Journal of Network Computing and Applications (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/jnca.2025.100112
ISSN 2371-9214 Vol. 10 Num. 1

Cyberspace Anti-Mapping: An Intelligent Defense Framework Integrating Network Deception Technologies

Dexin Li, Han Li*, Liang Guo

360 Digital Security Technology Group Co., Ltd., Beijing, 100020, China

Keywords: Cyberspace Assets; Anti-Mapping; Intelligent Defense; Evidence Perturbation Network Deception; Topology Hiding

Abstract: Within the analytical framework of continuous advancement and evolution of cyberspace mapping technologies, traditional network security defense mechanisms have encountered unprecedented challenges. This paper conducts an in-depth exploration of cyberspace anti-mapping strategies with substantial theoretical significance. Particularly, it presents an intelligent defense framework developed from our research, which is established on the semantic abstraction of attack-defense elements and threat representation, integrated with network deception-based technical implementations. Empirical evidence demonstrates that the adoption of such semantic abstraction facilitates the construction of an effective model for feasibility characterization and constraint optimization of anti-mapping targets. The integration of evidence perturbation, adaptive strategy domain orchestration, and concrete technical modules (e.g., source address spoofing, host fingerprint obfuscation) provides practical defense mechanisms. These mechanisms address the complex and diverse mapping attack scenarios while ensuring asset concealment and system availability.

1. Introduction

With the accelerated informatization process, the attack surface of cyberspace assets has expanded progressively with growing complexity. (Guo Li, 2018)Mapping technologies have become a pivotal means for attackers to acquire information and analyze system vulnerabilitie. (Xue X, 2025)Data infrastructure, serving as the foundational pillar for the construction and operation of data space, is the cornerstone of high-quality development in the digital economy. Traditional defense mechanisms (e.g., firewalls, basic encryption protocols) exhibit limited efficacy in mitigating this multifaceted challenge, especially in environments involving large-scale automated detection and fingerprint fusion, where asset identifiability and mergeability have emerged as prominent concerns. This paper proposes intelligent defense countermeasures that integrate theoretical frameworks with concrete technical implementations. By conducting in-depth analysis of attack-defense elements and supplementing with proposed topology obfuscation, source address spoofing, and host fingerprint confusion techniques, this research provides a novel theoretical framework and technical pathway for anti-mapping efforts, thereby promoting the effective enhancement of defense systems.

2. Theoretical Foundation and Formal Framework for Anti-Mapping

2.1 Semantic Abstraction of Attack-Defense Elements and Threat Representation

Cyberspace mapping demonstrates distinct global and systemic attributes across dimensions including asset identification, structural analysis, and fingerprint fusion processes. The mapping process involves a complex high-dimensional mapping relationship between observed signals and feature patterns. Under passive or active detection scenarios, assets, protocols, services, and topologies generate semantic traces that constitute the evidence domain for mapping activities—enabling attackers to reconstruct the system's external structure within a multi-dimensional feature space (context-dependent capability). Anti-mapping research necessitates formal abstraction of attack-defense elements at the semantic level, integrating detection intentions, observation channels, and fusion logic into a unified representation framework. This abstraction facilitates the definition of threat establishment conditions and boundaries, while the semantic modeling approach focuses on the theoretical characterization of detectability and feature stability (rather than concentrating on specific implementation details), providing a logical and computational reasoning foundation for intelligent defense mechanisms. Consequently, threat perception and defense strategies can be constrained and aligned within a unified semantic space.

It is worth noting that the semantic abstraction of attack-defense elements is distinctly manifested in the differentiation between traditional IT security technologies and network deception technologies. Traditional IT security technologies adhere to the "CIAA" (Confidentiality, Integrity, Authentication, Availability) framework, prioritizing data confidentiality, integrity maintenance, identity verification, and service availability. (Harshitha DH, 2025)In contrast, network deception technologies—designed to mislead attackers, disrupt mapping behaviors, and capture attack actions—adopt the "CACA" (Confidentiality, Authentication, Controllability, Availability) framework. This framework de-emphasizes integrity protection while em.

2.2 Feasibility Characterization and Constraint Optimization of Anti-Mapping Targets

The construction of anti-mapping targets relies on systematic constraints of the "visibility-identity-mergeability" ternary relationship. Defensive actions typically maintain business continuity while reducing detection confidence in a computable manner. Formalized modeling indicates that the anti-mapping problem can be represented as a multi-objective constrained optimization problem, with core focuses on defining the cost function for observable attributes and balancing significance minimization with interference load control. Feasibility characterization requires the finite closure of the anti-mapping space: strategies should converge smoothly to the optimal feasible domain under given resource constraints. Through a hierarchical constraint model, defense mechanisms maintain logical consistency across network layers, ensuring that operations and business attributes function effectively under the semantic meaning of mapping detectability—rendering the anti-mapping system theoretically complete and structurally self-consistent.

A paradigmatic implementation of this feasibility characterization and constraint optimization is the Source Address Spoofing and Distributed Topology Mapping Verification System, which comprises four interrelated subsystems embodying the balance between anti-mapping effectiveness and business feasibility:

- **Intranet Feature Analysis and Generation Subsystem:** Collects topology data from scenarios such as IoT, industrial control systems (ICS), and data centers via non-intrusive mapping techniques. It extracts key topological features (connection degree, betweenness centrality, clustering coefficient) and intelligently generates simulated intranet topologies (with assigned IP addresses for fake nodes)—ensuring real business operations remain undisturbed while providing a basis for deception.

- **Topology Information Hiding Subsystem:** Identifies topology-probing traffic (e.g., Traceroute packets) via deep packet inspection. For non-whitelisted IPs, it modifies the source address of response packets (to match fake nodes in the simulated topology) based on TTL (Time To Live) values—reducing attackers' detection confidence without disrupting normal network connectivity (upholding "business availability" in the CACA framework).
- **Behavior Audit and Tracking Subsystem:** Correlates scanning behaviors with cybersecurity intelligence (stored in a security intelligence database) to trace malicious entities and identify APT (Advanced Persistent Threat) attack chains. This ensures "controllability" (a core tenet of CACA) by preventing unmonitored deception and attack escalation.
- **Distributed Topology Mapping Verification Subsystem:** Deploys probe nodes across global network regions to verify the effectiveness of topology hiding. It compares attackers' "perceived topology" (derived from probe results) with the simulated topology—ensuring the strategy converges to the "optimal feasible domain" without excessive resource consumption.

This system directly addresses the multi-objective optimization of "minimizing mapping visibility" and "controlling interference load," serving as a concrete case for feasibility characterization in anti-mapping.

3. Intelligent Anti-Mapping Methodology and Strategy Orchestration

3.1 Active Defense Mechanism Family Centered on "Evidence Perturbation"

The core conceptual framework of the intelligent defense system is evidence perturbation (EP), which disrupts key transitional stages in the detection chain (from observation to fusion) to weaken the credibility of external mapping activities across data and logical layers. This mechanism family encompasses three technical dimensions: dynamic polymorphism of protocol behaviors, temporal perturbation of fingerprint features, and semantic substitution of service mappings. Its essence lies in generating non-deterministic visibility patterns via controlled noise modulation—disrupting stable feature matching in mapping systems. This interference is not random noise but constrained intelligent modulation: the design principle adheres to minimizing interference within the boundaries of business availability. During the evolution of defense strategies, perturbation intensity and network topology coupling require careful consideration to ensure high entropy in evidence distribution—rendering external detection systems unable to establish a foundation for analytical fusion.

The evidence perturbation mechanism is significantly enriched by two technical modules, which provide actionable pathways for "controlled noise modulation":

3.1.1 Targeted Probing Behavior Detection

(LIU Qingyun, 2023)To avoid blind perturbation (which risks disrupting business operations), the system first identifies mapping-specific probing traffic, with a focus on three common Traceroute variants (a primary tool for topology mapping), as shown in the following table 1:

Table 1 Characteristics of Common Traceroute Variants

Traceroute Type	Detection Features	Distinguishing Characteristics from Normal Traffic
ICMP-based	Approximately 64-byte packet size, 1-3s fixed interval, incrementing TTL (step size of 1)	Rarely utilized for legitimate communication; fixed interval distinguishes from random ICMP packets
UDP-based	High target ports (>1024), incrementing TTL, frequent "Destination Unreachable" responses	Legitimate UDP employs well-known ports; "Destination Unreachable" responses are anomalous
TCP-based	TCP SYN packets, incrementing TTL, ICMP "Time Exceeded" or TCP RST responses	Normal TCP handshakes use consistent TTL values; SYN-only patterns indicate scanning behavior

This targeted detection ensures perturbation is exclusively applied to mapping traffic—strictly adhering to the "minimal interference under business availability" principle.

3.1.2 Host Mapping Obfuscation via Protocol Reverse Engineering

Complementing topology perturbation, the Host Mapping Obfuscation System Based on Protocol Reverse Engineering addresses host-level mapping threats. For ICS and Internet terminals, the system operates through three sequential steps:

1) Reverses protocol interaction processes (e.g., Modbus for ICS, SSH for servers) to extract unique fingerprint features (e.g., packet structure, handshake sequences) and constructs a protocol fingerprint database.

2) Detects host fingerprint scanning (e.g., Nmap fingerprinting) via traffic pattern analysis.

3) Applies a fingerprint confusion algorithm to select fake fingerprints from the database (e.g., returning a "Windows 10" fingerprint for a critical ICS host) and transmits them to attackers—inducing misjudgments in host identification and breaking the "observation-to-fusion" chain in mapping.

(Abdelnabi S, 2023)This module directly achieves "semantic substitution of service mappings" in evidence perturbation, which is particularly critical for protecting key assets such as ICS controllers.

3.2 Adaptive Orchestration and Governance for "Strategy Domain Convergence"

The adaptive orchestration mechanism is responsible for strategy coordination and global convergence in the intelligent defense system, ensuring consistency and stability of different defense units across temporal and spatial scales. Based on real-time perception of detection behavior patterns, the strategy system constructs dynamic feedback channels—enabling perturbation parameters to evolve self-consistently in non-stationary environments. At the governance level, hierarchical modeling of the strategy domain resolves constraints such as resource allocation, strategy weights, and interaction rules to maintain system stability. The core idea of adaptive governance is iteratively converging strategies toward the Pareto optimal boundary—minimizing business costs while maximizing the defense system's anti-mapping performance. This process is not a simple strategy overlay but cross-layer collaborative optimization, enabling anti-mapping capabilities to form a robust self-balancing state from algorithmic and structural perspectives (distinct from conventional defense system optimization). Internationally, similar adaptive deception frameworks—such as the Cognitive-Adaptive

Deception Layer (CADL)—have demonstrated the critical role of adaptive strategies in enhancing defensive efficacy. (AL-Zahrani B A, 2025)By integrating ensemble machine learning with behavioral analysis, CADL achieved a detection rate of 99.88% and a false positive rate of merely 0.13% on the CSE-CIC-IDS2017 dataset, further validating the effectiveness of such approaches in advanced cyber defense.

The Distributed Topology Mapping Verification Subsystem (a component of the Source Address Spoofing System) serves as a linchpin for adaptive orchestration and "strategy domain convergence." Its four modules close the "execution→verification→adjustment" loop to support Pareto optimization:

- **Probe Node Management Module:** Manages probe nodes across diverse network regions (e.g., North America, Asia, Europe), including node addition, status monitoring, and fault recovery—ensuring spatial coverage of strategy verification (avoiding local network bias).
- **Probe Task Management Module:** Creates, pauses, and modifies topology probing tasks (e.g., simulating attackers' Traceroute scans) and monitors task execution in real time—aligning with temporal scale consistency requirements.
- **Probe Task Execution Module:** Constructs a simulated mapping environment on each node to execute tasks (mimicking real attacker tools and behaviors) and collects raw probe results (e.g., perceived node IPs, hop counts).
- **Probe Result Recovery Module:** Merges results from all nodes to reconstruct the "attacker-perceived topology," then compares it with the simulated topology generated by the defense system. If the similarity exceeds a threshold (e.g., 70%), the system adjusts perturbation parameters (e.g., increases fake node density, modifies TTL response logic)—pushing the strategy toward the Pareto optimal boundary (maximizing hiding effect with minimal node resources).

This subsystem ensures that adaptive governance is not merely theoretical but data-driven, directly enhancing the system's ability to converge to optimal performance.

4. Conclusion

The intelligent anti-mapping defense strategy proposed in this paper provides a comprehensive approach to enhancing cyberspace asset security from both theoretical and practical perspectives. Through accurate semantic abstraction (exemplified by the CIAA vs. CACA frameworks), efficient evidence perturbation (strengthened by Traceroute detection and fingerprint obfuscation), adaptive strategy orchestration (supported by distributed verification), and concrete technical implementations from two proposed frameworks (i.e., Source Address Spoofing System and Host Mapping Obfuscation System), this defense framework substantially mitigates the efficacy of mapping attacks while preserving core business operations. This intelligent defense approach maintains high anti-detection capability in dynamic environments (e.g., ICS, large-scale data centers), offering a feasible and effective solution for security protection in complex network environments.

Acknowledgements

National Key R&D Program of China under Grant "Cybersecurity Governance" Key Special Project Anti-network scanning, probing, and identification technology (2022YFB3102902)

References

[1] Guo Li, Cao Yanan, Su Majing, et al. Cyberspace Resources Surveying and Mapping: The Concepts and

Technologies [J]. Journal of Information Security, 2018, 3(4): 1-14. (in Chinese)

[2] Xue X, Zou H, Zhao J, et al. Advances in Anti-Surveying-and-Mapping Theory and Technologies for Data Infrastructure[J]. Strategic Study of Chinese Academy of Engineering, 2025, 27(1): 72-87. ((in Chinese)

[3] Harshitha DH, Swaroop Pattar, Chandan Kumar. THE PERFECT STORM: INSIDER THREATS AND ADVANCED DECEPTION TACTICS IN CYBERSECURITY[J]. International Research Journal of Modernization in Engineering Technology and Science, 2025,7(1):1071-1077

[4] LIU Qingyun, LI Renjie, ZHOU Zhou, ZHONG Youbing, SHI Fengyuan, GUO Li. Research on Cyberspace Anti-Surveying and Mapping[J].Journal of Cyber Security, Accept.(in Chinese)2023

[5] Abdelnabi S, Fritz M. {Fact-Saboteurs}: A taxonomy of evidence manipulation attacks against {Fact-Verification} systems[C]//32nd USENIX Security Symposium (USENIX Security 23). 2023: 6719-6736.

[6] AL-Zahrani B A. Adaptive Deception Framework with Behavioral Analysis for Enhanced Cybersecurity Defense[J]. arXiv preprint arXiv:2510.02424, 2025.