Vuvuzela

Jelle van den Hooff, David Lazar, Matei Zaharia, and Nickolai Zeldovich
~ MIT CSAIL ~

Presentation by: Alexander Gaidis

Goal?

Prevent an adversary from learning information about a single individual

How?

Identify and minimize the number of observable variables and then obfuscate these with differential privacy.

Outline

Pathway to Metadata Anonymous Communication

Dialing Protocol

Threat Model Recap & Analysis

Results

Discussion

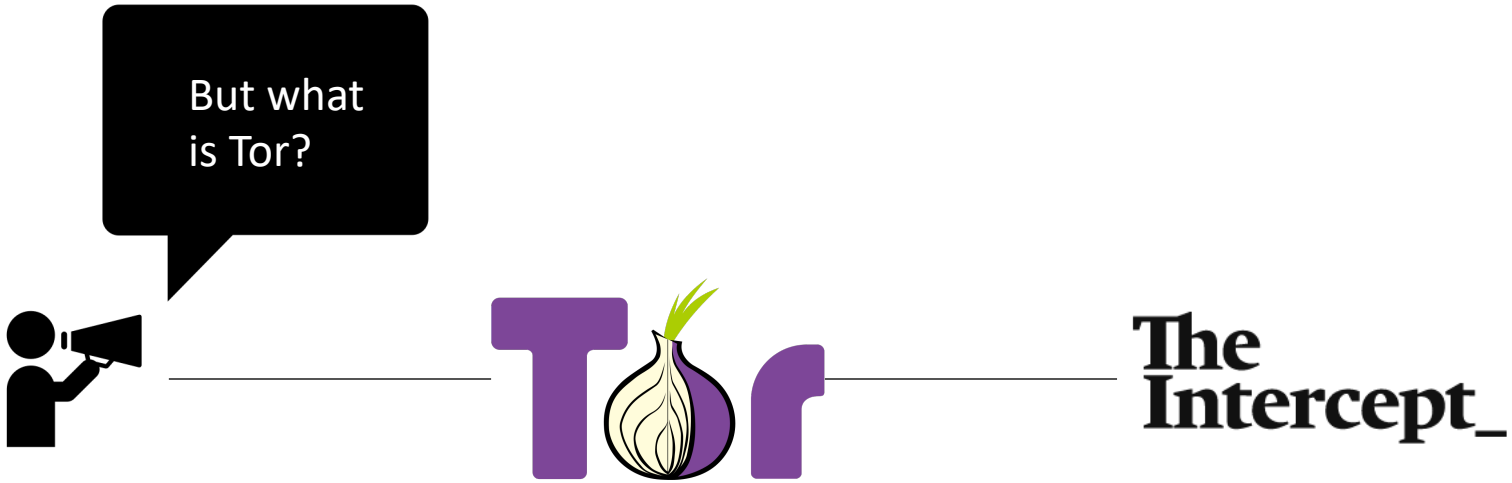
Pathway to Metadata Private Communication

Problem Setup

The Intercept_

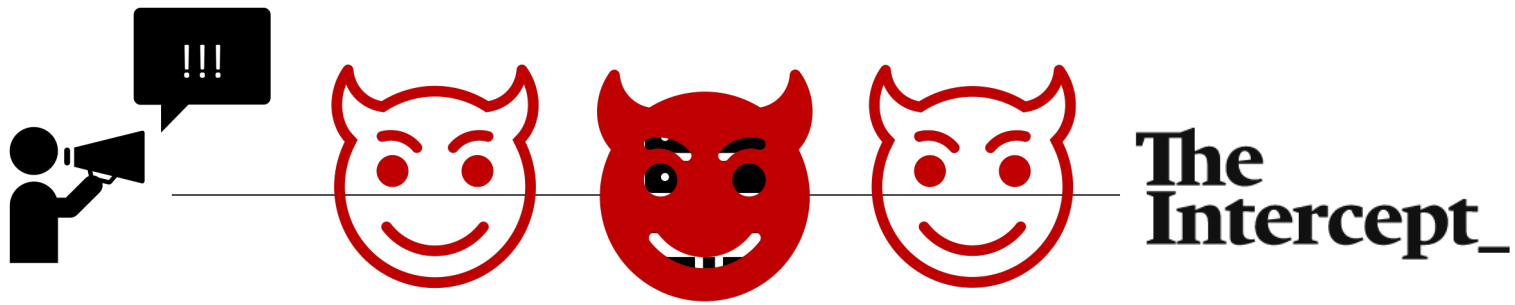
Pathway to Metadata Private Communication

Tor is in style! Let’s use it!



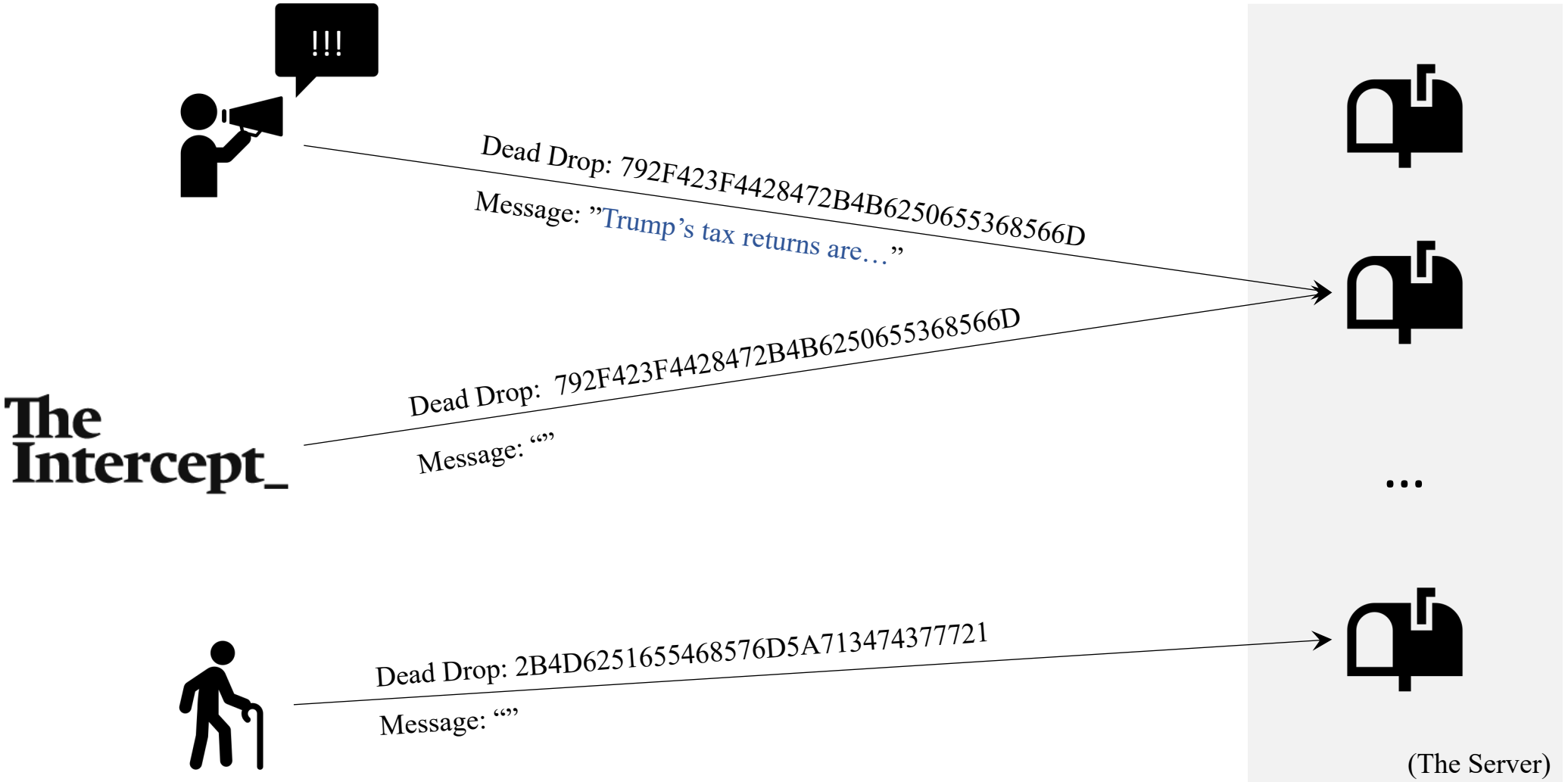
Pathway to Metadata Private Communication

Attempt #1: Single Server



Pathway to Metadata Private Communication

Attempt #2: Dead Drops



ROUND 1

Pathway to Metadata Private Communication

Attempt #2: Dead Drops

ROUND 1

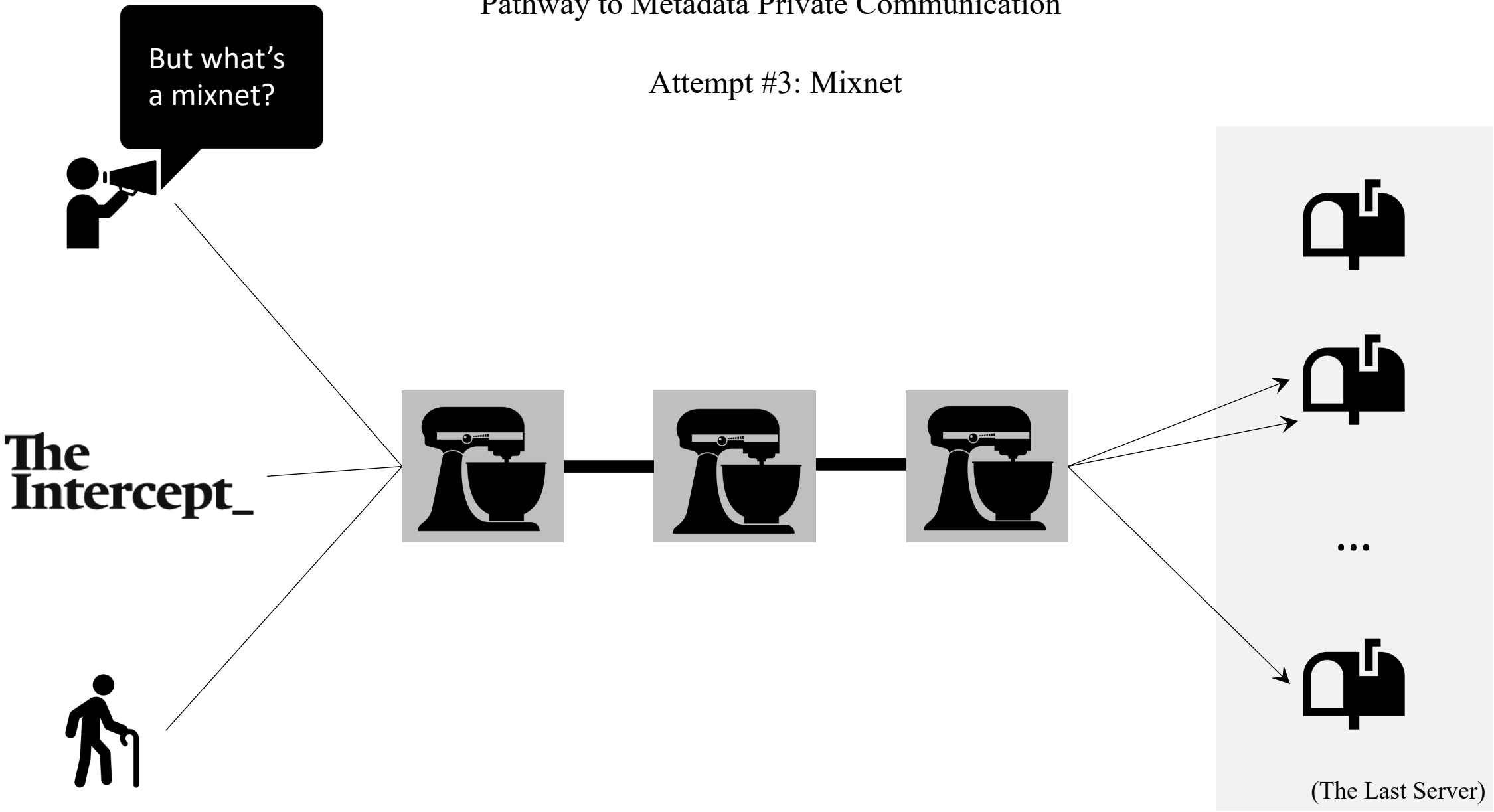
Pathway to Metadata Private Communication

Attempt #2: Dead Drops

ROUND 1

Pathway to Metadata Private Communication

Attempt #3: Mixnet



Pathway to Metadata Private Communication

Attempt #4: Noise

Pathway to Metadata Private Communication

Attempt #4: Noise

Let d_2 = # dead drops with two accesses in a single round. Then,

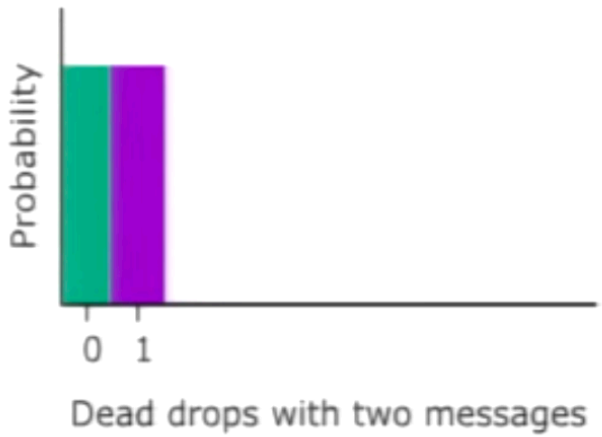
$$\Pr[d_2 = x \mid \textit{Alice talked to Bob}] \approx \Pr[d_2 = x \mid \textit{Alice did not talk to Bob}]$$

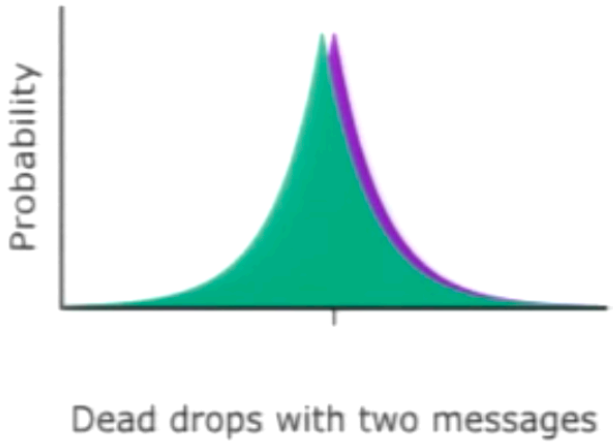
Pathway to Metadata Private Communication

Attempt #4: Noise

We achieve differential privacy through the addition of noise.

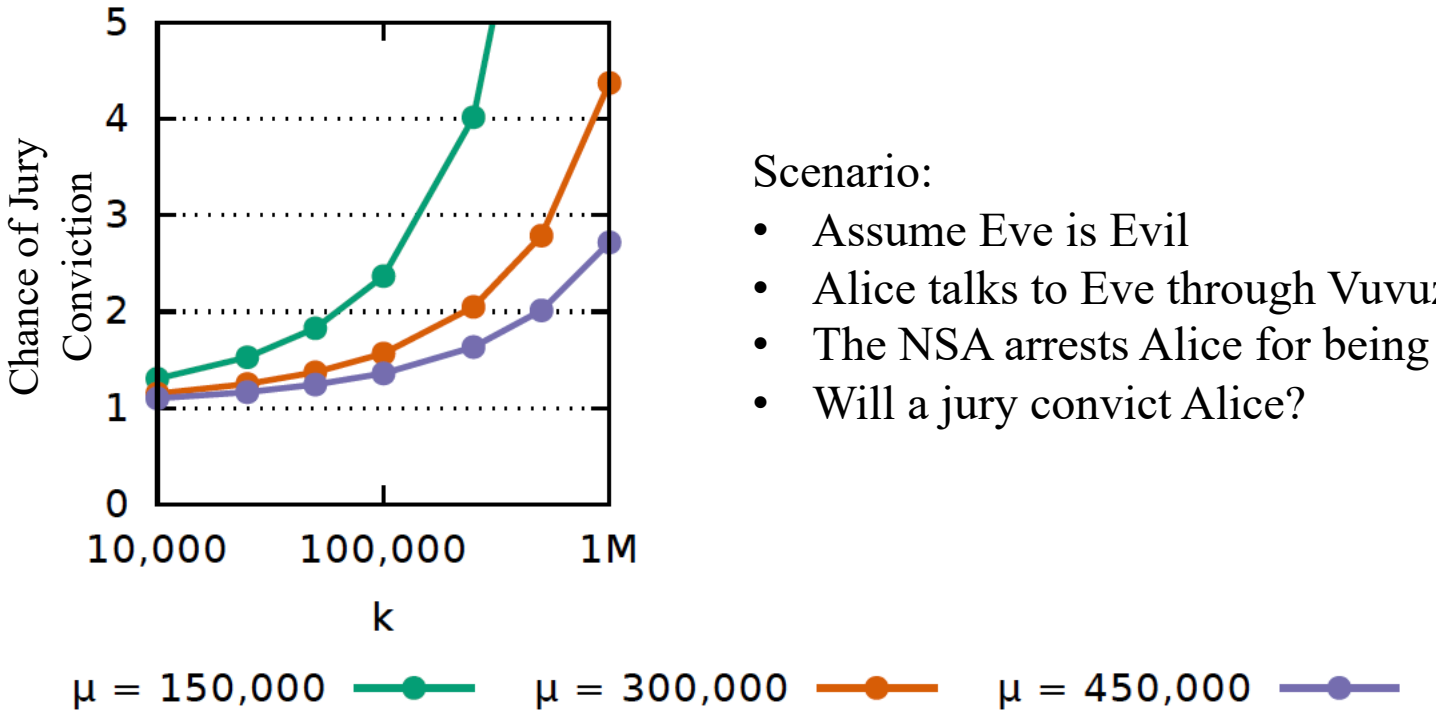
$$\Pr[d_2 = x \mid \textit{Alice talked to Bob}] \approx \Pr[d_2 = x \mid \textit{Alice did not talk to Bob}]$$





Pathway to Metadata Private Communication

Attempt #4: Noise



Scenario:

- Assume Eve is Evil
- Alice talks to Eve through Vuvuzela
- The NSA arrests Alice for being an accomplice to Eve
- Will a jury convict Alice?

Walkthrough of the Full System

Outline

Pathway to Metadata Anonymous Communication

Dialing Protocol

Threat Model Recap & Analysis

Results

Discussion

The Last Piece: The Dialing Protocol

Communication Protocol	Dialing Protocol
Conversation Dead Drops	Invitation Dead Drops (much larger)
Conversation Round < 1 Minute	Dialing Round = 10 Minutes
1 Message = 240 Bytes	Invitation Download = Variable Size
Responses Travel through Mixnet	Invitations Downloaded Directly

Outline

Pathway to Metadata Anonymous Communication

Dialing Protocol

Threat Model Recap & Analysis

Results

Discussion

Goal Reminder:
Prevent an adversary from learning information about a single individual

Threat Model

- N – 1 Servers Compromised
- Complete Network Surveillance
- X Sybil Clients
- Interference over Multiple Rounds

Trust Model

- 1 Honest Server
- You and Your Friend are Honest
- Honest Client/Server Runs Bug-Free Code

Outline

Pathway to Metadata Anonymous Communication

Dialing Protocol

Threat Model Recap

Results

Discussion

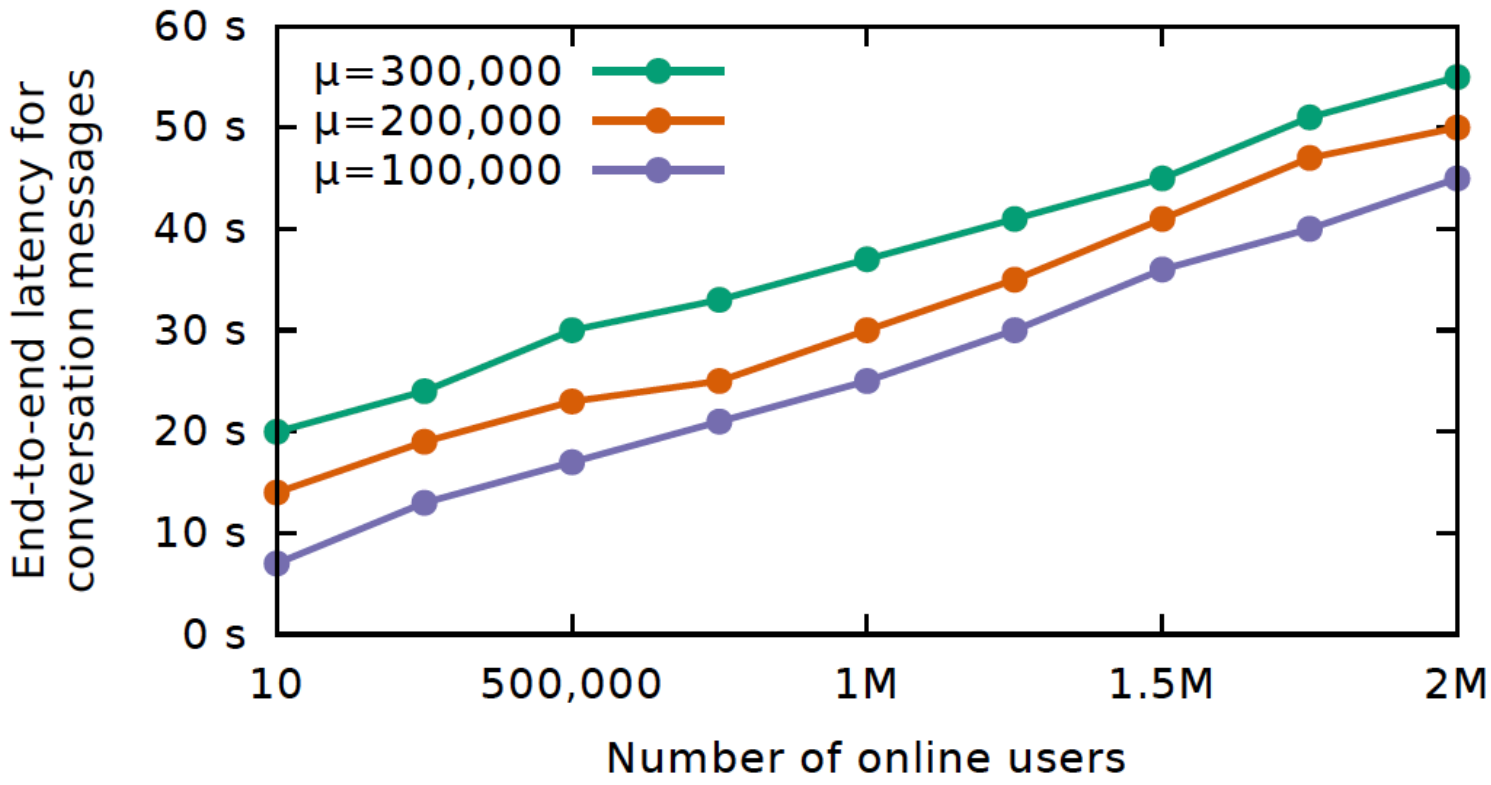


Figure 9: Performance of Vuvuzela's conversation protocol when varying the number of users online. Every user sends a message every round.

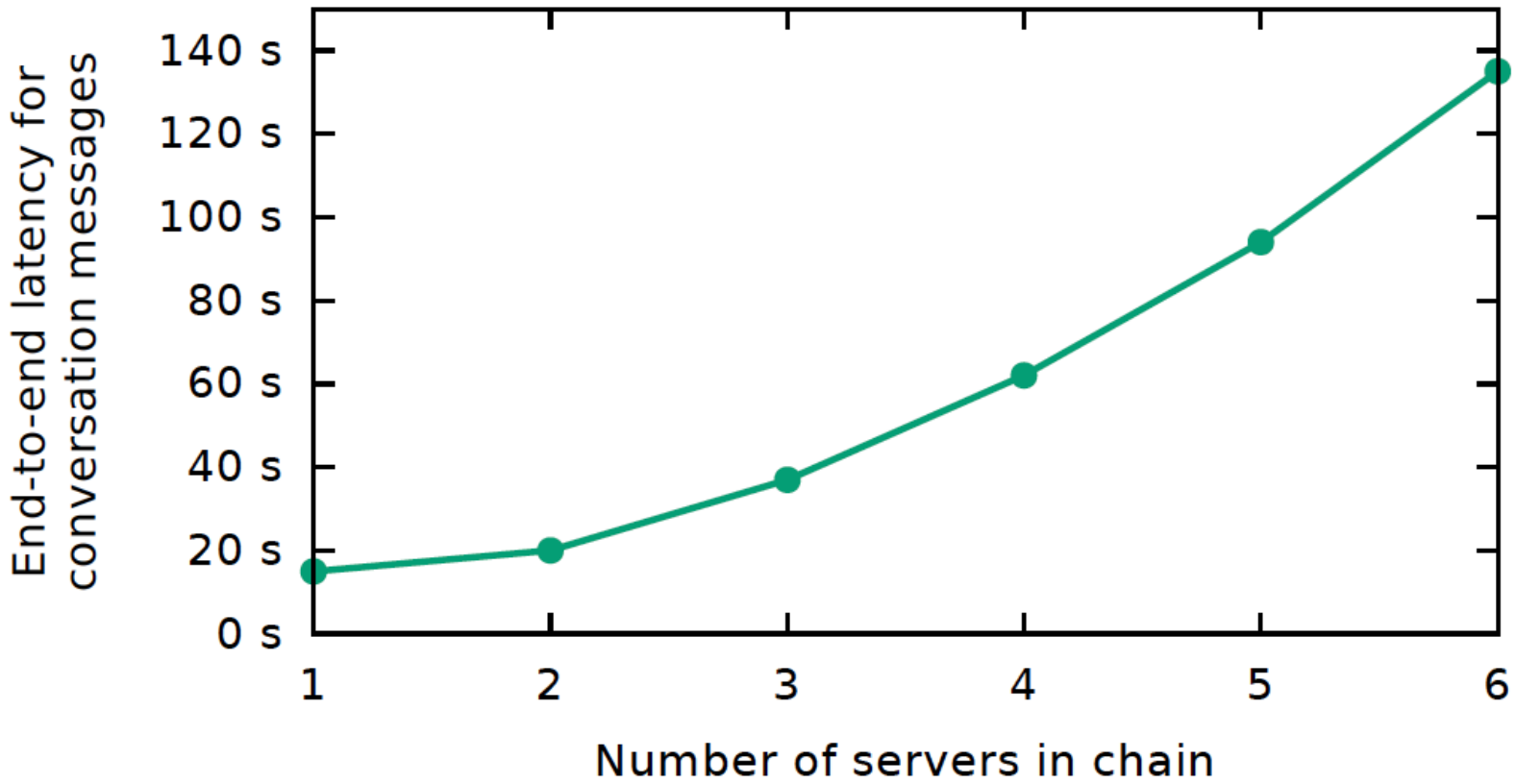
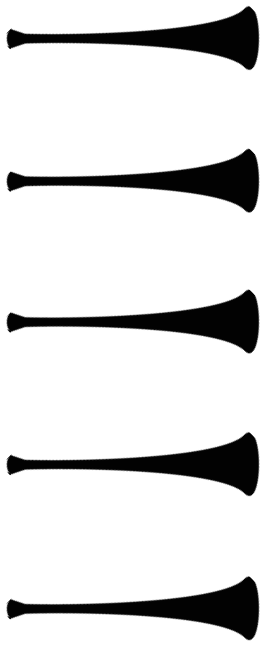


Figure 11: Performance of Vuvuzela's conversation protocol when varying the number of servers with 1 million active users and μ=300,000.

Results

Pros	Cons
Constant bandwidth cost for client (in convo protocol)	Dialing protocol is expensive for clients
Protection against a strong adversary	Dialing protocol is not forwardly secret
System can be abstracted, leaving a clean messaging UI	Bandwidth cost incurred by servers
More users = more traffic = more privacy	Does not guarantee group privacy
Security guarantee holds with many or few users	Sending tons of messages degrades privacy
	Fixed message size, roughly as big as a tweet
	Infrequent dialing rounds

Outline



Pathway to Metadata Anonymous Communication

Dialing Protocol

Threat Model Recap & Analysis

Results

Discussion

You Asked, We Will Try to Answer

Group chat?

Improve scalability while maintaining privacy?

Can the dialing and conversation protocols happen at the same time?

If dead drops are erased each round, how does retransmission work?

Would adding random delays to messages (stall message passing) give the same guarantees as shuffling messages?