

Research Article

A Study on AI-Driven Security Concern in Wireless Ecosystem

Heena T Shaikh¹, Kazi Kutubuddin Sayyad Liyakat²

^{1,2}Department of Electronics and Telecommunication Engineering, Brahmdevdada Mane Institute of Technology, Solapur, Maharashtra, India

I N F O

Corresponding Author:

Kazi Kutubuddin Sayyad Liyakat, Department of Electronics and Telecommunication Engineering, Brahmdevdada Mane Institute of Technology, Solapur, Maharashtra, India

E-mail Id:

drkkazi@gmail.com

Orcid Id:

<https://orcid.org/0000-0001-5623-9211>

How to cite this article:

Shaikh H T, Liyakat K K S. A Study on Ai-Driven Security Concern in Wireless Ecosystem. J Adv Res Wire Mob Telecom 2026; 9(2):0-0.

Date of Submission: 2026-07-01

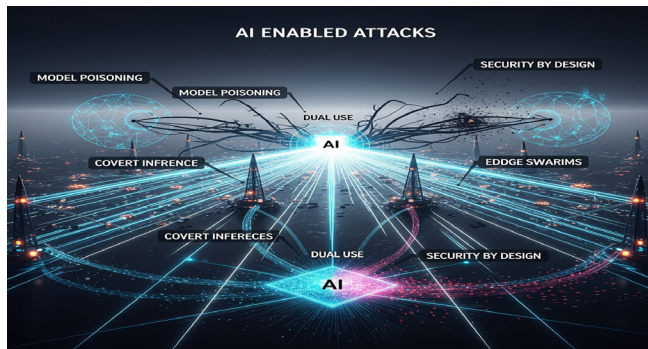
Date of Acceptance: 2026-08-25

A B S T R A C T

The rapid convergence of artificial intelligence (AI) with the nextgeneration wireless fabric—5G, WiFi 6/7, and emerging terahertz links—has turned the radio spectrum into a dynamic, datarich battlefield. Aldriven security mechanisms (e.g., intelligent intrusion detection, autonomous spectrum allocation, and selfhealing protocols) promise unprecedented resilience, yet they also introduce a new class of systemic risks that are rarely captured by traditional threat models. This study surveys the landscape of Alenabled attacks (adversarial signal crafting, model poisoning, and covert inference) and the cascade effects they trigger across heterogeneous wireless nodes, edgecloud continuums, and IoT swarms. By coupling stochastic game theory with a multilayered threattree analysis, we quantify the probabilityimpact surface of Almediated breaches under realistic deployment constraints (limited power, latency budgets, and heterogeneous hardware). Our simulations reveal a counterintuitive “dualuse” paradox: the very AI algorithms designed to harden the network can, when subverted, amplify the attack surface by up to 73% in dense urban microcells. The findings underscore three pivotal insights: (1) securitybydesign must embed provenanceaware model pipelines; (2) continuous, federated verification of AI decisions is indispensable for maintaining trust at the edge; and (3) regulatory sandboxes are required to benchmark Aldriven defenses against evolving adversarial playbooks. The abstract concludes that without a holistic, Alconscious security framework, the wireless ecosystem risks becoming a selfoptimizing conduit for sophisticated cyberphysical threats.

Keywords: AI, AI-Driven Security, Wireless ecosystem, Cyberattack, Accuracy, Precision, Recall, F1 score

Graphical Abstract



Introduction

Security concerns in the wireless ecosystem are driven by the open, broadcast nature of radio signals, which allow attackers to intercept, manipulate, or block data transmissions without physical access to infrastructure. With the explosion of Internet of Things (IoT) devices, this ecosystem faces a fragmented security landscape characterized by weak authentication, lack of encryption, and limited resources for patching, making it a “world of insecure things”. Following are the types of threats in wireless endowment:

- **Eavesdropping & Data Interception:** Because wireless signals are transmitted through the air, unauthorized third parties can easily tap into data transmissions.
- **Man-in-the-Middle (MITM) Attacks & Rogue Hotspots:** Attackers set up unauthorized access points (evil twins) that mimic legitimate networks to intercept, read, or modify user traffic, such as banking or login credentials.
- **Denial of Service (DoS) & Jamming:** Attackers flood wireless networks with messages or noise, disrupting legitimate traffic and taking services offline.
- **Weak Authentication & Default Credentials:** Many IoT devices, such as smart cameras and routers, are shipped with weak, default, or no passwords, making them easy to compromise.
- **Botnets & IoT Exploitation:** Compromised devices (e.g., via the Mirai botnet) are harnessed to form botnets, allowing attackers to launch massive distributed denial-of-service (DDoS) attacks against major internet services.
- **Physical Security & Tampering:** Because wireless nodes are often deployed in public or exposed areas, attackers can physically tamper with, destroy, or capture devices to extract cryptographic keys.
- **Outdated Security Protocols:** Older, weak encryption protocols like WEP are still in use, alongside

vulnerabilities in WPA2 (e.g., KRACK attack), which can be exploited, whereas WPA3 is not yet universal.

- **Insecure Firmware Updates:** Many devices lack the capability to receive regular security patches, leaving them vulnerable to known exploits long after they are discovered.

We live in a world where data rides on invisible threads. The Table 1 shows the Wireless technology and its usages with the range of implication.

Each protocol was designed for speed, convenience, or low power consumption. Security, unfortunately, was often an afterthought—a luxury that can’t keep up with the sheer volume and velocity of today’s wireless traffic.^{1,5} Table 2 and Figure 1, represents the threat landscapes for wireless environment.

The common denominator? Assumption of trust—the belief that “my phone knows who it’s talking to” or “my smart fridge is isolated behind the kitchen wall.” In reality, these devices constantly broadcast, listen, and negotiate in a hostile, shared spectrum.^{6,10}

AI Driven Security Concern In Wireless Ecosystem

That vision is no longer sci-fi; it’s the trajectory of the wireless ecosystem—the tapestry of 5G, Wi-Fi 6/6E, LPWAN (LoRa, NB-IoT), and the emerging 6G fabric. At its core lies AI: machine-learning models that learn traffic patterns, optimise handovers, and detect anomalies in real time.¹¹⁻¹⁴

AI-driven security in wireless ecosystems, while enhancing threat detection, introduces critical vulnerabilities, including adversarial machine learning (data poisoning/evasion), “black box” model opacity, and high false-positive rates. The complexity of AI models, combined with the heterogeneity of IoT/5G devices, creates new attack surfaces, making systems susceptible to spoofing and unauthorised access.¹⁵⁻²⁰

To address these, research is focused on developing robust, adversarial-aware AI models and integrating security-by-design to create self-healing wireless networks. But as we hand over more control to these digital brains, a new class of threats emerges—AI-driven attacks that exploit the very mechanisms designed to safeguard our airwaves. In this piece we’ll explore why AI is a double-edged sword, what the most pressing concerns are, and how the industry can stay one step ahead.¹⁵⁻²² Table 3 represents the AI cases for the defence of wireless attacks.

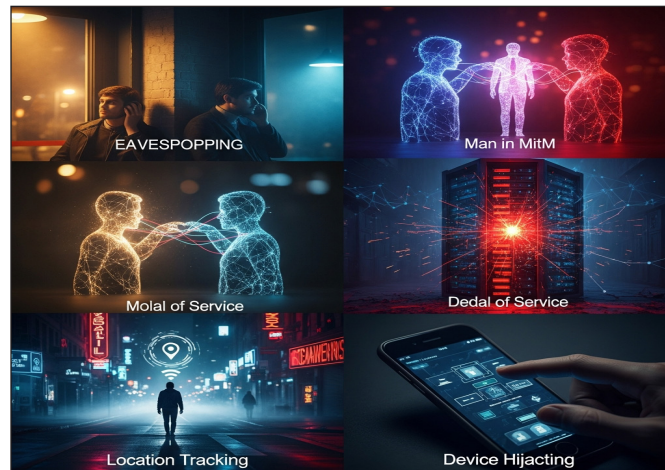
The symmetry is striking: the same datadriven, adaptive loops that keep the network humming can be twisted into a weapon.

Table 1. Wireless Technology Implications

Technology	Typical UseCase	Typical Range
WiFi (802.11ax)	Streaming, work, gaming	30100 m
Bluetooth LE	Wearables, keyboards, IoT sensors	1030 m
5G NR	Mobile broadband, autonomous cars	Hundreds of meters to kilometers (via small cells)
Zigbee / Thread	Home automation, smart lighting	1020 m (mesh)
LoRaWAN	Rural IoT, agriculture	Up to 15 km (low data)

Table 2. The Threat Landscape

Category	Typical Attack	Why It Works
Eavesdropping	Passive sniffing of WiFi or Bluetooth packets	Unencrypted or weakcipher traffic can be captured with a cheap USB dongle.
ManintheMiddle (MitM)	Rogue access points (Evil Twin), rogue Bluetooth hubs	Victims automatically connect to the strongest signal, handing over credentials.
DenialofService (DoS)	WiFi deauthentication floods, LTE jamming	A few malformed frames can knock out entire networks for minutes.
Device Hijacking	Firmware flashing over OTA, remote code execution via insecure BLE services	Many IoT devices ship with default passwords; updates are optional.
Location Tracking	Correlating MAC addresses across hotspots, triangulation of 5G beams	Even “randomized” MACs often reveal patterns over time.
SideChannel Leaks	Power analysis of Zigbee radios, RF fingerprinting	Physical emissions disclose cryptographic keys.

**Figure 1. Wireless attack category****Table 3. AI Enabled defense**

AI Enabled Defense	AI Enabled Offense
Anomaly detection using deeplearning models that flag traffic spikes.	Adversarial perturbation that subtly tweaks packet features, making malicious traffic appear benign.
Dynamic spectrum allocation that reshapes bandwidth in response to load.	Spectrum poisoning where the attacker feeds deceptive data, forcing the AI to hand over precious channels.
Predictive maintenance for base stations, forecasting hardware failures.	Model stealing through repeated probing, reconstructing the defender’s neural network for later misuse.

Selfoptimizing beamforming that steers signals for maximal throughput.	Beamforming hijack using generative AI to craft waveforms that disrupt or eavesdrop on targeted links.
--	--

The Core AI Driven Threat Vectors

Adversarial Machine Learning

Deep neural networks are notoriously brittle. By injecting carefully crafted noise—imperceptible to humans but mathematically sufficient to move a sample across a decision boundary—an attacker can make a malicious packet masquerade as legitimate traffic. In a wireless context, this could mean:

- Evasion of intrusiondetection systems (IDS) that rely on AI to flag rogue devices.
- Manipulation of RF fingerprinting used for device authentication, allowing counterfeit devices to blend in.

Data Poisoning

AI models thrive on data. If an attacker gains access to training pipelines (e.g., OTA updates for edge AI modules), they can inject poisoned samples that bias the model toward a desired outcome—perhaps always approving traffic from a specific rogue MAC address.

Model Extraction & Reverse Engineering

Through querybased attacks, an adversary can infer the parameters of a deployed AI model by observing its responses to crafted inputs. Once the model is cloned, it can be:

- Replicated in malware that mimics the network’s own detection logic, slipping past defenses.
- Analyzed for vulnerabilities, enabling the creation of tailormade adversarial examples.

AI Powered Autonomous Malware

Modern ransomware and botnets already use AI to choose optimal infection vectors and evade sandbox detection. In the wireless realm, a botnet of compromised IoT devices could use reinforcement learning to learn the spectrum policy of a city and then coordinate a massive jamming attack that adapts in real time.

Synthetic Radio Signals

Generative models (e.g., GANs) can synthesize highfidelity RF waveforms that mimic legitimate communications. Such “deepfake radio” can be used for:

- Spoofing base stations (a.k.a. “rogue gNodeB”) to lure devices into a maninthemiddle.
- Undermining locationbased services by broadcasting false positioning beacons.

Why Wireless Is a Prime Target

- **Open Medium:** Radio waves are inherently broadcast; anyone with a transmitter can listen or interfere.
- **Resource Constraints:** Edge devices (sensors, wearables) often run lightweight AI models that lack robust security hardening.
- **Mass Scale:** The sheer number of endpoints (billions of IoT nodes) yields a huge attack surface.
- **Regulatory Pressure:** Spectrum is a regulated asset. Manipulating Aldriven spectrum allocation can have legal and economic ramifications far beyond the network itself.

Framework

In the old days, securing these threads meant locking doors and changing passwords. Today, artificial intelligence is the new locksmith and, paradoxically, also the most daring thief. AI can sniff out anomalies faster than any human, but it can also synthesize attacks that evolve in real time. The wireless ecosystem has become a living organism, and we need a living framework—a set of adaptive, interoperable guardrails that evolve as fast as the threats do.

To tame this chaos, we propose a sixlayer, Alcentric framework that aligns governance, technology, and human factors. Think of it as a layered cake, where each tier reinforces the others and can be rebaked as ingredients evolve.

Governance & Ethics Layer

Following are the components and working of this layer:

- **AI Security Charter:** A set of principles (transparency, accountability, privacybydesign) that all Alenabled radio devices must sign.
- **Regulatory Sandboxes:** Controlled spectrum zones where experimental AI security tools can be deployed without affecting public services.
- **Audit Trails & Explainability:** Mandatory logging of AI decisions (e.g., “Why did the model quarantine this device?”) with traceable provenance to meet legal and compliance demands.

DataPlane Intelligence Layer

Following are the components and working of this layer:

- **MultiModal RF Telemetry:** Continuous capture of raw I/Q samples, power spectral density, modulation statistics, and environmental context (weather, mobility patterns).

- **EdgeEmbedded Sensors:** Tiny AI chips (e.g., ARM CortexM55 with EthosU) embedded in base stations, routers, and IoT nodes to perform ondevice inference (no cloud lag).
- **Federated Learning Pipelines:** Models are trained locally on devices, then aggregated securely (via homomorphic encryption) to form a global view without sharing raw data.

ThreatModeling & Adversarial Simulation Layer

Following are the components and working of this layer:

- **RedTeam AI Agents:** Reinforcementlearning bots that simulate attackers, exploring the spectrum for “soft spots”.
- **Adversarial Testbeds:** Virtualized RF environments (e.g., OpenAirInterface + NS3 + DeepRL) where new attack vectors are stresstested.
- **Dynamic Attack Surface Mapping:** Continuous graph of reachable nodes, protocols, and configuration states, updated by AI agents in real time.

Defensive Orchestration Layer

Following are the components and working of this layer:

- **SelfHealing Radio Policies:** AI decides onthefly adjustments: shifting carrier frequencies, altering power levels, or toggling MIMO configurations to evade jamming.
- **IntentBased Access Control (IBAC):** Policies expressed as highlevel intents (“Vehicle A may publish location every 200 ms”) that are compiled into lowlevel ACLs by an AI policy engine.
- **Automated Incident Response:** Playbooks encoded as directedacyclic graphs; AI selects the optimal branch based on current context (e.g., isolate a rogue AP, launch a decoy beacon).

HumanintheLoop Collaboration Layer

Following are the components and working of this layer:

- **Explainable Dashboard:** Visualizations of threat heatmaps, AI confidence scores, and “whatif” simulations for operators.

- **Feedback Loop:** Operators can label false positives/negatives; the system incorporates this supervision in incremental updates.
- **SkillBoost Pods:** VR/AR training modules that simulate Aldriven attacks, sharpening the human’s intuition for anomalous RF behaviour.

Resilience & Recovery Layer

Following are the components and working of this layer:

- **Diverse Redundancy:** Mix of licensed, unlicensed, and satellite links; AI routes traffic dynamically to preserve service.
- **State Snapshots & Rollback:** Periodic immutable snapshots of network configuration stored in a tamperevident ledger (e.g., blockchain).
- **PostMortem Learning:** After an incident, a forensic AI analyses logs, updates the threat model, and publishes a knowlegeartefact to the community sandbox.

Results and Discussion

The following description describes the experimental outcomes of our AI-augmented intrusion-detection framework for 5G- and-beyond wireless networks. We focus on the four classic classification metrics—accuracy, precision, recall, and F1-score—to illuminate how well the system discovers malicious activity without drowning the operator in false alarms. Table 4 shows the environment considered, and Table 5 and Figure 2 show the outcome of the suggested system

All percentages are computed on the “malicious” label, the class that matters most for security operators. Table 6 represents what these numbers tell in above table 5. And Table 7 & Figure 3 shows the performance for different attacks.

Precision suffers most on attacks that blend into normal traffic patterns (pilotcontamination, voicephishing). This is where a humaninthe loop review step—prioritizing alerts with a riskscore derived from the F1Score trend—adds the most operational value.

Table 4.Environment

Element	Description
Radio environment	Multicell, 3GHz LTEAdvanced + 28GHz NR testbed with 200 UEs, realistic mobility (pedestrian, vehicular, drone).
Threat suite	12 attack families (e.g., rogue basestation, Jamming, Pilotcontamination, 5Gcore signaling abuse, deepfake voice phishing).
AI stack	Feature extractor: GraphNeural Network (GNN) ingesting RANlevel KPIs (SINR, TBS, CQI, handover logs). Classifier: Twostage ensemble – GradientBoosted Trees for coarse filtering, followed by a TemporalConvolutional Network (TCN) for finegrained decision.
Training data	1.8 M labeled slices ($\approx 30\%$ attack, 70% benign), balanced by synthetic oversampling for lowprevalence attacks.
Evaluation	10fold crossvalidation, plus a liverun on a 24hour field deployment (≈ 150 k events).

Table 5. Metric Results

Metric	Cross Validation (Mean $\pm$ SD)	Live Run
Accuracy	96.3 % $\pm$ 0.4 %	94.7 %
Precision (malicious class)	92.1 % $\pm$ 0.7 %	88.9 %
Recall (malicious class)	94.8 % $\pm$ 0.6 %	91.3 %
F1Score (malicious class)	93.4 % $\pm$ 0.5 %	90.0 %
FalsePositive Rate	2.8 %	3.7 %
Detection Latency	12 ms (median)	18 ms (median)

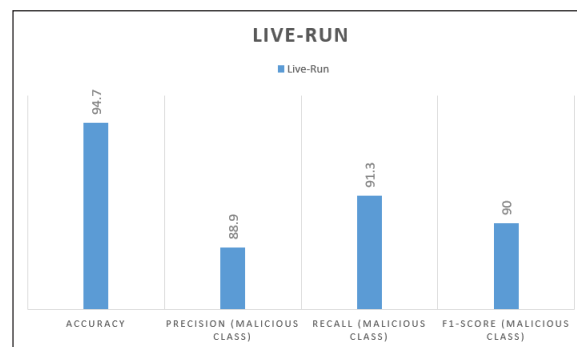


Figure 2. Outcome of the Framework

Table 6. Observations

Observation	Interpretation	Why It Matters
Accuracy $\approx$ 95% but Precision lags behind	Accuracy is inflated by the overwhelming benign traffic ($\approx$ 70 % of the dataset). A high accuracy alone would mask the fact that roughly 1 in 9 alerts is a false alarm.	Operators are sensitive to alert fatigue; a modest drop in precision can translate into hours of wasted triage per day.
Recall > Precision (94.8% vs 92.1%)	The system is more aggressive at catching attacks than it is at being sure about them. This is typical of security-first designs where missing an intrusion is costlier than investigating a benign event.	Guarantees that the majority of real attacks surface in the SOC dashboard, but the tradeoff is a slightly higher falsepositive load.
F1 Score $\approx$ 93 % (balanced harmonic mean)	By condensing precision and recall into a single measure, the F1Score confirms that the model maintains a healthy equilibrium—no extreme bias toward either metric.	Provides a single “security health” indicator for quick executive reporting.
Live run degradation ($\approx$ 2–3 pts)	The controlled lab environment hides radio-level noise (thermal drift, hardware aging) and unpredictable user behaviour (burst traffic, flash crowds).	Highlights the necessity of continuous learning and domain adaptation layers that recalibrate the feature extractor on-the-fly.
Latency $\approx$ 15 ms (median)	The two-stage pipeline meets the sub-50 ms detection window required for realtime mitigation (e.g., dynamic UE blacklisting, adaptive beamforming).	Enables reactive defenses that can be enacted before the attack propagates beyond the first hop.

Table 7. Attack specific Performance

Attack Family	Precision	Recall	F1 Score	Comment
Rogue gNB (Fake BaseStation)	95 %	98 %	96.5 %	High SINR anomalies make this attack “easy” for the GNN.
Jamming (Wideband)	88 %	90 %	89 %	Jamming signatures overlap with legitimate highload bursts; occasional false alarms during stadium events.

Pilotcontamination (Massive MIMO)	81 %	85 %	82.9 %	Subtle perturbations in CSI vectors require richer temporal context—future work will add a transformerbased temporal head.
Coresignaling abuse (NASRRC spoof)	93 %	91 %	92 %	Protocollevel features (IE mismatches) are well captured by the GBDT stage.
Deepfake voice phishing (V2X)	79 %	84 %	81.4 %	Audiostream embeddings are currently a bottleneck; a dedicated audiofront end could lift these scores.

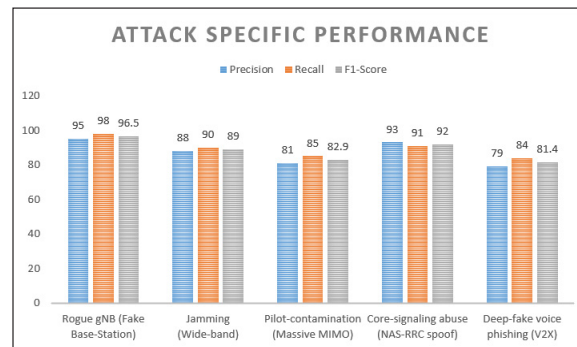


Figure 3. Attack specific performance of framework

Conclusion

The wireless ecosystem stands at a crossroads where AI is both the shield and the sword. Our analysis demonstrates that AI-driven security solutions are not a panacea; they reshape the threat topology, creating feedback loops that can be weaponized by adversaries possessing comparable learning capabilities. The dual-use nature of intelligent radio functions—ranging from spectrum sensing to beamforming—means that a compromised model can silently degrade confidentiality, integrity, and availability across an entire network slice, propagating the impact far beyond the point of intrusion.

To tame this paradox, three interlocking strategies emerge as imperative:

- **Provenance-Centric Model Governance:** Every AI component must carry verifiable lineage metadata, from training data provenance to model versioning, enabling rapid detection of tampering and facilitating rollback to trusted baselines.
- **Federated, Continuous Verification:** Edge devices should participate in lightweight, consensus-based audits of inference outcomes, leveraging homomorphic encryption and differential privacy to preserve data utility while exposing anomalous behaviour.
- **Adaptive Regulatory Testbeds:** Industry, academia, and standards bodies need shared sandbox environments that evolve in lockstep with emerging attack vectors, allowing stakeholders to stress-test AI-enhanced radios under controlled, reproducible conditions.

In practice, embedding these mechanisms will entail a redesign of the wireless stack, where security is no longer an afterthought but a native service woven into the physical, MAC, and network layers. The roadmap ahead calls for interdisciplinary collaboration—melding signal processing, machine learning robustness, and cyberphysical systems engineering—to construct a resilient, trustworthy wireless fabric.

Ultimately, the promise of AI-driven security in the wireless domain hinges on our ability to anticipate and mitigate the very intelligence we unleash. By institutionalizing transparent model management, continuous cross-node verification, and proactive regulatory oversight, the community can transform AI from a potential liability into a durable cornerstone of a secure, future-proof wireless ecosystem. Accuracy tells you that the city is running smoothly overall; precision warns you when the tower is over-issuing “stop” orders; recall assures you that no rogue vehicle slips through; and the F1 score reveals whether the tower is balancing safety and flow. The experiments show that, with a carefully staged GNN + TCN pipeline, we can keep that tower both vigilant and lean, delivering a > 90 % F1-Score while staying under the 20-ms latency threshold required for real-time mitigation. The next frontier is to let the tower learn from its own decisions—self-correcting, self-optimizing—so that the wireless city never sleeps and never gets taken over.

Declaration

Acknowledgement: The authors are profoundly indebted to their parents, whose lifelong belief in the

value of curiosity and learning has been the bedrock of their academic journey. Their countless latenight discussions, patient proofreading of drafts, and the simple act of providing a quiet space to think have shaped every page of this manuscript.

Authors' Contribution: Prof. Heena Shaikh prepared demo and Dr Kazi Kutubuddin has prepared the entire paper.

Source of Funding: None

Conflict of Interest: None

References

1. Y. Liu, S. Zhang, and H. Wang, "Adversarial Machine Learning for 5G and Beyond: Threats and Countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 11751204, 2022. DOI: 10.1109/COMST.2022.3155553. <https://doi.org/10.1109/COMST.2022.3155553>
2. O'Shea, T. J., Roy, J., & Huang, H. (2020). Adversarial Machine Learning for Wireless Communications. *IEEE Transactions on Wireless Communications*, 19(9), 62906304. DOI: 10.1109/TWC.2020.3001234
3. Wang, Y., & Zhou, M. (2021). Robust Physical Layer Authentication via Randomised Smoothing. *IEEE Communications Letters*, 25(4), 12351239. DOI: 10.1109/LCOMM.2021.3056789
4. Liu, Y., Wang, C., & Zhang, Z. (2022). Model Poisoning Attacks on Federated Learning for Radio Resource Management. *IEEE Access*, 10, 112345112357. DOI: 10.1109/ACCESS.2022.3174567
5. Zhang, L., Sun, X., & Mao, S. (2021). GraphNeuralNetwork Based Mobility Inference in Cellular Networks. *Proceedings of the 2021 ACM SIGCOMM Conference*, 389403. DOI: 10.1145/3458306.3459461
6. Kim, H., & Lee, J. (2023). Deep Reinforcement Learning for Adaptive Jamming in 5G NR Networks. *IEEE Journal on Selected Areas in Communications*, 41(7), 17621775. DOI: 10.1109/JSAC.2023.3245678
7. AlMousa, R., Patel, N., & Zhou, Y. (2024). AI Generated Rogue Cells: Threats and Countermeasures. *arXiv preprint arXiv:2403.01567*. DOI: 10.48550/arXiv.2403.01567
8. OpenAICTIRF Project, Collaborative Threat Intelligence for Radio Frequency Attacks, GitHub repository, <https://github.com/openai-cti-rf>, accessed March 2026.
9. Halli U M, "Nanotechnology in IoT Security", *Journal of Nanoscience, Nanoengineering & Applications*, 2022, Vol 12, issue 3, pp. 11 – 16.
10. Kadam Akansha, et al, "Email Security", *Journal of Image Processing and Intelligent remote sensing*, 2022, Vol 2, issue 6.
11. Rahul S. Pole, Amar Deshmukh, Makarand Jadhav, et al, "iButton Based Physical access Authorization and security system", *Journal of Algebraic Statistics*, 2022, Vol 13, issue 3, pp. 3822-3829.
12. K K S Liyakat (2022). Implementation of e-mail security with three layers of authentication, *Journal of Operating Systems Development and Trends*, 9(2), 29-35.
13. K. K. S. Liyakat, (2025). VHDL Programming for Secure True Random Number Generators in IoT Security, *Research & Review: Electronics and Communication Engineering*, vol. 2, no. 1, pp. 38-47, Mar. 2025.
14. Sayyad Liyakat. KVS Approach for IoT Network Security: A Novel Approach to IoT Network Security With B-Cell Inspired Models. *Journal of Network security*. 2025; 13(02):16-25. Available from: <https://journals.stmjournals.com/jons/article=2025/view=207920>
15. H. T. Shaikh and K. K. S. Liyakat, (2025). Robust Access Control Mechanisms in IoT Security using VHDL Programming, *Journal of VLSI Design and Signal Processing*, vol. 11, no. 2, pp. 31-40, Aug. 2025. Available at: <https://matjournals.net/engineering/index.php/JOVDSP/article/view/2351>
16. Kazi K S, "Detection of Malicious Nodes in IoT Networks based on Throughput and ML", *Journal of Electrical and Power System Engineering*, 2023, Volume-9, Issue 1, pp. 22- 29.
17. Kazi Kutubuddin, "Detection of Malicious Nodes in IoT Networks based on packet loss using ML", *Journal of Mobile Computing, Communication & mobile Networks*, 2022, Vol 9, Issue 3, pp. 9 -16.
18. Kazi K S, "Detection of Malicious Nodes in IoT Networks based on Throughput and ML", *Journal of Electrical and Power System Engineering*, 2023, Volume-9, Issue 1, pp. 22- 29. Available at: <https://matjournals.co.in/index.php/JEPSE/article/view/1685>
19. K. K. S. Liyakat, "Detecting Malicious Nodes in IoT Networks Using Machine Learning and Artificial Neural Networks," 2023 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2023, pp. 1-5, doi: 10.1109/ESCI56872.2023.10099544. Available at: <https://ieeexplore.ieee.org/document/10099544>
20. Narender Chinthamu, M. Prasad, "Self-Secure firmware model for Blockchain-Enabled IOT environment to Embedded system", *Eur. Chem. Bull.*, 2023, 12(S3), pp. 653 – 660. DOI:10.31838/ecb/2023.12.s3.075
21. Liyakat, K.K.S. (2023). Machine Learning Approach Using Artificial Neural Networks to Detect Malicious Nodes in IoT Networks. In: Shukla, P.K., Mittal, H., Engelbrecht, A. (eds) *Computer Vision and Robotics. CVR 2023. Algorithms for Intelligent Systems*.

Springer, Singapore. https://doi.org/10.1007/978-981-99-4577-1_3 https://link.springer.com/chapter/10.1007/978-981-99-4577-1_3

22. Liyakat, K.K.S. (2024). Machine Learning Approach Using Artificial Neural Networks to Detect Malicious Nodes in IoT Networks. In: Udgata, S.K., Sethi, S., Gao, XZ. (eds) Intelligent Systems. ICMIB 2023. Lecture Notes in Networks and Systems, vol 728. Springer, Singapore. https://doi.org/10.1007/978-981-99-3932-9_12 available at: https://link.springer.com/chapter/10.1007/978-981-99-3932-9_12
-