New Wi-Fi Jamming Attack Disables Targeted Wi-Fi Devices Using RIS Technology

A major development in wireless security research has revealed a sophisticated Wi-Fi jamming technique capable of disabling individual devices with millimeter-level precision, leveraging emerging Reconfigurable Intelligent Surface (RIS) technology.
Developed by researchers at Ruhr University Bochum and the Max Planck Institute for Security and Privacy, this method exploits programmable metamaterials to manipulate radio frequency (RF) signals with unprecedented spatial resolution.

RIS devices consist of arrays of sub-wavelength metallic patches controlled via software-defined tuning components.

These surfaces dynamically alter electromagnetic wave propagation characteristics, enabling selective amplification or cancellation of 802.11 protocols (Wi-Fi 6/6E) at specific spatial coordinates.

In experimental setups, the team demonstrated the ability to jam a Raspberry Pi 4B connected to a Wi-Fi 6 access point while leaving an identical device positioned just 5mm away fully operational.

This represents a 1000x improvement in targeting resolution compared to conventional jamming methods that rely on omnidirectional antenna arrays.

New Wi-Fi Jamming Attack
Passive Channel Optimization:
The attacker eavesdrops on target devices (e.g., Wi-Fi pings) to estimate channel state information (CSI).

Using a greedy genetic algorithm, the RIS computes a configuration vector c that maximizes the Jamming-to-Signal Ratio (JSR) at the target device while minimizing interference at non-targets.

Active Jamming:
With the optimized RIS configuration, the attacker transmits a 5 GHz Wi-Fi jamming signal (20 MHz bandwidth, MCS 1).

The RIS passively reflects this signal to constructively interfere at the targets location while destructively canceling it elsewhere.

In controlled tests, the team achieved:

5 mm targeting resolution: Complete denial-of-service (0 Mbit/s throughput) against one Raspberry Pi 4B while a second device 5 mm away sustained 25 Mbit/s.

This defies conventional diffraction limits through mutual antenna coupling effects and RIS-enabled sub-wavelength field manipulation.

Multi-target scenarios: Simultaneous disruption of four-device clusters (C1-C4 in floorplan testing) with 17 dB power margin before non-target interference.

Robustness: Sustained attack efficacy for 24 hours post-optimization, though human movement within 1m reduced non-target JSR by 6 dB.

The attack bypasses cryptographic protections by operating at Layer 1. Vulnerable scenarios include:

Industrial IoT: Selective disruption of actuators in automated assembly lines without triggering plant-wide failsafes.
Healthcare: Targeting medical IoT devices (e.g., infusion pumps) while leaving patient monitors operational.
Smart Homes: Precision jamming of security cameras/alarms, a capability already exploited by burglars using crude jammers.
Dependency on reciprocity fails against FDD systems or devices with separate Tx/Rx antennas. Further, Non-transmitting devices experience 13 dB JSR reduction through RIS focal spillover. Current detection methods (RSSI monitoring, MAC randomization) are ineffective against this physical-layer attack.

Mitigation
The study suggests mitigation strategies focusing on breaking attack prerequisites:

Randomized Transmit Beamforming: Introduce spatial channel variability via MIMO beam hopping to confuse RIS optimization.
Non-Reciprocal Hardware: Use frequency-division duplexing (FDD) or isolators between Tx/Rx chains.
Cross-Layer Monitoring: Deploy auxiliary sensors to detect localized SNR anomalies characteristic of RIS focusing.
While RIS manufacturing costs (~750 for 768-element surfaces) currently limit widespread abuse, 6Gs integration of RIS could democratize these attacks, Dr. Aydin Sezgin, co-author and RIS pioneer.

According to the Report, The demonstrated attack exposes a paradigm shift in wireless security, transforming an anticipated 6G enabler into a precision cyber-physical weapon.

The findings underscore the urgent need for hardware-secure 6G architectures and revised regulatory frameworks as RIS deployments expand.

With optimization times under 5 minutes and commercial RIS availability rising, this threat vector demands immediate cross-disciplinary attention from industry, academia, and policymakers.

Quelle:	Cyber Security Monitor Worldwide vom 01.03.2025
Ressort:	Cyber Security
Dokumentnummer:	477944118

Dauerhafte Adresse des Dokuments:
https://dokument.genios.de/document/SCMW__f152b3680c59bae4c769df049134f515b48c6245