Phantom Protocol

Dual-Domain Cyber & Electronic Warfare Threat Detection and Defence

Team: Rajat G (22BEC038)

Hemanth Kumar M U (22BEC019)

Vijayakumar N J (22BCS136)

Swaroop Patil (22BCS083)

Summary

The **Phantom Protocol** is a unified, simulation-driven defense system addressing the convergence of cyber and electronic warfare (**EW**) threats in modern operational environments. Leveraging programmable software-defined networking (**SDN**), advanced signal processing, and real-time threat correlation, the project delivers autonomous detection, fusion, and mitigation of coordinated attacks across both cyberspace and the electromagnetic spectrum.[1][2]

Introduction

Modern electronic battlespaces increasingly experience attacks where adversaries blend **cyber intrusions** with **electromagnetic disruption**. Traditional defenses operate in silos, impairing the rapid, coordinated response required for multi-domain threats. This report outlines the background, motivation, technical approach, threat models, defense strategies, experimental setup, evaluation metrics, results, and future work for the Phantom Protocol.

Problem Statement

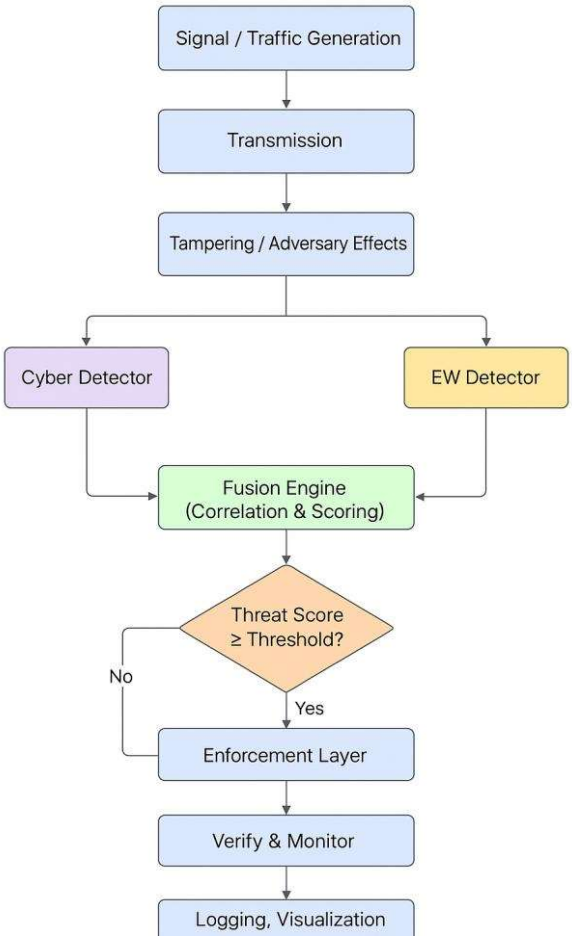
Adversaries now synchronize cyber and EW tactics—such as coupling a **DDoS** with **RF jamming**—to maximize impact. Existing tools struggle with:

- Delayed recognition due to domain-specific isolation.
- Inefficient, uncoordinated responses unable to counter multi-domain campaigns.
- Limited operational visibility, preventing optimal decision-making

Related Work & Technology Landscape

- **Cybersecurity:** IDS/IPS (Snort, Suricata), SDN-based mitigations, forensic analytics.
- **Electronic Warfare:** Spectrum analyzers, SIGINT, GNU Radio, protocol-agnostic anomaly detection.
- **Integration Research:** NATO, defense agencies, and academia highlight the growing imperative for Cyber-Electromagnetic Activities (**CEMA**) platforms.

High-Level Architecture



A designated space for a flow diagram that visually details the interaction between Mininet, SDN controllers, cyber/EW detectors, Fusion Engine, and Mitigation modules is reserved here.

[Suggested diagram sections: Traffic Generation → SDN Control Plane → Cyber Detection → EW Detection → Messaging Bus (ZeroMQ/MQTT) → Fusion Engine → Automated Mitigation → Visualization]

Methodology

Simulation Environment

- Configurable network topologies in **Mininet**.
- Centralized control leveraging the **Ryu SDN controller**.
- Attack and legitimate traffic orchestrated using **Scapy**, **hping3**, and **iperf3**.

EW Signal Generation

- Realistic simulation of normal, jamming, spoofing, meaconing, and interference signals via **GNU Radio** and scientific Python tools.
- Spectral features (band power, peak detection, occupancy metrics) enable robust EW anomaly detection.

Detection Modules

Cyber Detection

- **Continuous telemetry:** Flow stats, RTT, packet drops, flow counts.
- **Attacks Detected:** DDoS, port scans, lateral movement, exfiltration, flow irregularities.
- **Alert Output:** Structured JSON alerts with severity metadata

EW Detection

- Spectral and time-domain analysis to track jamming, spoofing, replay, and targeted interference.
- **Alert Output:** EW event JSON with affected bands/links and severity.

Messaging & Integration

- **ZeroMQ/MQTT** for ultra-low-latency, reliable pub/sub between all sensing components and the Fusion Engine.
- Timestamped messages ensure proper event correlation.

Fusion and Mitigation

- The **Fusion Engine** receives alerts, correlates them across time-windows, and computes threat scores using a tunable rule-set or lightweight ML.
- Automated SDN-based responses: drop rules, flow re-routing, host quarantining, and rate limits.

- Simulated EW responses: frequency hopping, filtering, backup links.

Dynamic MTD Layer

- Optional Moving Target Defense: Periodically shifts topology, IP/MAC mapping, and injects decoys.
- Attack resilience is enhanced by disrupting adversarial reconnaissance and mapping.

Visualization

- Real-time dashboard with topology, flow heatmaps, spectrum waterfalls, and threat/action logs.
- Supports detailed analysis and replay.

Threat Models & Countermeasures

Cyber Threats

Threat	Detection Cues	Simulated Mitigations	MTD Integration Notes
DDoS	High-rate flows, flow table surges	Drop/rate-limit by flow, reroute sensitive	Remap monitored IPs post-MTD
Port Scan	Burst of short-lived connections, SYN patterns	Blackhole/mirror scanning flows	Ignore noise during MTD windows
Lateral Movement	New east-west flows, changed port usage	Micro-segmentation, temporary quarantine	Whitelist post-MTD flows
Exfiltration	Persistent low-rate to rare dest., timing channels	Mirror/drop, DPI, host isolation	Track by logical flow, not address

EW Threats

Threat	Detection Methods	Simulated Mitigations	MTD Integration Notes

Broadband Jamming	Wideband energy rise, SNR drops	Freq. hop, reroute via SDN, notch filtering	Use timestamps to sync hops vs attacks	
Narrowband Jamming	Local spectral spike, channel-specific errors	Targeted null/hop, per-flow agile routing	Reset baselines on hop	
Spoofing/Meaconing	Duplicate signals, timing anomalies	Require nonce/timestamp, drop/redirect traffic	Tolerance for migration/timing shifts	
Smart/Targeted Interf.	Interference tied to protocol/traffic patterns	Randomized flow/freq., SDN pacing, blackhole attackers	Widen detection time windows	[3][4]

Security Features

- **Programmable SDN Control:** Enables rapid, fine-grained isolation and containment.
- **Advanced Detection:** Statistical and behavioral analysis beyond static signatures.
- **Autonomous Response:** Machine-speed defense reduces mean-time-to-mitigation (MTTM).
- **MTD Integration:** Continual assessment of moving target defense impacts on detection thresholds and response strategies; detectors re-learn baselines post shift to minimize both evasion and false alarm rates.
- **Privacy and Replay Protection:** Use of cryptographic nonces/timestamps in simulated protocols.
- **Comprehensive Logging:** All events, mitigations, and system state changes are timestamped and stored for forensic analysis.

Metrics & Evaluation

- **Detection/Mitigation Latency:** Time from event onset to action.
- **Mitigation Efficacy:** PDR, post-mitigation service levels.
- **False Positive/Negative Rates:** For all detectors, cross-domain.
- **System Load:** Resource footprint under active defense.
- **Baseline vs Defense Outcomes:** Comparative performance under attack.

Results

The results section for this project is not available at this time, as Phantom Protocol is a comprehensive end-to-end platform whose outcomes—such as detection accuracy, mitigation latency, and real-world defense

performance—can only be assessed and reported after the full system has been implemented and all modules are integrated and tested. Apologies for the inconvenience; detailed results and evaluation metrics will be provided at later stages of development once all components have been completed and validated through practical experimentation.

Conclusions

The Phantom Protocol demonstrates a robust, extensible, and operational testbed for research in cyber-EW defense integration. The framework's fusion of **SDN cyber defense** and **EW signal intelligence**, enhanced by automation and MTD compatibility, advances the state-of-the-art in resilient network and spectrum operations.

References

https://www.japcc.org/articles/cyber-electromagnetic-domain/

https://www.japcc.org/articles/navigating-the-digital-battlefield/

https://assets.publishing.service.gov.uk/media/667d6471c7f64e23420900d6/ARCHIVE-JDN_1_18_Cyber_and_electromagnetic_activities.pdf

https://ijisae.org/index.php/IJISAE/article/view/7036

https://blog.lumen.com/what-is-software-defined-networking-security/

https://journals.rta.lv/index.php/ETR/article/download/8483/6930/10828

https://www.youtube.com/watch?v=ZjwNtDSSZgM

https://www.lupovis.io/what-is-moving-target-defense-in-cybersecurity/

https://github.com/girishsg24/Moving-Target-Defense-RHM-using-SDN

https://www.obriain.com/training/sdn/RYU_Soft_Testbed_v1.6_odt.pdf

https://blog.geekinstitute.org/2025/05/mastering-hping3-advanced-guide-to-network-testing.html