# Too Many Cooks

## Analysis of Mix Network Behavior Against Multiple Adversaries

J David Smith

# Problem Statement

One Mix Network

Multiple GA Attackers $\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots \in A, |A| > 1$

Attackers are oblivious $\forall \mathcal{A}, \mathcal{B} \in A : \mathcal{A}$ has no knowledge of $\mathcal{B}$

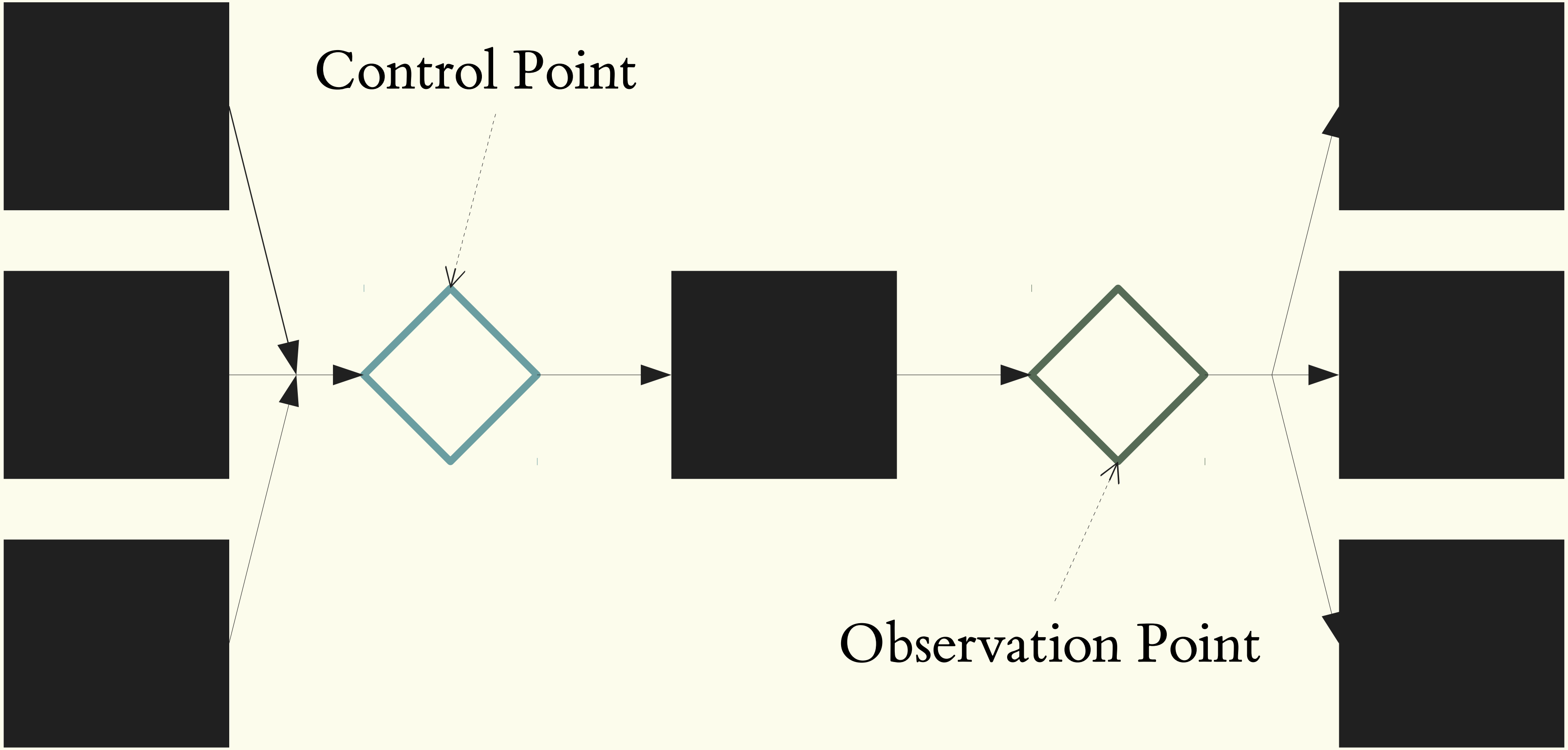
Question: How effective are the attackers?

# Problem Statement

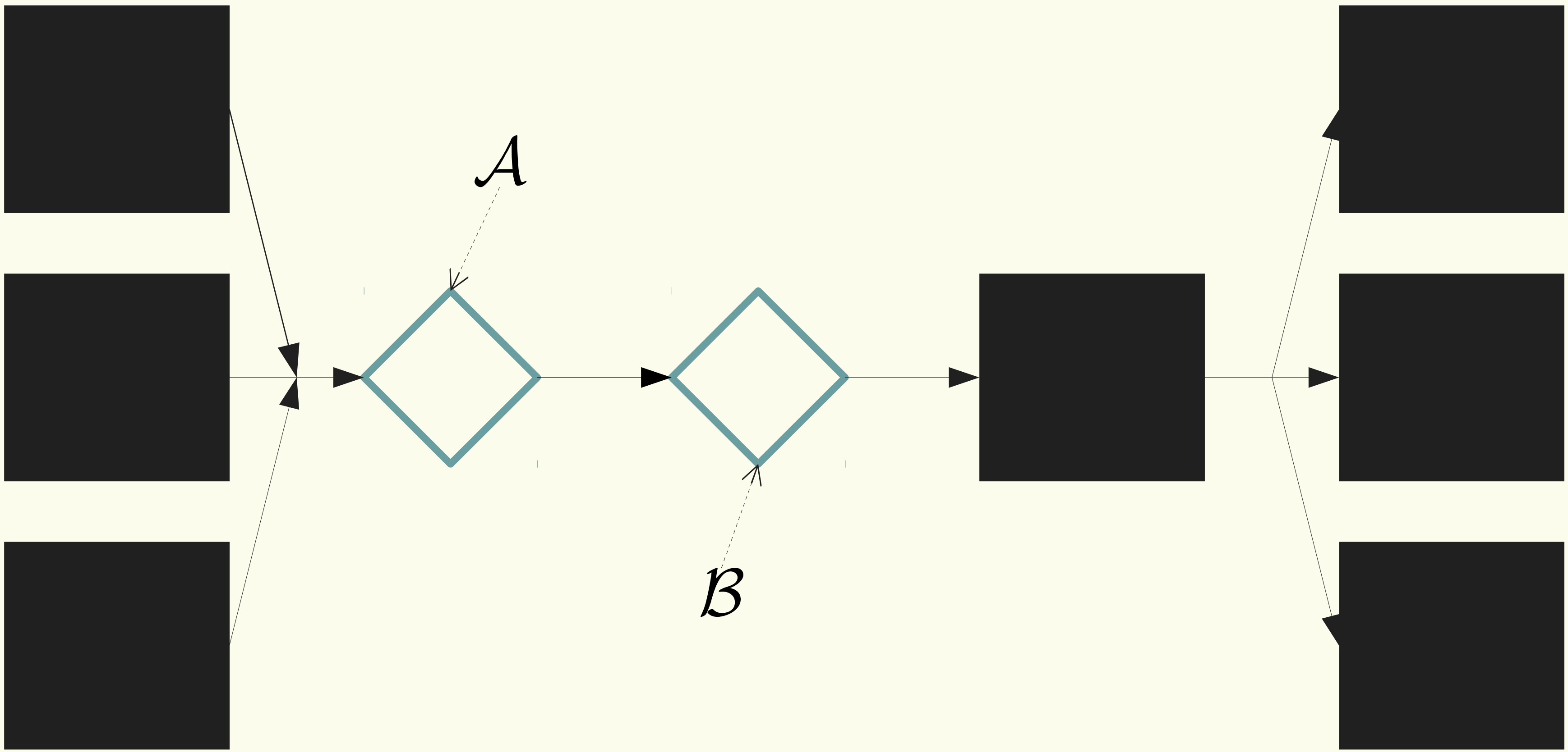
Answer: It depends.

Let's look at the Flooding attack.

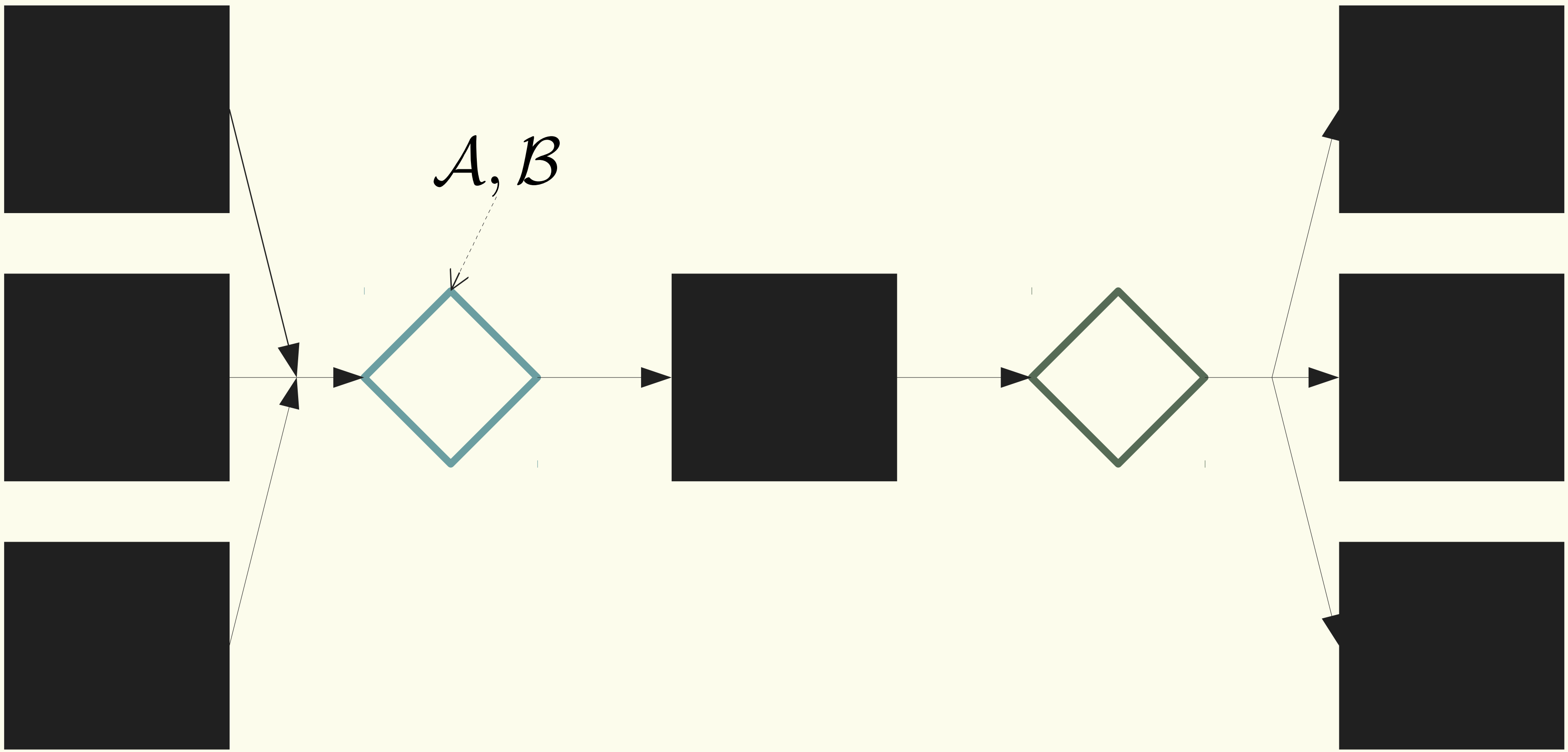
# Basic Construction



# Scenario: Multiple Control Points



# Scenario: Colocation



# What is Success?

Intuitively: Success is when a single adversary knows all messages received by the target mix.

But that's binary. What about degrees of success?

Formally: Success is when a single adversary has reduced the effective anonymity set size of the target to 1.

# What is Success?

$$\Pr\left(\mathcal{A} \text{ is succesful}\right) = \Pr\left(\mathcal{A} \text{ sent } n-1 \text{ messages before } \mathcal{B} \text{ sent } 1\right)$$

Suppose at time $t$ each adversary $\mathcal{A}$ has probability $p_{\mathcal{A}}$ of sending a message. Then

$$\Pr\left(\mathcal{A} \text{ is successful}\right) = p_{\mathcal{A}}^{n-1}$$

# What about Partial Success?

Want: Probability distribution over number of messages $\mathcal{A}$ sent before $n-1$ messages were sent.

# What about Partial Success?

Solution: Binomial Theorem

$$\sum_{k=0}^{n-1} \binom{n-1}{k} p_{\mathcal{A}}^{k} p_{\mathcal{B}}^{n-1-k}$$

Specifically: each term of the binomial represents a the probability of a $\mathcal{A}$ sending $k$ messages

# Expected Anonymity Set Size (EAS)

From the persepective of $\mathcal{A}$

| $n-1$ | $p_{\mathcal{A}}$ | $p_{\mathcal{B}}$ | EAS |
|---|---|---|---|
| 10 | 0.5 | 0.5 | 1.89 |
| 10 | 0.2 | 0.8 | 2.21 |
| 10 | 0.05 | 0.95 | 2.29 |
| 50 | 0.5 | 0.5 | 3.34 |
| 100 | 0.5 | 0.5 | 4.00 |
| 100 | 0.2 | 0.8 | 4.43 |

# Generalizing to More Adversaries

**Conjecture**

The probability distribution of this model satisfies the multinomial theorem:

$$\sum_{k_1+k_2+\ldots+k_m=n} \binom{n}{k_1, k_2, \ldots, k_m} \prod_{1\leq t\leq m} x_t^{k_t}$$

# Markov Chains

A Markov Chain is a finite sequence of states drawn from a finite space such that

$$\forall Z : \Pr(X, Y) = \Pr(X, Y, Z)$$

# Modelling with Markov Chains

Initial State $\quad q_0 = (0, \ldots, 0)$

Transition Probability

$$\Pr\left((a, \ldots, m+1, \ldots), (a, \ldots, m, \ldots)\right) = \begin{cases} \sum k < n-1 & p_m \\ \sum k \geq n-1 \wedge A = B & 1 \\ \text{else} & 0 \end{cases}$$

If we write out the transition matrix, then the stationary distribution satisfies

$$\pi = \pi P$$

# Expected Anonymity Set Size (EAS)

From the persepective of $\mathcal{A}$

| $n-1$ | $p_{\mathcal{A}}$ | $p_{\mathcal{B}}$ | $p_{\mathcal{C}}$ | EAS |
|---|---|---|---|---|
| 10 | 0.33 | 0.33 | 0.33 | 2.09 |
| 10 | 0.2 | 0.5 | 0.3 | 2.21 |
| 10 | 0.05 | 0.8 | 0.15 | 2.29 |
| 50 | 0.33 | 0.33 | 0.33 | 3.59 |
| 100 | 0.33 | 0.33 | 0.33 | 4.26 |
| 100 | 0.2 | 0.5 | 0.3 | 4.43 |

# Generalizing the Markov Chain Model

By changing the transition function, we can model different behaviors. For example:

$$\Pr\left((a, \ldots, m+1, \ldots), (a, \ldots, m, \ldots)\right) = \begin{cases} m < n-1 & p_m \\ m \geq n-1 \land A = B & 1 \\ \text{else} & 0 \end{cases}$$

# Questions?