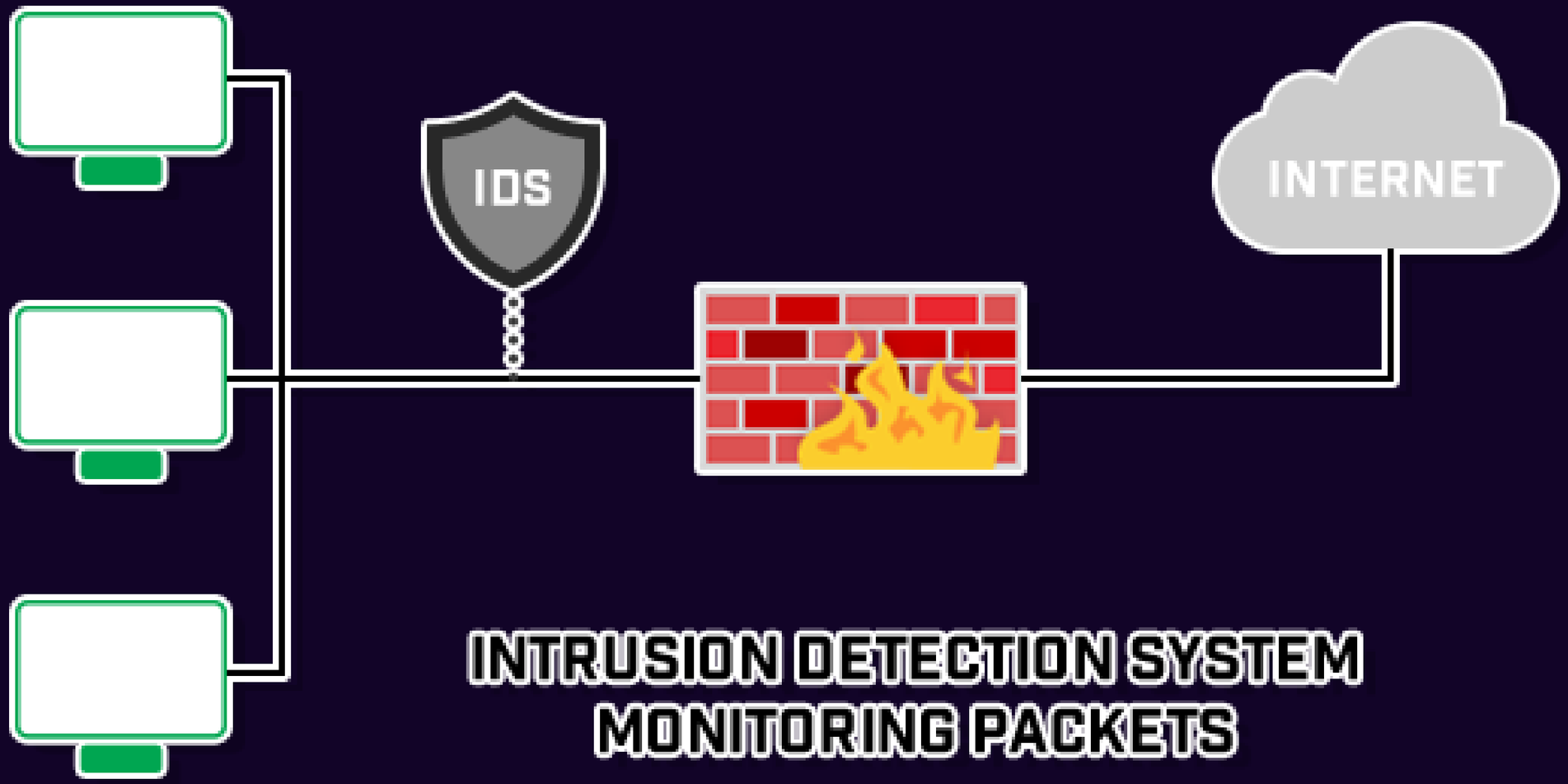
NETWORK INTRUSION DETECTION USING GAME THEORY

Securing Your Digital World

dr. narimani
parniyan malekzadeh

What is IDS?

A network security technology originally built for detecting vulnerability exploits against a target application or computer.



INTRUSION DETECTION SYSTEM
MONITORING PACKETS

Network Model & Assumptions

1. The network is modeled as a graph G = (N, E)
2. attack is divided into multiple fragments
3. reach the target without being detected
4. IDS uses sampling to detect attack fragments

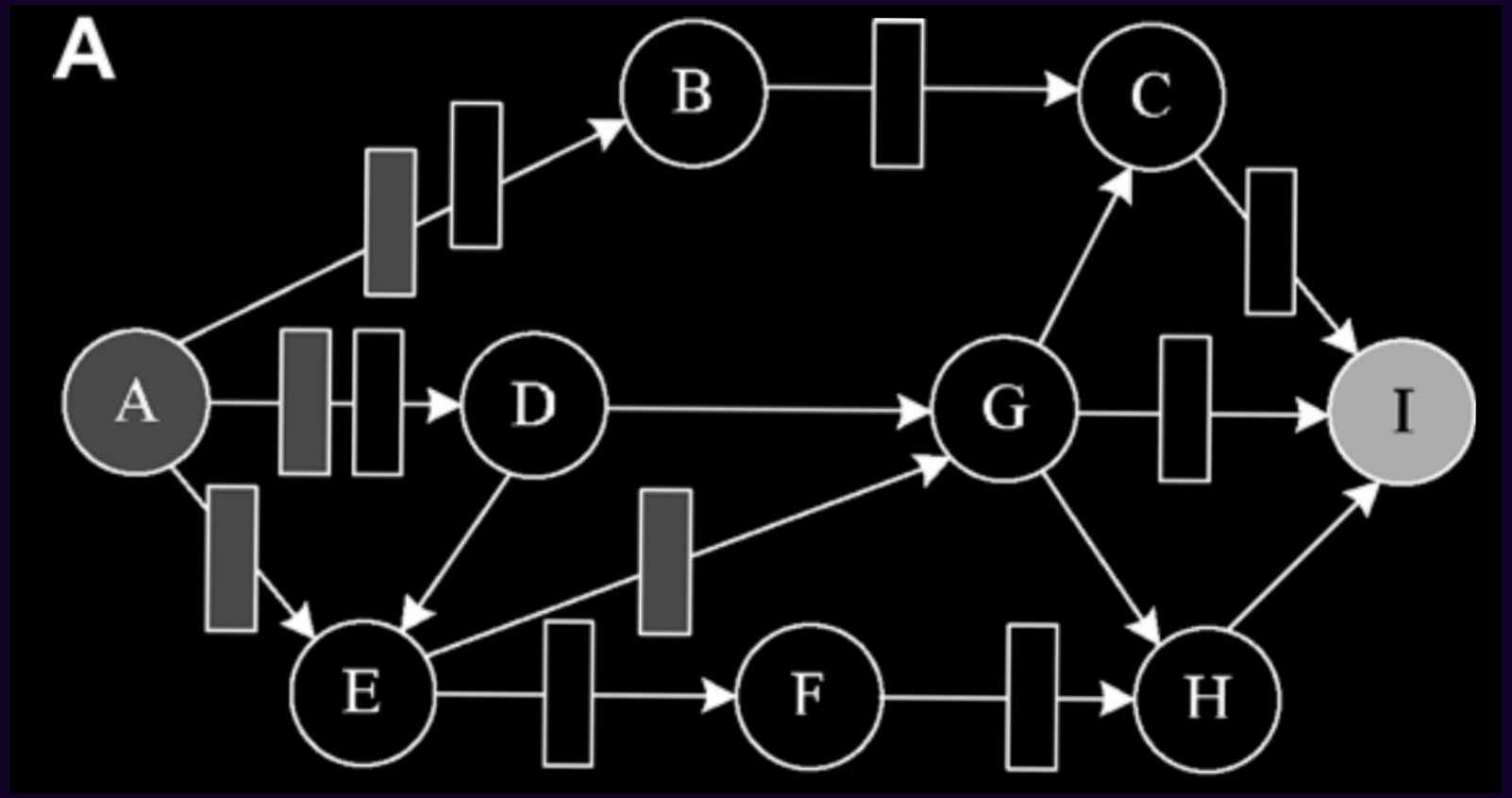
Scenario I Single intruder

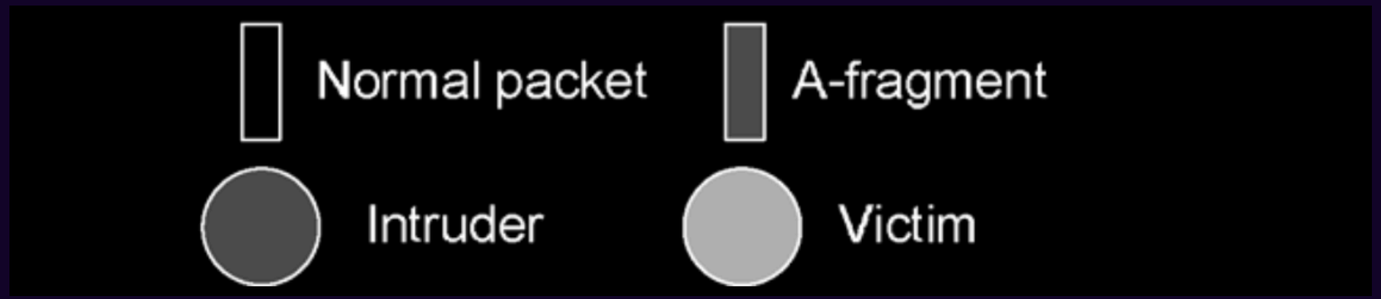
1. The attacker splits the attack into multiple fragments
2. Each fragment is sent through a different path to avoid detection
3. at least m out of n fragments are needed to detect an intrusion

Scenario I Single intruder

4 zero-sum two-player game with

5 complete information about the players


A
B
C
A
D
G
I
E
F
H


Normal packet
A-fragment
Intruder
Victim

Game constraints

IDS has a sampling budget

$$\sum_{e \in E} S_e \leqslant B_s$$

Strategies for the two players

Intruder

$$q_x = (q(P_{1_x}), \ldots, q(P_{z_x}))$$

$$\sum_{P \in p_a^t} q(P) = 1$$

IDS

choose the sampling rate

$$\sum_{e \in E} S_e \leqslant B_s$$

Game formulation

$$\theta = \max_{p \in U} \min_{n \in \mathbb{N}, q \in V} \sum_{i=m}^{n} \alpha^i \times (1-\alpha)^{n-i}$$

$$= \min_{n \in \mathbb{N}, q \in V} \max_{p \in U} \sum_{i=m}^{n} \alpha^i \times (1-\alpha)^{n-i},$$

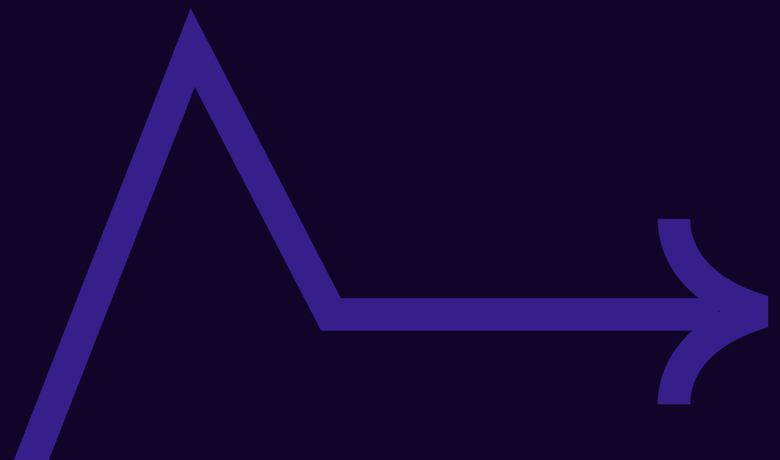
equilibrium

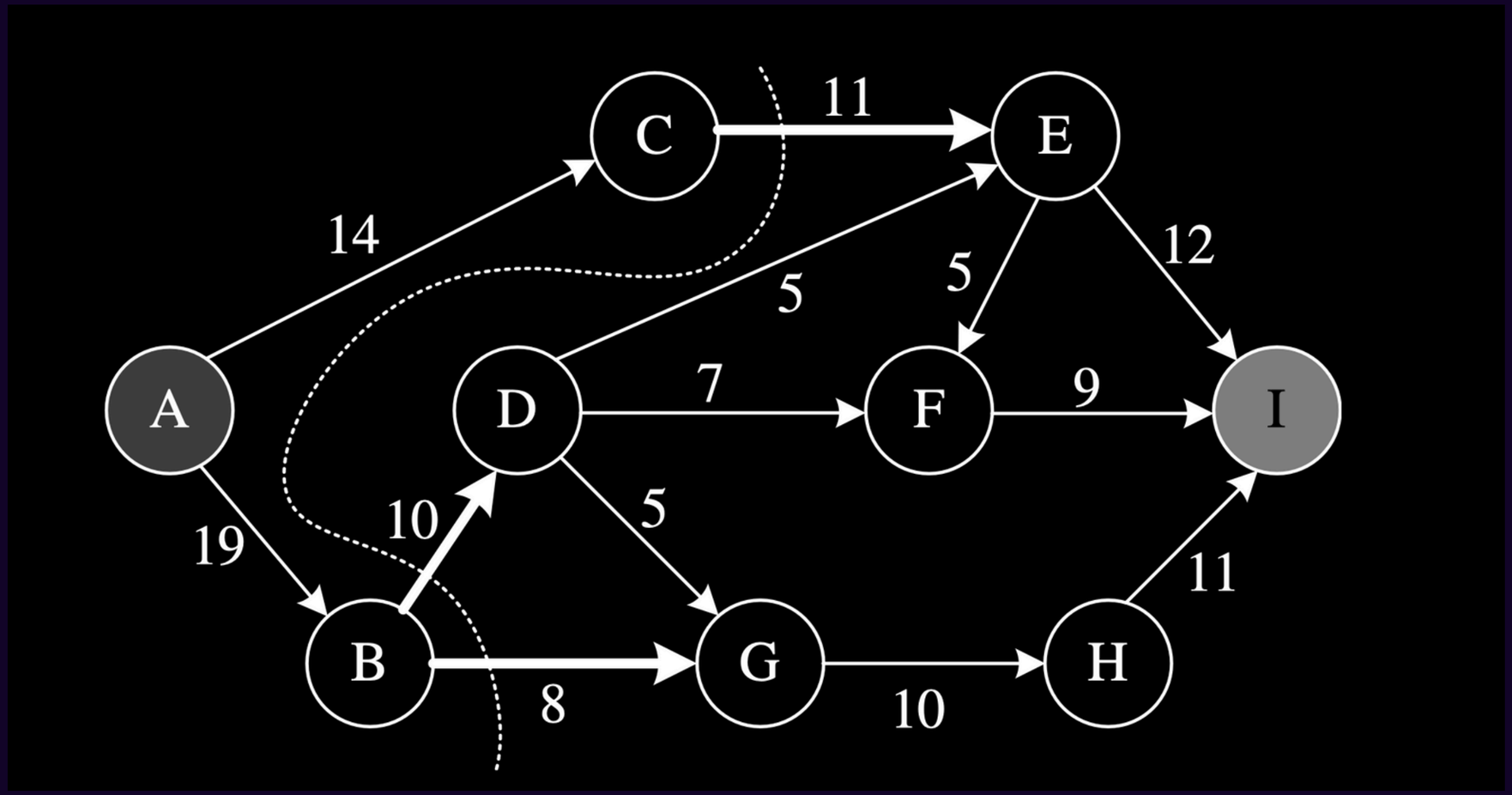
- Flow decomposition for the intruder for each path:

$$m_i MF_a^t(f)^{-1}$$

- Minimum cut and sampling rate allocation for the IDS

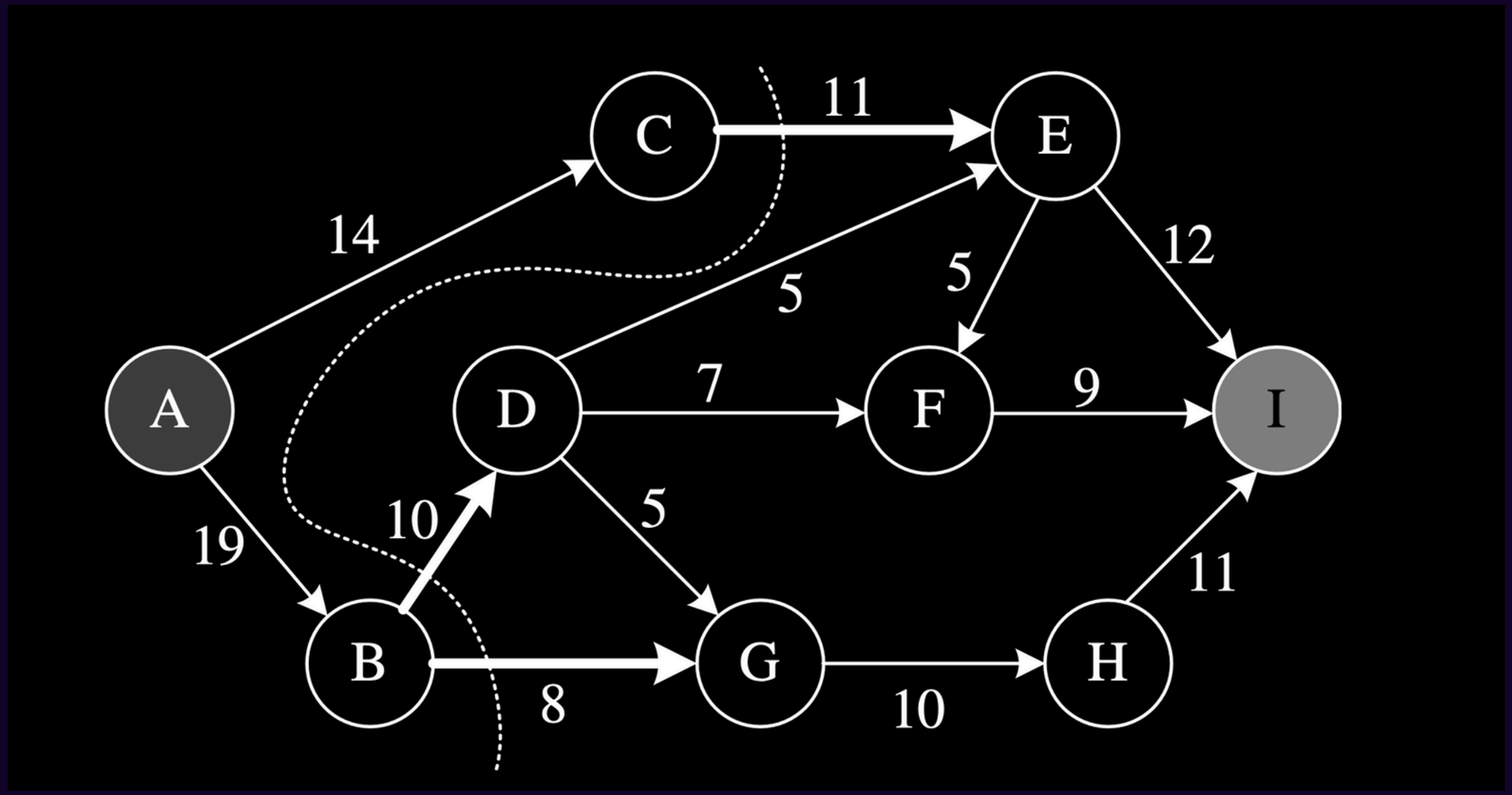
$$B_s f_e MF_a^t(f)^{-1}$$





Intruder :

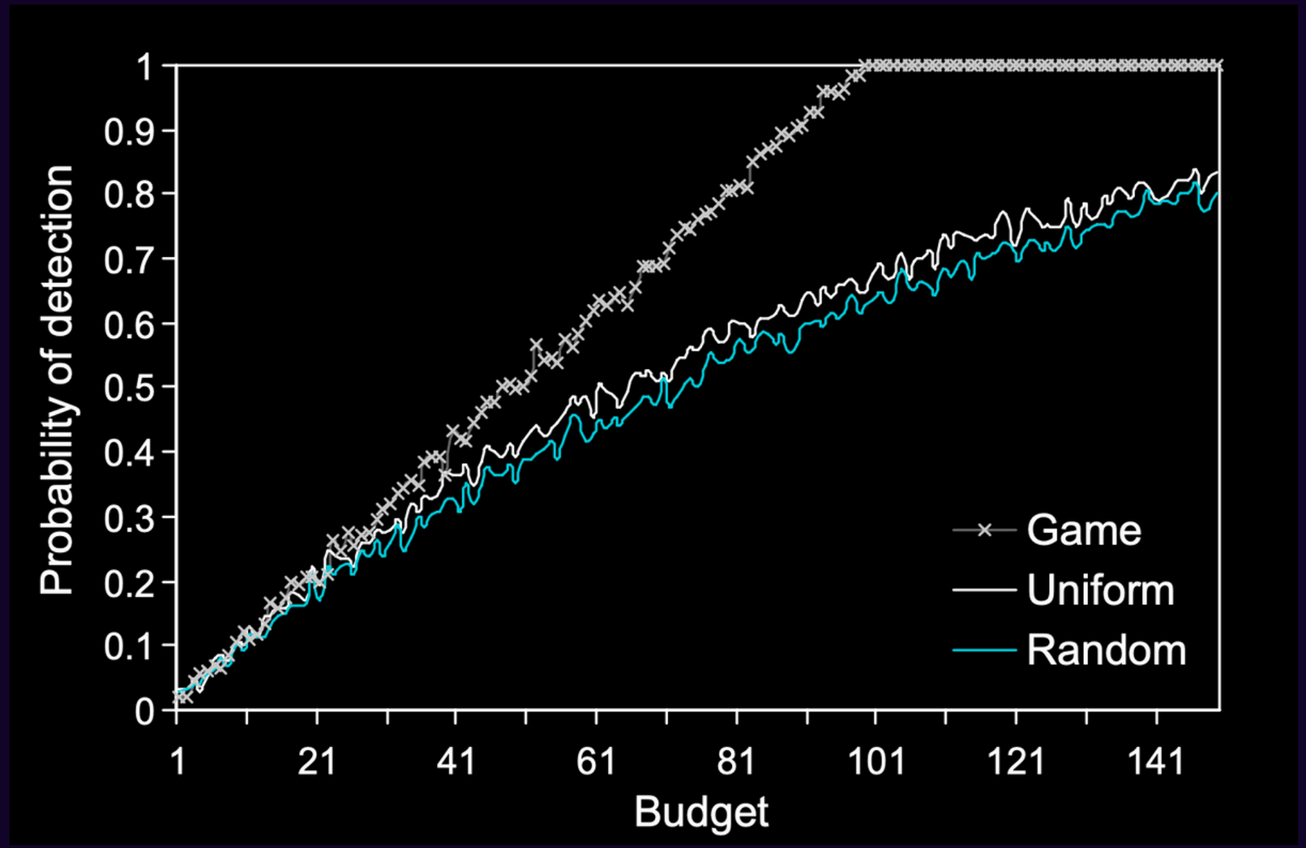
- Transmit the malicious fragment along the path A–C– E–I with probability 11/29
- Transmit the malicious fragment along the path A–B– G–H–I with probability 8/29



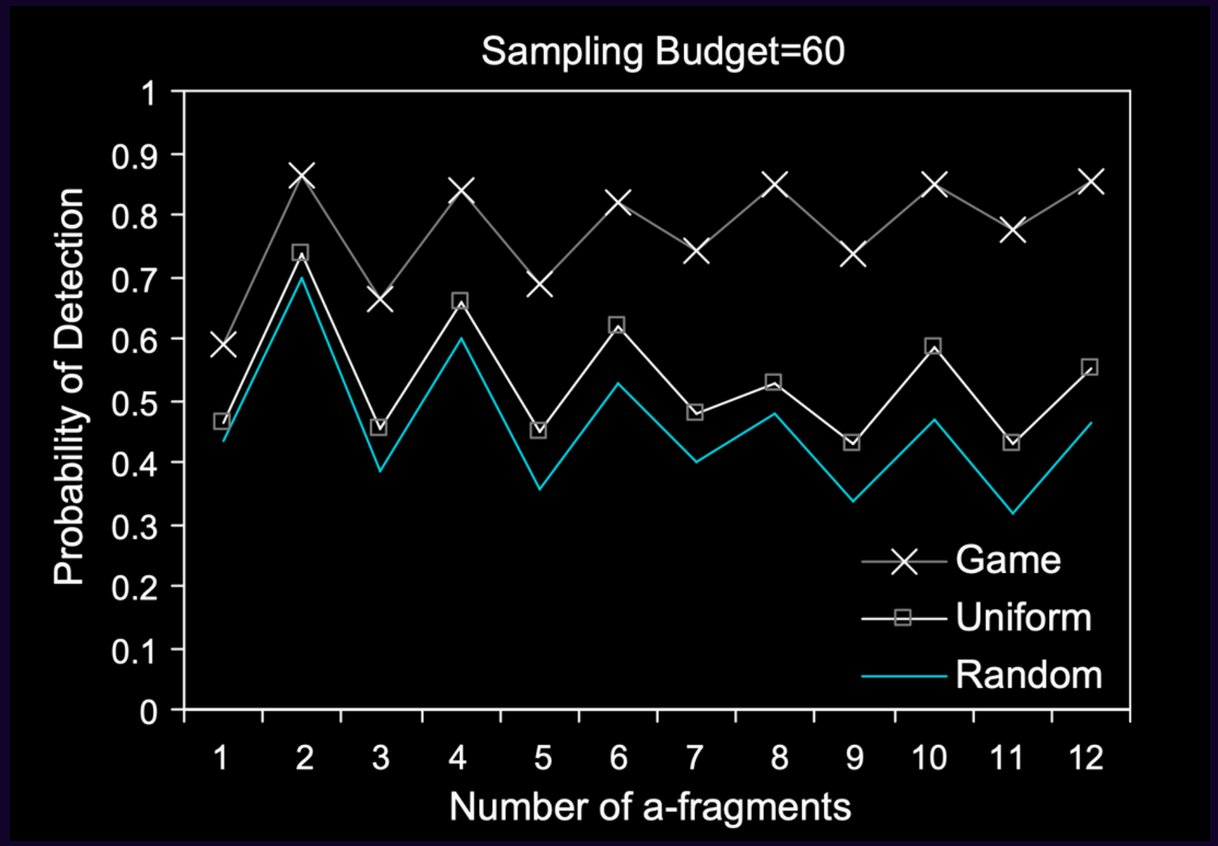
IDS :

- Sample link (C,E) with sampling rate = (12 x 11) /29
- Sample link (B,G) with sampling rate = (12 x 8) /29
- Sample link (B,D) with sampling rate = (12 x 10) /29

Numerical resaults



NUMERICAL RESAULTS



Reference

Otrok, H., Mehrandish, M., Assi, C., Debbabi, M., & Bhattacharya, P. "Game Theoretic Models for Detecting Network Intrusions."

ANY QUESTIONS?