

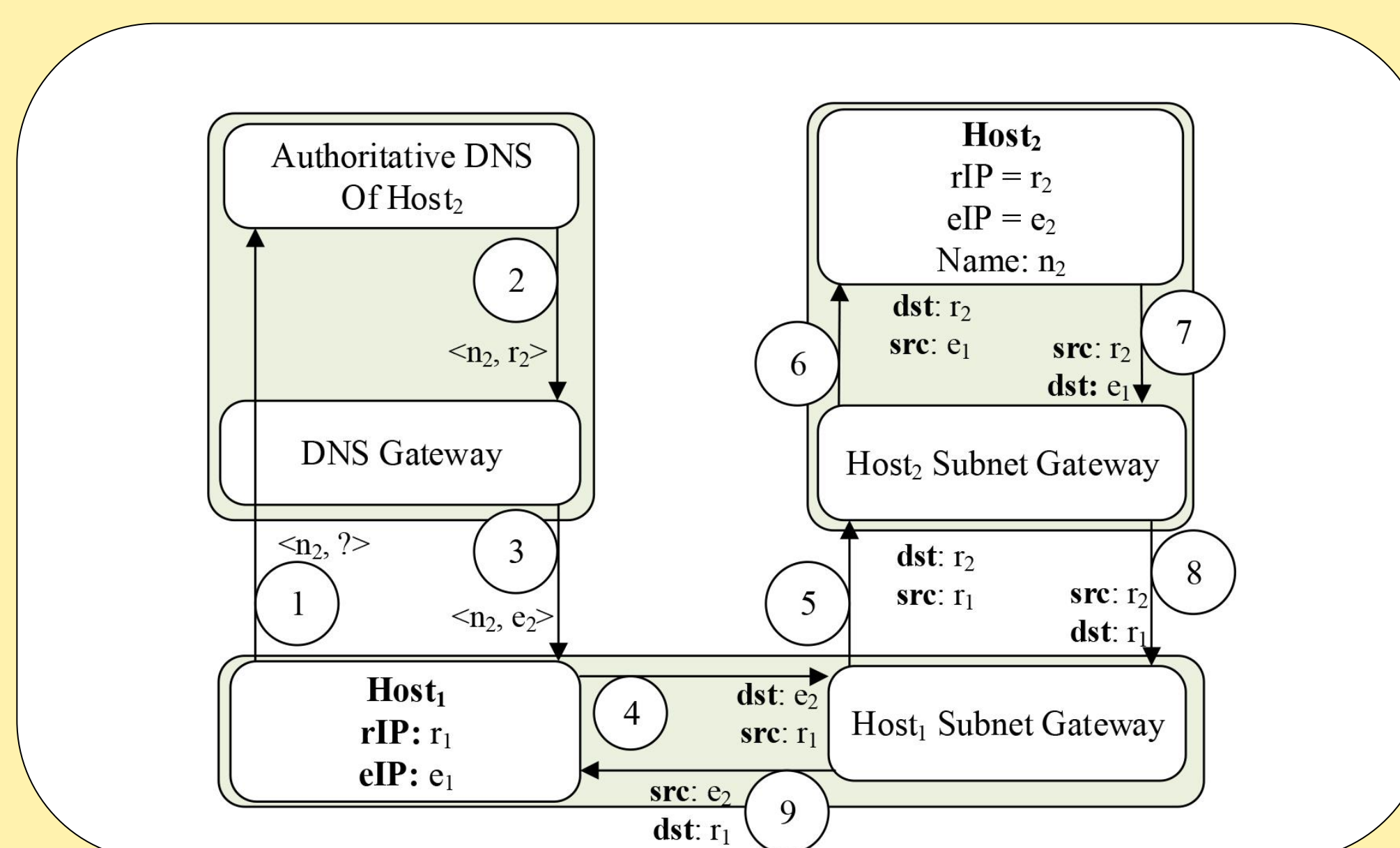
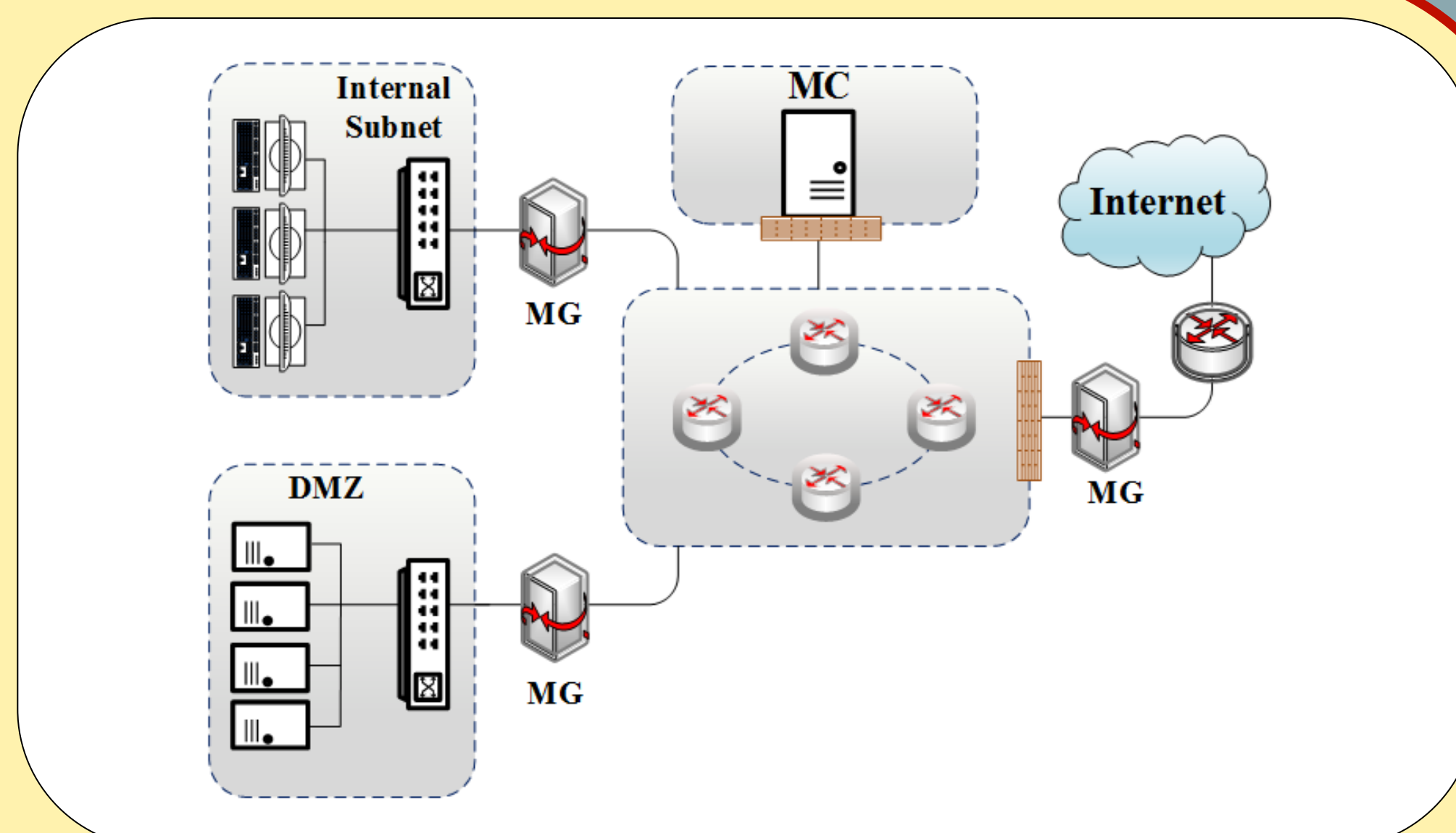
Adversary-aware Host Address Mutation

PIs: Ehab Al-Shaer; Researchers: J. Haadi Jafarian, Qi Duan



Motivation & Objectives

- **Static** and **predictable** behavior of cyber systems a fundamental design **vulnerability**
 - **Reconnaissance** is simple
 - **Evasion** is simple via careful selection of attack parameters
- IP address allocation is mostly **static**
- Several approaches for IP hopping were proposed but they lack effectiveness
 - Based on **DHCP** or **NAT** (DyNAT, NASR): too **infrequent** and **traceable**
 - Uniform mutation limits the effectiveness due to **lack of adaptiveness**
- The goal of adaptive mutation is to **increase benefit**, while **reducing cost**.
- To be adaptive, we must **characterize** adversarial scanning.
- **Ref:** Adversary-aware IP address randomization for proactive agility against sophisticated attackers, IEEE INFOCOM, May 2015.



Approach: - allocating new IPs from address ranges that have **lower risk**

- Observe the sequence of **unsuccessful probes** generated by network hosts
- Use **statistical hypothesis testing** to estimate their **distribution**

Two hypotheses

Non-uniformity: tests if scans are skewed toward certain ranges of address space

Non-repetition: tests if scans are avoiding repeated probing of same IP address

- Changing real IP (rIP) address of hosts disrupts active sessions
Instead, we associate hosts with **ephemeral IP addresses (eIP)**

- Chosen from unused address space
- Automatically translated to/from rIPs at network edges →
 - Not used for routing

- New eIP is announced to clients through **DNS** with short **TTL**

IP addresses are mutated without jeopardizing cyber operation or breaking active sessions

Non-uniformity test

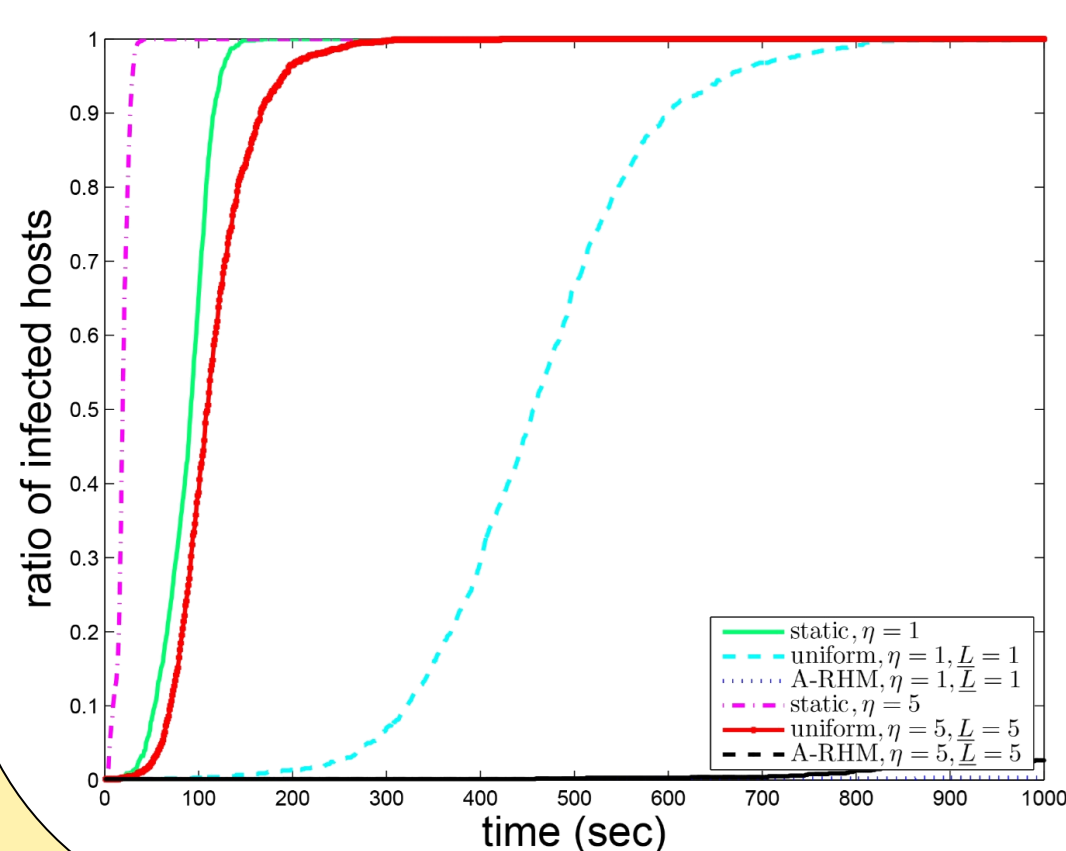
Q1: Are scans **locally concentrated** in specific ranges?

- Increases success rate and decreases detectability
 - e.g. Local-preference, sequential, divide-and-conquer
- Use **Pearson's χ -squared test** to calculate **deviation from uniform distribution** with $p\text{-value} = 0.05$

• If deviation is very high, scans are non-uniform

Q2: If accepted, which ranges are more hazardous?

- Ranges with abnormal number of scans (outliers)



Game-changing

Attacker's worst strategy (uniform scanning) in static networks becomes her best in our adaptive network

If attacker uninformed of adaptive mutation → attack is deterred

If attacker informed of adaptive mutation → forced to do uniform scanning → attack becomes more detectable

Non-repetition test

Q1: Are scanners avoiding/limiting repeated scanning?

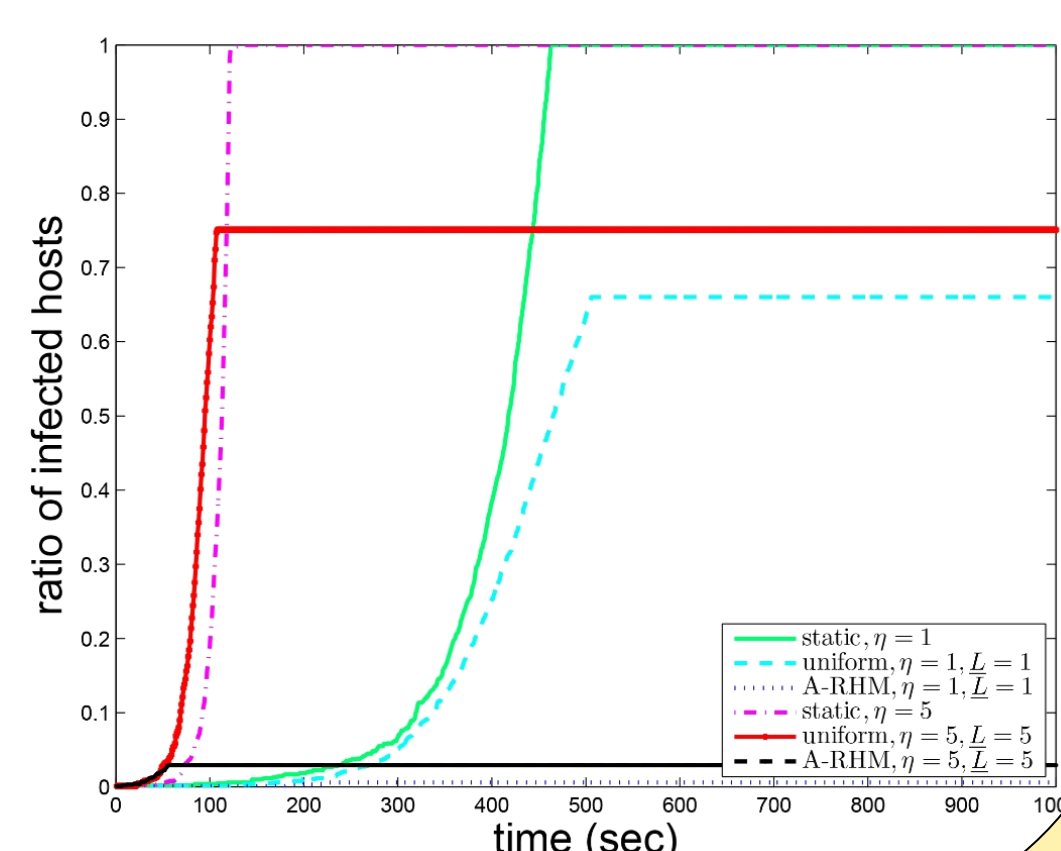
- Reduces detectability and scanning budget
 - e.g. Cooperative, divide-and-conquer

Calculate **standard deviation** of scan distribution

- If deviation is very low, repetition is limited

Q2: if accepted, which addresses are more hazardous?

- Addresses with low num. of scans
- Avoid using these addresses as eIPs



Interested in meeting the PIs? Attach post-it note below!



National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

