Savunma Bilimleri Dergisi, 43(1): 493-517 (2023)

Elektronik/Online ISSN: **2148-1776**

Basılı/Printed ISSN: **1303-6831**

https://dergipark.org.tr/tr/pub/khosbd

SAVUNMA BİLİMLERİ DERGİSİ

The Journal of Defense Sciences

Sınır Güvenliği için Etkin ve Güvenli Bir Çözüm – Blokzincir Tabanlı Nesnelerin İnterneti

An Effective and Secure Solution for Border Security – Blockchain Based Internet of Things

Seyyit Alper SERT [1,*]

[1]*Orta Doğu Teknik Üniversitesi, Bilgisayar Mühendisliği Bölümü, 06800, Çankaya/ANKARA*

Makale Bilgisi

Araştırma makalesi
Başvuru: 19.05.2023
Düzeltme: 18.08.2023
Kabul: 24.08.2023

Keywords

Internet of Things
Blockchain
Border Security
UAV
Sensor Networks

Anahtar Kelimeler

Nesnelerin İnterneti
Blokzincir
Sınır Güvenliği
İHA
Algılayıcı Ağlar

Özet

Çeşitli sistemlerin gerçek zamanlı izlenmesini ve yönetimini sunma kapasitesi nedeniyle, Kablosuz Algılayıcı Ağ (Wireless Sensor Networks-WSN) ve Nesnelerin İnterneti (Internet of Things-IoT) teknolojileri, askeri ve güvenlik alanlarında giderek daha popüler hale gelmektedir. Akıllı gözetim sistemleri, video analitiği, akıllı ev uygulamaları ve savunma ve güvenlik sistemleri, gözetim uygulamaları için IoT kullanımındaki güncel gelişmelerden bazılarıdır. Bununla birlikte, IoT alanında birtakım zorluklar vardır ve bu zorluklar kabaca iki sınıfa ayrılabilir: kaynak sınırlamaları birinci sınıf, gizlilik ve güvenlik konuları ise ikinci sınıftır. Kaynak açısından zengin ağ geçidi düğümleri veya ağ ömrünü artırmaya çalışan etkili algoritmalar gibi farklı stratejiler oluşturulmuş ve kaynak sınırlamalarının üstesinden gelmek için temel araştırma çabaları haline gelmiştir. Buna ilave olarak, IoT alanında gizlilik ve güvenlik endişelerini gidermeye yönelik çok sayıda öneri literatürde yer almaktadır. Ancak, bunların çoğu WSN ve IoT alanının kendine özgü özellikleri nedeniyle beklentilerin altında kalmıştır. Alanın bu benzeri görülmemiş zorluklarını göz önünde bulunduran bu çalışma, öncelikle savunma ve güvenlik alanında WSN ve IoT kullanımına ilişkin literatürü kapsamlı bir şekilde gözden geçirmekte ve ardından sınır güvenliği uygulamaları için Blokzincir tabanlı IoT kullanarak etkili ve güvenli bir çözüm önermektedir. Öneri, konsept doğrulama ve bağımlılık yönlerinden deneysel testlere tabi tutulmuş ve testlerden elde edilen bulgular önerilen yaklaşımın uygunluğunu ve fizibilitesini doğrulamaktadır.

Abstract

Due to its capacity to offer real-time monitoring and management of diverse systems, Wireless Sensor Network (WSN) and Internet of Things (IoT) technologies are becoming more and more popular in the military and security fields. Smart surveillance systems, video analytics, smart home applications, and defense and security systems are some of the current developments in IoT utilization for surveillance applications. However, there are a number of difficulties in the IoT area, and these difficulties may be loosely divided into two classes: resource limitations are the first class, and privacy and security issues are the second. Different strategies, such as resource-rich gateway nodes or effective algorithms that strive to increase network lifetime, have been created and have become the key research efforts in order to overcome resource limitations. Additionally, numerous proposals to address privacy and security concerns of the IoT domain reside in the literature. However, most of them fell short of expectations because of the domain's particular features. Considering these unprecedented challenges of the domain, this study initially reviews the literature extensively on the usage of WSN and IoT in the defense and security domain and then proposes an effective and secure solution using Blockchain-based IoT for border security applications. The proposed approach was put through experimental testing for concept validation and reliance, and the obtained results of the tests supports its applicability and viability.

* Seyyit Alper SERT, e-posta: alper.sert@ceng.metu.edu.tr

DOI: 10.17134/khosbd.1299598

1. GİRİŞ

Savunma ve güvenlik alanı; askeri teçhizat, sınır güvenliği, kritik altyapı gibi çeşitli tesis ve sistemlerin sürekli izlenmesini ve kontrolünü gerektiren bir alandır. Son yıllarda, bu tip tesis ve sistemlerin gerçek ya da yakın gerçek zamanlı olarak izlenmesini ve kontrolünü sağlama yetenekleri nedeniyle Nesnelerin İnterneti (Internet of Things- IoT) teknolojisi bu alanlarda ön plana çıkmaktadır.

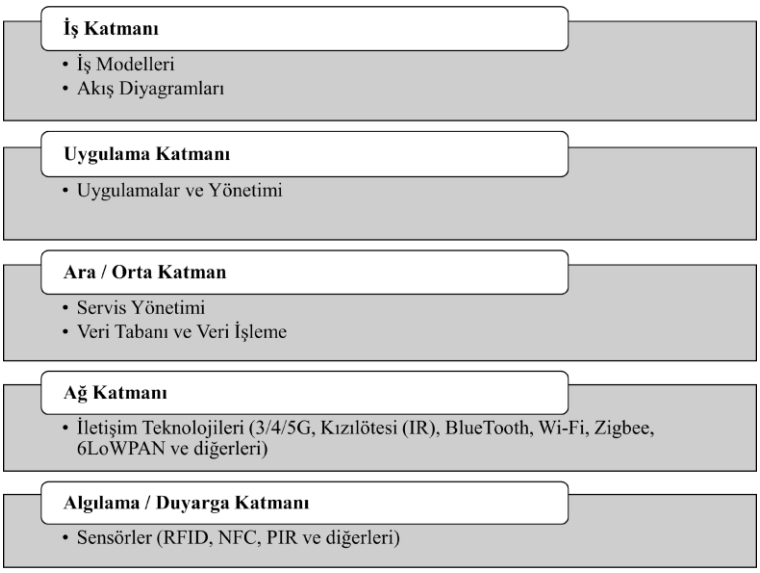
IoT terimi, ilk olarak 1999 yılında çevredeki nesnelerin algılayıcıları ve haberleşme teknolojileri ile birbirine ve internete bağlanabildiği bir ekosistemi tanımlamak için kullanılmış ve aslen GSM, Bluetooth, Zigbee ve Wi-Fi gibi farklı bağlantı imkân ve kabiliyeti olan nesnelerin bu ekosistem içerisindeki durumunu ifade eden bir paradigmadır. Paradigma aynı zamanda, algılayıcılar (sensörler), çalıştırıcılar (aktüatörler) ve iletişim yetenekleri ile gömülü, birbirine bağlı fiziksel nesnelerden oluşan bir ağı da tanımlamaktadır. Nesneler, çeşitli sistemlerin gerçek zamanlı izlenmesini ve kontrolünü sağlamak için birbirleriyle ve bulutla (İng. Cloud) iletişim kurar. Bu yönüyle, IoT'nin etkin ve önemli bileşenlerinden birini Kablosuz Algılayıcı Ağlar (İng. Wireless Sensor Networks- WSNs) oluşturmaktadır. WSN'ler, algılama, işleme ve iletişim yetenekleri ile donatılmış sensör düğümleri adı verilen düşük maliyetli ve fiziksel olarak küçük otonom cihazlardan oluşur. Düğümler birbirleriyle kablosuz olarak iletişim kurar ve ortak bir hedefe ulaşmak için bir ağ oluştururlar. Bu yönlerden bakıldığında, farklı haberleşme teknolojileri ile bağlanan cihazların günümüz ve yakın geleceğin önemli teknolojileri arasında yer aldığı ifade edilmekte (Yaqoob vd., 2017) ve gelecek internet uygulamaları için IoT'nin bir paradigma değişimi getirdiği belirtilmektedir (Agrawal ve Das, 2011).

Sayısız uygulama alanına sahip olan IoT cihazlar; çevre izlemede (Hassan vd., 2020), endüstriyel makine performanslarının değerlendirilmesinde (Saez vd., 2018), trafik yoğunluğunun takip edilmesinde (Labib vd., 2019), deprem tespit ve erken uyarı sistemlerinde (Wu vd., 2021) ve diğer benzer birçok alanda karşımıza çıkmaktadır. Kullanım alanlarına bakıldığında veri toplama, işleme ve farklı haberleşme teknolojilerine sahip cihazların ortak bir amaca (üst seviye anlamsal bilginin üretilmesine) hizmet ettikleri görülmektedir.

IoT'nin günümüz itibariyle gelişen bir teknoloji olduğu değerlendirildiğinde, mimari yapısı konusunda literatürde olgunlaşmış ve genel kabul gören fikir birliği olmamakla birlikte yapılan çalışma ve araştırmalar iki temel tasarım etrafında şekillenmektedir. Bunlardan ilki, üç katmanlı yapının esas aldığı tasarımdır (Jammes ve Smit, 2005). Aslen servis tabanlı olarak gerçek zamanlı gömülü ağ uygulamaları için ortaya konan ve esasen IoT için tasarlanmayan bu yaklaşım; bağlantı, soyutlama ve uygulama katmanlarını içermektedir. Belirtilen model, IoT yapısını daha standart bir mimari üzerine inşa etmek için, Yang ve diğerleri (2011) tarafından, ağ, uygulama ve algılama katmanlarını içeren bir tasarım olarak güncellenmiştir. Bu yapıda algılama katmanı, Radyo Frekans Tanımlama (Radio Frequency Identification- RFID) ve WSN gibi algılayıcı ağ teknolojileri vasıtasıyla olguların algılanmasını ve çevresel olayların oluşturduğu verilerin toplanmasını sağlamaktadır. Ağ tabakası, toplanan verilerin İnternet Protokol (IP) adreslerini sağlayıp kullanıcıya servis sağlamak için kurallara dayalı olarak

uygulama tabakasına iletmekte ve uygulama tabakası ise gelen verinin çözümlenmesi sonrası son kullanıcılar için servis sağlamaktadır.

R. Khan ve diğerleri (2012) tarafından yapılan ve günümüzde de kabul gören beş katmanlı yapıya ışık tutan araştırmada, IoT için her nesneyi birbirine bağlamayı amaçlayan yeni bir katmanlı mimari model sunulmuştur. Bu model; iş, uygulama, ara katman, ağ ve algılama (duyarga) katmanı olarak beş seviyeden oluşmaktadır ve Şekil 1'de özetlenmiştir.



Şekil 1: IoT mimari yapısı.

Algılama Katmanı fiziksel katman olarak da bilinir. Bu katman, çevre hakkında bilgi almak ve toplamak için sensörlere sahip olan fiziksel katmandır. Gömülü algılayıcıları ve çalıştırıcıları içerir. Bu katman, iki boyutlu barkod etiket ve okuyucuları, RFID etiketleri ve okuyucu-yazıcılar, kamera, GPS, sensörler, terminaller ve sensör ağını içerir.

İletim katmanı olarak da bilinen ağ katmanı; ağda bulunan diğer nesnelere, ağ cihazlarına ve sunuculara bağlanmaktan sorumludur. Ana işlevi, algılama katmanından gelen bilgileri iletmek ve işlemektir. İletim ortamı kablolu veya kablosuz olabilir ve düğüm cihazlarına bağlı olarak 3/4/5G, Wi-Fi, Bluetooth, ZigBee ya da benzeri haberleşme teknolojilerini kullanabilir.

Ara/Orta Katman (Middleware) üzerindeki cihazlar farklı türde hizmetler sağlarlar. Her cihaz, yalnızca aynı hizmet türünü uygulayan diğer cihazlarla bağlanır ve iletişim kurar. Bu katman hizmet yönetiminden sorumludur ve bilgileri ağ katmanından alarak veri tabanında saklamakta; bilgi işleme ve hesaplama yaparak sonuçlara göre otomatik karar vermekten sorumludur.

Uygulama Katmanı, uygulamaya özel hizmetleri kullanıcıya sunmaktan sorumludur. Akıllı evler, akıllı şehirler ve akıllı sağlık gibi IoT ile ilgili farklı uygulamalar bu katman içerisinde tanımlanmaktadır.

En üst katman olarak tasarımlanan iş katmanı, uygulamalar ve hizmetler dâhil olmak üzere genel IoT sisteminin yönetiminden sorumludur. Uygulama katmanından alınan verilere göre iş modelleri, grafikler, akış şemaları ve benzeri bu katman içerisinde oluşturulur.

Mimari tasarıma ilişkin yaklaşımlardan da görüleceği üzere gelişmekte olan bir teknoloji olması nedeniyle IoT, öncelikle cihazların (düğüm noktaları) birbirleri ile görüşebilmesi üzerine kurgulanmış ve "*önce tamamiyet sonra mükemmeliyet*" yaklaşımına da uyacak şekilde güvenlik gereksinimlerini ilk çalışmalarda göz ardı etmiştir. Halbuki, bu çalışmanın da konusunu oluşturan sınır güvenliği gibi alanlarda ve görev kritik (Mission Critical) uygulamalarda kullanıldığında, verinin doğru ya da diğer bir ifadeyle istenilen/doğru noktalara iletimi oldukça önemlidir.

Sınır güvenliği, günümüz dünyasında ülkeler için büyük bir endişe kaynağıdır. Terörizm, yasadışı göç ve kaçakçılığın artmasıyla birlikte, sınırların güvenliğini sağlamak devletler için en kritik güvenlik önceliklerinden biri haline gelmiştir. Bu maksatlarla kullanıldıklarında, IoT ve WSN teknolojilerinin sınır güvenliği uygulamalarında çeşitli avantajları vardır. Davetsiz misafirler, araçlar ve hayvanlar da dâhil olmak üzere çok çeşitli tehdit türlerini izleyebilir ve tespit edebilirler. Bunun yanı sıra, sınır güvenliğinden sorumlu güvenlik kurumlarının bilinçli (karar destek sistemleri ile desteklenen) kararlar almasına yardımcı olabilecek verileri toplayabilir ve analiz etmek için de kullanılabilirler.

Sınır güvenliği uygulamaları için IoT kullanımı ve etkinliği üzerine çeşitli araştırma çalışmaları yapılmıştır. Fiziksel ve silahlı devriyeyi gelişmiş gözetim teknolojisiyle değiştiren yerleşik bir uyarı sistemine sahip 'Akıllı Sınır' olarak da ifade edilen ve fiziksel engellere yeni bir alternatif olarak IoT kullanımı önerilmiştir (Fatima vd., 2021). Bu sistem, fiziksel engellere ve teknolojik kaynaklara zarar veren ağır silahlı devriyelere ihtiyaç duymadan sınır güvenliği sorunlarına çözüm olarak önerilmiş ve Makine Öğrenmesi (Machine Learning – ML) teknikleri kullanılmıştır. Geliştirilen sistemde, izinsiz giriş yapanları tespit etmek için güvenlik kameraları ve termal görüntüleme ile birlikte sensörler kullanılmış ve yarı otonom bir sistem tasarlanmıştır.

Sınırların farklı türde özellikleri göz önünde bulundurularak yapılan çalışmalar sınır güvenliğine yönelik olarak şekillendirilmiş, aşırı iklim koşullarına, çeşitli arazi arızalarına, nehir yataklarına ve bu yönü itibariyle fiziksel olarak izleme ve takibi zor olan, erişilemeyen yoğun orman alanlarına sahip tehlikeli sınır bölgelerinin güvenliğini sağlamak için akıllı IoT tabanlı bir sistem de probleme çözüm olarak önerilmiştir (Bhattacharya ve Roy, 2020). Tasarlanan sistem, algılanan verileri örün (web) ve masaüstü uygulaması kullanılarak bir baz istasyonu vasıtasıyla bulut sunucusuna aktarabilmektedir. Sistem vasıtasıyla algılanan veriler işlenerek baz istasyonuna uyarı da gönderilebilmektedir. Ayrıca, kullanıcının yani eğitimli güvenlik personelinin algılayıcılardan biri olan kamerayı kontrol etmesine ve uzaktan veri erişimine olanak tanınmıştır.

Genel olarak, WSN'ler ve IoT uygulamaları, ağı oluşturan bir veya daha fazla düğüm noktasına ilişkin kaynak ya da kaynaklar üzerinde kısıtlara (sınırlılıklara) sahiptir. Bu açıdan değerlendirildiğinde IoT, çeşitli açılardan düşük performans gösteren farklı tip düğüm noktaları içermekte ve kaynak kısıtlamaları,

özellikle kablosuz cihazlar için kritik hale gelmektedir. Bir kaynak baskısı, bant genişliği gibi ağın ana özelliklerinde ortaya çıkabileceği gibi, kablosuz cihaz bileşenlerinin bir özelliği olan besleme (güç ya da enerji) olarak da gündeme gelebilmekte ve özellikle enerji baskısı, IoT uygulamalarının faydalı/kullanılabilir ömrünü ciddi şekilde etkilemektedir.

Kaynak kısıtlı yapıları nedeniyle IoT cihazlar için önerilen bilgi güvenliği çözümlerinin, bu kısıtlara riayet edecek şekilde ve karmaşık yapıda olmaması aranan özelliklerdendir. Bilgi güvenliği açısında ele alındığında IoT güvenlik gereksinimleri; ağ güvenliği, kimlik yönetimi ve doğrulama, gizlilik, güven ve esneklik olarak özetlenebilir. Bununla birlikte, kaynak kısıtlarıyla beraber değerlendirildiğinde, literatürde yer alan ya da önerilen çözümlerin belirtilen tüm gereksinimleri birlikte karşılayabilmesi durumu, günümüz teknolojik ve bilimsel gelişmeleri ışığında henüz mümkün değildir. Bu nedenle bu çalışmada, belirtilen faktörler göz önünde bulundurularak, sınır güvenliği için etkin ve güvenli bir çözüm olarak Blokzincir tabanlı IoT önerilmektedir. Düğüm kimlik doğrulama sorununu dağıtık bir yaklaşımla çözmeyi öneren bu araştırma ile çok seviyeli bir blokzincir tabanlı düğüm kimlik doğrulama stratejisi ortaya konularak IoT içerisinde güvenli veri iletimi sağlanabilmektedir.

Çalışmanın geri kalanı şu şekilde düzenlenmiştir: Geçmiş ve ilgili çalışmalar Bölüm 2'de sunulmaktadır. Bölüm 3'de, önerilen yöntem ve uygulama mimarisi detaylarıyla ele alınmaktadır. Bölüm 4'de deneysel çalışmalar yapılarak öneri değerlendirilmekte ve geçerliliği tartışılmaktadır. Son bölüm olan Bölüm 5'de, sonuçlar ve gelecek araştırma alanları ile olası çalışma konuları yer almaktadır.

2. GEÇMİŞ VE İLGİLİ ÇALIŞMALAR

Akıllı gözetim sistemleri, çeşitli nesne ve olayların gerçek zamanlı izlenmesini ve kontrolünü sağlama yetenekleri nedeniyle giderek daha popüler hale gelmektedir. Günümüz teknolojisinde bu sistemler, verileri toplamak ve işlenmek üzere buluta iletmek için sensör düğümleri, kameralar ve ağ geçitleri gibi çeşitli IoT cihazlarını kullanmaktadır. İşlenen veriler daha sonra normal dışı durumları tespit etmek ve böyle bir hususun tespiti durumunda uyarı tetiklemek için kullanılmaktadır. Bu açıdan incelendiğinde video analitiği, video verilerini gerçek zamanlı olarak analiz etmek için kameralar gibi IoT cihazlarını kullanan gözetim endüstrisinde son dönemde ortaya çıkan yeni bir eğilimdir (Yazici vd., 2019). Video analitiği, endüstriyel açıdan bakıldığında kalabalık yönetimi, trafik izleme ve yüz tanıma gibi çeşitli uygulamalar için kullanılmakla birlikte; savunma ve güvenlik açılarından incelendiğinde gözetim ve takip operasyonlarının verimliliğini artırmaya yönelik görev almaktadır.

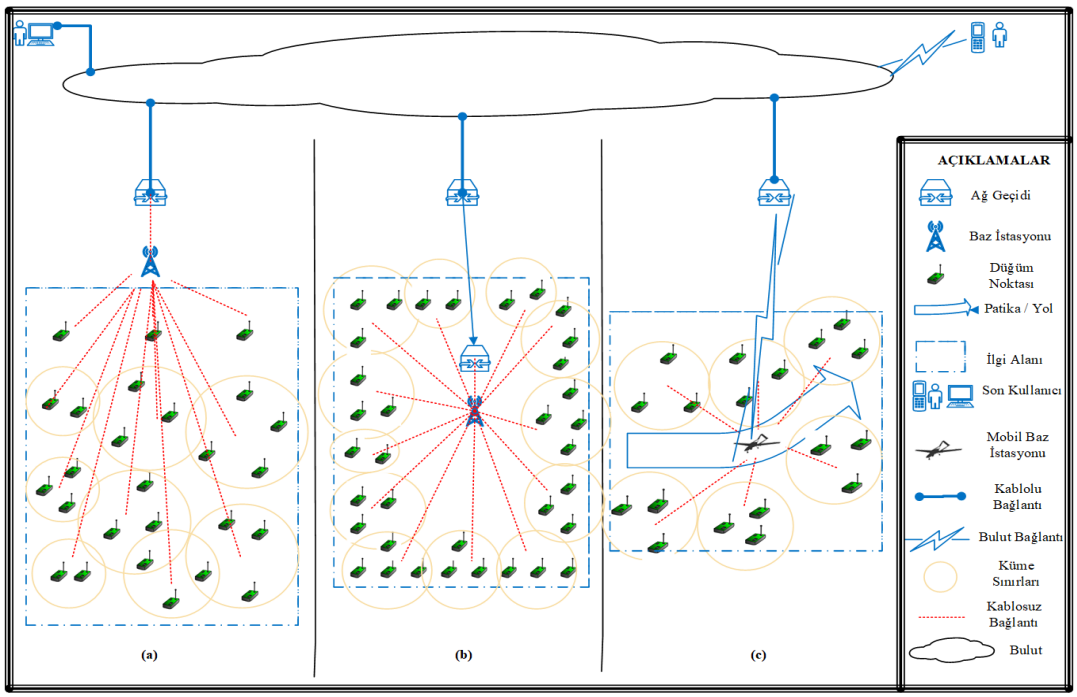
IoT'nin savunma ve güvenlik uygulamalarında kullanımı son yıllarda büyük ilgi görmüştür (Laouira vd., 2021). Özellikle savunma ve kamu güvenliği için IoT kullanımı hakkında kapsamlı bir literatür taraması yayınlanarak IoT'nin artan kullanımına dikkat çekilmiştir (Fraga-Lamas vd., 2016). Çalışmanın giriş bölümünde de belirtildiği üzere IoT cihazları, işlevlerini sınırlayan kısıtlı enerji, işlem kapasitesi ve bant genişliği gibi düşük performans göstermelerine sebep olan özelliklere sahiptir. Genellikle bu cihazlar, düşük kapasiteleri nedeniyle verileri işlenmek üzere baz ya da diğer adıyla merkez istasyona (base

station) veya bulut gibi bir kaynağa iletmek için kullanılırlar. Bu durum, sınır güvenliği gibi iletişim bağlantısının ve cihazlara erişimin sınırlı olduğu uzak noktalarda etkin kullanımlarını oldukça kısıtlamaktadır. Bu nedenle merkez istasyona erişimin kısıtlı olduğu ve işlem gücünün gerektirdiği durumlarda yük dağıtımı için kümele ve işlem değişim uygulamaları mevcuttur (Sert vd., 2018).

Laouira ve diğerleri (2021) tarafından yapılan çalışmada, sınır güvenliği uygulamaları için WSN tabanlı bir sistem önerilmiştir. Önerilen sistem ile, sınırda izinsiz girişleri tespit etmek için kademeli/katmanlı yapıda sensör kullanımından yararlanılmış ve yeni bir mimari sunulmuştur. Çalışmada, sistemin ömrü ile ilgili kaygılardan dolayı düğüm noktalarının konuşlandırma stratejileri ve aktivasyon hususlarına önem verilmekle birlikte düğüm noktaları arasında güven ilişkisine ve düğümlerin doğrulanması gibi güvenlik sorunlarına odaklanılmamıştır.

Ani ve diğerleri (2019) tarafından yapılan çalışmada ise, kritik altyapı koruma yaklaşımları gözden geçirilmiş ve IoT'nin artan kullanımı vurgulanarak dinamik modelleme ortamına yanıt verilerek güvenliğin artırılması gerekliliği vurgulanmıştır.

Sınır güvenliği maksadıyla kullanıldığında IoT'nin en büyük bileşenlerinden biri günümüz teknolojisi içerisinde WSN'lerdir. Literatürde farklı tanımlamalarla yer almakla birlikte örnek WSN konuşlandırma mimarileri Şekil 2'de sunulmuştur.



Şekil 2: IoT konuşlandırma mimari yapısı.

Şekil 2'de görüleceği üzere; alan (a) ya da kritik tesis/altyapı (b) izleme için konuşlandırıldıklarında IoT cihazları genellikle dörtgen alan içerisinde görev almakla birlikte sınır güvenliği gibi hat ya da yol güvenliği (c) maksatlarıyla konuşlandırıldıklarında daha sıklıkla şerit tipi konuşlandırma mimarisi tercih edilmektedir.

Şerit tipi konuşlandırma mimarisinde ve özellikle uzun hatlar boyunca kullanılması nedeniyle sınır güvenliği uygulamalarında, dikkate değer hususların en önemlilerinden biri konuşlandırılan her düğüm noktasının doğrudan ana istasyon ile irtibat kuramaması durumudur. Bu durum; düğüm noktalarının sahip olduğu iletişim teknolojilerinin menzili ile ilgili olarak teknolojik yetersizlikler kaynaklı olabildiği gibi, teknolojik olarak mümkün olsa da enerji tasarrufu ve ağ ömrünün uzatılması gibi ihtiyaçlar nedeniyle beliren kümeleme ihtiyaçları kaynaklı da olabilir.

Kümeleme, konuşlandırılan IoT içerisinde yer alan WSN düğüm noktalarının enerji, ana istasyona uzaklık ve diğer parametreler kullanılarak mekânsal olarak gruplanması işlemine denir. Kümeleme işlemi sonucunda; konuşlandırılmış düğümler bir ya da daha fazla sayıda oluşan kümelerden birinin içerisinde ya normal düğüm ya da küme başı (İng. Cluster Head – CH) tanımlamasıyla yer alırlar. Kümelenmiş WSN'lerde enerjinin etkin ve dengeli kullanım amaçlarına uygun olarak, normal düğümler algılanan veriyi üye oldukları küme içerisinde yer alan küme başına gönderir ve küme başları da ana istasyona doğrudan erişebilme imkanına sahip ise doğrudan, değil ise diğer küme başları üzerinden atlamalı olarak (İng. multi-hop) ulaştırırlar. Literatürde kümeleme algoritma ve yaklaşımları ile ilgili oldukça fazla sayıda araştırma bulunmakla birlikte, önerilen çalışmanın ana konusu ve katkılarından bir tanesi olmaması nedeniyle, kümeleme algoritma ve yaklaşımları kapsam dışında tutularak detaylı olarak incelenmemiş; araştırmacılara bilgi vermesi açısından temel unsurları yönüyle özetlenmiştir.

Kümelenmiş WSN'lerde, çoğunlukla birden fazla atlamanın neden olduğu enerji sorunlarını (küme başları üzerinden yoğun veri trafiği akışı ya da sıcak noktalar problemi ve benzeri) önlemek için, son dönemdeki araştırmalar, kaynak açısından zengin (kısıt bulunmayan) bir veya daha fazla Mobil Baz (merkez) İstasyonunun (MBİ) IoT entegrasyonuna yönelmiştir. MBİ, özellikle kablolu bir altyapı kurmanın zor veya imkânsız olduğu alanlarda görev yapan WSN'lerin kritik bir bileşenidir ve literatürde çevresel izleme, afet müdahalesi ve askeri operasyonlar dâhil olmak üzere mevcut enerjinin etkin kullanımının zarurî olduğu çeşitli uygulamalarda kullanılmıştır. Popescu ve diğerleri (2019) tarafından, etkin gözetleme için mobil (kara ve hava) istasyon kullanımına ilişkin literatür taraması yapılarak iç ve ülke güvenliği konularının önemli uygulama alanları arasında olduğu vurgulanmıştır.

İnsansız Kara Aracı (İKA) ya da robot gibi karasal olan MBİ'lere ilave olarak son dönemde özellikle karasal ulaşımın zor ya da imkânsız olduğu noktalarda baz istasyonu görevi görmek üzere İnsansız Hava Araçları (İHA, İng. Unmanned Aerial Vehicles- UAVs) da sıklıkla kullanılmaktadır. MBİ olarak İHA kullanımı, özellikle düğüm noktalarının hızlı ve zamanında konuşlandırılması gereken ya da gerçek veya yakın gerçek zamanlı gözetim ve güvenlik uygulamalarında oldukça kullanışlıdır. Buna ilave olarak IoT kapsamında İHA'lar, MBİ görevleri dışında mevcut altyapının kapsamadığı alanlarda geçici kapsama sağlamak için düğüm noktası olarak da kullanılabilmektedir.

Tazibt ve diğerleri tarafından yapılan çalışmada, düğümlerin enerji tüketimi sorununa, kaynak açısından zengin ağ geçidi düğümlerine göre İHA kullanımının nispeten daha üstün bir çözüm sunmakta olduğu, ayrıca ağ enerji dengesine ve ömrüne katkıda bulunduğu belirtilmiştir (Tazibt vd., 2017). WSN'lerdeki

MBİ'lere yönelik literatürdeki son dönemdeki eğilimler, otonom MBİ'leri, İHA destekli MBİ'leri, hibrit (otonom ve İHA destekli) MBİ'leri ve enerji hasat (İng. Harvesting) yeteneklerine sahip MBİ'leri içerir. Bu eğilimler incelendiğinde, WSN kapsama alanını iyileştirme, toplanan verinin kalitesini artırma ve ağ kurulum ile bakım maliyetlerini azaltma ihtiyaçlarının, MBİ kullanımının ana nedenleri arasında olduğu görülmektedir.

İHA'ların MBİ olarak kullanımı, sınır gözetleme uygulamalarında WSN'lerin performansını artırmaktadır. Bu kapsamda yapılan bir çalışmada, İHA destekli WSN kullanımının özellikle engebeli arazide enerji efektif ve hızlı veri toplanmasına imkân veren bir kullanım olduğu sonucuna ulaşılmıştır (Nazib ve Moh, 2021). Bu açından incelendiğinde İHA'lar, karasal WSN'leri tamamlayabilmekte ve sınırın kuşbakışı görüntüsünü de gerçek zamanlı olarak sağlayarak WSN'nin kapsama alanını artırabilen mobil düğümler olarak da görev yapabilmektedir. Bir IoT uygulamasında MBİ'lerin sayısı, uygulama alanına ve yedeklilik gereksinimlerine bağlı olarak değişebilmektedir.

İHA'ların MBİ olarak kullanımın bir sonucu olarak araştırma alanları, mobil düğüm noktası veya mobil istasyon mevcut olan durumlar için, yeniden bu ağların güvenlik özelliklerine çevrilmiştir. WSN ve IoT alanındaki güvenlik araştırmaları literatürde yoğun olarak çalışılan konular arasındadır ve çeşitli güvenlik saldırıları ve uygulanabilen tedbirlerin özetlendiği çalışmalar bulunmaktadır (Sert vd., 2015). Yakın dönemde, Mobil Tasarsız Ağlar (İng. Mobile Ad hoc Networks – MANETs) için güncel güvenlik açıkları, problem sahaları ve saldırılar ile ilgili literatür taraması da yayınlanarak alanın ihtiyaçları ve güncel gelişmeler özetlenmiştir (AlRubaiei vd., 2020).

İzleme uygulamalarında IoT kullanımındaki en büyük zorluklardan biri, teknolojiyle ilgili gizlilik ve güvenlik endişeleridir. Bağlanan cihaz sayısı arttıkça siber saldırı ve veri ihlâli riski de artmaktadır. Bu durum kişi ve kurum mahremiyeti ve güvenliği için önemli bir tehdit oluşturmaktadır. Özellikle güvenlik uygulamalarında IoT kullanımındaki bir başka zorluk ise endüstride standardizasyon eksikliğidir. Farklı IoT cihazları tarafından kullanılan farklı protokoller ve standartlar mevuttur ve bunun doğal bir sonucu olarak da bu cihazların birleşik şekilde entegre edilmesi ve yönetilmesi karmaşık bir problem haline dönüşmektedir. Bu ise, birlikte çalışabilirlik (İng. Interoperability) sorunlarına yol açabilmekte ve IoT tabanlı sistemlerinin ölçeklenebilirliğini azaltmaktadır.

MBİ olarak İHA kullanılan durumlarda; kablosuz düğümler, kimlik doğrulama (İng. authentication) kullanılarak kiminle bağlantı kurduğundan emin olabilir. Kimlik doğrulama ve güven yönetiminden sorumlu bir ana ya da merkezî otoritenin varlığı dikkate alındığında, ağda yüksek derecede gizlilik ve güvenlik kolaylıkla garanti edilebilir ve literatürde bu tür kimlik doğrulama konusunda çok sayıda çalışma vardır. Bununla birlikte, merkezî otoritenin ağ güvenliğinin odak noktası haline gelmesi ve onu aynı zamanda hayati bir güvenlik açığı noktası ve ağın tek hata noktası (İng. Single Point of Failure – SPoF) haline getirmesi bakımından önemli bir sorundur. Buna ilave olarak merkezî yöntemler, her zaman ağa bağlantıyı garanti edebilecek bir düğüm olmadığı için gerçek yaşam koşullarında uygulanabilirliği kısıtlamaktadır.

IoT düğüm kimlik doğrulamasını ve veri bütünlüğünü (İng. Integrity) hedefleyen aktarım katmanı güvenliği (İng. Transport Layer Security- TLS) tabanlı yöntemler literatürde (Kothmayr vd., 2013; Panwar ve Kumar, 2015) tasvir edilmiştir. Bu çalışmalarda, bir Açık Anahtar Altyapısının (A3, Public Key Infrastructure- PKI) yönettiği ve sağladığı sertifikalar kullanılmıştır. Bu yöntemler, güvenli veri aktarımı ve güvenilir kimlik doğrulama sağlayabilmektedir ancak Rivest Shamir Adleman (RSA) (Rivest vd., 1978) ve diğer asimetrik algoritmaların yürütülmesi için kaynak kısıtlı olan IoT ve benzeri ağlarda önemli miktarda zaman ve enerjiye ihtiyaç duyulmaktadır. Belirtilen kaynak kısıtının sebep olduğu olumsuz durumun üstesinden gelebilmek için Kısıtlı Uygulama Protokolü (İng. Constrained Application Protocol- CoAP) (Shelby vd., 2014) ile Eliptik Eğri (İng. Elliptic Curve- EC) (Hankerson vd., 2004) kombinasyonu, özellikle enerji tüketim sorununun üstesinden gelmek için kullanılmıştır (Capossele vd., 2015). Bununla birlikte, sistemin çok yönlülüğü ve ölçeklenebilirliği, gereksinim duyulan merkezî kök sertifika yetkilisi (İng. Root Certification Authority) nedeniyle azalmıştır.

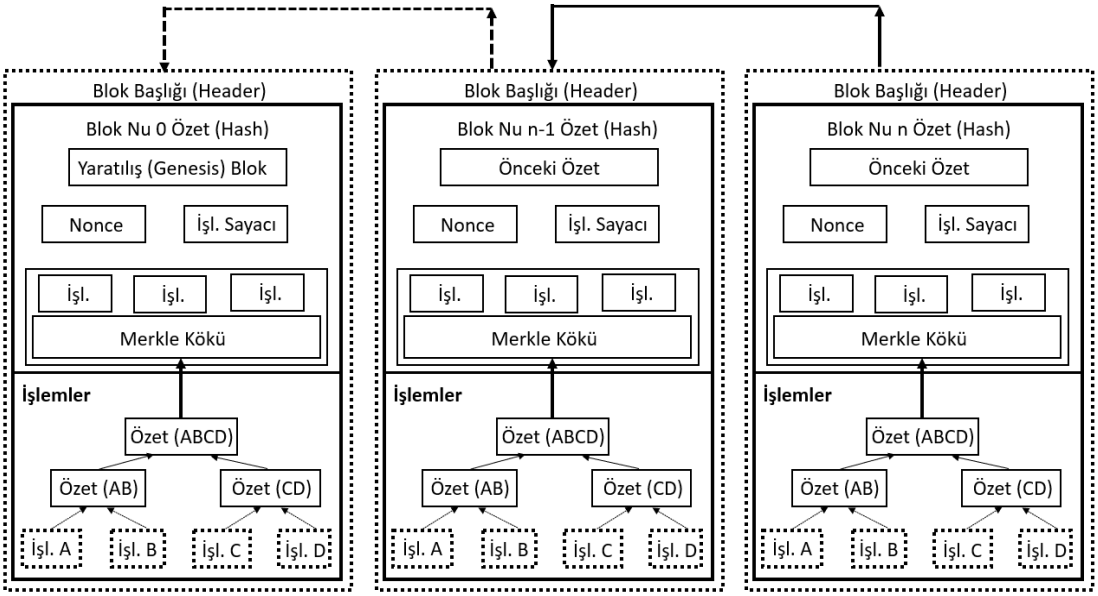
Literatürde, tek kullanımlık şerit (İng. One Time Pad – OTP) tekniği tabanlı bir mekanizmadan yararlanan Ön Paylaşımlı Anahtar (İng. Pre-Shared Key- PSK) yöntemi çözüm olarak önerilen çalışmalar arasındadır (Hammi vd., 2017). Buna ek olarak, Gelişmiş Şifreleme Standardı (İng. Advanced Encryption Standard- AES) için Galois/Sayaç Modu, veri gizliliğini ve bütünlüğünü garanti etmek için ise Sayaç Şifre Blok Zincirleme (Cipher Block Chaining-CBC) Ortam Erişim Kontrolü (Medium Access Control-MAC) çalışma modları kullanılmıştır (Dworkin, 2007). Belirtilen yöntemler, enerji kullanımı açısından güvenilirliklerini, taşınabilirliklerini ve etkinliklerini kanıtlamıştır. Ancak, önceden paylaşılan anahtarların dağıtımı ve hareketli düğümlerin desteklenmemesi nedeniyle esneklik kısıtlanmaktadır. Buna ilave olarak, geleneksel WSN ve IoT kimlik doğrulama protokolleri, güvenilir üçüncü taraf (Trusted Third Party- TTP) uygulamalarına ihtiyaç duyması nedeniyle çeşitli hata noktalarına da duyarlı hale gelmektedir (Cui vd., 2020).

Özetlenen çalışmaların birçoğu özellikle sınır güvenliği gibi görev kritik gerçek yaşam uygulamalarında beklenen katkıyı sunamamıştır. Buna ilave olarak, MBİ kullanımı nedeniyle ağ sınırlarının genişlemesi, geleneksel merkezi güvenlik önlemlerinin yerine merkezî olmayan (diğer bir ifadeyle dağıtık) önlemlere olan ihtiyacı daha da belirgin hale getirmiş ve Blokzincir teknolojisi bu konuda uygulanabilir bir çözüm olarak ortaya çıkmıştır.

Bitcoin, 2008 yılında Satoshi Nakamoto adıyla açıklanan, eşler arasında (İng. Peer-to-Peer) bir elektronik para birimi şemasıdır (Nakamoto, 2008). Şemanın sunulduğu çalışmadaki Satoshi Nakamoto adının tek bir kişiyi mi yoksa bir grubu mu tasvir ettiği henüz bilinmemektedir. Yapılan çalışmada, Blokzincir, ağdaki güvenilirliğini garanti etmek için, finansal işlemleri, eşlik eden bir protokolle birlikte tutmak için yeni bir veri formatı olarak tanıtılmıştır. Çalışmanın yazar(lar)ı, Blokzincir'i, sürekliliği (İng. Continuity) ve değişmezliği (İng. Immutability) sağlamak için, her biri önceki ve mevcut bloklara karşılık gelen kriptografik özetler (İng. Hash) içeren ve doğrusal bir blok dizisi tarafından modellenen bir veri tabanı olarak nitelendirmiştir. Finansal işlemleri kayıt altına almak için Bitcoin tarafından

Blokzincir kullanılmaktadır. Sistem kullanılarak işlemler, üçüncü bir otoriteye güven yerine elektronik kanıtlara dayanılarak, doğrudan ve güvenli bir şekilde iletişim kuran eşler arasında merkezi olmayan (İng. Decentralized) bir şekilde yapılabilir. Bu yapı, blokzincirde dağıtılmış defterler olarak tanımlanmaktadır ve her düğümde işlemlerin kayıtları yer almaktadır. Bu sayede tüm düğümler blokzincirin doğruluğunu ve değişmezliğini doğrulayabilmektedir. Blokzincirde işlemlerin bloklara yazılması için doğrulanması gerekmektedir. Bu doğrulama işlemi fikir birliğiyle yapılmakta ve uzlaşma/fikir birliği (İng. consensus) algoritmaları olarak tanımlanmaktadır. Üçüncü bir otoriteye ihtiyaç duymadan düğümlerin yapılan işlemleri doğruluğu üzerinde fikir birliğine erişmeleri, geleneksel fikir birliği algoritmalarına benzemekle beraber otonom olarak kriptografik temellere dayalı olarak yapılmaktadır. Dağıtılmış bir defter aracılığıyla blok zincirine güç sağlayan fikir birliği sürecinin, Bitcoin'in gerçekte nasıl çalıştığının temeli olduğu belirtilmektedir (Eyal vd., 2016). Bu defter kayıtları, bağlantılı bloklar oldukları için silinmeye, değiştirilmeye ve kurcalanmaya karşı korunan veriler içermektedir (Iansiti ve Lakhani, 2017).

Blokzincir teknolojisi, Bitcoin üzerinden sanal para transferi maksadıyla geliştirilmiştir. Yani blokzincir temeliyle Bitcoin ağında sadece para transferi mümkündür. Blokzincir teknolojisinin kullanım alanları ve etkinliği görüldükçe, Bitcoin ekosisteminin dışında birçok alanda kullanımı ve çeşitli varyasyonları ortaya çıkmış literatürde yaygın olarak yer bulmaya devam etmektedir. Bu açıdan Blokzincir, eşler olarak da bilinen bir düğüm koleksiyonu üzerine kopyalanan ve dağıtılan bir işlem veri tabanı olarak karakterize edilebilir. Bu veri tabanı, işlemler olarak bilinen bir veri defterini tanımlamaktadır. Zincirdeki her blok bir gövde ve başlıktan oluşmaktadır. Gövde olarak bilinen işlem grubu, açık metin (İng. Plaintext) veya şifreli metin (İng. Ciphertext) biçiminde tutulabilmektedir. Buna karşılık, başlık, blok numarası, sürüm, zaman damgası ve önceki blok özeti gibi blok öğelerinin hesaplanan karma değeri olan Merkle kökü (İng. root) gibi ayrıntıları içerir (Bitcoin Developer Guide, b.t.). Her bir blok kendisinden önce oluşan bloğun özet (hash) değerini tutar, bu sayede; doğrusal olarak sıralanmış ve birbirine bağlı bloklar şeklinde oluşan organize zincir serisi oluşur. Özet algoritmalarının temelinde geriye döndürülemezlik (İng. irreversibility) yani özet değerinden orijinal değerin elde edilememesi vardır. Sabit boyutta çıktı vermesi ve değişikliğe karşı dayanıklı, yani en küçük bit değişikliğinde tamamen farklı bir sonuç elde edilmesi ise diğer özelliklerindendir. Bu zincirde oluşan bir bloktaki tek bir işlemin bile değiştirilmesi, kendisinden sonra gelen tüm blokların değiştirilmesini gerektirmektedir. Bu nedenle blokzincirin güvenliği düğümlerin fazlalığından ve doğruluğunda gelmekle beraber, aynı zamanda zincir boyutunun büyümesiyle, işlemlerin değiştirilmesi de o kadar zorlaşır. Bir saldırgan bloktaki herhangi bir işlemi değiştirmeye çalışırsa, tek bir bitin değişmesi sonucu başlık özetinin değişmesi nedeniyle diğer tüm blokları değiştirmek zorundadır. Blokzincir temsili yapısı Şekil 3'de verilmiştir.



Şekil 3: Blokzincir temsili yapısı.

Blokzincir, endüstri ve akademide; kaynak takibi (Zhu vd., 2018), akıllı ev mimarisi (Moniruzzaman vd., 2020) ve tedarik zinciri yönetimi (Dujak ve Sajter, 2019) konularında yoğun olarak kullanılmakta; WSN ve IoT güvenliğine ilişkin çalışmaların önemi giderek artmaktadır (Faris vd., 2023). Bu bağlamda, WSN ve IoT ağlarında, düğüm kimlik doğrulaması için güvenli ve merkezi olmayan bir tekniğin kullanılması kısmen bir zorunluluk ve amaç haline gelmiş; Blokzincir teknolojisi, merkezi olmayan, yüksek veri güvenliği ve sistem çapında bir bakış açısı sağlayarak uygun bir seçenek haline ve gelecek vaat eden bir çözüme dönüşmüştür (A. Khan vd., 2022).

Mevcut çözümlerin çoğu genelde statik topolojilere odaklanmış ve düğümlerin dinamik davranışını büyük ölçüde göz ardı etmiştir. Bununla birlikte, bir eşler arası (P2P) ağda ve özellikle IoT ortamlarında, bant genişliği ve depolama kısıtları üstesinden gelinmesi gereken iki zorluktur ve herhangi bir blokzincir uygulamasının bu sorunları göz ardı etmemesi gerekliliği literatürde belirtilmiştir (Liu vd., 2019).

Blokzincir teknolojisi, IoT ağlarında, çok sayıda düğüm noktasının tüm defteri kopyalaması gerekliliğinden dolayı oluşturulan verinin etkin yönetimi konusunda (özellikle depolama alanı ve hesaplama maliyeti yönleriyle) problem yaşamaktadır. Bu da blok zinciri mimarisine bağlı olarak düğümlerde büyük depolama kapasitesi gereksinimini beraberinde getirmektedir (Uddin vd., 2019). Bu cihazların kısıtları nedeniyle, blokzincir kayıtlarının birebir yerel bir kopyasını oluşturmak da genellikle mümkün veya pratik değildir (Danzi vd., 2019).

Bahsedilen veri depolama sorunları, WSN ve IoT ortamlarında Blokzincir kullanımı için hala geçerli olsa da önerilen çözüm, literatürde yer alan çalışmalarda (Mubarakali, 2021; A.U. Khan vd., 2022) olduğu üzere, önemli ölçüde daha az veri gerektiren düğüm kimlik doğrulaması maksadıyla blokzincir teknolojisini kullanmaya odaklanmıştır. Bu çalışma açısından bakıldığında, değişmezlik ve merkezi olmayan operasyon mimarisi gibi blokzincirin faydalı özellikleri, teknolojiyi bu çalışmada önerilen sınır güvenliği uygulama alanında önemli bir araç ve öne çıkan bir çözüm haline getirmiştir.

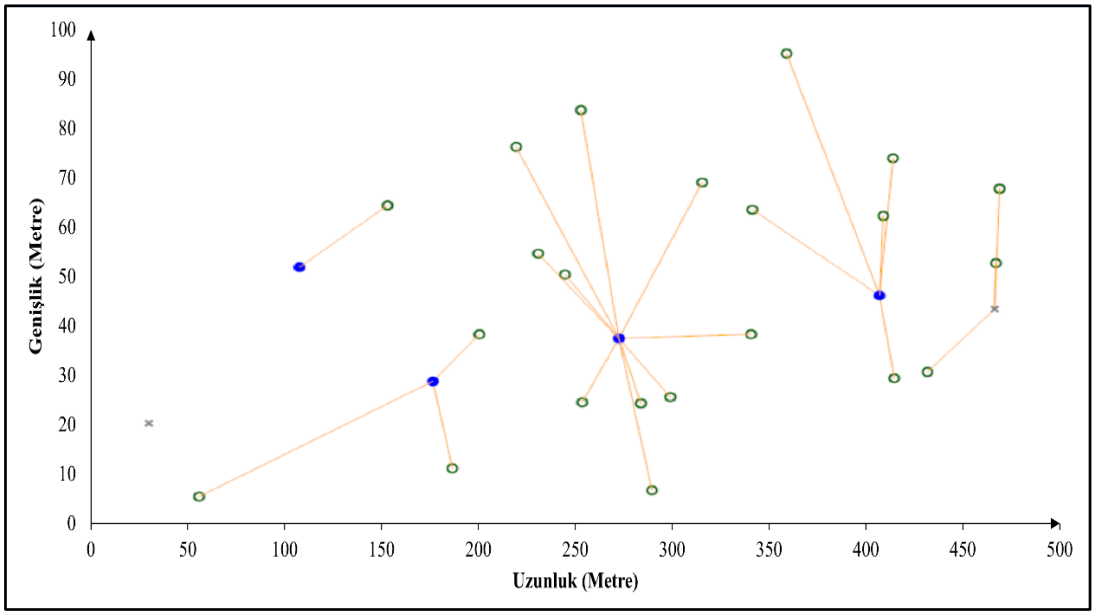
Uygulama detayları bir sonraki bölümde verilecek olmakla birlikte bu çalışma, literatürde yer alan hiyerarşik blokzincir yapısına (Ahmed vd., 2022) benzer bir yaklaşım olup düğüm kimlik doğrulama çalışmasının (Sert, 2023) küme üye düğüm sayısı üzerinde kısıt bulunmayan genişletilmiş sürümüdür.

3. YÖNTEM

3.1 Sistem Modeli

Öneri, temel unsurları ve varsayımları aşağıda detaylarıyla verilen sistem modeli üzerine tasarlanmıştır. Aynı model, karşılaştırılan yöntemlerin değerlendirilmesinde de kullanılmaktadır. Sistemde; normal düğümler, elde ettikleri verileri bağlı oldukları küme başlarına (CH) aktarır. Her küme için toplanan veri, doğrudan iletim yöntemiyle, MBİ'ye iletilir.

Şekil 4'de bir WSN'nin temsili konuşlandırılması gösterilmektedir. Şekilde görüleceği gibi, deneylerde kullanım kolaylığı için tüm düğümler x ve y düzlemleri üzerindeki koordinatlarıyla temsil edilen konuşlandırma alanı içerisinde bulunmakta ve enerji etkin bir çalışma için kümeleme yaklaşımından yararlanılmaktadır.



Şekil 4: Temsili WSN konuşlandırma.

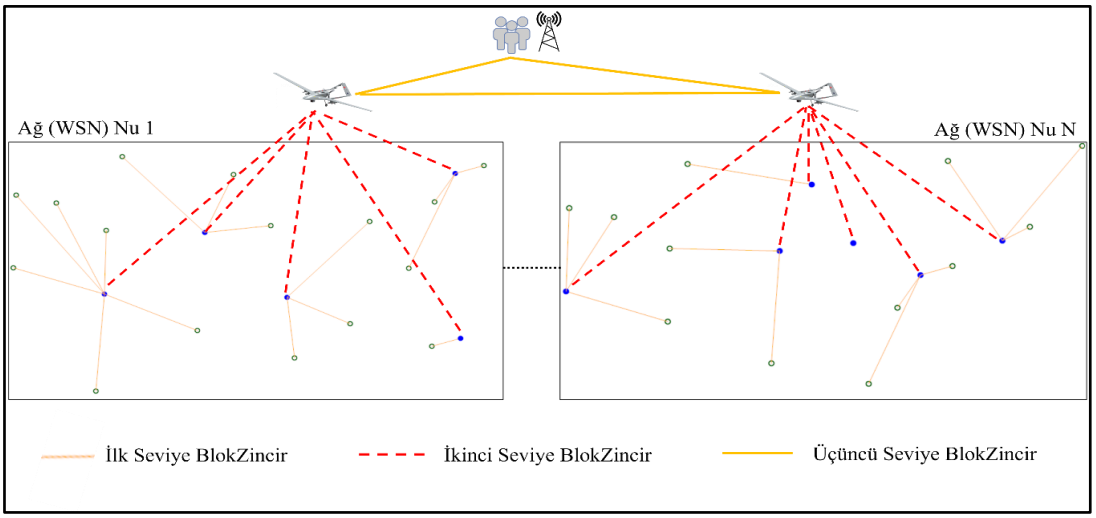
Şekil 4'de, küme başları mavi daireler olarak betimlenmiş, belirlenen kümedeki bağlı/normal düğümler koyu yeşil çemberler olarak çizdirilmiştir ve çeşitli nedenlerle kullanım dışı kalan düğüm noktaları ise çarpı ile tasvir edilmiştir. Konuşlandırma alanı sınır güvenliği uygulamalarında da çoğunlukla uygulandığı şekliyle genişlik (y düzlemi) olarak göreli kısa ve uzunluk olarak (x düzlemi) yüksek mesafededir ($x > y$). Bu durumda MBİ olarak geçmiş çalışmalarda da belirtildiği üzere karasal araçların kullanımından ziyade mesafenin artışına bağlı nedenle İHA kullanımı tercih edilir bir kullanım haline gelmektedir.

Sistem modeline ilişkin varsayımlar şu şekilde açıklanabilir: Düğümler ve İHA'lar (birden fazla olduğunda) özellikleri yönüyle birbirlerinin aynıdır ve İHA'lar haricinde konuşlandırılan düğümler hareketsizdir. Yer düğümlerinin konuşlandırılması, Şekil 4'de belirtilen WSN konuşlandırma alanı ($x > y$) esas alınarak tek biçimli (uniform) dağıtım modeli izlenerek yapılmıştır. Düğüm noktaları yeterli veri depolama alanı ile donatılmıştır. Deneysel değerlendirmeye esas olmak üzere, eşler (iletişim kuran düğüm noktaları) arasında direk (doğrudan) iletişime engel olabilecek bir arıza/yeryüzü şekli bulunmadığı ve İHA uçuş irtifasının operasyon boyunca değişmeyerek belirlenen her bir kümenin Ağırlık Merkezinin (İng. Center of Gravity- CoG) tam olarak üzerinden uçtuğu varsayılmıştır.

Müteakip alt başlıklarda açıklanan çok düzeyli blokzincir yapısının gerçeklenebilmesi için öncelikle kümeleme yaklaşımı takip edilerek kümelenmiş bir ağ kurulması ve ardından blokzincir uygulamasına geçilmesi gerekmektedir.

3.2 Çok Düzeyli (Multi-Level) Blokzincir Yapısı

Çok düzeyli blokzincir yapısını uygun bir yöntem haline getiren başlıca üç temel özellik vardır. Bunlar; özellikle enerji tasarrufu yapmak için uygulanan kümeleme yaklaşımları sonucunda oluşan ağaç yapısı çok düzeyli Blokzincir yapısının kullanımına uygun bir ortam hazırlamaktadır. Bununla birlikte, IoT veya WSN ortamlarındaki kaynak kısıtları nedeniyle blokzincir kaynaklı sisteme getirilen yük (depolama ve veri işleme) kontrollü bir seviyede tutulmaktadır. Son olarak da MBİ varlığı nedeniyle yer değiştirebilen düğümlerin ağ düzeyindeki kimlik doğrulaması kolaylıkla sağlanabilmektedir. Önerilen yapı, Şekil 5'de sunulmuştur. Bu nedenle, İHA gibi bir MBİ'nin varlığında ağ düzeyinde kimlik doğrulaması fonksiyonu sağlayabilmek için, hiyerarşik yapıdaki kümelenmiş WSN'ler için çok düzeyli bir Blokzincir tabanlı düğüm kimlik doğrulama yönetiminin kullanılması umut veren bir seçimdir.



Şekil 5: Çok düzeyli blokzincir yapısı.

Birinci düzey (ilk seviye) zincir, küme seviyesinde oluşturulur. Her küme, küme başı ve küme üye düğümleri arasında kendi yerel zincirine sahipken, her bir WSN, gösterilen CH ve kendi MBİ olan

İHA'sı arasında kırmızı kesik çizgilerle betimlendiği şekliyle ikinci düzey zinciri oluşturur. Bu ikinci düzey zincir, bir MBİ mevcudiyeti olduğunda tek bir WSN'de düğüm kimlik doğrulaması için genellikle yeterlidir. MBİ'ler arasında üçüncü düzey zincir gerekliliği, çok sayıda WSN'nin aynı amaç için kapsama alanını genişletme gibi nedenlerle birbirine yakın konuşlandırılması veya tek hata noktası durumundan kaçınmak için birden fazla hareketli mobil baz istasyonuna sahip olması durumundan kaynaklanmaktadır. Bu üçüncü düzey zincir, şekildeki İHA'lar arasında doğrudan iletim (turuncu düz çizgi) yoluyla tasvir edilmiştir.

Küme üyesi (normal) düğümler, tasvir edilen CH'leri ile düğümlerin kimliklerini (authentication) doğrulamak için kullanılan bu çok düzeyli zincirin yalnızca ilk düzeyinde bulunur. Birinci ve ikinci düzey zincirler üye olarak CH düğümlerini içerir. Birinci düzey zincirin amacının küme içerisinde kimlik doğrulaması olduğu belirtilmiştir. CH'lerin İHA ile tek bir WSN'de kimliğini doğrulamak için, CH'ler ile İHA arasında ikinci düzey zincir kullanılır. Üçüncü düzey zincirin işlevi, küresel düğüm kimlik doğrulaması için farklı WSN'lerdeki MBİ'lerin ve gerektiğinde WSN'lere sonradan katılacak düğümlerin kimliğini doğrulamaktır.

3.3 Uygulama Detayları

Bu çalışmanın temelini oluşturan çok seviyeli blokzincir çalışmasında (Sert, 2023) düğümlerin sabit sayıda olma ve yer değiştirmeme kısıtı bulunmaktadır. Bu nedenle bu çalışma, belirtilen kısıtları ortadan kaldırmaya odaklanarak yapılmıştır. Bu çalışmanın literatüre katkısının ortaya konabilmesi maksadıyla, müteakip alt bölümlerde kaynak çalışmanın uygulama esasları verilerek yapılan güncelleme karşılaştırmalar vasıtasıyla vurgulanmıştır.

3.3.1 Temel Uygulama

Açıklanan sistem modeli ve çok düzeyli blokzincir yapısı gereksinimlerine uygun olarak, kimlik doğrulama stratejisi aşağıdaki şekilde uygulanabilir:

- *Başlatma*: Bir WSN'nin parçası olan herhangi bir İHA'nın veya CH'nin ayarlarının başlatılması gerekir. Başlatma işlemi İHA'lar için MBİ, CH'ler için ikinci seviye blokzincirdeki İHA (lar) tarafından yapılır,
- *Kayıt*: Her düğümün kriptografik adresi (Id) ilgili zincire kaydedilir ve tutulur,
- *Kimlik Doğrulama:* Çok seviyeli blokzincir yaklaşımı, ilgili zincirde tutulan kriptografik adresleri kullanarak kimlik doğrulama isteklerini doğrular ve onaylar,
- *Sonlandırma:* Hasar alan, enerji tüketimi nedeniyle kullanım dışı kalan her düğüm ağdan ayrılır.

Ethereum blokzincir, *Truffle* çerçevesi ve *Ganache* kullanılarak önerinin doğrulanması için simüle edilebilir. Çalışma kapsamında Ethereum, akıllı sözleşmeleri desteklemesi ve işlemleri daha hızlı gerçekleştirmesi nedeniyle tercih sebebidir. Buna ilave olarak, Ganache ve Truffle, Ethereum Blokzincir için geliştirme ortamı sunması ve canlı kullanım için uygun olmamasına rağmen anında kesinliği (İng.

immediate finality) desteklemesi nedeniyle doğrulama testlerinde tercih edilmiştir. Çok düzeyli zincir yapısı, bu açıklamalara uygun olarak belirtilen uygulama platformunda geliştirilebilmiştir.

Gerçek yaşam koşullarında, zincirler, fiziksel adreslerini kullanan düğümler tarafından oluşturulur. Ancak, test ortamında, herhangi bir düğüm (normal düğümler, CH'ler veya İHA'lar) son kullanıcı tarafından atanan tekil (benzersiz) bir adres verilerek bu değere sahip olur. Simülasyona dahil her düğüm, kimlik doğrulama işlemi başlamadan önce Eliptic Curve algoritmasını kullanarak bir anahtar çifti oluşturur. Eliptic Curve şifreleme algoritması PKI'ya dayanan bir algoritmadır. PKI'da açık (public) ve gizli (private) anahtar çifti üretilir. Açık anahtar herkes tarafından erişilebilir ve imza doğrulaması gibi sahibini doğrulama işlemlerinde kullanılır. Gizli anahtar ise sadece kullanıcı tarafından bilinen ve şifreli mesajların iletilmesinde kullanılan anahtardır. Üretilen açık anahtar kullanılarak elde edilen adres bilgisi zincirin düğüm tanımlaması için kullanılır. Bu işlem, ağ düğümlerinin anonimliğini korurken, merkezi olarak yönetilen bir anahtar oluşturma yetkilisi gereksinimini de ortadan kaldırmaktadır.

Aynı kümede olmadıklarında her bir normal düğüm, belirlenmiş CH'leri ile farklı bir birinci seviye blokzincir oluşturur. Bu ilk (birinci) düzey zincir için oluşum (İng. Genesis) blokları, o kümelerin CH'leri tarafından sağlanır. Bu durum aynı zamanda, ortamdaki CH'ler oluşum özetini (hash) sağlayıncaya kadar herhangi bir kümenin üye düğümleri tarafından blok oluşturulamayacağını da göstermektedir. Ayrıca, bu çalışma modu, aynı kümedeki CH ve diğer normal düğümlerin, söz konusu kümeye bağlanan her yeni normal düğümü de yetkilendirmesi gerekliliğini sağlamaktadır. CH oluşum bloğunu elde etmeden önce zinciri çatallamak (İng. forking) imkânsız olduğundan, bu durum aynı zamanda, gölgede bırakma (İng. eclipsing) tip saldırı çabalarını da engellemektedir. Blokzincir işlemleri için bir Ethereum cüzdanı gereklidir, Truffle'ın kendi oluşturduğu hesaplar ve yönetim seçenekleri sayesinde PKI anahtar çiftlerini depolamak için *Metamask* veya benzeri herhangi bir üçüncü taraf aracı kullanım gerekliliği ortadan kalkmaktadır.

Kablosuz düğümlerin sınırlı yetenekleri göz önüne alındığında, temel çalışmada izlenen yaklaşım, WSN alanında blokzincir kullanmak için etkin bir yol sunduğu testler ile ortaya konulmuştur (Sert, 2023). Bu, blokzincirin çok düzeyli yapısını kümelenmiş ağ mimarisi ile birleştirerek mümkün olmaktadır. Belirtilen temel çalışmada IoT düğüm kimlik doğrulama işlemleri için kimlik doğrulama tablosu kullanılmıştır. Bu çalışmada, konsept doğrulaması gereklilikleri nedeniyle üç düzeyli blok zinciri yapısı gösterilmektedir.

Aşağıdaki senaryo, çok düzeyli zincir yapısının detaylı bir açıklamasını yaparak düğüm kimlik doğrulaması için kullanım şeklini göstermektedir. Önerilen yaklaşım doğrulama testleri yapılması nedeniyle canlı ortamda test edilmemiş, ancak kurulan deneysel ortam ile gelecek çalışmaların temeli oluşturulmuştur. Senaryodaki temel amaç, WSN ve IoT ağlarında kullanıma uygun olabilmesi için, blokzincir yapısının değişmezliğinden (immutability) yararlanarak dağıtık özelliğini ön plana çıkarmaktır.

Kümeleme işlemi, önerinin uygulanmasındaki ilk aşamadır. Ağda hiyerarşik bir yapı oluşturmak için bir mobil baz istasyonu bulunan WSN'de literatürde yer alan bir kümeleme tekniği kullanılabilir. Sunulan yaklaşım kümeleme algoritmalarından bağımsız olarak çalışabilmektedir. Örnekte, WSN'lerin kurulumundan sorumlu olan ve ağa bağlı yüksek işlem kabiliyetine sahip son kullanıcının hiyerarşinin en üstünde olduğu ve üçüncü seviye zincirin başlatıcısı olarak görev yaptığı varsayılmıştır. Kendi WSN'leri için ikinci seviye zincirin oluşturucuları olarak görev yapan İHA'lar, üçüncü seviye başlatıldığında kendileri ile o WSN'de tasvir edilen CH'ler arasında ikinci seviye zinciri başlatır.

Ağ üzerinden veri göndermek için önce bir cihazın kimliğinin doğrulanması gerekir. Bu, düğümün kimliğini ve atanan CH'yi kimlik doğrulama tablosunda saklanan değerlerle karşılaştırarak ve ayrıca kimlik doğrulama talebinin blok özetini küme blokzinciri blok özeti ve karşılık gelen blok endeksi ile karşılaştırarak yapılır. Bu işlem, diğer ağ kümelerinde yer alan düğümler için de yapılır. Ayrıca, tüm ağın hiyerarşisini doğrulayan ek zincirler (bu öneride üçüncü seviye zincir) oluşturmak için aynı işlem tekrarlanabilir ve kimlik doğrulama tablosu değerleri ile kontrol edilerek doğrulanabilir.

3.3.2 Genişletilmiş Uygulama

Özeti açıklanan temel çalışmada kimlik doğrulama, blokzincir üzerinde tutulan çok seviyeli kimlik doğrulama tablo yapısı kullanılarak yapılmış; bu yöntem ise sınır güvenliği uygulamalarında düğümlerin devre dışı kalması ya da yer değişikliği sonucu doğrulanamama nedeniyle bağlantı kısıtını da beraberinde getirmiştir. Bununla birlikte her ne kadar kümeleme yaklaşımının öneri üzerinde herhangi bir etkisi olmadığı belirtilmişse de yaklaşım değişikliği ile kümelere üye olan düğüm sayısı değişiklikleri nedeniyle çok seviyeli doğrulama tablosunun güncellenmesi gereğini de beraberinde getirmiştir. Bu nedenle bu çalışma; belirtilen problemlerin üstesinden gelmek için Şekil 5'de sunulan blokzincir yapısında; gerçek yaşam koşulları ile de uyumlu olarak detayları aşağıdaki paragraflarda açıklanan bir yaklaşımla tasarlanmıştır.

İlk seviye blokzincir belirtildiği üzere her bir küme içerisinde CH ile o kümeye dahil düğüm noktalarından teşkil edilir ve bu zincirler üzerinde sadece bu düğümlerin kriptografik Id değerleri tutulur. İkinci seviye blokzincir CH'ler ile WSN kapsamında görevli İHA arasında kurulur. Üçüncü seviye blokzincire dahil düğümler olan MBİ ve İHA'larda herhangi bir kaynak kısıtı bulunmaması nedeniyle, sınır güvenliğini merkezi olarak kontrolden sorumlu olan MBİ, birden fazla konuşlandırıldığında tüm WSN'lerdeki konuşlandırılan IoT düğüm cihazlarının Id değerlerini konuşlandırma esnasında üçüncü seviye olan bu blokzincirde tutar ve gerektiğinde günceller.

Doğrulama tablosundan yukarıda belirtilen çalışma esaslarına geçiş ile birlikte belirtilen kısıtlar ortadan kalkmakta ve sınır güvenliği uygulamaları için elverişli bir ortam oluşmaktadır. Bu çalışma mimarisinde periyodik veri üreten IoT düğümlerinde temel olarak değişiklik olabileceği (kullanım dışı kalma ya da farklı kümeye dahil olma) varsayımı yapılmıştır. Böylelikle, literatürde belirtilen çeşitli kümeleme yaklaşımlarının tur başına küme oluşturması ya da üye düğümlerin kümelerinin değiştirilmesi ya da düğüm ilavesi durumlarına karşı dayanıklılık hedeflenmiştir.

4. DENEYSEL DEĞERLENDİRME

Bu bölümde, sınır güvenliği uygulamaları için etkin ve güvenli bir çözüm olarak önerilen blokzincir tabanlı nesnelerin interneti yaklaşımı deneysel olarak değerlendirilmiş, elde edilen bulgular sunularak performans analiz sonuçları tartışılmıştır. Bir önceki alt bölümde gereksinimler perspektifinden detaylandırılan kümeleme süreci bu çalışmanın kapsamı dışında olduğundan, bu çalışmada herhangi bir kümeleme performans analizi yapılmamış; deneysel değerlendirme blokzincir üzerine odaklandırılmıştır.

Önerinin performans analizi iki senaryo dahilinde icra edilmiştir. Bunlardan ilki senaryo kümeleme yaklaşımından bağımsız olarak sınır güvenliği maksadıyla konuşlandırılan IoT'nin kimlik doğrulama konsept geçerlemesidir; ikinci senaryo ise, doğrulanan konseptin kümeleme yaklaşımları bağımlılığını ve performansını incelemeye yöneliktir.

4.1 Senaryo 1 (Konsept Geçerleme)

Testlerin gerçekleştirilmesi maksadıyla üç seviyeli blokzincir yapısına uygun olarak senaryoların oluşturulması için uygulama geliştirilmiştir. Geliştirilen test uygulaması yordamıyla Tablo 1'de verilen eşik değerlerinde (İng. threshold) çok seviyeli blokzincir yapısına uygun olarak rastgele (İng. random) WSN'ler oluşturulmuştur. Bu sayede küme yapısından bağımsız olarak testlerin yapılması mümkün olmuştur.

Tablo 1: Eşik Değerleri

	3. Seviye	**2. Seviye**	**1. Seviye**
En az	2	2	8
En çok	4	10	72

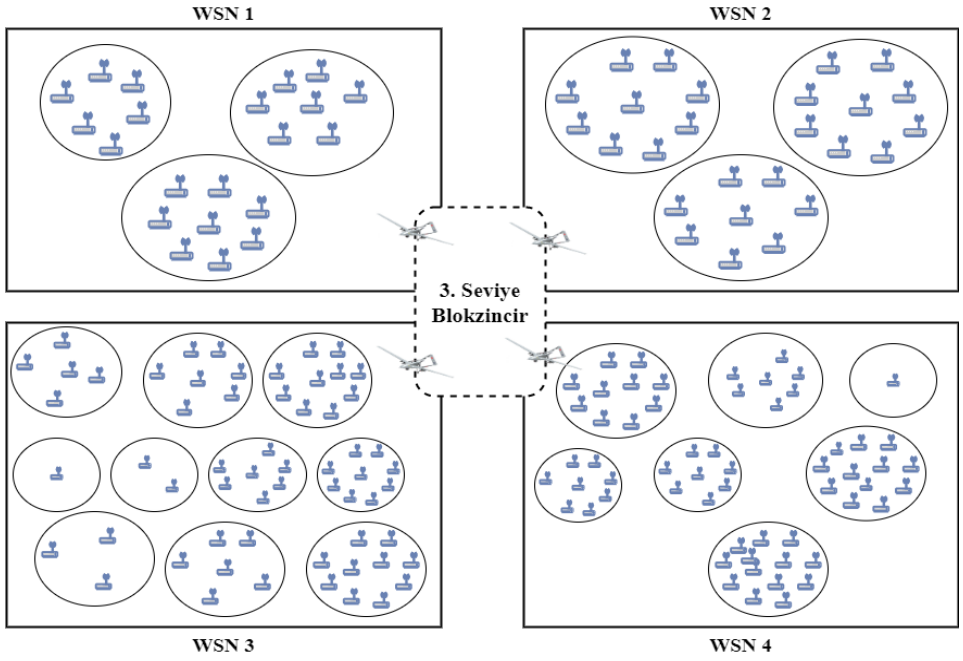
Senaryo amacının konsept doğrulaması olması nedeniyle, çok seviyeli blokzincir yaklaşımının değişen sayıda düğüm cihazı içeren WSN'ler üzerindeki çalışma ve performans analizi bu senaryo kapsamında incelenmiştir. Uygulama kapsamında özellikleri değişen farklı yapıdaki on adet test durumu ele alınmış ve durumlar senaryo yapılandırması olarak Tablo 2'de verilmiştir. Depolama ve özellikle enerji kısıtı, birinci seviye düğümlerde daha fazla öem arz etmektedir. Bu nedenle, kimlik doğrulama için kullanılan bu düğümlerde çok seviyeli blokzincir yapısının depolama alanı üzerindeki etkisi değerlendirilmiştir.

Tablo 2: Senaryo 1 Test Durumları

Durum Nu	**WSN Sayısı**	**Üçüncü Seviye Düğüm Noktası Sayısı**	**İkinci Seviye Düğüm Noktası Sayısı**	**Birinci Seviye Düğüm Noktası Sayısı**	**Toplam Düğüm Noktası Sayısı**
1	2	2	7	57	110
			6	36	110
2		2	2	17	98
			9	66	98
3		2	5	14	79
			9	47	79

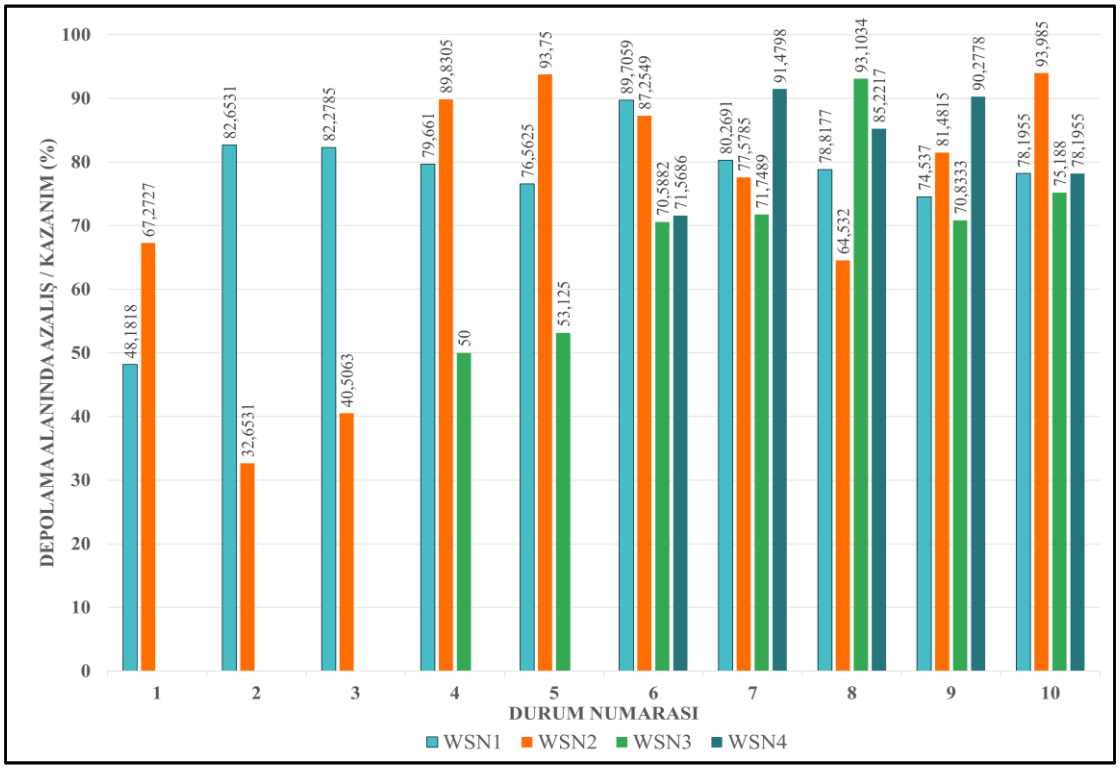
Durum Nu	WSN Sayısı	Üçüncü Seviye Düğüm Noktası Sayısı	İkinci Seviye Düğüm Noktası Sayısı	Birinci Seviye Düğüm Noktası Sayısı	Toplam Düğüm Noktası Sayısı
4	3	3	4	24	118
			2	12	118
			8	59	118
5		3	8	30	128
			3	8	128
			10	60	128
6	4	4	3	21	204
			3	26	204
			10	60	204
			7	58	204
7		4	10	44	223
			7	50	223
			9	63	223
			5	19	223
8		4	10	43	203
			9	72	203
			2	14	203
			7	30	203
9		4	8	55	216
			4	40	216
			7	63	216
			2	21	216
10		4	5	29	133
			2	8	133
			6	33	133
			5	29	133

Tablo 2'de sunulan test senaryoları geliştirilen uygulama yordamıyla elde edilmiş ve örnek olarak altı (6) numaralı durumun gösterimi Şekil 6'da verilmiştir.



Şekil 6: Durum 6 örnek gösterim.

Yapılan testler, blokzincirin tek ve çok seviyeli olması durumlarına göre yapılarak depolama alanındaki değişim (kazanım yönüyle) Şekil 7'de verilmiştir.



Şekil 7: Senaryo 1 test sonuçları.

Senaryo-1 test sonuçları analiz edildiğinde; çok seviyeli blokzincir uygulamasının tek seviyeli blokzincir uygulamasına göre depolama maliyeti yönüyle ortalama tüm senaryolarda %76 gibi büyük bir azalış getirdiği görülmektedir. Detaylı inceleme sonuçlarına göre; iki WSN konuşlandırılan ilk üç durumda birinci seviye düğüm sayısı azaldıkça bu seviyelerde tutulması gereken blokzincir boyutunun da azaldığı ve böylelikle depolama maliyetinin düştüğü / kazanımın arttığı görülmektedir. Üç WSN konuşlandırılan dört ve beşinci durum ile dört WSN konuşlandırılan diğer durumlarda da depolama maliyet azalışı doğrulanmaktadır. Bununla birlikte altı, yedi, sekiz ve dokuzuncu durumlarda konuşlandırılan düğüm sayısı artışının çok seviyeli blokzincir uygulamasını desteklediği ve sık (İng. dense) düğüm noktası konuşlandırılan ağlarda önerilen yaklaşım sonucu kazanımın oldukça arttığı tespit edilmiştir.

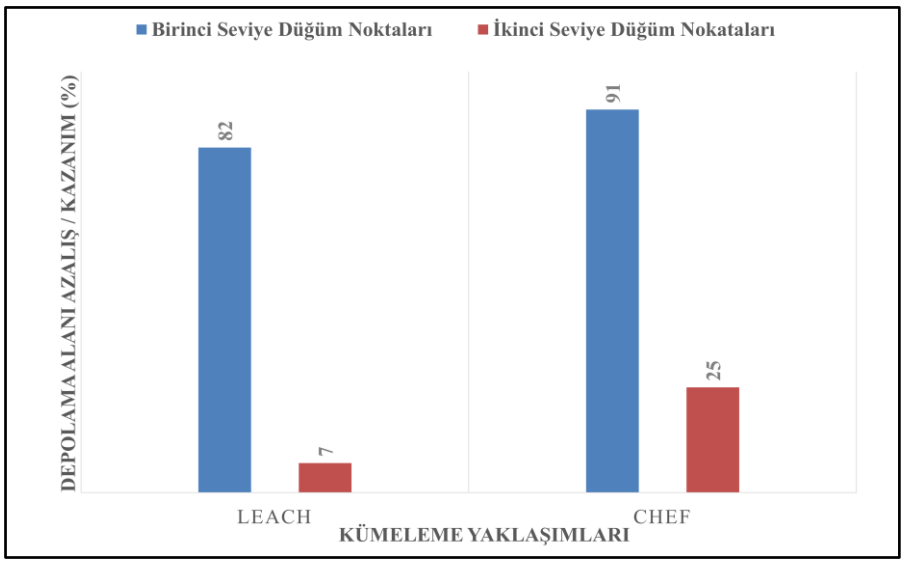
4.2 Senaryo 2 (Bağımlılık ve Performans Analizi)

Önerilen yöntemin, kümeleme yaklaşımı kaynaklı herhangi bir hassasiyetinin olup olmadığı, literatürde karşılaştırmalarda sıklıkla kullanılan iki yöntem olan Düşük-Enerji Adaptif Kümeleme Hiyerarşisi (Low-Energy Adaptive Clustering Hierarchy-LEACH) algoritması (Heinzelman vd., 2000) ile Bulanık Mantık Küme Başı Seçimi (Cluster Head Election using Fuzzy) algoritması (Kim vd., 2008) kullanılarak analiz edilmiştir. Yapılan değerlendirmeye esas senaryo yapılandırması Tablo 3'de verilmiştir.

Tablo 3: Senaryo 2 Yapılandırma

İlgi (Konuşlandırma) Alanı	Kümeleme Algoritması	Toplam Düğüm Sayısı
1000 x 1000 (m.)	LEACH (Heinzelman vd., 2000)	100
	CHEF (Kim vd., 2008)	

Çok seviyeli blokzincir yönteminin belirtilen yaklaşımlarda değerlendirilebilmesi maksadıyla, kaynak çalışmalardan farklı olarak her iki yaklaşım için baz istasyonları MBİ olacak şekilde ve CH ile MBİ arası iletişim doğrudan (direkt) yapılacak şekilde güncellenmiştir. Literatürde sıklıkla başvurulan bu yaklaşımlar, küme ve küme başı seçimini her tur (round) için tekrarlamaları nedeniyle periyodik veri toplayan uygulamalar için tasarlanmıştır. Bu nedenle yapılan testler sonucu bulgular; yaklaşımların her tur (İng. round) küme sayılarının değişmesi nedeniyle, konuşlandırılan bütün düğüm noktalarının çalışır durumda olduğu (devre dışı kalmadığı) bir tur değeri baz alınarak birinci ve ikinci seviyelerdeki blokzincir depolama alanındaki değişim yönüyle Şekil 8'de gösterilmiştir.



Şekil 8: Bağımlılık ve performans analizi sonuçları.

Şekil 8 bağımlılık ve performans analizi sonuçları incelendiğinde, LEACH ve CHEF yaklaşımlarının her ikisinde de çok seviyeli blokzincir yaklaşımı olumlu sonuçlar vererek depolama maliyetini düşürmüştür. Depolama maliyet azalışı, CHEF algoritması için her iki seviyede de LEACH algoritmasına göre üstünlük göstermiştir. Yapılan analiz sonucu belirtilen üstünlüğün algoritmaların çalışma şekilleri gereğince oluşturdukları küme sayıları farklılığından kaynaklandığı; daha fazla küme oluşturan CHEF yaklaşımında birinci seviye düğüm sayısı değerinin azaldığı ve bu nedenle kazanımın da doğru orantılı olarak arttığı yapılan tespitler arasındadır.

Elde edilen bulgulara göre; önerinin CHEF algoritması tarafında daha iyi sonuçlar vermesi, önerinin CHEF'e daha uygun olmasından ziyade bu yaklaşımın ürettiği küme sayısındaki artışa bağlıdır. Algoritma değişikliği sonucunda CHEF yaklaşımı yerine farklı bir kümeleme algoritması da kullanılsa, WSN içerisinde aynı/benzer sayıda küme üretiyor ise benzer şekilde birinci seviye (üye) düğüm sayısı azalarak aynı ya da benzer depolama alanı maliyet azalışı elde edileceği değerlendirilmektedir.

5. SONUÇLAR

Blokzincir teknolojisi kullanılarak IoT ağları ve önemli bir bileşeni olan WSN'lerdeki güvenlik sorunlarının bir kısmı dağıtık (merkezi olmayan) bir yaklaşımla çözülebilmektedir. Bu çalışmada, sınır güvenliğinde etkin ve güvenli bir çözüm olarak blokzincir tabanlı nesnelerin interneti kullanımı önerilmiştir. Yapılan önerinin, deneysel olarak değerlendirilmesi ve elde edilen bulgular sonucunda ümit vaat eden bir yaklaşım olduğu sonucuna varılmıştır. Bununla birlikte, gerçek hayatta genel kullanım olan tek seviyeli / katmanlı blokzincir kullanımının yetersiz olabileceği ve gerçek hayattaki vakaların çoğunda enerji tüketimi ile depolama ve işlem gücünün birincil belirleyici olması durumunda en iyi seçenek olmayabileceği de gösterilmiştir.

Çalışmanın bulguları, depolama ihtiyaçları yönüyle öneriyi geçerlemektedir. Kümeleme yaklaşımı, çok seviyeli blokzincir için birincil ön koşul olan bir düğüm hiyerarşisi oluşturduğu sürece, uygulanacak kümeleme yaklaşımına bir bağımlılık tespit edilmemiştir. Bununla birlikte, her ne kadar bir bağımlılık olmasa da kümeleme metodolojisi kaynaklı olarak kümelerin üye düğüm sayısı değişiklikleri nedeniyle, farklı seviyelerdeki zincirlerin boyutları da kümeleme yaklaşımına uygun olarak değişecektir. Düğüm sayısının artmasına bağlı olarak blokzincir saklama alanı ihtiyacı artmasına rağmen, testlerde de görüldüğü üzere düğüm sayısının artmasıyla doğrulama tablosu boyutu artmaktadır. Bu nedenle blokzincir boyutunun artış seviyesinin ihmal edilebilir seviyede olduğu değerlendirilmekle beraber açık araştırma sahası olarak karşımıza çıkmaktadır.

Gelecek araştırma alanları yönüyle önerinin ölçeklenebilirlik analizini hedefleyen yoğun ağlar için zincir oluşturma ve güncelleme sürelerine ilişkin deneyler yapılabilir. Ayrıca, özellikle periyodik veri toplayan IoT ve WSN'ler için, kümeleme hiyerarşisinin farklı seviyelerinde elde edilen verinin blokzincir üzerinde tutulma maliyeti ve özellikle kötücül (İng. malicious) düğüm olduğu durumlarda çok seviyeli blokzincir ve kimlik doğrulama yaklaşımının WSN veri iletimindeki verim (İng. throughput) ve gecikme (İng. latency) üzerine etkileri ile işlem gücü gereksinimleri ve enerji tüketimine etkileri gelecek araştırma konuları arasındadır.

TEŞEKKÜR

Bu çalışmanın yapılarak genişletilmiş sürümün hazırlanması yönünde yapıcı eleştirileri için Havacılık ve Uzay Teknolojilerindeki Son Gelişmeler (İng. Recent Advances in Air and Space Technologies) 2023 (RAST23) Konferansı'nın anonim eleştirmenleri ile Blokzincir verimliliği konusunda deneysel

yardımları, konsept doğrulama tartışmaları ve taslağı büyük ölçüde geliştiren katkı ve yorumları için Hacettepe Üniversitesi Bilgisayar Mühendisliği doktora öğrencisi Ozan Zorlu'ya teşekkür ederim.

KAYNAKLAR

Agrawal, S., ve Das, M. L. (2011). Internet of Things — A paradigm shift of future Internet applications. In *Nirma University International Conference on Engineering*. https://doi.org/10.1109/nuicone.2011.6153246

Ahmed, M. T. A., Hashim, F., Hashim, S. J., ve Abdullah, A. (2022). Hierarchical blockchain structure for node authentication in IoT networks. *Egyptian Informatics Journal*, *23*(2), 345–361. https://doi.org/10.1016/j.eij.2022.02.005

AlRubaiei, M., Jassim, H. S., Sharef, B. T., Safdar, S., Sharef, Z. T., ve Malallah, F. L. (2020). Current vulnerabilities, challenges and attacks on routing protocols for mobile ad hoc network: a review. In *Elsevier eBooks* (pp. 109–129). Elsevier BV. https://doi.org/10.1016/b978-0-12-818287-1.00012-7

Ani, U., Watson, J. D., Nurse, J. R. C., Cook, A. M., ve Maple, C. (2019). A review of critical infrastructure protection approaches: improving security through responsiveness to the dynamic modelling landscape. In *The Internet of Things*. https://doi.org/10.1049/cp.2019.0131

Bhattacharya, M., ve Roy, A. (2020). Smart Border Security System Using Internet of Things. In *Communications in computer and information science*. Springer Science+Business Media. https://doi.org/10.1007/978-3-030-66763-4_23

Capossele, A., Cervo, V., De Cicco, G., ve Petrioli, C. (2015). Security as a CoAP resource: An optimized DTLS implementation for the IoT. In *International Conference on Communications*. https://doi.org/10.1109/icc.2015.7248379

Cui, Z., Xue, F., Zhang, S., Cao, Y., Zhang, W., ve Chen, J. (2020). A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN. *IEEE Transactions on Services Computing*, 1. https://doi.org/10.1109/tsc.2020.2964537

Danzi, P., Kalør, A. E., Stefanovic, C., ve Popovski, P. (2019). Delay and Communication Tradeoffs for Blockchain Systems With Lightweight IoT Clients. *IEEE Internet of Things Journal*, *6*(2), 2354–2365. https://doi.org/10.1109/jiot.2019.2906615

Developer Guides — Bitcoin. (b.t.). https://developer.bitcoin.org/devguide/

Dujak, D., ve Sajter, D. (2019). Blockchain Applications in Supply Chain. In *Ecoproduction* (pp. 21–46). Springer International Publishing. https://doi.org/10.1007/978-3-319-91668-2_2

Dworkin, M. J. (2007). *Recommendation for block cipher modes of operation :* https://doi.org/10.6028/nist.sp.800-38d

Eyal, I., Gencer, A. E., Sirer, E. G., ve Van Renesse, R. (2016). Bitcoin-NG: a scalable blockchain protocol. In *Networked Systems Design and Implementation* (pp. 45–59). https://arxiv.org/pdf/1510.02037

Faris, M., Mahmud, M. N., Salleh, M. F. M., ve Alnoor, A. (2023). Wireless sensor network security: A recent review based on state-of-the-art works. *International Journal of Engineering Business Management*, *15*, 184797902311572. https://doi.org/10.1177/18479790231157220

Fatima, N., Siddiqui, S., ve Ahmad, A. (2021). IoT based Border Security System using Machine Learning. In *2021 International Conference on Communication, Control and Information Sciences (ICCISc)*. https://doi.org/10.1109/iccisc52257.2021.9484934

Fraga-Lamas, P., Fernández-Caramés, T. M., Suárez-Albela, M., Castedo, L., ve González-López, M. (2016). A Review on Internet of Things for Defense and Public Safety. *Sensors*, *16*(10), 1644. https://doi.org/10.3390/s16101644

Hammi, M. T., Livolant, E., Bellot, P., Serhrouchni, A., ve Minet, P. (2017). A lightweight IoT security protocol. In *HAL (Le Centre pour la Communication Scientifique Directe)*. Le Centre pour la Communication Scientifique Directe. https://doi.org/10.1109/csnet.2017.8242001

Hankerson, D., Menezes, A., ve Vanstone, S. A. (2004). Guide to Elliptic Curve Cryptography. In *Springer eBooks*. Springer Nature. https://doi.org/10.1007/b97644

Hassan, M. N., Islam, S. M. S., Faisal, F., Semantha, F. H., Siddique, A. H., ve Hasan, M. (2020). An IoT based Environment Monitoring System. In *International Conference Intelligent Sustainable Systems*. https://doi.org/10.1109/iciss49785.2020.9316050

Heinzelman, W. R., Chandrakasan, A. P., & Balakrishnan, H. (2000). *Energy-efficient communication protocol for wireless microsensor networks*. https://doi.org/10.1109/hicss.2000.926982

Iansiti, M., ve Lakhani, K. R. (2017). The Truth about Blockchain. Harvard Business Review, 95(1), 118–127.

Jammes, F., ve Smit, H. A. (2005). Service-Oriented Paradigms in Industrial Automation. *IEEE Transactions on Industrial Informatics*, *1*(1), 62–70. https://doi.org/10.1109/tii.2005.844419

Khan, A., Laghari, A. A., Shaikh, Z. A., Dacko-Pikiewicz, Z., ve Kot, S. (2022). Internet of Things (IoT) Security With Blockchain Technology: A State-of-the-Art Review. *IEEE Access*, *10*, 122679–122695. https://doi.org/10.1109/access.2022.3223370

Khan, A. U., Javaid, N., Khan, M. S., ve Ullah, I. (2022). A blockchain scheme for authentication, data sharing and nonrepudiation to secure internet of wireless sensor things. *Cluster Computing*. https://doi.org/10.1007/s10586-022-03722-z

Khan, R., Khan, S. U., Zaheer, R., ve Khan, S. B. (2012). Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. In *Frontiers of Information Technology*. https://doi.org/10.1109/fit.2012.53

Kim, J., Park, S., Han, Y., & Chung, T. (2008). CHEF: Cluster Head Election mechanism using Fuzzy logic in Wireless Sensor Networks. In *International Conference on Advanced Communication Technology*. Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/icact.2008.4493846

Kothmayr, T., Schmitt, C., Hu, W., Brünig, M., ve Carle, G. (2013). DTLS based security and two-way authentication for the Internet of Things. Ad Hoc Networks, 11(8), 2710–2723. https://doi.org/10.1016/j.adhoc.2013.05.003

Labib, N. S., Danoy, G., Musial, J., Brust, M. R., ve Bouvry, P. (2019). Internet of Unmanned Aerial Vehicles—A Multilayer Low-Altitude Airspace Model for Distributed UAV Traffic Management. *Sensors*, *19*(21), 4779. https://doi.org/10.3390/s19214779

Laouira, M. L., Abdelli, A., Othman, J. B., ve Kim, H. (2021). An Efficient WSN Based Solution for Border Surveillance. *IEEE Transactions on Sustainable Computing*, *6*(1), 54–65. https://doi.org/10.1109/tsusc.2019.2904855

Liu, Y., Wang, K., Lin, Y., ve Xu, W. (2019). LightChain: A Lightweight Blockchain System for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, *15*(6), 3571–3581. https://doi.org/10.1109/tii.2019.2904049

Moniruzzaman, M., Khezr, S. N., Yassine, A., ve Benlamri, R. (2020). Blockchain for smart homes: Review of current trends and research challenges. *Computers & Electrical Engineering*, *83*, 106585. https://doi.org/10.1016/j.compeleceng.2020.106585

Mubarakali, A. (2021). An Efficient Authentication Scheme Using Blockchain Technology for Wireless Sensor Networks. *Wireless Personal Communications*, *127*(1), 255–269. https://doi.org/10.1007/s11277-021-08212-w

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

Nazib, R. A., ve Moh, S. (2021). Energy-Efficient and Fast Data Collection in UAV-Aided Wireless Sensor Networks for Hilly Terrains. *IEEE Access*, *9*, 23168–23190. https://doi.org/10.1109/access.2021.3056701

Panwar, M., ve Kumar, A. (2015). Security for IoT: An effective DTLS with public certificates. In *International Conference on Advances in Computer Engineering and Applications*. https://doi.org/10.1109/icacea.2015.7164688

Popescu, D., Stoican, F., Stamatescu, G., Chenaru, O., ve Ichim, L. (2019). A Survey of Collaborative UAV–WSN Systems for Efficient Monitoring. *Sensors*, *19*(21), 4690. https://doi.org/10.3390/s19214690

Rivest, R. L., Shamir, A., ve Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342

Saez, M., Maturana, F. P., Barton, K., ve Tilbury, D. M. (2018). Real-Time Manufacturing Machine and System Performance Monitoring Using Internet of Things. *IEEE Transactions on Automation Science and Engineering*, *15*(4), 1735–1748. https://doi.org/10.1109/tase.2017.2784826

Sert, S. A., Onur, E., ve Yazici, A. (2015). Security attacks and countermeasures in Surveillance Wireless Sensor Networks. In *Advanced Industrial Conference on Telecommunications*. https://doi.org/10.1109/icaict.2015.7338546

Sert, S. A., Alchihabi, A., ve Yazici, A. (2018). A Two-Tier Distributed Fuzzy Logic Based Protocol for Efficient Data Aggregation in Multihop Wireless Sensor Networks. *IEEE Transactions on Fuzzy Systems*, *26*(6), 3615–3629. https://doi.org/10.1109/tfuzz.2018.2841369

Sert, S. A. (2023). A Multi-Level Blockchain-based Node Authentication Approach for UAV-assisted Wireless Sensor Networks. In International Conference on Recent Advances in Air and Space Technologies. https://doi.org/10.1109/RAST57548.2023.10197943

Shelby, Z., Hartke, K., ve Bormann, C. (2014). The Constrained Application Protocol (CoAP). In *RFC*. https://doi.org/10.17487/rfc7252

Tazibt, C. Y., Bekhti, M., Djamah, T., Achir, N., ve Boussetta, K. (2017). Wireless sensor network clustering for UAV-based data gathering. In *HAL (Le Centre pour la Communication Scientifique Directe)*. https://doi.org/10.1109/wd.2017.7918154

Uddin, A., Stranieri, A., Gondal, I., ve Balasurbramanian, V. (2019). A Lightweight Blockchain Based Framework for Underwater IoT. *Electronics*, *8*(12), 1552. https://doi.org/10.3390/electronics8121552

Wu, A., Lee, J., Khan, I., ve Kwon, Y. (2021). CrowdQuake+: Data-driven Earthquake Early Warning via IoT and Deep Learning. In *2021 IEEE International Conference on Big Data (Big Data)*. https://doi.org/10.1109/bigdata52589.2021.9671971

Yang, Z., Yue, Y., Yang, Y., Peng, Y., Wang, X., ve Liu, W. (2011). Study and application on the architecture and key technologies for IOT. In *International Conference on Model Transformation*. https://doi.org/10.1109/icmt.2011.6002149

Yaqoob, I., Ahmed, E., Hashem, I. a. T., Ahmed, A. I. A., Gani, A., Imran, M., ve Guizani, M. (2017). Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. *IEEE Wireless Communications*, *24*(3), 10–16. https://doi.org/10.1109/mwc.2017.1600421

Yazici, A., Koyuncu, M., Sert, S. A., ve Yilmaz, T. (2019). A Fusion-Based Framework for Wireless Multimedia Sensor Networks in Surveillance Applications. *IEEE Access*, *7*, 88418–88434. https://doi.org/10.1109/access.2019.2926206

Zhu, Y., Qin, Y., Zhou, Z., Song, X., Liu, G., ve Chu, W. C. (2018). Digital Asset Management with Distributed Permission over Blockchain and Attribute-Based Access Control. In IEEE International Conference on Services Computing. https://doi.org/10.1109/scc.2018.00032