The AI Paradox: Dual-Edged Sword in DNS Security

Lightening talk ICANN’83 Prague

Nabil Benamar

SSAC

The AI Paradox

DNS: Universal resolver, critical infrastructure, pervasive attack vector.

The "**AI Shift**": Redefining Cyber Attack & Defense.

Paradox: AI weaponized by adversaries

AI as our most potent defense.

Today's Focus: Understanding the AI vs. AI arms race in DNS.

The Attacker's Arsenal: AI-Enhanced DNS Attacks

- DNS is foundational to Internet communications.
- Threats include cache poisoning, DDoS, and tunneling.
- AI is making these threats more dynamic and evasive.
- But…. **How AI Helps?**
  - **Payload Anomaly Detection**
  - **Behavioral Analysis and Pattern Recognition**

AI in DNS Attacks – Emerging Threats

- AI-Driven DDoS Attacks:
  - increasing attack sophistication and evasion capabilities
- Algorithmic Complexity Attacks:
  - New attacks like KeyTrap exploit DNSSEC with high computational complexity, potentially disabling DNS services at scale
- Botnet Evolution:
  - Domain Generation Algorithms (DGAs) to evade detection and sustain malicious command-and-control via DNS

Computer Science > Cryptography and Security

[Submitted on 22 Mar 2025]

Detecting and Mitigating DDoS Attacks with AI: A Survey

Alexandru Apostu, Silviu Gheorghe, Andrei Hîji, Nicolae Cleju, Andrei Pătraşcu, Cristian Rusu, Radu Ionescu, Paul Irofti

Distributed Denial of Service attacks represent an active cybersecurity research problem. Recent research shifted from static rule-based defenses towards AI-based detection and mitigation. This comprehensive survey covers several key topics. Preeminently, state-of-the-art AI detection methods are discussed. An in-depth taxonomy based on manual expert hierarchies and an AI-generated dendrogram are provided, thus settling DDoS categorization ambiguities. An important discussion on available datasets follows, covering data format options and their role in training AI detection methods together with adversarial training and examples augmentation. Beyond detection, AI based mitigation techniques are surveyed as well. Finally, multiple open research directions are proposed.

AI in DNS Attacks: Next-Gen DGAs

- From static malware to adaptive AI-powered threats.
- Use of:
  - LLMs for domain generation
  - GANs for stealthy traffic
  - RL for DNS tunneling

PeerJ Computer Science

Hybrid rule-based botnet detection approach using machine learning for analysing DNS traffic

Saif Al-mashhadi[1,2], Mohammed Anbar[1], Iznan Hasbullah[1] and Taief Alaa Alamiedy[1,3]

[1] National Advanced IPv6 Centre, Universiti Sains Malaysia, Penang, Malaysia
[2] Electrical Engineering, University of Baghdad, Baghdad, Baghdad, Iraq
[3] ECE Department- Faculty of Engineering, University of Kufa, Kufa, Najaf, Iraq

ABSTRACT

Botnets can simultaneously control millions of Internet-connected devices to launch damaging cyber-attacks that pose significant threats to the Internet. In a botnet, bot-masters communicate with the command and control server using various

LLM-Generated Domain Generation Algorithms (DGA)

GPT and LLAMA-based DGAs mimic linguistic properties of legitimate domains.

Outperform traditional algorithmic DGAs in evading detection.

Achieve ~98% stealth rate vs entropy-based filters.

How AI Detects DGAs

Traditional methods struggle with DGA because they look for *known bad* domains. AI, on the other hand, looks for *patterns of badness*.

AI models are trained on vast datasets of both legitimate domain names and known DGA-generated domains. They learn to identify the statistical and linguistic characteristics that differentiate DGA domains from normal ones.

Detecting DNS Tunneling on Edge Devices

- **Behavioral Analytics and Machine Learning (AI):**
  - AI and ML are increasingly used to detect DoH traffic even without decryption. This involves:
  - Analyzing connection patterns.
  - Identifying statistical anomalies in TLS handshake characteristics.
  - Leveraging threat intelligence about known DoH malware.
  - Recognizing application-specific DoH client behaviors.

Information Fusion 121 (2025) 103125

Contents lists available at ScienceDirect

Information Fusion

journal homepage: www.elsevier.com/locate/inffus

Full length article

METC: A Hybrid Deep Learning Framework for Cross-Network Encrypted DNS over HTTPS Traffic Detection and Tunnel Identification

Ming Zuo[1], Changyong Guo[1], Haiyan Xu[1], Zhaoxin Zhang[*,2], Yanan Cheng[*,3]

Harbin Institute of Technology, Harbin, 1043 NX, China

Federated Learning for DNS Defense

- Cross-organization federated learning.
- No raw data sharing—models trained locally and aggregated securely.

CO-DEFEND: Continuous Decentralized Federated Learning for Secure DoH-Based Threat Detection

Diego Cajaraville-Aboy, Marta Moure-Garrido, Carlos Beis-Penedo, Carlos Garcia-Rubio, Rebeca P. Díaz-Redondo, Celeste Campo, Ana Fernández-Vilas, and Manuel Fernández-Veiga

Abstract

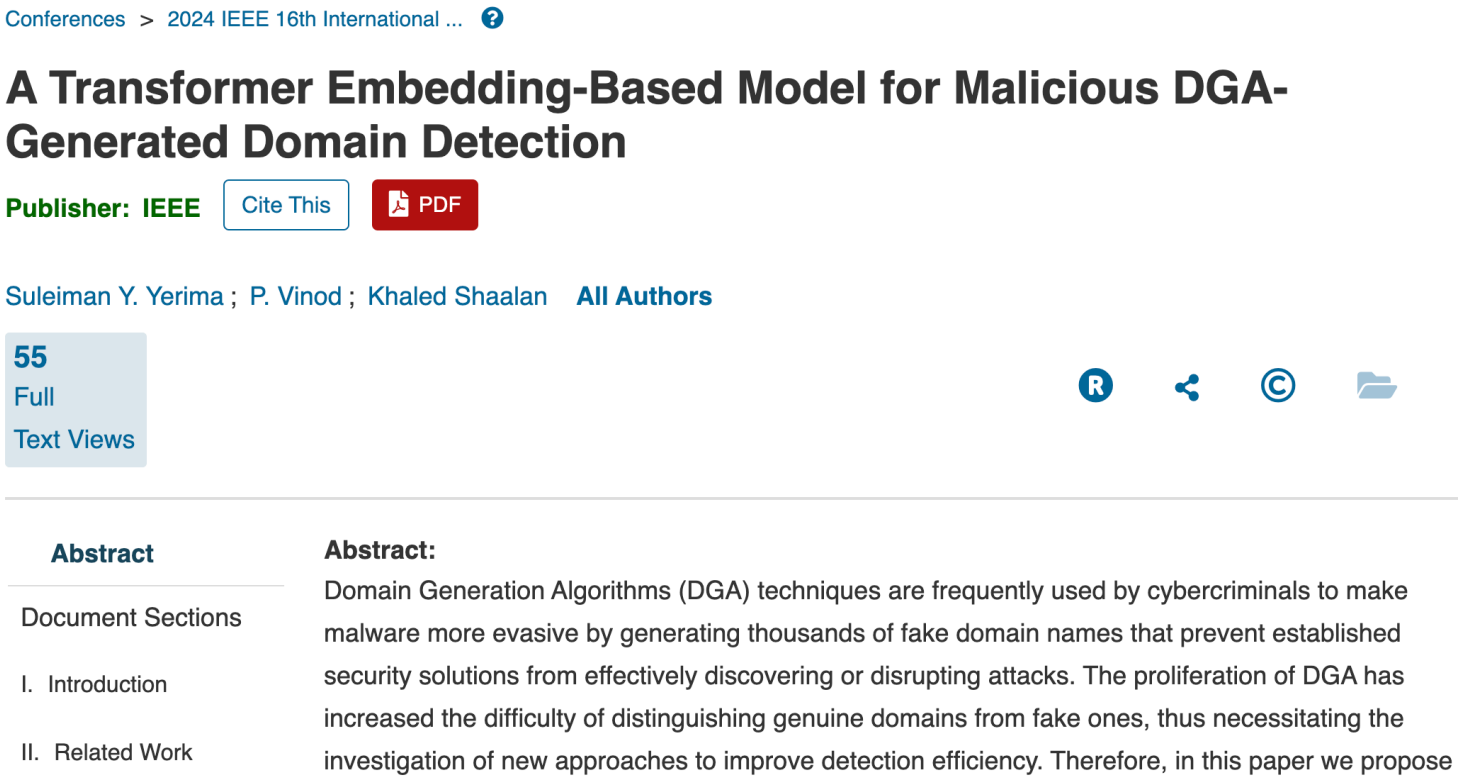
The use of DNS over HTTPS (DoH) tunneling by an attacker to hide malicious activity within encrypted DNS traffic poses a serious threat to network security, as it allows malicious actors to bypass traditional monitoring and intrusion detection systems while evading detection by conventional traffic analysis techniques. Machine Learning (ML) techniques can be used to detect DoH tunnels; however, their effectiveness relies on large datasets containing both benign and malicious traffic. Sharing such datasets across entities is challenging due to privacy concerns. In this work, we propose CO-DEFEND (Continuous Decentralized Federated Learning for Secure DoH-Based Threat Detection), a Decentralized Federated Learning (DFL) framework that enables multiple entities to collaboratively train a classification machine learning model while preserving data privacy and enhancing resilience against single points of failure. The proposed DFL framework, which is scalable and privacy-preserving, is based on a federation process that allows multiple entities to train online their local models using incoming DoH flows in real time as they are processed by the entity. In addition, we adapt four classical machine learning algorithms, Support Vector Machines (SVM), Logistic Regression (LR), Decision Trees (DT), and Random Forest (RF), for federated scenarios, comparing their results with

Graph Neural Networks for DNS Tunneling

- GNNs model relationships between domains, IPs, sessions.
- Capture behavior patterns missed by single-flow models.
- Robust even in encrypted contexts.

Transformer-Based DGA Detection

- Fine-tuned LLMs (LLAMA3, GPT-Neo) trained on large domain corpora.
- Capture contextual and syntactic features of malicious domains.
- 98.6% detection accuracy on novel DGAs.



Conferences > 2024 IEEE 16th International ...

A Transformer Embedding-Based Model for Malicious DGA-Generated Domain Detection

Publisher: IEEE | Cite This | PDF

Suleiman Y. Yerima ; P. Vinod ; Khaled Shaalan All Authors

55 Full Text Views

Abstract

Document Sections

I. Introduction

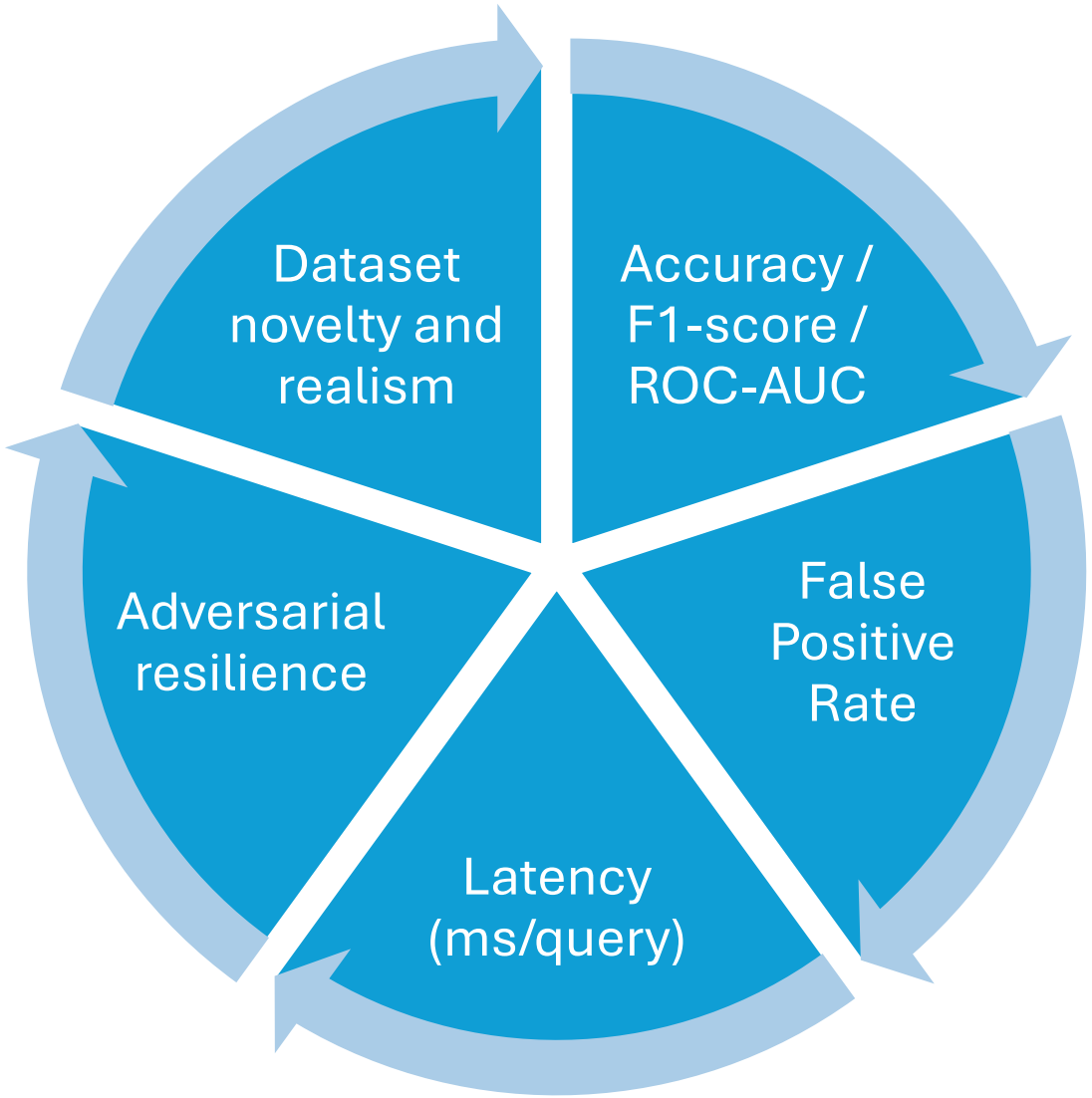
II. Related Work

Abstract:
Domain Generation Algorithms (DGA) techniques are frequently used by cybercriminals to make malware more evasive by generating thousands of fake domain names that prevent established security solutions from effectively discovering or disrupting attacks. The proliferation of DGA has increased the difficulty of distinguishing genuine domains from fake ones, thus necessitating the investigation of new approaches to improve detection efficiency. Therefore, in this paper we propose

Adversarial Robustness via Simulated Attacks

- Training defenses using GAN/RL-generated adversarial examples.
- Improves model robustness and reduces overfitting.
- Essential for real-world deployments.

Key Evaluation Metrics



Key Research Findings

- AI-powered DGAs outperform old malware DGAs.
- Lightweight ML works on edge devices.
- GNNs excel at modeling tunneling behavior.
- FL enables privacy-aware collaboration.
- **AI is Central:** AI is not just a peripheral tool or an optional add-on; it's a fundamental and indispensable component.

Explainable AI (XAI)

- Explainable AI (**XAI**) is paramount.
- "**black box**" nature of complex AI models.
- **XAI** allows to understand *why* an AI model made a particular decision.
- **Human-AI Collaboration**

Next-Generation Ai for Advanced Threat Detection and Security Enhancement in Dns Over Https

32 Pages • Posted: 21 Apr 2025

Basharat Ali
Nanjing University

Abstract

The mass deployment of DNS over HTTPS (DoH) has introduced a new paradigm of network privacy using the encryption of DNS requests, but the very same feature has been exploited by nefarious forces to orchestrate stealthy cyberattacks, from polymorphic malware delivery, data theft, to command-and-control (C2) activities. Existing signaturebased detection using static legacy security controls and deep packet inspection become rendered ineffective in detecting encrypted DoH traffic, while existing AI solutions are lacking in being adversarially strong, explainable, and scalable in real time. This article bridges these significant gaps by recommending a future-ready AI system merging stateof-art machine learning paradigms and secure execution environment to ensure end-to-end resilience, interpretability, and real-time speed-

The AI Paradox: A Continuous Evolution

- AI defines the modern DNS threat landscape.
- Attacker AI: Faster, more sophisticated, evasive attacks.
- Defender AI: Scalable, adaptive, proactive mitigation.
- **The Future:** An "AI vs. AI" arms race.
- **Key:** Continuous innovation in defensive AI, robust training, and intelligent human-AI collaboration.