Tekle E., Can K. (2026). HashDrone: Otonom İHA Sürü Ağları için Hafif Blokzincir Tabanlı Veri bütünlüğü Doğrulama Mimarisi. EMO Bilimsel Dergi, 16(2), 91-101.

Makale Türü: Araştırma Makalesi
Makale Gönderim Tarihi: 26 Ocak 2026
Makale Kabul Tarihi: 25 Mayıs 2026

HashDrone: Otonom İHA Sürü Ağları için Hafif Blokzincir Tabanlı Veri Bütünlüğü Doğrulama Mimarisi

HashDrone: A Lightweight Blockchain-Based Integrity Verification Architecture for Autonomous UAV Swarm Networks

Elif Tekle[1], *Kaan Can*[2*]

[1]Yönetim Bilişim Sistemleri, İktisadi ve İdari Bilimler Fakültesi,
Atatürk Üniversitesi, Erzurum, Türkiye
eliftekle4@gmail.com

[2] Elektrik-Elektronik Mühendisliği Bölümü, Mühendislik Fakültesi,
Atatürk Üniversitesi, Erzurum, Türkiye
kaan.can@atauni.edu.tr

Özet

Bu çalışmada, dağıtık İnsansız Hava Araçları (İHA) sürü sistemlerinde sensör verilerinin güvenli ve güvenilir biçimde bütünlüğünü sağlamak amacıyla, hafif bir blokzincir tabanlı veri bütünlüğü doğrulama mekanizması olan HashDrone algoritması önerilmektedir. Tasarım bilimi araştırma metodolojisi izlenerek geliştirilen HashDrone, SHA-256 karma (hash) algoritmasını kullanan, Python tabanlı ve kaynak açısından verimli bir blokzincir mimarisi sunmakta olup, kısıtlı donanım kaynaklarına sahip gömülü platformlarda çalışabilecek şekilde tasarlanmıştır. Benzetim sonuçları, kullanılan SHA-256 algoritmasının deterministik yapısının doğal bir sonucu olarak, HashDrone mimarisinin veri manipülasyonu girişimlerine karşı anında yüksek duyarlılıkla tespit imkânı sunduğunu ve teorik olarak milisaniye mertebesinde doğrulama potansiyeline sahip olduğunu göstermektedir. Ayrıca, önerilen yöntemin geleneksel uzlaşma protokollerinin getirdiği mesajlaşma ve hesaplama yükünü barındırmaması sebebiyle, kaynakları kısıtlı otonom İHA sürü sistemlerinde güvenli veri yönetimi için etkili ve uygulanabilir bir alternatif çözüm olduğu ortaya konmuştur.
Anahtar kelimeler: Blokzincir, SHA-256, Veri Bütünlüğü, Hafifletilmiş Doğrulama, İnsansız Hava Araçları.

Abstract

This paper proposes the HashDrone algorithm, a lightweight blockchain-based data integrity verification mechanism designed to ensure secure and reliable sensor data integrity in distributed Unmanned Aerial Vehicle (UAV) swarms. Developed following the design science research methodology, HashDrone employs a Python-based, resource-efficient blockchain architecture using the SHA-256 hashing algorithm, enabling deployment on constrained embedded platforms. Due to the deterministic nature of the SHA-256 algorithm, simulation results show that the HashDrone architecture provides instantaneous, high-sensitivity detection against data tampering attempts while maintaining a theoretical millisecond-level verification potential. Furthermore, by avoiding the computational and messaging overhead of traditional consensus protocols, the proposed method offers an effective and viable alternative for secure data management in resource-constrained autonomous UAV swarm systems.
Keywords: Blockchain, SHA-256, Data Integrity, Lightweight Verification, Unmanned Aerial Vehicles.

1. Giriş

İHA'lar, savunma, afet müdahalesi ve altyapı izleme gibi alanlarda yaygın olarak kullanılmaktadır [1,2]. Ancak mevcut sürü haberleşme mimarilerinin büyük bir bölümü merkezi sunuculara dayanmaktadır. Bu durum, söz konusu sistemleri siber saldırılara, veri manipülasyonuna ve tek nokta arızalarına karşı savunmasız hâle getirmektedir [3]. Son on yılda, İHA teknolojisindeki gelişmeler, operasyonel yaklaşımları tek araçlı görevlerden Çok Etmenli Sistemler (ÇES) ve sürü zekâsı temelli yapılara doğru yönlendirmiştir. İHA sürüleri; ölçeklenebilirlik, verimlilik ve dayanıklılık açısından önemli avantajlar sunarak geniş alan haritalama, arama-kurtarma operasyonları, çevresel izleme ve askerî keşif gibi kritik görevlerin yüksek performansla icra edilmesini mümkün kılmaktadır. Bu tür sistemler iş birliği içinde çalıştığından, etkinlikleri büyük ölçüde GPS koordinatları, termal görüntüler ve telemetri bilgileri gibi toplanan ve paylaşılan verilerin doğruluğuna, bütünlüğüne ve güvenilirliğine bağlıdır. Bu avantajlara rağmen, mevcut İHA sürü haberleşme mimarilerinin büyük bir bölümü veri depolama, doğrulama ve koordinasyon işlemleri için merkezi bulut sunucularına veya yer kontrol istasyonlarına dayanmaktadır [4]. Bu tür merkezi yapılar sistem yönetimini kolaylaştırsa da ciddi güvenlik açıklarını beraberinde getirmektedir. En önemli tehditlerden biri, bir saldırganın merkezi veritabanına yetkisiz erişim sağlayarak uçuş kayıtlarını veya görev açısından kritik keşif verilerini sonradan değiştirdiği veri manipülasyonudur. Bir diğer kritik sorun ise güvenilmez iletişim (spoofing) saldırılarıdır. Bu durumda ele geçirilmiş bir İHA, bağlı olduğu ağa sahte veya uydurma veriler enjekte ederek yanlış bilgilerin

sürü geneline yayılmasına ve sistem güvenilirliğinin ciddi biçimde azalmasına neden olabilmektedir. Bu güvenlik açıklarını gidermek amacıyla, merkeziyetsiz mimari, kriptografik değiştirilemezlik özelliği ve dağıtık doğrulama mekanizmaları sayesinde blokzincir teknolojisi umut vadeden bir çözüm olarak öne çıkmıştır. Kriptografik Karma (hash) fonksiyonları aracılığıyla veri bloklarının birbirine bağlanması ve işlemlerin birden fazla düğüm tarafından doğrulanması sayesinde, blokzincir yapıları manipülasyona dayanıklı ve denetlenebilir veri depolama imkânı sunmaktadır. Ancak, mevcut blokzincir tabanlı İHA sürü mimarileri incelendiğinde, çeşitli pratik sınırlamalar ortaya çıkmaktadır. Önerilen çözümlerin büyük bir kısmı, başlangıçta finansal uygulamalar için tasarlanmış blokzincir yapılarını benimsemektedir. Bu durum yüksek hesaplama yükü, büyük depolama gereksinimleri ve kayda değer gecikmelerle sonuçlanmaktadır. Özellikle blokzincir destekli İHA formasyon kontrolüne odaklanan çalışmalar, Linux tabanlı işlemciler (örneğin Raspberry Pi) ve yerleşik veri depolama için katı hâl sürücüleri gibi katı donanım gereksinimleri rapor etmektedir [5-7]. Bu gereksinimler, faydalı yük ağırlığını önemli ölçüde artırarak uçuş süresini, enerji verimliliğini ve görev dayanımını olumsuz etkilemektedir. Dolayısıyla mevcut yaklaşımlar, ölçeklenebilirlik açısından ciddi zorluklarla karşı karşıya kalmakta ve hafif veya kaynakları kısıtlı İHA platformları için çoğu zaman uygun olmamaktadır. Belirtilen duruma örnek olarak; Can ve Başçi, lider-takipçi (L-T) formasyonlarında lider İHA'nın takipçilere seyrüsefer verilerini ilettiği senaryoları analiz etmişlerdir [8]. Bu yapıda, lider İHA'yı hedef alan bir donanım arızası veya siber saldırı, "Lider Kaybı" durumuna yol açarak tüm sürünün operasyonel kabiliyetini yitirmesine neden olmaktadır. Benzer şekilde literatürde, tüm sensör verilerinin tek bir merkezi sunucuda toplandığı mimarilerin "Tek Nokta Arızası" (Single-Point-of-Failure) riski taşıdığı vurgulanmıştır [9]. Merkezi mimarilerin temel problemi, güvenin tek bir otoriteye (sunucu veya lider) devredilmesidir. Bu otoritenin ele geçirilmesi, ağ genelindeki tüm verilerin güvenilirliğini ve bütünlüğünü anında geçersiz kılmaktadır.Ayrıca mevcut literatürde, geleneksel blokzincir sistemlerinin aşırı işlem yükü ve donanım gereksinimlerini hafifletirken veri bütünlüğü ve manipülasyona karşı dayanıklılığı koruyabilen hafif bir blokzincir tabanlı doğrulama mimarisinin eksikliği dikkat çekmektedir [10-12].Bu boşluğun giderilmesi, gerçek dünya koşullarında güvenli ve enerji verimli sürü İHA dağıtımlarının mümkün kılınması açısından kritik öneme sahiptir.

Bu motivasyon doğrultusunda, bu çalışmada sürü İHA sistemleri için özel olarak tasarlanmış, SHA-256 tabanlı, optimize edilmiş ve hafif bir veri bütünlüğü doğrulama mekanizması önerilmektedir. Önerilen yaklaşım, blokzincirin temel güvenlik avantajlarını korurken hesaplama yükünü ve işlem gecikmesini tasarımsal olarak en aza indirmeyi hedeflemekte olup, kaynakları kısıtlı gömülü İHA donanımları üzerinde çalışabilecek yalın bir yapıda geliştirilmiştir. Nesnelerin İHA İnterneti (İHAİ (Internet of Drones)) paradigması bağlamında, bu çalışma mevcut İHA sürü mimarilerini incelemekte, veri katmanlarındaki yapısal zafiyetleri analiz etmekte ve hafif bir kriptografik yapının operasyonel performanstan ödün vermeden güvenliği nasıl etkin biçimde artırabileceğini ortaya koymaktadır.

2. Yöntem ve sistem mimarisi

Bu bölüm, önerilen "HashDrone" protokolünün matematiksel modellemesi, donanım arayüzleri ve kriptografik algoritmaları hakkında ayrıntılı bir açıklama sunmaktadır. Makale, bir bilgi teknolojisi yapısının geliştirilmesi ve test edilmesine odaklanan Tasarım Bilimi Araştırması (DSR) metodolojisi çerçevesinde yapılandırılmıştır.

2.1. Blokzincir tabanlı doğrulama mekanizması tasarımı

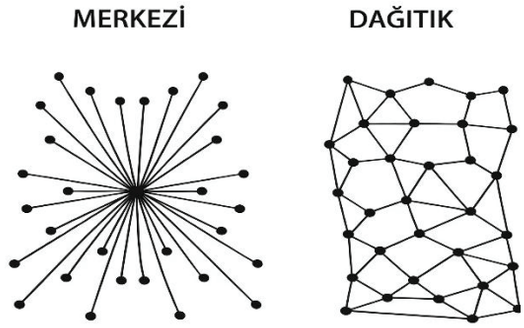
Önerilen otonom İHA sürü ağı, Graf Teorisi prensiplerine dayalı olarak yönlü ve bağlantılı bir çizge yapısı şeklinde modellenmiştir. Buna bağlı olarak; temel bağlantıya ait matematiksel sistem aşağıdaki şekilde ifade edilmektedir [11-13];

$$\mathcal{G} = (V, \mathcal{E}) \tag{1}$$

burada $\mathcal{V} = \{\mathrm{d}_1, \mathrm{d}_2, \ldots, \mathrm{d}_\mathrm{n}\}$ düğüm kümesini ifade etmekte olup, sürü içerisindeki her bir otonom İHA'yı; d_i sensör verisi üreten ve blokzincir ağına katılım sağlayan bir düğümü temsil etmektedir [11-13]. Ayrıca, $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ kenar kümesini ifade etmekte olup, İHA'lar arasındaki şifrelenmiş veri iletişim kanallarını temsil etmektedir. Bununla birlikte sistem, her bir düğüm tarafından üretilen verilerin bütünlüğünü yerel (her bir İHA üzerinde) hesaplamalar aracılığıyla güvence altına almakta ve merkezi bir otoriteye olan ihtiyacı ortadan kaldırmaktadır. Öte yandan, İHA sürüsünün önceden tanımlanmış formasyonu gerçekleştirebilmesi için, ilgili birinci dereceden konsensus tabanlı formasyon denklemi aşağıdaki şekilde tanımlanabilir [14];

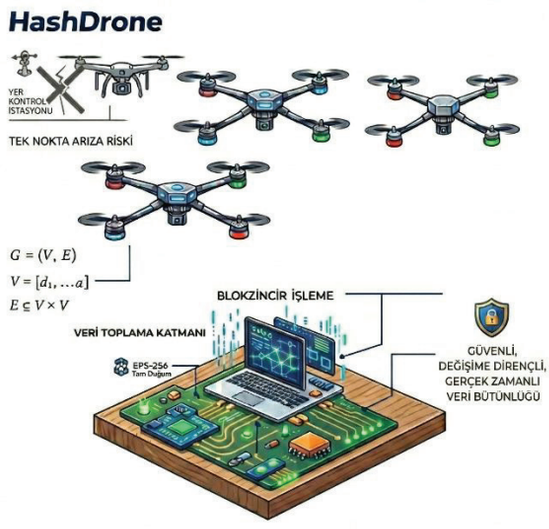
$$u_i = -\sum_{j \in N_i} a_{ij}(x_i - x_j) \tag{2}$$

burada; a_{ij} komşuluk matrisini, N_i İHA sayısını ve $x_i = [x_1^T \ldots x_N^T]^T$ ifadesi ise *i.* İHA'nın konum vektörünü temsil etmektedir. Çoğu çalışmalarda, mevcut İHA sürü haberleşme ve kontrol mimarileri ağırlıklı olarak iki paradigma üzerine kuruludur. Bunlar, merkezi bir yapı olan yer kontrol istasyonu modeli ve L–T modelleridir. Bu yaklaşımlar, doğası gereği merkezi karar verme mekanizmaları içerdiklerinden, ölçeklenebilirlik sorunları ve tek nokta arızası sınırlamaları ile karşı karşıya kalmaktadır. Bu yapısal sınırlamaların üstesinden gelebilmek amacıyla, bu çalışmada HashDrone algoritması önerilmiştir. HashDrone yöntemi; tek nokta arızası risklerini ortadan kaldıran, dağıtık ve hafif bir blokzincir tabanlı veri doğrulama mekanizması sunmakta olup; sürü İHA içerisinde güvenli, manipülasyona dayanıklı ve gerçek zamanlı veri bütünlüğünü sağlamaktadır. Ayrıca, yukarıda bahsedilen sürü İHA'larına ait formasyon oluşturma sürecinde kullanılan ağ topoloji yöntemleri Şekil 1'de gösterilmiştir.



Şekil 1: Merkezi ve dağıtık ağ mimarileri.

Bununla birlikte, ilgili makale kapsamında önerilen blokzincir destekli sürü İHA iletişim sisteminin mimarisi Şekil 2'de sunulmuştur.



Şekil 2: Önerilen blok zincirinin mimarisi.

2.2. Dijital veri katmanını hedef alan siber tehditler

İHA ağlarına yönelik güvenlik tehditleri giderek fiziksel katmandan (örneğin; sinyal karıştırma) veri bütünlüğü saldırılarına doğru kaymakta olup tespit edilmesi çok daha zordur. Temel güvenlik üçlüsü olan gizlilik, bütünlük ve erişilebilirlik içinde bütünlük; İHA uygulamaları için en kritik ve en az korunan bileşendir. Literatürde bilinen ve bu makalede de vurgulanan başlıca tehditler sırasıyla bu bölümde sunulmuştur.

A. Yanlış veri enjeksiyonu (False data ınjection (FDI))

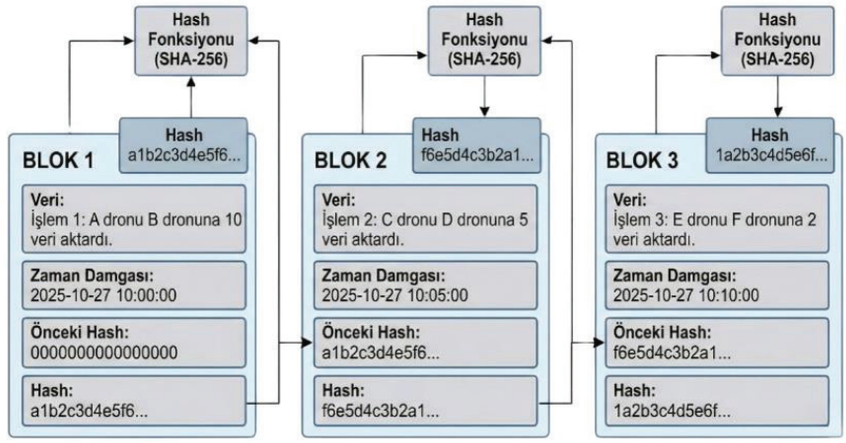
Bu tür tehditler, ağ içinde bir tür "kimlik hırsızlığı" olarak düşünülebilir. Bir saldırgan sürüye sızar, kimliği belirsiz bir İHA gibi davranır ve sisteme yanlış GPS koordinatları veya telemetri verileri göndermeye başlayabilir. Özellikle askeri bağlamda bu durum, kritik bir güvenlik zafiyeti oluşturmakta olup sistemi müttefik unsurların düşman olarak yanlış tanımlanmasına (misidentification) neden olabilir**.** Temelde sürü, sahte verilere dayanarak görev açısından kritik ve geri döndürülemez kararlar almaya başlar ve bu kararlar, ağın iç güven mekanizmalarını istismar eden kötü niyetli bir düğüm tarafından sisteme enjekte edilen bir tür yanıltıcı veri enjeksiyonu (deceptive data injection) olarak tanımlanabilir [7,8].

B. Veri müdahalesi (Data tampering)

Görev sonrası analizlerde kullanılan uçuş günlüklerinin, veritabanı düzeyinde geriye dönük olarak değiştirilebilmesi mümkündür. Mevcut şifreleme protokolleri (örneğin TLS/SSL) verilerin iletim sırasında korunmasını sağlasa da depolanmış verilerin değiştirilemezliğini garanti edemezler. Bu durum, işlem tamamlandıktan sonra verilerin manipüle edilmesiyle 'tarihi yeniden yazma' riskini temsil eder. TLS/SSL gibi geleneksel güvenlik protokolleri, verinin A noktasından B noktasına (aktarılan veriler) hareket ederken üstün koruma sağlarken, bu koruyucu kalkanlar veri depolandığında ve statik hale geldiğinde (duraklı veri) etkisiz hale gelir. Bir saldırgan, geriye dönük olarak uçuş kayıtlarına müdahale edebilir ve operasyonun gerçeklerini tamamen gizleyebilir. Bu sebeple HashDrone, tanımlanan güvenlik açığını kaydedildiği anda veriyi kriptografik olarak mühürleyerek kapatır ve 'değişmez' hale getirir. Bu nedenle, sistem tarihin sahtekarlığına asla izin vermez.

2.3. Blokzincir tabanlı çözümler ve araştırma boşluğu

Merkezi mimarilerden kaynaklanan ve yukarıda belirtilen zafiyetleri azaltmak amacıyla, Dağıtık Defter Teknolojileri (DDT (Distributed Ledger Technologies)) ve blokzincir tabanlı yaklaşımlar son yıllarda giderek artan biçimde çalışılmakta ve akademi çevrelerince araştırılmaktadır [15-19]. Blokzincir, verilerin ağ düğümleri tarafından kolektif olarak doğrulandığı ve kriptografik özet (hash) fonksiyonları aracılığıyla birbirine bağlandığı, değiştirilemez ve kurcalamaya dayanıklı bir defter yapısı sunmaktadır. Bununla birlikte, mevcut literatürün eleştirel bir incelemesi önemli bir sınırlamayı ortaya koymaktadır. Örneğin; blokzincir güvenlik ve veri bütünlüğünü artırsa da özellikle İş İspatı (Proof-of-Work- PoW) gibi geleneksel uzlaşım mekanizmaları (örneğin: Bitcoin ve Ethereum gibi ağlarda kullanıldığı üzere), aşırı hesaplama yükü, yüksek enerji tüketimi ve gecikme kısıtları nedeniyle sürü İHA sistemleri için uygun görülmemektedir [9,10]. Bir araştırma boşluğu olarak İHA'lar (özellikle mini/mikro sınıflar), sınırlı batarya kapasitesine ve düşük işlem gücüne sahip gömülü sistemlerdir. Bu sebeple, mevcut literatürde kritik bir eksiklik bulunmaktadır. Örneğin, finansal blokzincirlerdeki yüksek hesaplama yükü ve enerji tüketimini ortadan kaldırırken, veri bütünlüğünü kriptografik olarak garanti edebilen, hafif ve aviyonik sistemlerle uyumlu bir protokolün eksikliğidir.



Şekil 3: Basit bir blokzincirin temel yapısı.

Mevcut çalışmaların büyük bir kısmı ya teorik simülasyonlarla sınırlı kalmakta ya da pratik donanım kısıtlarını göz ardı etmektedir. Buna karşılık, önerilen HashDrone protokolü, literatürde belirtilen söz konusu boşluğu gidermeyi amaçlamaktadır. Bu çalışma, deterministik SHA-256 tabanlı bir hash zinciri mimarisi önererek, geleneksel bir uzlaşım mekanizmasına (örneğin madencilik) ihtiyaç duymadan, doğrulama odaklı yapısıyla gecikme ve hesaplama yükünü tasarımsal olarak hafifletmektedir. Bu yaklaşım, merkezi bir sunucuya olan bağımlılığı ortadan kaldırmakta ve veriyi kaynağında (uç/edge seviyesinde) kriptografik olarak mühürleyerek kaynakları kısıtlı sürü İHA ağları için güvenli bir doğrulama altyapısı sunmaktadır.

2.4. Donanım ve yazılım mimarisi

Kaynakları kısıtlı aviyonik sistemlerin verimliliğini artırmak amacıyla HashDrone mimarisi, Uç Bilişim (Edge Computing) prensibine dayalı olarak iki fiziksel katmana ayrılmıştır [13,14]. Bunlardan ilki olan Veri Toplama Katmanı (Data Acquisition Layer), fiziksel dünyadan ham verilerin toplanmasından sorumludur. Prototip tasarımında Arduino mikrodenetleyiciler kullanılmıştır. Sistem; GPS modülünden, Ataletsel Ölçüm Birimlerinden (IMU) ve çevresel sensörlerden gelen analog sinyalleri işleyerek bunları sayısal veri paketlerine dönüştürmektedir. İkinci katman ise, sistemin kriptografik güvenliğinin sağlandığı Blokzincir İşleme Katmanı (Blockchain Processing Layer)'dır. Her bir İHA üzerinde konumlandırılan Raspberry Pi, bir "Tam Düğüm (Full Node)" olarak görev yapmaktadır. Python tabanlı yazılım, verileri seri port üzerinden almakta ve bu verileri blokzincir algoritmasına entegre etmektedir.

2.5. Kriptografik yapı ve algoritma tasarımı

Sistemin güvenlik çekirdeği, veri değiştirilemezliğini sağlamak amacıyla tek yönlü hash fonksiyonlarına dayanmaktadır. HashDrone, yüksek çakışma direnci sunan *Secure Hash Algorithm – 256 bit* (SHA-256) algoritmasını kullanmaktadır [16-19].

A. Blok yapısı ve hash fonksiyonu

Blokzincirdeki her birB_i bloğu, bir zaman damgası (T_i), benzersiz bir indeks (I_i), sensör verileri (D_i) ve bir önceki bloğun hash değeri (H_{i-1}) bileşenlerini içermektedir. B_i bloğunun dijital parmak izi olarak tanımlanan H_i değeri, aşağıdaki matematiksel ilişkisi kullanılarak hesaplanmaktadır [16-19].

$$H_i = SHA\text{-}256\,(I_i \parallel T_i \parallel D_i \parallel H_{i-1}) \quad (3)$$

Burada $\parallel$ sembolü, veri alanlarının birleştirilmesini (concatenation) temsil etmektedir. Bu özyinelemeli yapı sayesinde (blok Hash'in H_{i-1}'e bağımlı olmasıyla), zincirdeki önceki herhangi bir blokta meydana gelen en küçük bit düzeyindeki değişiklik, bir zincirleme reaksiyonu (çığ etkisi) tetikleyerek kendisinden sonraki tüm blokların hash değerlerini geçersiz kılmaktadır [16]. Ayrıca, bir blokzincirin temel yapısı Şekil 3'te gösterildiği şekilde temsil edilebilir.

B. Deterministik serileştirme

Dağıtık sistemlerde veri tutarlılığının sağlanması kritik öneme sahiptir. Python sözlük yapılarının sırasız (unordered) doğası nedeniyle, Deterministik Serileştirme (Deterministic Serialization) yöntemi ***sort_keys=True*** parametresi kullanılarak uygulanmaktadır. Bu sayede, aynı verinin farklı düğümlerde farklı hash çıktıları üretmesi engellenmektedir. Veriler; anahtarlar alfabetik olarak sıralandıktan sonra standart bir JSON metni hâline getirilerek serileştirilmektedir.

2.6. Bütünlük doğrulama mekanizması ve matematiksel tespit süreci

Önerilen sistemin güvenilirliği, deftere her yeni blok eklendiğinde çalıştırılan ***is_chain_valid ()*** algoritması ile sağlanmaktadır. Bu algoritma, blokzinciri en güncel bloktan genesis bloğuna kadar dolaşarak, iki temel koşulu sağlayacak şekilde matematiksel olarak doğrular. Birinci temel koşul olan Veri Bütünlüğü Koşulu (Data Integrity Condition), mevcut bloğun saklanan hash $\boldsymbol{H_i}$ değeri ile, bloğun içeriğinden yeniden hesaplanan hash değerinin birebir aynı olması gerektiğini ifade

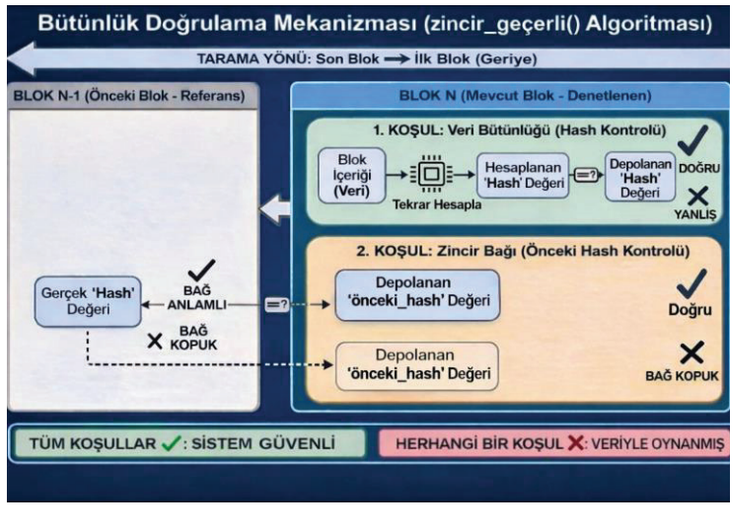
eder. Bu doğrulama, bloğun içsel verilerinin oluşturulmasından sonra değiştirilmediğini veya kurcalanmadığını garanti etmektedir. Ayrıca, bu durumun matematiksel gösterimi aşağıdaki gibi ifade edilebilir [16-19].

$$H_i = SHA\text{-}256\,(I_i \parallel T_i \parallel D_i \parallel H_{i-1}) \quad (4)$$

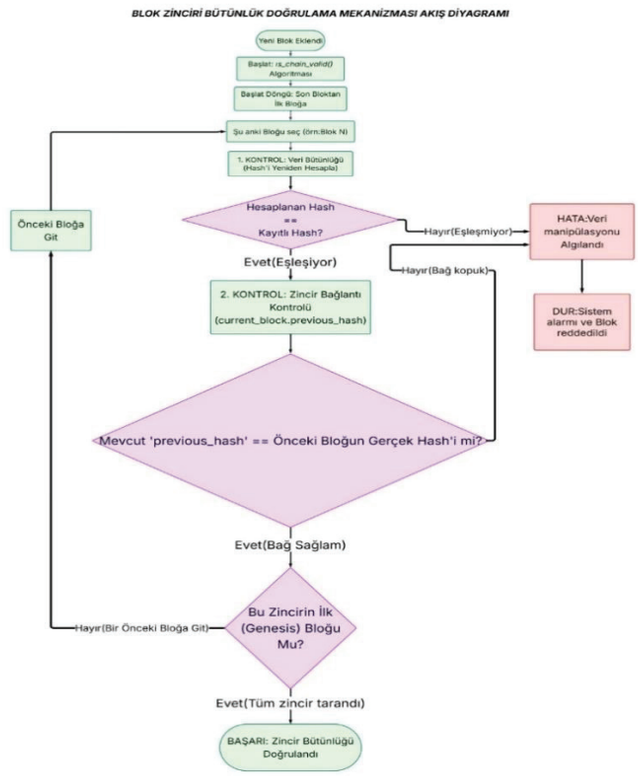
İkinci temel koşul olan Zincir Bağlantı Koşulu (ZBK (Chain Linkage Condition)) kapsamında, mevcut bloğun **previous_hash** alanının, zincirde kendisinden önce gelen bloğun hesaplanan hash değeriyle birebir aynı olması gerekmektedir [16-19]. Bu koşul, ardışık bloklar arasındaki kriptografik zincir bağlantısını garanti altına almaktadır. ZBK'nin matematiksel gösterimi aşağıdaki eşitlikte verildiği şekilde yazılabilir [16-19].

$$B_i.previous\_hash = B_{i-1}.hash \quad (5)$$

Bu iki koşuldan herhangi birinin sağlanmaması, sistem tarafından "Veri Kurcalama (Data Tampering)" olarak derhal tespit edilmekte ve işaretlenmektedir. Bununla birlikte, ilgili algoritmaya ait blokzincir veri yapısı ve akış şeması sırasıyla Şekil 4 ve 5'te sunulmuştur.



Şekil 4: Blokzincir veri yapısı ve bütünlük doğrulaması.



Şekil 5: Blockchain veri yapısı ve zincir bütünlüğü doğrulama akış şeması.

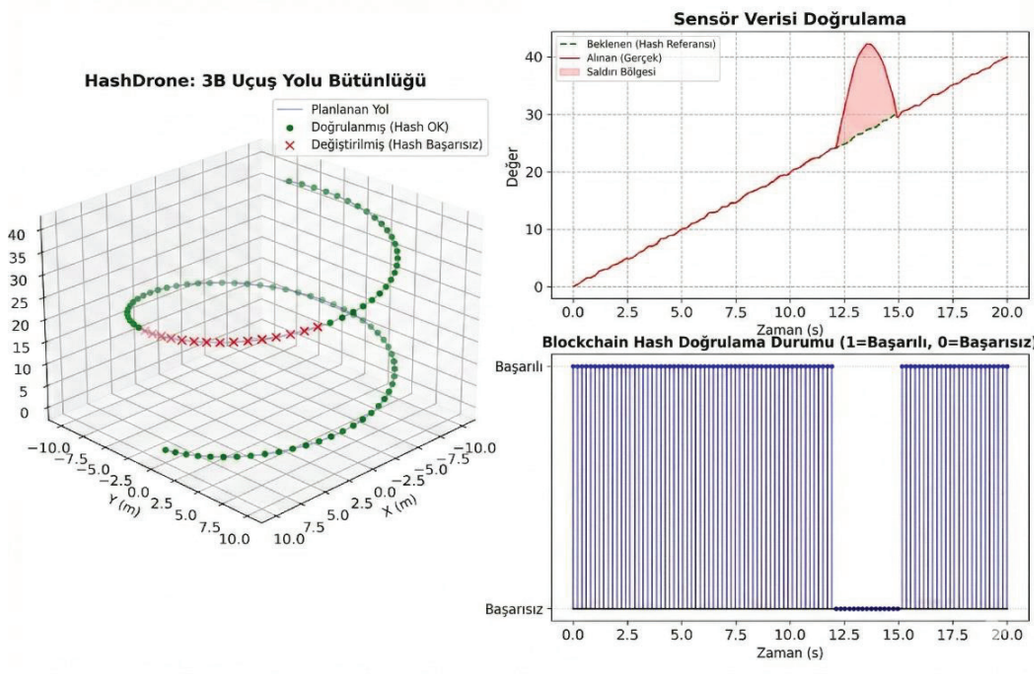
3. Simülasyon sonuçları

Bu bölümde, önerilen HashDrone protokolünün performansı, veri bütünlüğü yetenekleri ve saldırı tespit etkinliği sunulmaktadır. Protokol, veri yapısının ve temel şifreleme işlevselliğinin test edilmesi amacıyla Python tabanlı bir benzetim ortamında değerlendirilmiştir. Bu benzetim, önerilen blokzincir mimarisinin uygulama katmanındaki (application-layer) geçerliliğini doğrulamayı amaçlayan bir Kavram Kanıtı Proof of Concept- (PoC) niteliğindedir. Ağ gecikmeleri ve donanım senkronizasyonu gibi fiziksel/veri bağı katmanı dinamikleri basitleştirilmiş bir model üzerinden ele alınarak, öncelikli olarak şifreleme ve bütünlük doğrulama mantığına odaklanılmıştır. Ayrıca bu bölümde, benzetim senaryosu, blokzincir oluşturma süreci ve gerçekleştirilen güvenlik değerlendirmelerinden elde edilen nicel sonuçlar ayrıntılı olarak açıklanmaktadır. Önerilen sistemin uygulanabilirliğini test etmek amacıyla, Erzurum Atatürk Üniversitesi Yerleşkesi'nin coğrafi sınırları (Enlem: 39°, Boylam: 41°) içerisinde çok-etmenli bir görev senaryosu tasarlanmıştır [20]. Ayrıca, ilgili çalışmaya ait benzetim videosuna buradan erişilebilir.

Python tabanlı benzetim ortamında, farklı donanım özelliklerine göre özelleştirilmiş üç farklı otonom İHA'ya ait bilgiler Tablo 1'de tanımlanmıştır. Tüm İHA'lar, verileri eşzamansız olarak üretmiş ve merkeziyetsiz ağa (P2P ağ) yayınlamış ve daha sonra, söz konusu veriler HashDrone protokolü tarafından işlenmiştir.

Tablo 1: Simülasyonda tanımlanan ajanlar ve görev tanımları.

İHA Adı	*İHA Numarası*	*Görev*
Kargo İHA'sı	İHA-1	Lojistik yük verilerini ve teslimat zaman damgalarını simüle eder.
Gözlemci İHA	İHA-2	Güvenlik gözetimi amacıyla gerçek zamanlı GPS koordinatları üretir.
Çevresel İzleme İHA'sı	İHA-3	Bölgeden meteorolojik verileri (sıcaklık/nem) toplar.



Şekil 6: 3B uçuş yörüngesinde veri bütünlüğü ve sensör doğrulama sonuçları.

***Test 1:* Zincir bağlantısı ve veri sürekliliği**

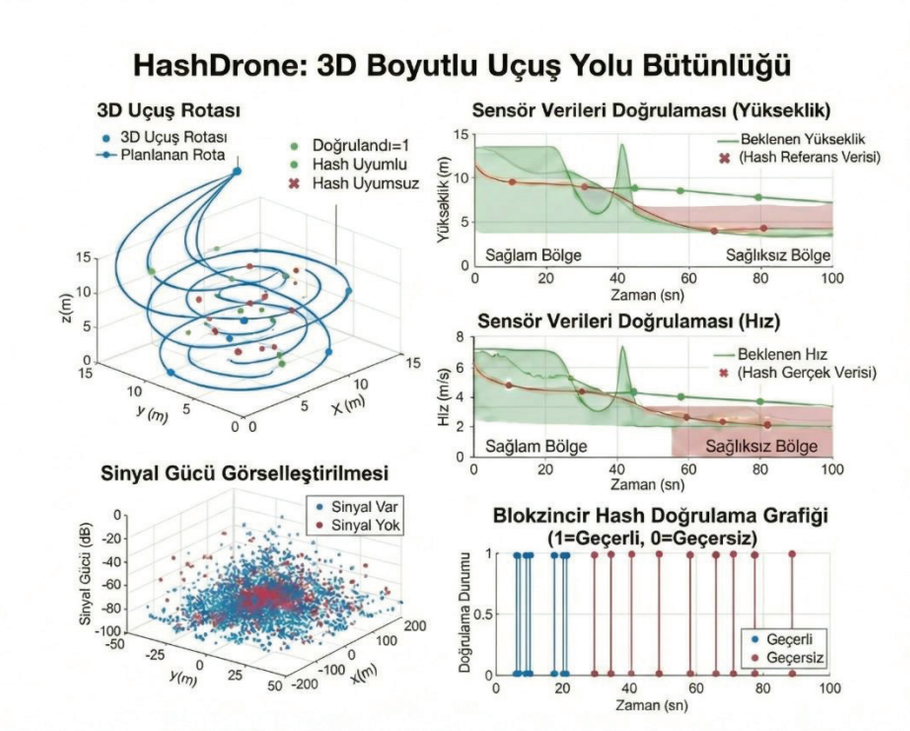
Test 1 kapsamında, sistemin temel işlevi olan değiştirilemez (immutable) bir zincir oluşturma yeteneği test edilmiştir. Simülasyonun başlatılmasıyla birlikte sistem, önce "Genesis Block" olarak adlandırılan ve ***previous_hash*** değeri "**0**" olan başlangıç bloğunu üretmiştir. Ardından, heterojen İHA'lardan kaynaklanan 15'ten fazla veri paketi başarıyla zincire dâhil edilmiştir. İlk olarak Şekil 6'da Test 1'e ait simülasyon sonuçları sunulmuştur. İlgili görselde; HashDrone sisteminin uçuş sırasındaki veri bütünlüğünü koruma ve siber saldırıların anlık olarak tespit etme kapasitesini göstermektedir.

Görsel, simüle edilmiş bir saldırı senaryosu altında sistemin davranışını üç farklı perspektiften incelemektedir. İlk olarak şekilde sol kısımda bulunan görsel, İHA'ların 3 boyutlu uzaydaki (X, Y, Z eksenleri boyunca) tırmanma manevrasını temsil etmektedir. Yeşil noktalar (doğrulanmış); blokzincir üzerindeki hash kayıtlarıyla eşleşen, güvenli uçuş verilerini göstermektedir. Kırmızı çarpılar ise; sisteme yapılan veri enjeksiyon saldırısı sonucu manipüle edilen koordinatları temsil etmektedir. Sistem; bu noktaların hash değerlerinin zincirdeki önceki bloklarla uyuşmadığını tespit ederek bunları "güvensiz" olarak işaretlemiştir.

Bununla birlikte şekilde sağ üst taraftaki görsel; sistemin zaman serisi boyunca sensör verilerindeki sapmaları analiz etmektedir. 12.5 ila 15. saniyeler aralığında "Saldırı Bölgesi" olarak işaretlenen bölgede, İHA'dan elde edilen ham ölçüm verisi kırmızı eğri ile gösterilmiş olup, blokzincir üzerinde doğrulanmış referans veriyi temsil eden yeşil eğriden anlamlı düzeyde ayrışmaktadır. Gözlemlenen bu tutarsızlık, sistemin sensör veri akışına yönelik Ortadaki Adam (Man in the Middle) saldırılarını veya dışarıdan müdahale tabanlı manipülasyon girişimlerini etkili biçimde algılayıp izole edebildiğini doğrulamaktadır. Son olarak şekilde sağ alt görselde sunulan grafik, sistemin SHA-256 algoritması kullanarak yaptığı doğrulama sonucunun ikili (binary) durumunu göstermektedir.

Burada;

- Pass (1): Veri bütünlüğünün sağlandığı normal uçuş durumunu temsil etmektedir.
- Fail (0): Saldırı anında (t=12.5-15 sn), hesaplanan hash değeri ile beklenen hash değeri uyuşmadığı için doğrulama durumu 0 (Başarısız) seviyesine düşmüştür.
- Saldırı sona erdiğinde sistemin tekrar güvenli duruma (1) dönmesi, HashDrone'un dinamik ve dayanıklı yapısını ortaya koymuştur.



Şekil 7: İHA'nın blokzincir hash doğrulama görseli: 3B uçuş yörüngesi ve mekânsal doğrulama (sol üst); sensör verileri doğrulaması: yükseklik ve hız (sağ üst ve orta grafikler); sinyal gücü (sol alt grafik); blokzincir hash doğrulama analizi (sağ alt grafik).

Şekil 7'de, önerilen yönteme ait İHA'nın üç boyutlu bir yörünge boyunca uçuş sırasında elde edilen çeşitli simülasyon sonuçları sunulmuştur. İlk olarak, şekilde sol üst görselde sunulan ve ilgili İHA'ya ait üç boyutlu uçuş yörüngesi ve mekânsal doğrulama çıktıları sunulmuştur. Bu görselde mavi hat planlanan yörüngeyi temsil ederken, üzerindeki noktalar blokzincir tabanlı kontrol noktalarını (checkpoints) ifade etmektedir. Ayrıca şekilde yeşil noktalar ile sunulan hash uyumluluk durumu ise; İHA'nın o andaki konum verisinin, blokzincirdeki hash değeriyle eşleştiğini, yani verinin değiştirilmediğini göstermektedir. Diğer taraftan kırmızı noktalar ile sunulan hash uyumsuzluğu ise; konum verisinde bir sapma veya dışarıdan bir müdahale olduğunu ve sistemin bunu tespit ederek "doğrulama başarısız" uyarısı verdiğini göstermektedir. İkinci olarak, şekilde sağ üst ve ortada sunulan görselde, İHA'nın sensör verilerinin yükseklik ve hıza bağlı olarak sensör verilerinin doğrulaması gerçekleştirilmiştir. Bu grafikler, telemetri verilerinin zaman ekseninde güvenilirliğini analiz etmektedir. Sağlam bölge olarak tasvir edilen yeşil alan; sensörden gelen hız veya yükseklik verilerinin beklenen değerler ve blokzincir referans verisi ile örtüştüğü güvenli zaman aralıklarını temsil etmektedir. Diğer taraftan sağlıksız bölge olarak sunulan kırmızı alan; kırmızı çizgi ile gösterilen "Hash Referans Verisi" veya "Gerçek Veri"nin beklenen değerden saptığı anları göstermektedir. Sapma başladığı anda sistemin, ilgili veriyi blokzincir kayıtları ile karşılaştırarak olası veri manipülasyonunu veya sensör kaynaklı hatalı ölçümü tespit ettiği gözlemlenmiştir. Şekilde sol alt görselde İHA'nın ilgili yöntem altında sahip olduğu sinyal gücüne ait görsel sunulmuştur. Bu üç boyutlu saçılım grafiği, uçuş hacmi içerisindeki sinyal kalitesini RSSI- desibel (dB) cinsinden

göstermektedir. Ayrıca, mavi ve kırmızı noktaların dağılımı, İHA'nın konumuna göre iletişim ağının güvenilirliğini ve veri paketlerinin blokzincire işlenmesi sırasındaki sinyal kararlılığını analiz etmek için kullanılmıştır.

Son olarak görselde sağ alt kısımda sunulan grafik, Blokzincir Hash Doğrulama Grafiği'ni temsil etmektedir. Bu sistemin karar mekanizmasını temsil etmektedir. Burada;

- 1 Değeri (Geçerli): O saniyedeki veri bloğunun SHA-256 imzası, bir önceki bloğun hash değeri ile uyumludur. Bu da zincirin kırılmadığı anlamına gelmektedir.
- 0 Değeri (Geçersiz): Zincirde bir kopukluk veya veride değişiklik tespit edildiğini ifade etmektedir. Grafik; zaman çizelgesinde hangi saniyelerde veri bütünlüğünün bozulduğunu net bir şekilde raporlamaktadır. Sonuç olarak Test 1'e ait çıktılar aşağıdaki gibi doğrulanmıştır.

• Her yeni bloğun, kendisinden önceki bloğa ait hash değerini doğru bir şekilde aldığı doğrulanmıştır.

• Verilerin zaman damgasına bağlı olarak kronolojik sırada başarıyla zincirlendiği gözlemlenmiştir.

• Farklı türdeki heterojen verilerin (JSON formatında) tek ve standartlaştırılmış bir defter (ledger) yapısı altında başarıyla birleştirildiği doğrulanmıştır. Ayrıca, ilgili teste karşılık gelen akış diyagramı senaryosu Şekil 5'te sunulmuştur.

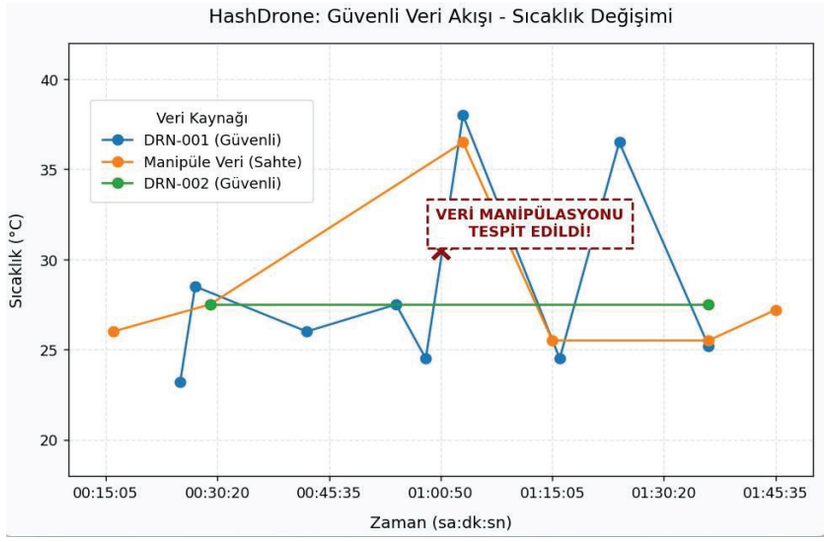
Test 2: **Veri tahrifatı saldırısı ve tespit analizi**

Test 2'de, protokolün güvenliğinin doğrulanması açısından en kritik aşama olan "Veri Kurcalama" testi gerçekleştirilmiştir. Bu senaryoda, kötü niyetli bir aktörün veritabanına sızarak geçmişe ait bir kaydı değiştirmeye çalıştığı varsayılmıştır. Bir saldırı senaryosu olarak aşağıdaki varsayımlar dikkate alınmıştır;

Zincir uzunluğu 15 bloğa ulaştığında, harici bir müdahale simüle edilmiş ve 5 numaralı bloktaki "Sıcaklık" verisi 20 °C'den 50 °C'ye değiştirilmiştir. Ayrıca, ilgili senaryoya ait görsel Şekil 8'de sunulmuştur. Diğer taraftan sistemin doğrulama algoritması (*is_chain_valid*), zincir boyunca iterasyon yaparken Şekil 8'de sunulan matematiksel tutarsızlığı tespit etmiştir. Blok #5 isimli bloğun içeriği değiştirildiği için, SHA-256 algoritması tamamen farklı bir hash değeri üretmiş ve bu durum $H_5' \neq H_{5(\text{stored})}$ şeklinde ifade edilmiştir.

Şekil 8. İHA'nın blokzincir veri yapısı, işlem akışı ve zincir bütünlüğü doğrulama mekanizmaları.

Bu değişiklik, Blok #6 isimli blok tarafından referans alınan *previous_hash* değeriyle çeliştiği ve bu sebeple, $H_5' \neq B_6.previous\_hash$ durumunun meydana geldiği görülmüştür. Böylece test sonuçlarından, sistemin zincirdeki kopmayı anında tespit ettiği ve tüm zinciri "GEÇERSİZ (INVALID)" olarak işaretlediği gözlemlenmiştir. Dolayısıyla sistem, kullanılan SHA-256 algoritmasının deterministik doğasının matematiksel bir sonucu olarak, zincir kopmalarını başarılı bir şekilde tespit etmiş ve veriye yapılan manipülasyon girişimlerini anında geçersiz kılmıştır. Ayrıca Şekil 9, HashDrone protokolünün veri bütünlüğünü sağlama ve olası veri manipülasyonlarını tespit etme performansını simülasyon ortamında gerçekleştirilen test sonuçları aracılığıyla açıkça göstermektedir. Zaman ekseninde iki farklı İHA'ya (DRN-001 ve DRN-002) ait sıcaklık ölçümleri sunulmuş olup, normal çalışma koşullarında sensör verilerinin fiziksel olarak tutarlı bir eğilim izlediği gözlemlenmektedir. Ancak, belirli bir zaman diliminde gerçekleştirilen yapay veri müdahalesi, sıcaklık değerinde ani ve olağan dışı bir sıçrama ile temsil edilmiştir. Bu müdahale, HashDrone'un doğrulama algoritması (*is_chain_valid*) tarafından anında tespit edilmiş ve ilgili veri zinciri geçersiz olarak işaretlenmiştir. Görselde, ağa dahil olan DRN-001 (mavi) ve DRN-002 (yeşil) kodlu insansız hava araçlarının ilettiği güvenli ve doğrulanmış telemetri verileri olağan seyrinde devam etmektedir. Ancak "00:45:35" zaman diliminden sonra, sisteme sızmaya çalışan bir tehdit unsuru tarafından sıcaklık verisinin kasıtlı olarak yüksek gösterildiği bir manipülasyon girişimi (turuncu çizgi) başlatılmıştır. HashDrone güvenlik algoritması, gelen bu sahte verinin doğrulama aşamalarını (hash/şifreleme uyumsuzluğu) geçememesi ve kabul edilebilir eşik değerlerini aşması üzerine "01:00:50" sularında duruma müdahale etmiştir. Ayrıca grafikteki kırmızı "X" işareti, sahte verinin tespit edilip sistemden izole edildiği ve ağ güvenliğinin sağlandığı anı göstermektedir.



Şekil 9: HashDrone protokolünün güvenli veri akışı-sıcaklık değişim grafiği.

4. Tartışma

Bu çalışma, geleneksel finansal blokzincir mekanizmalarının gerektirdiği yüksek işlem gücü ve enerji tüketiminden ayrışarak, aviyonik sistemlerin kaynak kısıtlarına özel olarak uyarlanmış, hafif ve kriptografik olarak daha güvenli bir veri kayıt protokolü olan HashDrone'u önermektedir. Çalışmanın temel amacı, merkezi bir otoriteye ihtiyaç duymaksızın, toplanan verilerin kökenini ve bütünlüğünü matematiksel olarak garanti altına almaktır. DDT tabanlı HashDrone protokolü, otonom sürü İHA sistemlerinin dijital veri katmanındaki kritik güvenlik açıklarını gidermek amacıyla tasarlanmış ve sistematik olarak değerlendirilmiştir. Önerilen yaklaşım, gerçekçi görev senaryoları altında çalışan heterojen İHA ajanlarını içerecek şekilde, Atatürk Üniversitesi Kampüsü topolojisi üzerinde gerçekleştirilen kapsamlı simülasyonlar aracılığıyla doğrulanmıştır. Değerlendirme sonuçları; HashDrone protokolünün, düşük hesaplama yükü ve minimum gecikme sağladığını, aynı zamanda veri özgünlüğünü ve bütünlüğünü de etkin biçimde garanti ettiğini göstermektedir. Finansal uygulamalar için geliştirilmiş geleneksel blokzincir çerçevelerinin, özellikle yüksek işlem gücü, enerji tüketimi ve depolama gereksinimleri dayatan iş ispatı tabanlı sistemlerin aksine HashDrone protokolü, kaynakları kısıtlı aviyonik platformlara özel olarak tasarlanmış, SHA-256 tabanlı hafif bir kriptografik yapı benimsemektedir. Merkezi bir otorite ihtiyacını ortadan kaldırarak ve aşırı donanım bağımlılıklarını önleyerek, önerilen protokol toplanan İHA verilerinin doğrulanabilir kökenini ve değiştirilemezliğini tamamen merkeziyetsiz bir yapı içerisinde garanti altına almaktadır. Genel olarak HashDrone protokolü, İHA sürülerinde veri kaydı ve doğrulama için ölçeklenebilir, enerji verimli ve güvenli bir yerel mimari sunmakta olup, gelişmekte olan İHAİ paradigması kapsamında pratik uygulamalar için de son derece uygun bir çözüm teşkil etmektedir. Bu çalışmanın bulguları, hafif DDT tabanlı çözümlerin, güvenlik gereksinimleri ile gerçek dünya İHA donanım sınırlamaları arasındaki boşluğu doldurabildiğini ve sürü tabanlı hava sistemleri için geleneksel blokzincir yaklaşımlarına uygulanabilir bir alternatif sunduğunu ortaya koymaktadır.

4.1. Mevcut mimariler ile karşılaştırmalı analiz

Geliştirilen HashDrone protokolü, literatürde yaygın olarak önerilen İş İspatı (Proof of Work, PoW) ve akıllı sözleşme (smart contract) tabanlı karmaşık yapılara kıyasla üç temel avantaj sunmaktadır.

* **Gecikme ve gerçek zamanlı tepkisellik:** [21] numaralı çalışmada önerilen blokzincir mimarisinde, blok onay süreleri nedeniyle 1,8 saniyelik bir gecikme gözlemlenmiştir. Buna karşılık, HashDrone protokolünde kullanılan SHA-256 tabanlı yapı, ağ uzlaşımına (network consensus) ihtiyaç duymadan çalıştığı için tasarımsal olarak milisaniye mertebesinde doğrulama yapabilme potansiyeline sahiptir. Bu yalın mimari yaklaşım, özellikle çarpışma önleme gibi refleksif manevralar sırasında sistemde darboğaz oluşma riskini en aza indirerek İHA'ların operasyonel çalışabilirliğini desteklemektedir.

* **Enerji ve donanım verimliliği:** Geleneksel blokzincir mimarilerinde, her bir İHA'nın tam düğüm olarak çalışabilmesi için SSD depolama birimi ve yüksek işlem gücü taşıması gerekliliği, batarya ömrünü (havada kalış süresini) doğrudan azaltmaktadır. Buna karşılık HashDrone doğrulama mekanizması, Uç Bilişim prensibini benimseyerek ek ve ağır yardımcı donanımlara ihtiyaç duymadan, mevcut aviyonik kartlar üzerinde çalışabilmektedir [22,23]. Bu sayede sistem, "enerji-verimli güvenlik (energy-efficient security)" sağlamaktadır.

* **Merkeziyetsiz güven mimarisi:** HashDrone protokolü, L-T tabanlı sürü mimarilerinde doğası gereği bulunan tekil hata noktası (single point of failure) riskini ortadan kaldırmaktadır. Bunu, her bir İHA'nın kendi verisini kriptografik olarak imzaladığı, tamamen dağıtık bir tasarım benimseyerek başarmaktadır. Böylece, herhangi bir tek lider düğüme bağımlı olmaksızın, veri güvenliği ve güvenilirliği garanti altına alınmaktadır.

5. Sonuç

Bu çalışmada, otonom sürü İHA sistemlerinin dijital veri katmanındaki kritik güvenlik açıklarını ele almak amacıyla DDT tabanlı HashDrone protokolü geliştirilmiş ve sistematik olarak değerlendirilmiştir. Elde edilen sonuçlar, mevcut literatür, yaygın yaklaşımlar ve çalışmanın özgün hedefleri bağlamında analiz edilmiştir. Önerilen protokol, heterojen İHA ajanları kullanılarak Atatürk Üniversitesi Kampüsü topolojisi üzerinde gerçekleştirilen simülasyon deneyleri ile doğrulanmıştır. Python tabanlı simülasyon çalışmaları sonucunda elde edilen bulgular, HashDrone protokolünün, ortaya çıkan İHAİ paradigması kapsamında veri bütünlüğünü ve güvenilirliğini sağlamaya yönelik ölçeklenebilir, güvenli ve yerel bir mimari çözüm sunduğunu göstermektedir.

6. Gelecek çalışmalar ve öneriler

HashDrone protokolünün mevcut başarımı, simülasyon ve prototip ortamlarında doğrulanmıştır. Çalışmanın kapsamını genişletmek amacıyla, gelecek çalışmalar için aşağıdaki adımlar önerilmektedir.

*** Kapsamlı ağ simülasyonu ve ölçeklenebilirlik Analizi:** Çalışmanın dağıtık ağ performansı ve merkeziyetsizlik iddialarını daha geniş çapta (örneğin 50+ otonom İHA) doğrulamak amacıyla NS-3 veya OMNeT++ gibi gerçek ağ simülatörlerinin kullanılması planlanmaktadır. Bu sayede işlem yükü, CPU/RAM kullanımı, uçtan uca ağ gecikmesi ve düğüm senkronizasyonunu içeren sistematik benchmark testlerinin yapılması hedeflenmektedir.

*** Fiziksel saha testleri:** Simülasyon ortamının ötesine geçilerek, protokolün rüzgâr etkisi ve sinyal gürültüsü gibi gerçek uçuş koşulları altında çalışan fiziksel bir sürü İHA üzerinde test edilmesi önerilmektedir.

*** P2P mesh ağ entegrasyonu:** Verilerin yer istasyonuna indirilmesine ihtiyaç duymadan, İHA'ların kendi aralarında (Air-to-Air) veri doğrulaması yaptığı, tamamen merkeziyetsiz bir Mesh Ağ yapısının kurulması önerilmektedir.

*** Akıllı sözleşme entegrasyonu:** Belirli koşulların sağlanması durumunda (örneğin "Hedef tespit edildi") otonom karar verme mekanizmalarını mümkün kılacak hafif (lightweight) akıllı sözleşmelerin sisteme entegre edilebilir.

*** Olay tabanlı mimari ve heartbeat mekanizması:** Sistem verimliliğini artırmak amacıyla, sürekli veri doğrulama yaklaşımından, yalnızca kritik olaylar tarafından tetiklenen bir yapıya geçilmesi planlanmaktadır. Ayrıca, ağdaki İHA'ların aktif durumlarını izlemek ve arızalı/işlevsiz İHA'ları tespit etmek için sisteme periyodik "Heartbeat" sinyallerinin entegre edilmesi öngörülmektedir.

*** Haversine formülü kullanılarak coğrafi konum doğrulaması:** GPS verilerinin manipülasyonuna karşı ek bir güvenlik katmanı olarak yeni bir algoritma geliştirilecektir. Bu algoritma, Haversine formülü kullanarak İHA'lar arasındaki fiziksel mesafeleri matematiksel olarak doğrulayacak ve raporlanan konum bilgileri ile hesaplanan konumlar arasındaki tutarlılığı kontrol edecektir.

*** Batarya tabanlı dinamik lider seçimi:** Ağ içerisindeki doğrulama yükünü dengelemek amacıyla, anlık batarya seviyesi en yüksek olan İHA'nın geçici olarak "Doğrulayıcı (Validator)" rolünü üstlendiği, dinamik ve enerji duyarlı bir doğrulama (verification) mekanizması üzerinde çalışmalar yürütülecektir.

7. Kaynaklar

[1] M. Mesbahi and M. Egerstedt, Graph Theoretic Methods in Multiagent Networks, Princeton Univ. Press, Princeton, NJ, USA, 2010.

[2] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications of blockchain in unmanned aerial vehicles: A review," Vehicular Communications, vol. 23, Art. no. 100249, 2020, doi: 10.1016/j.vehcom.2020.100249.

[3] S. Samonas and D. Coss, "The CIA triad: A review of information security," J. Inf. Syst. Secur., vol. 10, no. 3, pp. 14–26, 2014.

[4] N. Zhao et al., "Vulnerabilities of centralized UAV networks and potential of decentralization," IEEE Wireless Commun., vol. 25, no. 1, pp. 2–7, Feb. 2018.

[5] R. W. Sinnott, "Virtues of the Haversine," Sky Telescope, vol. 68, no. 2, p. 159, Aug. 1984.

[6] H. Feistel, "Cryptography and computer privacy," Sci. Amer., vol. 228, no. 5, pp. 15–23, May 1973.

[7] NIST, "FIPS PUB 180-4: Secure Hash Standard (SHS)," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Tech. Rep., Aug. 2015.

[8] K. Can and A. Başçi, "Leader-Follower Formation Control of Quadrotor: A Simple Virtual Leader Approach," in Proc. Int. Symp. on Applied Sciences and Engineering (ISASE), 2021, pp. 479–483.

[9] X. Li et al., "Real-time verification delays in conventional blockchain-UAV architectures," J. Syst. Archit., vol. 154, pp. 103–115, Jan. 2025.

[10] A. Koulianos and A. Litke, "Hardware constraints in blockchain-enabled edge computing for drones," IEEE Access, vol. 11, pp. 1422–1435, 2023.

[11] W. Shi et al., "Edge computing: Vision and challenges," IEEE Internet Things J., vol. 3, no. 5, pp. 637–646, Oct. 2016.

[12] A. Muslimov and R. Munasypov, "Energy efficiency challenges of consensus mechanisms in mini-UAVs," Appl. Sci., vol. 11, no. 9, p. 3851, Apr. 2021.

[13] R. Diestel, Graph Theory, 5th ed., Springer-Verlag, Berlin, Germany, 2017.

[14] K. Can and A. Başçi, "Robust Consensus-Based Formation Control of a Group of UAVs," Elektronika ir Elektrotechnika, vol. 29, no. 4, pp. 4–10, 2023, doi: 10.5755/j02.eie.34306.

[15] T.C. Strateji ve Bütçe Başkanlığı, "On İkinci Kalkınma Planı (2024–2028)," Ankara, Türkiye, Teknik Rapor, 2023.

[16] A. R. Hevner et al., "Design science in information systems research," MIS Quart., vol. 28, no. 1, pp. 75–105, Mar. 2004.

[17] L. Roque et al., "Blockchain for swarm robotics: A survey," Sensors, vol. 20, no. 18, p. 5244, Sep. 2020, doi: 10.3390/s20185244.

[18] M. Javaid et al., "Blockchain technology applications in Industry 4.0: A review," J. Ind. Inf. Integr., vol. 24, p. 100209, Dec. 2021.

[19] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. URL: https://bitcoin.org (Erişim zamanı: Mayıs 27, 2026).
[20] Folium Developers, "Interactive maps with Python," 2023. URL: https://python-visualization.github.io/folium/ (Erişim zamanı: Mayıs 27, 2026).
[21] X. Huang and D. Huang, "Performance Analysis of Blockchain Consensus Algorithm in Unmanned Aerial Vehicle Ad Hoc Networks," Drones, vol. 9, no. 5, Art. no. 334, 2025, doi: 10.3390/drones9050334.
[22] L. Wang, Y. Chen, and H. Gupta, "Edge computing for resource-constrained avionics: A performance study," in Proc. Eur. Conf. Embedded Syst. (ECES), 2024.
[23] R. Xu, Z. Chang, X. Zhang, and T. Hämäläinen, "Blockchain-Based Resource Trading in Multi-UAV Edge Computing System," IEEE Internet Things J., vol. 11, no. 12, pp. 21559–21573, Jun. 2024, doi: 10.1109/JIOT.2024.3375918.

Özgeçmişler

Elif Tekle, Atatürk Üniversitesi İktisadi ve İdari Bilimler Fakültesi Yönetim Bilişim Sistemleri Bölümü'nde lisans eğitimine devam etmektedir. Eğitim süreci boyunca bilişim sistemleri, yazılım geliştirme, veri yönetimi, dijital dönüşüm ve teknoloji tabanlı proje geliştirme alanlarına ilgi duymuştur. Akademik çalışmalarında bilgi teknolojilerinin farklı alanlarda uygulanması, sistem analizi, veri güvenliği ve yenilikçi dijital çözümler üzerine yoğunlaşmaktadır. Üniversite eğitimi sırasında edindiği teorik bilgileri uygulamalı projelerle destekleyerek teknik becerilerini geliştirmeyi hedeflemektedir. İlgi alanları arasında yapay zekâ, siber güvenlik, veri bilimi ve analizi, blokzincir teknolojileri, insansız sistemler ve dijital inovasyon yer almaktadır. Ayrıca kullanıcı gereksinimlerinin belirlenmesi, sistemlerin analiz edilmesi ve geliştirilen çözümlerin kullanılabilirlik açısından değerlendirilmesi konularına ilgi göstermektedir.

Kaan Can, lisans derecesini 2014 yılında Niğde Üniversitesi Elektrik-Elektronik Mühendisliği Bölümü'nden, yüksek lisans ve doktora derecelerini ise Atatürk Üniversitesi Fen Bilimleri Enstitüsü Elektrik-Elektronik Mühendisliği Anabilim Dalı Kontrol ve Kumanda Programı'ndan sırasıyla 2017 ve 2023 yıllarında almıştır. Halen Atatürk Üniversitesi Elektrik-Elektronik Mühendisliği Bölümü'nde Dr. Öğretim Üyesi olarak görev yapmaktadır. Araştırma alanları arasında kontrol teorisi, robotik sistemler, insansız hava ve kara araçların kontrolü, kayan kipli kontrol, adaptif kontrol, optimizasyon tabanlı kontrol, sürü kontrol uygulamaları ve insansız hava araçlarının formasyon kontrolü yer almaktadır.