UDC 004.056.5
IRSTI 05.13.19

https://doi.org/10.55452/1998-6688-2026-23-1-197-208

***[1]Imanbayev A.Zh.,**
Assistant Professor, ORCID ID: 0000-0003-3719-4091,
e-mail: imanbaevazamat@gmail.com
[2]Berdibayev R.S.,
Professor, ORCID ID: 0000-0002-8341-9645,
e-mail: r.berdybaev@aues.kz
[3]Odarchenko R.S.,
Professor, ORCID ID: 0000-0002-7130-1375,
e-mail: odarchenko.r.s@ukr.net
[4]Tynymbayev S.,
Professor, ORCID ID: 0000-0002-9326-9476,
e-mail: s.tynym@mail.ru

[1]Kazakh-British Technical University, Almaty, Kazakhstan
[2]Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan
[3]State University «Kyiv Aviation Institute», Kyiv, Ukraine
[4]International Information Technology University, Almaty, Kazakhstan

IINTELLIGENT HYBRID METHOD FOR AUTOMATED PENETRATION TESTING IN 5G AND BEYOND NETWORKS

Abstract

The evolution of 5G and the anticipated introduction of 6G technologies significantly increases network complexity through service-based architecture, network slicing, virtualization and distributed cloud-native functions. These advancements improve scalability and flexibility but simultaneously expand the attack surface and introduce novel vulnerabilities. Traditional penetration testing methodologies are not suitable for such dynamic and virtualized environments because they rely on static procedures and manual testing that cannot match the speed and structural variability of modern mobile networks. In parallel, machine learning–based intrusion detection systems (IDS) demonstrate strong capabilities in detecting anomalous and zero-day behaviors but operate independently from penetration testing processes. This paper presents an intelligent hybrid method for automated penetration testing in 5G and beyond networks, integrating a machine-learning intrusion detection system based on incremental learning, autoencoders and generative adversarial networks (GANs) – with an attack optimization module driven by the Differential Evolution (DE) algorithm. Instead of a genetic algorithm, DE is employed due to its fast convergence, robustness to local minima, and suitability for optimizing high-dimensional representations of attack strategies. An experimental evaluation on a real OpenAirInterface-based 5G Standalone testbed demonstrates that the DE-driven approach improves vulnerability identification efficiency, produces optimal multi-stage attack strategies, and enables realistic automated penetration scenarios. These results indicate that DE-based optimization provides a scalable, adaptive and efficient foundation for continuous security assessment of next-generation mobile networks.

Keywords: 5G security, intrusion detection system, Differential Evolution, automated penetration testing, attack graph.

Received: November 19, 2025; revised: March 2, 2026, March 10, 2026; accepted: March 16, 2026.

Introduction

5G Standalone deployments increasingly rely on service-based architecture, network slicing, MEC, and cloud-native virtualization of core functions [1–3]. While these mechanisms improve

elasticity and service agility, they also create a security environment that changes at runtime: network functions are instantiated and scaled on demand, slices share infrastructure, and control-plane and user-plane components interact through numerous APIs and protocols. As a result, the attack surface expands, and identifying multi-stage compromise chains becomes more difficult compared with relatively static networks [4].

Penetration-testing standards such as OSSTMM, PTES, NIST SP 800-115, and OWASP provide valuable guidance for conventional IT infrastructures, but they assume relatively stable assets and rely primarily on manual execution. In 5G networks, slice composition, exposure points, and virtualized network functions can change faster than periodic assessments can track, which makes static test plans difficult to maintain and expensive to scale [5–8]. Consequently, relying only on manual and procedure-driven penetration testing provides limited and potentially outdated evidence of resilience in cloud-native 5G deployments [9].

Machine-learning-based intrusion detection systems (IDS) have demonstrated strong capability in detecting anomalous and previously unseen behaviors in high-volume 5G traffic [10, 11]. However, in most operational workflows, IDS output remains limited to alerts and classification results, while penetration testing focuses on generating and validating exploitation steps. This separation prevents detections observed in a live network from being systematically converted into hypotheses about feasible multi-stage attack sequences and then validated through controlled execution.

Motivated by this gap, we propose an intelligent hybrid method that couples an ML-based IDS (autoencoder reconstruction with incremental updates and GAN-based augmentation) with attack graph reasoning and DE optimization to generate and rank multi-stage attack strategies, forming a feedback-driven closed loop where detections refine the attack graph and executed paths update the IDS [12]. The method is validated on an OpenAirInterface-based 5G Standalone (SA) testbed and assumes a remote adversary with limited initial access, excluding physical access and management-plane compromise.

The contributions of this work are as follows:

1. A hybrid intrusion detection and attack graph generation pipeline capable of translating detected anomalies into structured multi-stage exploitation opportunities.
2. A DE–based optimization mechanism for identifying high-impact, high-probability attack paths while balancing success probability, impact and execution cost in dynamic 5G environments.
3. A fully automated 5G Standalone (SA) testbed implementation used to evaluate the effectiveness and realism of the proposed method.

Together, these components form an automated security-assessment workflow that continuously links anomaly detection with attacker-centric reasoning and optimization-driven penetration testing.

Materials and methods

Background and Related Work

Machine learning–based intrusion detection in 5G has been actively studied using deep learning models, autoencoders, GAN-based augmentation, and incremental learning to distinguish malicious and benign traffic [10, 13]. Although such systems can be effective at anomaly detection, they are typically alert-centric: they detect anomalies but do not translate detections into attacker-centric hypotheses about feasible multi-stage compromise chains, nor do they provide evidence by systematically validating such hypotheses through controlled exploitation.

Network analytics frameworks such as NWDAF enhance observability by enabling structured data collection and statistical evaluation of service behavior [14]. However, their primary goal is monitoring and deviation detection; they do not construct executable adversarial scenarios or reason about how observed deviations can be chained into multi-stage attacks under realistic attacker constraints.

In parallel, automated penetration testing and attack graph reasoning model attacker capabilities, privilege transitions, and vulnerability dependencies to support multi-stage analysis [15, 16].

Evolutionary search (e.g., genetic algorithms) has been used to explore large attack spaces, but it may suffer from premature convergence or stagnation when the search space becomes high-dimensional or changes over time [15]. DE provides robust convergence characteristics with a comparatively simple control scheme, which makes it attractive for optimizing complex attack strategies [17]. Nevertheless, existing approaches rarely integrate ML-based IDS, attack graph construction, and DE-driven optimization into a feedback-driven closed loop that continuously re-prioritizes attack hypotheses based on live traffic observations.

Literature, therefore, lacks an integrated mechanism that (i) converts IDS detections into attack graph updates, (ii) optimizes multi-stage strategies under explicit success/impact/cost trade-offs, and (iii) validates the resulting strategies through automated execution with feedback to refine both detection and attack reasoning. This motivates the unified hybrid method proposed in this paper [18].

Classical penetration testing methodologies such as OSSTMM, PTES, NIST SP 800-115, OWASP remain widely used, but their static structure and procedural rigidity limit their applicability to highly dynamic, virtualized and reconfigurable 5G architectures [5–8]. Table 1 summarizes these methodologies and highlights their limitations in the context of 5G security assessment, motivating the need for an automation-driven closed-loop approach.

Table 1 – Comparison of classical penetration testing methodologies and their applicability to 5G networks

Methodology	Description	Strengths for 5G	Limitations for 5G
OSSTMM (Open-Source Security Testing Methodology Manual)	Comprehensive framework for security testing.	Thorough analysis of all attack vectors.	Does not provide explicit guidance on advanced 5G-specific features (e.g., network slicing, virtualization, etc.).
ISSAF (Information Systems Security Assessment Framework)	Framework for security assessments.	Useful for assessing organizational risks in 5G.	Focuses more on traditional systems, limited applicability to dynamic and distributed 5G architectures.
PTES (Penetration Testing Execution Standard)	Standardized approach to penetration testing.	Clear guidelines can be adapted for 5G environments.	Lacks coverage of high-frequency vulnerabilities and IoT-specific threats common in 5G networks.
NIST SP800-115	Guidelines for conducting penetration testing.	Strong focus on risk management applicable to 5G.	Primarily designed for traditional IT infrastructure penetration testing. Does not address 5G-specific protocols (NGAP, HTTP/2, PFCP), network slicing isolation vulnerabilities, or virtualized network function exploitation. Lacks guidance on testing service-based architecture (SBA) security and cloud-native 5G deployments.
OWASP	Focused on web application security.	Valuable for testing web components of 5G networks.	Exclusively focused on web application security (OWASP Top 10). Does not cover Radio Access Network attacks, core network signaling vulnerabilities, or 5G-specific threat vectors such as slice hijacking, SUPI exposure, or gNodeB compromise scenarios.

Proposed Intelligent Hybrid Method

The proposed method implements a feedback-driven closed loop that links anomaly detection to automated penetration testing in 5G networks. First, the IDS monitors signaling and user-plane traffic and produces anomaly indicators. These indicators are then converted into attack graph updates, after

which DE searches the graph to generate and rank multi-stage attack strategies under a success/impact/cost fitness formulation. Finally, the top-ranked strategy is executed in a controlled environment, and the resulting execution traces are fed back to refine both the IDS boundaries and subsequent attack graph prioritization. The output of each cycle is a ranked set of multi-stage strategies and an execution log that updates detection and attack reasoning. The overall system architecture is shown in Figure 1.

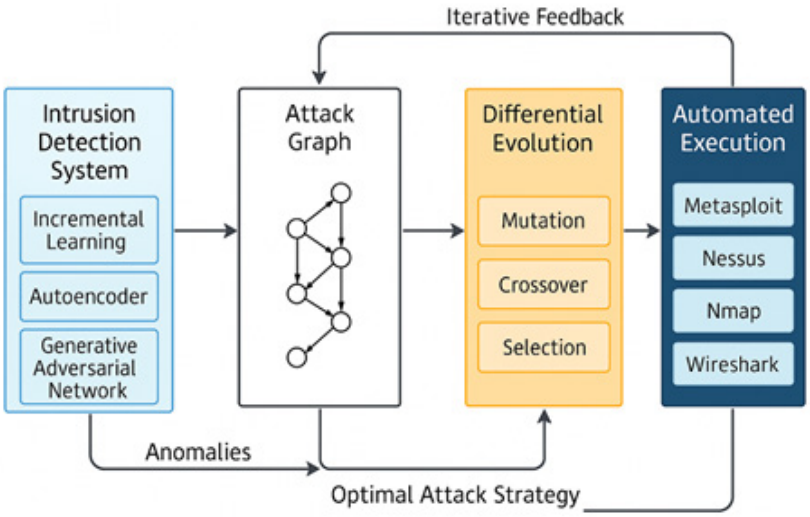

Figure 1 – Closed-loop architecture integrating IDS-driven anomaly detection, attack graph construction, DE-based strategy optimization, and automated execution with feedback for iterative refinement

Hybrid Intrusion Detection System

The IDS monitors signaling and user-plane traffic across the 5G Core and radio access network. A deep autoencoder reconstructs the statistical properties of benign traffic; deviations between input and reconstruction indicate anomalous behavior. An anomaly score is computed from the reconstruction error, and the decision threshold is calibrated on a benign validation subset. To maintain adaptability within the evolving environment of 5G networks, the incremental learning updates model parameters as new traffic distributions appear.

To improve the detection of rare or unseen threat categories, a Generative Adversarial Network (GAN) synthesizes realistic malicious samples. In our implementation, these generated samples are used as feature-level augmentations rather than raw packet traces. These generated samples augment the training set and strengthen the discriminative boundaries within the latent representation space of the autoencoder.

Attack Graph Construction

Detected anomalies are translated into attack graph facts and transitions. The attack graph is represented as a directed structure in which nodes capture security-relevant states (e.g., privilege level, access to a network function, or compromise of a slice-specific resource) and edges denote feasible adversarial transitions derived from misconfigurations, vulnerabilities, or signaling weaknesses. The graph models potential multi-stage adversarial behavior by capturing privilege escalation, lateral movement, and chained exploitation paths.

In our implementation, anomaly indicators produced by the IDS are mapped to a MulVAL-based reasoning model used to materialize attack graph predicates and derivation rules. Vulnerability facts and exposure conditions are obtained from scanner outputs and controlled misconfiguration injections, while reachability relations are derived from the testbed topology and access-control

settings. IDS detections are used to update the likelihood (or priority) of exploit transitions consistent with observed anomalous behavior, enabling runtime refinement of feasible multi-stage paths. This makes the attack graph a dynamically updated representation aligned with live traffic rather than a static artifact.

Mathematical Formulation of the Optimization Problem

The 5G network is represented as a directed graph:

$$G = (V, E),$$

where vertices V denote security-relevant states and edges E denote feasible adversarial transitions.

Each edge $e \in E$ is assigned three quantities:

$P(e)$: probability of exploit success,

$I(e)$: impact score,

$C(e)$: operational cost.

A candidate attack strategy S is a sequence of edges. Its fitness is defined as:

$$F(S) = \alpha \cdot P(S) + \beta \cdot I(S) - \gamma \cdot C(S),$$

where S represents an attack strategy (sequence of edges in the attack graph), $P(S)$ is the cumulative success probability computed as the product of individual exploit success rates along the path, $I(S)$ denotes the aggregated impact score based on CVSS severity and affected slice criticality, and $C(S)$ represents the operational cost including detection likelihood and resource expenditure. In this work, $I(S)$and $C(S)$are computed as additive scores over the selected edges, and impact/cost terms are normalized to a comparable scale before aggregation. Candidate strategies are constrained by a maximum hop length and must correspond to feasible transitions in the attack graph; infeasible paths or cycles beyond the hop limit are penalized in fitness.

The weighting parameters α, β, and γ are configured to balance exploration of high-impact paths against practical constraints. In our experiments, we set $\alpha = 0.5$, $\beta = 0.3$, and $\gamma = 0.2$ after empirical tuning on a validation subset of the attack graph.

This formulation transforms multi-stage penetration testing into a formal optimization problem.

Differential Evolution Optimization

Each DE individual is represented as a real-valued vector that is deterministically mapped to a discrete multi-stage path in the attack graph (node/edge indices). To enforce feasibility, candidates are projected to valid transitions by removing invalid edges, limiting hop length, and applying a simple repair step that reconnects broken sequences using a valid connector path when possible; otherwise, the candidate is penalized in fitness.

DE is employed to optimize the attack strategy selection process by searching for high-fitness solutions in the attack graph. A population of candidate strategies is initialized and iteratively evolved through mutation, crossover, and selection. Each candidate encodes a potential attack path, and its fitness is evaluated based on the objective function defined in the previous section. DE is well-suited for optimizing complex and non-linear objective functions in high-dimensional and dynamically changing attack spaces such as cloud-native 5G deployments.

In experiments, DE was configured with a population size of 40, a mutation factor of 0.6, a crossover rate of 0.7, and 50 generations.

Threat model

The framework assumes a realistic adversary model consistent with contemporary 5G deployments. The attacker begins with limited initial access — for example, a compromised UE connected to a gNB or low-privileged access inside a virtualized network function. The adversary possesses only partial knowledge of network structure obtainable through reconnaissance of exposed interfaces and can exploit misconfigurations, publicly known vulnerabilities, and malformed signaling exchanges.

However, the attacker is restricted from accessing physical hardware, extracting operator cryptographic keys, or compromising the management plane. These constraints ensure that all attack paths generated by DE remain feasible for a remote adversary operating under realistic resource limitations given the modeled reachability and vulnerability facts of the testbed.

Experimental setup

The proposed hybrid method was evaluated on a fully operational 5G Standalone (SA) testbed built using OpenAirInterface (OAI). The objective of the experimental environment was to replicate the behavior of a realistic 5G deployment while maintaining complete control over signaling flows, traffic generation and system instrumentation.

The radio access network was implemented using an OAI-based gNB connected to a USRP B210 software-defined radio. The RF configuration followed the n78 band, operating at 3.5 GHz with a 20 MHz channel bandwidth. The system used a subcarrier spacing (SCS) of 30 kHz and numerology $\mu = 1$, consistent with 5G NR mid-band deployments. The SDR front-end was configured with a 30.72 MS/s sampling rate and an RF gain of 65 dB, ensuring reliable downlink and uplink transmission under controlled conditions. This setup enabled the generation and capture of both user-plane and control-plane traffic for anomaly detection and penetration testing procedures.

The 5G Core was deployed as a set of virtualized network functions running on an Intel Xeon server equipped with 128 GB RAM and KVM virtualization. Individual VMs hosted AMF, SMF, UPF and NRF, each configured with Ubuntu 22.04. This modular deployment made it possible to introduce controlled misconfigurations, expose vulnerable services and manipulate slice-specific isolation settings during the evaluation.

User-plane traffic and signaling activity were generated using a software UE emulator capable of producing TCP, UDP and NAS/NGAP exchanges under adjustable load conditions. The hybrid IDS monitored traffic across the AMF, SMF and UPF interfaces as well as the OAI-gNB. Anomaly indicators derived from the IDS were mapped onto the MulVAL-based attack graph, which was subsequently processed by the DE engine responsible for identifying multi-stage attack strategies.

For IDS evaluation, the model was trained on the 5G-NIDD dataset and compared against an incremental-learning-only baseline. For optimization baselines, we compared DE against genetic algorithms, particle swarm optimization and random search.

All system modules — IDS, attack graph builder, DE optimizer and execution engine — operated within a unified orchestration layer that logged system state, detection outcomes, exploitation steps and deviations between predicted and observed behavior. This integration ensured that the testbed not only served as a platform for evaluating detection performance but also enabled full automation of penetration testing workflows. The complete testbed architecture is shown in Figure 2.

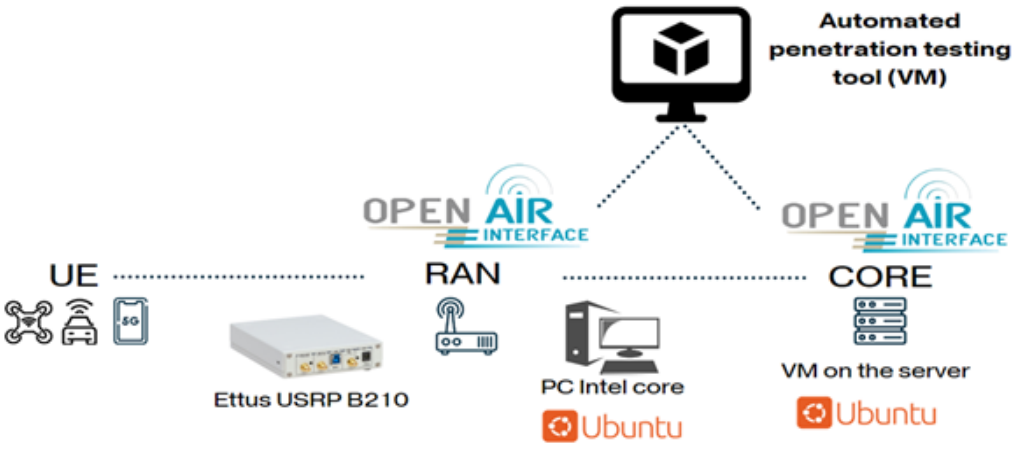

Figure 2 – Experimental 5G Standalone testbed composed of an OAI-based gNB, USRP B210 radio hardware, a virtualized 5G Core and an automated penetration testing host

Results and discussion

The proposed hybrid method was evaluated on a fully operational 5G Standalone testbed to assess (i) whether IDS-driven anomaly detection is sufficiently reliable to trigger attacker-centric reasoning, (ii) whether vulnerability evidence can be translated into multi-stage exploitation hypotheses via an attack graph, and (iii) whether DE can efficiently prioritize high-quality multi-stage strategies under the proposed fitness formulation. Overall, the results support the central claim of this work: integrating intrusion detection, attack-graph reasoning, and optimization into a feedback-driven workflow improves both the quality of discovered attack chains and the practicality of automated security assessment in dynamic 5G environments.

The analysis begins with intrusion detection performance. The hybrid IDS was trained on the 5G-NIDD dataset and compared against an incremental-learning-only baseline. Figure 3 consolidates the F1-score comparison for both known attack scenarios (left panel) and the previously unseen UDPScan trace (right panel). On known attacks, the baseline reaches an F1-score of 0.61, whereas the proposed hybrid IDS reaches 0.98, indicating substantially stronger detection under the evaluated workload. On the unseen UDPScan trace, generalization improves from 0.30 (baseline) to 0.87 (hybrid), suggesting that the hybrid training strategy strengthens sensitivity to low-frequency and novel behaviors–an essential property when IDS outputs are used to steer downstream attack-graph refinement rather than only to raise alerts. This result indicates that GAN-augmented training and incremental updates significantly improve the model's ability to generalize to previously unseen attack patterns.

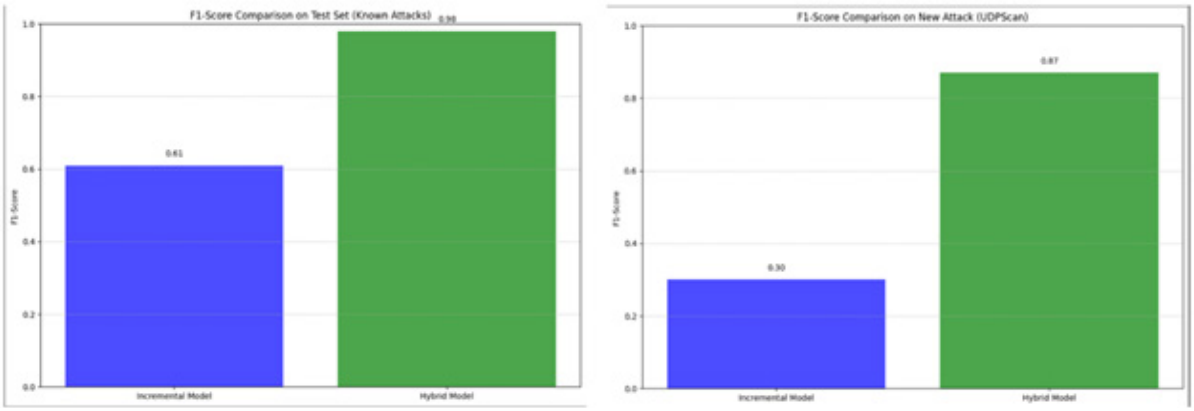

Figure 3 – F1-score comparison of the incremental baseline and the proposed hybrid IDS on known attack scenarios and the previously unseen UDPScan trace

Class-wise metrics confirm that the improvement is not driven by a single-class trade-off. For the incremental baseline, performance is notably imbalanced: for the malicious class, recall is 0.37 with precision 1.00 (F1 0.54), while the benign class shows recall 1.00 with precision 0.51 (F1 0.68), resulting in 0.62 overall accuracy and macro-F1 of 0.61. In contrast, the proposed hybrid IDS achieves balanced performance across both classes: for benign traffic it reaches precision/recall/F1 of 1.00/0.97/0.98, and for malicious traffic it reaches 0.97/1.00/0.98, with 0.98 overall accuracy. This balance matters for the closed-loop design: skewed class behavior would either over-trigger penetration cycles or miss meaningful multi-stage hypotheses, whereas the hybrid IDS provides stable triggers for subsequent attacker-centric analysis.

After validating detection quality, attention was directed to the testbed attack surface to establish a factual basis for multi-stage reasoning. A security scan identified 25 vulnerabilities across 15 network elements, including exposed management interfaces, insecure SCTP configurations, insufficient slice isolation, misconfigured APIs, and outdated services. Table 2 summarizes the distribution of findings across testbed components and severity levels, and these findings are treated as prerequisites and

transition enablers in the attack graph. Importantly, the attack-graph view highlights why multi-stage reasoning is necessary: issues that appear moderate in isolation can form high-impact chains when combined through reachable interfaces, privilege transitions, and slice-specific dependencies in a virtualized core. This observation motivates attacker-centric path search rather than isolated, single-step vulnerability ranking in cloud-native 5G deployments.

Table 2 – Distribution of detected vulnerabilities across 5G SA testbed components

Network Function	Critical	High	Medium	Low	Total
gNB (OAI-based)	1	2	2	2	7
AMF (Core)	2	1	1	0	4
SMF (Core)	1	1	1	0	3
UPF (User Plane)	2	2	0	0	4
NRF / NSSF / PCF (Support Functions)	0	1	1	0	2
Firewall / Routing Layer	1	1	1	0	3
Penetration Testing Host Exposure	0	1	1	0	2
Total	7	9	7	2	25

Critical and high-severity findings concentrate in the gNB, AMF, and UPF, which explains why optimized multi-stage paths repeatedly traverse these functions as high-leverage transitions. The DE optimization engine was then applied to the constructed attack graph to identify realistic and impactful multi-stage strategies under the fitness formulation balancing success probability, impact, and execution cost. DE was configured with a population size of 40, mutation factor 0.6, crossover rate 0.7, and 50 generations. In comparison with alternative heuristics (genetic algorithms, particle swarm optimization, and random search), DE reaches high fitness values earlier and does so more reliably within the same computational budget. Convergence is assessed by tracking the best fitness value per generation. This behavior indicates that DE provides an effective exploration–exploitation balance for high-dimensional attack spaces where feasible paths may evolve as the attack graph is updated based on new detections. Figure 4 reports the convergence comparison, showing faster and more stable fitness improvement for DE relative to GA and PSO, while random search remains inconsistent.

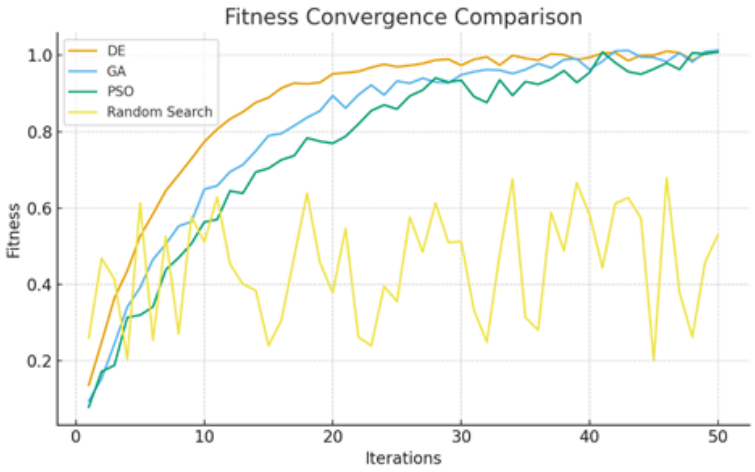

Figure 4 – Fitness Convergence Comparison

Execution-time measurements, presented in Figure 5, further emphasize DE's advantages. Although random search completed fastest, it failed to identify meaningful attack strategies. GA and

PSO required significantly more time to converge, while DE maintained a favorable balance between computation time and optimization quality. These results demonstrate that DE can be efficiently integrated into near real-time penetration testing workflows, where both speed and solution quality matter.

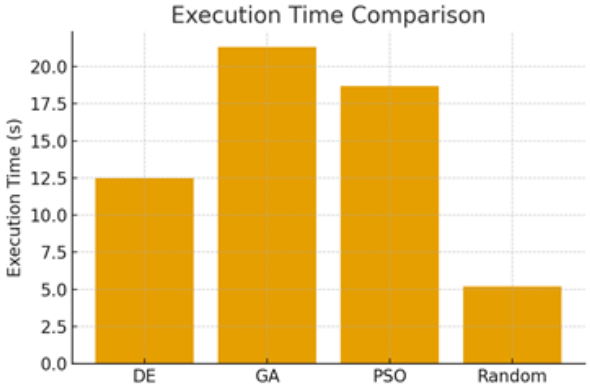

Figure 5 – Execution Time Comparison

Finally, the IDS and DE optimizer were integrated into a unified feedback-driven workflow. When the IDS detects new anomalies – either from real traffic deviations or augmentation-induced rare patterns – these signals refine the attack graph and steer the optimizer toward newly relevant regions of the search space; conversely, execution traces from DE-generated strategies feed back into detection updates, improving the stability of IDS boundaries over repeated cycles. Across repeated test cycles, this closed-loop mechanism produced measurable operational gains. We quantify closed-loop gains using anomaly-detection latency (time from attack onset to IDS trigger), optimization-cycle time (end-to-end strategy search time per iteration), and sensitivity on the evaluation set. Anomaly detection time decreased by 41%, the average optimization cycle shortened by 33%, and sensitivity to previously unseen threats improved by approximately 15%. These outcomes indicate that the proposed approach yields not only higher offline detection/optimization metrics, but also practical acceleration of end-to-end automated assessment in a dynamic 5G setting.

Conclusion

This paper proposed a closed-loop intelligent method for automated penetration testing in 5G and beyond networks that integrates a hybrid machine learning–based intrusion detection system, attack-graph reasoning, and DE optimization to generate and prioritize multi-stage attack strategies. Unlike approaches that treat intrusion detection and penetration testing as separate workflows, the proposed architecture uses IDS outputs to refine attack-graph hypotheses and feeds execution outcomes back to improve subsequent detection and strategy selection.

Experimental validation on an OpenAirInterface-based 5G Standalone testbed demonstrated that the hybrid IDS significantly improves detection performance over an incremental-only baseline, achieving F1-scores of 0.98 on known attacks and 0.87 on a previously unseen UDPScan trace. In parallel, DE provided an effective quality–time trade-off for multi-stage strategy optimization and converged more reliably than alternative heuristics, enabling practical iterative penetration cycles in a dynamic and virtualized 5G environment. Finally, the end-to-end closed loop yielded measurable operational gains, reducing anomaly-detection latency by 41% and optimization-cycle time by 33%, while improving sensitivity to previously unseen threats by approximately 15%.

The current study is limited to a controlled 5G SA testbed and a scripted set of attack traces; results may vary under different traffic mixes, slice policies, and operator deployments. Future work will extend evaluation to larger and more heterogeneous environments and investigate adaptive decision-

making modules such as reinforcement learning for strategy selection, integration with digital twins for scalable what-if analysis, and incorporation of threat intelligence to prioritize evolving attack techniques. Overall, the proposed method provides a practical foundation for scalable, feedback-driven, and autonomous security assessment of cloud-native mobile networks.

Information on funding. This research was funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP26199941).

REFERENCES

1 3GPP. System Architecture for the 5G System (5GS). 3GPP TS 23.501, Release 19 (2025).

2 3GPP. Security Architecture and Procedures for 5G System. 3GPP TS 33.501, Release 19 (2025).

3 3GPP. Management and Orchestration: Concepts, Use Cases and Architecture. 3GPP TS 28.530, Release 19 (2025).

4 Singh, A., Juneja, D., Singh, J., and Aggarwal, S. Security Technologies for 6G Mobile Systems and Challenges Associated with AI Technologies. Lecture Notes in Electrical Engineering, 1444, 1–13 (2026). https://doi.org/10.1007/978-981-96-8283-6_1

5 Albrecht, M.R., and Jensen, R.B. The Vacuity of the Open Source Security Testing Methodology Manual. Lecture Notes in Computer Science, 12529, 114–147 (2020). https://doi.org/10.1007/978-3-030-64357-7_6

6 Lidanta, F.Z., Almaarif, A., and Budiyono, A. Vulnerability Analysis of Wireless LAN Networks Using Penetration Testing Execution Standard: A Case Study of Cafes in Palembang. Proceedings of the 2021 International Conference on ICT for Smart Society (ICISS), 1–5 (2021). https://doi.org/10.1109/ICISS53185.2021.9533216

7 Scarfone, K., Souppaya, M., Cody, A., and Orebaugh, A. Technical Guide to Information Security Testing and Assessment. NIST Special Publication 800-115 (2008). https://doi.org/10.6028/NIST.SP.800-115

8 OWASP Foundation. OWASP Web Security Testing Guide v4 (2021). https://owasp.org/www-project-web-security-testing-guide/v41/

9 Harvanek, M., Bolcek, J., Kufa, J., Polak, L., Simka, M., and Marsalek, R. Survey on 5G Physical Layer Security Threats and Countermeasures. Sensors, 24, 5523 (2024). https://doi.org/10.3390/s24175523

10 Imanbayev, A., Tynymbayev, S., Odarchenko, R., Gnatyuk, S., Berdibayev, R., Baikenov, A., and Kaniyeva, N. Research of Machine Learning Algorithms for the Development of Intrusion Detection Systems in 5G Mobile Networks and Beyond. Sensors, 22 (24), 9957 (2022). https://doi.org/10.3390/s22249957

11 Pinchuk, A., Odarchenko, R., Samoilenko, V., and Imanbayev, A. 5G Network Deployment Based on Open-source Projects: A Comparative Analysis. Proceedings of the IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), 596–601 (2023). https://doi.org/10.1109/IDAACS58523.2023.10348675

12 Storn, R., and Price, K. Differential Evolution – A Simple and Efficient Heuristic for Global Optimization over Continuous Spaces. Journal of Global Optimization, 11, 341–359 (1997). https://doi.org/10.1023/A:1008202821328

13 Almutairi, M.S. Deep Learning-Based Solutions for 5G Network and 5G-Enabled Internet of Vehicles: Advances, Meta-Data Analysis, and Future Direction. Mathematical Problems in Engineering, Article ID 6855435 (2022). https://doi.org/10.1155/2022/6855435

14 Dai, W., Zhou, J., Ye, C., and Xu, G. Automated Penetration Testing System Based on PTES and ATT&CK. Communications in Computer and Information Science, 2594, 433–444 (2026). https://doi.org/10.1007/978-981-95-1340-6_35

15 Odarchenko, R., Iavich, M., and Pinchuk, A. Development of a Method for Automated 5G and Beyond Network Slices Penetration Testing. Radioelectronic and Computer Systems, 1 (113), 248–263 (2025). https://doi.org/10.32620/reks.2025.1.17

16 Allaw, Z., Zein, O., and Ahmad, A.-M. Cross-Layer Security for 5G/6G Network Slices: An SDN, NFV, and AI-Based Hybrid Framework. Sensors, 25 (11), 3335 (2025). https://doi.org/10.3390/s25113335

17 Eltaeib, T., and Mahmood, A. Differential Evolution: A Survey and Analysis. Applied Sciences, 8 (10), 1945 (2018). https://doi.org/10.3390/app8101945

18 Noor, K., Imoize, A.L., Li, C.-T., and Weng, C.-Y. A Review of Machine Learning and Transfer Learning Strategies for Intrusion Detection Systems in 5G and Beyond. Mathematics, 13 (7), 1088 (2025). https://doi.org/10.3390/math13071088

***[1]Иманбаев А.Ж.,**
ассистент-профессор, ORCID ID: 0000-0003-3719-4091,
*e-mail: imanbaevazamat@gmail.com
[2]Бердібаев Р.Ш.,
профессор, ORCID ID: 0000-0002-8341-9645,
e-mail: r.berdybaev@aues.kz
[3]Одарченко Р.С.,
профессор, ORCID ID: 0000-0002-7130-1375,
e-mail: odarchenko.r.s@ukr.net
[4]Тынымбаев С.,
профессор, ORCID ID: 0000-0002-9326-9476,
e-mail: s.tynym@mail.ru

[1]Қазақстан-Британ техникалық университеті, Алматы қ., Қазақстан
[2]Алматы энергетика және байланыс университеті, Алматы қ., Қазақстан
[3]«Киев авиациялық институты» мемлекеттік университеті, Киев қ., Украина
[4]Халықаралық ақпараттық технологиялар университеті, Алматы қ., Қазақстан

5G ЖӘНЕ ОДАН КЕЙІНГІ ЖЕЛІЛЕРДЕ АВТОМАТТЫ ПЕНЕТРАЦИЯЛЫҚ ТЕСТІЛЕУГЕ АРНАЛҒАН ЗИЯТКЕРЛІК ГИБРИДТІ ӘДІС

Аңдатпа

5G технологияларының дамуы мен 6G желілерінің енгізілуі мобильді жүйелердің күрделілігін арттыруда. Бұл қызметке негізделген архитектура, желілік слайсинг, виртуализация және таратылған cloud-native функциялар арқылы жүзеге асады. Мұндай мүмкіндіктер желінің икемділігі мен масштабталуын қамтамасыз еткенімен, шабуыл жасалатын бетті кеңейтіп, жаңа осалдықтардың пайда болуына әкеледі. Дәстүрлі пентест әдістемелері мұндай динамикалық және виртуалданған ортаға бейімделмеген, өйткені олар статикалық процедураларға және қолмен тестілеуге сүйенеді. Сонымен қатар, машиналық оқытуды қолданатын шабуылдарды анықтау жүйелері (IDS) аномалиялар мен белгісіз қауіптерді тиімді анықтағанымен, penetration testing үдерістерінен бөлек жұмыс істейді. Бұл мақалада 5G және болашақ желілер үшін автоматтандырылған пентест жүргізуге арналған зияткерлік гибридті әдіс ұсынылады. Әдіс инкременттік оқыту, автоэнкодерлер және генеративті қарсылас желілер (GAN) негізіндегі шабуылдарды анықтау жүйесін дифференциалды эволюция (DE) алгоритмімен басқарылатын шабуылдарды оңтайландыру модулімен біріктіреді. Генетикалық алгоритмнің орнына DE жоғары жинақталу жылдамдығына, локалды минимумдарға төзімділігіне және шабуыл стратегияларының жоғары өлшемді сипаттамаларын оңтайландыруға қолайлылығына байланысты қолданылады. OpenAirInterface негізіндегі 5G Standalone тесттік ортасында жүргізілген тәжірибелер DE алгоритмінің осалдықтарды анықтау тиімділігін арттыратынын, көпқадамды шабуыл стратегияларын оңтайландыратынын және шынайы автоматтандырылған пентест сценарийлерін қамтамасыз ететінін көрсетті. Бұл нәтижелер DE-ге негізделген оңтайландыру келесі буын мобильді желілерінің қауіпсіздігін үздіксіз бағалауға арналған масштабталатын, бейімделгіш және тиімді негіз ұсынатынын көрсетеді.

Тірек сөздер: 5G қауіпсіздігі, шабуылдарды анықтау жүйесі, дифференциалды эволюция, автоматтандырылған пентест, шабуыл графы.

***[1]Иманбаев А.Ж.,**
ассистент-профессор, ORCID ID: 0000-0003-3719-4091,
*e-mail: imanbaevazamat@gmail.com
[2]Бердибаев Р.Ш.,
профессор, ORCID ID: 0000-0002-8341-9645,
e-mail: r.berdybaev@aues.kz
[3]Одарченко Р.С.,
профессор, ORCID ID: 0000-0002-7130-1375,
e-mail: odarchenko.r.s@ukr.net
[4]Тынымбаев С.,
профессор, ORCID ID: 0000-0002-9326-9476,
e-mail: s.tynym@mail.ru

[1]Казахстанско-Британский технический университет, г. Алматы, Казахстан
[2]Алматинский университет энергетики и связи, г. Алматы, Казахстан
[3]Государственный университет «Киевский авиационный институт», г. Киев, Украина
[4]Международный университет информационных технологий, г. Алматы, Казахстан

ИНТЕЛЛЕКТУАЛЬНЫЙ ГИБРИДНЫЙ МЕТОД ДЛЯ АВТОМАТИЗИРОВАННОГО ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ В СЕТЯХ 5G И ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

Аннотация

Развитие технологий 5G и предстоящее внедрение сетей 6G приводят к существенному усложнению архитектуры мобильных систем за счет сервисно ориентированной архитектуры, сетевого слайсинга, виртуализации и распределенных cloud-native функций. Эти изменения повышают масштабируемость и гибкость, но одновременно увеличивают атакуемую поверхность и формируют новые типы уязвимостей. Традиционные методы тестирования на проникновение не соответствуют таким динамичным и виртуализированным средам, поскольку полагаются на статические процедуры и ручные действия, не успевающие за изменениями сетевой инфраструктуры. В то же время системы обнаружения вторжений (IDS), основанные на машинном обучении, способны выявлять аномалии и неизвестные угрозы, но остаются отделенными от процессов тестирования на проникновение. В работе представлен интеллектуальный гибридный метод автоматизированного тестирования на проникновение в сетях 5G и будущих поколений. Подход объединяет IDS, основанную на инкрементальном обучении, автоэнкодерах и GAN-моделях, с модулем оптимизации атак на основе алгоритма дифференциальной эволюции (DE). Вместо генетического алгоритма используется DE благодаря высокой скорости сходимости, устойчивости к локальным минимумам и пригодности для оптимизации высокоразмерных представлений стратегий атак. Эксперименты на тестовой платформе 5G Standalone, реализованной с использованием OpenAirInterface, показали, что DE повышает эффективность идентификации уязвимостей и формирует оптимальные многоэтапные стратегии атак. Эти результаты показывают, что оптимизация на основе DE обеспечивает масштабируемую, адаптивную и эффективную основу для непрерывной оценки безопасности мобильных сетей следующего поколения.

Ключевые слова: безопасность 5G, система обнаружения вторжений, дифференциальная эволюция, автоматизированное тестирование на проникновение, граф атак.