemi
- Algılama alt sistemi

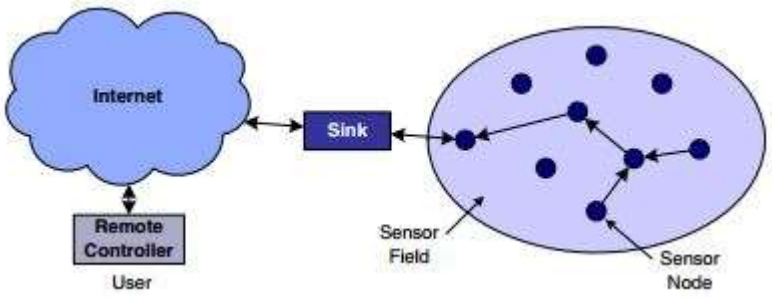
Bir algılayıcı ağının ömrü farklı tekniklerin birlikte kullanılmasıyla uzatılabilir [120]. Örneğin, enerji etkinlik protokolleri ağ faaliyetleri sırasında enerji tüketimini en aza indirmeyi hedeflemektedir. Bununla birlikte, düğüm bileşenleri aktif olmasa dahi enerji büyük miktarda bu düğüm bileşenleri (CPU, radyo, vs) tarafından tüketilir. Bu nedenle düğüm bileşenlerini kapatmak için güç yönetim planlarına ihtiyaç duyulmamıştır.

6.2 Genel Enerji Tasarruf Yaklaşımları

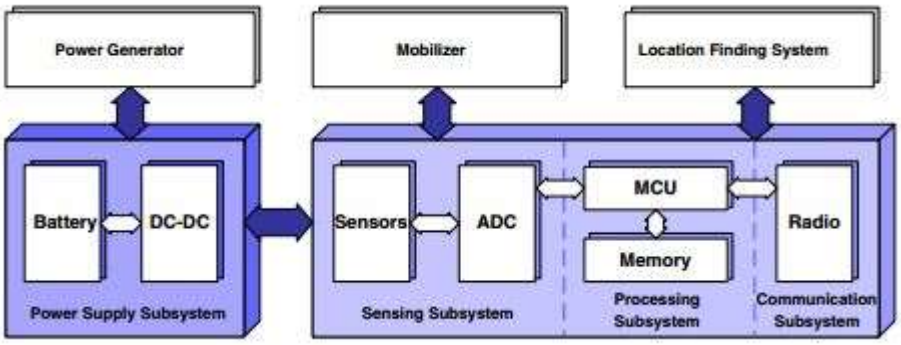
Bir algılayıcı ağ açısından bakıldığında, literatürde en yaygın kabul modelin Şekil 6.1'deki model olduğu düşünülmektedir. Diğer taraftan, genellikle literatürde de varsayıldığı gibi Şekil 6.2 tipik bir kablosuz algılayıcı düğümünün mimarisini göstermektedir ve 4 ana bileşenden oluşmaktadır.

- Veri toplama için, bir ya da daha fazla algılayıcı içeren bir algılama alt sistemi
- Yerel veri işleme için bir mikro-denetleyicisi ve bellek içeren bir işleme alt sistemi
- Kablosuz veri iletişimi için bir radyo alt sistemi
- Bir güç besleme birimi

Özel uygulamalara bağlı olarak, algılayıcı düğümleri, kendi konumunu belirlemek için bir yer bulma sistemi veya konumlarını veya yapılandırmasını değiştirmek için mobilizer gibi ilave bileşenleri de içerebilir. Bununla birlikte, ikinci bileşenleri isteğe bağlıdır ve sadece ara sıra kullanılır.



Şekil 6. 1 Algılayıcı ağ mimarisi [121]



Şekil 6. 2 Kablosuz algılayıcı ağ düğüm mimarisi [121]

Güç dağılımı büyük ölçüde belirli bir düğüme bağlıdır. Bir Mote sınıf düğümün güç karakteristiğinin Stargate düğümün güç karakteristiğinden farklı olduğu görülmüştür [118]. Ancak, aşağıdaki bilgileri de genellikle kavramak gerekir [118].

- İletişim alt sistemi, hesaplama alt sisteminden çok daha yüksek bir enerji tüketimine sahiptir. Bu nedenle iletişim hesaplamadan faydalanabilir.
- Radyo enerji tüketim miktarı alım, iletim ve boş durumlarda aynıdır ama uyku durumunda enerji tüketimi en az seviyeye düşer. Bu yüzden, radyoyu mümkün olduğu kadar uyku durumunda tutmak gerekir.
- Özel uygulamaya bağlı olarak, algılama alt sistemi enerji tüketiminin bir diğer önemli kaynağı olabilir bu yüzden güç tüketimi de azaltılmalıdır.

Yukarıdaki mimari ve güç dağılımına dayanarak, kablosuz algılayıcı ağlar güç tüketimini azaltmak için çeşitli yaklaşımlardan aynı anda faydalanmalıdır. Genel olarak teknikler üç ana gruba ayrılır.

- Duty cycling,
- Veri odaklı yaklaşımlar
- Hareketlilik

Duty Cycling ağırlıklı olarak ağ alt sistemine odaklanmıştır. İletişim gerekli olmadığında, en etkili enerji tasarrufu operasyonu radyo alıcı-vericinin uyku durumuna(düşük-güç) geçilmesidir. İdeal olanı veri gönderimi ve alımı olmadığı zaman radyonun kapatılmasıdır ve yeni bir paket hazır olduğu zamanda ise hemen devam edilmelidir. Böylece, düğümler ağ etkinliğine bağlı olarak aktif ve uyku dönemleri arasındaki işlemlerini sırasıyla yapabilir. Bu davranış, genellikle duty Cycling olarak adlandırılır ve yaşamları boyunca bir kısım düğümün aktif kalması olarak da tanımlanabilir. Algılayıcı düğümleri bir kooperatif görevi gerçekleştirmek üzereyken, düğümlerin uyku ve uyanık durumlarını koordine etmek gerekir. Bunu sağlamak için de bir uyku ve uyandırma algoritması duty Cycling ile birlikte çalışır. Bu algoritma, algılayıcı düğümlerinin aktif durumdan uyku durumuna ve tekrardan uyku durumundan aktif duruma geçmesine karar veren dağıtık bir doğaya sahiptir. Bu komşu düğümlerin aynı anda etkin olmasını sağlar, böylece düğümleri düşük görev döngüsü ile çalıştırdığınız zaman bile paket değişimi mümkün hale gelir. Duty Cycling şemaları, algılayıcı düğümler tarafından örneklenmiş olan verilerden genellikle habersizdir. Bu nedenle veri odaklı yaklaşımlar, enerji verimliliğini artırmak için daha çok kullanılabilir. Aslında veri algılama, algılayıcı düğümlerin enerji tüketimini iki şekilde etkiler:

- Gerekli olmayan örnekler. Örneklenmiş veriler, genellikle güçlü konumsal ve zamansal korelasyona sahiptir [122]. Yani gereksiz olan verilerin alıcıya gönderilmemesi gerekir.
- Algılama alt sisteminin güç tüketimi. Algılayıcının kendisinin güce ihtiyaç duyduğunda iletişiminin azaltılması yeterli değildir.

İlk durumda, örnekleme maliyeti göz ardı edilebilir olsa bile, gereksiz olan örnekler faydasız enerji tüketimine neden olur. Algılama alt sisteminin tüketimi göz ardı edilemez olduğunda ikinci sorun ortaya çıkar. Aşağıdaki sunulan veri odaklı teknikler, uygulama için algılama hassasiyetini kabul edilebilir bir seviye içinde tutarak, örneklenmiş veri miktarını azaltmak için tasarlanmıştır.

Bazı algılayıcı düğümlerinin hareketli olduğu durumlarda, hareketlilik, enerji tüketimini azaltmak için bir araç olarak da kullanılabilir(duty cycling sonrası ve veri odaklı teknikler). Bir statik algılama ağında algılayıcılardan gelen paketler alıcıya ulaşırken birden çok atlamalı bir yol izlerler. Bu durumda, birkaç tane yol, diğerlerine göre daha yoğun olabilir ve alıcıya yakın düğümlerde daha fazla paket geçişi olabilir bu yüzden alıcıya yakın düğümlerdeki enerji daha çabuk tükenecektir (funneling effect) [123]. Bazı düğümlerin hareketli olması durumunda, mobil cihazlar statik düğümlerden doğrudan veri toplayabilir böylelikle trafik akışı da değişmiş olur. Buna karşı, sıradan düğümler mobil cihaz ve rota mesajların geçişi için bekler böylelikle iletişim yakında(doğrudan veya çoğunlukla sınırlı birden çok atlamalı geçiş ile) meydana gelir. Sonuç olarak, sıradan düğümler ile de enerji tasarrufu yapılabilir, çünkü yol uzunluğu, çekişme ve yönlendirme giderleri de azalır. Buna ek olarak mobil cihaz enerji tüketimini eşit bir şekilde yaymak için ağ içerisinde gezebilir.

6.3 Küme Tabanlı Kooperatif MIMO Şeması Kullanılarak Enerji Tüketiminin Hesaplanması

Kablosuz algılayıcı ağlar, askeri ve çevresel izleme gibi birçok geniş alanda veri toplama uygulamalarında kullanılan binlerce küçük düğümlerden meydana gelmektedir [13]. Çok sayıda algılayıcı düğümü şarj etme zorluğundan ve kısıtlı enerjilerinden dolayı enerji verimliliği ve ağ ömrünü maksimize etme bir algılayıcı ağının en önemli tasarım hedeflerini teşkil etmektedirler. İletişimde meydana gelen zayıflama, parazit ve radyo düzensizliği verimli ağ iletişim protokollerini geliştirmede karşılaşılan temel sorunlardır.

MIMO(multi-input and multi-output) sistemler, zayıflamanın meydana geldiği kablosuz ağ iletişiminde, iletim enerji tüketimini azaltarak büyük oranda tasarruf sağlamaktadır [124], [125]. İş birliğine dayalı iletimde ve algılayıcılar arasındaki veri alımında, düğüm başına enerji tüketimini azaltarak ağ ömrünü artırdığı bilinmektedir [126]. Bu

şemalarda, çoklu ve birbirinden bağımsız olan anten düğümleri, enerji verimli enerji iletişimi için veri iletimi ve alımında iş birliği içerisinde çalışırlar.

M metrekarelik bir alana rastgele dağıtılmış N tane düğümün olduğunu varsayalım. Tüm yaprak düğümlerinin hareketsiz, heterojen ve kısıtlı enerjiye sahip olduğu ve her yaprak düğümün bir baş düğüme, bir baş düğümün de farklı bir baş düğüme veya merkez düğüme veri gönderdiği varsayılır. Merkez düğümlerinin ise enerji kısıtlarının olmadığı ve bir veya daha fazla alıcı anten ile donatıldığı varsayılmaktadır. Algılayıcı düğümleri bir baş düğümden oluşan kümeler halinde gruplanmıştır. Yaprak düğümleri hâkim oldukları alandaki verileri algılamakla ilgilenirler.

6.3.1 MIMO Şemasının Enerji Tüketim Modeli

Her turdaki veri iletimi sırasında enerjinin tükenmesine neden olan başlıklar aşağıda sıralanmıştır [127].

- Yaprak düğümlerinin elde ettikleri verileri baş düğüme iletmesi
- Baş düğümler tarafından yönlendirme tablosunun inşa edilmesi
- Birinci seviye baş düğümlerin elde ettikleri verileri İkinci seviye baş düğüme iletmeleri

6.3.1.1 Yaprak Düğümlerin Enerji Tüketim Modeli

Yaprak düğümlerden baş düğümlere 1 bitlik verinin iletimi için tüketilen enerji miktarı eşitlik 6.1'de verilmiştir [127].

$$E_{bs}(k_c) = -\frac{1}{\pi k_c}(1+\alpha).N_f.\sigma^2 \ln(P_b)G_1M^2M_1 + \frac{P_{ct+}P_{cr}}{B} \quad (6.1)$$

- k_c küme sayısı
- α radyo frekans güç yükselticinin verimliliği
- N_f alıcı gürültü miktarı
- σ^2 =No/2 AWGN(additive white Gaussian noise) iletim güç yoğunluğu
- P_b faz kaydırmalı anahtarlama kullanırken elde edilen bit hata oranı

- G_1 kazanç faktörü
- M_1 kazanç marjı
- B bant genişliği
- P_{ct} verici devresinin güç tüketimi
- P_{cr} alıcı devresin güç tüketimi

Her turda her baş kümeye iletilen toplam bit sayısı:

$$S_1(k_c) = \left\lceil \frac{N}{k_c} \right\rceil F_n Ps \tag{6.2}$$

- F_n bir çerçeve içindeki simgelerin sayısı
- P , her bir düğümün gönderme olasılığı
- s paket boyutu

Her bir yaprak düğümün baş düğüme veri iletirken tükettiği enerji miktarı:

$$E_s(k_c) = k_c S_1(k_c) E_{bs}(k_c) \tag{6.3}$$

6.3.1.2 Baş Düğümlerin Enerji Tüketim Modeli

Baş düğümler tarafından yönlendirme tablosu oluşturulurken tüketilen enerji miktarı:

$$E_r(k_c) = k_c R_{ts} R_{bt} \left((1+\alpha) M_1 N_f \frac{N_0 (4\pi)^2 (2M)^k}{P_b G_t G_r \lambda^2 (\pi k_c)^{k_c/2}} + \frac{P_{ct} + 4P_{cr}}{B} \right) \tag{6.4}$$

- R_{bt} yönlendirme bilgi alışverişi için gerekli olan süredir
- R_{ts} yönlendirme tablosu boyutu
- G_t ileten anten kazancı
- G_r alıcı anten kazancı
- λ iletim dalga boyu

Birinci seviye baş düğüm tarafından ikinci seviye baş düğüme bir bitlik veri gönderim sırasında tüketilen enerji miktarı:

$$E_{bc0}(k_c, J) = -\frac{1}{\pi k_c}(1+\alpha)N_f\sigma^2 \ln(P_b)G_1M^2M_1 + \frac{P_{ct} + JP_{cr}}{B} \quad (6.5)$$

Baş düğüm tarafından her turdan sonra toplanan veri miktarı:

$$S_2(k_c) = \frac{S_1(k_c)}{(\frac{N}{k_c})Pagg - agg + 1} \quad (6.6)$$

- agg toplama faktörü

Birinci seviye baş düğüm tarafından iletim için toplanmış olan verinin ikinci seviye baş düğüme iletilirken harcadığı enerji:

$$E_{c0}(k_c, J) = k_c S_2(k_c) E_{bc0}(k_c, J) \quad (6.7)$$

BÖLÜM 7

DENEYSEL SONUÇLAR

Bu bölümde sırasıyla Deney I'de yeni mimariye eklenen Kalman filtresiyle beraber düğümlerin anlık güven değerleri incelenmiştir. Deney II' de MultiPro'nun enerji tüketim modeli açıklanmıştır. Deney III'te ProTruKa mimarisinin, Deney IV'te ise MultiProTru mimarisinin hata miktarları hakkında çeşitli deneyler yapılmıştır. Deney V'te bu tez kapsamında bahsedilen mimarilerin ortalama hata miktarları karşılaştırılmıştır. Deney VI'da MultiProTru mimarisinde kullanılan Kalman filtresinin gelecek fark değerini tahmin etmek için depoladığı ağın son fark değer sayılarına göre ağın ortalama hata miktarında meydana gelen değişim gözlemlenmiştir. Deney VII' de ise bir baş düğüme bağlı yaprak düğüm sayısındaki değişikliğin ağın ortalama hata miktarını nasıl etkilediği incelenmiştir. Deney VII MultiProTru mimarisinin dinamik bir şekilde güncellenmesiyle tasarlanan DynamicMultiProTru mimarisinde eşik güven değerine göre ağın hata miktarının nasıl değiştiği gözlemlenmiştir. Son deney olan Deney IX' te ise MultiProTru mimarisinde kullanılan güven modeliyle ve EDTM (Effficient Distributed Trust Model) [88] modelinin performansları karşılaştırılımıştır.

Deneyler kapsamında ProTru, ProTruKa, MultiProTru, DynamicMultiProTru, Baseline ve EDTM mimarileri test edilmiştir. Simulasyonlarda test edilen mimariler hakkında kısa bilgiler aşağıda mevcuttur.

ProTru provenansa dayalı ve güven hesaplanmasında veri benzerliğine dayalı güven modelinin kullanıldığı bir mimaridir. ProTru ile ilgili daha geniş bilgiler bu çalışmadan edinilebilir [29].

ProTruKa mimarisi ise ProTru mimarisine Kalman filtresi eklenmesiyle tasarlanmıştır. Bu sayede ağın sadece anlık davranışı göz önüne alınmamış ağın geçmiş davranışları da göz önüne alınarak daha güvenli bir mimari tasarlanmıştır.

MultiProTru mimarisi, ProTru mimarisinin birden çok atlamalı bir şekilde genişletilmesiyle tasarlanmıştır. ProTru'dan bir diğer farkı ise güven değerlendirmesinde Kalman filtresi yöntemi kullanılmıştır.

DynamicMultiProTru mimarisinin MultiProTru' dan temel farkı algılayıcı hata oranına göre güven eşik değerinin güncellenmesidir. Bu mimari, algılayıcı hata oranı arttığı zaman güven eşik değerini de artırarak yanlış veri gönderen düğümlerin eşik değeri altında kalmasını amaçlamaktadır. Bu sayede algılayıcı hata oranının fazla olduğu durumlarda ağın ortalama hata miktarını optimize edilmeye çalışılmıştır.

Baseline mimarisinde herhangi bir güven modeli kullanılmamıştır. Her düğümün güven değeri eşittir ve ağ boyunca düğümlerin gönderdiği tüm veriler doğru kabul edilmiştir. Bu mimaride ağ aktif olduğu sürece güven değerleri sabit kalır.

Deneyde geçen iterasyon sayısı ağdaki düğümlerin veri gönderme sayısını ifade etmektedir. Örneğin iterasyon sayısı 20 olması ağdaki her bir düğümün 20 defa veri göndermesi demektir. Simulasyonda her bir düğümün aynı anda veri gönderdiği varsayılmıştır.

Hata miktarı ise algılayıcının ölçmesi gereken gerçek miktar ile ölçtüğü miktarın mutlak değer olarak farkının alınmasıyla hesaplanmıştır. Öreneğin algılayıcımızın bir koordinatın sıcaklık değerinin ölçtüğünü varsayalım. Ortamın gerçek sıcaklık değeri 30 santigrat lakin algılayıcı ortamın sıcaklık değerini 25 ölçtüğü zaman hata miktarımız bu iki değerin farkı olan 5' tir.

7.1 Deney I

Deney I kapsamında bir alana rastgele olarak dağıtılmış olan 10 yaprak düğüm ve 10 yaprak düğümün bağlı olduğu bir baş düğümden elde edilen veriler kullanılmıştır. Hesaplamalarda Netbeans derleyicisi kullanılmış ve hesaplamalar Java dilinde kodlanmıştır. Bir baş düğüme bağlı üç yaprak düğümün k=1 anından k=10 anına kadar baş düğüme gönderdikleri veriler Çizelge 7.1'de gösterilmiştir.

İlk aşamada düğümlerden elde edilen verilerin, bir ortamın sürekli değişen sıcaklık değerleri olduğu varsayılmış ve bu sıcaklık değerleri rastgele bir şekilde üretilmiştir. Sıcaklık değerlerinin birimi santigrattır.

İkinci aşamada ise her k anında baş düğüme gönderilen sıcaklık değerleri baş düğüm tarafından (4.8) numaralı denklem kullanılarak düğümlerden toplanan verilerin ortalama değeri hesaplanmıştır. Daha sonra baş düğüm tarafından hesaplanan bu ortalama değerden her yaprak düğümün farkı alınmıştır.

Bir sonraki aşamada ise elde edilen fark değerleri Kalman filtresinden geçirilmiştir. Bu veriler (4.9) numaralı denklemde kullanılarak her k anı için düğümlerin sahip olduğu güven değerleri hesaplanmıştır. Sonuç olarak da hesaplamalar sonucunda her k anı için güncellenen güven değerleri Çizelge 7.2'de gösterilmiştir. Hesaplamalarda λ değeri 0.1 alınmıştır ve k=1 anında her düğüme e güven değeri atanmıştır.

Çizelge 7.1 Anlık düğüm verileri

Zaman	T1	T2	T3	T 4	T 5	T 6	T 7	T 8	T 9	T 10
Düğüm1	44	33	36	48	33	27	51	18	35	47
Düğüm2	43	44	23	10	39	45	45	27	36	38
Düğüm3	28	54	31	44	48	39	74	10	33	44
Düğüm4	35	28	29	16	18	34	47	55	39	61
Düğüm5	57	35	40	42	54	27	11	33	42	74
Düğüm6	49	27	30	25	34	43	48	54	27	16
Düğüm7	33	53	72	19	13	80	77	56	22	13
Düğüm8	10	76	15	44	33	28	39	40	43	27
Düğüm8	85	49	46	50	44	41	25	16	45	16
Düğüm10	13	25	33	21	25	44	10	72	48	45

Çizelge 7.2 Anlık güven değerleri

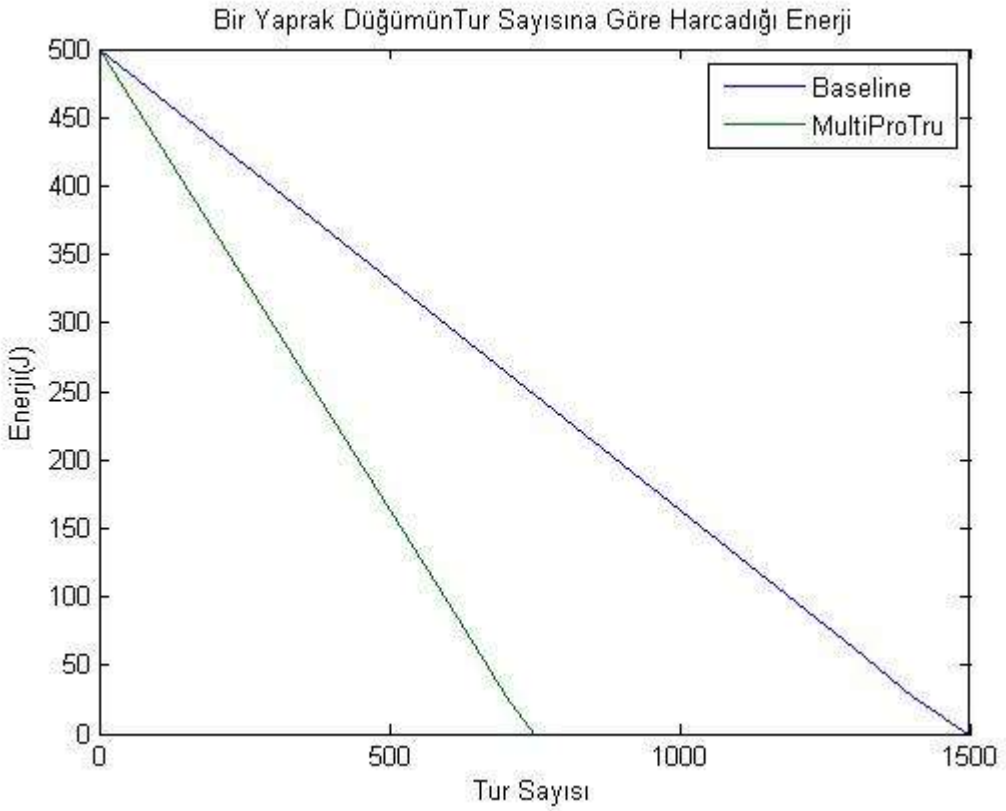
	T1	T2	T3	T 4	T 5	T 6	T 7	T 8	T 9	T 10
D1	1.035	1.018	1.024	1.014	1.017	1.014	1.014	1.011	1.012	1.012
D2	1.046	1.051	1.020	1.0115	1.012	1.013	1.014	1.013	1.015	1.016
D3	1.012	1.010	1.012	1.0113	1.010	1.011	1.008	1.007	1.008	1.008
D4	1.032	1.013	1.013	1.0109	1.009	1.010	1.010	1.009	1.010	1.009
D5	1.008	1.010	1.012	1.0115	1.009	1.008	1.007	1.007	1.008	1.006
D6	1.016	1.010	1.011	1.012	1.014	1.016	1.016	1.014	1.013	1.011
D7	1.022	1.014	1.006	1.006	1.006	1.005	1.004	1.004	1.004	1.004
D8	1.005	1.003	1.004	1.004	1.005	1.005	1.006	1.007	1.007	1.007
D9	1.003	1.004	1.005	1.005	1.006	1.007	1.006	1.006	1.006	1.006
D10	1.005	1.005	1.007	1.007	1.008	1.009	1.007	1.006	1.006	1.006

7.2 Deney II

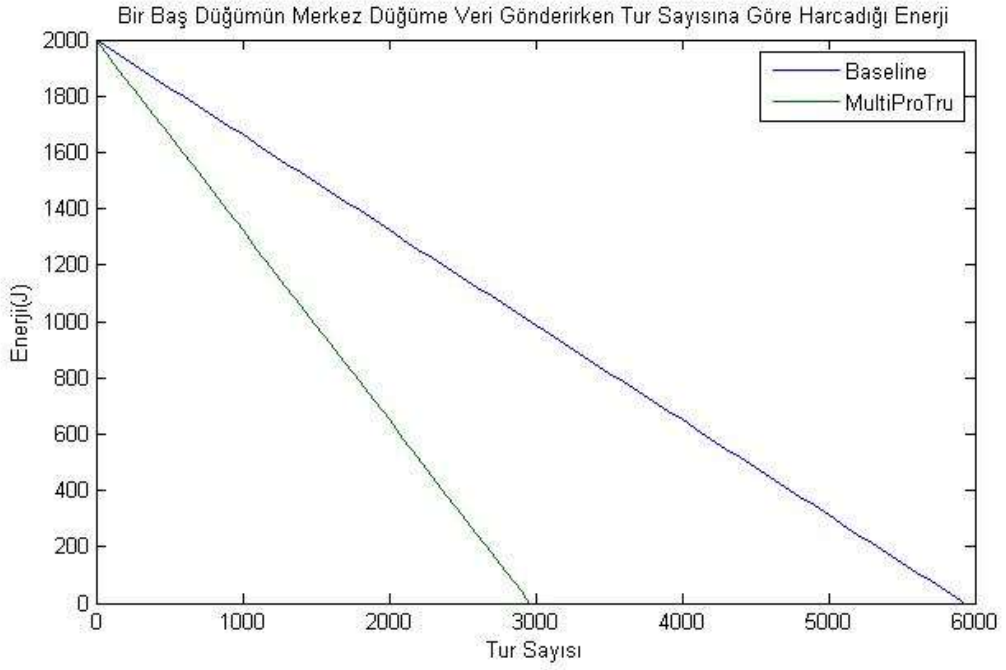
Deney II kapsamında geliştirilen MultiProTru mimarisinin iletişim esnasında harcadığı enerji MIMO şeması kullanılarak hesaplanmıştır. Hesaplamalarda ağda 100 adet yaprak düğüm ve 10 adet baş düğüm olduğu ve her yaprak düğümün 0.5 J ve her baş düğümün 2 J enerjiye sahip olduğu varsayılmıştır. Simülasyon için kullanılan sistem parametreleri Çizelge 7.3'te yer almaktadır. Baseline ve MultiProTru mimarilerinin enerji tüketimlerine bakıldığı zaman Baseline mimarisinde herhangi bir güven modeli kullanılmadığından dolayı ağ ömrünün daha uzun olduğu görülecektir. MultiProTru mimarisinde ise iletim esnasında hem veri hem de güven değeri aynı anda gönderildiğinden dolayı enerji tüketimi artmış dolayısıyla ağ ömrü azalmıştır. Kablosuz algılayıcı ağlarında iletim esnasında harcanan enerjinin hesaplama noktasında harcanan enerjiden çok olduğu düşünüldüğü zaman yeni iletim modellerinin geliştirilmesine olan ihtiyacın hala devam edildiği görülecektir.

Çizelge 7.3 İletişim parametreleri

Parametre	Değer
RF güç yükseltici verimlilik oranı (α)	0.4706
Bağlantı marjı (M_1)	40 dB
Kazanç faktörü (G_1)	30 dB
AWGN kanalının güç yoğunluğu (σ2)	-134 dBm /Hz
Alıcı gürültü seviyesi (N_f)	10 dB
Yol kaybı (k)	3-5
Taşıyıcı frekansı (f_c)	2.5 GHz
Bant genişliği (B)	20 KHz
BER performansı (P_b)	10^{-3}
Vericinin devre güç tüketimi (P_{ct})	98.2 mw
Alıcının devre güç tüketimi (P_{cr})	112.6 mw
Verici ve alıcı anten kazancı (G_t, G_r)	5 dB
Her tur için yönlendirme tablosunu değişimi	5
Yönlendirme tablosu boyutu (R_{ts})	100
İletim hızı (R)	0.75
Paket boyutu (s)	2 kbits
Tur başına frame sayısı (F_n)	2
Her bir düğüm iletim olasılığı (P)	0.8



Şekil 7.1 Bir yaprak düğümün tur sayısına göre harcadığı enerji



Şekil 7.2 Bir baş düğümün tur sayısına göre harcadığı enerji

7.3 Deney III

Deneyde kullanılan parametreler Çizelge 7.4' te verilmiştir. 100 x 100 m bir alana rastgele dağıtılmış olan 100 adet yaprak ve 10 adet baş düğümün olduğu varsayılmaktadır. Her baş düğüme bağlı 10 tane yaprak düğüm vardır. Algılayıcıların amacı bulundukları alanın sıcaklık değerini ölçmektir ve her bir simülasyonda, sıcaklık değerleri rastgele seçilmiştir. Ölçümler matlab dilinde kodlanmış ve sıcaklık birimi santigrattır. Her bir hata yüzdesi için aynı deney 20, 80, 800 ve 1000 kez tekrarlanmıştır. Sonuç olarak ProTruKa ve Baseline mimarileri için hata miktarı hesaplanmıştır.

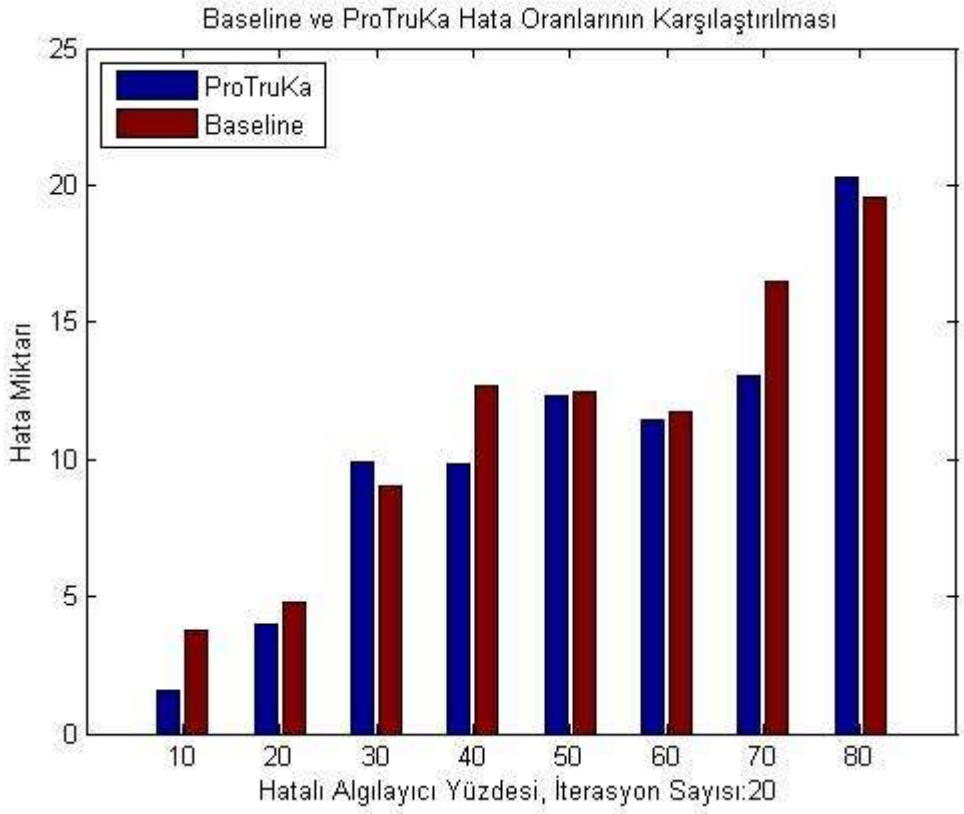
Çizelge 7.4 Deney III parametreleri

Olay	Sıcaklık İzleme
Hatalı Veri Yüzdesi	10%
Grup Sayısı	10
Ağın Boyutu	10 Baş Düğüm (10 groups), 100 Yaprak Düğüm
Düğüm Türü	Sıcaklık Düğümleri (Sıcaklık Verileri)
β (güven eşik değeri)	0.1
λ	0.1

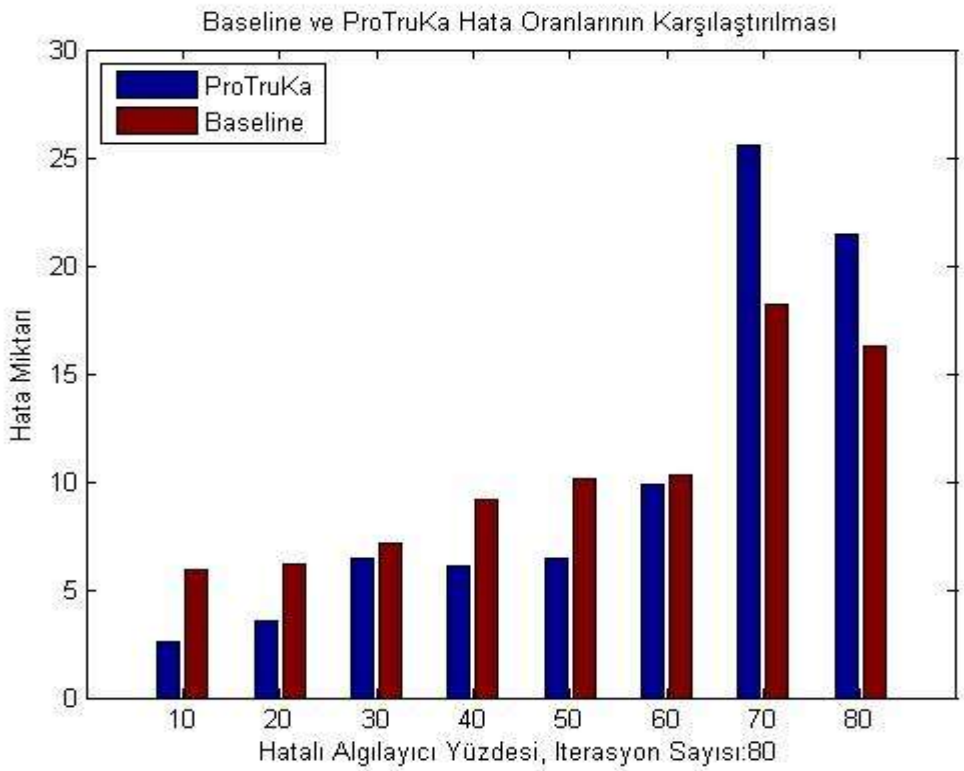
Simülasyon kapsamında ProTruKa ve Baseline mimarilerinin güven değerleri hesaplanmıştır. Baseline mimarisinde herhangi bir güven modeli kullanılmamıştır. ProTruKa mimarisine ise Kalman Filtresi tekniği eklenerek düğümlerin güven değerleri veri benzerliğine dayalı yöntemlerle ölçülmüştür. Daha sonra hatalı algılayıcı oranına göre ProTruKa ve Baseline mimarilerinin ortalama hata miktarları karşılaştırılmıştır. Hatalı algılayıcı oranı, arızalı algılayıcıların sayısının dağıtılan algılayıcıların toplam sayısına oranıdır.

7.3.1 Hatalı Algılayıcı Yüzdesine Göre Hata Miktarlarının Karşılaştırılması

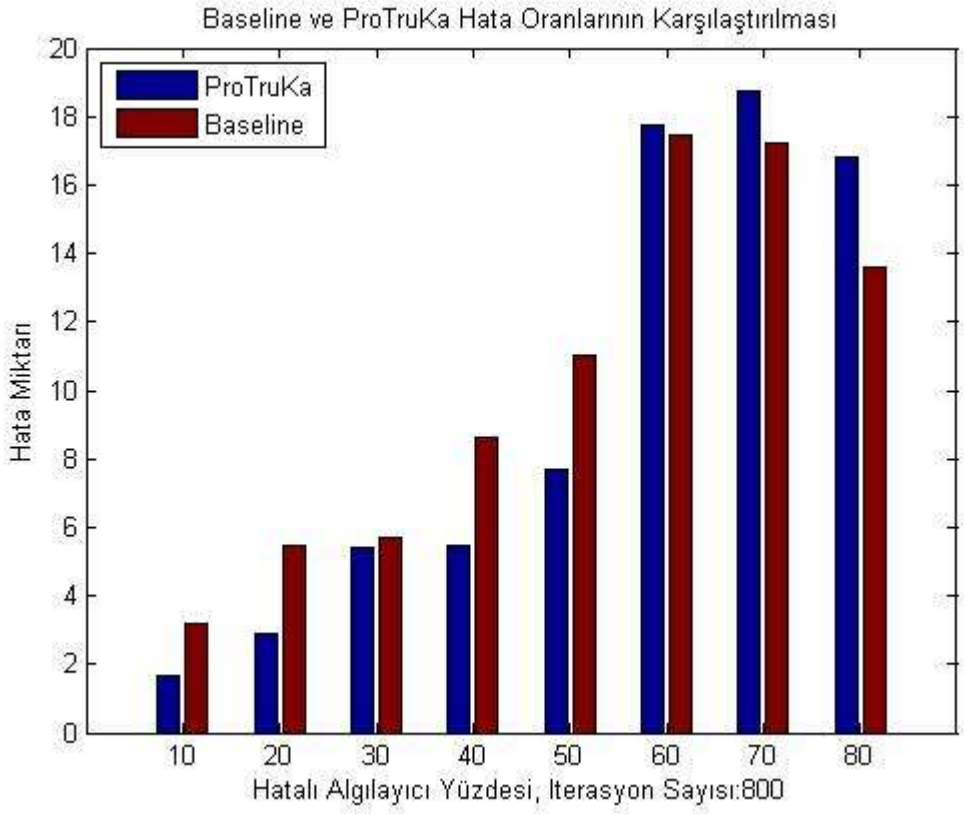
Bu deneyde ProTruKa ve Baseline mimarilerin hatalı algılayıcı yüzdesine göre hata miktarları karşılaştırılmıştır. Aynı deney 20, 80, 800 ve 1000 iterasyon değerleri için tekrarlanmıştır. Bu deney kapsamında ProTruKa mimarisine Kalman filtresi eklenerek her iterasyon sonucunda hatalı veriler üreten düğümün güven değeri azaltılarak ağın ortalama hata miktarı minimize edilmeye çalışılmıştır. Kalman filtresiyle yanlış veri rapor eden düğümlerin güven değeri azaltılmış, doğru bilgi gönderen düğümlerin güven değeri artırılmıştır. Hatalı algılayıcı yüzdesinin düşük olduğu noktalarda ProTruKa'nın Baseline göre daha başarılı, hatalı algılayıcı yüzdesinin yüksek olduğu noktalarda ise ProTruKa daha hatalı sonuçlar elde ederek ağın ortalama hata miktarını yükseltmiştir. ProTruKa mimarisi zamanla hatalı verilerin güven değerini düşürerek ağın ortalama hata miktarını düşürme becerisine sahiptir. Özellikle ProTruKa mimarisine Kalman filtresi eklenerek ağın sadece anlık davranışı değil, geçmiş davranışlarını da göz önüne alındığından dolayı başarı oranının arttığı gözlemlenmiştir.



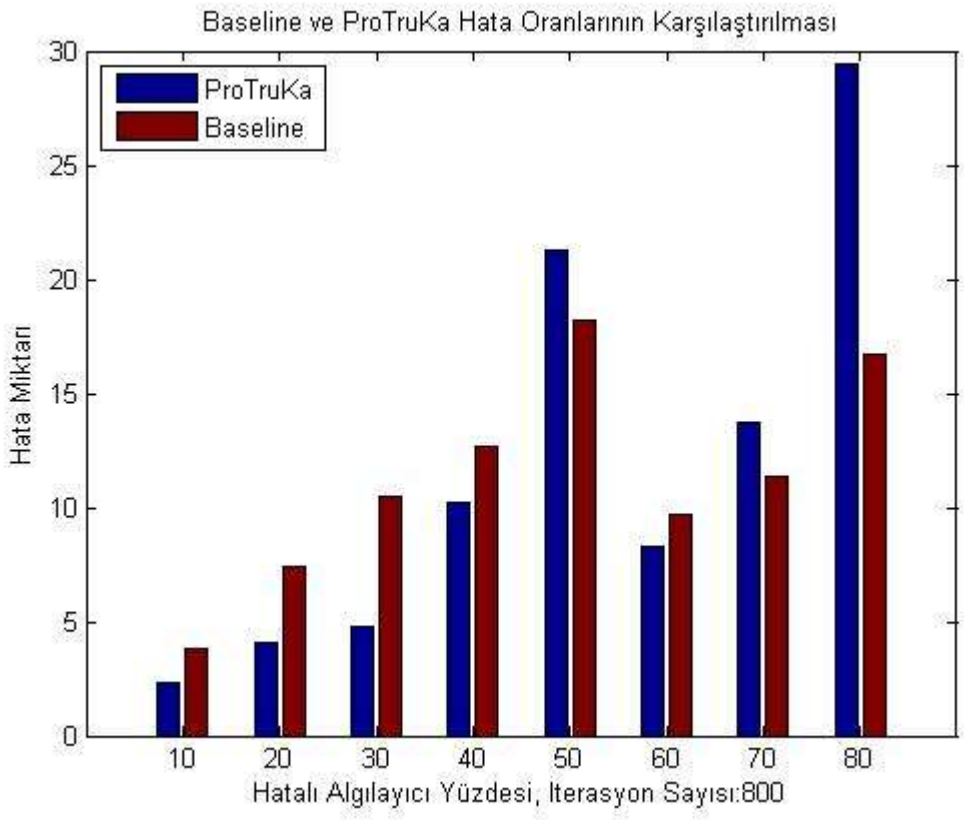
Şekil 7.3 Sıcaklık izleme algılayıcı ağındaki hata miktarı (iterasyon: 20)



Şekil 7.4 Sıcaklık izleme algılayıcı ağındaki hata miktarı (iterasyon: 80)



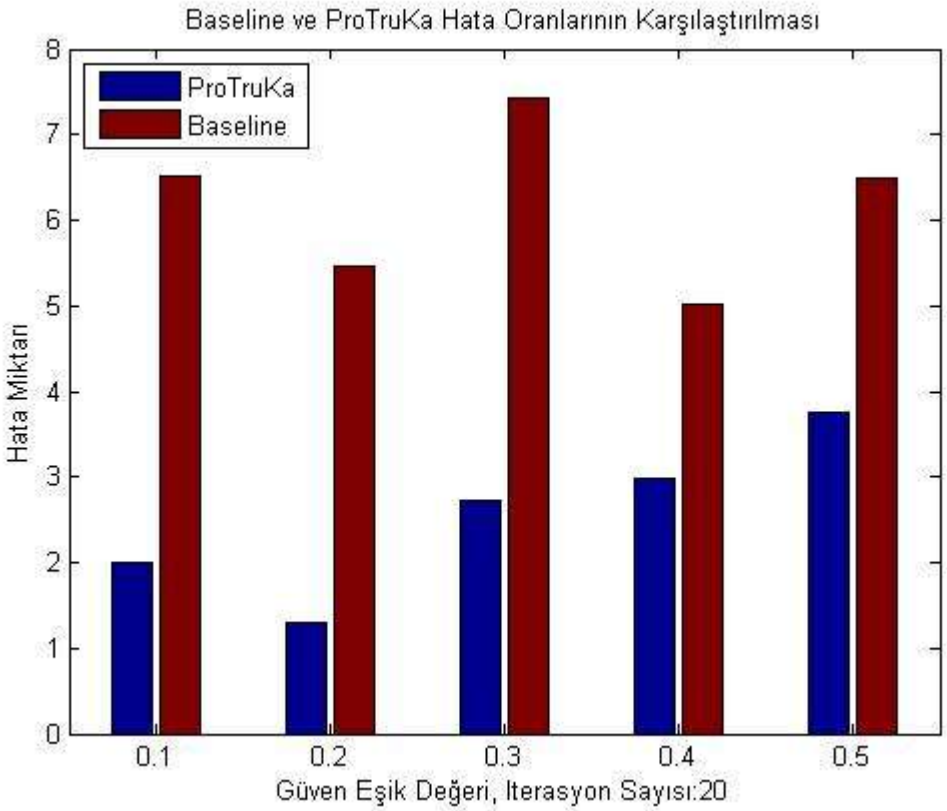
Şekil 7.5 Sıcaklık izleme algılayıcı ağındaki hata miktarı(iterasyon: 800)



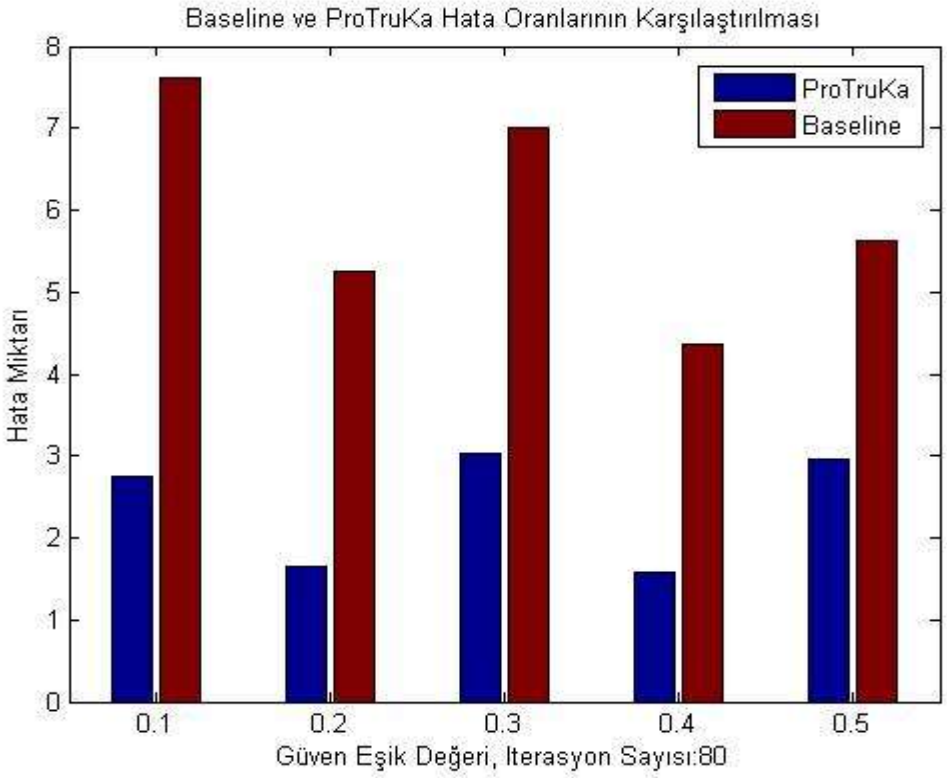
Şekil 7.6 Sıcaklık izleme algılayıcı ağındaki hata miktarı(iterasyon: 1000)

7.3.2 Eşik Güven Değerine Göre Hata Miktarlarının Karşılaştırılması

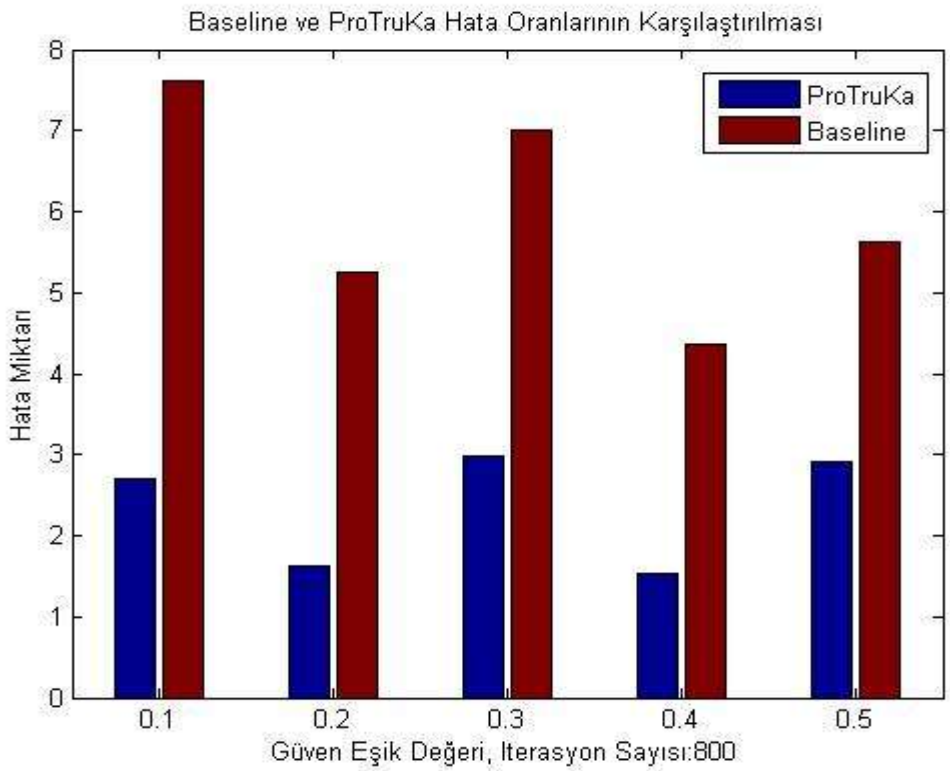
Bu bölümde ağın güven eşik değerine ProTruKa ve Baseline mimarilerinin hata miktarları hesaplanmıştır. Deneyler 20, 80, 800 ve 1000 iterasyon değerleri için tekrarlanmıştır. ProTruKa mimarisinde düğümler belirlenen güven eşik değerinden daha küçük bir güven değerine sahip olduğunda bu düğüm uyku durumuna geçirilmektedir. Uyku durumuna geçirilen düğümün veri ve güven değerleri genel hesaplamalara dâhil edilmezler. Bir sonraki iterasyonda uyku durumuna geçirilen düğüm uyanır tekrardan veri gönderir ve güven değeri tekrardan hesaplanır. Aşağıdaki şekillere de bakıldığı zaman güven eşik değerine göre hesaplanan hata miktarlarına göre ProTruKa mimarisinin Baseline mimarisine göre daha başarılı olduğu ve rasyonel güven değerleri ürettiği görülecektir. Deney sonucunda ağın güven eşik değerinin küçüldükçe, ağın hata toleransında artış meydana geldiği görülmüştür.



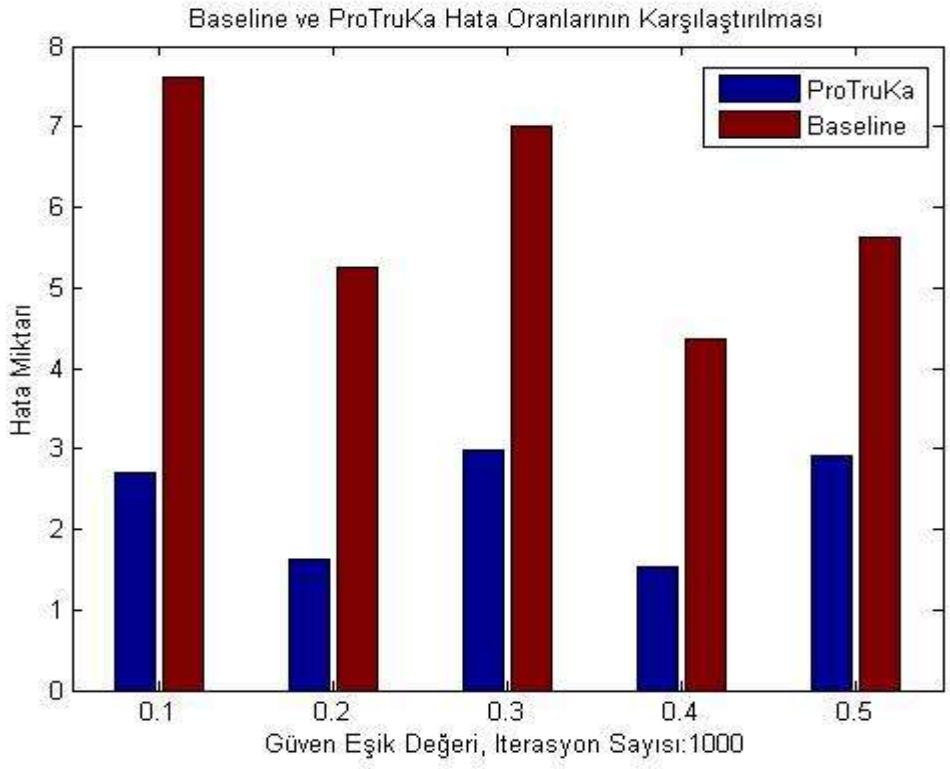
Şekil 7.7 Farklı güven eşikleri için hata miktarı(iterasyon: 20)



Şekil 7.8 Farklı güven eşikleri için hata miktarı (iterasyon: 80)



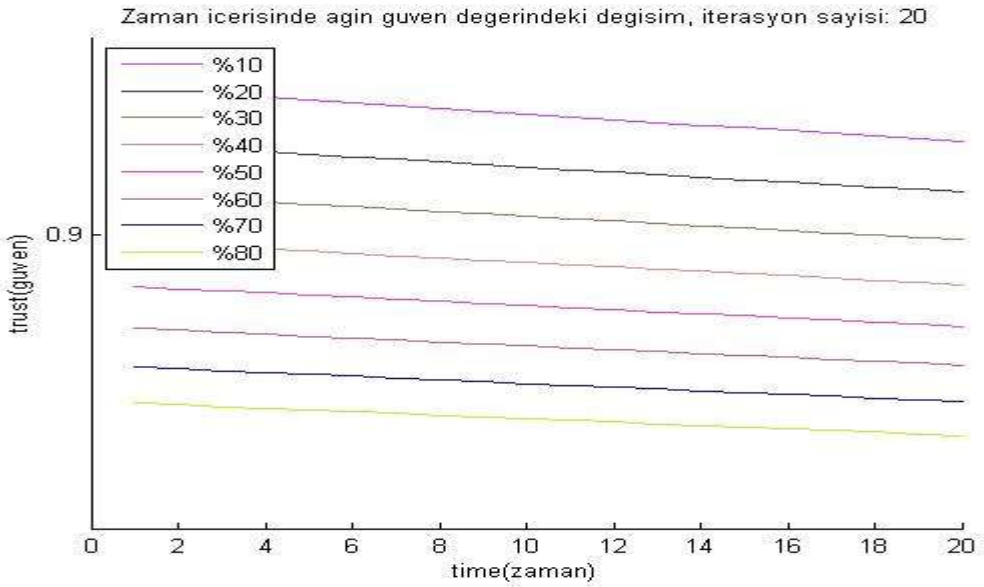
Şekil 7.9 Farklı güven eşikleri için hata miktarı (iterasyon: 800)



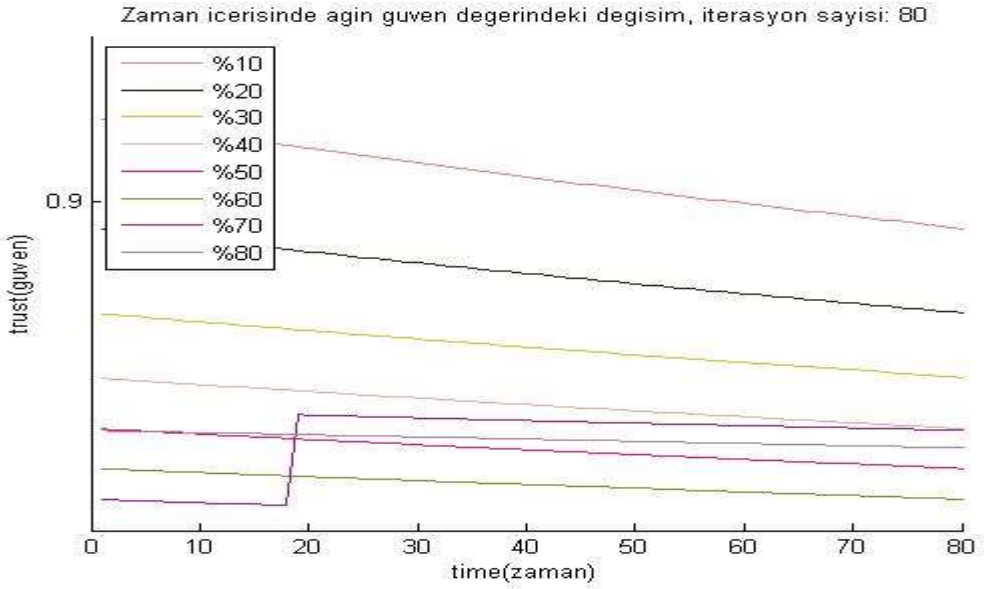
Şekil 7.10 Farklı güven eşikleri için hata miktarı (iterasyon: 1000)

7.3.3 Zamana Göre Ağın Güven Değerinde Meydana Gelen Değişim

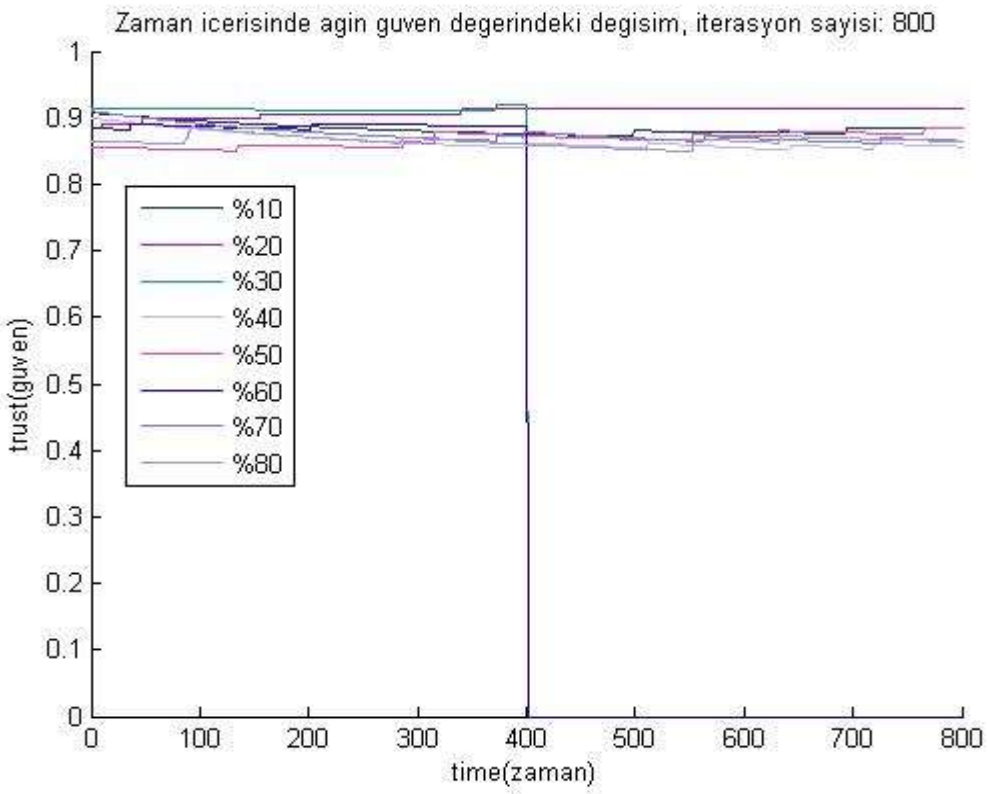
Bu bölümde hatalı algılayıcı yüzdesine göre ProTruKa'nın güven değerinde meydana gelen değişim izlenmiştir. Deneyde düğümler güven eşik değerine ulaşmadan gruba dâhil edilmemişlerdir. Düğümler doğru bilgi rapor ettiklerinde güven değerleri artmış, yanlış bilgi rapor ettiklerinden güven değerleri azalmıştır. Baseline mimarisinde herhangi bir güven tekniği kullanılmadığı için güven değerleri sürekli sabit kalmıştır.



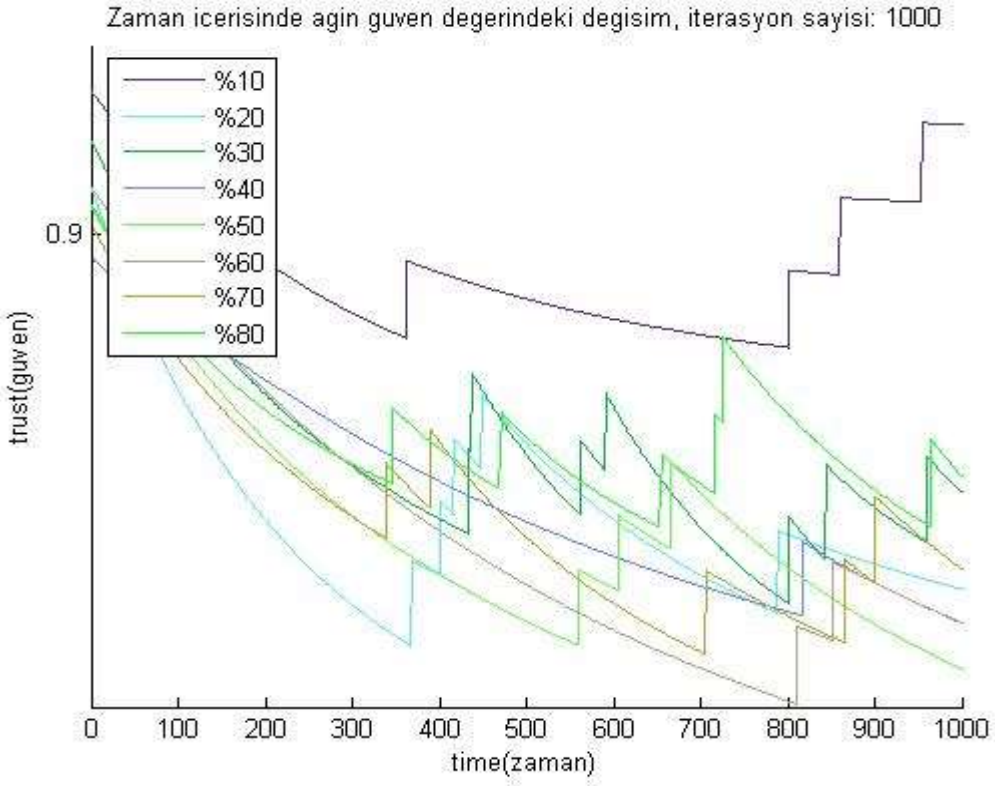
Şekil 7.11 Ağın güven değerindeki değişim (iterasyon: 20)



Şekil 7.12 Ağın güven değerindeki değişim (iterasyon: 80)



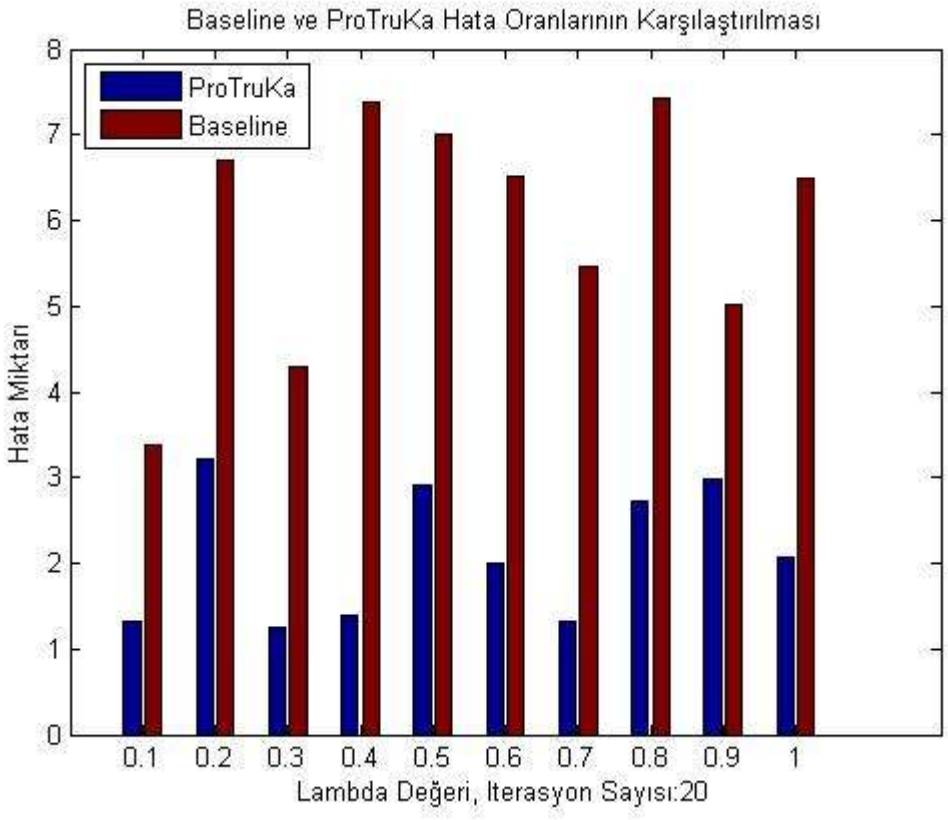
Şekil 7.13 Ağın güven değerindeki değişim (iterasyon: 800)



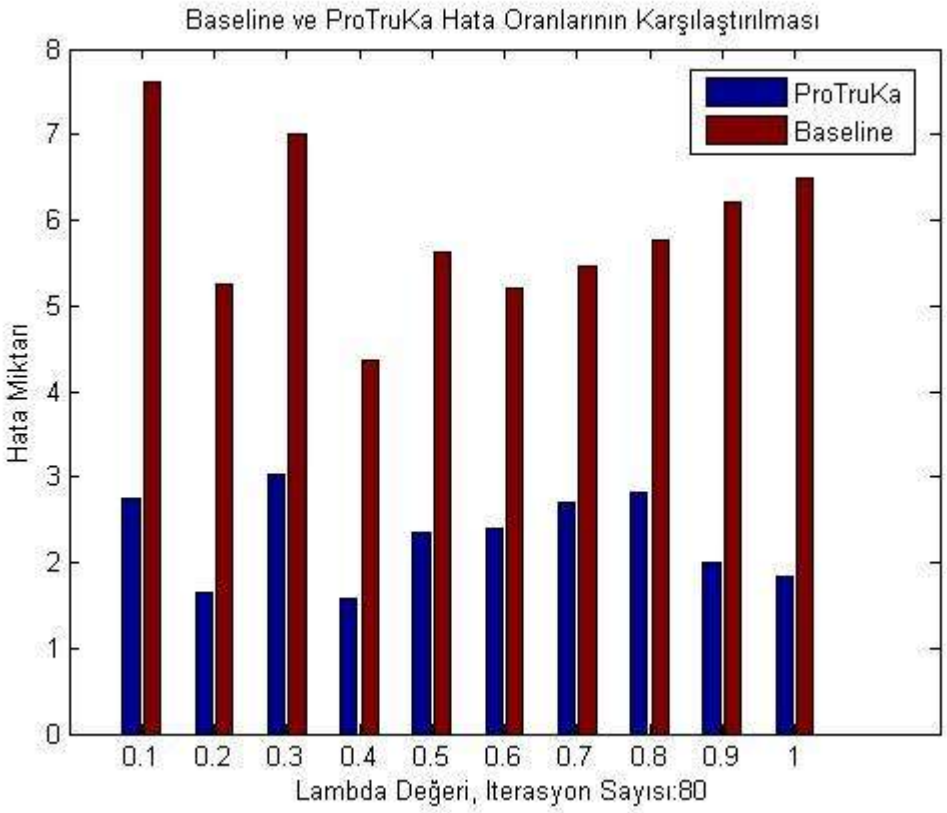
Şekil 7.14 Ağın güven değerindeki değişim (iterasyon: 1000)

7.3.4 Lambda Değerine Göre Hata Miktarlarının Karşılaştırılması

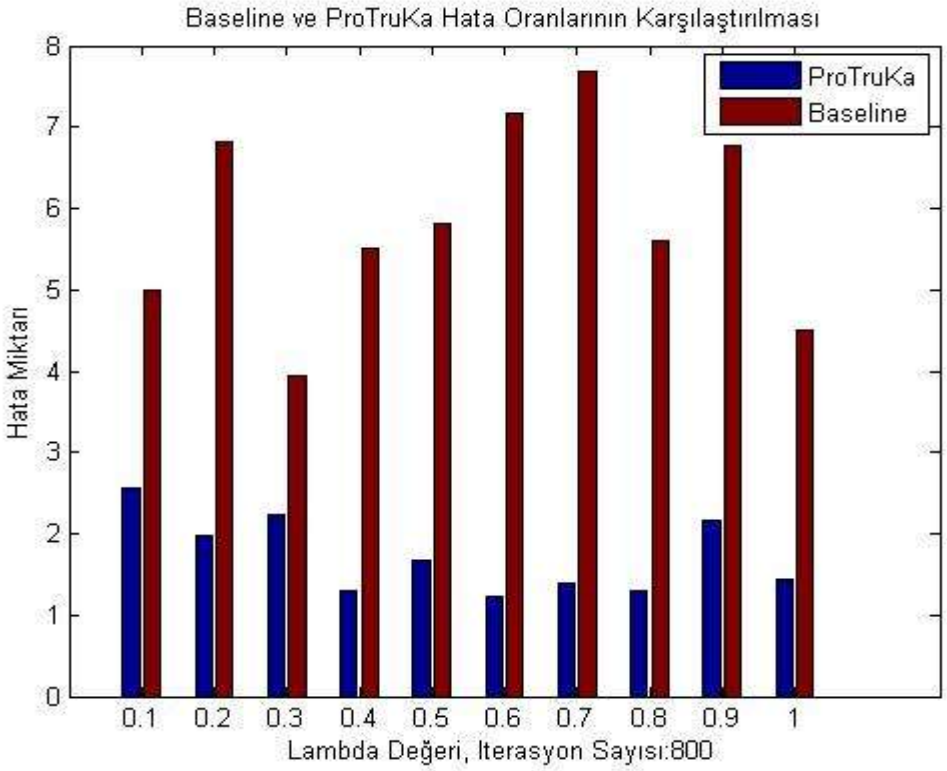
Bu bölümde formül (4.9)'da kullanılan lambda değerine ProTruKa ve Baseline mimarilerinin hata miktarları karşılaştırılmıştır. Lamda değeri 0 ile 1 arasındadır. Şekillerde de görüldüğü üzere genel olarak lambda değeri ve güven değeri arasında ters orantı mevcuttur. Deney 20, 80, 800, 1000 iterasyon değerleri için tekrarlanmıştır. Lambda değerleri 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9 ve 1 değerleri için ProTruKa mimarisinin Baseline mimarisine göre hata miktarının düşük olduğu dolayısıyla ProTruKa mimarisinin daha başarılı olduğu Şekil 7.15, Şekil 7.16, Şekil 7.17, ve Şekil 7.18'de görülmektedir.



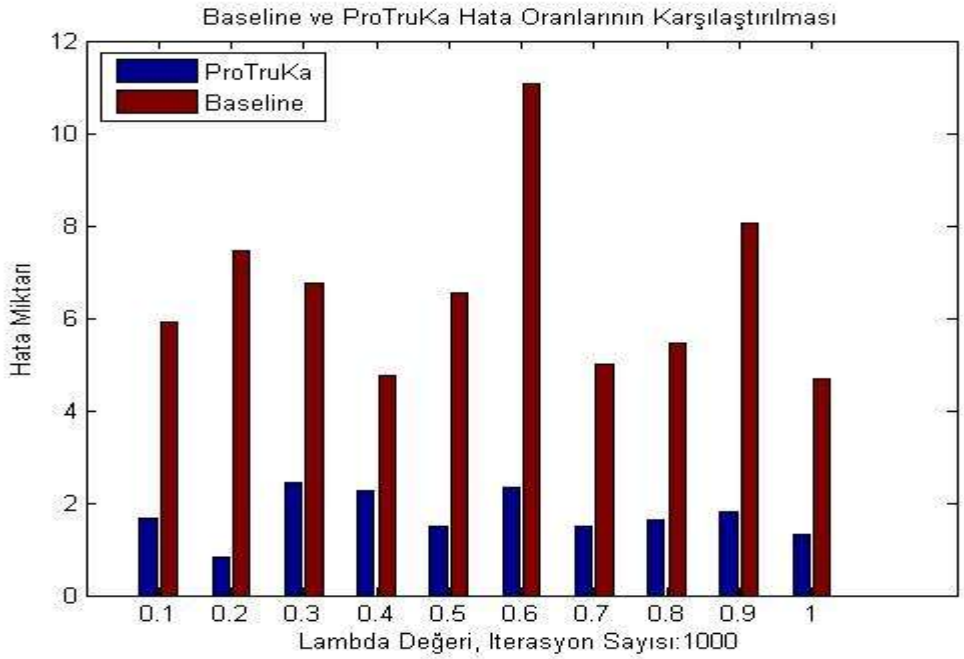
Şekil 7.15 Farklı lambda değerlerine göre hata miktarları (iterasyon: 20)



Şekil 7.16 Farklı lambda değerlerine göre hata miktarları (iterasyon: 80)



Şekil 7.17 Farklı lambda değerlerine göre hata miktarları (iterasyon: 800)



Şekil 7.18 Farklı lambda değerlerine göre hata miktarları (iterasyon: 1000)

7.4 Deney IV

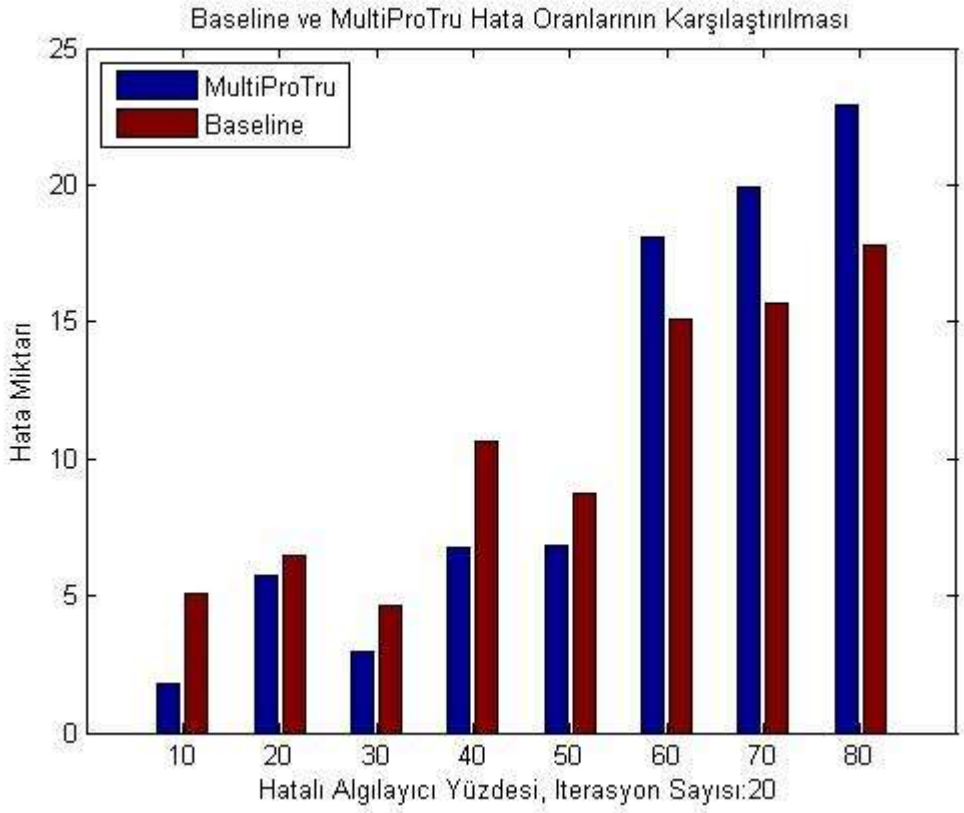
Bu bölümde ProTru mimarisin genişletilmesiyle tasarlanan MultiPro mimarisiyle ilgili çeşitli deneyler yapılmıştır. Deney kapsamında Çizelge 7.5 'teki veriler kullanılmıştır.

Çizelge 7.5 Deney IV parametreleri

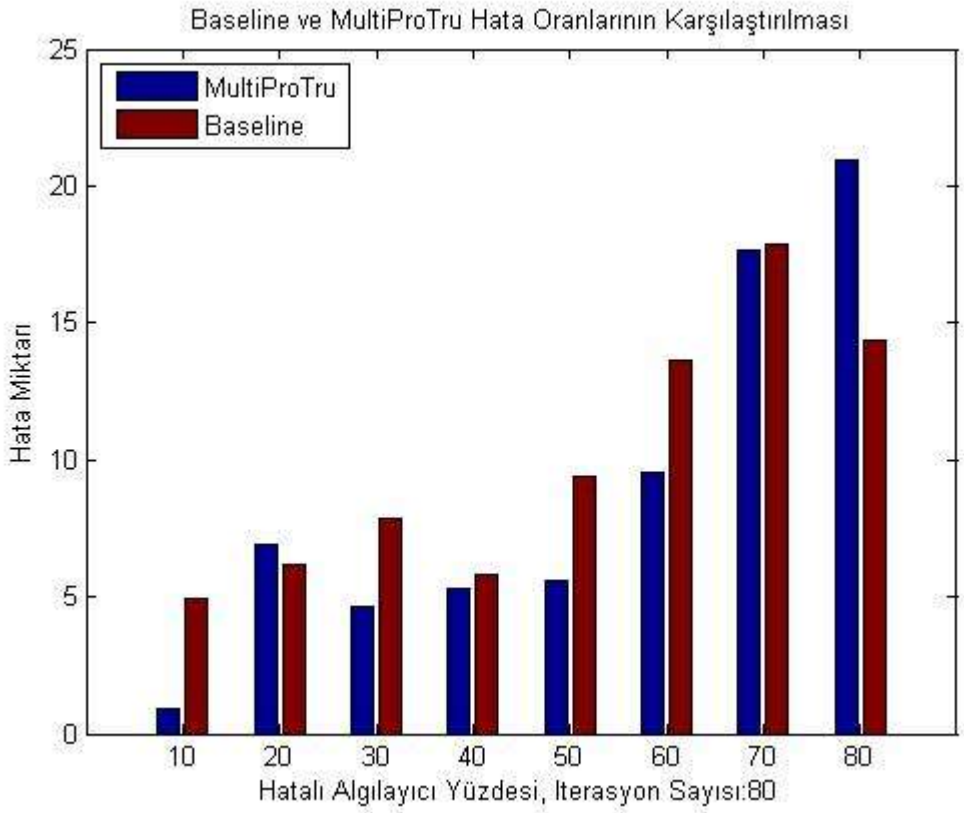
Olay	Sıcaklık İzleme
Hatalı Veri Yüzdesi	20%
Grup Sayısı	10 Adet Birinci Seviye Baş Düğüm 10 Adet İkinci Seviye Baş Düğüm
Ağın Boyutu	200 Yaprak Düğüm
Düğüm Türü	Sıcaklık Düğümleri (Sıcaklık Verileri)
β (güven eşik değeri)	0.1
λ	0.1

7.4.1 Hatalı Algılayıcı Yüzdesine Göre Hata Miktarlarının Karşılaştırılması

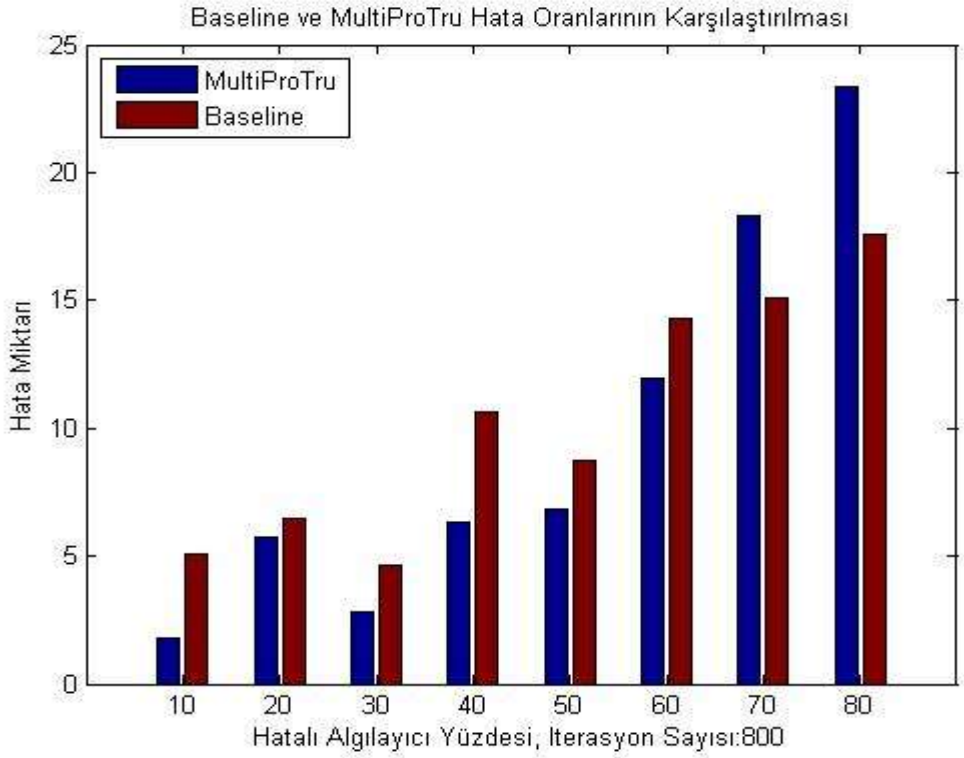
Bu deneyde MultiProTru ve Baseline mimarilerin hatalı algılayıcı yüzdesine göre hata miktarları karşılaştırılmıştır. Deneyler 20, 80, 800 ve 1000 iterasyon değerleri için tekrarlanmıştır. MultiProTru mimarisi ProTru mimarisinin birden çok atlamalı bir şekilde güncellenmesiyle tasarlanmıştır. MultiProTru'da güven değerlendirmesinde Kalman filtresi kullanılırken Baseline mimarisinde herhangi bir güven modeli kullanılmamıştır. Kalman filtresi ağın sadece anlık davranışından ziyade ağın geçmiş davranışlarını da göz önüne alarak bir güven değeri hesaplamıştır. Kalman filtresi yanlış veriler üreten düğümlerin hata miktarını düşürürken doğru veri üreten düğümlerin güven değerini artırmıştır. Bu işlemlerin yapılmasındaki temel amaç ağın hata miktarını minumum bir seviye getirmek ve düğümlerin ürettiği değerlerin doğruluk derecesini iyi ölçmektir. Baseline mimarisine herhangi bir güven modeli kullanılmadığından dolayı düğümlerin güven değerleri sürekli sabittir. Şekil 7.19, Şekil 7.20, Şekil 7.21, ve Şekil 7.22'ye bakıldığı zaman hatalı algılayıcı yüzdesinin düşük olduğu noktalarda MultiProTru mimarisinin Baseline mimarisine göre daha başarılı olduğu görülecektir.



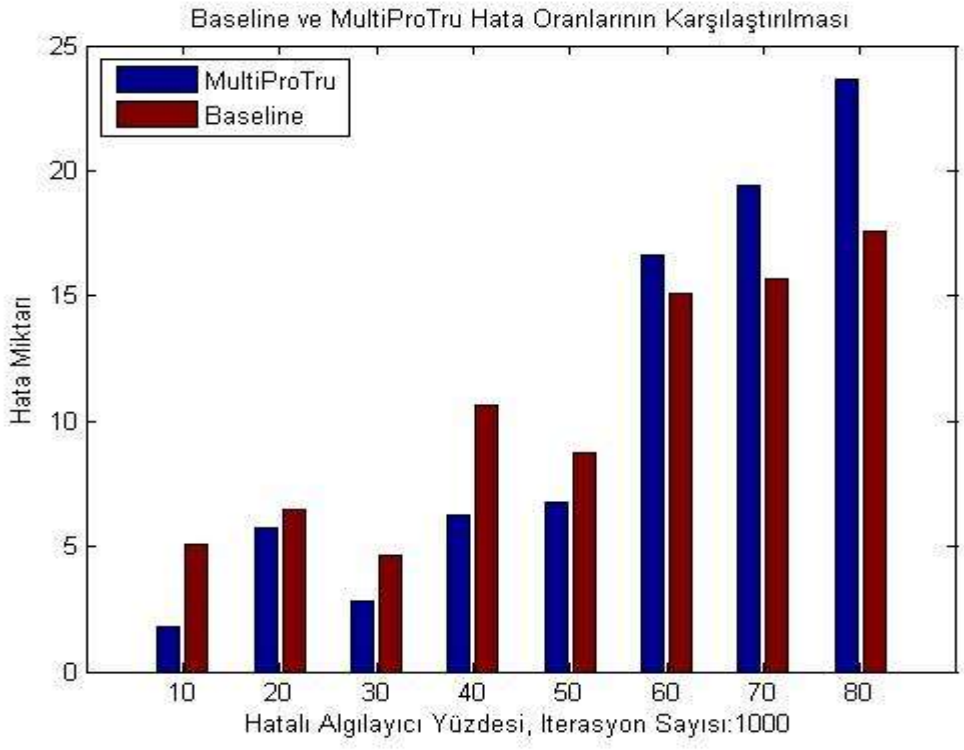
Şekil 7.19 Sıcaklık izleme algılayıcı ağındaki hata miktarı(iterasyon: 20)



Şekil 7.20 Sıcaklık izleme algılayıcı ağındaki hata miktarı(iterasyon: 80)



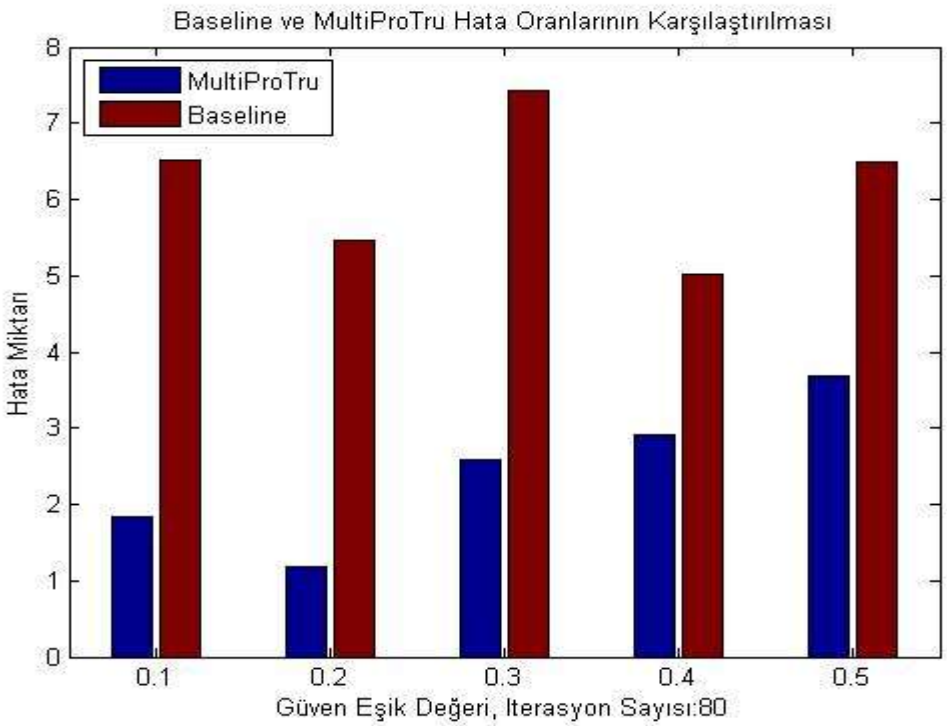
Şekil 7.21 Sıcaklık izleme algılayıcı ağındaki hata miktarı(iterasyon: 800)



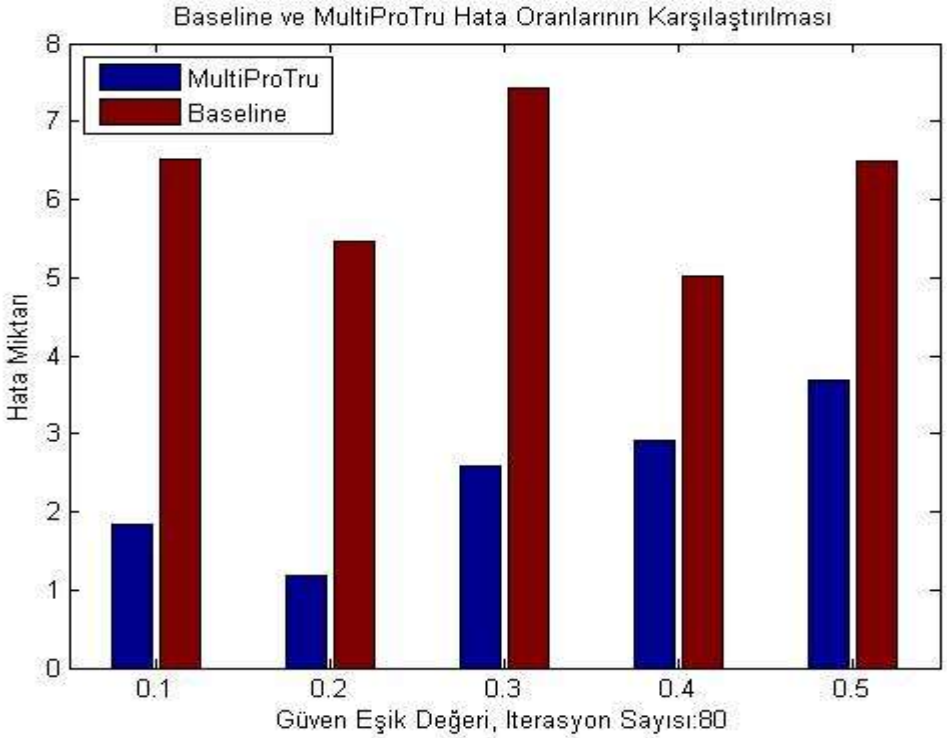
Şekil 7.22 Sıcaklık izleme algılayıcı ağındaki hata miktarı (iterasyon: 1000)

7.4.2 Eşik Güven Değerine Göre Hata Miktarlarının Karşılaştırılması

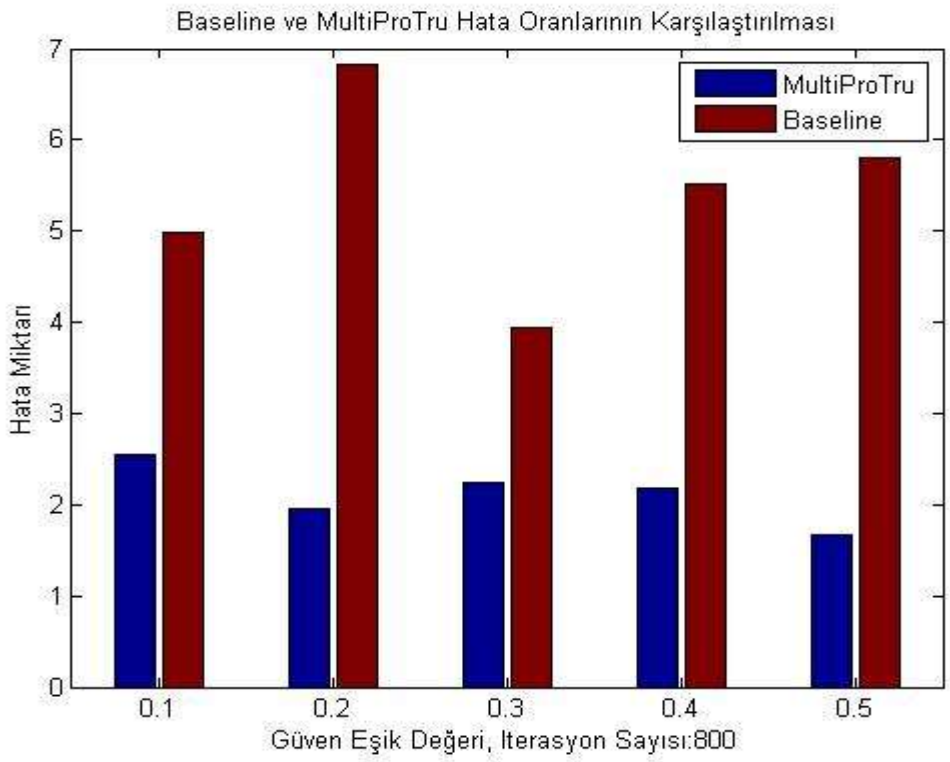
Bu bölümde ağın güven eşik değerine MultiProTru ve Baseline için hesapladığı ortalama hata miktarları verilmiştir. Deneyler 20, 80, 800 ve 1000 iterasyon değerleri için tekrarlanmıştır. Deney kapsamında ağın hata oranı 0.1, 0.2, 0.3, 0.4 ve 0.5 güven eşik değerleri değerleri için test edilmiştir. MultiProTru mimarisinde düğümün güven değeri eşik değerinin altında kaldığı zaman düğüm uyku durumuna geçirilmektedir. Bu sayede yanlış veri gönderen düğümün güven değeri eşik değerinin üstüne çıkmadan bu düğümden gelen verinin yanlış değeri ağa katılmayıp ağın ortalama hata miktarı minimize edilmeye çalışılmıştır. Şekil 7.23, Şekil 7.24, Şekil 7.25, ve Şekil 7.26'ya bakıldığı zaman iterasyon sayısı arttıkça hata miktarının azaldığı görülecektir çünkü belli bir iterasyona gelince zamanla güven değerleri düşüp, eşik güven değerine çarpıyor ve o noktadan sonra yanlış veri üreten algılayıcıların güven değeri eşik değerine çarptığı için ignore ediliyor ve hata miktarı daha az oluyor. Şekil 7.23, Şekil 7.24, Şekil 7.25, ve Şekil 7.26'ya bakıldığı zaman güven eşik değerinin düştükçe ağın hata tolerasyonu arttığı görülecektir. Bu yüzden ağda kullanılacak olan güven eşik değerinin dikkatli seçilmesi büyük önem arz etmektedir.



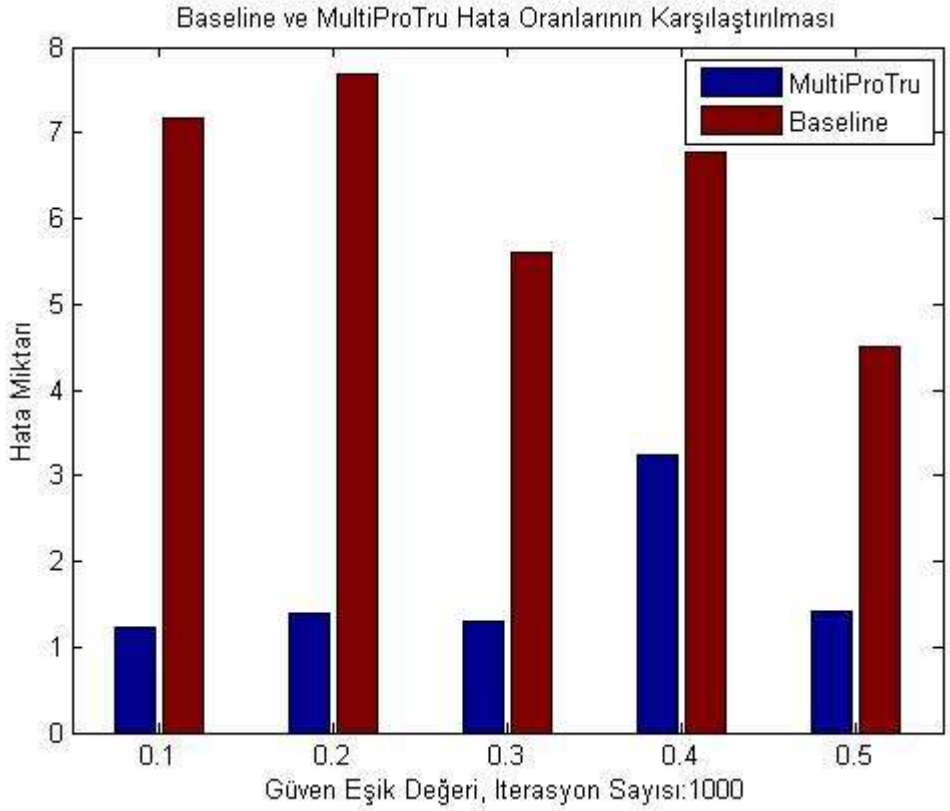
Şekil 7.23 Farklı güven eşikleri için hata miktarı(iterasyon: 20)



Şekil 7.24 Farklı güven eşikleri için hata miktarı (iterasyon: 80)



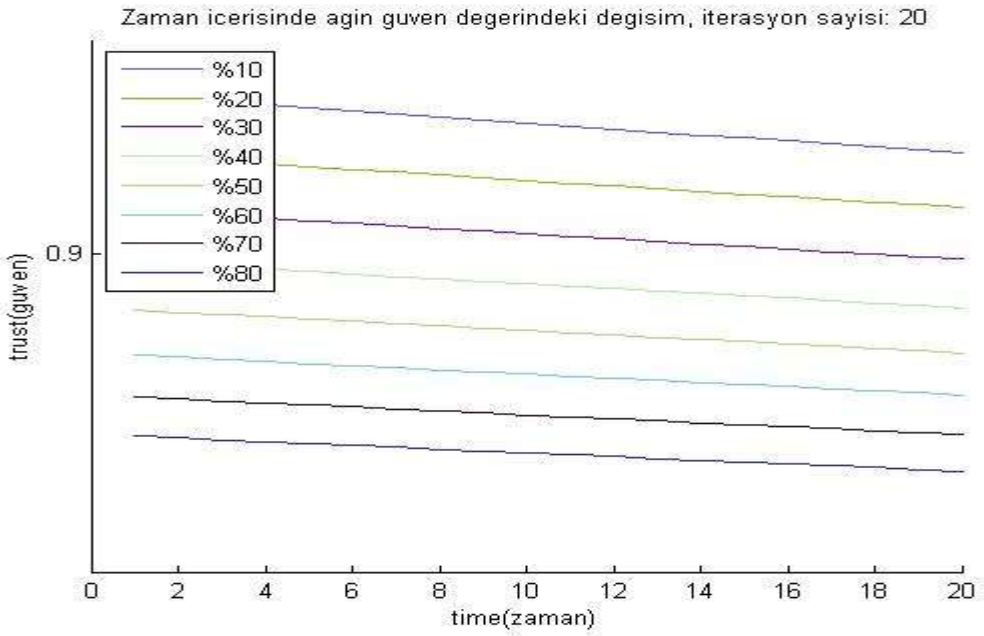
Şekil 7.25 Farklı güven eşikleri için hata miktarı (iterasyon: 800)



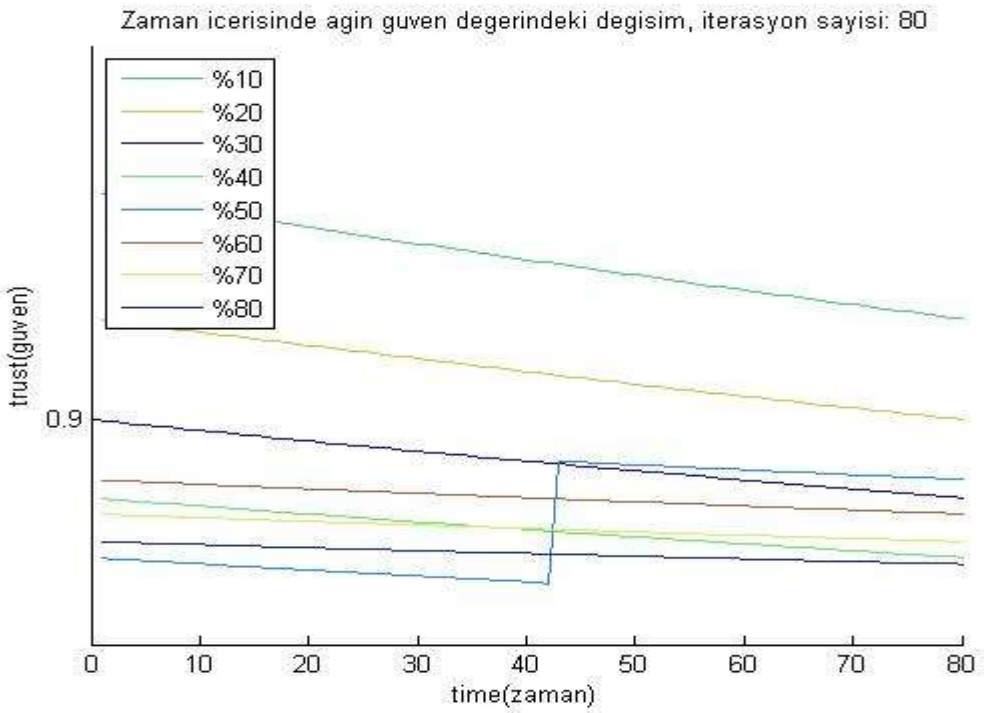
Şekil 7.26 Farklı güven eşikleri için hata miktarı (iterasyon: 1000)

7.4.3 Zamana Göre Ağın Güven Değerinde Meydana Gelen Değişim

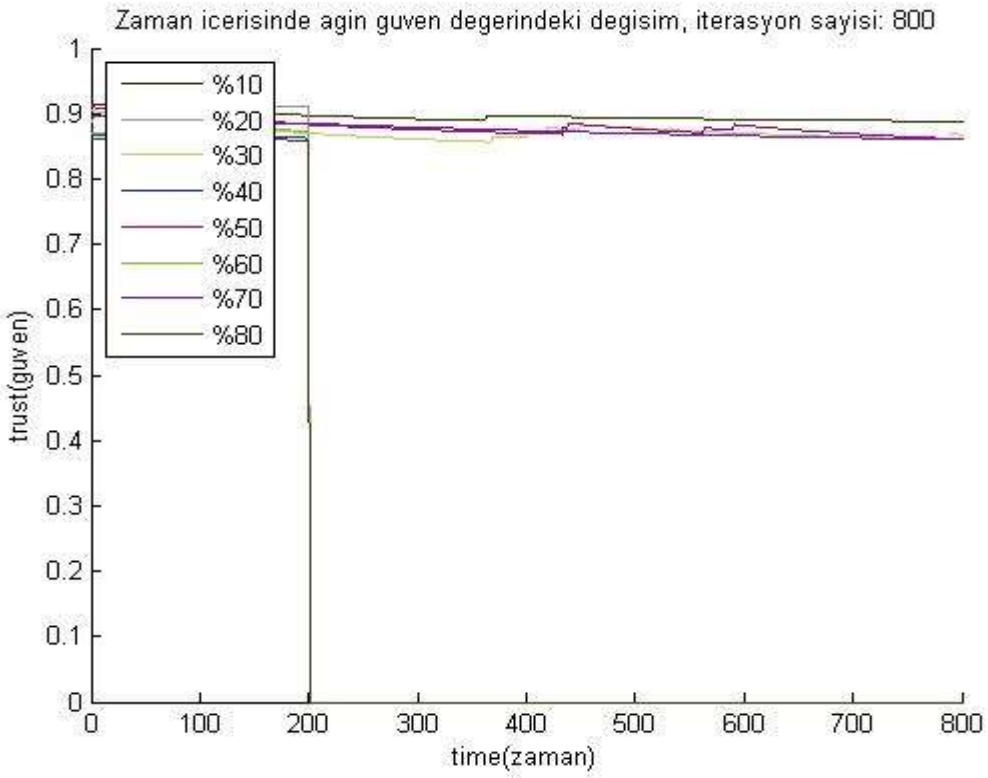
Bu bölümde hatalı algılayıcı yüzdesine göre MultiProTru'nun güven değerinde meydana gelen değişim izlenmiştir. MultiProTru mimarisi yanlış veri gönderen düğümün güven değerini düşürmekte doğru bilgi gönderen düğümün güven değerini artırmaktadır. MultiProTru mimarisine Kalman filtresi eklenerek ağın sadece o anki veri değerleri kullanılmayıp geçmiş davranışları da kullanılmaktadır. Bu sayede daha objektif bir güven değeri elde edilmeye çalışılmıştır. Kalman filtresi sayesinde yanlış bilgi gönderen düğümün güven değeri aşağı çekilmiş, doru bilgi gönderen düğümün güven değeri artırılmıştır. Düğümün güven değerinin eşik değerinin altında kalması durumunda düğüm uyku durumuna geçirilmiştir. Bu sayede ağ boyunca gönderilen verilerin doğruluk derecesi artırılmaya çalışılmıştır.



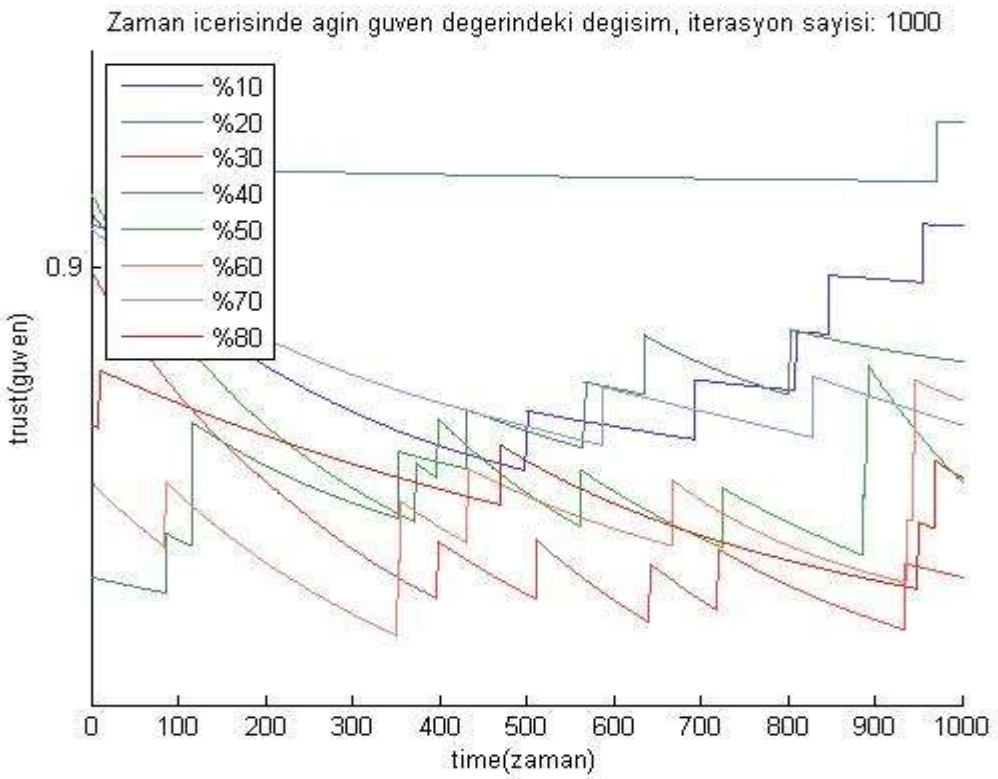
Şekil 7.27 Ağın güven değerindeki değişim (iterasyon: 20)



Şekil 7.28 Ağın güven değerindeki değişim (iterasyon: 80)



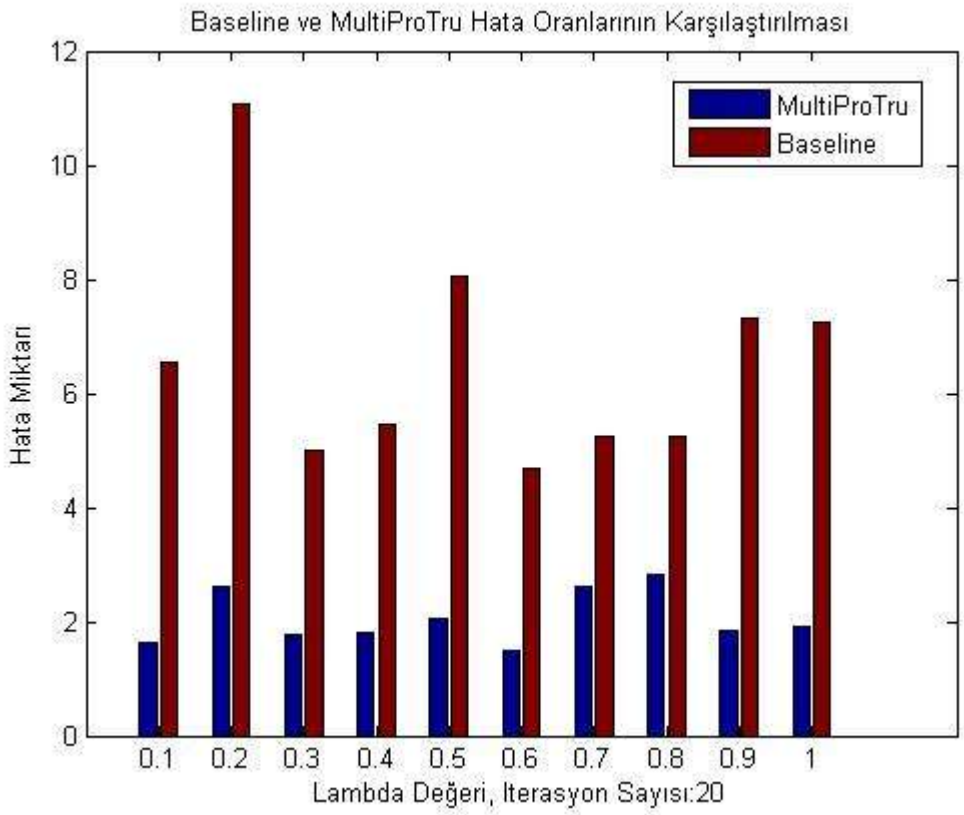
Şekil 7.29 Ağın güven değerindeki değişim (iterasyon: 800)



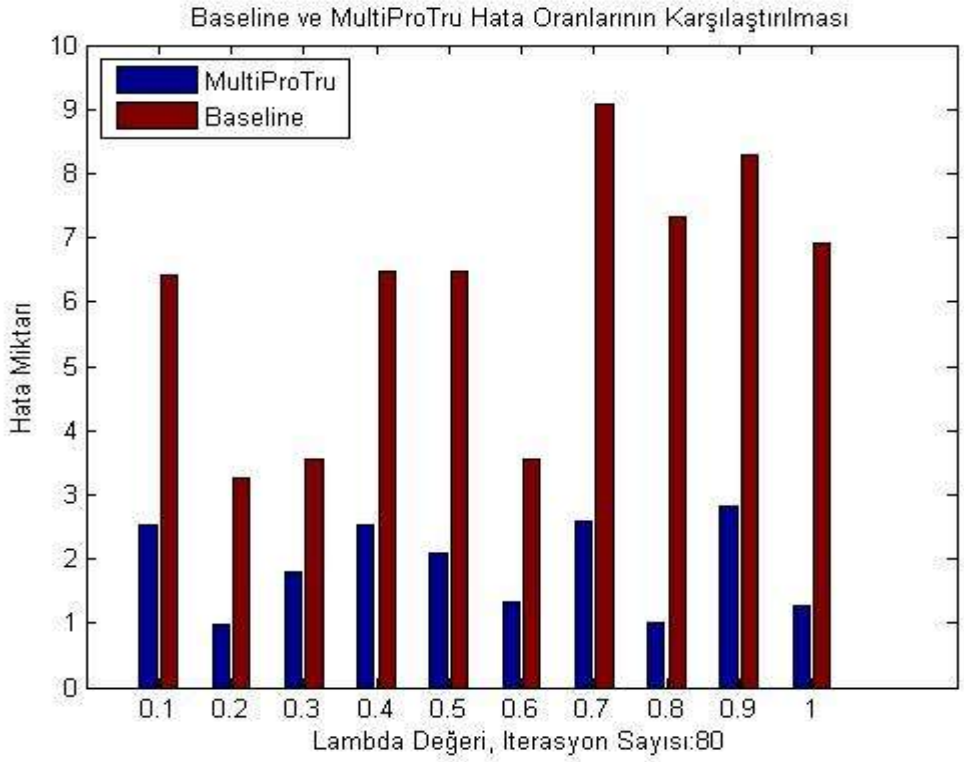
Şekil 7.30 Ağın güven değerindeki değişim (iterasyon: 1000)

7.4.4 Lambda Değerine Göre Hata Miktarlarının Karşılaştırılması

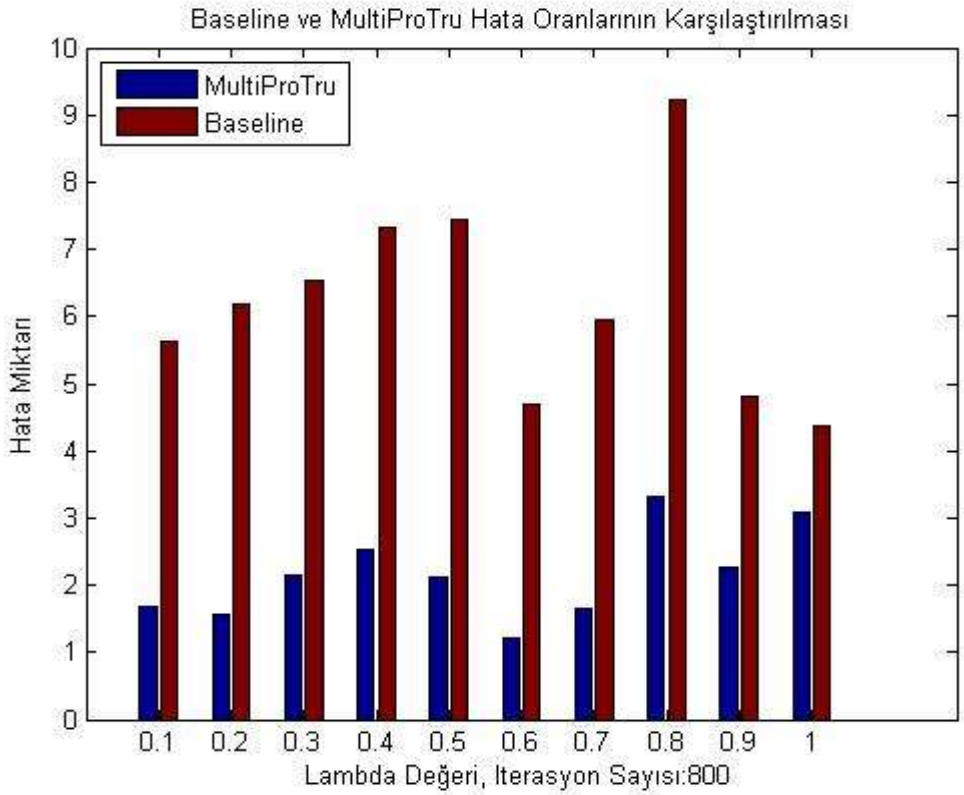
Bu bölümde formül (4.9)'da kullanılan lambda değerine MultiProTru ve Baseline'nın hata miktarları karşılaştırılmıştır. Lamda değeri 0 ile 1 arasındadır. Şekillerde de görüldüğü üzere genel olarak lambda değeri ve güven değeri arasında ters orantı mevcuttur. Şekillerde de görüleceği üzere Lamda değerine göre MultiProTru ve Baseline karşılaştırıldığında MultiProTru mimarisinin hata miktarının daha düşük ve dolayısıyla MultiProTru mimarisinin Baseline mimarisine göre daha başarılı olduğu görülecektir.



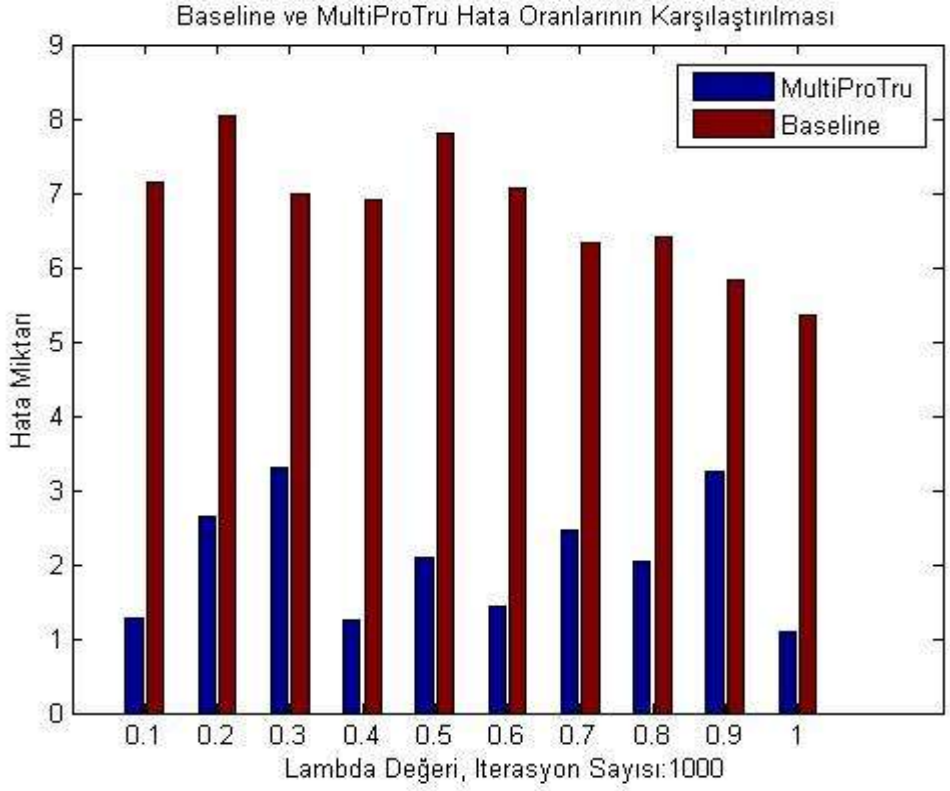
Şekil 7.31 Farklı lambda değerlerine göre hata miktarları (iterasyon: 20)



Şekil 7.32 Farklı lambda değerlerine göre hata miktarları (iterasyon: 80)



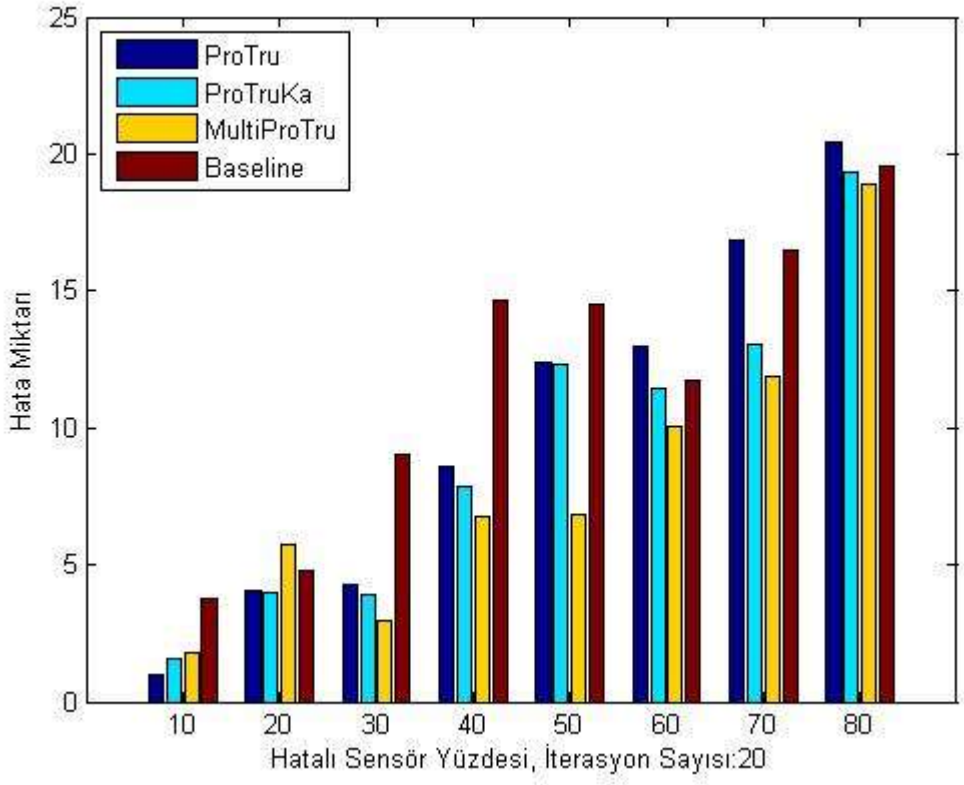
Şekil 7.33 Farklı lambda değerlerine göre hata miktarları (iterasyon: 800)



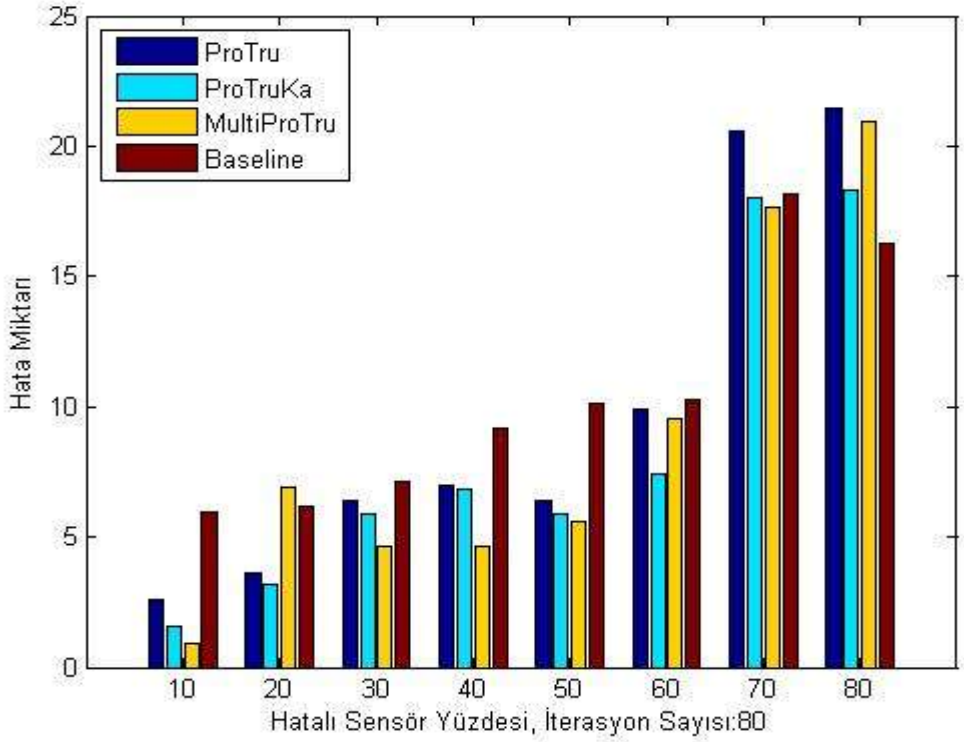
Şekil 7.34 Farklı lambda değerlerine göre hata miktarları (iterasyon: 1000)

7.5 Deney V

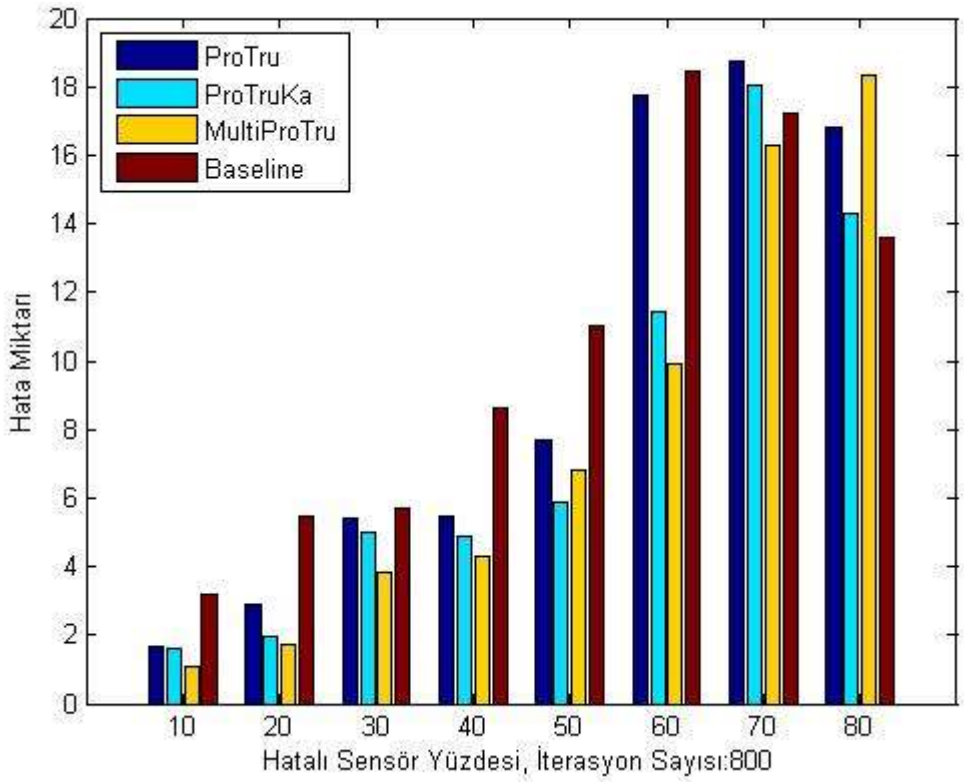
Bu deney kapsamında ProTru, ProTruKa, MultiProTru ve Baseline mimarilerinin algılayıcı hata miktarları karşılaştırılmıştır. Deney 20, 80, 800 ve 1000 iterasyon değerleri için tekrarlanmıştır. Grafiklere bakıldığı zaman ProTru mimarisine Kalman filtresi eklenerek tasarlanan ProTruKa mimarisinin ProTru mimarisine göre daha başarılı olduğu görülecektir. ProTru mimarisinin birden çok atlamalı bir şekilde tasarlanması ve güven analizine Kalman filtresi tekniğinin eklenmesiyle geliştirilen MultiproTru mimarisinin diğer 3 mimariye göre algılayıcı hata miktarının daha düşük olduğu ve dolayısıyla MultiProTru mimarisinin daha başarılı olduğu görülecektir. Genel olarak 4 mimaride de algılayıcı hata yüzdesinin artmasına paralel olarak algılayıcı hata miktarının da arttığı görülecektir. Bu dört mimari içerisinde güven değerlendirmesinde herhangi bir teknik kullanılmayan Baseline mimarisinin en başarısız mimari olduğu açıkça görülmektedir.



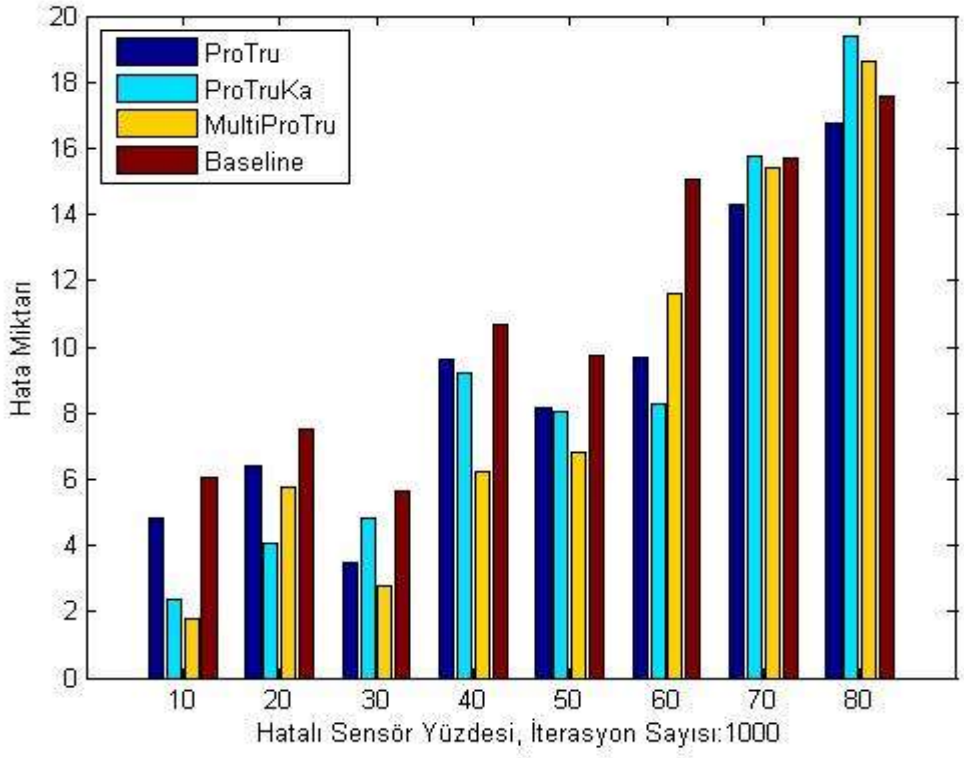
Şekil 7.35 Mimarilerin hata miktarlarının karşılaştırılması (iterasyon:20)



Şekil 7.36 Mimarilerin hata miktarlarının karşılaştırılması (iterasyon:80)



Şekil 7.37 Mimarilerin hata miktarlarının karşılaştırılması (iterasyon:800)

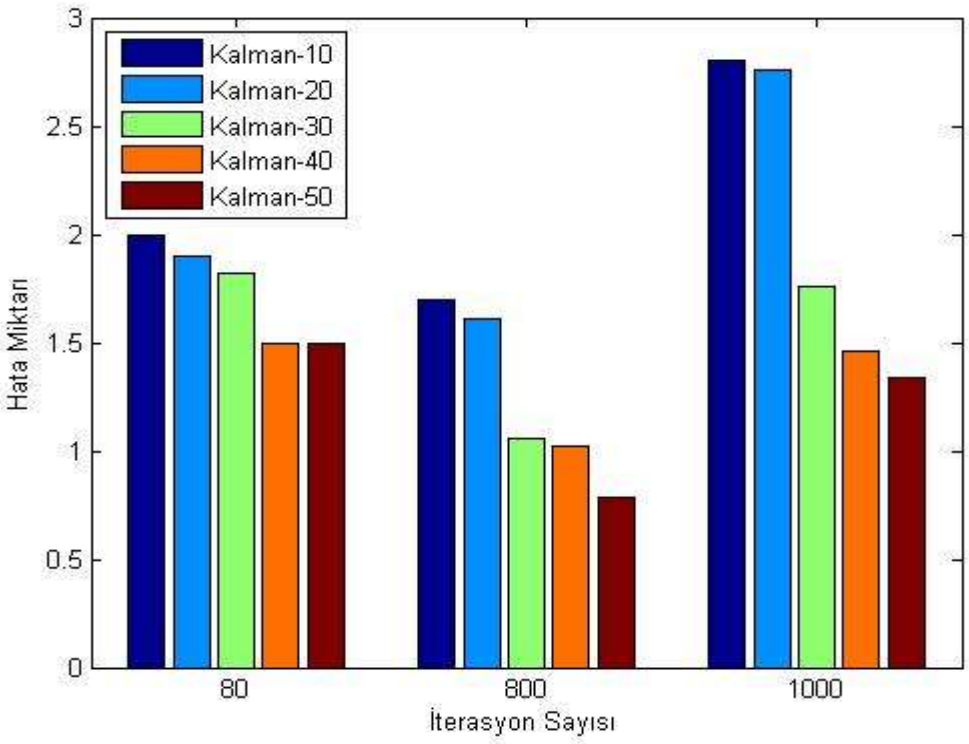


Şekil 7.38 Mimarilerin hata miktarlarının karşılaştırılması (iterasyon:1000)

7.6 Deney VI

Bu deney kapsamında MultiProTru mimarisine eklenen Kalman filtresiyle ilgili deneyler yapılmıştır. Kalman filtresi, ağın geçmiş davranışlarını göz önüne alarak düğümün bir sonraki güven değerini hesaplama yeteneğine sahiptir. Kablosuz algılama ağlarında depolama problemi olduğundan dolayı ağın tüm geçmiş davranışlarını depolamak olanaksızdır. Bu deneyle birlikte Kalman filtresinin kullanımı için ağın son 10, 20, 30, 40 ve 50 fark değerleri kullanılarak deneyler yapılmıştır. Deneyler sonucunda geçmiş ağ davranışlarının kullanımının artmasıyla beraber ağın hata miktarının giderek azaldığı ve daha rasyonel güven değerleri elde edildiği görülmüştür. Şekil 7.39' da da görüleceği üzere ağın son 10 fark değeri kullanıldığında hata miktarının yükseldiği gözlemlenmiş buna karşın ağın sırasıyla son 20, 30, 40, 50 fark değerleri kullanıldığı zaman ağın algılayıcı hata miktarının giderek düştüğü görülmüştür. Sonuç olarak Kalman filtresinin kullanacağı geçmiş veri sayısı arttığında performansının arttığı ve bu sayede daha güvenilir bir ağ mimarisinin elde edildiği görülmektedir.

Kablosuz algılama ağları sınırlı hesaplama, enerji ve depolama kapasitesine sahiptirler. Bu ağların ömrü enerji miktarıyla paralel olduğundan dolayı enerjinin kullanımı oldukça önemlidir. Kalman filtresinde tutulan fark değerlerini artması depolama ve hesaplama noktasında problem teşkil etmektedir. Bu yüzden Kalman filtresinde tutulan fark değer sayısı önemlidir. Simulasyonlar sonucunda elde edilen grafiklerde son 10 fark değerinin tutulması önerilmektedir.

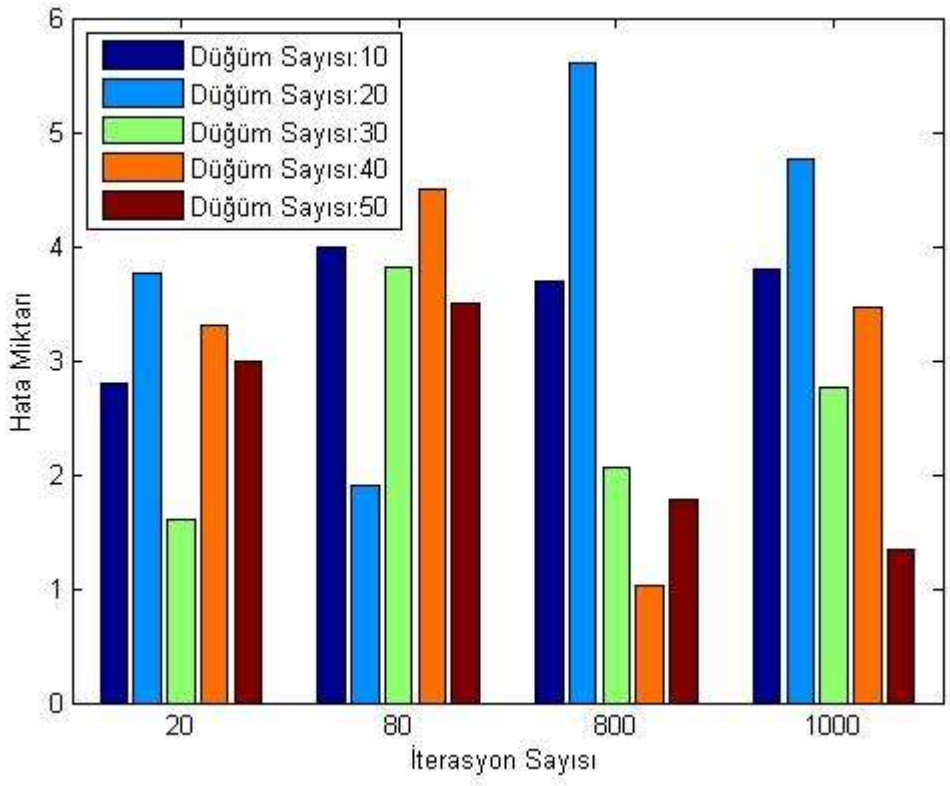


Şekil 7.39 Ağın geçmiş fark değerleri kullanılarak hata miktarlarının hesaplanması

7.7 Deney VII

Bu deney kapsamında bir baş düğüme veri gönderen yaprak düğüm sayısına göre ağın algılayıcı hata miktarında meydana gelen değişim izlenmiştir. Baş düğüme veri gönderen 10, 20, 30, 40 ve 50 yaprak düğüm sayısına göre ağın algılayıcı hata miktarında meydana gelen değişim Şekil 7.40' ta gösterilmiştir. Deneyde hatalı algılayıcı oranı %10 olarak varsayılmış ve 10 adet baş düğüm kullanılmıştır. Her baş düğüme bağlı yaprak sayısı 10, 20, 30, 40 ve 50 şeklinde güncellenip bir baş düğüme bağlı yaprak düğüm sayısında meydana gelişimin ağın hata miktarını değiştirip değiştirmediği gözlemlenmiştir. Bir baş düğüme bağlı düğüm sayısı 10 olduğunda ağda

100 adet yaprak düğüm, 20 olduğunda 200 adet yaprak düğüm, 30 olduğunda 300 adet yaprak düğüm, 40 olduğunda 400 adet yaprak düğüm, 50 olduğunda 500 adet yaprak düğüm yer almaktadır. Deney sonucunda baş düğüme veri gönderen düğüm sayısında meydana gelen değişim ile ağın hata miktarı arasında anlamlı bir ilişki kurulamamıştır.



Şekil 7.40 Baş düğüme bağlı yaprak düğüm sayısına göre hata miktarının izlenmesi

7.8 Deney VIII

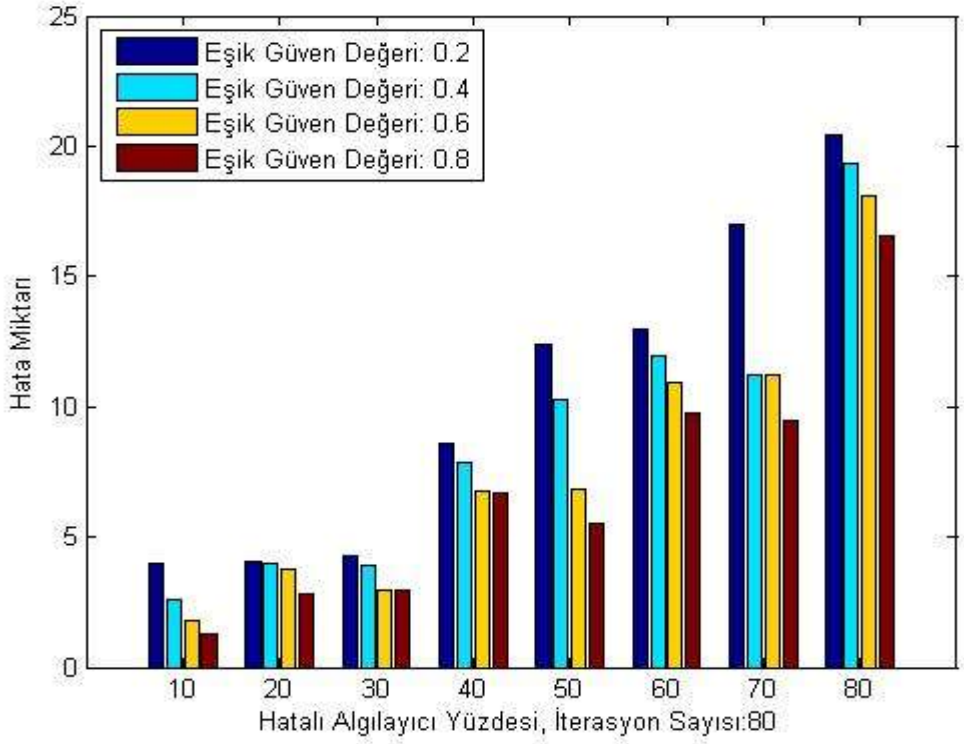
Bu deney kapsamına MultiProTru mimarisinin güven eşik değerinin dinamik bir şekilde yapılandırılmasıyla tasarlanan DynamicMultiProTru adındaki mimariyle ilgili deneyler yapılmıştır. Algılayıcı hata oranı arttığı zaman DynamicMultiProTru mimarisi güven eşik değerini yükselterek ağın ortalama hata miktarını düşürmüştür. Güven eşik değeri yükseldiği zaman hatalı veri gönderen düğümün eşik değeri altında kalma ihtimali artar. Böylece hatalı veri gönderen düğümlerin veri füzyonun noktasında kullanılmasının önüne geçilmiş olur. Bu sayede ağın ortalama hata miktarı optimize edilmiştir. Deney %10, %20, %10, %30, %40, %50, %60, %70, %80 hatalı algılayıcı oranları için 0.2, 0.4, 0.6 ve 0.8 güven eşik değerleri için test edilmiştir.

Güven eşik değerinin güncellenmesinde temel olarak şu iki problem meydana gelmektedir. Güven eşik değeri arttığında ağda güven eşik değerini aşacak düğüm sayısı azalmaktadır. Bu da bilgi alacağımız algılayıcı yüzdesini düşürmektedir. Diğer problem ise güven eşik değeri küçüldüğünde güven eşik değerini aşacak düğüm sayısı artmakta ve dolayısıyla algılayıcılardan toplanan verinin güven değeri düşmektedir.

Bu iki probleme çözüm olarak geliştirilen adaptive DynamicMultiProTru mimarisinde şu çözüm yolları düşünülmüştür.

- Ağdaki düğüm sayısının en az %80'i için veri füzyonu hedeflenmiştir. Buna bağlı olarak ağdaki düğüm sayısının %80' inden bilgi alacak şekilde aşağıdaki güven eşik değerleri belirlenmiştir.
- Ağdaki hatalı algılayıcı yüzdesine göre bir eşik değeri belirlenmiştir. Hatalı algılayıcı yüzdesi %10, %20, %30 ve %40 olduğunda güven eşik değeri 0.4 olarak, hatalı algılayıcı yüzdesi %50, %60, %70 olduğunda güven eşik değeri 0.6 olarak belirlenmiştir. Hatalı algılayıcı yüzdesinin %70' ten fazla olduğu durumlarda ise güven eşik değeri 0.8 olarak belirlenmiştir.

Şekil 7.41'e de bakıldığı zaman güven eşik değeri arttıkça ağın hata miktarı düşürülmüştür.



Şekil 7.41 Eşik güven değerine göre algılayıcı hata miktarının ölçülmesi

7.9 Deney IX

Bu deney kapsamında MultiProTru mimarisinde kullanılan güven modeliyle Effficient Distributed Trust Model (EDTM)'i [88] hata miktarına göre karşılaştırılmıştır. EDTM güven modelinin seçilmesinin nedeni MultiProTru mimarisi gibi dağıtık bir yapıya sahip olması ve veri benzerliğine dayalı bir algoritma yapısını kullanmasıdır. EDTM ' de verilerin normal dağılıma göre dağıldığı varsayılmaktadır. Ortalama değere sahip olan düğümün en yüksek güven değerine sahip olduğu varsayılmıştır. Bu güven modelinde bir veri öğesinin değeri ortalamaya yakın olduğunda bu veri öğesinin güven değeri de yüksek olur. Düğümlerin güven değerleri 0 ve 1 arasındadır. 1 değeri tamamen güvenilir 0 değeri ise tersi anlamına gelir. MultiProTru mimarisinde kullanılan güven modeliyle ETDM'in bir diğer ortak noktası ise eşik güven değerinin kullanılmasıdır.

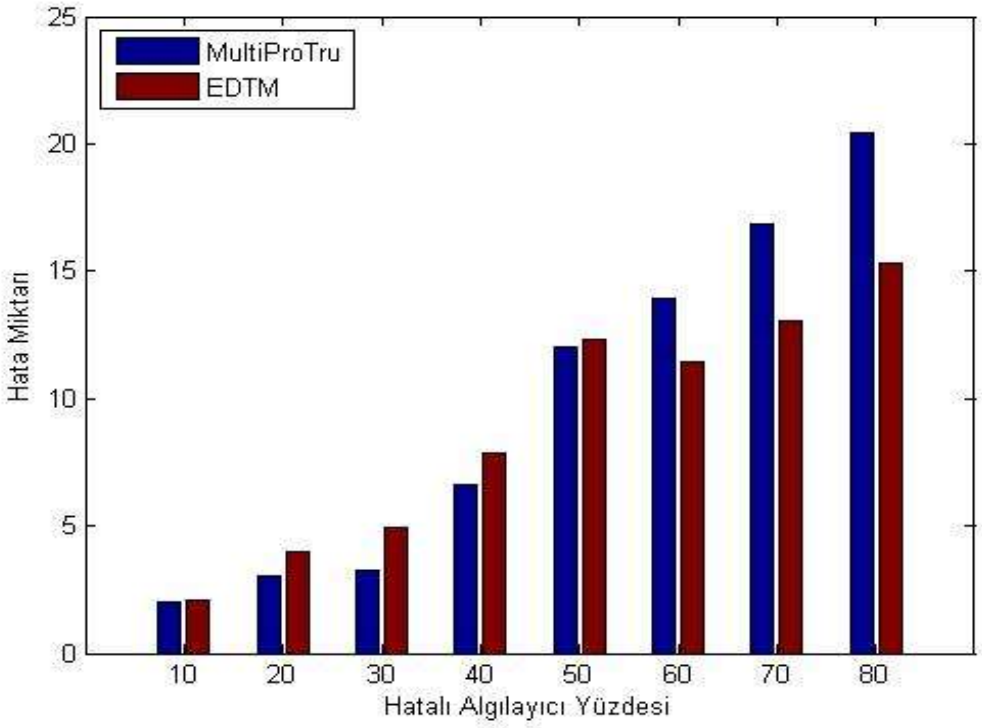
EDTM' de verilerin güven değerleri (7.2) numaralı formül kullanılarak hesaplanmıştır.

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-(x-\mu)^2}{2\sigma^2}} \tag{7.1}$$

$$T_{data} = 2(0.5 - \int_{\mu}^{v_d} f(x)dx) \quad (7.2)$$

- $f(x)$ olasılık yoğunluk fonksiyonu
- μ verilerin ortalaması
- σ varyans değeri
- T_{data} düğümün güven değeri
- v_d algılayıcının ölçtüğü değer
- x v_d veri öğesinin özniteliği

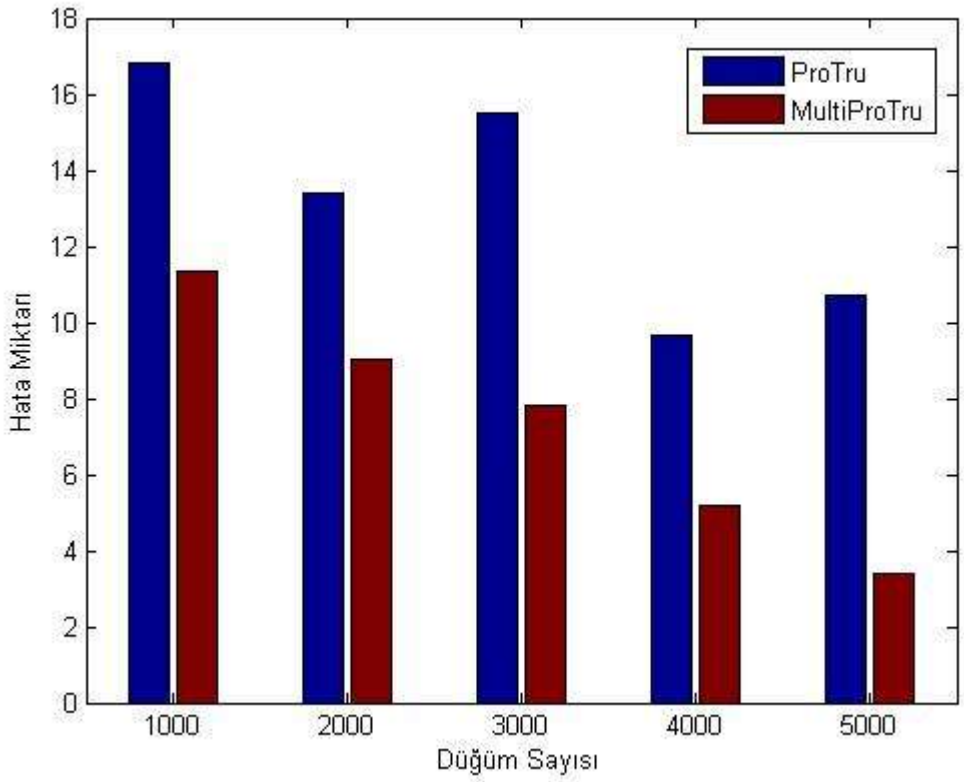
Şekil 7.42' ye bakıldığı zaman hatalı algılayıcı yüzdelerinin 10, 20, 30, 40 ve 50 olduğu durumlarda MultiProTru mimarisinin hata miktarının daha az ve dolayısıyla EDTM' e göre daha başarılı olduğu görülecektir. Algılayıcı hata yüzdelerinin 60, 70 ve 80 olduğu durumlarda EDTM MultiProTru' ya daha başarılıdır. MultiProTru mimarisinin algılayıcı hata yüzdelerinin çok olduğu yerlerde başarısız olmasının sebebi bu mimarinin algılayıcılar tarafından ölçülen değerler içersinde çoğunluğa göre hareket etmesidir.



Şekil 7.42 EDTM ve multiprotru güven modellerinin karşılaştırılması

7.10 Deney X

Bu deney kapsamında ağın büyüklüğünde meydana değişime göre ProTru ve MultiProTru Mimarileri karşılaştırılmıştır. Ağdaki düğüm sayısının 1000, 2000, 3000, 4000 ve 5000 olduğu değerler için simülasyonlar tekrarlanmıştır. Ağdaki hatalı algılayıcı yüzdesi %10 ve güven eşik değeri 0. 4 olarak belirlenmiştir. Şekik 7.43' te görüleceği üzere ağdaki düğüm sayısının arrtığı durumlarda MultiProTru mimarisindeki hata miktarının giderek azaldığı görülecektir. Bunun temele nedeni ise MultiProTru mimarisinin birden çok atlamalı bir şekilde tasarlanması ve güven değeririnin hesaplanılmasında Kalman filtresinin kullanılmasıdır. 1000, 2000, 3000, 4000 ve 5000 düğüm sayıları için MultiProTru mimarisi ProTru mimarisine göre daha başarıldır.



Şekil 7.43 Ağdaki düğüm sayısına göre hata miktarlarının karşılaştırılması

BÖLÜM 8

SONUÇ VE ÖNERİLER

Kablosuz algılama ağları esnek bir yapıya sahip olmaları, maliyetlerinin düşük olması ve her türlü çevresel ortama göre tasarlanabilmeleri gibi özelliklerinden dolayı kullanımları giderek artmıştır. Kullanım noktasındaki artışla beraber bu ağlarda karşılaşılan sorunlar da giderek ilgi görmeye başlamıştır. Bu problemlerin en temel olanları enerji ve güvenlik problemleridir. Bu ağlarda, ağın ömrü düğümlerin sahip olduğu enerji miktarıyla doğrudan ilişkili olduğundan dolayı düğümlerin enerji kullanımı oldukça önemli bir yere sahiptir. Bundan dolayı kablosuz algılama ağlarında verimli enerji tüketim modellerinin geliştirilmesine olan ihtiyaç giderek artmıştır. Bununla beraber algılayıcıların ölçtüğü değerlerin doğru olması ve dışarıdan gelebilecek ağ saldırılarına karşı kendini koruyabilmeleri de hayati bir önem taşımaktadır. Kablosuz algılama ağlarının sınırlı hesaplama yetenekleri ve kısıtlı enerjiye sahip olmalarından dolayı bu sistemlerde paralel olarak hem güvenliği sağlamak hem de enerji optimizasyonunu gerçekleştirmek oldukça güçtür.

Bu tez kapsamında kablosuz algılama ağlarında karşılaşılan enerji ve güvenlik problemlerine çözüm bulmak adına daha önce geliştirilen tek yönlü ProTru[29] mimarisi geliştirilerek birden çok atlamalı bir yapıya sahip olan MultiProTru mimarisi geliştirilmiştir. MultiProTru mimarisinde ağın güvenliğini sağlamak için daha önce kablosuz algılama ağlarının güvenliğini sağlama noktasında hiçbir çalışmada kullanılmayan istatistiki bir yöntem olan Kalman filtresi kullanılmıştır. Kalman filtresi düğümlerin geçmiş değerlerini kullanarak düğüm o anki güven değerini hesaplamaya çalışmıştır. Bu sayede düğümün sadece anlık davranışını baz alarak bir güven değeri

hesaplamak yerine ağın geçmiş davranışları da kullanılarak bir güven değeri hesaplanmıştır.

Bununla birlikte geliştirilmiş olan MultiProTru mimarisinin enerji verimliliği ölçülmüştür. Zaman ve bellek karmaşıklığı az olan Kalman filtresi yöntemi sayesinde hem ağın güvenliği sağlanmış hem de kısıtlı enerjiye sahip kablosuz algılama ağlarının ömrü uzatılmaya çalışılmıştır.

Güven değerlerinin hesaplanmasında veri benzerliğine dayalı yöntemlerin [128] kullanıldığı durumlarda şu sorunlarla karşılaşılmaktadır. Binlerce yaprak düğümün dağıtıldığı bir alanda sürekli doğru bilgi gönderen bir yaprak düğümün hâkim olduğu alanda ani bir değişiklik meydana gelebilir. Bu değişiklik, yaprak düğümün göndereceği değeri büyük miktarda aşağı veya yukarı bir değere çekebilmektedir. Yaprak düğümden bağımsız olarak gelişen bu durum itibariyle yaprak düğümün bağlı olduğu baş düğüm, kendisine bağlı diğer yaprak düğümlerin gönderdiği değerlere bakarak bu yaprak düğümün güven değerini büyük miktarda düşürebilmekte ve doğru bilgi gönderen bu düğümü uyku durumuna geçirebilmektedir. Bu problemi çözmek adına güven değerinin hesaplanmasında Kalman filtrelemesi kullanılmış ve daha rasyonel bir güven değeri hesaplanmaya çalışılmıştır. Kalman filtresi, gerçek fark değerlerini filtreleyerek daha ideal bir fark değeri elde etmiştir. Kalman filtresiyle yaprak düğümlerin geçmişte gönderdiği veriler ve güven değerleri kullanılarak bu ani güven değerinin düşüşünün önüne geçilmeye çalışılmıştır. Veri benzerliğine dayalı yöntemlerle karşılaştırıldığı zaman bu mimaride Kalman filtreleme yönteminin kullanılması, bu problemi çözmek adına avantaj sağlamaktadır. Ayrıca yaprak düğümlerin, veri gönderdikten hemen sonra güven değerlerinin hesaplanması ve güven değerinin sürekli güncel tutulması ise mimarimizin bir diğer özgün yönüdür.

Şekil 7.35, 7.36, 7.37 ve 7.38' e bakıldığı zaman ProTru mimarisine Kalman filtresi eklenerek geliştirlen ProTruKa mimarisinin ProTru mimarisine göre %20 daha başarılı olduğu görülecektir. Bunun en temel sebebi ise ProTruKa mimarisine eklenen Kalman filtresinin ağın sadece anlık durumunu değil geçmiş davranışlarını da göz önüne alarak bir güven değeri hesaplamasıdır.

ProTru mimarisine Kalman filtresi eklenip mimarinin birden çok atlamalı bir şekilde tasarlanmasıyla elde edilen MultiProTru mimarisi ProTru mimarisine göre %45 daha başarılıdır.

MultiProTru mimarisinin ağ genişliğinin büyük olduğu kablosuz algılama ağlarında ProTru mimarisine göre Deney X' te de görüleceği üzere daha başarılı olduğu görülecektir. Bunun temel nedeni ise birden çok atlamalı bir yapıya sahip olması ve güven değerlendirmesinde Kalman filtresinin kullanılmasıdır. Deney X' te elde edilen sonuçlara göre 1000, 2000, 3000, 4000 ve 5000 düğüm sayılarına göre ortalama olarak MultiProTru mimarisinin ProTru mimarisine göre %55 daha başarılıdır.

Deney VI' te de görüleceği üzere Kalman filtresinde tutulan fark değerleri arttıkça daha doğru bir güven değeri elde edilmiş ve bu sayede ağın hata miktarı giderek düşmüştür.

Sonuç olarak kablosuz algılama ağlarında enerji optimizasyonu ve güvenliği paralel olarak sağlayan yeni enerji ve güvenlik modellerinin geliştirilmesi gerektiği kanaatine varılmıştır.

KAYNAKLAR

[1] Yick, J. Mukherjee, B. ve Ghosal, D., (2008). "Wireless Sensor Network Survey", Computer Networks, 52: 2292-2330.

[2] Simon, G. Maróti, M. Lédeczi, Á. Balogh, G. Kusy, B. Nádas, A. Pap, G. Sallai, J. ve Frampton, K., (2004). "Sensor Network-Based Countersniper System", In Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, 3-5 November 2004, Baltimore.

[3] Yick, J. Mukherjee, B. ve Ghosal, D., (2005). "Analysis of a Prediction-Based Mobility Adaptive Tracking Algorithm", 2nd International Conference on Broadband Networks, 03 Oct - 07 Oct 2005, Boston.

[4] Castillo-Effer, M. Quintela, D.H. Moreno, W. Jordan, R. ve Westhoff, W., (2004). "Wireless Sensor Networks for Flash-Flood Alerting", Proceedings of the 5th IEEE International Caracas Conference , 1: 142-146.

[5] Gao, T. Greenspan, D. Welsh, M. Juang, R. ve Alm, A., (2006). "Vital Signs Monitoring and Patient Tracking Over a Wireless Network", 27th Annual International Conference of the IEEE, 1-4 September 2006, China.

[6] Lorincz, K. Malan, D.J. Fulford-Jones, T.R. Nawoj, A. Clavel, A. Shnayder, V. Mainland, G. Welsh, M. ve Moulton, S., (2004). "Sensor Networks for Emergency Response: Challenges and Opportunities", Pervasive Computing IEEE, 3: 16-23.

[7] Werner-Allen, G. Lorincz, K. Ruiz, M. Marcillo, O. Johnson, J. Lees, J. ve Welsh, M., (2006). "Deploying a Wireless Sensor Network on an Active Volcano", Internet Computing IEEE, 10: 18-25.

[8] Raghunathan, V. Kansal, A. Hsu, J. Friedman, J. ve Srivastava, M., (2005). "Design Considerations for Solar Energy Harvesting Wireless Embedded Systems", In Proceedings of the 4th International Symposium on Information Processing in Sensor Networks, April 25-27 ,USA.

[9] Zhang, P. Sadler, C.M. Lyon, S.A. ve Martonosi, M., (2004). "Hardware Design Experiences in ZebraNet", Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems , 3-5 November 2004, Baltimore.

[10] Roundy, S. Wright, P.K. ve Rabaey, J.M., (2003). "Energy Scavenging for Wireless Sensor Networks", Norwell.

[11] Rahimi, M. Shah, H. Sukhatme, G. Heideman, J. ve Estrin, D., (2003). "Studying the Feasibility of Energy Harvesting in a Mobile Sensor Network", Proceedings of the 2003 IEEE International Conference on Robotics and Automation, 14-19 September 2003, Taiwan.

[12] Kansal, A. ve Srivastava, M.B., (2003). "An environmental Energy Harvesting Framework for Sensor Networks", The International Symposium on Low Power Electronics and Design,25-27 August 2003, Seoul, Korea.

[13] Akyildiz, I.F. Su, W. Sankarasubramaniam, Y. ve Cayirci, E., (2002). "Wireless Sensor Networks: a Survey", Computer Networks, 38: 393-422.

[14] Toumpis, S. ve Tassiulas, L., (2006). "Optimal Deployment of Large Wireless Sensor Networks", Information Theory, IEEE Transactions on, 52: 2935-2953.

[15] Yick, J. Pasternack, G. Mukherjee, B. ve Ghosal, D., (2006). "Placement of Network Services in a Sensor Network", International Journal of Wireless and Mobile Computing, 1: 101-112.

[16] Pompili, D. Melodia, T. ve Akyildiz, I.F., (2006). "Deployment Analysis in Underwater Acoustic Wireless Sensor Networks", Proceedings of the 1st ACM International Workshop on Underwater Networks, 25-29 September 2006, Los Angeles, CA, USA.

[17] Akyildiz, I.F. ve Stuntebeck, E.P., (2006). "Wireless Underground Sensor Networks: Research Challenges", Ad Hoc Networks, 4: 669-686.

[18] Li, M. ve Liu, Y., (2007). "Underground Structure Monitoring with Wireless Sensor Networks", Proceedings of the 6th International Conference on Information Processing in Sensor Networks, 25-27 April, Cambridge, USA.

[19] Akyildiz, I.F. Pompili, D. ve Melodia, T., (2004). "Challenges for Efficient Communication in Underwater Acoustic Sensor Networks", ACM Sigbed Review, 1: 3-8.

[20] Heidemann, J. Li, Y. Syed, A. Wills, J. ve Ye, W., (2005). "Underwater Sensor Networking: Research Challenges and Potential Applications", Proceedings of the Technical Report ISI-TR-2005-603, USC/Information Sciences Institute.

[21] Tolle, G. Polastre, J. Szewczyk, R. Culler, D. Turner, N. Tu, K. Burgess, S. Dawson, T. Buonadonna, P. ve Gay, D., (2005). "A Macroscope in The Redwoods", Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems, 2-4 November 2005, San Diego, USA.

[22] Vasilescu, I. Kotay, K. Rus, D. Dunbabin, M. ve Corke, P., (2005). "Data Collection, Storage, and Retrieval with an Underwater Sensor Network", Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems, 2-4 November 2005, San Diego, USA.

[23] Yap, K.-K. Srinivasan, V. ve Motani, M., (2005). "MAX: Human-Centric Search of the Physical World", Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems, 2-4 November 2005, San Diego, USA.

[24] Huang, J.-H. Amjad, S. ve Mishra, S., (2005). "Cenwits: a Sensor-Based Loosely Coupled Search and Rescue System Using Witnesses", Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems, 2-4 November 2005, San Diego, USA.

[25] Rahimi, M. Baer, R. Iroezi, O.I. Garcia, J.C. Warrior, J. Estrin, D. ve Srivastava, M., (2005). "Cyclops: in Situ Image Sensing and Interpretation in Wireless Sensor Networks", Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems, 2-4 November 2005, San Diego, USA.

[26] Johnstone, I. Nicholson, J. Shehzad, B. ve Slipp, J., (2007). "Experiences from a Wireless Sensor Network Deployment in a Petroleum Environment", International Wireless Communications and Mobile Computing Conference, 12-16 August 2007, Hawaii.

[27] Baker, C.R. Armijo, K. Belka, S. Benhabib, M. Bhargava, V. Burkhart, N. Der Minassians, A. Dervisoglu, G. Gutnik, L. ve Haick, M.B., (2007). "Wireless Sensor Networks for Home Health Care", Advanced Information Networking and Applications Workshops, 21-23 May 2007, Canada.

[28] Momani, M. ve Challa, S., (2010). "Survey of Trust Models in Different Network Domains", arXiv Preprint arXiv:1010.0168.

[29] Dogan, G., (2013). Protru: Leveraging Provenance to Enhance Network Trust in a Wireless Sensor Network, Doktora Tezi, City University of New York, New York,USA.

[30] Ganeriwal, S. Balzano, L.K. ve Srivastava, M.B., (2008). "Reputation-Based Framework for High Integrity Sensor Networks", ACM Transactions on Sensor Networks (TOSN), 4: 15.

[31] Yao, Z. Kim, D. Lee, I. Kim, K. ve Jang, J., (2005). "A Security Framework with Trust Management for Sensor Networks", Workshop of the 1st Intl Conference on Security and Privacy for Emerging Areas in Communication Networks, 5-9 September 2005, Athens, Greece.

[32] Fernandez-Gago, M.C. Roman, R. ve Lopez, J., (2007). "A Survey on the Applicability of Trust Management Systems for Wireless Sensor Networks", Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 19 July 2007, Istanbul,Turkey.

[33] Jøsang, A. ve Presti, S.L., (2004). "Analysing the Relationship between Risk and Trust", ed. Trust Management. Springer, 135-145.

[34] Gambetta, D., (2000). "Can We Trust Trust", Trust: Making and Breaking Cooperative Relations, 2000: 213-237.

[35] Solhaug, B. Elgesem, D. ve Stølen, K., (2007). "Why Trust is not Proportional to Risk", The Second International Conference on Availability, Reliability and Security, 10-13 April, Vienna.

[36] Cho, J.-H. Swami, A. ve Chen, R., (2011). "A Survey on Trust Management for Mobile Ad Hoc Networks", Communications Surveys & Tutorials, IEEE, 13: 562-583.

[37] Abdul-Rahman, A. ve Hailes, S., (1997). "Using Recommendations for Managing Trust in Distributed Systems", Proceedings of IEEE International Conference on Communication, 12 June 1997, USA.

[38] Bhargava, B. Lilien, L. Rosenthal, A. Winslett, M. Sloman, M. Dillon, T. Chang, E. Hussain, F. Nejdl, W. ve Olmedilla, D., (2004). "The Pudding of Trust [Intelligent Systems]", Intelligent Systems, IEEE, 19: 74-88.

[39] Scott, J., (2012). "Social Network Analysis", Third Edition, Sage, Washington .

[40] Ries, S. Kangasharju, J. ve Mühlhäuser, M., (2006). "A Classification of Trust Systems", On the Move to Meaningful Internet Systems, 20 December 2006, France.

[41] Resnick, P. ve Zeckhauser, R., (2002). "Trust Among Strangers in Internet Transactions: Empirical Analysis of Ebay's Reputation System", The Economics of the Internet and E-commerce, 11: 23-25.

[42] Blaze, M. Feigenbaum, J. ve Keromytis, A.D., (1999). "KeyNote: Trust Management for Public-Key Infrastructures", Security Protocols Springer Berlin Heidelberg, 59-63 .

[43] Blaze, M. Feigenbaum, J. ve Lacy, J., (1996). "Decentralized Trust Management", Proceedings 1996 IEEE Symposium on Security and Privacy, 6-8 May 1996, California, USA.

[44] Abdul-Rahman, A. ve Hailes, S., (2000). "Supporting Trust in Virtual Communities", Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 4-7 January 2000, Hawaii.

[45] Jsang, A. ve Ismail, R., (2002). "The Beta Reputation System", 15th Bled Electronic Commerce Conference, 17-19 June 2002, Slovenia.

[46] Xiong, L. ve Liu, L., (2003). "A Reputation-Based Trust Model for Peer-to-Peer e-Commerce Communities", Proceedings IEEE International Conference on E-Commerce, 24-27 June 2003, Newport Beach, CA, USA.

[47] Wang, Y. ve Vassileva, J., (2003). "Bayesian Network-Based Trust Model":, The 2004 IEEE/WIC/ACM International Confernce on Web Intelligence, 13-16 October 2003, Canada.

[48] Aberer, K. ve Despotovic, Z., (2001). "Managing trust in a Peer-2-Peer Information System", Proceedings of the Tenth International Conference on Information and Knowledge Management, 6-11 November 2001, McLean, VA, USA.

[49] Cahill, V., (2003). "Using Trust for Secure Collaboration in Uncertain Environments", Pervasive Computing IEEE, 2:52-61 .

[50] Kinateder, M. Baschny, E. ve Rothermel, K., (2005). "Towards a Generic Trust Model–Comparison of Various Trust Update Algorithms", Trust Management Springer, 177-192.

[51] Kotsovinos, E. ve Williams, A., (2006). "BambooTrust: Practical Scalable Trust Management for Global Public Computing", The 21st Annual ACM Symposium on Applied Computing, 23-27 April 2006, France.

[52] Quercia, D. Hailes, S. ve Capra, L., (2006). B-trust: Bayesian Trust Framework for Pervasive Computing, Trust Management Springer, 298-312.

[53] Zhou, D., (2003). "Security Issues in Ad Hoc Networks", CRC Press, Inc.

[54] Buchegger, S. ve Le Boudec, J.-Y., (2002). "Performance Analysis of the CONFIDANT Protocol", Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing, 9-11 June 2002, Lausanne, Switzerland.

[55] Michiardi, P. ve Molva, R., (2002). Core: a Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks, Advanced Communications and Multimedia Security Springer, 107-121.

[56] Aivaloglou, E. Gritzalis, S. ve Skianis, C., (2008). "Trust Establishment in Sensor Networks: Behaviour-Based, Certificate-Based and a Combinational Approach", International Journal of System of Systems Engineering, 1: 128-148.

[57] Wang, Y. Attebury, G. ve Ramamurthy, B., (2006). "A Survey of Security Issues in Wireless Sensor Networks", Communications Surveys & Tutorials, IEEE, 8:2-23.

[58] Papadimitratos, P. ve Haas, Z.J., (2002). "Securing Mobile Ad Hoc Networks", Handbook of Ad Hoc Wireless Networks, 665-671.

[59] Walters, J.P. Liang, Z. Shi, W. ve Chaudhary, V., (2007). "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid, Mobile, and Pervasive Computing, 1: 367.

[60] Newsome, J. Shi, E. Song, D. ve Perrig, A., (2004). "The Sybil Attack in Sensor Networks: Analysis & Defenses", Proceedings of The 3rd International Symposium on Information Processing in Sensor Networks, 26-27 April 2004, Berkeley, CA, USA.

[61] Zia, T. ve Zomaya, A., (2006). "Security Issues in Wireless Sensor Networks", International Conference on Systems and Networks Communication, 29 0ctober-3 November, Tahiti, French Polynesia .

[62] Perrig, A. Stankovic, J. ve Wagner, D., (2004). "Security in Wireless Sensor Networks", Communications of the ACM, 47: 53-57.

[63] McKnight, D.H. ve Chervany, N.L., (1996). "The Meanings of Trust",First Edition, Minneapolis.

[64] Rothstein, B., (2000). "Trust, Social Dilemmas and Collective Memories", Journal of Theoretical Politics, 12: 477-501.

[65] Deelmann, T. ve Loos, P., (2002). "Trust Economy: Aspects of Reputation and Trust Building for SMEs in e-Business", AMCIS 2002 Proceedings: 302.

[66] Pirzada, A.A. ve McDonald, C., (2004). "Establishing Trust in Pure Ad-Hoc Networks", Proceedings of the 27th Australasian Conference on Computer Science, 26:47-54.

[67] Lopez, J. Roman, R. Agudo, I. ve Fernandez-Gago, C., (2010). "Trust Management Systems for Wireless Sensor Networks: Best Practices", Computer Communications, 33: 1086-1093.

[68] Jøsang, A. Gray, E. ve Kinateder, M., (2006). "Simplification and Analysis of Transitive Trust Networks", Web Intelligence and Agent Systems, 4: 139-161.

[69] Jøsang, A. Ismail, R. ve Boyd, C., (2007). "A Survey of Trust and Reputation Systems for Online Service Provision", Decision Support Systems, 43: 618-644.

[70] Srinivasan, A. Teitelbaum, J. ve Wu, J., (2006). "DRBTS: Distributed Reputation-Based Beacon Trust System", 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, 29 September-1 October 2006, Indianapolis, USA.

[71] Dai, C. Lin, D. Bertino, E. ve Kantarcioglu, M., (2008). "Trust Evaluation of Data Provenance", Computer.

[72] Lim, H.-S. Moon, Y.-S. ve Bertino, E., (2009). "Research Issues in Data Provenance for Streaming Environments", Proceedings of The 2nd SIGSPATIAL ACM GIS 2009 International Workshop on Security and Privacy in GIS and LBS, 4-6 November 2009, İstanbul, Turkey

[73] Lim, H.-S. Moon, Y.-S. ve Bertino, E., (2010). Assessing the Trustworthiness of Streaming Data,Technical Report TR 2010-09, CERIAS.

[74] Misra, A. Blount, M. Kementsietsidis, A. Sow, D. ve Wang, M., (2008). "Advances and Challenges for Scalable Provenance in Stream Processing systems", Provenance and Annotation of Data and Processes Springer, 253-265.

[75] Blount, M. Davis, J. Ebling, M. Kim, J.H. Kim, K.H. Lee, K. Misra, A. Park, S. Sow, D. ve Tak, Y.J., (2007). "Century: Automated Aspects of Patient Care", 13th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, 21-24 August 2007, Daegu, Korea.

[76] Krasniewski, M. Varadharajan, P. Rabeler, B. Bagchi, S. ve Hu, Y.C., (2005). "Tibfit: Trust Index Based Fault Tolerance for Arbitrary Data Faults in Sensor Networks", International Conference on Dependable Systems and Networks, 28 June - 1 July 2005, Yokohama, Japan .

[77] Wang, Y. ve Vassileva, J., (2003). "Trust and Reputation Model in Peer-to-Peer Networks", IEEE International Conference on Peer-to-Peer Computing, 1-3 September 2003, Linköping, Sweden.

[78] Crosby, G.V. Pissinou, N. ve Gadze, J., (2006). "A Framework for Trust-Based Cluster Head Election in Wireless Sensor Networks", The Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems, 24-28 April 2006, Maryland, Columbia.

[79] Hur, J. Lee, Y. Yoon, H. Choi, D. ve Jin, S., (2005). "Trust Evaluation Model for Wireless Sensor Networks", The 7th International Conference on Advanced Communication Technology, 21-23 February 2005, USA.

[80] Chen, H. Wu, H. Zhou, X. ve Gao, C., (2007). "Reputation-Based Trust in Wireless Sensor Networks", International Conference on Multimedia and Ubiquitous Engineering, 26-28 April 2007, Seoul, Korea.

[81] Xiao, X.-Y. Peng, W.-C. Hung, C.-C. ve Lee, W.-C., (2007). "Using Sensorranks for in-Network Detection of Faulty Readings in Wireless Sensor Networks", Proceedings of the 6th ACM International Workshop on Data Engineering for Wireless and Mobile Access, 10 June 2007, China .

[82] Tanachaiwiwat, S. Dave, P. Bhindwale, R. ve Helmy, A., (2004). "Location-Centric Isolation of Misbehavior and Trust Routing in Energy-Constrained Sensor Networks", 23rd IEEE International Performance Computing and Communications Conference, 15-17 April 2004, Phoenix, Arizona.

[83] Srinivasan, A. Li, F. ve Wu, J., (2008). "A Novel CDS-Based Reputation Monitoring System for Wireless Sensor Networks", 28th International Conference on Distributed Computing Systems, 17-20 June 2008, Beijing, China.

[84] Momani, M. Aboura, K. ve Challa, S., (2007). "RBATMWSN: Recursive Bayesian Approachto Trust Management in Wireless Sensor Networks", 3rd International Conference on Intelligent Sensors, Sensor Networks and Information Processing, 3-6 December 2007, Melbourne, Australia.

[85] Shaikh, R.A. Jameel, H. Lee, S. Rajput, S. ve Song, Y.J., (2006). "Trust Management Problem in Distributed Wireless Sensor Networks", 12th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, 16-18 August 2006, Sydney, Australia.

[86] Boukerch, A. Xu, L. ve El-Khatib, K., (2007). "Trust-Based Security for Wireless Ad Hoc and Sensor Networks", Computer Communications, 30: 2413-2427.

[87] Eschenauer, L. Gligor, V.D. ve Baras, J., (2004). "On Trust Establishment in Mobile Ad-Hoc Networks", Springer Berlin Heidelberg .

[88] Jiang, J. Han, G. Wang, F. Shu, L. ve Guizani, M., (2015). "An Efficient Distributed Trust Model for Wireless Sensor Networks", Parallel and Distributed Systems on IEEE Transactions, 26: 1228-1237.

[89] Raje, R. ve Sakhare, A.V., (2014). "Routing in Wireless Sensor Network Using Fuzzy Based Trust Model", The 4th International Conference on Communication Systems and Network Technologies, 7-9 April 2014, Bhopal, India.

[90] Jiang, W. ve Wu, J., (2014). "Trust Models in Wireless Sensor Networks and Online Social Networks: A Comparative Study", 11th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, 27-30 0ctober 2014, Philadelphia, USA.

[91] Rani, V.U. ve Sundaram, K.S., (2014). "Review of Trust Models in Wireless Sensor Networks", International Journal of Computer, Information, Systems and Control Engineering, 8:361-367.

[92] Mishra, S., (2015). "Modelling of A Trust and Reputation Model in Wireless Networks", Indonesian Journal of Electrical Engineering and Informatics (IJEEI), 3:150-156.

[93] Han, G. Jiang, J. Shu, L. Niu, J. ve Chao, H.-C., (2014). "Management and applications of trust in Wireless Sensor Networks: A survey", Journal of Computer and System Sciences, 80: 602-617.

[94] Ozdemir, S., (2008). "Functional Reputation Based Reliable Data Aggregation and Transmission for Wireless Sensor Networks", Computer Communications, 31: 3941-3953.

[95] Liao, Y. Qi, H. ve Chen, C., (2010). "Clustering Algorithms of Wireless Sensor Networks", 2nd International Workshop on Intelligent Systems and Applications, 22-23 May 2010, USA.

[96] Xu, Y. Heidemann, J. ve Estrin, D., (2001). "Geography-Informed Energy Conservation for Ad Hoc Routing", Proceedings of the 7th Annual International Conference on Mobile Computing and Networking, 16-21 July 2001, Italy.

[97] Xu, Y. Bien, S. Mori, Y. Heidemann, J. ve Estrin, D., (2003). "Topology Control Protocols to Conserve Energy in Wireless Ad Hoc Networks", IEEE Transactions on Mobile Computing.

[98] Welch, G. ve Bishop, G.,(2006) "An Introduction to the Kalman Filter", University of North Carolina:Chapel Hill, North Carolina, US.

[99] Doğan, G. ve Brown, T., (2014). "ProTru: A Provenance Based Trust Architecture for Wireless Sensor Networks", International Journal of Network Management, 1–36.

[100] Cheney, J. Chong, S. Foster, N. Seltzer, M. ve Vansummeren, S., (2009). "Provenance: a Future History", Proceedings of the 24th ACM SIGPLAN Conference Companion on Object Oriented Programming Systems Languages and Applications, 25-29 October 2009, Orlando, USA.

[101] Rebahi, Y. Mujica-V, V.E. ve Sisalem, D., (2005). "A Reputation-Based Trust Mechanism for Ad Hoc Networks", The 10th IEEE Symposium on Computers and Communications, 27-30 June 2005, Cartagena, Spain.

[102] Barseghian, D. Altintas, I. Jones, M.B. Crawl, D. Potter, N. Gallagher, J. Cornillon, P. Schildhauer, M. Borer, E.T. ve Seabloom, E.W., (2010). "Workflows and Extensions to the Kepler Scientific Workflow System to Support Environmental Sensor Data Access and aAalysis", Ecological Informatics, 5: 42-50.

[103] Crawl, D. ve Altintas, I., (2008). A Provenance-Based Fault Tolerance Mechanism for Scientific Workflows, Provenance and Annotation of Data and Processes Springer, 152-159.

[104] Feng, T.H. ve Lee, E.A., (2008). "Real-Time Distributed Discrete-Event Execution with Fault Tolerance", 14th IEEE Real-Time and Embedded Technology and Applications Symposium, 22-24 April 2008, USA.

[105] Rajbhandari, S. Wootten, I. Ali, A.S. ve Rana, O.F., (2006). "Evaluating Provenance-Based Trust for Scientific Workflows", 6th IEEE International Symposium on Cluster Computing and the Grid, 16-19 2006, Singapore.

[106] Widom, J., (2004). "Trio: A system for integrated management of data, accuracy, and lineage", Technical Report.

[107] Khan, M.M.H. Abdelzaher, T. Han, J. ve Ahmadi, H., (2009). "Finding Symbolic Bug Patterns in Sensor Networks", Distributed Computing in Sensor Systems Springer, 131-144.

[108] Khan, M.M.H. Luo, L. Huang, C. ve Abdelzaher, T., (2007). SNTS: Sensor Network Troubleshooting Suite, Springer Berlin Heidelberg,.

[109] Stephan, E.G. Halter, T.D. ve Ermold, B.D., (2010). "Leveraging the Open Provenance Model as a Multi-tier Model for Global Climate Research", Provenance and Annotation of Data and Processes Springer, 34-41.

[110] Patni, H.K. Sahoo, S.S. Henson, C.A. ve Sheth, A.P., (2010). "Provenance Aware Linked Sensor Data", 2nd Workshop on Trust and Privacy on the Social and Semantic Web, 29-30 May 2010, Greece.

[111] Shebaro, B. Sultana, S. Reddy Gopavaram, S. ve Bertino, E., (2012). "Demonstrating a Lightweight Data Provenance for Sensor Networks", Proceedings of the 2012 ACM Conference on Computer and Communications Security, 16-18 October 2012, USA.

[112] Lim, H.-S. Ghinita, G. Bertino, E. ve Kantarcioglu, M., (2012). "A Game-Theoretic Approach for High-assurance of Data Trustworthiness in Sensor Networks", IEEE International Conference on Data Engineering, 1-5 April 2012, Virgina, USA.

[113] Sultana, S. Shehab, M. ve Bertino, E., (2013). "Secure Provenance Transmission for Streaming Data", Knowledge and Data Engineering, IEEE Transactions on, 25: 1890-1903.

[114] Park, U. ve Heidemann, J., (2008). "Provenance in Sensornet Republishing", eProvenance and Annotation of Data and Processes. Springer, 280-292.

[115] Khan, M.M.H. Ahmadi, H. Dogan, G. Govindan, K. Ganti, R. Brown, T. Han, J. Mohapatra, P. ve Abdelzaher, T., (2011). "DustDoctor: A Self-Healing Sensor Data Collection System", The 10th International Conference on Information Processing in Sensor Networks, 12-14 April 2011, Chicago, USA.

[116] Seo, E. Khan, M.M.H. Mohapatra, P. Han, J. ve Abdelzaher, T., (2011). "Exposing Complex Bug-Triggering Conditions in Distributed Systems via Graph Mining", International Conference on Parallel Processing, 13-16 Semptember, Taiwan .

[117] Want, R. Farkas, K.I. ve Narayanaswami, C., (2005). "Guest Editors' Introduction: Energy Harvesting and Conservation", Pervasive Computing, IEEE, 4: 14-17.

[118] Raghunathan, V. Schurgers, C. Park, S. ve Srivastava, M.B., (2002). "Energy-Aware Wireless Microsensor Networks", Signal Processing Magazine, IEEE, 19: 40-50.

[119] Pottie, G.J. ve Kaiser, W.J., (2000). "Wireless Integrated Network Sensors", Communications of the ACM, 43: 51-58.

[120] Anastasi, G. Conti, M. Di Francesco, M. ve Passarella, A., (2006). "How to Prolong the Lifetime of Wireless Sensor Networks", Mobile Ad Hoc and Pervasive Communications, 1-26.

[121] Anastasi, G. Conti, M. Di Francesco, M. ve Passarella, A., (2009). "Energy Conservation in Wireless Sensor Networks: A survey", Ad Hoc Networks, 7: 537-568.

[122] Vuran, M.C. Akan, Ö.B. ve Akyildiz, I.F., (2004). "Spatio-Temporal Correlation: Theory and Applications for Wireless Sensor Networks", Computer Networks, 45: 245-259.

[123] Li, J. ve Mohapatra, P., (2007). "Analytical Modeling and Mitigation Techniques for the Energy Hole Problem in Sensor Networks", Pervasive and Mobile Computing, 3: 233-254.

[124] Bravos, G.N. Efthymoglou, G. ve Kanatas, A.G., (2007). "MIMO-Based and SISO Multihop Sensor Networks: Energy Efficiency Evaluation", 3rd IEEE International Conference On Wireless and Mobile Computing, Networking and Communications, 8-10 October 2007, New York, USA.

[125] Cui, S. Goldsmith, A.J. ve Bahai, A., (2004). "Energy-Efficiency of MIMO and Cooperative MIMO Techniques in Sensor Networks", Selected Areas in Communications, IEEE Journal on, 22: 1089-1098.

[126] Jayaweera, S.K., (2004). "Energy Analysis of MIMO Techniques in Wireless Sensor Networks", 38th Annual Conference on Information, Sciences, and Systems, 1-4 March 2004, USA.

[127] Vidhya, J. ve Dananjayan, P., (2010). "Lifetime Maximisation of Multihop WSN Using Cluster-Based Cooperative MIMO Scheme", Int. J. Comput. Theory Eng, 2: 20-25.

[128] Fischler, M.A. ve Bolles, R.C., (1981). "Random Sample Consensus: a Paradigm for Model Fitting with Applications to Image Analysis and Automated Cartography", Communications of the ACM, 24: 381-395.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı	:Köksal AVİNCAN
Doğum Tarihi ve Yeri	:19.05.1991, Digor
Yabancı Dili	:İngilizce
E-posta	:kavincan@yildiz.edu.tr

ÖĞRENİM DURUMU

Derece	**Alan**	**Okul/Üniversite**	**Mezuniyet Yılı**
Lisans	Bilgisayar Mühendisliği	İstanbul Üniversitesi	2013
Lise	Fen Bilimleri	Hüsnü M. Özyeğin Anadolu Lisesi	2008

İŞ TECRÜBESİ

Yıl	**Firma/Kurum**	**Görevi**
2014-	Yıldız Teknik Üniversitesi	Araştırma Görevlisi

YAYINLARI

Bildiri

1. Kert, S.B. Erkoç, M.F. Kayak, S. ve Avincan, K., (2014). "Kodu İle Kendi Oyununu Geliştiren Çocuklar", 8th International Computer & Instructional Technologies Symposium, 18-20 Eylül 2015, Edirne.
2. Doğan, G. ve Avincan, K., (2015). "Kalman Filtreleme Tekniğinin Kablosuz Algılama Ağlarında Güven Analizine Uygulanması ", 3rd International Symposium on Digital Forensics and Security, 11-12 Mayıs 2015, Ankara.
3. Doğan, G. Brown, T. ve Avincan, K., (2015). "Kablosuz Algılama Ağlarında Öz Organizasyon İçin Kullanılan Provenans ve Güven Faktörü", IEEE 23. Sinyal İşleme ve İletişim Uygulamaları Kurultayı, 16-19 Mayıs 2015, Malatya.

Değerlendirme Aşamasında Olan Makaleler

1. Dogan, G. ve Avincan, K., (2015). "Kablosuz Algılayıcı Ağlarda Kalman Filtrelemeye Dayalı Güven Mekanizması", Uluslararası Bilgi Güvenliği Mühendisliği Dergisi.