AI in Networking

AI-Driven Network Anomaly Detection: Protecting Networks in Real-Time

Margarita Stoilova
Ripe See 13, 7-8 April 2025

Why Network Anomaly Detection Matters?

- **Security Threats:** DDoS attacks, BGP hijacks, unauthorized access.
- **Performance Issues:** Latency spikes, bandwidth exhaustion, unexpected failures.
- **Traditional detection methods struggle** due to increasing network scale and sophistication of attacks.

Example:

- In 2023, a large-scale **BGP hijack** redirected traffic from major ISPs, leading to severe disruptions.
- **AI-based anomaly detection could have prevented it in real time**.

How AI Detects Network Anomalies?

AI models analyze network data and identify unusual patterns by:

- **Learning normal behavior** (baseline traffic patterns).
- **Detecting deviations** from normal traffic (unexpected packet rates, BGP route changes, suspicious flows).
- **Classifying threats** (DDoS, botnets, route leaks) with machine learning models.

1. **Data Collection** → 2. **Feature Extraction** → 3. **Model Training** → 4. **Real-Time Detection** → 5. **Automated Response**

Data Sources for AI-Based Detection

To train AI models, we need real network data:

- **Traffic Logs** (NetFlow/IPFIX, PCAP files)
- **Routing Data** (BGP updates, RPKI validations)
- **IDS/IPS Alerts** (Suricata, Zeek)
- **Security Event Logs** (Wazuh, TheHive)

Where to get public datasets?

- **CICIDS 2018** – Includes labeled network attacks.
- **MAWI Traffic** – Real ISP traffic logs.
- **CTU-13 Botnet Dataset** – Detects botnet activities.

Machine Learning Models for Anomaly Detection

AI models analyze network data and identify unusual patterns by:

- **Supervised Learning** – Uses labeled attack data (e.g., Random Forest, SVM).
- **Unsupervised Learning** – Detects unknown threats (e.g., Isolation Forest, Autoencoders).
- **Deep Learning** – Detects temporal patterns in traffic (e.g., LSTMs, CNNs for packet classification).

AI-Powered DDoS and BGP Hijack Detection

DDoS detection:

- AI can differentiate **high-traffic legitimate users vs. volumetric attacks**.
- Analyzes packet size, flow rate, and source diversity to classify traffic.
- **AI-based models can automatically mitigate attacks in real-time.**

BGP Hijack Detection:

- AI can monitor **BGP updates** for anomalies in route announcements.
- Tools like **BGPalerter** + AI can trigger alerts in real time.

How It Works?

1. **Collect BGP updates from RIPE RIS**.
2. **Train AI model** to detect prefix anomalies.
3. **Block malicious announcements** before traffic reroutes.

Open-Source Tools for AI-Powered Detection

Integrate AI models with existing tools:

- **Traffic Analysis:** Zeek, Suricata, Wireshark.
- **Machine Learning Frameworks:** TensorFlow, PyTorch, Scikit-learn.
- **Routing Security:** BGPalerter, ExaBGP.
- **Monitoring & Visualization:** ELK Stack, Prometheus, Grafana.

Step-by-Step: How AI Detects and Blocks Malicious Traffic

Suricata IDS inspects traffic for known threats

Flags suspicious activity based on existing **IDS** rules and signatures.

Logs flagged events in **.json** or forwards them to **Redis/Kafka**.

Zeek captures and analyzes full network traffic

Independently inspects **all packets**, even those Suricata did not flag.

Extracts metadata (e.g., connection duration, byte patterns) and sends logs to **AI**.

AI model processes both Suricata and Zeek data

Supervised ML models (Random Forest, SVM) detect known attack signatures.

Unsupervised ML (Isolation Forest, Autoencoders) identifies novel threats.

AI correlates findings between Zeek & Suricata to reduce false positives.

AI takes automated action if a threat is confirmed

Sends **API requests to firewall systems** (e.g., IPTables, MikroTik, Cisco ACLs) to block malicious IPs.

Generates new rules for **Suricata IDS**, improving future detections.

Stores logs in **Elasticsearch** and alerts security teams via **Prometheus AlertManager, TheHive, or Wazuh**.

Continuous AI model improvement

Feedback loop: Security teams validate flagged traffic, refining AI training.

Dashboard visualization: Grafana/Kibana monitors threats in real-time.

Adaptive IDS rules: AI continuously updates Suricata to improve detection accuracy.

Q&A

👩‍💻Contact: **Margarita Stoilova**

📧 Email: margarita@sdnix.com