CERIAS
The Center for Education and Research in Information Assurance and Security

PURDUE
UNIVERSITY

Create Moving Target Defense in Static Networks by Learning from Botnets

Feng Li, Assistant Professor, fengli@iupui.edu

Moving-Target Defense

This project will deliver an moving-target defense (MTD) framework, in which the network configuration constantly evolves to confuse attackers without significantly degrading the quality of service. The MTD framework increases the cost for potential attackers by complicating the attack process and limiting the exposure of network vulnerability, and thus makes the network more resilient against persistent attacks.

MTD Framwork: Against disruptive attacks

Roadmap:
Physically static networks ← Targets of disruptive attacks
↑ Moving-target techniques ← Success of recent botnets

Three major thrusts:

- **Polymorphism:** evolving network topology
- **Agility:** security-context-aware opportunistic data exchange
- **Poisoning prevention:** dynamic group creation and secret sharing

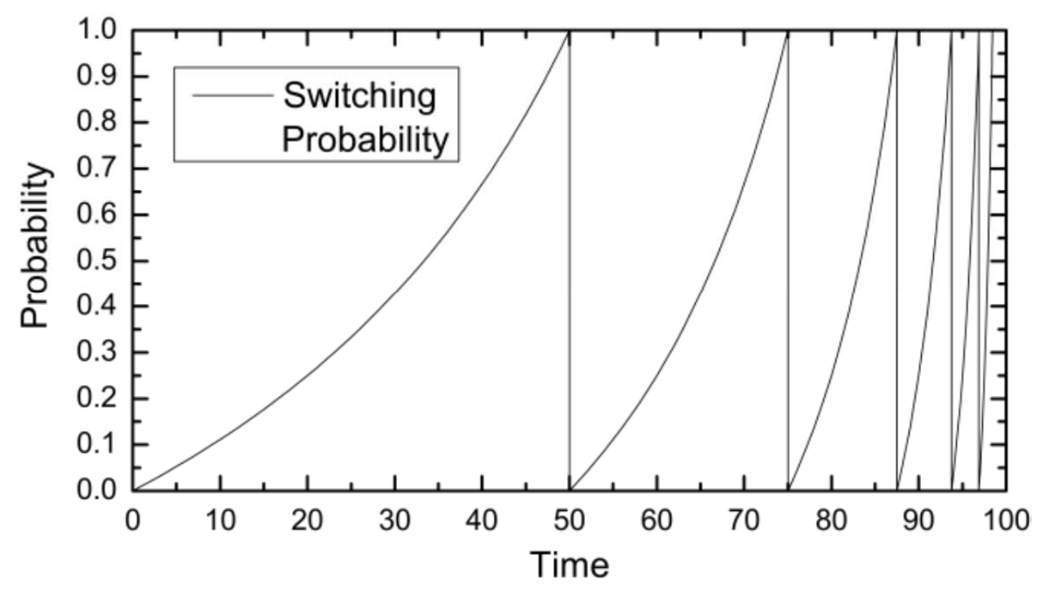
Polymorphism

Dynamic C&C structure inspires network topological polymorphism

Quantitative security exposure measurement

- Attack exposure measure: accumulated risk of being compromised over time

Globally coordinated mechanisms
Locally coordinated virtual node mechanism
Locally coordinated probabilistic switching mechanism



$$p_{switch} = \begin{cases} 1 - \frac{\overline{E_{N[i]}}}{E_i} & \text{if } \overline{E_{N[i]}} \leq E_i \\ 0 & \text{otherwise} \end{cases}$$

Botnet Lesson

Example: Operation Ghost Click

- A botnet with millions of infected computers
- Crackdown by FBI

Why? Static target.

- Centralized Command and Control (C&C) architecture
- Poisoning attack by FBI

Anti-crackdown? Trojan.Peacomm botnet and Storm worm [1].

1) Dynamic C&C mechanisms;
2) Multiple attack vectors and the strategy of using them;
3) Disruption-tolerant P2P update sharing;
4) Index poisoning prevention .

Poisoning prevention

Poisoning techniques: A severe threat to the MTD framework

Arbitrary subset of nodes → a privileged subgroup
No online central authority

Dynamic secret sharing mechanism based on private polynomial and public values

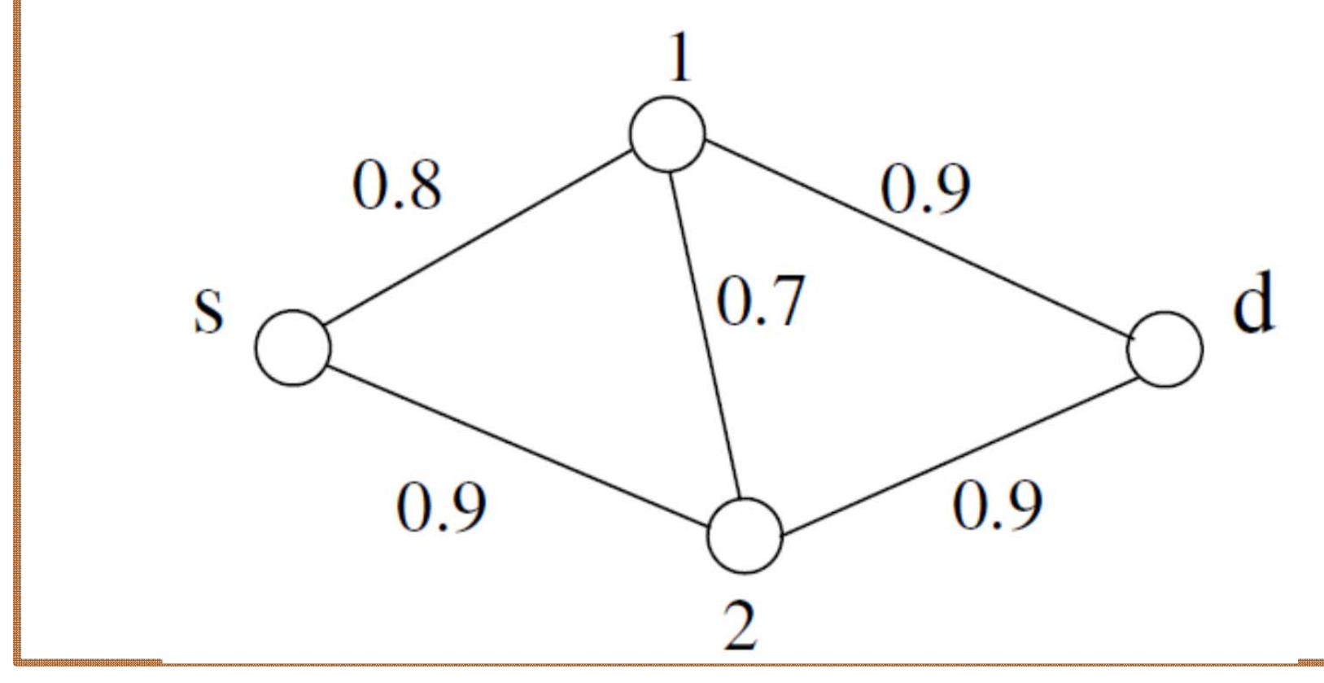
Agility

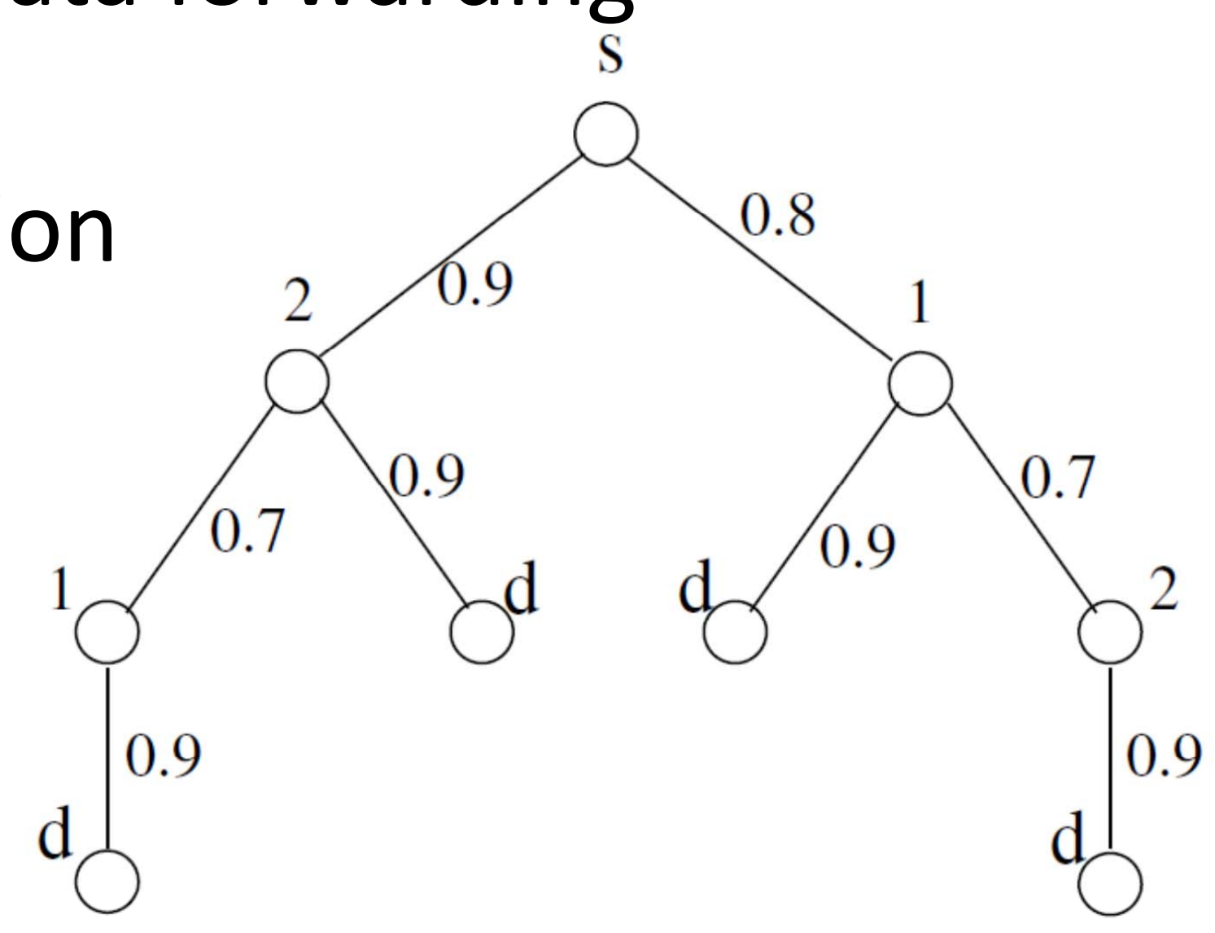
Links are still vulnerable to the network disruptive attacks

- Single fixed route

Locally coordinated opportunistic data forwarding

- Adaptive relay set selection
- Probabilistic priority determination





Botnet Lesson

[1] T. Holz, M. Steiner, F. Dahl, E. Biersack, and F. Freiling. Measurements and mitigation of peer-to-peer-based botnets: a case study on storm worm. In *Proc. of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats*, 2008.

[2] E. Al-Shaer. Toward network configuration randomization for moving target defense. In *Moving Target Defense*, volume 54 of *Advances in Information Security*, pages 153–159. Springer New York, 2011.

CERIAS®

Discovery Park
e-Enterprise Center