Two-Sided
Statistical Disclosure Attack

George Danezis
Claudia Diaz
Carmela Troncoso
ESAT/COSIC (KU Leuven)

Talk Outline

- Disclosure Attacks and Anonymity
- Modelling replies
- The Two-Sided Statistical Disclosure Attack
- Evaluation
- Discussion and Conclusions

Disclosure Attacks

- Anonymous communications: hide communication partners
- Attacker objective: reveal Alice’s contacts
- Threshold mix
- Passive attacker
  - Observes the network for many rounds
  - Exploit persistent patterns

Disclosure Attacks: Previous work

- Solving NP-Complete problem [Kesdogan03]
- Simplified model
  - Sensitive to changes

↓

- Statistical Disclosure Attacks [Danezis03]
  - Reduce complexity

↓

- Two-sided Statistical Disclosure Attacks
  - Include replies

Introducing replies in the model

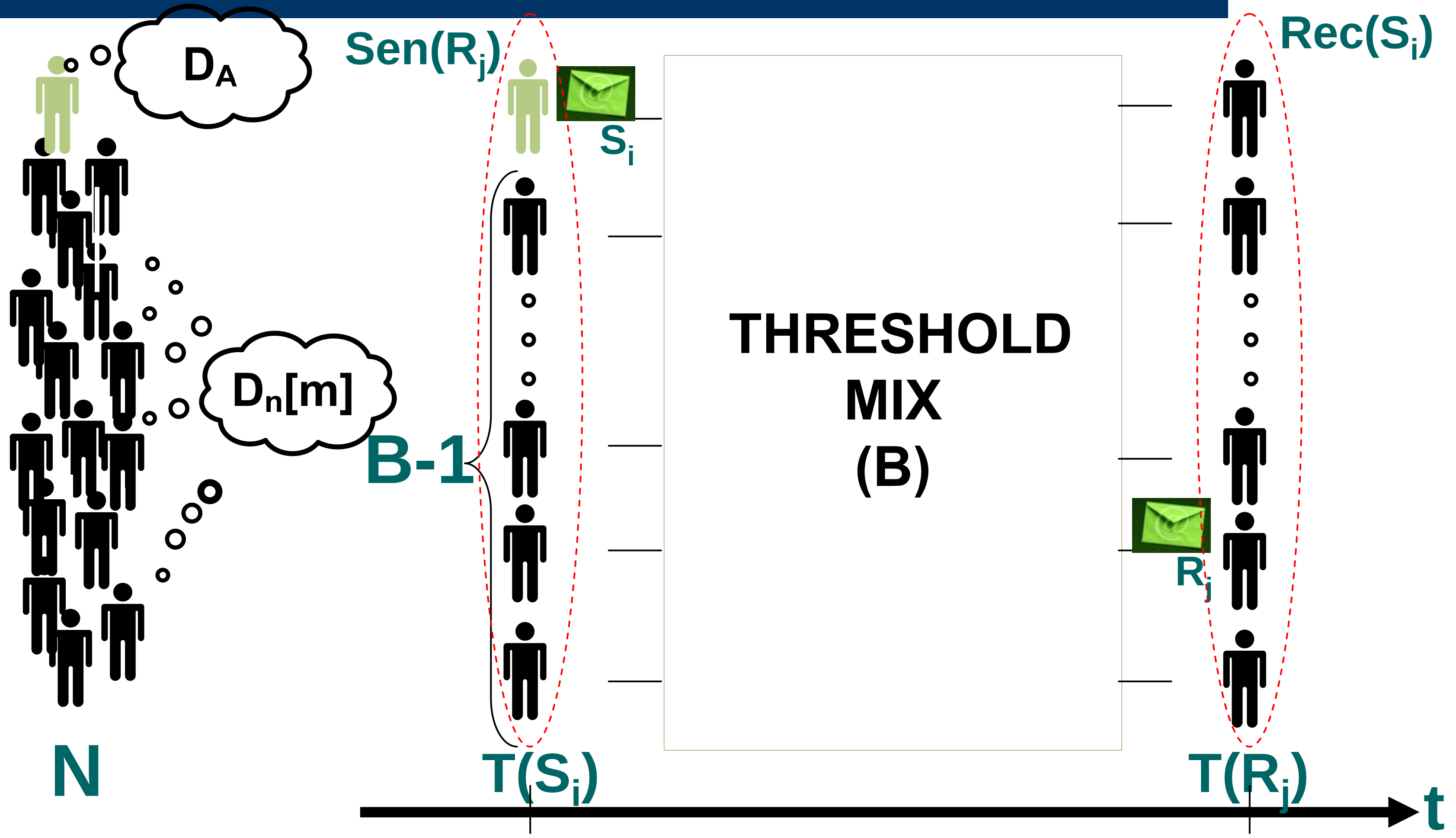
- Indistinguishable from normal messages

- Parameters:

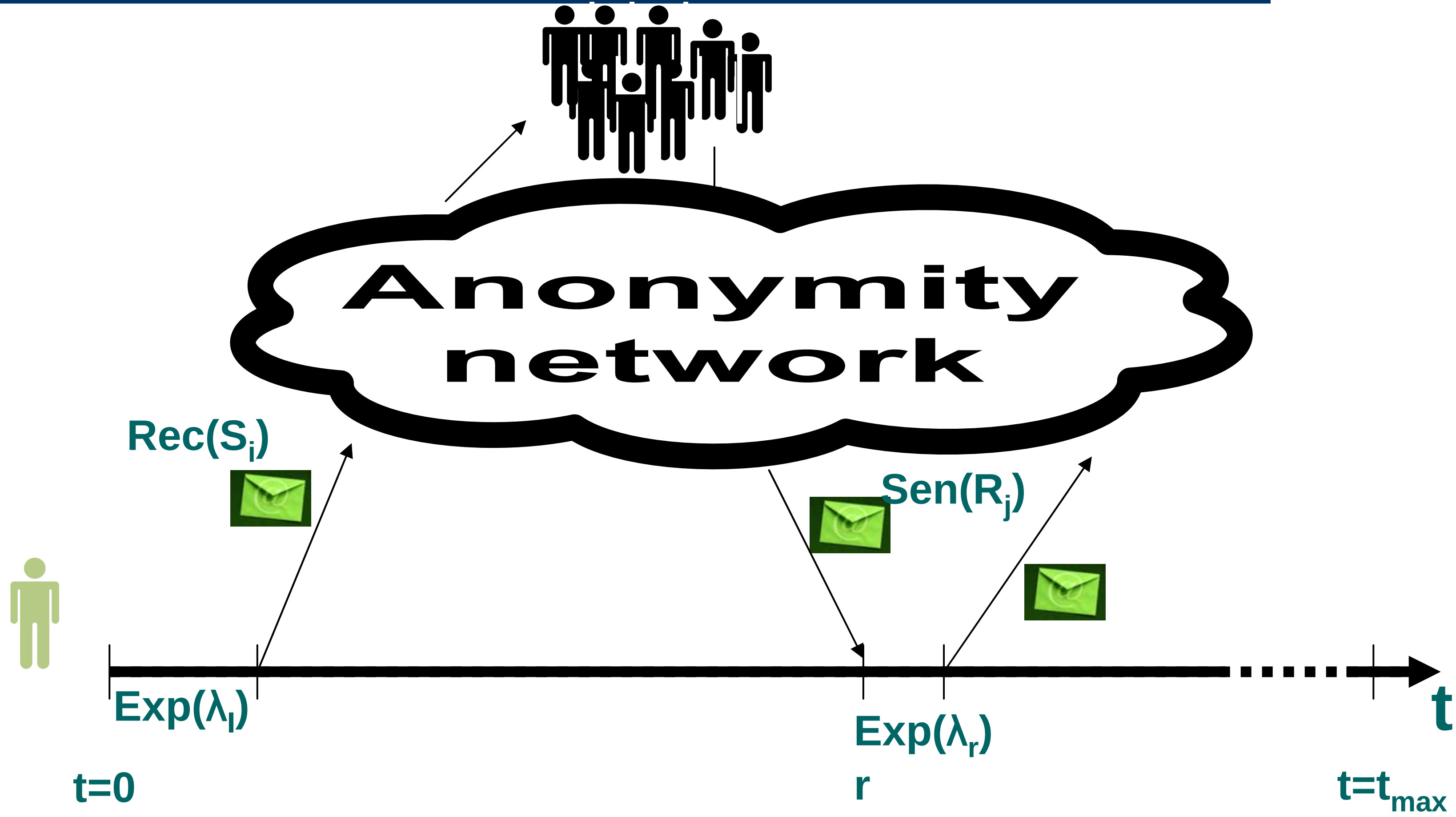
– Choice of partners	▸ Distribution of contacts
– Start a new discussion	▸ Poisson process
– Replying?	▸ Fixed known probability
– Time to reply	▸ Exponential

- Independent

Introducing replies: The general formal model



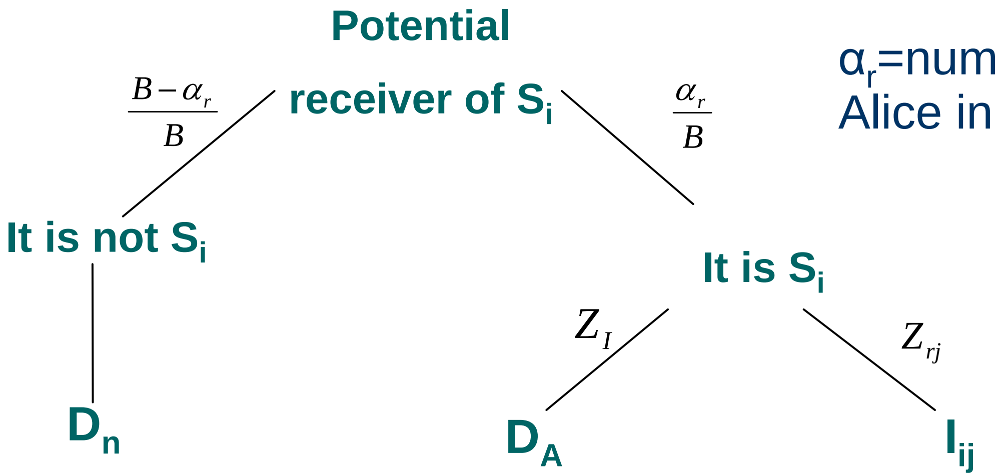
Introducing replies:
The replies in the formal model



The Two-Sided Statistical Disclosure Attack

- Uses
  - Rounds with Alice sending/receiving
  - Time sending/reception
- Objective
  - Estimate D_A
  - Infer receiver per round
    - Contribution from Alice (D_A)
    - Contributions from other senders (D_n)
    - Potential receivers of replies

The Two-Sided Statistical Disclosure Attack



Potential receiver of S_i

$\frac{B-\alpha_r}{B}$

$\frac{\alpha_r}{B}$

It is not S_i

It is S_i

Z_I

Z_{rj}

D_n

D_A

I_{ij}

α_r=number of messages sent by Alice in round r

$$I_{ij} = \frac{\operatorname{Re}c(S_i)\cdot Sen(R_j)}{\left\|\operatorname{Re}c(S_i)\cdot Sen(R_j)\right\|_1}$$

$$\operatorname{Re}c(S_i) \sim \frac{\alpha_r}{B}\,\frac{Z_I D_A + \sum_j Z_{rj} I_{ij}}{Z_I + Z_r} + \frac{B-\alpha_r}{B} D_n$$

The Two-Sided Statistical Disclosure Attack

$$\mathrm{Re}\,c(S_i) \sim \frac{\alpha_r}{B}\frac{Z_I D_A + \sum_j Z_{rj} I_{ij}}{Z_I + Z_r} + \frac{B-\alpha_r}{B} D_n$$

$$D_A \sim \frac{(B\cdot \mathrm{Re}\,c(S_i) - (B-\alpha_r)D_n)(Z_I+Z_r)}{\alpha_r Z_I} \equiv C_i \Rightarrow \boxed{\hat{D}_A \approx \frac{1}{K_s}\sum_{\forall i} C_i}$$

$$\mathrm{Re}\,c(S_i)' \sim \left(\frac{\alpha_r}{B}\frac{Z_I \hat{D}_A + \sum_j Z_{rj} I_{ij}}{Z_I + Z_r} + \frac{B-\alpha_r}{B} D_n\right)\cdot \mathrm{Re}\,c(S_i)$$

From traffic in rounds where Alice is not present [Mathewson and Dingledine 04]

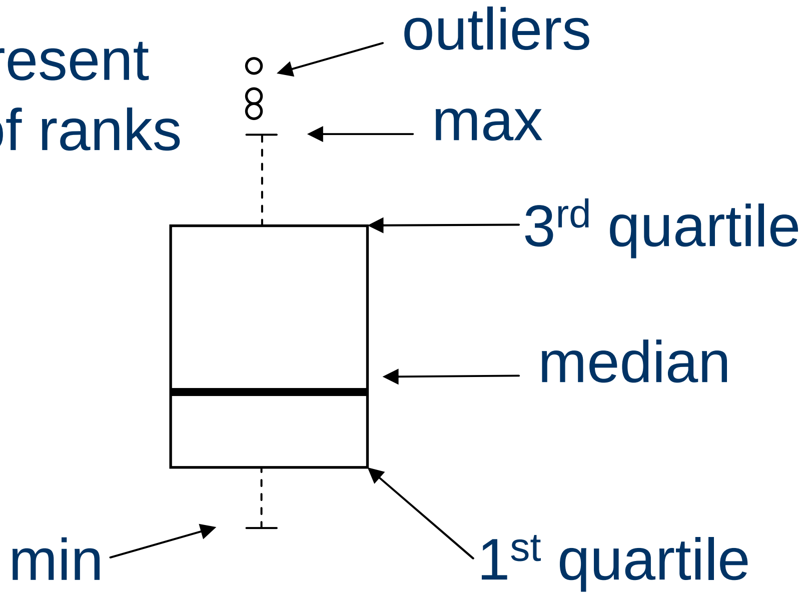
Evaluation: Method

- We compare with SDA
- **Rank**: number of receivers in Rec(S_i)’ with at least the same probability as the real receiver

Rec(S_i)’
0.1
[✓ 0.2]
0.05
★ [✓ 0.125]
0.07
[✓ 0.155]
0.1
[✓ 0.2]

Rank = 4

- Box plot represent distribution of ranks

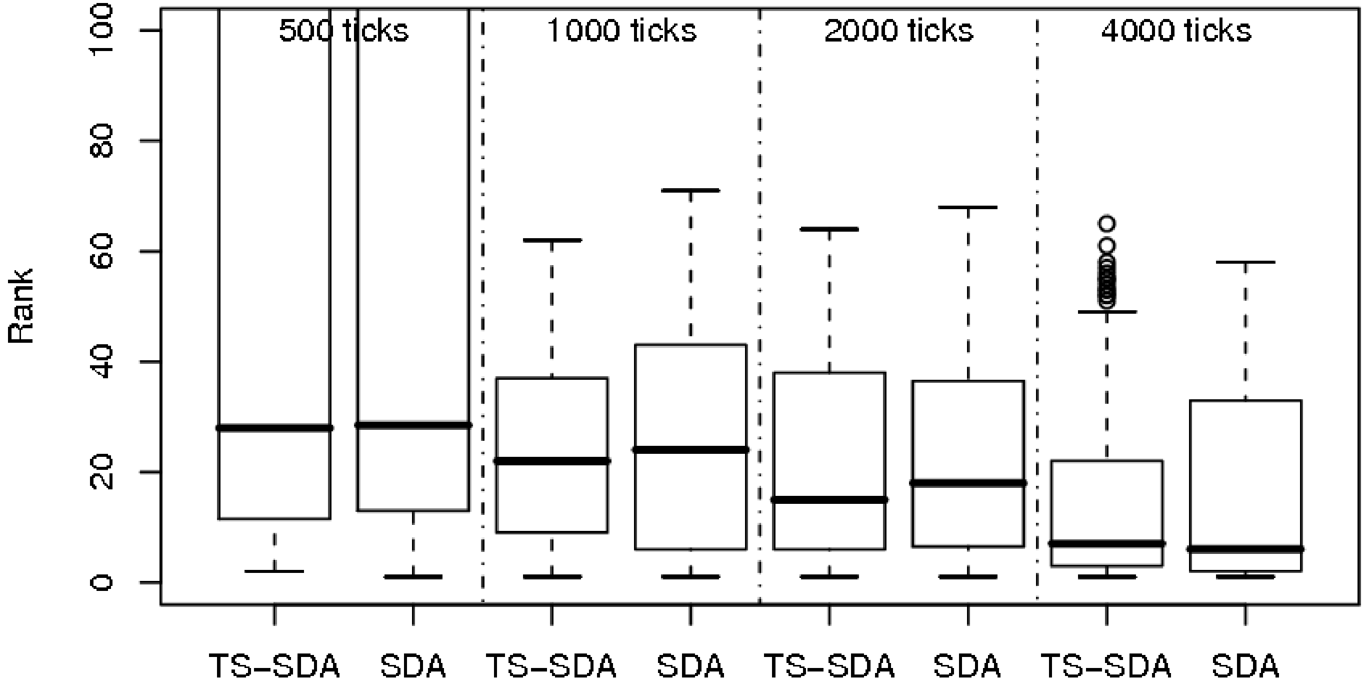


Evaluation: Standard parameters

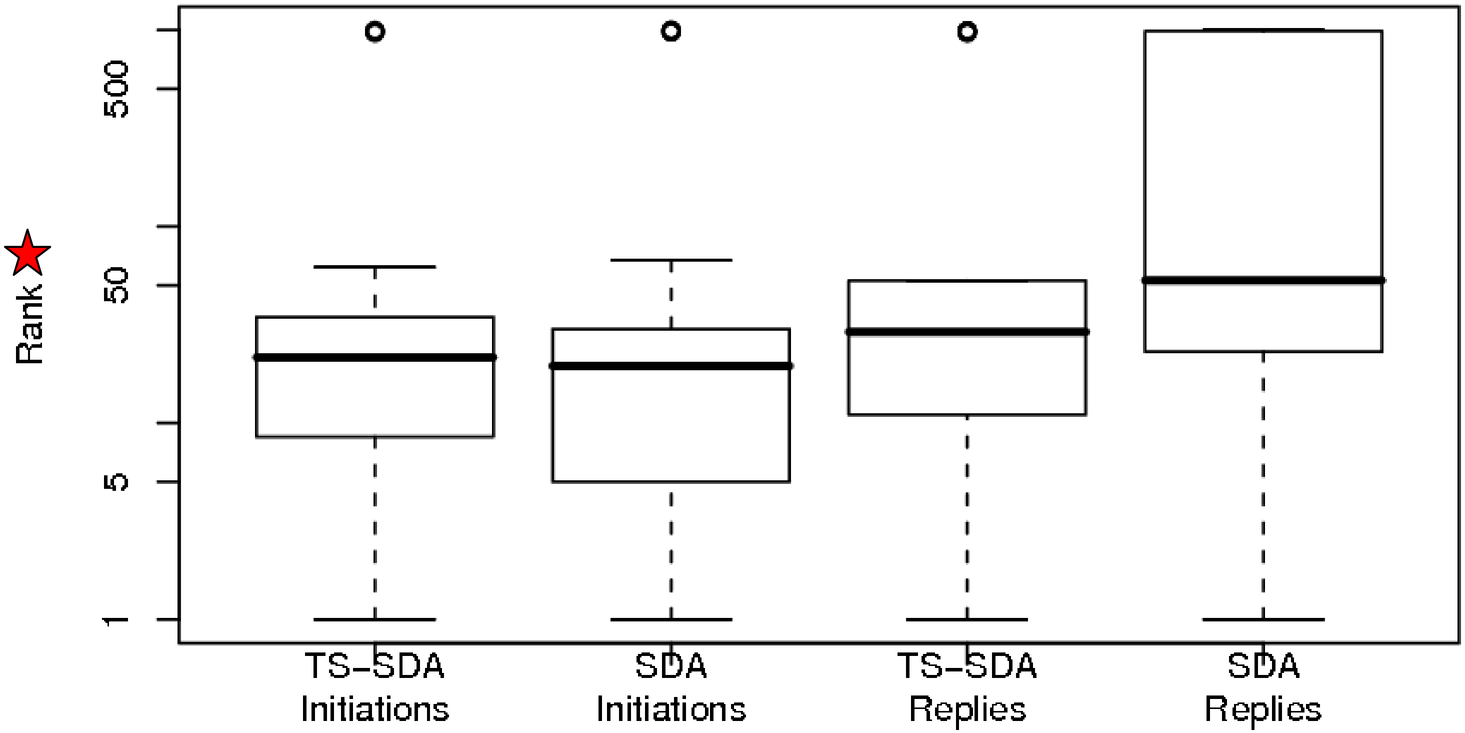
Name	Value	Description
N	1000	Number participants
k	20	Alice’s contacts
B	100	Mix threshold
t_{max}	4000	Observation time
λ_I	1/10	Initiation rate
r	0.5	Reply probability
λ_r	1/2	Reply delay rate

- Alice sends with uniform probability to her contacts
- The rest send with uniform probability to all the users
- Only Alice replies to messages

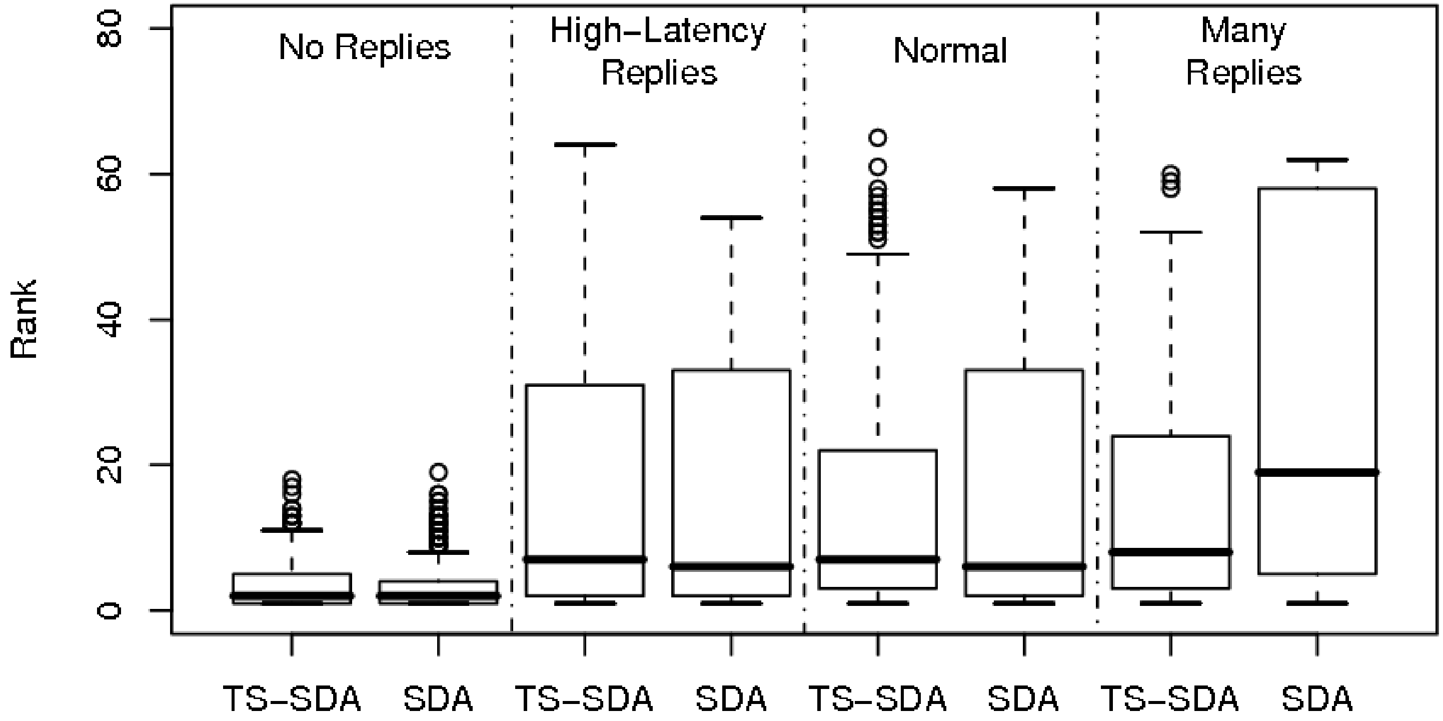
Evaluation: Observation time



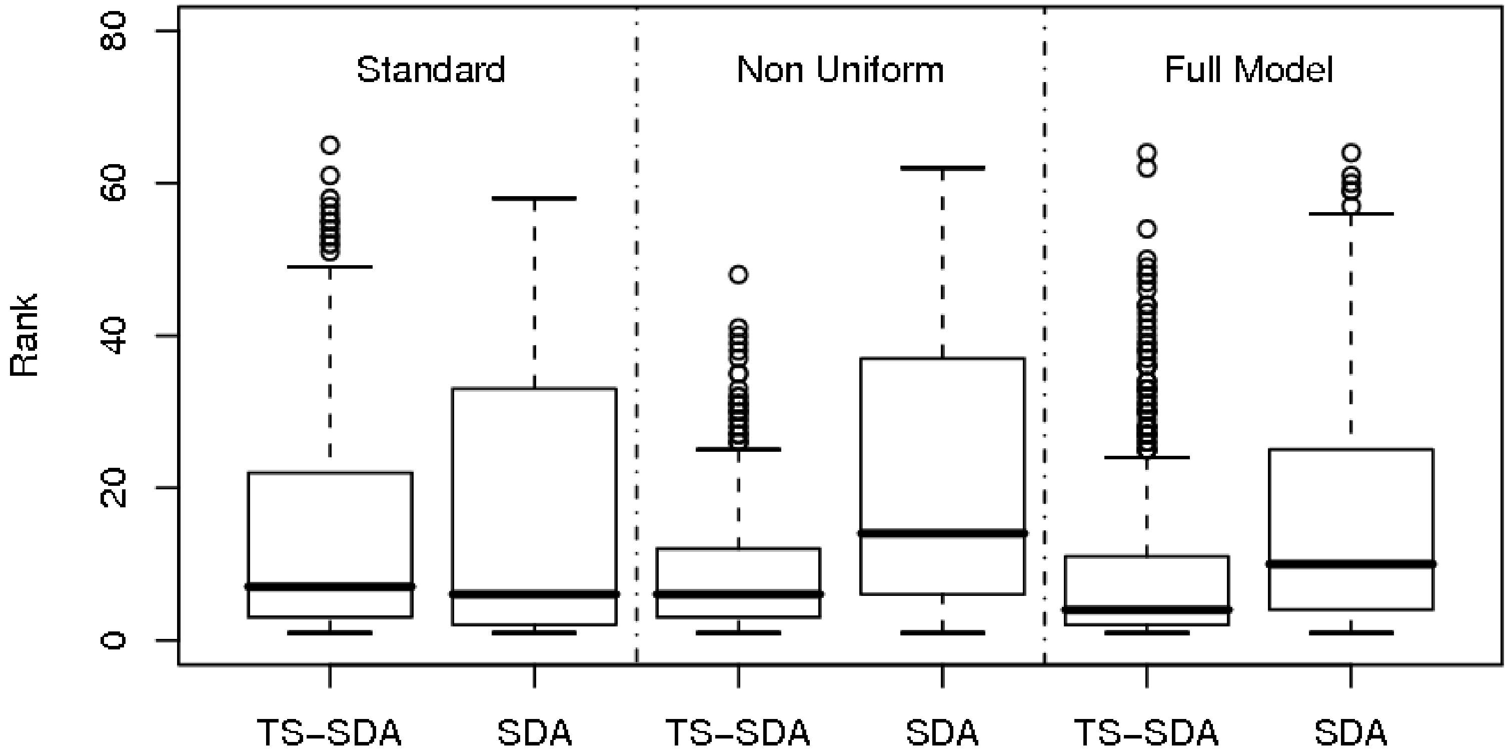
Evaluation: Initiations vs. replies



Evaluation: Replies rate



Evaluation: Background traffic



Discussion

- The model is not realistic
  - Poisson process for initiating discussions
  - Parameters independent
  - Replying uniformly
  - Only one reply per message
  - Other anonymity systems

Conclusion

- First attack and model including anonymous replies
- The attack is fast
  - Only operations on vectors
  - Linear with the number of messages $O(K_s)$
- Evaluation in different conditions
- The timing of replies is crucial
- Indistinguishable replies increase anonymity
- Unrealistic model: lack of data

Thank you

Carmela.Troncoso@esat.kuleuven.be