Future Artificial Intelligence Research

GENERAL CONFERENCE ROME 10/12 DEC 2025

National PhD in Artificial Intelligence for Society

NotLine: Dynamic Network Topology and Risk Assessment Through Passive Discovery

Vincenzo Sammartino

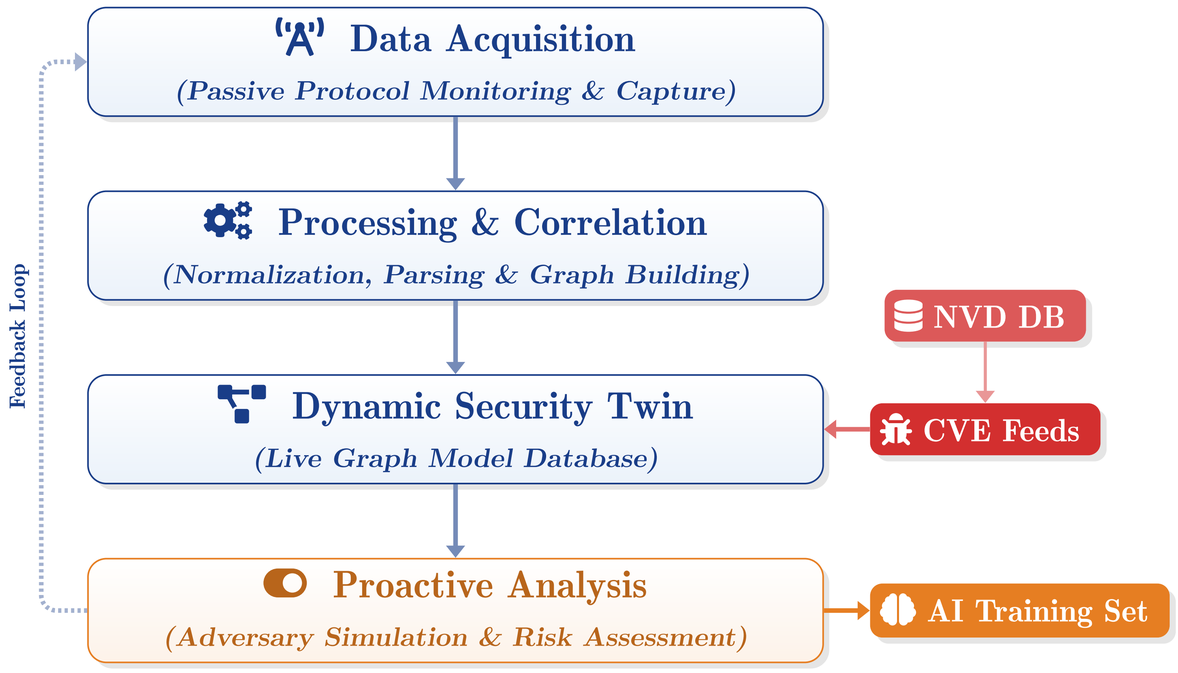
Introduction

Digital twin technology is revolutionizing cybersecurity by creating real-time replicas of ICT/OT infrastructures. We introduce **NotLine**, a **non-intrusive, automated platform** that builds and updates a digital twin through continuous passive monitoring. It enhances network visibility without impacting live systems.

Key Contributions

- **Non-Intrusive Reverse Engineering:** Builds network topology purely from passive traffic, avoiding active scanning risks.
- **Fully Automated Pipeline:** Data collection, normalization, and graph building.
- **Security Enrichment:** Dynamically aquire real-time vulnerability data (CVEs).
- **Scalability:** Designed for sensitive environments (OT/Healthcare) with zero downtime requirements.

NotLine Pipeline



The Zero-Touch Advantage

Traditional scanners such as Nmap generate active traffic that can crash legacy OT devices. **NotLine is invisible.**

- **No Network Overhead:** Uses TAP/SPAN ports only.
- **Undetectable:** The monitor has no IP address on the production network.
- **Continuous:** Updates topology in real-time, not just during scheduled scans.

Key Protocols Analyzed

- **ARP** Maps IP to MAC addresses; foundational for device identity.
- **mDNS** Reveals device roles via multicast service discovery.
- **DHCP** Tracks dynamic IP assignments and lease times.
- **ICMP** Maps connectivity and potential reachability issues.

Synthetic Data & AI Applications

Data drift undermines AI security models. NotLine leverages a dual-twin scenario to generate high-fidelity synthetic data.

1. **Training** Creates labeled datasets (Attack vs. Normal) to train robust IDS models.
2. **Validation** Tests security check (ie firewall rules) by simulating attack paths on the twin.
3. **Risk Quant.** Calculates node compromise probability using graph centrality metrics.

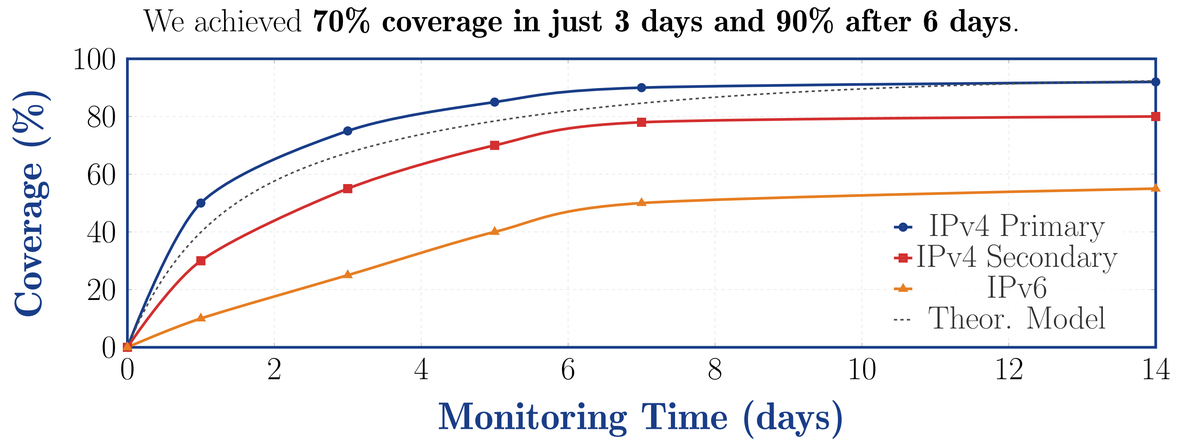
Experimental Setup

Deployed in a heterogeneous university production network.

- **Duration:** 42 days continuous monitoring.
- **Scope:** 77 distinct devices (IoT, Workstations, Servers).
- **Traffic:** Mixed IPv4/IPv6 captured from a central mirror port.

Results: Discovery Efficiency

Insight: Node discovery follows a "steep-then-slow" logarithmic curve.
We achieved **70% coverage in just 3 days and 90% after 6 days**.



$$Hypoexponential function: f(t) = \alpha_1 e^{-\beta_1 t} + \alpha_2 e^{-\beta_2 t}$$

Real-world Insight: Device Profiling

Lucias-iMac

Detected Profile:

- **Identity:** `3C:A6:F6:...` (Apple Inc.)
- **Behavior:** Frequent UDP flow to Cloud Storage.
- **Vulnerability:** Linked to **CVE-2025-31194** (Privilege Escalation) via User-Agent version fingerprinting.

Conclusion & Future Outlook

NotLine strongly generalize traditional topology mapping by establishing a **symbiotic digital twin** that evolves alongside the infrastructure. By decoupling security analysis from operational risk, it lays the foundation for **autonomous, self-healing networks**.

This non-intrusive metodology support the next generation of **predictive AI defense**, capable of simulating and neutralizing complex threat vectors in the virtual realm before they ever impact physical reality.

Contact

vincenzo.sammartino@phd.unipi.it

Funded by the European Union NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA