AI & CYBER FORUM
AN INTERNATIONAL JOURNAL
OPEN ACCESS
ISSN 3117-6399
Review Article
Check for updates

Lightweight Identifier Mutation for Proactive Cyber Defense: An IP-Port Hopping Approach

Abdullahi Adam Galadima[1], Usman Idris Ismail*[2], Ezeh Ikechukwu Harrison[1], Ewunonu Toochi Chima[1], Muhammad Adam[3], and Mbamala Chinyere Vivian[4]

[1]*Department of Cyber Security Federal University of Technology Owerri, Nigeria*
[2]*Department of Computer Science, Federal University Kashere, Nigeria*
[3]*Department of Computer and Information Sciences, Towson University, MD 21252, USA, Towson*
[4]*Department of Information Technology Federal University of Technology Owerri, Nigeria*

Corresponding author: **Usman Idris Ismail** | E-mail: **usmanidrisismail@fukashere.edu.ng**

Citation: Abdullahi Adam Galadima, Usman Idris Ismail, Ezeh Ikechukwu Harrison, Ewunonu Toochi Chima, Muhammad Adam, and Mbamala Chinyere Vivian (2026). Lightweight Identifier Mutation for Proactive Cyber Defense: An IP-Port Hopping Approach. *AI & Cyber Forum: An International Journal.* **DOI: https://doi.org/10.51470/AI.2026.5.1.41**

Received 17 January 2026 | Revised 18 February 2026 | Accepted 14 March 2026 | Available Online April 25, 2026

Abstract

The static nature of conventional network configurations creates predictable attack surfaces that enable adversaries to perform efficient reconnaissance using automated scanning tools. This limitation is particularly critical at the early stage of cyber-attacks, where accurate network enumeration facilitates subsequent exploitation. To address this challenge, this paper proposes a lightweight Moving Target Defense (MTD) framework based on synchronized IP and port hopping to obscure network visibility and disrupt attacker reconnaissance activities. The proposed approach employs coordinated interface-level IP reconfiguration and Network Address Translation (NAT)-based port remapping to introduce continuous and unpredictable identifier mutation without relying on Software-Defined Networking (SDN) infrastructure or complex topology manipulation. The framework is implemented and evaluated in a controlled Mininet environment using an Nmap-driven attacker model. Experimental results show that the proposed system reduces reconnaissance success from 85% to 20%, significantly increases scan time, and generates high entropy in port distribution while maintaining service stability. These findings demonstrate that lightweight, host-level mutation strategies can effectively degrade attacker visibility and impose operational uncertainty. This work contributes a practical, low-overhead MTD solution suitable for deployment in resource-constrained environments, offering a viable alternative to more complex SDN-based defense mechanisms.

Keywords: *Moving Target Defense, IP Hopping, Port Hopping, Network Security, Reconnaissance Mitigation, Dynamic Reconfiguration.*

1.0 Introduction

The persistence of reconnaissance driven attacks continues to expose a fundamental weakness in static network configurations such as fixed IP addresses and unchanging service ports. Static network environments provide adversaries with predictable and easily discoverable attack surfaces, enabling reconnaissance tools most notably Nmap, to enumerate hosts, fingerprint services, and identify exploitable vulnerabilities with minimal effort [1]. As attackers continue to refine automated scanning and enumeration techniques, the window for defensive reaction narrows significantly, making proactive security paradigms increasingly critical [2].

Moving Target Defense (MTD) has emerged as one of the most promising proactive strategies for countering modern cyber threats [3]. By continuously altering network attributes such as IP addresses, port numbers, routing paths, and even network topology, MTD disrupts an attacker's ability to rely on static reconnaissance data. This enforced uncertainty increases the cost, complexity, and time required to mount a successful attack [4]. Across recent literature, MTD has been successfully applied in domains such as distributed denial-of-service (DDoS) mitigation, topology mutation, routing randomization, and identity obfuscation [5,3]. For instance, studies show that dynamic reconfiguration can significantly reduce attacker visibility, limit eavesdropping success rates, and improve service resilience under attack conditions. In Software-Defined Networking (SDN)-enabled environments, dynamic reconfiguration can be achieved with millisecond-level responsiveness, with mitigation occurring in as little as three seconds [6]. Similarly, routing dispersion and topology mutation strategies have demonstrated reductions of up to 63% in packet eavesdropping rates. Other approaches, such as fake IP hopping, effectively break spatial and temporal traffic correlations, thereby reducing the success of

sniffing and identity inference attacks [7].

Despite these advancements, the practical deployment of MTD in real-world environments remains challenging. Many existing approaches introduce significant computational overhead. Many existing approaches introduce significant computational overhead, require complex coordination mechanisms, or depend heavily on SDN infrastructure [8,9]. Additionally, a large portion of existing research focuses on isolated MTD techniques such as address mutation or DDoS mitigation without providing lightweight, integrated, and deployable solutions specifically designed to counter reconnaissance attacks in small- to medium-scale networks. This creates a critical gap between theoretical MTD capabilities and practical, scalable implementations that can be easily adopted in resource-constrained environments.

This study aims to design and evaluate a lightweight and scalable Moving Target Defense (MTD) framework that employs synchronized IP and port hopping to obscure network topology and disrupt attacker reconnaissance activities. Unlike existing approaches that rely on SDN infrastructure or complex coordination mechanisms, the proposed framework introduces a host-level, dual-layer mutation strategy that significantly reduces reconnaissance success rates, increases scanning uncertainty and delay, and maintains service stability under dynamic reconfiguration. The objective is to provide a practical, low-overhead, and deployable solution tailored for real-world and resource-constrained network environments. This work distinguishes itself from existing MTD approaches by introducing a lightweight, host-level mutation framework that eliminates reliance on SDN infrastructure while enabling synchronized IP–port hopping. This dual-layer mutation strategy enhances multi-dimensional unpredictability specifically at the reconnaissance stage, providing a practical and deployable alternative to existing complex MTD solutions.

This study adopts an experimental and system design approach grounded in established MTD principles. The proposed framework implements synchronized IP and port hopping through coordinated interface-level reconfiguration and Network Address Translation (NAT)-based port remapping. The system is developed and evaluated within a controlled Mininet simulation environment, where an attacker model based on Nmap-driven reconnaissance is used to assess effectiveness. Periodic and randomized hopping events are introduced to increase entropy and disrupt attacker visibility. Performance evaluation is conducted using key metrics such as reconnaissance success rate, scan time, detection delay, and port distribution entropy. This methodology aligns with experimental practices used in prior MTD, routing mutation, and address-hopping studies, ensuring comparability with existing research.

The contributions of this is as follows:

- Design of a synchronized dual-layer mutation mechanism that simultaneously performs IP and port hopping to disrupt spatial and temporal attack patterns.
- Optimization of mutation responsiveness and entropy generation with a significant reduction in reconnaissance success while maintaining minimal system overhead.
- Development of a lightweight and modular MTD architecture that operates at the host level and can be extended to SDN-integrated or adaptive defense environments.

The remainder of this paper is organized as follows: Section 2 presents a review of related work on Moving Target Defense techniques. Section 3 describes the proposed methodology and system architecture. Section 4 presents the experimental results and discusses the effectiveness of the proposed approach. Section 5 concludes the paper and outlines directions for future research.

2.0 Related Work

In practical Moving Target Defense (MTD) systems, various hopping techniques such as routing mutation, IP mutation, and topology mutation operate synergistically to disrupt attacker exploration and impede network mapping. Dynamic routing alters forwarding paths, IP mutation changes communication identifiers, and topology mutation restructures network connectivity. Combined these techniques significantly increase uncertainty for adversaries and provide a layered defense across diverse threat environments.

2.1 Routing Mutation

Routing mutation techniques generally operate at either the flow level or at the packet level. In flow-level mutation, packets belonging to the same flow follow a consistent sub-path, allowing attackers who intercept consecutive sub-flows to infer ordering or reconstruct sequences. To address this, [10] introduced a Randomized Routing Mutation (RRM) technique that computes effective path variations using satisfiability modulo theories. Other studies [11] incorporate spatial randomness to diversify routing paths, with [12] accounting for attacker background knowledge and [13] employing Jaccard distance and temporal constraints to optimize mutation diversity while limiting latency.

Packet-level mutation, by contrast, randomizes forwarding decisions for each packet, enhancing unpredictability. [14] proposed the P4-based Network Immune Scheme (P4NIS), which disperses encrypted packets across multiple routes. Similarly, [15] combines random neighbor selection with cryptographic primitives, while [16] applies a Deep Deterministic Policy Gradient (DDPG) to derive adaptive packet-level routing strategies on programmable switches.

Despite their effectiveness, many routing-mutation approaches rely on global topology knowledge or centralized control, which limits scalability. RL-based approaches introduce additional complexity and training overhead.

In contrast, the K-Randomized Routing Dispersion (KRRD) method integrates SDN-coordinated per-hop address rewriting with multi-objective optimization, offering explicit control over trade-offs such as delay, load balance, and dispersion while maintaining practical deployability in large-scale networks.

2.2 Topology Mutation

Topology mutation research has grown rapidly, focusing on obfuscation, decoy systems, and probe-packet deception. AntiTomo [17] disrupts topology inference by generating deceptive topologies. Similarly, Zhu et al. [18] introduced EigenObfu, which hides critical nodes while preserving global connectivity. Hou et al. [19] proposed ProTO, which delays probe packets to mislead adversaries into constructing inaccurate topologies. Other work integrates decoys with topology shuffling, using strategies such as genetic optimization and attack-path analysis to guide mutation in IoT networks.

A key challenge in overlay networks is the overlap between underlay and overlay paths. Studies [20, 21] highlight that naïve randomization can overload critical links and expose high-traffic nodes to targeted attacks. Effective topology mutation must therefore consider link independence, path diversity, and traffic balance, ensuring that mutation reduces attacker visibility without destabilizing network operations.

2.3 Address Mutation

Address mutation is another widely explored MTD strategy. Sharma et al. [22] proposed joint IP and port randomization using endpoint agents that rewrite packet headers dynamically. Azab et al. [23] presented an Intelligence-Driven Host Address Mutation (ID-HAM) model using a Markov decision process to ensure seamless address transitions. Mayone et al. [24] developed Randomized Host and Service Shuffling for IPv6 (RHSS6), leveraging the large IPv6 address space to reduce scanning effectiveness, albeit with measurable performance overhead.

At the network layer, Chavez et al. [25] implemented IP randomization by validating source–destination pairs and dynamically installing encoding/decoding rules, reducing host-side complexity. Mani et al. [26] explored machine-learning approaches to detect MTD deployments and predict future address assignments, highlighting potential adversarial learning risks.

Despite progress, many address-mutation mechanisms face limitations such as restricted address space, scanning predictability, or session disruption. Recent work proposes per-hop address rewriting in ICN/SDN environments, guided by standards such as ITU-T Y.3083 [27, 28] and SEANet's instant re-addressing technology [29, 30]. By operating on identifiers rather than IP addresses, these techniques overcome space limitations and significantly hinder reconnaissance, offering a stronger foundation for dynamic, scalable MTD.

Table 1: Summary of Related Work on Moving Target Defense Techniques

Study	MTD Technique	Key Mechanism	Strengths	Limitations
Ribeiro et al. (target1)	SDN-based Dynamic Reconfiguration	Machine-learning-driven traffic classification combined with proactive and reactive flow redirection	Rapid mitigation (~3s), high detection accuracy, centralized control	Requires SDN infrastructure; higher computational and deployment complexity
Du et al. (target2)	Routing Dispersion & Topology Mutation (KRRD)	Multi-objective optimization, per-hop address rewriting, randomized routing across overlay paths	Reduces eavesdropping by up to 63%, increases path diversity, explicit control over performance trade-offs	Requires global topology knowledge; optimization overhead; primarily designed for overlay networks
Qu et al. (target3)	Fake IP Hopping	Dynamic mapping and rewriting of IP identifiers using SDN control plane	Breaks spatial–temporal traffic correlations, hinders reconnaissance, maintains reasonable overhead	Depends on SDN controller integration; focus on communication networks; limited mutation scope

Table 1 provides a concise comparison of three representative MTD studies, outlining their core techniques, underlying mechanisms, strengths, and limitations. It highlights how different mutation strategies dynamic reconfiguration, routing dispersion, and fake IP hopping offer varying levels of unpredictability and deployment complexity.

3.0 Methodology

The methodology adopted in this study encompasses the design of the Moving Target Defense (MTD) framework, the development of synchronized IP and port hopping mechanisms, and the construction of a simulation environment for performance evaluation. This approach follows the methodological rigor demonstrated in recent SDN-based MTD systems, topology mutation frameworks, and fake IP hopping strategies discussed in prior research. The goal of the methodology is to provide a lightweight yet effective defensive mechanism capable of disrupting reconnaissance attempts while maintaining network stability.

3.1 Threat Model and Assumptions

This study focuses on an external attacker whose main goal is to gather information about the network before launching an attack. The attacker operates remotely, has no login credentials or insider access, and relies on common scanning tools such as Nmap to discover active hosts, open ports, and running services.

The attacker is assumed to understand standard networking protocols and scanning techniques, but has no prior knowledge of the IP addresses or service ports generated by the Moving Target Defense (MTD) system. Although repeated scans may be performed to observe patterns over time, the attacker cannot access or interfere with the MTD controller, internal mapping tables, or mutation logic.

The scope of this work is limited to reconnaissance activity, which represents an early and critical stage of most cyber-attacks. More advanced threats such as insider abuse, denial-of-service attacks, traffic analysis across multiple monitoring points, or attempts to predict mutation behavior using machine learning are not considered.

Legitimate users are assumed to be trusted and able to tolerate brief changes in network identifiers during hopping events. The experimental environment is kept lightly loaded to ensure that observed effects are due to the mutation mechanism rather than network congestion.

Under these assumptions, the proposed IP and port hopping approach is designed to prevent attackers from maintaining an accurate and stable view of the network, thereby reducing the effectiveness of reconnaissance attempts.

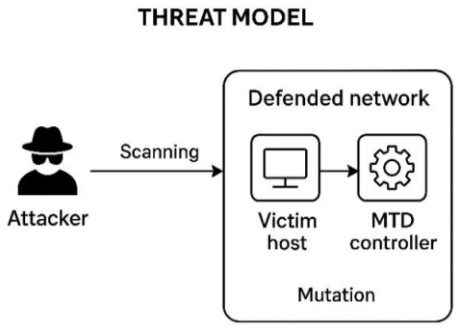

Figure 1: Threat Model of the Proposed IP-Port Hopping MTD Framework

Figure 1 illustrates the attacker model and operational assumptions guiding the proposed MTD design. It shows how an external adversary performs reconnaissance while the system defends through unpredictable identifier mutation.

The proposed architecture consists of three functional layers that work together to introduce continuous and unpredictable reconfiguration. At the control layer, a hopping scheduler and entropy generator coordinate the timing and randomness of IP and port mutations. The scheduler governs the hopping intervals, while the entropy generator produces new address and port values with sufficient randomness to minimize predictability. This design reflects the control data plane separation model used in SDN-enabled MTD approaches and ensures that the mutation process can be executed consistently without interfering with service operations as shown in Figure 2 below. Supporting this, a synchronization unit ensures that ongoing communication sessions are minimally affected during transitions.

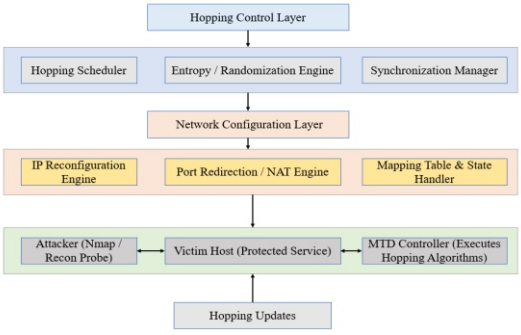

Figure 2: Conceptual Architecture of the Proposed MTD Framework

Figure 2 outlines the three-layer architecture control, configuration, and execution that enables synchronized IP and port hopping.

It visualizes how scheduling, entropy generation, and interface-level rewriting work together to produce continuous mutation.

The network configuration layer operationalizes the decisions made by the control layer. When a new hopping event is triggered, the host's IP address is updated through interface-level rewriting, and the service port is reassigned through NAT-based redirection. Both operations are conducted in a manner that preserves short-term compatibility between old and new mappings, allowing for smooth transitions. This dual mapping approach is similar to the techniques observed in fake IP hopping architectures, where source destination address fields are dynamically reassigned without interrupting communication. By coordinating IP and port mutation simultaneously, the system enhances obfuscation and introduces multi-dimensional unpredictability.

The execution layer consists of the nodes participating in the experiment: the victim node hosting the service, the attacker node conducting scanning attempts, and the MTD controller executing the hopping algorithms. While the framework does not rely on a centralized SDN controller, it remains modular and could be extended to an SDN-based deployment in future work, similar to earlier mitigation systems that utilize flow-table reconfiguration as part of their defensive strategies.

The hopping process follows a continuous loop in which random values are generated, validated, and deployed to the network configuration layer. At the start of each cycle, the controller generates a new IP address and port number, ensuring they fall within the valid operational ranges. These parameters are temporarily inserted into a local mapping table to coordinate the transition. The host interface is then updated to the new IP address, and NAT policies are refreshed to map incoming traffic to the new service port. Upon successfully applying these changes, the system discards previous mappings and enters a stabilization period before initiating the next cycle. The continuous nature of this loop parallels the design seen in dynamic address-mutation systems for power communication networks, where frequent and unpredictable updates reduce the attacker's ability to track active hosts as shown in Figure 3 below.

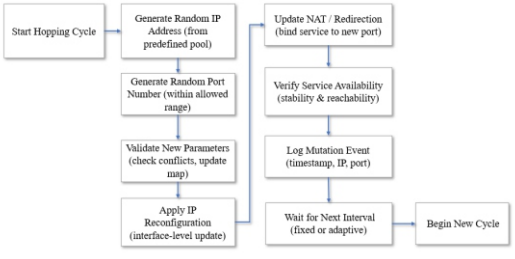

Figure 3: Workflow of the IP and Port Hopping Mechanism

Figure 3 depicts the sequential steps of the hopping process, from generating new identifiers to applying them and stabilizing active sessions. It highlights the continuous-loop nature of the mutation cycle.

To evaluate the effectiveness of the proposed MTD framework, a controlled testbed was developed in Mininet.

The environment included an MTD controller node, a victim node, and an attacker node performing reconnaissance. The selection of a simplified three-node topology mirrors previous studies that isolate mutation effects without the influence of complex routing behavior. The MTD controller executed the hopping algorithm, while the attacker node continuously probed the network using Nmap to assess how rapidly changing network identifiers influence reconnaissance success.

The configuration parameters included a private IP pool, a wide port selection range to maximize entropy, and a set of hopping intervals designed to evaluate responsiveness and attack disruption under different timing conditions. Wireshark was used to verify hopping behavior and to analyze packet traces during mutation events. The attacker model remained consistent with reconnaissance focused threat models used in earlier MTD studies, relying on repeated scanning to identify services exposed by the victim host.

Table 2: System Parameters and Simulation Settings

Parameter Category	Configuration Details
Network Environment	Mininet virtual network; three-node topology (MTD Controller, Victim Host, Attacker Host); virtual switch interconnection
Operating System	Ubuntu-based Mininet environment; Linux kernel networking stack
MTD Mechanism	Synchronized IP and port hopping at host level
IP Address Pool	Private addressing range (10.0.x.y) allocated for mutation cycles
Port Range	1024–65535 (ephemeral and registered ports)
Hopping Intervals Evaluated	5s, 10s, 20s, 30s (fixed-interval approach)
Reconfiguration Method	Interface-level IP rewriting; NAT/port redirection to bind new service port
Attacker Model	Reconnaissance adversary using Nmap for host discovery, SYN probing, and service enumeration
Monitoring Tools	Wireshark for packet inspection; system logs for mutation event tracking
Traffic Pattern	Light traffic environment to isolate mutation impact; single protected service exposed on the victim host
Number of Experiment Runs	100 hopping cycles recorded per interval configuration

Table 2 summarizes the experimental setup used to evaluate the proposed IP–port hopping framework. It lists key configuration details, including the network environment, mutation parameters, attacker model, monitoring tools, and number of experimental runs, establishing the basis for reproducibility.

Performance was assessed using four key metrics. Reconnaissance success rate measured the percentage of successful host or port identifications under both static and MTD-active conditions, providing a direct indicator of the framework's defensive effectiveness. Scan time analysis captured the additional time required for attackers to complete network enumeration when faced with continuous reconfiguration, reflecting the increased workload. Detection delay quantified the system's responsiveness by measuring the time between an attacker's scan attempt and the execution of a new hopping event. Finally, port distribution entropy captured the randomness of generated port values across mutation cycles, offering insight into the unpredictability of the service exposure pattern. These metrics are consistent with those used in prior SDN-based MTD experiments, topology mutation evaluations, and IP hopping studies, ensuring comparability with existing research. Through this methodological approach, the proposed framework provides a structured, reproducible, and defensively robust environment for studying the effects of synchronized IP and port mutation on attacker reconnaissance capabilities, as shown in figure 3 below.

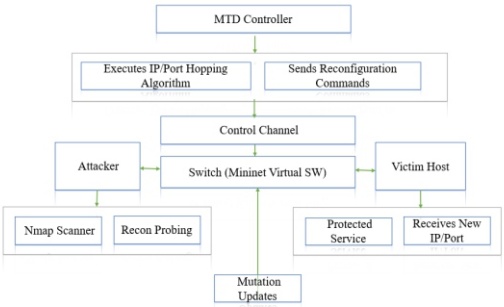

Figure 4: Experimental Network Topology

Figure 4 shows the simplified three-node Mininet topology used in the experiment, consisting of the MTD controller, victim host, and attacker machine connected through a virtual switch.

4.0 Results and Discussion

This section presents the experimental results obtained from evaluating the proposed Moving Target Defense (MTD) framework and discusses their implications in relation to existing findings in the literature. The evaluation focused on understanding how synchronized IP and port hopping influences reconnaissance success, scan time, detection delay, and port distribution entropy. The experiments were performed in a controlled network environment to isolate the effects of dynamic mutation and compare the behavior of a static configuration against an MTD-protected system.

A significant reduction in reconnaissance success was observed when the hopping mechanism was activated. In the static configuration, the attacker was able to consistently identify the victim host and detect its open services, resulting in an 85% success rate during repeated scanning cycles. When the MTD mechanism was applied, this rate fell dramatically to 20%, demonstrating that the frequent reconfiguration of network identifiers effectively disrupts the attacker's ability to correlate observed responses or maintain a persistent view of the system. This result aligns with trends reported in earlier MTD studies, where address mutation and randomized forwarding patterns reduced attacker visibility and impeded sustained reconnaissance attempts. The improvement observed in this work reinforces the idea that even lightweight host-level mutation strategies can impose substantial uncertainty on adversaries, similar to the gains seen in more complex SDN-driven architectures, as shown in figure below.

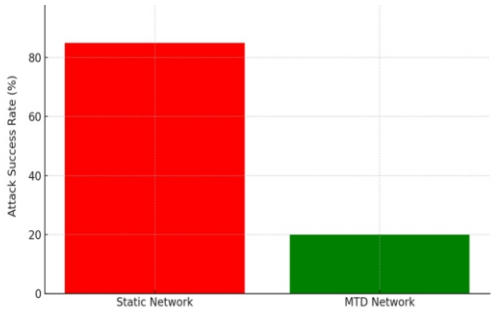

Figure 5: Attack Success Rate Comparison

Figure 5 compares the attacker's reconnaissance success under static and MTD-protected conditions, demonstrating the significant reduction achieved through continuous identifier mutation.

In addition to lowering the attack success rate, the MTD framework substantially increased the scan time required by the attacker. Under static conditions, exploration scans is completed within predictable time intervals, enabling attackers to rapidly enumerate the target's attributes. With MTD enabled, however, scan operations became less reliable and required significantly longer to complete. This increased delay is attributed to the continuous mutation of both IP addresses and service ports, which causes incomplete and outdated scan results before the attacker can finish a full enumeration cycle. These observations reflect similar findings in routing and topology mutation research, where adversaries experienced substantial delays due to frequent changes in path structure and node identifiers, as shown in Figure 5 below. The longer scan time thus indicates that the proposed framework imposes a meaningful operational burden on attackers, reducing the feasibility of rapid exploitation.

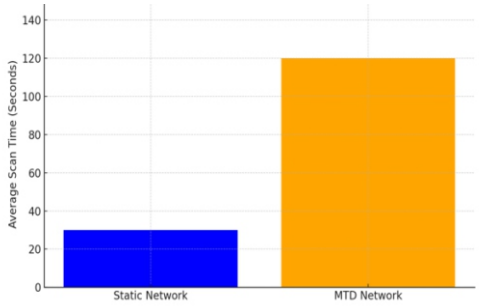

Figure 6: Scan Time Comparison chart

Figure 6 illustrates how the MTD mechanism increases the time required for the attacker to complete reconnaissance, emphasizing the additional workload imposed by dynamic reconfiguration.

The relationship between hopping interval and detection delay was also examined to understand how quickly the system responds to adversarial activity. The results showed that shorter hopping intervals produced lower detection delays, with the system reacting within approximately one second of a scan attempt during the most aggressive configurations. As intervals increased, the detection delay grew correspondingly, creating slightly wider exposure windows for an adversary.

This performance pattern is comparable to behavior reported in dynamic address-mutation systems, where higher mutation frequency enhances resilience but may introduce additional overhead. In this study, shorter intervals consistently yielded superior defensive responsiveness without causing service instability, indicating that the chosen hopping strategy maintains an acceptable balance between performance cost and security benefit. Figure 7 below shows how these processes happened in a line chart.

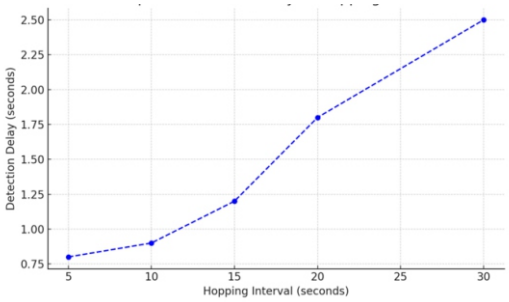

Figure 7: Detection Delay vs Hopping Interval line graph

Figure 7 visualizes the relationship between hopping interval and defensive responsiveness, showing that shorter intervals yield faster reaction times to scanning activity.

The distribution of port values generated during the experiment further demonstrates the randomness and unpredictability of the hopping mechanism. Across 100 mutation cycles, the system produced a nearly uniform distribution of port assignments spanning the available range. No clustering patterns are repeated and sequences were observed, suggesting that the port-hopping algorithm introduces sufficient entropy to prevent adversaries from predicting upcoming service exposure points. This characteristic mirrors the behavior of entropy-driven mutation schemes in packet level mutation frameworks and topology obfuscation systems where randomness plays a critical role in minimizing the reliability of attacker inference. Figure 8 shows this distribution foe frequency against port distribution on the entropy chart.

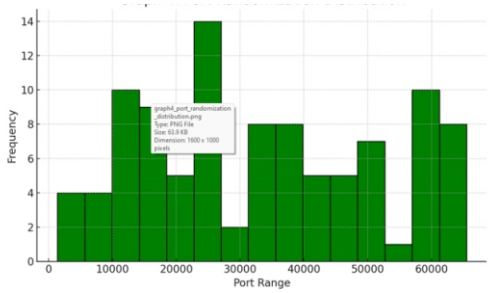

Figure 8: Port Distribution Entropy chart

Figure 8 demonstrates the randomness of port allocation across mutation cycles, reflecting the high entropy and unpredictability of the proposed port-hopping strategy.

Taken together, these results confirm the effectiveness of synchronized IP and port mutation as a practical MTD approach.

The substantial reduction in attacker success rate, the increased scan time, the rapid responsiveness at shorter intervals, and the high entropy of port distribution all point to a significant enhancement in defensive capability. Importantly, these benefits were achieved using a mechanism that operate at the host layer without requiring complex SDN-based control channels. This distinguishes the proposed method from broader mutation frameworks, such as those involving rerouting or topology reshaping, while still achieving comparable security gains in resisting reconnaissance.

The findings demonstrate that even minimalistic MTD mechanisms can meaningfully degrade the attacker's ability to maintain an accurate or timely understanding of network conditions. As in the studies on dynamic topology mutation and large-scale address hopping, the underlying principle remains consistent: frequent, unpredictable changes invalidate the attacker's assumptions and reduce the likelihood of successful exploitation. The results support the potential of lightweight, deployable MTD techniques to enhance security in environments where the complexity of full SDN deployment or sophisticated path-randomization strategies may be impractical.

Table 3: Summary of Experimental Results

Performance Metric	Static Configuration	MTD-Enabled Configuration	Observation
Reconnaissance Success Rate	85%	20%	Significant reduction in attacker success due to continuous IP–port mutation
Average Scan Time	Low and stable	Increased duration with repeated incomplete scans	MTD disrupts adversary enumeration and increases workload
Detection Delay	Not applicable	Short delay at aggressive intervals (≈1s), increases with larger intervals	Faster hopping intervals provide quicker defensive response
Port Distribution Entropy	Low (fixed port)	High entropy across 100 mutation cycles	Demonstrates strong randomness and unpredictability in port selection
Service Stability	Stable	Stable across intervals	Reconfiguration does not disrupt legitimate access

Table 3 presents the performance comparison between the static baseline and the MTD-enabled configuration across key metrics. It highlights the reduction in reconnaissance success, increased scan time, improved responsiveness, and high port entropy achieved by the proposed framework.

4.1 Comparison Between the Proposed MTD Framework and Existing Techniques

To contextualize the effectiveness of the proposed IP-Port Hopping MTD framework, it is essential to compare its characteristics with representative techniques reported in current literature. Existing MTD approaches generally focus on SDN-driven flow reconfiguration, topology and routing mutation, or network-layer address hopping. Each of these methods introduces varying degrees of unpredictability to hinder attacker inference, but they also differ in deployment complexity, scalability, and operational overhead.

SDN-based solutions, such as those integrating machine-learning-driven flow classification and dynamic redirection, achieve rapid attack mitigation and centralized control but require dedicated controller infrastructure and incur higher configuration costs. Topology and routing mutation strategies, such as multi-objective optimized randomized routing, provide strong resilience against eavesdropping and path inference but rely on global network knowledge and significant computational resources. Network-layer fake-IP hopping approaches emphasize identifier obfuscation to disrupt spatial and temporal flow correlation, yet they depend heavily on SDN support and are designed for specific environments such as power communication networks.

In contrast, the proposed framework adopts a lightweight, host-level mutation mechanism that does not rely on SDN orchestration or large-scale topology manipulation. By synchronizing IP and port changes, the system effectively reduces reconnaissance success while maintaining ease of deployment and minimal overhead. This positions the proposed solution as a practical alternative for environments where complex MTD infrastructures are infeasible, yet proactive defense is still required

Table 4: Comparison Between the Proposed MTD Framework and Existing Techniques

Study Technique	Mutation Focus	Mechanism	Strengths	Limitations	Relation to This Work
Ribeiro et al. (target1)	Flow and service redirection	SDN-based dynamic reconfiguration with ML-driven attack diagnosis	Fast reaction time (~3s), centralized control, effective DDoS mitigation	Requires SDN controller; higher deployment overhead	Demonstrates effectiveness of dynamic reconfiguration; inspires modular MTD control concept
Du et al. (target2)	Routing and topology mutation	KRRD: randomized routing, topology mutation, per-hop address rewriting via multi-objective optimization	High path diversity, strong eavesdropping resistance, interpretable trade-offs	Computational complexity; requires global network view	Reinforces value of continuous mutation; motivates lightweight alternative without topology changes
Qu et al. (target3)	Network-layer address mutation	Fake-IP hopping via SDN controller; dynamic identifier mapping	Breaks spatial/temporal traffic correlations; mitigates reconnaissance	SDN dependence; focus on power communication networks	Provides conceptual foundation for IP-level mutation used in this work
This Work (Proposed MTD)	IP and Port mutation	Synchronized host-level IP and port hopping	Lightweight, deployable, reduces reconnaissance success (85%→20%), low overhead	Fixed intervals; no network-wide coordination	Extends mutation to port layer; offers simpler alternative to SDN-heavy approaches

Table 4 offers a structured comparison between the proposed IP–port hopping approach and notable MTD techniques in the literature. It contrasts mechanisms, strengths, and limitations, showing how the proposed framework provides a lightweight alternative to more complex SDN- or topology-based solutions.

5.0 Conclusion and Future Work

This work introduced a lightweight Moving Target Defense framework based on synchronized IP and port hopping to counter reconnaissance-driven attacks. The experimental results demonstrate that continuous reconfiguration of network identifiers substantially reduces adversarial visibility, lowering reconnaissance success from 85% in static settings to 20% under MTD protection. The increase in scan time and the high entropy observed in port allocation further validate the framework's ability to impose uncertainty while maintaining stable service operation. These findings align with emerging evidence from contemporary MTD research, reinforcing the value of dynamic, low-overhead mutation strategies in strengthening network resilience.

Despite its effectiveness, the current design employs fixed mutation intervals and operates solely at the host level. Future research may extend this work by incorporating adaptive hopping mechanisms triggered by real-time threat indicators or anomaly detection models. Integrating the framework with SDN controllers could also enable coordinated, network-wide mutation strategies, offering broader defensive coverage. Moreover, evaluating the system in larger and more heterogeneous environments would help ascertain scalability, operational robustness, and long-term performance. Expanding mutation to additional network attributes such as MAC addresses, flow identifiers, or routing metadata presents another promising direction for enhancing unpredictability against increasingly sophisticated reconnaissance techniques. The results illustrate that synchronized IP and port hopping offers a practical and effective approach for degrading attacker reconnaissance capabilities, contributing meaningful insight into the development of deployable and adaptive MTD solutions.

CRediT authorship contribution statement

Abdullahi Adam Galadima: Conceptualization, Methodology, Formal analysis, Visualization, Writing – original draft, Writing – review & editing. Usman Idris Ismail: Conceptualization, Methodology, Writing – review & editing. Ezeh Ikechukwu Harrison: Methodology, Supervision, Writing – review & editing. Ewunonu Toochi Chima: Writing – review & editing. Muhammad Adam: Supervision, Writing – review & editing. Mbamala Chinyere Vivian: Data curation, Formal analysis, Validation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

There is no data available for the research.

Declaration of generative AI use

During the preparation of this manuscript, the authors used ChatGPT (OpenAI) to improve readability and language. After using this tool/service, the authors reviewed and edited the content as needed and take full responsibility for the content of the published article.

References

1. Everson, D., & Cheng, L. (2024). A survey on network attack surface mapping. Digital Threats Research and Practice, 5(2), 1–25. https://doi.org/10.1145/3640019
2. Aladiyan, A. (2025). Digital Safeguards: unravelling the complex interplay between emerging threats and proactive cyber defence strategies. Journal of Internet Services and Information Security, 15(1), 348–360. https://doi.org/10.58346/jisis.2025.i1.022
3. Nguyen, M., & Debroy, S. (2022). Moving target Defense-Based Denial-of-Service mitigation in cloud environments: a survey. Security and Communication Networks, 2022, 1–24. https://doi.org/10.1155/2022/2223050
4. Sun, R., Zhu, Y., Fei, J., & Chen, X. (2023). A survey on Moving Target Defense: Intelligently Affordable, Optimized and Self-Adaptive. Applied Sciences, 13(9), 5367. https://doi.org/10.3390/app13095367
5. Abdi, A. H., Audah, L., Salh, A., Alhartomi, M. A., Rasheed, H., Ahmed, S., & Tahir, A. (2024). Security Control and Data Planes of SDN: A Comprehensive review of traditional, AI, and MTD approaches to security solutions. IEEE Access, 12, 69941–69980. https://doi.org/10.1109/access.2024.3393548
6. Park, J., Mohaisen, M., Nyang, D., & Mohaisen, A. (2020). Assessing the effectiveness of pulsing denial of service attacks under realistic network synchronization assumptions. Computer Networks, 173, 107146. https://doi.org/10.1016/j.comnet.2020.107146
7. Gu, X., Wang, Q., Yan, Q., Liu, J., & Pu, C. (2024). Sync-Millibottleneck attack on microservices cloud architecture. ASIA CCS '24: Proceedings of the 19th ACM Asia Conference on Computer and Communications Security, 799–813. https://doi.org/10.1145/3634737.3644991
8. Liu, J., Fan, W., Lim, E., Dai, Y., & Lisitsa, A. (2025). ML-BF: Responsive and Dynamic Intrusion Detection towards Intelligent Connected Vehicles. Peer-to-Peer Networking and Applications, 19(1). https://doi.org/10.1007/s12083-025-02113-6
9. Liu, S., Xi, L., & Chen, H. (2025). Enhancing security in smart distribution networks: proximal policy cooperative optimization against false data injection attacks. IEEE Transactions on Industry Applications, 1–14. https://doi.org/10.1109/tia.2025.3618822
10. Zhang, B., Han, L., & Sun, S. (2021b). Dynamic Random Route Mutation Mechanism for Moving Target Defense in SDN. 6th International Symposium on Computer and Information Processing Technology (ISCIPT), 536–541. https://doi.org/10.1109/iscipt53667.2021.00114
11. Zhou, Z., Yuan, Y., Yang, X., Gan, L., Du, Y., Yu, R., Wang, L., Qu, J., Zheng, X., & Cui, Z. (2018). Speech detection enhancement in optical fiber acoustic sensor via adaptive threshold function. Optical Fiber Technology, 47, 1–6. https://doi.org/10.1016/j.yofte.2018.11.013

12. Liu, M., Quan, W., Liu, Z., Zhang, Y., Gao, D., & Zhang, H. (2022). Combating Eavesdropping with Resilient Multipath Transmission for Space/aerial-assisted IoT. ICC 2022 - IEEE International Conference on Communications, 2230–2235. https://doi.org/10.1109/icc45855.2022.9839147
13. Duan, N. Q., Al-Shaer, E., & Jafarian, H. (2013). Efficient Random Route Mutation considering flow and network constraints. 2013 IEEE Conference on Communications and Network Security, CNS 2013, 260–268.
14. Beltrán, E. T. M., Sánchez, P. M. S., Bernal, S. L., Bovet, G., Pérez, M. G., Pérez, G. M., & Celdrán, A. H. (2024). Mitigating communications threats in decentralized federated learning through moving target defense. Wireless Networks, 30(9), 7407–7421.
15. Xu, X., Hu, H., Liu, Y., Tan, J., Zhang, H., & Song, H. (2022). Moving target defense of routing randomization with deep reinforcement learning against eavesdropping attack. Digital Communications and Networks, 8(3), 373–387.
16. Liu, G., Quan, W., Cheng, N., Lu, N., Zhang, H., & Shen, X. (2020). P4NIS: Improving network immunity against eavesdropping with programmable data planes. IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS).
17. Liu, Y., Xing, C., Zhang, G., Song, L., & Lin, H. (2021). AntiTomo: Network topology obfuscation against adversarial tomography-based topology inference. Computers & Security, 113, 102570.
18. Zhu, Z., Zhu, G., Zhang, Y., Shi, J., Huang, X., & Fang, Y. (2024). EigenOBFU: A Novel Network Topology Obfuscation Defense Method. IEEE Transactions on Network Science and Engineering, 12(1), 451–462.
19. Hou, T., Qu, Z., Wang, T., Lu, Z., & Liu, Y. (2020). ProTO: Proactive Topology Obfuscation Against Adversarial Network Topology Inference. EEE INFOCOM 2020 - IEEE Conference on Computer Communications, 1598–1607.
20. Vaisman, R., & Sun, Y. (2021). Reliability and importance measure analysis of networks with shared risk link groups. Reliability Engineering & System Safety, 211, 107578.
21. Guan, Y., Lei, W., Zhang, W., Liu, S., & Li, H. (2018). Scalable orchestration of software defined service overlay network for multipath transmission. Computer Networks, 137, 132–146.
22. Jones, N. M., Paschos, G. S., Shrader, B., & Modiano, E. (2017). An overlay architecture for throughput optimal multipath routing. IEEE/ACM Transactions on Networking, 25(5), 2615–2628.
23. Ribeiro, D. P., Cho, J., Moore, T. J., Nelson, F. F., Lim, H., & Kim, D. S. (2019). Random Host and Service Multiplexing for Moving Target Defense in Software-Defined Networks. ICC 2019 - 2019 IEEE International Conference on Communications (ICC), 51, 1–6.
24. Azab, M., Samir, M., & Samir, E. (2022). "MystifY": A proactive Moving-Target Defense for a resilient SDN controller in Software Defined CPS. Computer Communications, 189, 205–220.
25. Mayone, N., Kunz, P., Yigit, B., Soussi, W., Stiller, B., & Gür, G. (2024). IPv6 Connection Shuffling for Moving Target Defense (MTD) in SDN. 2024 IEEE International Conference on Cyber Security and Resilience (CSR), 373–378.
26. Chavez, A. R., Stout, W. M., & Peisert, S. (2015). Techniques for the dynamic randomization of network attributes. International Carnahan Conference on Security Technology (ICCST), 1–6.
27. Mani, G., Haliem, M., Bhargava, B., Manickam, I., Kochpatcharin, K., Kim, M., Vugrin, E., Wang, W., Jenkins, C., Angin, P., & Yu, M. (2023). Machine learning based resilience testing of an address randomization cyber defense. IEEE Transactions on Dependable and Secure Computing, 20(6), 4853–4867.
28. I. T. U. T., Information-centric networking in networks beyond IMT-2020: reference model of on-site, elastic, and autonomous network, Recommendation Y.3083, ITUT, 2023.
29. Wang, J., Bai, S., Wang, Y., Luo, G., & Wang, T. (2019). Preparation of large In(OH)3 and In2O3 particles through a seed-mediated growth method in a microreactor. Particuology, 49, 1–8.
30. Usman, M., Garba, E. J., & Ismai'il, U. I. (2024). Neuro-Fuzzy Models for Electronic Banking Fraud Detection and Prevention: A Review of Recent advances. International Journal of Research and Innovation in Applied Science, IX(VII), 406–414.
31. Ismail, U. I., Jauro, S. S., Muhammad, N. A., Jijji, S. A., Shawulu, J. C., & Galadima, A. A. (2026, March 10). Machine Learning for Hate Text Speech Detection: A Comprehensive review of techniques, dataset and challenges.