

The Reverse Statistical Disclosure Attack

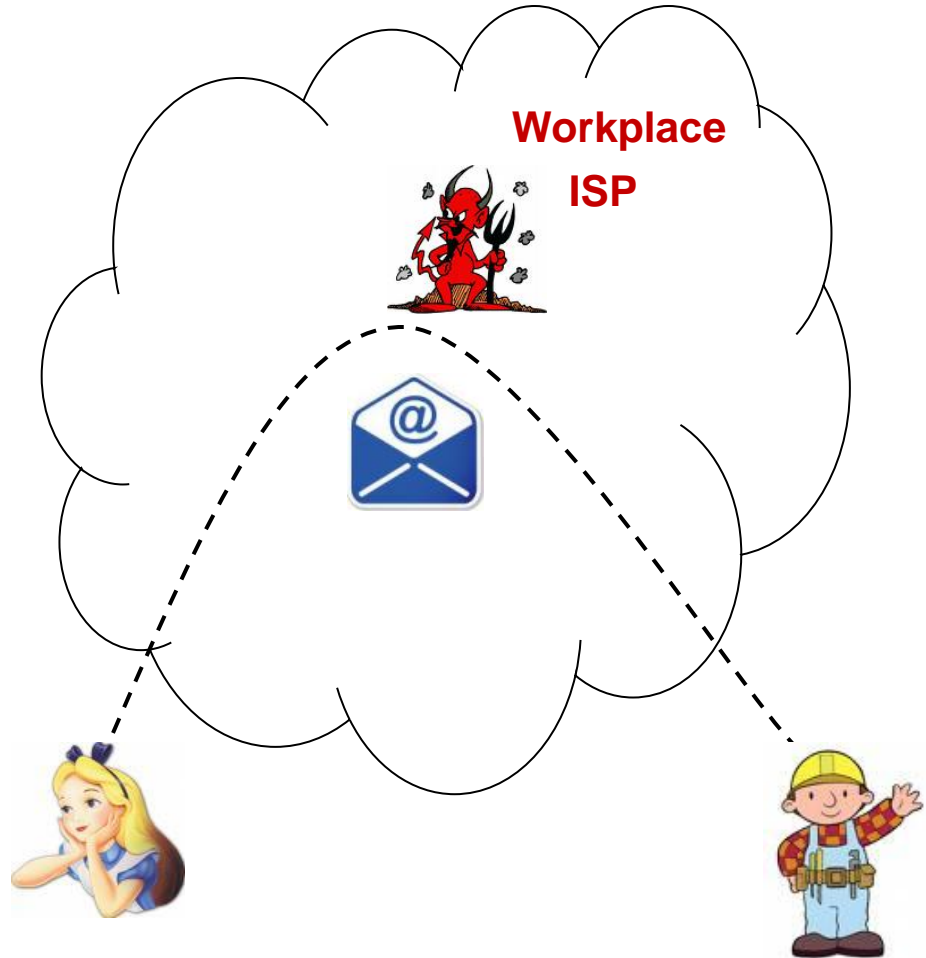
Nayantara Mallesh and Matthew Wright
Department of Computer Science & Engineering
The University of Texas at Arlington

Overview

- Motivation & Background
 - Online privacy
- Attacks on Email Privacy
 - SDA (existing)
 - Reverse SDA (our contribution)
- Defenses
 - Cover Traffic
- Simulation and Results
- Conclusions

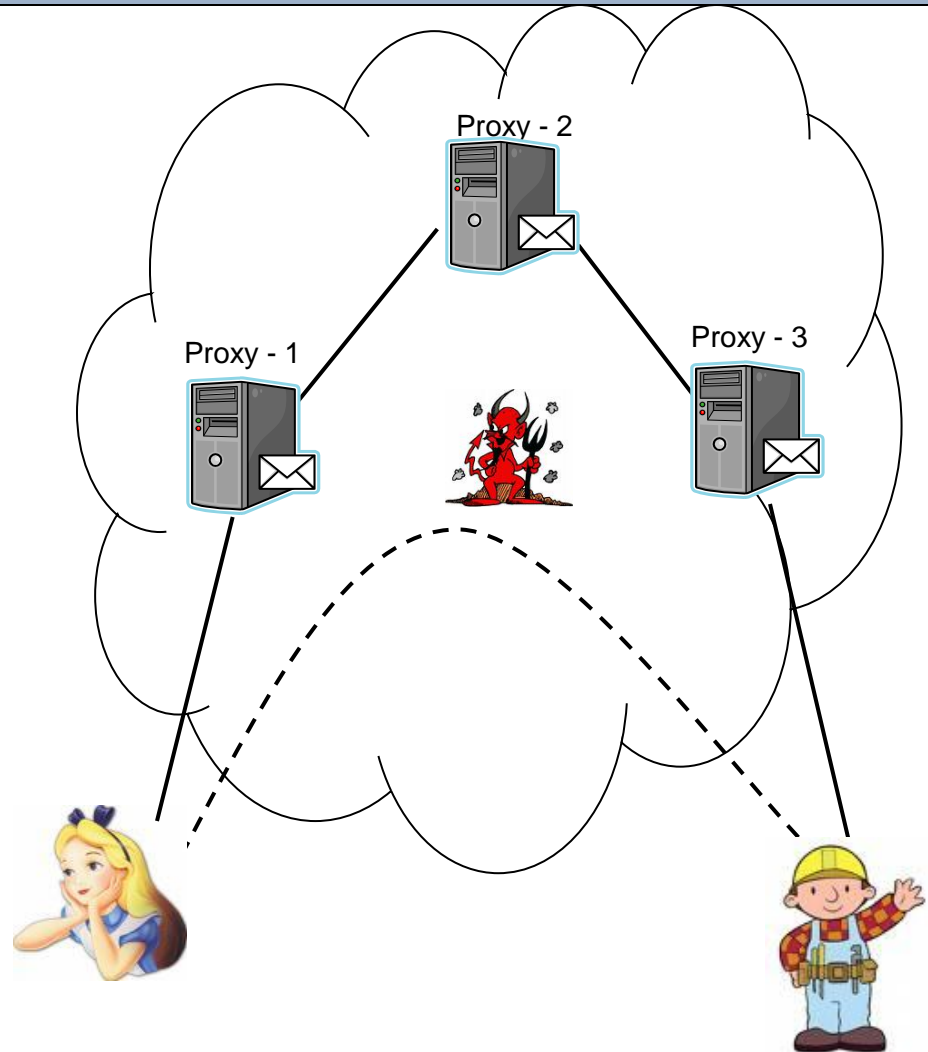
Motivation

- People spend a lot of their time online
 - Email **#1**
 - Information gathering, social interaction, entertainment, shopping
 - Business, Online Banking
- Online Privacy ?
 - Protect against network surveillance,
 - Profiling by service providers,
 - Breach of private data by irresponsible corporations
- Email Privacy
 - Email address visible
 - Encrypt content
 - IP address still visible
 - IP can be literally mapped to city or even street location and can be used to profile the user and how she connects to the Internet.

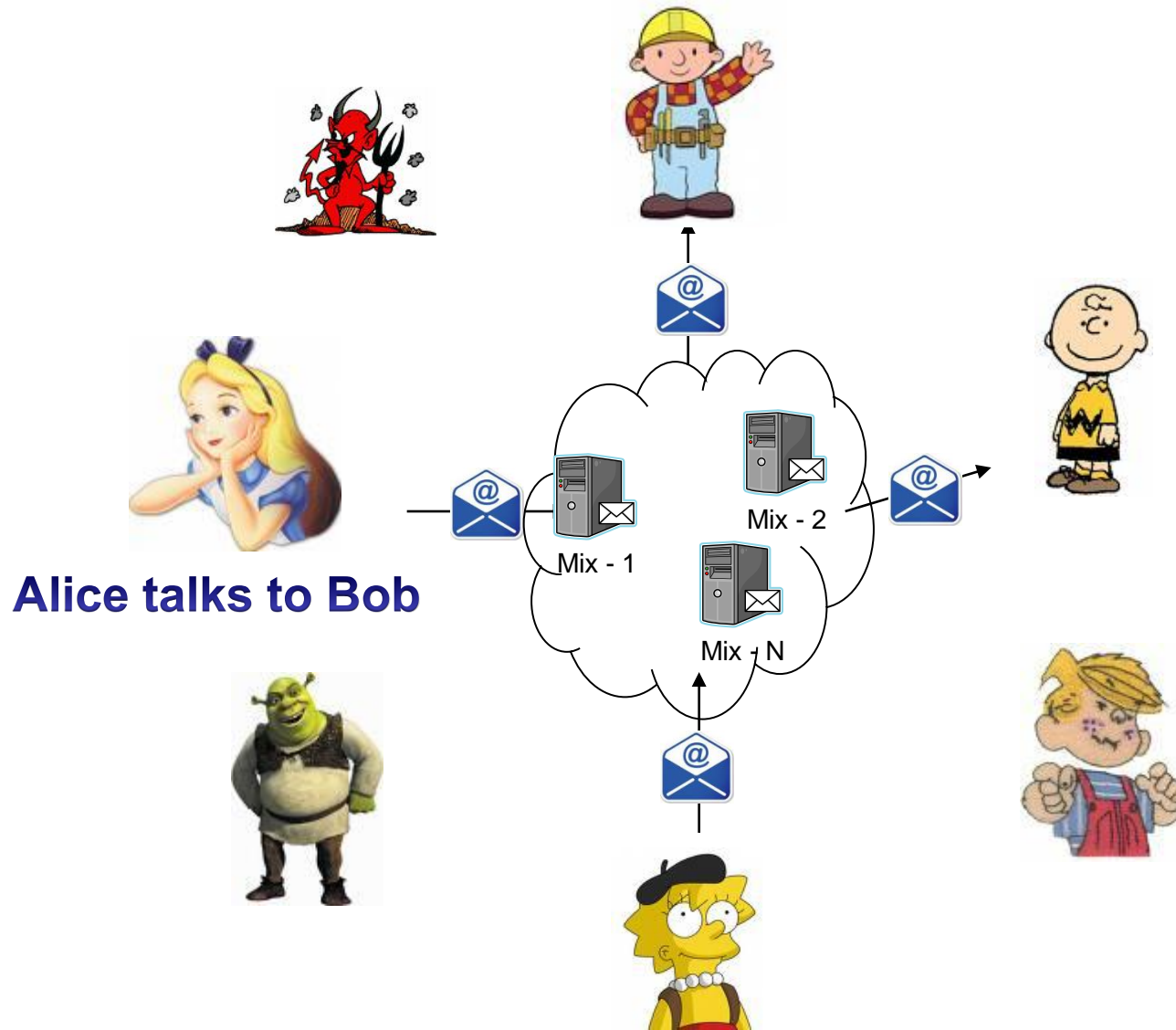


Anonymity Systems

- **Email Privacy Systems**
 - Multiple volunteer nodes
 - Pick random nodes to relay messages
 - Layered encryption, so a node knows only immediate source and destination.
 - Cannot link Alice to Bob unless all 3 nodes collude
- **Email privacy systems are vulnerable to long-term intersection attacks**
- **Statistical Disclosure Attack (SDA)**
 - Eavesdropper watches messages entering and exiting the system
 - Goal is to link a target user with her contacts



System Model



Alice & Bob

- Alice is a user of the anonymity system and is the target of the attacker
- Has a number of contacts she communicates with via the system
- Online some of the time, offline some of the time



- Bob is one of Alice's contacts
- Receives messages from Alice and from other users

Background Users

- Other people who use the anonymity system to communicate with their contacts
- Provide anonymity to Alice's messages
- Alice's messages are mixed with messages from background users inside the anonymity system.



Attacker Model

- Global or Partial
 - Can see all or some of the links
- Passive eavesdropper
 - Does not modify messages
 - Does not control any nodes in the anonymity system
- Eavesdrops on messages
 - Entering system
 - Exiting system
- Goal
 - To find Alice's contacts

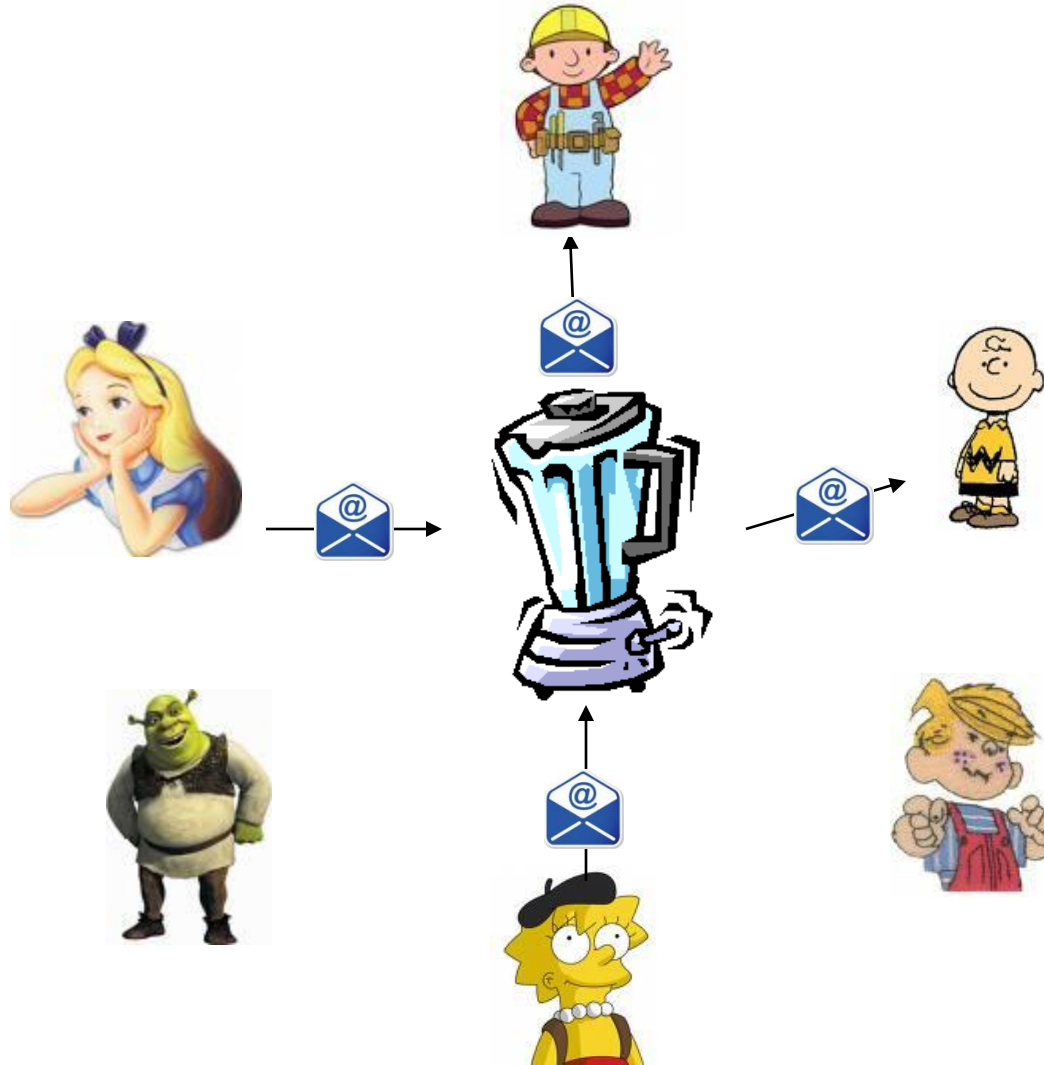


Anonymity System

- Network of re-mailers or mixes
- Abstract away internal details and refer to the system as a Mix
- Mix: Delays, Encrypts, and Reorders messages before forwarding to receivers
- Mixing Rounds
 - Collect messages
 - Flushes out messages in cycles called rounds
 - Round can be 1 minute, 1 hour or 1 day depending on the volume of messages
- Mix Types
 - Based on mixing strategies
 - Threshold mix (Batch Size)
 - Binomial mix (Message Delay)



Intersection Attack



Round 1

- Bob
- Charlie
- Dennis
- Lisa

Round 2

- Bob
- Charlie
- Dennis
- Shrek

Round 3

- Bob
- Charlie
- Lisa
- Shrek

Alice sends to Bob or Charlie!

Intersection Attack

- At the end of 3 rounds of observation
 - Since Bob and Charlie are the most common receivers when Alice participates, Alice is speaking to either Bob and Charlie
 - The attacker has reduced the anonymity of Alice's contact from 1 out of 5 to 1 out 2.



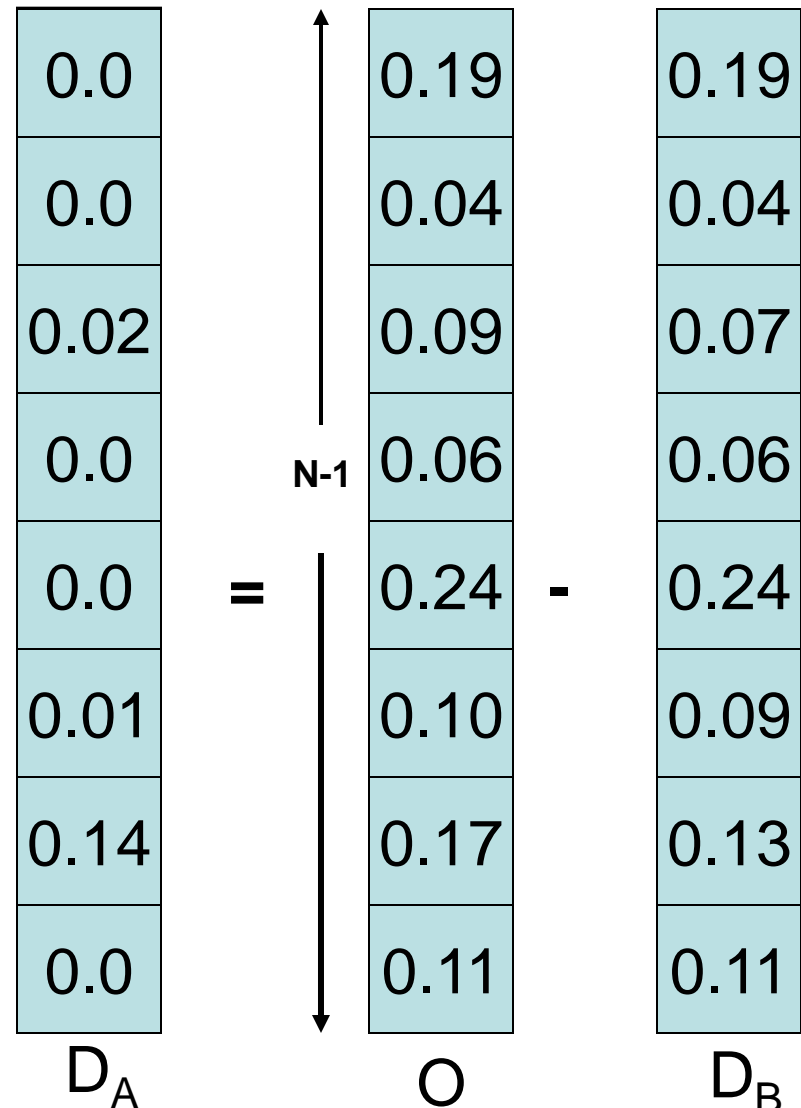
Statistical Disclosure Attack

- Statistical Disclosure Attack (SDA)
- SDA is based on the simple Intersection Attack we discussed earlier
- Attacker's Goal: Who does Alice's send to?
- Strategy
 - Record distribution of messages received when Alice and Background Users send messages. Call this vector O
 - Record distribution of messages received when only Background Users send. Call this vector $D_{\text{Background}}$

$$O = D_{\text{Alice}} + D_{\text{Background}}$$

SDA Implementation

- **Attacker's observation** – O
 - Distribution of messages received when Alice and Background Users send
- **Background sender behavior** – $D_{\text{Background}}$
 - Distribution of messages received when only Background Users send.
 - Can be assumed to be $1/N$ if no non-Alice observations can be made
- **Alice's behavior, unknown vector** – D_{Alice}
 - Likelihood that Alice sends to this receiver



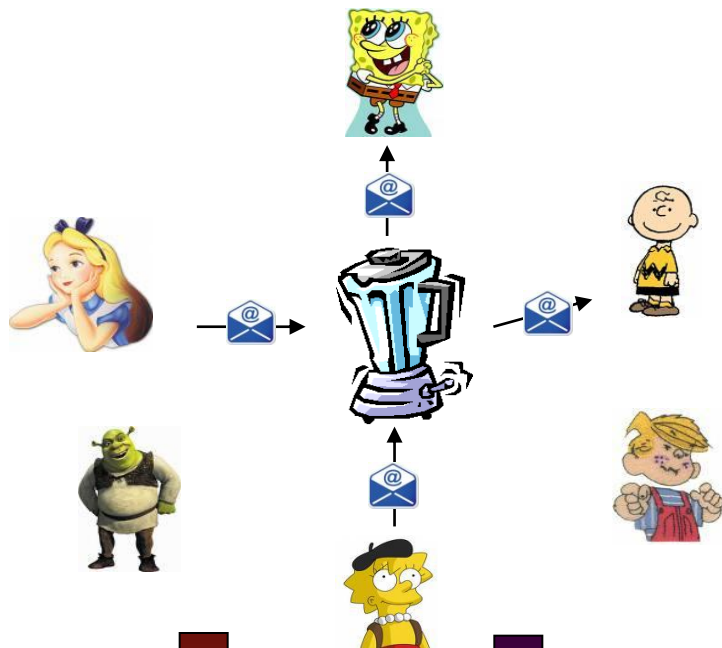
Outline

- Motivation & Background
 - Online privacy
- Attacks on Email Privacy
 - SDA (existing)
 - **Reverse SDA (our contribution)**
- Defenses
 - Cover Traffic
- Simulation and Results
- Conclusions

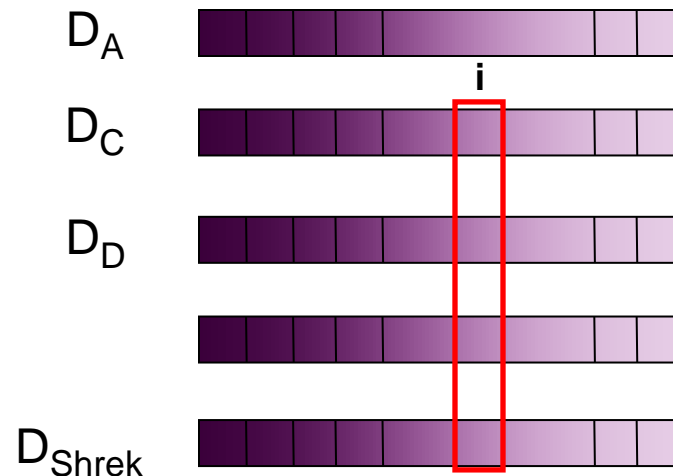
Reverse Statistical Disclosure Attack

- Enhancement to SDA called the Reverse SDA (RSDA)
- Uses information that is available in the current attacker model
- Reverse SDA
 - Assumption: Alice is likely to receive messages from people that she sends to
 - Attacker's Goal: Who are Alice's contacts?
 - Sub-goal: Who sends to Alice?
 - Strategy
 - Do the SDA on every user in the system
 - This gives a set of likely receivers of each user
 - Find out for which users Alice appears to be a receiver (D_R)
 - Combine D_A and D_R to get D_{AR}
 - Hypothesis: The attacker uses more of the available information and analyzes it to get D_{AR} . So, D_{AR} should provide a more accurate list of Alice's contacts than D_A .

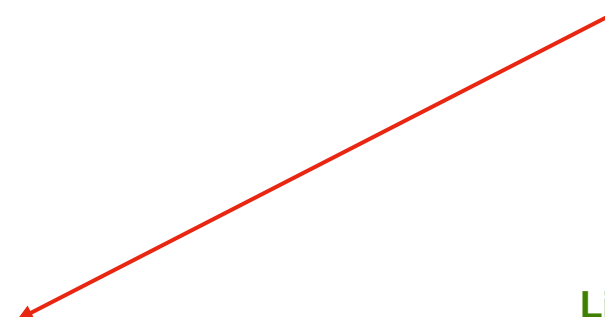
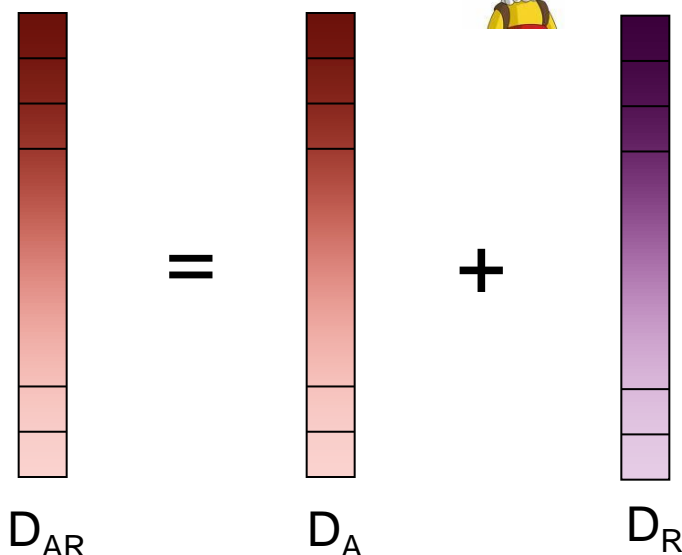
RSDA Implementation



Likelihood Alice sends to other users



Likelihood other users send to Alice




Overview

- Motivation & Background
 - Online privacy
- Attacks on Email Privacy
 - SDA (existing)
 - Reverse SDA (our contribution)
- **Defenses**
 - **Cover Traffic**
- Simulation and Results
- Conclusions

Defenses - Cover Traffic



- **Dummy packets**
 - Inserted into network
 - Indistinguishable from real traffic
- **Attacker**
 - Factor this message into calculations
 - Or, drop it ?
- **Recipient** 
 - Distinguishes cover from real
 - Drops dummy packets



Cover Traffic

- Alice cover
 - Sent from Alice to the mix
 - Dropped by the mix
 - Cover Generation
 - + Based on number of real messages
 - + Independent of number of real messages
- Receiver-bound cover (RBC)^[1]
 - Generated by the mix and sent to receivers
 - Inserted into outgoing traffic in every round
 - Recipients are chosen randomly in each round
 - Amount of cover traffic is proportional to the real outgoing traffic

[1] N. Malleh and M. Wright. Countering statistical disclosure with receiver-bound cover traffic. In Proceedings of ESORICS 2007

Overview

- Motivation & Background
 - Online privacy
- Attacks on Email Privacy
 - SDA (existing)
 - Reverse SDA (our contribution)
- Defenses
 - Cover Traffic
- **Simulation and Results**
- Conclusions

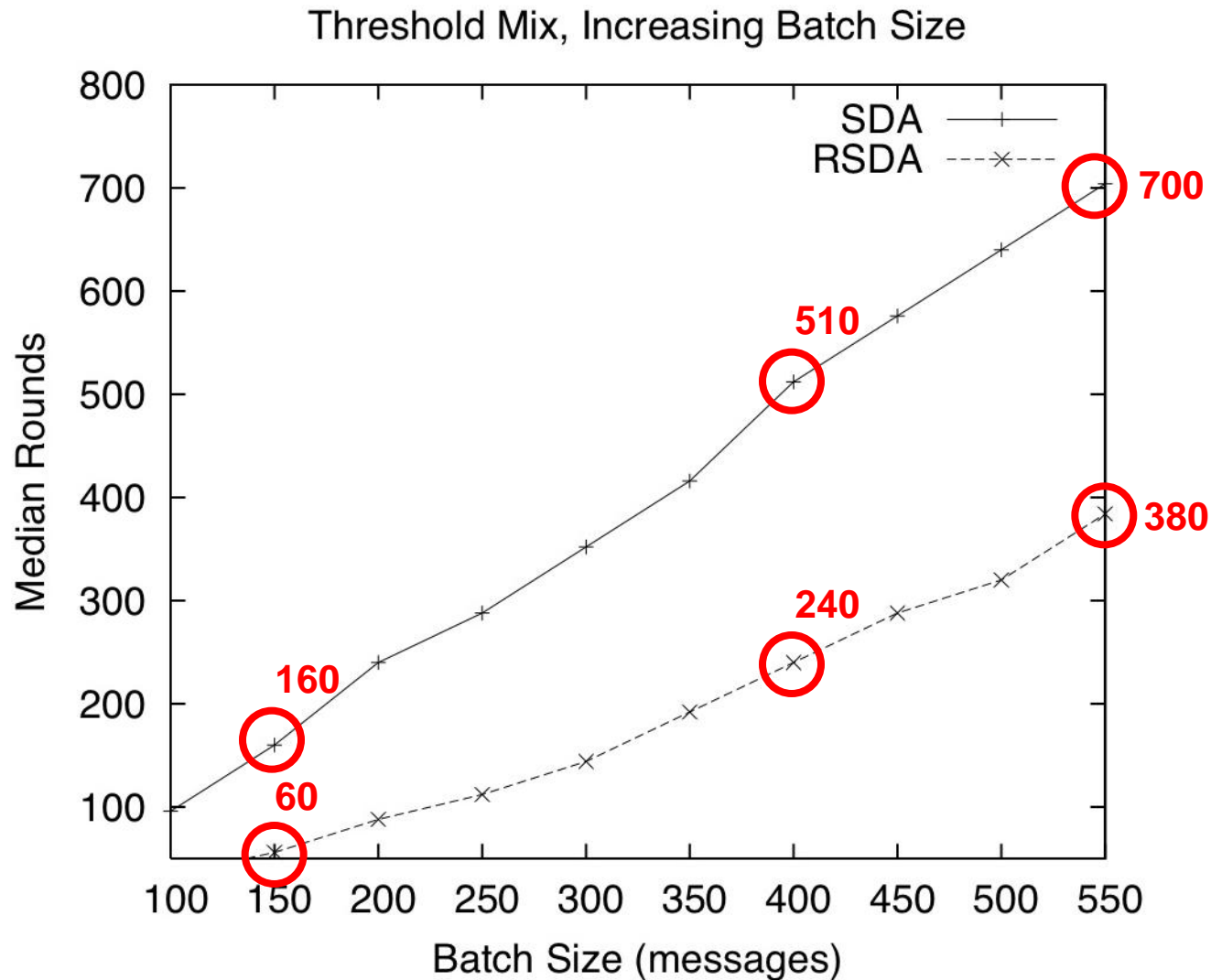
Simulation Details

- Number of users
 - $N = 1000$
 - Alice Contacts = 10
- Mixing Strategies
 - Threshold mix
 - Batch Size, $B=100$ to 500 messages
 - Binomial mix
 - Probability of delaying a message, $P_{\text{delay}} = 0.1$ to 0.9
- Contacts
 - Uniform Network
 - Each user has a random number of contacts
 - Uniformly selected from user set

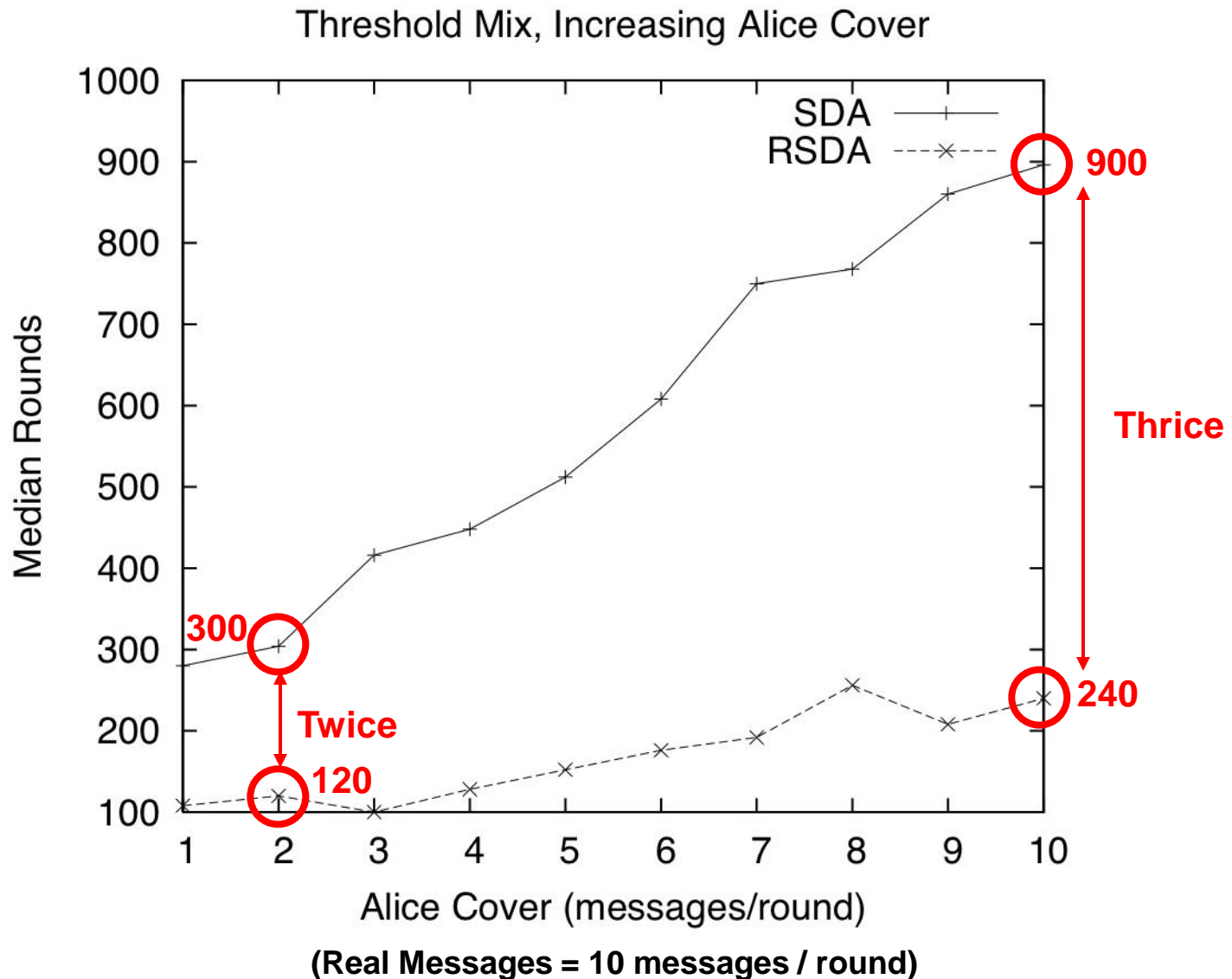
Simulation Details

- **Sending Behavior**
 - Number of messages/round is chosen from a Poisson distribution (Rate = 1 to 10 messages/round)
 - Sends uniformly to set of contacts
- **Cover Traffic Generation**
 - **Alice**
 - Number of dummy messages chosen from a Poisson distribution (Rate = 5 messages/round)
 - **RBC**
 - 10% to 100% volume of real messages
 - Recipients chosen uniformly & randomly
- **Metric**
 - Median rounds to find 50% of Alice's contacts

Threshold Mix With No Cover Traffic

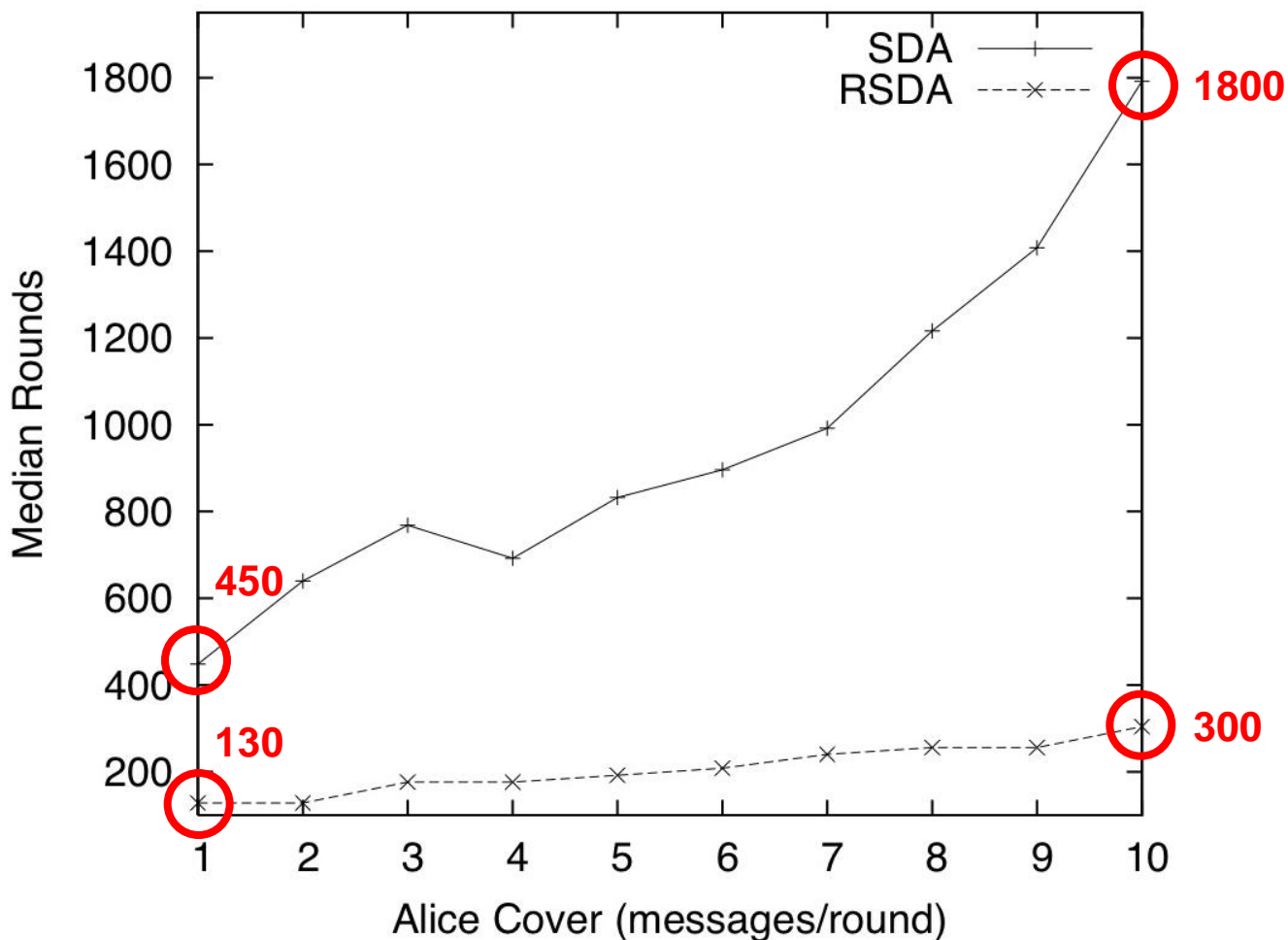


Threshold Mix With Alice Cover

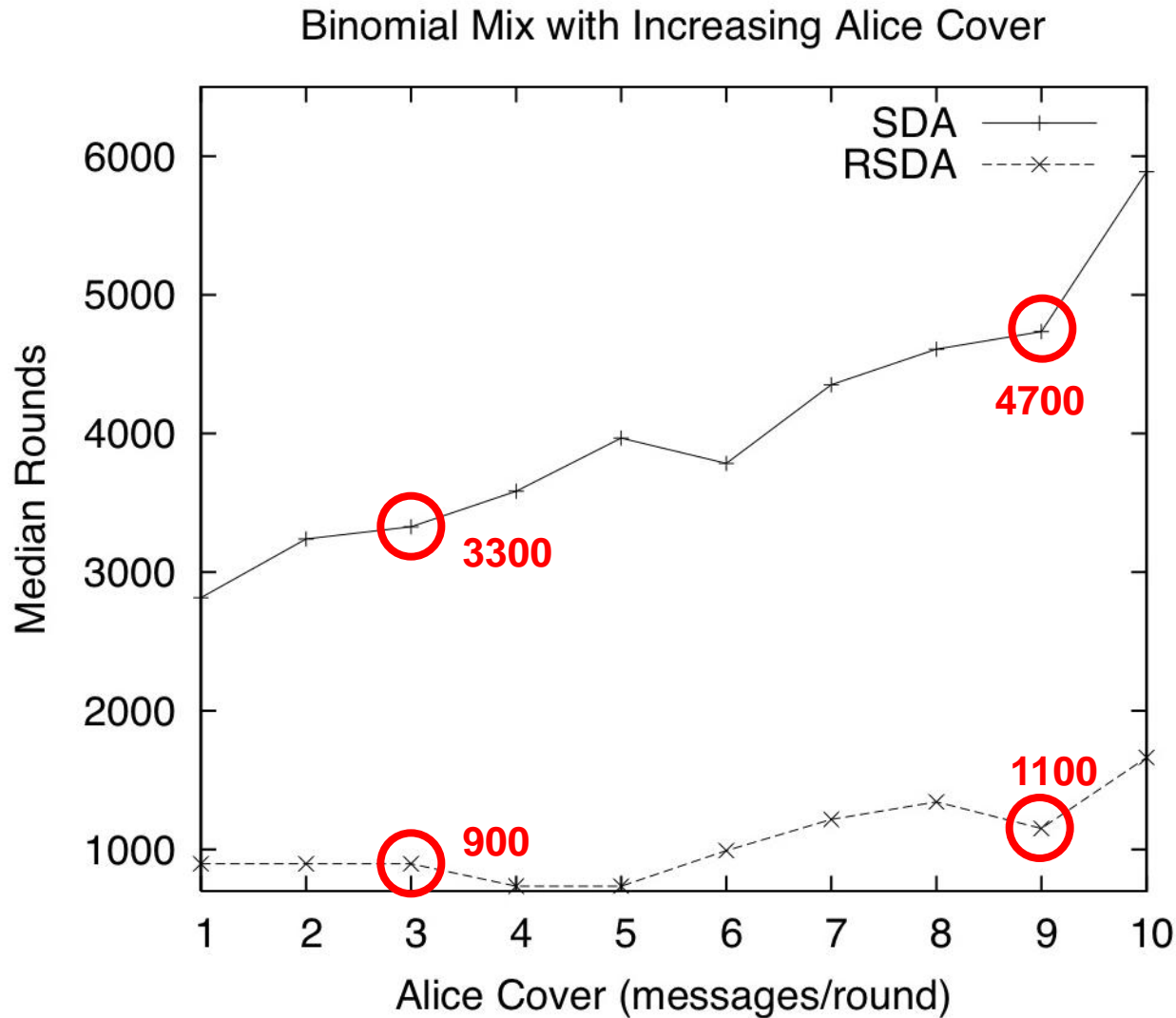


Threshold Mix With Alice Cover and RBC

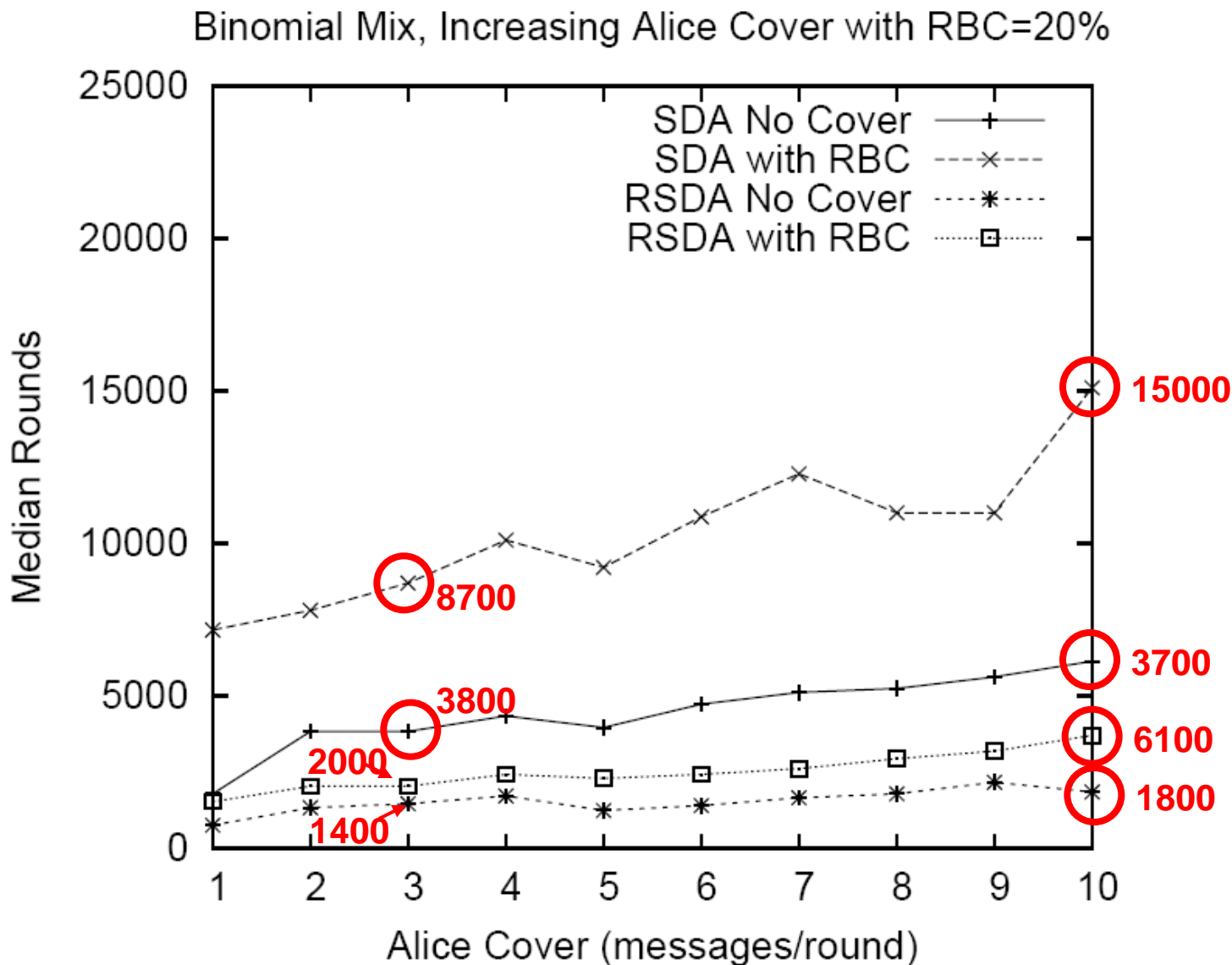
Threshold Mix with 100% RBC, Increasing Alice Cover



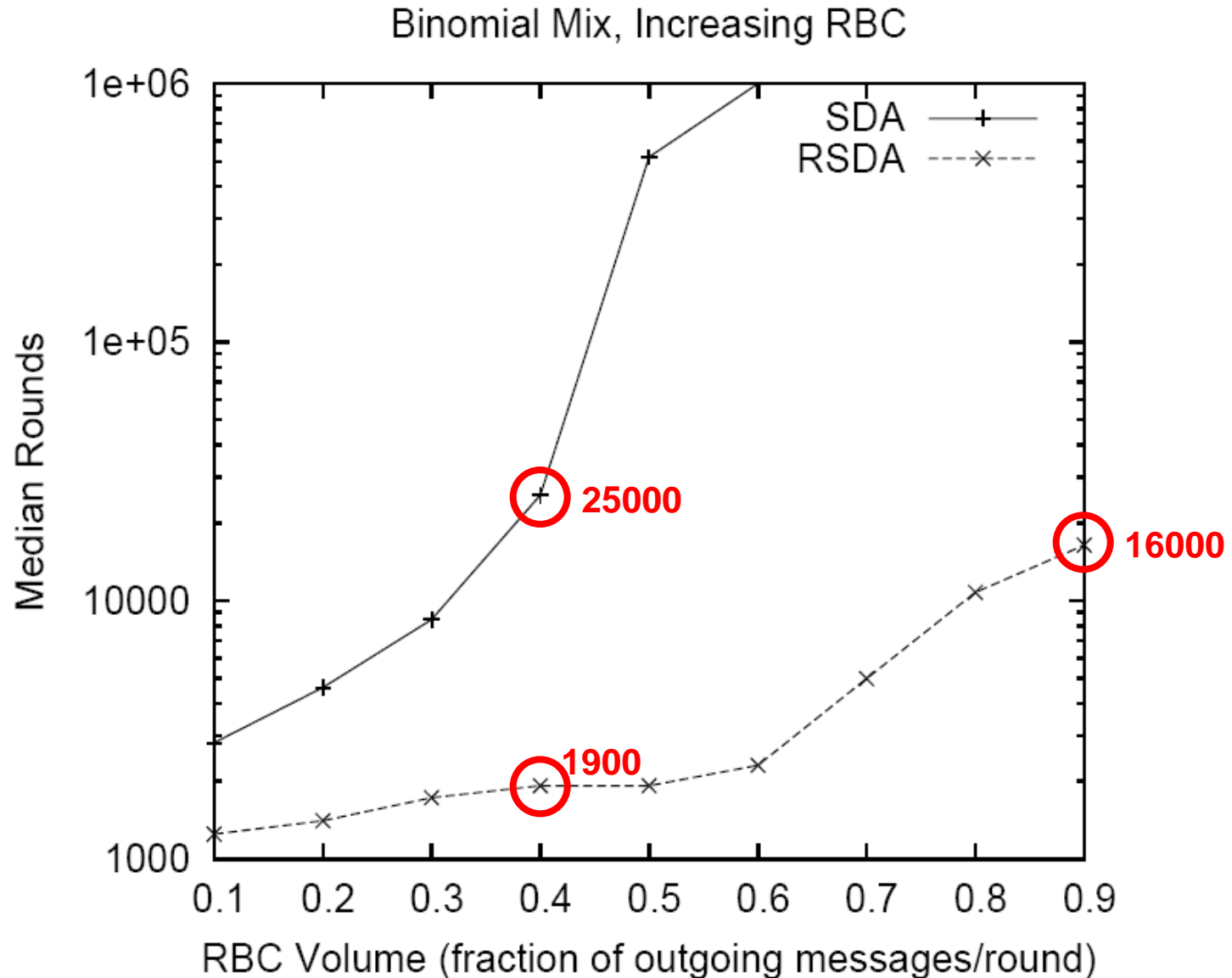
Binomial Mix With Alice Cover



Binomial Mix With Alice Cover and RBC=20%



Binomial Mix With Increasing RBC



Conclusions and Future Work

- **Reverse SDA**
 - Improvement over existing SDA
 - Uses traffic sent to target users in addition to traffic sent from target user to her contacts
 - Results show that SDA takes 2-3 times as long as RSDA in many of the cases we studied
 - As SDA becomes harder and takes longer for the attacker due to cover traffic, RSDA's relative improvement becomes larger.
 - Mix designers need to model and account for information leaked in receiving messages, not just sending.
- **Analysis of Reverse SDA (Future Work)**
 - Extend “Analysis of SDA and Receiver-Bound Cover” (in submission) to Reverse SDA