# A Review of Digital Twins for Security Testing and Threat Prediction for MLO Exploits in Wi-Fi7

P.D. Dissanayake
e20084@eng.pdn.ac.lk
Department of Computer Engineering, University of Peradeniya
Sri Lanka

A.T.L. Nanayakkara
e20262@eng.pdn.ac.lk
Department of Computer Engineering, University of Peradeniya
Sri Lanka

D.R.P. Nilupul
e20266@eng.pdn.ac.lk
Department of Computer Engineering, University of Peradeniya
Sri Lanka

Dr. Upul Jayasinghe
upuljm@eng.pdn.ac.lk
Department of Computer Engineering, University of Peradeniya
Sri Lanka

Dr. Suneth Namal Karunarathna
namal@eng.pdn.ac.lk
Department of Computer Engineering, University of Peradeniya
Sri Lanka

## Abstract

Abstract—The IEEE 802.11be (Wi-Fi 7) standard introduces Multi-Link Operations (MLOs), a shift in paradigms which is expected to provide extremely high throughput by offering multi-frequency bands and utilizing aggregated. While MLO has the potential to provide and enhance dramatic improvements in performance, the complexity of the MAC-layer coordination logic (which includes packet steering, channel access, and multi link backoffs) creates a new and complex attack surface. This literature review will consider the intersection of two domains, new mechanisms within Wi-Fi 7 MLOs and new capabilities asso ciated with Network Digital Twins (NDTs) for security testing and threat predictions. The literature review will demonstrate that the focus of the current literature is highly fragmented. The majority Wi-Fi 7 studies focus on performance improvements, and the majority of the security literature is focused on legacy threats. Most crucially, MLO-related anomalies, such as packet steering and backoff compensation, are treated as performance problems, not adversarial exploits. This review of the literature will reveal a clear research gap at this intersection: the absence of high fidelity NDTs capable of replicating and predicting MLO-related threats. The backoff compensation and free ride mechanisms will be targeted as a high impact, state based vulnerability that could be exploited for more sophisticated Denial of Service (DoS) attack scenarios. Attack scenarios that current testing approaches cannot model. This paper establishes a clear need for a NDT framework for security validation and mitigation for this new breed of exploits in wireless networks.

## 1 Introduction

The evolution of wireless networking is fueled by an insatiable need for higher throughput and, more reliable, lower latency. Demanding and Emerging applications, such as Extended Reality (XR), Augmented Reality (AR), 4K/8K video streaming, and cloud gaming, are testing legacy Wi-Fi solutions to their limits. To respond, the IEEE has developed the Wi-Fi 7 Standards to create a generational leap in perfor mance referred to as Extremely High Throughput (EHT).

Wi-Fi 7 offers innovative new aspects, such as 320 MHZ channels and 4096-QAM; however, the most disruptive and transformative aspect of the technology is Multi-Link Op eration (MLO). MLO is a new MAC layer paradigm that will allow a single Multi-Link Device (MLD) to transmit and receive simultaneously, and across multiple frequency bands such as 2.4 , 5 and 6 GHz as if they were a single aggregated pipe, or have multiple links behave independently and engage in asynchronous communication.While it holds the potential to vastly improve throughput and latency, it complicates op erations. MLO devices, rather than managing a one-channel mechanism, must undertake a complex and real-time task of selecting channels, assigning traffic to links, and coordinating access across channels for multiple parallel links. Although this complexity is crucial to performance, it represents an area for attack that has, to date, not been fully explored. This review will survey the literature on MLO operations, inspect new security challenges due to that operational complexity, and then introduce the Digital Twin (DT) framework as an approach for modeling.

### 1.1 Objectives and Overview

This review of the literature aims to take a critical perspec tive on the two rapidly evolving but comparatively isolated fields of new MAC-layer performance mechanisms for Wi-Fi 7 (IEEE 802.11be) and the capabilities of Network Digital Twins (NDTs) to test for security.

Although the majority of Wi-Fi 7 literature treats per formance optimization as its aim, this review contends that the essence of those performance optimizations can be seen as part of a new complex attack surface. In addition, we claim that the underlying coordination logic, which is subtly embedded in the state-based performance algorithms of Multi Link Operation provides potential vulnerabilities that existing and legacy security frameworks cannot assess.

This review pursues the following specific objectives:

- **Survey the Wi-Fi 7 MLO Attack Surface:** To move beyond legacy threats and identify novel vulnerabilities in MLO-specific mechanisms, such as packet steering, multi-link association, and backoff compensation

- **Re-frame Performance Anomalies as Security Exploits:** To critically analyze existing literature and demonstrate how documented "performance issues," such as backoff overflow, can be intentionally weaponized by an adversary.
- **Review State-of-the-Art NDTs:** TTo examine the current architectures, enabling technologies (e.g., simulation, AI/ML), and primary use cases for Network Digital Twins, which are currently focused on performance and optimization rather than security.
- **Identify the Critical Research Gap:** To synthesize these domains and demonstrate the urgent need for a security focused NDT framework specifically designed to model, test, and predict adversarial MLO behavior.

To fulfill these aims, this review is organized as three major surveys: First, a technical survey is provided comparing with a technical survey of key mechanisms behind Wi-Fi 7, establish ing the complex logic of MLO and its features. Next, a critical analysis entitled "From Features to Exploits," demonstrates how the features of MLO can be steadily manipulated. Next, the review continues to Digital Twins, providing a description of core concepts and architectures. Finally, the review brings all of the points described above together to explain the research gap, and establishes that the MLO backoff mechanism is a new and significant vulnerability, and importantly, opens up space for future work.

## 2 WI-FI 7: FROM PAST TO PRESENT

From the first wifi generation established in 1997, As [20, 35] and [20] suggest, every generation of technology has developed a new innovation to solve specific problems created by the limitations of current generations, such as performance bot tlenecks, and therefore offers users higher-performing, more efficient wireless communication technologies.

These innovations are represented by enhancements in many areas. Examples include increased channel bandwidth, increased spectral efficiency, and enhanced modulation ca pabilities that provide for higher levels of throughput and capacity on wireless networks. Continued advancement of these technologies also results in improvements to MAC layer coordination, as well as the implementation of multi user access methods and the mitigation of interference, all of which lead to a more reliable and fair wireless environment as the demands of the user and needs for increased wireless connectivity continue to grow and result in greater densities of users and devices in an area.

## 3 The Paradigm Shift: IEEE 802.11be

### 3.1 Multi-Link Operation (MLO)

WiFi 7 builds upon the standards of WiFi 6 to provide extremely high throughput using multiple frequency channels at the same time. The core idea is explained in [2]. Instead of using a single link with multiple channels for a connection, WiFi 7 utilizes a technology called Multi-Link Operation that uses multiple links for a single device and an access point.

The devices that are capable of performing multi link operations are named as multi-link devices. As [2, 8, 26] suggest, different architectures, the used modes of operation and the initial place of

| | Wi-Fi 5 | Wi-Fi 6 | Wi-Fi 6E | Wi-Fi 7 |
|---|---|---|---|---|
| Standard | IEEE 802.11ac | IEEE 802.11ax | IEEE 802.11ax | IEEE 802.11be |
| Bands | 5 GHz | 2.4 GHz, 5 GHz | 6 GHz | 2.4 GHz, 5 GHz, 6 GHz |
| Channel Bandwidth | 160 MHz | 160 MHz | 160 MHz | 320 MHz |
| Modulation (QAM) | 256 QAM | 1024 QAM | 1024 QAM | 4096 QAM |
| Security | WPA2 | WPA3 | WPA3 | WPA3 |

**Figure 1: Evolution of Wifi**

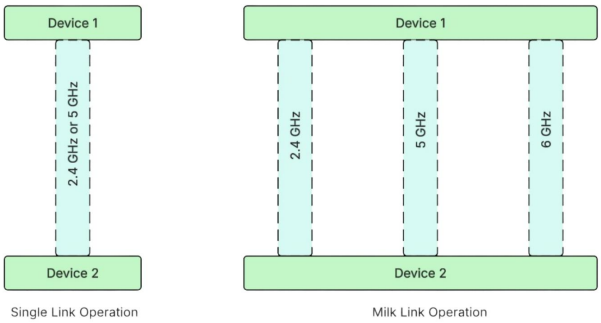


**Figure 2: Single link Vs Multi link operations**

station play a huge role in the speeds of the connection. STR (Simultaneous Transmit Receive) and Non STR modes show different speeds and architectures. STR uses multiple links to transmit and receive at the same time using all the links independently [10]. This provides asynchronous communication and thus different tasks of different frequency bands. In synchronous mode, the links are synchronized and thus all are needed to be free at the same time for a new transmission from either end.

### 3.2 4K-QAM (4096-QAM)

4096-QAM (4K-QAM) is a higher-order modulation technique introduced as part of Wi-Fi 7 to increase data throughput and spectral efficiency. Compared with 1024-QAM used in Wi-Fi 6, 4K-QAM encodes more bits per symbol, which improves peak data rates under favorable channel conditions [22]. This is particularly beneficial for bandwidth-intensive and latency-sensitive use cases, such as XR/AR/VR, cloud gaming, and high-definition streaming.

However, reliable 4K-QAM operation typically requires exceptionally high SNR and stable channel characteristics. As a result, practical deployment depends on hardware linearity, interference

conditions, and regulatory constraints, and the technique tends to benefit short-range or high-quality links [48]. Even so, higher-order modulation remains a key enabler for Wi-Fi 7's multi-gigabit and low-latency goals.

### 3.3 Ultra-Wide Bandwidth

The bandwidth of Wi-Fi 7 has been made into much wider channels (up to 320 MHz) and the newly opened 6 GHz band to provide orders-of-magnitude higher raw capacity and lower interference than legacy bands.Wider instantaneous bandwidths enable very high PHY rates and support higher order modulations, but also increase sensitivity to noise, hardware linearity and regulatory LBT/CCA constraints. As expressed in [11] having a larger bandwidth allows for more transmissions further increasing the throughput

### 3.4 Clear Channel Assessment (CCA) and Listen-Before-Talk (LBT)

[11, 50] discusses aspects of Clear channel assessment to identify the status of the links. Before any transmission, stations run a physical CCA (energy/preamble detection) and regulatory LBT rules to decide whether the medium is idle; these mechanisms gate entry to the channel and there fore directly shape access latency and collision probability. CCA/LBT thresholds and sensing durations are fundamental levers in coexistence and fairness.

### 3.5 EDCA and Contention Windows (CW)

The feature named Enhanced Distributed Channel Ac cess which was introduced in Wi-Fi 3 (IEEE 802.11e) pro vides differentiated access by assigning Access Categories (voice/video/best-effort/background) their own AIFSN and CWmin/CWmax values so that higher-priority traffic, on average, waits less time before winning access and sends more packets [12]. The exponential backoff (CW doubling on retries) is the basic anti-collision mechanic, but it is also the point at which attackers or careless opportunistic schedulers can bias access. In [51], the paper studies the effects of EDCA parameters on the potential for packet steering, improving link utilization.

### 3.6 Primary and Secondary Links in MLO

The differentiation between a primary link and a secondary link is a key concept only in Wi-Fi 7's Multi-Link Operation context and does not apply in the context of traditional SLOs. The primary link identifies the anchor link for the MLO device and is responsible for all initial association, authentication, and control traffic that is deemed critical. Additionally, it is the only link that can be utilized by legacy devices, ensuring backward compatibility. Secondary links are dedicated solely for use by MLDs for specific performance increases, such as aggregation of bandwidth between links and decreases in latency. This key distinction between primary links and secondary links is crucial to any MLO device's traffic steering, failure management, and network fairness requirements.

According to [10], This primary-secondary architecture dic tates traffic rules for MLDs and legacy clients.MLDs can operate on the primary link or secondary links or both. In the state that secondary links have arrived at congestion, an MLD can flow on the primary link. The reverse is not true for fairness to prevent starvation of resources on legacy devices. The implementation of this logic differs depending on the operational mode of the MLO configuration. In MLO-NSTR mode, the primary link enforce strict operational linkage to gether, controlling all channel contention for both links. In the MLO-STR mode, the links operate more independently, and asynchronously, with the primary link's primary responsibility to manage overall connection and with supporting legacy devices being a secondary responsibility rather than controlling contention of every single data packet's operation.

### 3.7 Radio Link Allocation and MLMR

In Wi-Fi 7, the allocation of radio links is the core of Multi-Link Operation (MLO) and allows a device to sustain concurrent links on 2.4, 5, and 6 GHz bands simultaneously. A critical aspect of allocation is how to allocate data streams on appropriate links for the best aggregate performance, balancing throughput, latency, and reliability. Linking traffic types, or Access Categories (AC) [51], to appropriate physical radio links is known as AC-to-Link Allocation. For example, latency-sensitive voice or gaming traffic may be prioritized on the least congested or shortest latency radio link, while bulk data transfer is routed to higher capacity bands.

Research and experiments on MLO optimization on Access Point Controller (APC) [52] demonstrate that MLO alone is not capable of exceeding MLO, but the allocation of radio links is equally important. The central APC is structured from real-time data to jointly coordinate AP-STA pairing and link allocation, ultimately optimizing throughput while meet ing basic proportional fairness. A high-performance Multi Link Multi-Radio (MLMR) device can transmit and receive concurrently (at the same time) on radios that operate inde pendently with each other. With the aid of a controller, the high-performance device can dynamically combine, duplicate, or steer traffic allocation based on real-time channel condi tions.While the adaptive autonomy can support fairness and security concerns, the vulnerabilities could arise from schedul ing algorithms being poorly tuned or attacked, causing devices to dominate high-capacity links, causing backoff inclusions and packet-steering bias to be key vulnerabilities in Wi-Fi 7 networks.

### 3.8 Packet Steering

In Wi-Fi 7, packet steering is the ability of a Multi-Link Device (MLD) to actively assign traffic to multiple links by taking advantage of the all the bands available from 2.4,5 and 6 GHz bands. Packet steering takes packet handling instructions from a layer called the Upper MAC (U-MAC), and then the respective Lower MAC (L-MAC) handles the actual steering logic. Packet steering is intended to maximize throughput and minimize latency. This helps maintain Quality of Service (QoS) levels by sending packets onto the link that will provide the best results at that moment. Steering decisions of which packets should be sent on which links are based on time-sensitive characteristics of each link such as signal-to-noise ratio, channel loading, and Access Category (AC) prioritization from Enhanced Distributed Channel Access (EDCA) parameters [51].

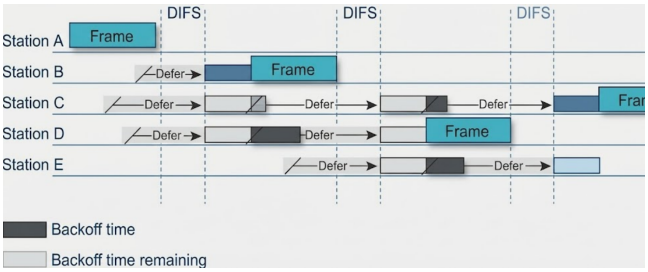


**Figure 3: Backoff implementation in Wi-Fi**

In regards to the time where a packet is assigned to a link, Wi-Fi 7 outlines 3 strategies: Early Steering Strategy, Late Steering Strategy, and Combined Steering Strategy. An Early Steering Strategy assigns packets to links in advance of the packet queue but has the advantage of having low scheduling overhead and the highest possible predictability. With the Late Steering Strategy, the selection of the link the packet will be sent on is made just before the packet is transmitted to the channel and can leverage more recent link conditions. The Combined Steering Strategy effectively combines both strategies; the packet will be assigned a link in advance and then re-evaluated before transmission. The Combined Steering Strategy allows for lower latency while also allowing adaptable packet contexts that are affected by complex and dynamic wireless environments.

Recent works such as [12], demonstrate that steering is a dy namic, per-packet process that can be implemented efficiently on existing Wi-Fi architectures using host-driven scheduling, enhancing both spectral utilization and determinism. Steering can enable fine-grained control over QoS traffic by rerouting low-latency voice or gaming flows over less congested links, while bundles of bulk data can be routed over wider bands. Yet with all of the adaptability and autonomy that steering can offer comes a new set of dilemmas. Poor calibration or mali cious steering behavior can favor high-capacity links towards certain devices, erode fairness, and even create an exploitable opportunity by manipulating backoffs and/or falsifying link metrics. Thus, secure, AC-aware, and context-adaptive steering algorithms become critical to ensuring fairness and reliability in Wi-Fi 7's multi-link technologies.

### 3.9 Backoffs and Free Rides

Wi-Fi's CSMA/CA protocol uses random backoff timers to manage channel access, a process which has known challenges like backoff overflow [34, 36]. Wi-Fi 7's Multi-Link Operation (MLO) adds complexity by using multiple backoff counters for its different links. To improve efficiency, Wi-Fi 7 implements backoff compensation to synchronize these counters, allowing all links on a single device to transmit simultaneously. This, however, introduces the phenomenon of free rides [36], where a link transmits without completing its full backoff simply because another link's timer expired.

While this synchronization boosts efficiency, it can lead to backoff overflow [36], where repeated compensations cause counter errors, and creates significant fairness challenges. Repeated free rides may allow MLO devices to consistently "skip the queue," undermining fairness for single-link devices. Although Wi-Fi 7 specifies safeguards like clamping backoff values, this mechanism presents a new vulnerability. Malicious devices could potentially exploit this by manipulating backoff timing to gain disproportionate and unfair channel access, making the security of backoff synchronization vital for Wi-Fi 7 networks.

## 4 THE CONVERGENCE OF WI-FI 7 AND NETWORK DIGITAL TWINS

Because of its complexity, the IEEE 802.11be standard is creating a validation crisis that cannot be addressed with conventional testing techniques. This section will explain how Network Digital Twins (NDTs) are the technological solution to secure MLO described in Section III.

### 4.1 Beyond Static Simulation

Traditional discrete-event network simulators (such as ns-3 or OMNeT++) are built on static configurations and rely on offline execution. However, MLO is an inherently changing and unpredictable state-based operation. The operation of a MLD is based on real-time data (the amount of congestion on the primary link, the backoff timer values on the secondary links as measured in milliseconds, and the instantaneous routing decisions made by the Packet Steering algorithms).

It's impossible to simulate live environments with capturing cascading impacts of exploits (or "free rides") improperly manipulated backoff counters through static simulations. As such, the functional relationship between Wi-Fi 7 and NDTs will continue, so to achieve this goal, the NDT performs the function of synchronizing the temporal aspects needed to capture these transient states. Additionally, the Digital Twin serves to reflect the MAC Layer Logic operating on a live network; therefore, Digital Twins are capable of detecting changes in handshake logic, which would otherwise result in standard jitter in a static log.

### 4.2 The Necessity of Sandbox Security

The cyber vulnerability or weaknesses of Wi-Fi 7 can only be understood through adversarial testing; however, testing backoff manipulation and steering exploit designs in produc tion networks runs the potential risk of degrading performance for legitimate users as well as creating denial of service (DoS) events.

What The Digital Twin provides is a risk-free sandbox; the fidelity of the twin is significantly greater than that of a typical "test environment." What the Security Researcher can do with a virtual Twin of the MLO network is to introduce malicious control frames or spoofed Channel State Information (CSI) feedback and observe how the packet steering logic reacts. This relationship allows the researcher to predict zero-day vulnerabilities in the MLO coordination logic without com promising the integrity of the operational enterprise network.

### 4.3 Data-Driven Threat Prediction

Moreover, the existence of this intersection creates an op portunity to address the lack of transparency surrounding how AI-driven

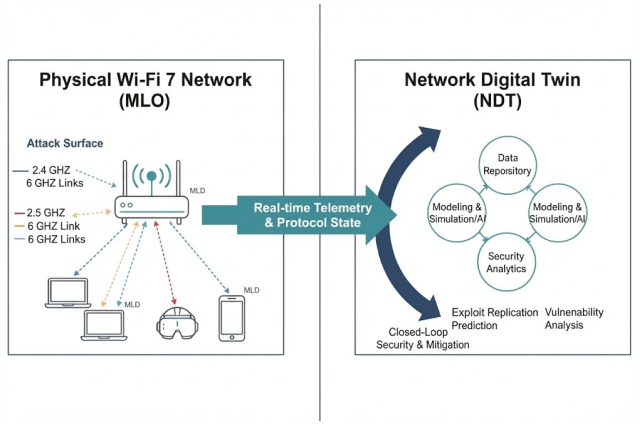


**Figure 4: Wifi 7 and Digital twin relationship**

scheduling works in Wi-Fi 7 systems. As Multi-Link Operation (MLO) implementations become more and more reliant on proprietary machine learning (ML) algorithms to determine channel selection and link allocation of devices, the New Digital Twin (NDT) is a way of running a shadow model. The NDT allows for direct correlation of real-time telemetry data generated by the Wi-Fi 7 Access Points (APs) with the telemetry data returned to the devices from the Twin. Tracking these metrics allows for identification of statistically significant divergences between the optimal predicted link (as calculated by the Twin) and the actual link selected by the device; it also offers the potential to identify either exploitation of a device's ML algorithm or a more sophisticated jamming attack that would evade traditional intrusion detection systems (IDS).

# 5 Digital Twins for Replication and Automation

## 5.1 Concept and Taxonomy of Network Digital Twins

Digital twins were initially used in manufacturing as high level virtual duplicates of physical objects. In networking, this takes the form of the Network Digital Twin (NDT), defined as a software-based representation of topology, configuration, traffic and performance that is continually synced with the live network and provides ability for what-if analysis, optimization and autonomous control [6, 24, 38]. The NDT is defined as a closed-loop system which mirrors the physical network at multiple layers of abstraction (topology, protocol state, KPIs) and aids in design, planning and operations for tasks like capacity planning, fault analysis and traffic engineering [6].

Recent systematic reviews have approached NDTs and dis tinguished their use from traditional offline simulation based on: (i) notwithstanding there is no request to provide a constant sync between a digital twin and physical system, moments when the sync is continuous, (ii) bi-directional engagement, as an NDT can actuate changes back into the scope of the physical network, and (iii) multi-impactor usage where there are distinct operational aspects from different challenges like management, control, AI agents [24, 38, 47]. NDTs can be classified by: based on scope, either intra-domain or end to-end, the layers supported either routing only or cross layer including wireless and applications, and by the primary aim (design, optimization, resilience, or security) in terms of generating the NDT. Most existing NDTs begin with the context of application to a performance and measure resource management approach, as opposed to specifically security centered work [47].

When discussing wireless systems, it is important to dif ferentiate between device-level twin, link-level twins (prop agation and interference) and network-level twins (multi cell, multi-RAT scenarios) [29]. The claim is made that it is necessary to have accurate channel models, interferences, user mobility, and protocol dynamics to "deserve" the title of "digital twin." In the context of Wi-Fi 7, it provides insight that Wi-Fi 7/MLO twins should not only replicate PHY capacity throughput, but must also replicate MAC-layer contention, multi-link scheduling and backoff dynamics [29].

## 5.2 Reference Architectures and Functional Frameworks

A range of literature has proposed reference architectures that decompose Network Digital Twins (NDTs) into structured functional building blocks. A common layer-view emerges across the literature [6, 38]:

- Data collection and integration layer: Exporters collect telemetry (counters, logs, traces) from devices and simu lators, normalizing information before streaming into the twin.
- Data repository and semantic model: Graph-based rep resentations of topology, configuration, KPIs, and event information encapsulate unified data representation.
- Modelling and simulation layer: Representational models, discrete-event simulators, and ML surrogates model net work behavior for different scenarios and configurations.
- Control and actuation layer: Closed-loop control, what-if analysis, and policy enforcement enable the twin to enact safe changes to physical network implementation.
- Orchestration and lifecycle management: MANO-style components deploy, version, and update the twin and its models over time.

The functional framework used in next-generation NDT efforts, like the 6G-TWIN model, organizes this architecture to understand explicit functions: Data Collection, Unified Data Repository (UDR), Simulation Framework, AI/ML Work flows, and NDT-MANO/ZSM automation, all encompassed within security, interoperability, and scalability requirements [18]. This framework aligns with the architecture proposed for Wi-Fi 7, which has a Wi-Fi 7 telemetry fabric feeding into a UDR, processing layer supporting AI/ML, and connects to simulation engine components orchestrated by MANO/ZSM throughout the units and visualized through a unified dash board.

Additional architectural perspectives derive the modules and openness is essential; NDT platforms should expose common interfaces to simulators, AI pipeline development, and OSS/BSS systems rather than be evaluated as monolithic vendor-specific emulators for the core architecture [24, 49]. This vision reinforces the adoption

of composable building blocks, for example: using the tools Containerlab, ns-3, OM NeT++, and ML services to build NDT environments with scalable and adaptive characteristics [24, 38, 43, 45].

## 5.3 Enabling Technologies

Existing research in network simulation and emulation that has informed the design of contemporary NDT platforms has shown extensions to ns-3 that incorporate OS level packet processing models and co-simulation interfaces (e.g., FMI) allow for genuine applications/protocol stacks to interact with a digital twin in real time [14, 27]. These architectures illustrate how to:

(1) couple ns-3 with external tools through interfaces,
(2) synchronize time across heterogeneous domains, and,
(3) cocreate ns-3 as a digital twin "engine" instead of standing alone as a simulator [14, 27].

Additional work supports complementary mechanisms for keeping physical, and digital replicas, state synchronizations over the communications [43].

Machine-learning-based propagation loss model to ns-3 has shown to shorten and add the complexity of wireless channel computations and remain accurate enough for network level decision-making [7]. These results represent an adults shift in simulation research, namely that not only large fidelity, but potentially computationally expensive modeling are being augmented or replaced, with learned surrogate models to support the near-real-time what-if experimentation [7].

Simultaneously, work on distributed Digital Twin network ing shows that Named Data Networking (NDN) can function as both the data and control plane for the purposes of synchro nizing state and content across physical and virtual domains [15]. These architectures are particularly useful for multi-site Wi-Fi 7 deployments, where a centralized or federated twin must ingest and publish telemetry at scale.

In addition to orchestration at the lab layer, tools such as Containerlab recently allow for the declarative construction of network testbeds through the orchestration of containers and VM-wrapped network operating systems into arbitrary topologies using Veth links and Linux bridges [45]. This allows the construction of dense, resource efficient emulated environments involving controllers; FRR/SONiC; AAA ser vices; Kafka/MQTT buses; and IDS pipelines that can be used as the non-RF-fraction of a Wi-Fi 7 digital twin in conjunction with wireless simulations or real access points.

## 5.4 AI-Enabled Network Digital Twins

Recent advances in Network Digital Twins are increasingly supplanting simulation with AI-driven surrogate modeling. One line of work introduces a GNN-based digital twin trained on packet-level OMNeT++ simulations, which uses message passing over pathways, links and queues represented as graphs to predict end-to-end QoS metrics while maintaining a com putational cost benefit and strong generalizability to unseen topologies [19].

Survey-based research in wireless communications demon strates GNNs as a natural representation of interference pat terns and topology relationships, establishing them as an acceptable mechanism for representing complex wireless envi ronments and makes them promising candidates for wireless focused digital twins [44].

Another stream of work develops a learnable digital twin which uses a neural embedding of nodes, links, and end to-end paths to replicate the KPIs from simulated outputs. By training the embedding with static simulation data, the inference can be made in one forward pass to accelerate the network evaluation and configuration optimization process, avoiding entering simulation data in discrete-event simulation each evaluation cycle [32].

Larger reviews of NDT systems lead to the observation that AI/ML capabilities may be foundational elements of digital twin pipelines. The reviews mention AI as methods to accomplish essential functions within the NDT space, namely, traffic prediction, anomaly detection, routing optimization, resource allocation, and closed-loop control [6, 29, 32, 38]. These agreements build a case for maintaining an AI workflow layer in the Wi-Fi 7/MLO twin proposed here: (i) GNN-based performance surrogates for representing MLO contention, scheduling, and steering decisions and (ii) deep learning/reinforcement learning models for attack detection, mitigation, and adaptive network reconfiguration.

Knowledge-centric research on digital twins indicates that the representation of the network entities, configurations and dependencies through knowledge graphs allows structured reasoning about policy, intent, and configuration state [39]. A Wi-Fi 7/MLO twin would also benefit from a graph-based semantic layer that could inform which APs, links, flows or multi-link paths were impacted during failures, contention events or security incidents [19, 39, 44].

## 5.5 Digital Twins for Wireless and Wi-Fi Networks

As of now, there is not yet a consideration of reliability or security, indicating that wireless work is largely efficiency driven with little to no consideration for adversarial common alities [29].

In the Wi-Fi space, experimental investigations on Multi Link Operation (MLO) offer an initial research perspective of digital-twin inspired testbeds. Here, a configurable AP/STA is connected with a virtual wireless environment to allow for throughput, latency and link reliability analysis under realistic conditions. However, its focus is on performance analysis, and it does not include modelling adversarial behaviour or threat prediction [41].

Current knowledge demonstrates that:

(1) Digital twins can model multi-band, multi-AP WLAN environments;
(2) Interest in applying twins to Wi-Fi 7 and MLO is increasing; and
(3) Security testing and attack modeling are not yet incor porated into wireless or Wi-Fi digital-twin platforms.

This indicates a clear research gap: digital twins for Wi-Fi 7 are primarily performance-based, with scarcely researched applications for security analysis and threat prediction.

## 5.6 Digital Twins, Intrusion Detection, and Threat Modeling

Digital twin uses with a security focus are more advanced in other cyber-physical domains than for Wi-Fi contexts. Prior work demonstrates the idea of a digital twin can itself be under attack: an attacker can change the inputs to the digital twin, manipulate the model outputs to give misleading impressions of system behavior, or disrupt the interplay of the interactions of the real world and the digital twin [46]. This body of work conveys that any security assessment should include assessment of the twin in consideration of the real system, as vulnerabilities in one may impact the other. Likewise, they position digital twins as uniquely contrived environments, allowing for security behaviors and system responses to be evaluated without impacting operational deployments [46].

Machine-learning methods for intrusion detection in wire less and critical-infrastructure contexts are considered more advantageous than convention rule-based IDS techniques, par ticularly in cases where more subtle or complexities in attack signatures are arising [9, 37]. However, conventionally, a dataset that is built ahead of time is used and disconnected from (use of) continuous learning and engagement of the IDS with a live or simulated network online behavior. Static data, as the training means, limits (ML) methods in the ability to capture changing behaviour: a closed-loop digital twin would produce the capability to generate and replay attack and observe it under realistic and distributed behaviours. Research on coexistence among next-generation wireless systems recog nizes new vulnerabilities when the systems share a spectrum or coexist in a common environment [40]. Such research underscores the challenges associated with the complexity of channel interference, the intertwining of protocols, and the idiosyncrasies of configuration vulnerabilities with heteroge neous systems. A digital twin of Wi-Fi 7 with Multi-Link Operation, because it can expose PHY/MAC-level informa tion and allow for controlled execution of cross-technology or cross-link attack scenarios that are impossible to test in production networks, could specifically support this type of study.

Digital-twin frameworks for future wireless management have exemplified options for operators to study configuration changes, resource strategies, and performance trade-offs prior to deploying them in practice [5]. While these frameworks primarily emphasize optimization and service performance, the dual of the framework to conduct security evaluations flows naturally. A twin developed to model Wi-Fi 7/MLO behavior would allow for controlled injection of adversarial actions and observations of these actions on throughput or fairness. It would also allow for testing of mitigation mechanisms while safely maintaining the operational system without disruption to the system.

## 5.7 Synthesis: Gap at the Intersection

Several themes motivate the proposed research focus:

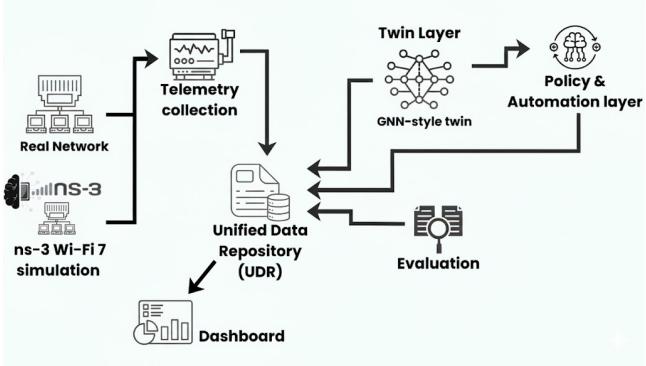


**Figure 5: Wifi threat model architecture for Digital twins**

- **Mature NDT architectures, but security is secondary:** Surveys and frameworks for NDT [6, 24, 38, 47] identify distinct building blocks (data collection, UDR, simulation, AI, MANO/ZSM) and have demonstrated use cases in network traffic engineering, planning and optimization, but they are primarily motivated by per formance or resource-management objectives. Security generally appears in these selections of work as a sup porting or non-functional requirement (i.e., protecting a twin and the network) rather than modeled as the main objective (stabby, developing models of attack surfaces, or predicting exploits) [6, 24, 38, 47]. Other work surveys threats to digital twins or cyber-physical systems more broadly. Security is considered a core topic, but again does not focus on Wi-Fi 7 or MLO [46].
- **Wireless and Wi-Fi twins emphasize performance rather than adversaries:** Wireless DT surveys [29] and all works on Wi-Fi based twins [41] describe how twins model propagation, load balancing, handover, or MLO behavior, but they all do so while largely ignoring inten tional malicious behavior like falsified CSI, HARQ ma nipulation, or backward exploitations present in the multi link environment (resets, etc.) [29, 40, 41]. Again, performance, reliability and mobility optimizations are the focus and security is included as an open issue, rather than an explicit part of the model in the twin.
- **AI-enabled twins exist, but not for Wi-Fi 7 MLO threat prediction:** GNN-based and learnable twins [19, 32] estimate network performance and enable rapid what-if analysis, while ML-based IDS work [9, 37] demonstrates robust capabilities for attack classification in Wi-Fi. Nonetheless, despite the studies reviewed here to date, no research paper identified a closed-loop twin that creates realistic MLO-level attack traces and re trains/evaluates ML models under different conditions [9, 19, 29, 32, 37]. AI-powered twins are often focused on performance enhancements and the majority of IDS studies do not use live or emulated Wi-Fi 7/MLO telemetry to develop datasets.

- **Digital twin threat work targets the twin, not Wi Fi 7 MLO exploits:** The digital twin threat survey [46] emphasizes threats targeting digital twins and cyber physical systems but does not consider Wi-Fi MAC layer coordination logic, backoff compensation, or "free ride" phenomena characterizing IEEE 802.11be MLO [5, 40, 41, 46]. Additionally, Wi-Fi and wireless management twins [5, 41] and coexistence studies [40] seem to not utilize twins as systematic digital MLO based threat modeling or predictions.

## 6 Critical Analysis of Existing Literature

A narrative review was performed on more than 50 pa pers. Level 3 of AI assessment, otherwise referred to as AI collaboration, was used in conducting the research covering Wi-Fi 7 and associated technologies. Overall, we found that the literature is primarily oriented towards two different but relatively unrelated areas of study:

**Performance and Optimization:** Most of the literature currently published [3, 8, 10, 11, 52] is focused on enhancing performance overall. These studies optimize MLO with respect to lower latency [10], higher throughput [52], or improved QoS for specific applications such as AR [8]. These studies are fundamental to the success of the technology and treat known limitations and delays for performance, which is fundamental to realizing MLO in practice.

**Legacy and General Security:** Research populated by research on security is largely based on legacy threats [20], namely in relation to “Evil Twin” type of attacks [25], or relating due dilemmas or deficiencies in the security of co existing standards (for example, Wi-Fi 6 and 5G) in surveys [40]. These studies have value but do not touch on new and unique, state-based vulnerabilities related to the MLO multi link coordination logic.

The comprehensive literature review indicated that, while the literature remains focused on performance, it has unknow ingly indicated several protocol-level anomalies, functional risks, and new complexities to resolve that have not yet been examined as actual security vulnerabilities. This research integrates these findings into a cohesive list of 11 significant issues reflective of an attack surface that is not yet addressed.

To establish a clear problem domain for each issue, Table II separates the identified vulnerabilities into two groups: physical protocol stresses versus higher-level algorithmic and scheduling exploitations.

Critically, papers addressing these issues treat them as performance and fairness anomalies rather than intentional ma licious exploitation vectors. This represents the key blind spot in current literature. A distinct gap exists at the intersection of Wi-Fi 7’s MLO-specific vulnerabilities and digital twin based security testing and threat prediction, where twins are explicitly designed to simulate, detect, and mitigate adversarial MLO behavior rather than just optimize performance.

Based on the previous discussion, the proposed architec ture is positioned as a novel contribution relative to existing works [5–7, 14, 15, 18, 27–30, 32, 38, 39, 43–45, 47, 49]. It uniquely combines Wi-Fi 7/MLO telemetry collection and inference engines through a unified data repository, GNN-based per formance twins, DL/RL-based anomaly detection approaches, and a simulation framework (ns-3/OMNeT++) orchestrated via Containerlab and NDT-MANO/ZSM. By specifically focusing on the MLO backoff mechanism, a currently under-explored area within the NDT framework, this architecture extends the state-of-the-art beyond performance optimization and towards the critical domain of security testing and threat prediction for MLO exploits. To this end, this literature review sets up a research plan where the proposed Wi-Fi 7/MLO twin will be explicitly used to: (i) replicate MLO backoff and packet steering behaviors under both benign and adversarial conditions; (ii) generate the labelled datasets required for ML models to detect these novel threats; and (iii) use the twin to explore and validate effective mitigation strategies, such as adaptive backoff strategies and link steering policies, in a closed-loop environment before deployment in real Wi-Fi networks [5, 9, 19, 37, 40, 41, 46].

## 7 From Features to Exploits

The very innovations that yield the unmatched performance of Wi-Fi 7- MLO, dynamic steering, and further contention mechanisms-substantially broaden the attack surface. The complexity required to manage multiple links in real time invokes new logical and state-based vulnerabilities not present when a single link architecture is deployed. An attacker has more to exploit than just jamming a single frequency; they can now target the logics of coordination that bind those link together. This section examines exploitable aspects of Wi-Fi 7, categorized by the particular feature being exploited by the attacker, with backoff mitigation as a particular focus.

### 7.1 Association and Link Management Vulnerabilities

**Multi-Link Association Hijack:** The MLO association procedure is a complex multi-stage handshake to set up and verify all of the links. This procedure increases the opportunity for similar attacks as "Evil Twin" or association spoofing. An attacker could inject during this handshake and either hijack a secondary link or spoof control frames. A successful attack could prohibit a legitimate MLD from fully establishing a complete MLO connection forcing it into a degraded single link mode, or create a man-in-the-middle (MITM) situation on one of the aggregated links. New research indicates there are even challenges in securing a modern Wi-Fi connection establishment [23].

**Primary Link Denial of Service:** It has already been established that the primary link is the fundamental link for control traffic and legacy compatibility [10]. An attacker could exploit this by pretending to be a legacy (non-MLD) device, which only associates with the primary link. By continually contending for and occupying the primary link, the attacker can stop the critical control, association, and management frames from the MLD device, better or worse rendering the entire MLO operation inoperable. This is the definition of cross-link interference where one link fails due to the completion of another link and this is a well-known issue of co-existing networks [16, 26].

## 7.2 PHY/MAC Feedback and Logic Exploits

**Spoofing CSI Feedback and Beam Hijacking:** High throughput 6 GHz links utilize beamforming, which relies on the active client to provide accurate Channel State Information (CSI) feedback to the access point. An attacker could spoof this CSI feedback, "lying" to the AP about the channel conditions. The attacker could then use this "spoofed" CSI to "hijack" the beam, compelling the AP to direct its RF signal toward the attacker to conduct eavesdropping, as shown in Wi Fi 6 [21], or worse, into a null space for a targeted denial of service.

**HARQ Vulnerability:** The newly introduced Hybrid ARQ (HARQ) for faster retransmissions adds a new, tight-timed transport layer protocol for an attack. An attacker success fully predicting or otherwise interfering with the HARQ ACK/NACK signaling could force unwanted retransmissions

causing throughput degradation or perhaps convince the sender that a missing packet was successfully acknowledged, causing potentially catastrophic effects higher in the data stream.

**Frame Aggregation and Frame Striping Risks:** The ability to aggregate, or stripe packets across multiple links (e.g., multiple STEPs) creates complications with reassembly. An attacker could selectively condition a packet, or fragment the packet, or stripe a packet in a manner that would overwhelm the receiver reassembly buffer, with the goal of creating a buffer overflow, out of order delivery, or logic crash in the MAC layer.

## 7.3 Data Steering and Allocation Attacks

**Packet Allocation and Steering Exploits** As [12] states, it is vital to select Early, Late, or Combined steering. The attacker could exploit this algorithm. Based on the measured quality of the links, the attacker could trick the steering algorithm into putting the high-priority traffic such as voice, on a congested link. The attacker could also exploit naive splitting logic for the traffic, causing massive out-of-order delivery of packets that would cause the receiver's reassembly buffers to overflow, and leading to a retransmission storm.

**Exploitation of MLO Scheduling Algorithms** MLO link selection is a complicated optimization problem and has typically been addressed with heuristic approaches or learning-based approaches (MAB) [52] that learn over time which link is the "best" to use based on feedback. These sampled feedback systems that create ML-driven steering are vulnerable to adversarial ML attack [1, 4]. For example, an attacker can poison the feedback loop by spoofing packet ACKs or by creating legitimate interference in the link, causing an otherwise high-quality link to seem poor connection quality [33, 52]. In this manner, the attacker "tricks" the MAB to "explore" the bad links and creates a systematic degradation of the target connection, while appearing relatively stealthy.

## 7.4 Contention and Backoff Manipulation

The most complex attacks involve the basic CSMA/CA protocol and are now dangerously complicated by MLO. Although there are always simple collision based attacks (e.g. sending during another device's countdown to increase the likelihood of a collision), the synchronized backoff of MLO generates a much more obscure vulnerability. This exploit, a focus of this research, exploits the free ride and backoff compensation functionality seen in [34, 36].

**The Attack Vector:** The malicious MLD can exploit backoff compensation rules. In Non-STR mode, where links must contend and transmit together, the malicious device could deliberately manipulate the backoff counter on one of its active links. For instance, it could "listen" on a link that it knows to be busy and pause its own backoff, while allowing the counter on a clear link to expire.

**The Objective (Backoff Overflow):** By intentionally desynchronizing internal counters, the attacker can repeatedly induce backoff overflow by then re-triggering the backoff compensation. Backoff overflow was explicitly identified as a problem in [36]. The end result is for the attacker to have a backoff counter reset to some minimal value without having "paid" the cost of a full random wait time.

**The Result (Fairness Collapse)** This principle successfully disrupts the fairness of the EDCA parameters [51]. Rather than waiting for a random backoff interval, the attacker's device now enters a continuous, asynchronous-like transmission mode in an otherwise synchronous environment. The attacker will thus enable itself to perpetually receive "free rides" [36] and dominate the channel while starving other devices (both MLD and legacy) of access.

# 8 Discussion

The literature review has mapped out the complicated and emerging space of Multi-Link Operation (MLO) in Wi-Fi 7. The findings indicate that moving to MLO [3, 17, 35] is not simply the performance improvement; it is a fundamental MAC-layer complexity change introducing an entire new class of security vulnerabilities that haven't been previously studied.

The central discovery of this review is the critical blind spot in the current works; the literature split into two nearly independent communities: one aiming to optimize MLO performance [11, 52], and one to conduct an attack analysis of legacy security vulnerabilities [20, 25]. In bridging this gap, this review proposes a new threat vector as the weaponization of MLO performance anomalies. While the "backoff overflow" problem [36], the literature focuses on as a fairness issue, is instead repurposed into a sophisticated, state-based DoS attack through operationalization.

This finding leads to the second major conclusion of this work; traditional security testing approaches are inadequate. The state-based, multi-link and time-sensitivity characteristics of a DoS exploit in MLO is fundamentally not the same as modeling a static analysis or a single-link and even simple simulation. This is where the Network Digital Twin (NDT) becomes invaluable. This review contends that NDT is not merely an analytic tool for "what-if" performance analysis [5] but offers the vital platform for MLO security-in-design. A high-fidelity NDT as offered in the literature [6, 38, 47] represents the only environment to:

(1) Replicate the intricate state of multi-link contention.

**Table 1: Identified Areas of Protocol Stress and Anomalies**

| **Fundamental Protocol & Link Stress** *(PHY/MAC Mechanics & Handshakes)* | **Algorithmic & Scheduling Exploitation** *(Optimization, AI & Decision Logic)* |
|---|---|
| 1. Backoff Manipulation—identified as fairness and performance issue [36] | 7. Exploitation of Naive Packet Splitting algorithms—potential out-of-order packet creation [12] |
| 2. Cross-Link Interference—legacy client dependence on primary link creates chokepoint problems [26] | 8. Exploitation of MAB Algorithms—ML-based scheduling vulnerabilities [51] |
| 3. Collision Probability and Access Exploitation—fundamental backoff mechanisms remain central to channel access [31, 51] | 9. Challenges of Packet Splitting—non-trivial optimization problem [12] |
| 4. Frame Aggregation & Striping Risks—frame reassembly complexity [42] | 10. Packet Steering—Early/Late steering method exploitation potential [12] |
| 5. Multi-Link Association—complex handshake for establishing multiple links [10] | 11. Potential Beam Hijacking/Spoofed CSI—beamforming feedback susceptibility [21] |
| 6. HARQ Disruption—new feedback mechanism exploitation layer [31] | |

(2) Create the high-fidelity datasets of both benign and adversarial MLO behavior for training ML-based detection models [9, 19].
(3) Validate mitigation strategies in a closed loop allowing vendors and standards organizations to evaluate and only deploy new backoff or packet steering mitigation algorithms if they provide resilience.

## 8.1 Future Directions

Although this study primarily examines the MLO backoff attack, the suggested Digital Twin framework establishes a foundation for a broad spectrum of future research. As highlighted in [5], the NDT serves as a robust platform for conducting "what-if" simulations, making it an ideal tool for investigating the additional protocol vulnerabilities identified in this review. Future inquiries should prioritize the following areas:

**Adversarial Packet Steering:** Research should investigate vulnerabilities within "Early" versus "Late" steering mechanisms [12]. An NDT environment can be utilized to simulate adversaries manipulating link-quality indicators to corrupt MLO scheduling algorithms [52] or Multi-Armed Bandit (MAB) decision logic [51], thereby forcing Access Points into suboptimal resource allocation. This domain intersects significantly with the emerging field of adversarial machine learning in wireless networks [1, 4].

**Vulnerabilities in PHY/MAC Feedback Loops:** NDTs should be leveraged to assess the resilience of rapid feedback mechanisms. Potential applications include modeling spoofed Channel State Information (CSI) to identify beam hijacking risks—similar to those observed in Wi-Fi 6 [21]—or injecting fabricated or latent ACK/NACK signals to stress-test the state consistency of the newly implemented HARQ protocols [21].

**MLO Association and Coexistence Exploits:** The NDT architecture is well-suited for modeling the complex multi-link association handshake. This allows for the feasibility analysis of sophisticated Man-in-the-Middle (MITM) attacks during link establishment. Furthermore, it provides a controlled environment to evaluate "Primary Link Denial-of-Service" scenarios, where adversaries mimic legacy devices to saturate the primary link, thereby disrupting MLO control signaling and intensifying coexistence challenges.

**Advancement of the Digital Twin Framework:** The development of a security-centric NDT for MLO constitutes a distinct research domain. Future endeavors must focus on scalability, potentially employing sampling techniques [28], and investigating the integration of Generative AI (GenAI) to synthesize realistic, large-scale traffic patterns and attack vectors [13]. Crucially, these advancements must be balanced against the need to maintain the NDT's fidelity and accuracy as a validation tool.

This review asserts that the safety of Wi-Fi 7 and future wireless systems is inherently tied to our capability to model their complexity. The MLO exploits presented offer a new category of threats that target protocol logic rather than weaknesses. This research asserts that the NDT is no longer a luxury for analyzing performance; however, it represents a vital component of the security for all future wireless systems.

# 9 Conclusion

This literature review has mapped the newly emerged, nuanced terrain of Multi-Link Operation in Wi-Fi 7 (MLO), showing that its complex MAC-layer coordination is not just about enhanced performance but a significant change that creates a new, unexplored attack surface. The key conclusion of this work is a dangerous gap in the associated literature, which is unfortunately fragmented; one community has focused on MLO performance [8, 52] while another has considered legacy security issues [20, 25, 40]. The review opens a dialogue between these two worlds and represents the first time documented performance-related issues with MLO, specifically the "backoff overflow" problem [36], are identified as purposeful and weaponized security exploits.

To summarize, this review shifts the conversation from MLO performance to MLO security. We have proposed the existence of a

new type of threat that targets protocol logic rather than cryptographic weakness. Consequently, the security of Wi-Fi 7 and future wireless systems will hinge on our ability to model and defend this new logical attack surface, and this work proposes that the Network Digital Twin is the foundational defense.

## References


[1] [n. d.]. Adversarial Machine Learning Attacks in Wireless Networks. Technical report (online). https://apnic.foundation/projects/adversarial-machine-learning-attacks-in-wireless-networks/technicalreport Accessed: 2025-10-20.

[2] [n. d.]. White Paper: Wi-Fi 7 Multi-Link Operation (MLO). Online. https://www.mediatek.com/tek-talk-blogs/white-paper-wi-fi-7-multi-link-operation-mlo Accessed: 2025-10-20.

[3] A. A. Abdalhafid, S. K. Subramaniam, Z. A. Zukarnain, and F. H. Ayob. 2024. Multi-Link Operation in IEEE802.11be Extremely High Throughput: A Survey. *IEEE Access* 12 (2024), 46891–46906. doi:10.1109/ACCESS.2024.3378997

[4] O. T. Ajayi, S. O. Onidare, and H. Tajudeen. 2024. A Study on Adversarial Machine Learning in Wireless Communication Systems. In *Lecture Notes in Electrical Engineering*. Vol. 1253. 384–392. doi:10.1007/978-981-97-6937-7-46

[5] E. Ak, B. Canberk, V. Sharma, O. A. Dobre, and T. Q. Duong. 2024. What-if Analysis Framework for Digital Twins in 6G Wireless Network Management. In *Proceedings of the 20th International Wireless Communications and Mobile Computing Conference (IWCMC)*. 232–237. doi:10.1109/IWCMC61514.2024.10592526

[6] P. Almasan et al. 2022. Network Digital Twin: Context, Enabling Technologies, and Opportunities. *IEEE Communications Magazine* 60, 11 (Nov. 2022), 22–27. doi:10.1109/MCOM.001.2200012

[7] E. N. Almeida et al. 2022. Machine Learning Based Propagation Loss Module for Enabling Digital Twins of Wireless Networks in ns-3. In *Proceedings of the 2022 Workshop on ns-3*. 17–24. doi:10.1145/3532577.3532607

[8] M. Alsakati, C. Pettersson, S. Max, V. N. Moothedath, and J. Gross. 2023. Performance of 802.11be Wi-Fi 7 with Multi-Link Operation on AR Applications. arXiv preprint. arXiv:2304.01693 http://arxiv.org/abs/2304.01693 Accessed: 2025-10-07.

[9] H. A. Bhutta, M. T. Jahangir, and A. A. Bhutta. 2025. Advancing Wi-Fi Intrusion Detection Systems with Machine Learning Techniques for Enhanced Classification of Wireless Attacks. In *Proceedings of the IEEE International Conference on Applied and Computational Sciences (ICACS)*. 1–7. doi:10.1109/ICACS64902.2025.10937819

[10] M. Carrascosa, G. Geraci, E. Knightly, and B. Bellalta. 2022. An Experimental Study of Latency for IEEE 802.11be Multi-Link Operation. In *Proceedings of the IEEE International Conference on Communications (ICC)*. doi:10.1109/ICC45855.2022.9838765 Accessed: 2025-10-08.

[11] M. Carrascosa-Zamacois, G. Geraci, L. Galati-Giordano, A. Jonsson, and B. Bellalta. 2022. Understanding Multi-link Operation in Wi-Fi 7: Performance, Anomalies, and Solutions. In *Proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. doi:10.1109/PIMRC56721.2023.10293865

[12] G. Cena, M. Rosani, and S. Scanzio. 2024. Packet Steering Mechanisms for MLO in Wi-Fi 7. In *Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. doi:10.1109/ETFA61755.2024.10710726

[13] H. Chai, H. Wang, T. Li, and Z. Wang. 2024. Generative AI-Driven Digital Twin for Mobile Networks. *IEEE Network* 38, 5 (2024), 84–92. doi:10.1109/MNET.2024.3420702

[14] K. Chang, Y. Du, M. Liu, J. Shi, Y. Zhou, and Y. Li. 2023. OS Packet Processing Mechanism Simulation Architecture for Enabling Digital Twins of Networks in ns-3. In *Proceedings of the IEEE International Performance, Computing, and Communications Conference (IPCCC)*. 186–193. doi:10.1109/IPCCC59175.2023.10253819

[15] C. Chen, Z. Jia, Z. Wang, L. Cui, and F. P. Tso. 2025. Design and Evaluation of an NDN-Based Network for Distributed Digital Twins. arXiv preprint. arXiv:2505.04326 https://arxiv.org/abs/2505.04326

[16] D. Croce, D. Garlisi, F. Giuliano, N. Inzerillo, and I. Tinnirello. 2018. Learning from Errors: Detecting Cross-Technology Interference in WiFi Networks. *IEEE Transactions on Cognitive Communications and Networking* 4, 2 (June 2018), 347–356. doi:10.1109/TCCN.2018.2816068

[17] C. Deng et al. 2020. IEEE 802.11be-Wi-Fi 7: New Challenges and Opportunities. *IEEE Communications Surveys & Tutorials* 22, 4 (July 2020), 2136–2166. doi:10.1109/COMST.2020.3012715

[18] S. Faye, P. Soto, G. Volpe, A. Zaki-Hindi, B. Hensel, G. Castellanos, I. Turcanu, C. Sommer, S. M. Senouci, A. Belogaev, and M. Camelo. 2025. A Functional Framework for Network Digital Twins. In *Proceedings of the IEEE EuCNC & 6G Summit*. Poznań, Poland.

[19] M. Ferriol-Galmés et al. 2022. Building a Digital Twin for Network Optimization Using Graph Neural Networks. *Computer Networks* 217 (Nov. 2022), 109329. doi:10.1016/J.COMNET.2022.109329

[20] E. Firdus et al. 2024. WiFi from past to today, consequences that can cause and measures of prevention from them, WiFi security protocols. *E3S Web of Conferences* 474 (Jan. 2024), 02004. doi:10.1051/E3SCONF/202447402004

[21] T. M. Hoang, A. Vahid, D. C. Sicker, and A. Sabharwal. 2024. Physical-Layer Spoofing in WiFi 6 to Steer the Beam Toward the Attacker. In *Proceedings of the IEEE International Conference on Communications (ICC)*. 4006–4011. doi:10.1109/ICC51166.2024.10622744

[22] R. P. F. Hoefel. 2024. Effects of Phase Noise and Frequency Offset on the Performance of 4K-QAM and 16K-QAM in 802.11be and 802.11bn WLANs. In *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*. doi:10.1109/WCNC57260.2024.10570887

[23] N. Hoque and H. Rahbari. 2025. Securing Wi-Fi 6 Connection Establishment Against Relay and Spoofing Threats. arXiv preprint. arXiv:2501.01517 https://arxiv.org/pdf/2501.01517 Accessed: 2025-10-08.

[24] B. Huff, K. Uregdthsa, K. Muhammad, C. Searcy, and K. M. Ammad. 2024. Network Digital Twins: Framework, Applications, and Challenges. Authorea Preprints. doi:10.36227/TECHRXIV.171995274.45268502/V1

[25] V. Jain, V. Laxmi, M. S. Gaur, and M. Mosbah. 2019. ETGuard: Detecting D2D Attacks Using Wireless Evil Twins. *Computers & Security* 83 (June 2019), 389–405. doi:10.1016/J.COSE.2019.02.014

[26] S. Jung, S. Choi, Y. Yoon, H. Son, and H. Kim. 2025. Modeling and Analysis of Coexistence Between MLO NSTR-based Wi-Fi 7 and Legacy Wi-Fi. arXiv preprint. arXiv:2509.01201 https://arxiv.org/pdf/2509.01201 Accessed: 2025-10-08.

[27] W. S. Jung, J. Kim, and D. S. Yoo. 2024. An FMI Compliant Co-Simulation Approach for NS-3 Network Simulator. In *Proceedings of the International Conference on ICT Convergence (ICTC)*. 1954–1959. doi:10.1109/ICTC62082.2024.10827338

[28] M. Kellil, S. ben Hadj Said, M. T. Thi, C. Janneteau, and A. Olivereau. 2024. Addressing the Scalability of Network Digital Twins: A Network Sampling Approach. In *Proceedings of the 20th International Conference on Network and Service Management (CNSM 2024)*.

[29] L. U. Khan, Z. Han, W. Saad, E. Hossain, M. Guizani, and C. S. Hong. 2022. Digital Twin of Wireless Systems: Overview, Taxonomy, Challenges, and Opportunities. *IEEE Communications Surveys & Tutorials* (2022). doi:10.1109/COMST.2022.3212830 Accessed: 2025-10-08.

[30] L. U. Khan, Z. Han, W. Saad, E. Hossain, M. Guizani, and C. S. Hong. 2023. Digital Twin of Wireless Systems: Overview, Taxonomy, Challenges, and Opportunities. *IEEE Communications Surveys & Tutorials* (2023). Early Access.

[31] E. Khorov, I. Levitsky, and I. F. Akyildiz. 2020. Current Status and Directions of IEEE 802.11be, the Future Wi-Fi 7. *IEEE Access* (2020). doi:10.1109/ACCESS.2020.2984964 Accessed: 2025-10-08.

[32] B. Li et al. 2023. Learnable Digital Twin for Efficient Wireless Network Evaluation. In *Proceedings of MILCOM 2023: IEEE Military Communications Conference*. 661–666. doi:10.1109/MILCOM58377.2023.10356320

[33] C. Li et al. 2024. Practical Adversarial Attack on WiFi Sensing Through Unnoticeable Communication Packet Perturbation. In *Proceedings of the 30th International Conference on Mobile Computing and Networking (MobiCom 2024)*. 373–387. doi:10.1145/3636534.3649367

[34] A. López-Raventós and B. Bellalta. 2022. Multi-link Operation in IEEE 802.11be WLANs. *IEEE Wireless Communications* (2022). doi:10.1109/MWC.004.2100414 Accessed: 2025-10-08.

[35] S. S. Murad, R. Badeel, B. B. Abdal, T. Rahman, and T. Al-Quraishi. 2024. Introduction to Wi-Fi 7: A Review of History, Applications, Challenges, Economical Impact and Research Development. *Mesopotamian Journal of Computer Science* 2024 (2024), 110–121. doi:10.58496/MJCSC/2024/009

[36] W. Murti and J. H. Yun. 2022. Multilink Operation in IEEE 802.11be Wireless LANs: Backoff Overflow Problem and Solutions. *Sensors* 22, 9 (May 2022), 3501. doi:10.3390/S22093501

[37] A. Pinto, L. C. Herrera, Y. Donoso, and J. A. Gutierrez. 2023. Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure. *Sensors* 23, 5 (Feb. 2023), 2415. doi:10.3390/S23052415

[38] R. Poorzare, D. N. Kanellopoulos, V. K. Sharma, P. Dalapati, and O. P. Waldhorst. 2025. Network Digital Twin Toward Networking, Telecommunications, and Traffic Engineering: A Survey. *IEEE Access* 13 (2025), 16489–16538. doi:10.1109/ACCESS.2025.3531947

[39] D. R. Ramachandran Raj, T. A. Shaik, A. Hirwe, P. Tammana, and K. Kataoka. 2023. Building a Digital Twin Network of SDN Using Knowledge Graphs. *IEEE Access* 11 (2023), 133789–133809. doi:10.1109/ACCESS.2023.3288813

[40] K. Ramezanpour, J. Jagannath, and A. Jagannath. 2023. Security and Privacy Vulnerabilities of 5G/6G and WiFi 6: Survey and Research Directions from a Coexistence Perspective. *Computer Networks* 221 (Feb. 2023), 109515. doi:10.1016/J.COMNET.2022.109515

[41] M. Rosani, G. Cena, D. Cavalcanti, V. Frascolla, G. Marchetto, and S. Scanzio. 2024. A Software Platform for Testing Multi-Link Operation in Industrial Wi-Fi Networks. In *Proceedings of the IEEE International Workshop on Factory Communication Systems (WFCS)*. doi:10.1109/WFCS60972.2024.10540967

[42] S. Scanzio et al. 2024. Multi-Link Operation and Wireless Digital Twin to Support Enhanced Roaming in Next-Gen Wi-Fi. In *Proceedings of the IEEE International Workshop on Factory Communication Systems (WFCS)*. doi:10.1109/WFCS60972.

2024.10540931

[43] J. Sengendo and F. Granelli. 2024. Building Network Digital Twins Part I: State Synchronization. In *Proceedings of the 3rd International Conference on 6G Networking (6GNet 2024)*. 182–188. doi:10.1109/6GNET63182.2024.10765759

[44] Y. Shen, J. Zhang, S. H. Song, and K. B. Letaief. 2023. Graph Neural Networks for Wireless Communications: From Theory to Practice. *IEEE Transactions on Wireless Communications* 22, 5 (May 2023), 3554–3569. doi:10.1109/TWC.2022.3219840

[45] S. S. Shestopalov. 2024. Containerlab . . If BibTeX has issues with Cyrillic/Ukrainian text, compile with XeLaTeX/LuaLaTeX or transliterate the title/author..

[46] M. Suárez-Román, M. Sanz-Rodrigo, A. Marín-López, and D. Arroyo. 2025. A Digital Twin Threat Survey. *Big Data and Cognitive Computing* 9, 10 (Oct. 2025), 252. doi:10.3390/BDCC9100252

[47] R. Verdecchia, L. Scommegna, B. Picano, M. Becattini, and E. Vicario. 2024. Network Digital Twins: A Systematic Review. *IEEE Access* 12 (2024), 145400–145416.

[48] H. Wang, H. Mohammadnezhad, and P. Heydari. 2019. Analysis and Design of High-Order QAM Direct-Modulation Transmitter for High-Speed Point-to-Point mm-Wave Wireless Links. *IEEE Journal of Solid-State Circuits* 54, 11 (Nov. 2019), 3161–3179. doi:10.1109/JSSC.2019.2931610

[49] J. Wieme, M. Baert, and J. Hoebeke. 2025. Architectural Design for Digital Twin Networks. *Network* 5, 3 (2025). https://www.mdpi.com/2673-8732/5/3/24 Article 24.

[50] Z. Xie, R. Xu, and L. Lei. 2014. A Study of Clear Channel Assessment Performance for Low Power Wide Area Networks. In *IET Seminar Digest*, Vol. 2014. 311–315. doi:10.1049/IC.2014.0119

[51] P. Yi, W. Cheng, J. Wang, J. Pan, Y. Ouyang, and W. Zhang. 2025. Intelligent Multi-link EDCA Optimization for Delay-Bounded QoS in Wi-Fi 7. arXiv preprint. arXiv:2509.25855v1 https://arxiv.org/pdf/2509.25855v1 Accessed: 2025-10-07.

[52] L. Zhang, H. Yin, S. Roy, L. Cao, X. Gao, and V. Sathya. 2023. IEEE 802.11be Network Throughput Optimization with Multi-Link Operation and AP Coordination. arXiv preprint. arXiv:2312.00345 https://arxiv.org/pdf/2312.00345 Accessed: 2025-10-14.