PRIVO: A PRIvacy-preserVing Opportunistic routing protocol for Delay-Tolerant Networks

Naercio Magaia, Carlos Borrego, Paulo Pereira, Miguel Correia

Outline

1. Introduction
2. Background and related work
3. The PRIVO protocol
4. Simulation model
5. Simulation results
6. Conclusions

1. Introduction

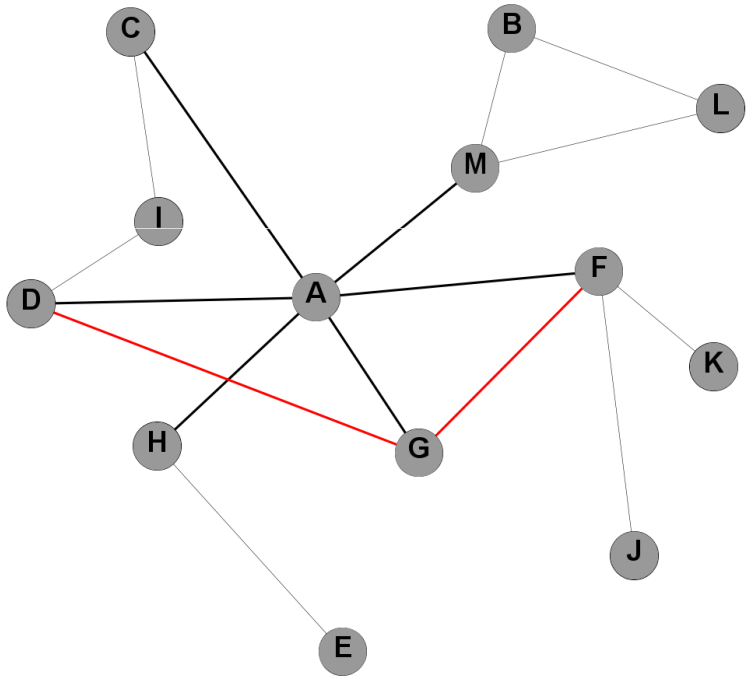
- Delay-Tolerant Networks (DTNs) are networks in which end-to-end connectivity between a source and target node may never exist.
- DTN routing involves the challenging task of **finding suitable nodes** to forward messages to.
- In DTNs there is information that may be **private**, such as the entities owning and managing DTN nodes and their relationships.
- If it is considered that some nodes might misbehave, **private information** such as contacts' history, list of neighbors, etc., which is required for computing some routing metrics **should not be disclosed to misbehaving nodes**.
- Privacy-preservation techniques allow **protecting privacy** through masking, modification and/or generalization of the original data without sacrificing the data utility.

2. Background and related work (1/2)

- Privacy can be understood as the **users' willingness to disclose or not** his/her information to others.
- Privacy **breaches** can be classified as
  - Identity disclosure
  - Link disclosure
  - Attribute disclosure.
- Anonymization methods
  - **protect** the privacy of information if sensitive information needs to be processed elsewhere.

2. Background and related work (2/2)

- **Homomorphic encryption**
  - a node to carry out computations on encrypted values, without needing to decrypt them first.
- **Centrality** of a node in a network
  - is a quantitative measure of the structural importance of this node in relation to others within the network.
- **Ego network**
  - consists of a central node along with its direct neighbors and all links among these neighbors.
- Betweenness centrality vs **Ego** betweenness centrality
- **Similarity** expresses the amount of common features of a group in social networks.



3. The PRIVO protocol

- PRIVO detects and utilizes the inherent social network structure to facilitate packet forwarding in DTNs
- PRIVO models a DTN as a time-varying neighboring graph
- PRIVO ensures privacy by means of anonymization and homomorphic encryption.
  - It uses **anonymization** to ensure **link privacy**, i.e., to avoid disclosing historical information associated to each node's *neighboring graph*.
  - It uses **homomorphic encryption** to ensure **attribute privacy**, i.e., to allow nodes to compare their *routing metrics* in a private manner.

3.1 Construction of the neighboring graph

- The **average separation period** is given by

$$\delta_{i,j}(x) = \frac{\int_{\tau} x_{i,j}(t)dt}{n_{i,j}}$$

where

- $x_{i,j}(t)$ denotes the separation period between nodes i and j
- τ denotes the elapsed time
- $n_{i,j}$ be the number of times that nodes i and j were away from each other.

- The **normalized** average separation period $\hat{\delta}_{i,j}$ is given by

$$\hat{\delta}_{i,j} = 1 - \frac{\delta_{i,j}}{\tau}$$

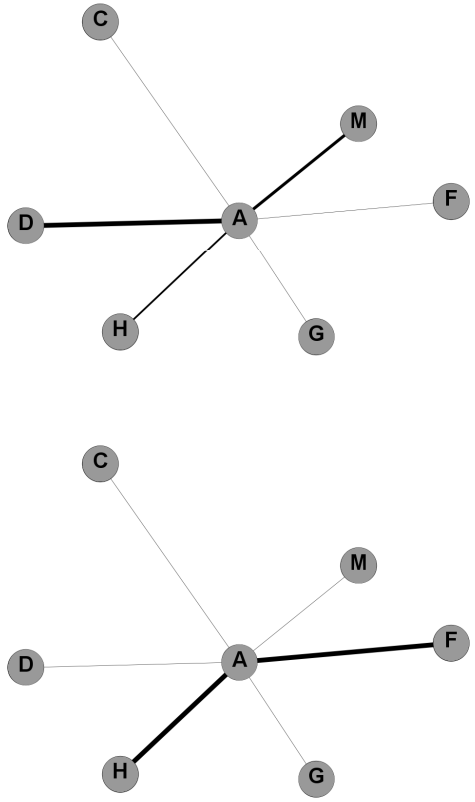
- The time-varying PRIVO weight (***pweight***) is given by

$$w_{i,j} = \frac{1}{\eta}\sum_{k=1}^{\eta} \hat{\delta}_k$$

where $\eta = |\tau|$ is the number of timeslots.

3.2 The link privacy mechanism

- Neighborhood randomization
  - consists in **partially hiding** each node's neighboring graph containing its historical encounter information.
  - nodes only exchange the **random least possible** number of nodes in their neighboring graphs.
- Binary anonymization
  - consists in **replacing the *pweight*** associated to a given link with 1 or 0, if the weight is above or below a given anonymization threshold, respectively.
  - The selection of the anonymization threshold is limited by the **utility** of the neighboring graph.

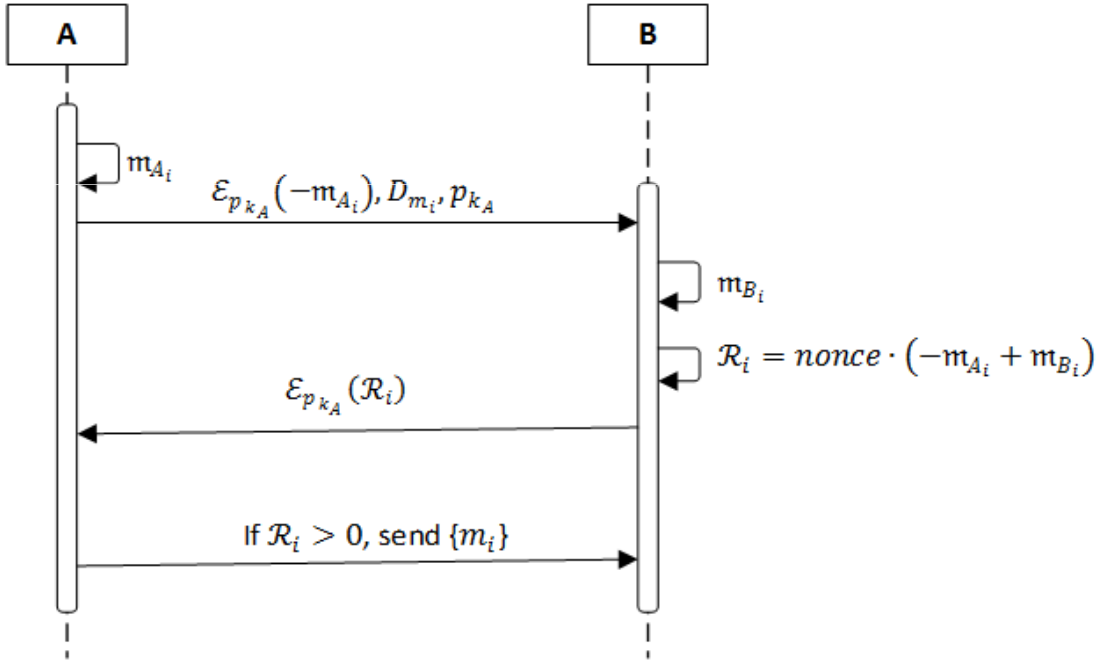


3.3 Routing algorithm (1/3)

- Let node A be a node carrying a set of messages $\mathcal{M}$ and node B be a neighbor of A.
- Upon an encounter, A wants to know if B is the best forwarder to carry message $m \in \mathcal{M}$ destined to D.
- Let each node have a public (p_k) and private (s_k) keys.

3.3 Routing algorithm (2/3)

- The attribute privacy mechanism works as follows:



3.3 Routing algorithm (3/3)

- Four variants of PRIVO were considered:
  - PrivoASP uses as routing metric *pweight*.
  - PrivoMTTE uses as routing metric the mean time to encounter.
  - PrivoSDBC which is the social version of PRIVO, uses as routing metric weighted similarity to the destination and ego betweenness centrality.
  - PrivoCOMBINED is a combination of PrivoMTTE and PrivoSDBC
- All buffered are sorted based on their TTL.
- PrivoSDBC compares
  - First: the nodes' weighted similarity to the destination
  - Then: the ego betweenness centrality

4. Simulation model

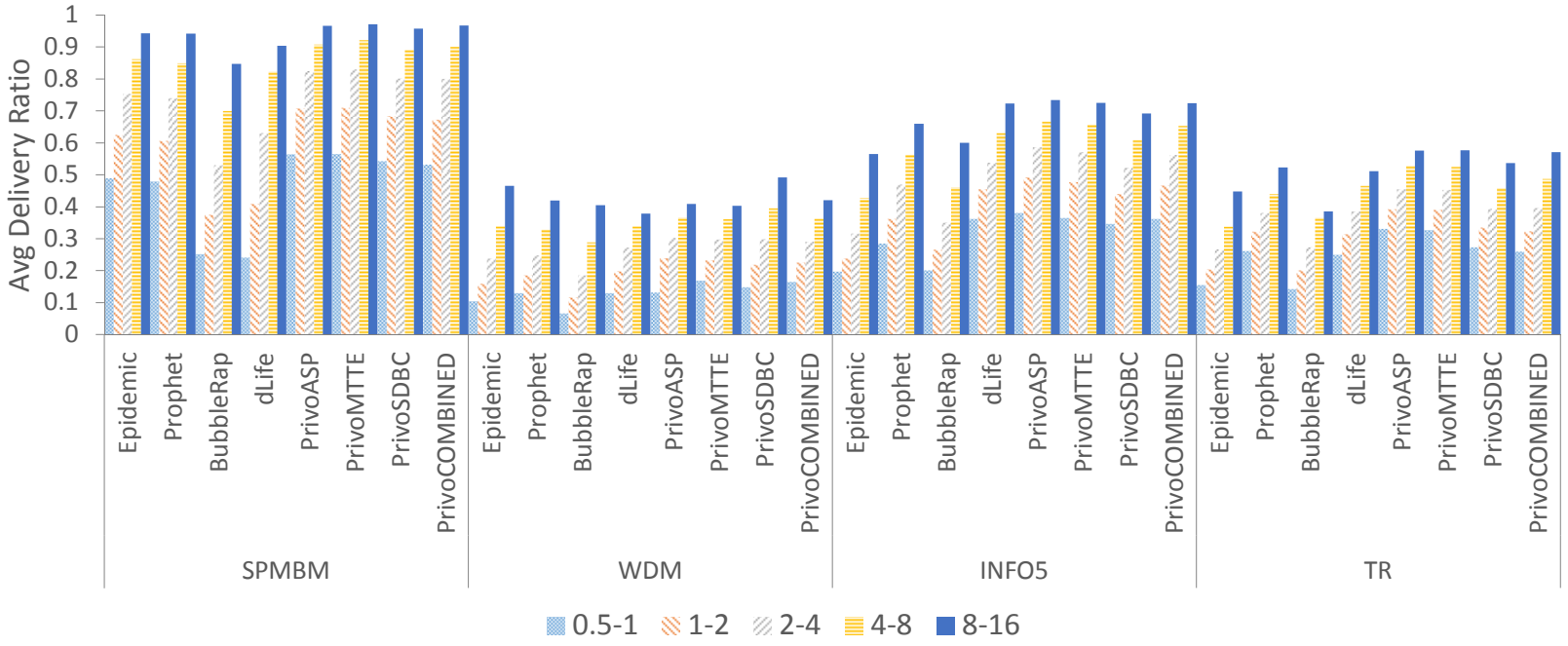
- The ONE Simulator
- Message generation rates: 0.5-1 min, 1-2 min, 2-4 min, 4-8 min, 6-12 min and 8-16 min.
- The length (number) of the timeslots was set to 5 min (288 slots), 10 (144), 15 (96), 30 (48) and 60 (24)
- Synthetic mobility models: Shortest-path Map-Based Movement (**SPMBM**) and Working Day Movement (**WDM**)
- Real mobility traces: CRAWDAD Haggle-one-infocom2005 (**INFO5**) and CRAWDAD Taxicabs in Rome (**TR**)
- Simulation time was set to 7 (synthetic) and 3 (real) days.
- The TTL attribute of each message was around 24 h.

5. Simulation results

- PRIVO variants were evaluated with well-known DTN routing protocols:
  - Two non-social-based routing protocols: Epidemic and Prophet
  - Two social-based routing protocols: BubbleRap and dLife.
- 15 independent simulations using different message generation seeds for statistical confidence.
- PRIVO was evaluated according to the following metrics: delivery ratio, overhead ratio and crypto-graphic cost.
- Information loss (or data utility) due to the use anonymization methods will also be evaluated.

5.2 Routing performance

- Delivery ratio



5.3 Cryptographic costs (1/2)

- Additive homomorphic encryption
  - PC specifications: Intel® CORE™ i7-2600 CPU @ 3.40GHz, 16 GB RAM and Windows 10 Pro (64-bits).

Average Paillier Execution Times (ms)

Key Size	$\mathcal{E}(a)$	$\mathcal{D}(c)$	$\mathcal{E}(a+b)$	$\mathcal{E}(a-b)$	$\mathcal{E}(k \cdot a)$
512	1.73	1.74	0.01	0.38	0.02
1024	11.03	11.29	0.03	0.74	0.05
2048	83.49	83.9	0.06	1.74	0.14

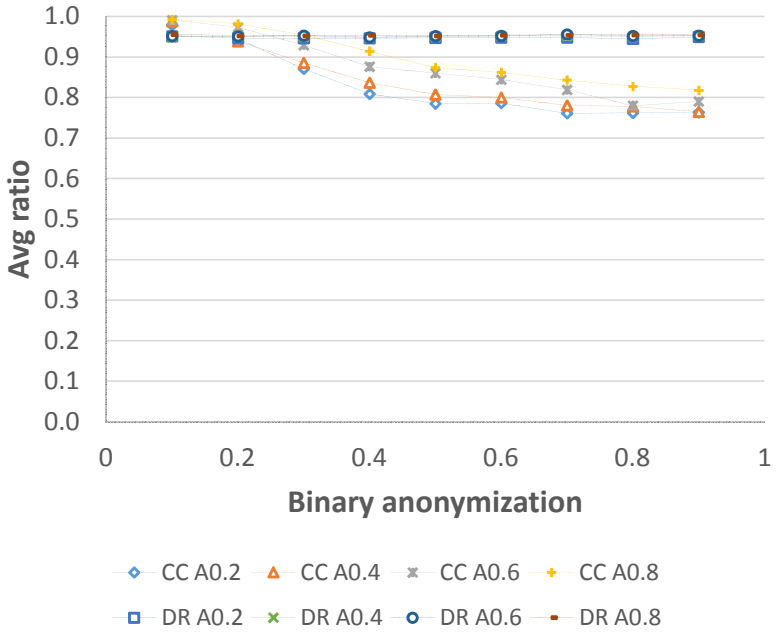
5.3 Cryptographic costs (2/2)

- PRIVO's performance with Paillier
  - Average delivery ratio losses (+) and gains (-) using the Paillier cryptosystem (%)

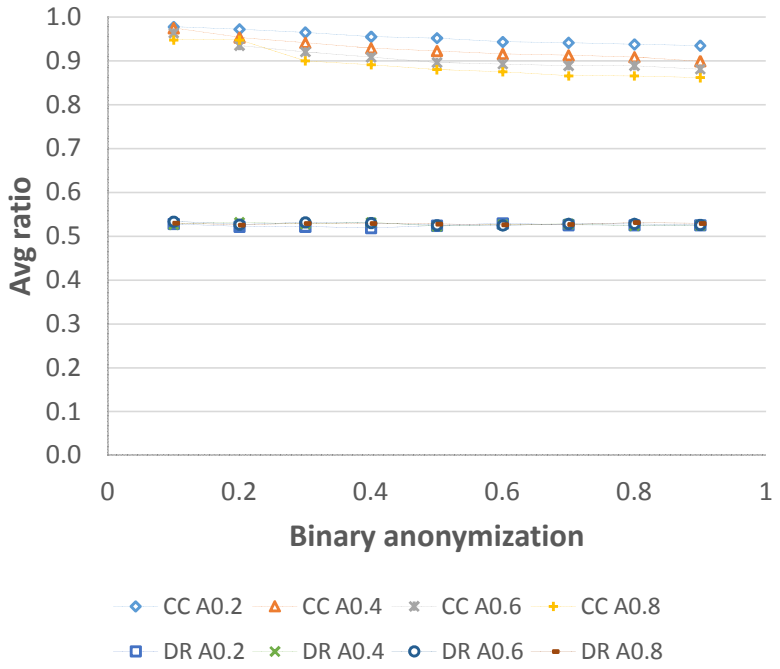
	512 bits	1024 bits	2048 bits
SPMBM	-0.08	-0.01	1.01
WDM	1.11	4.77	21.73
INFO5	0.00	-0.21	-0.09
TR	-0.11	-0.06	-0.88

5.4 Information loss

SPMBM



TR



CC: Correlation coefficient; DR: Delivery Ratio; A: Total Anonymization

6. Conclusions

- This paper proposed PRIVO, a PRIvacy-preserVing Opportunistic routing protocol for DTNs.
- PRIVO ensures
  - *Link privacy* by means of binary anonymization and neighborhood randomization
  - *Attribute privacy* by means of the Paillier homomorphic encryption scheme.
- PRIVO presents on average cryptographic costs below 1% in most scenarios
- If there are some repetitive movement patterns then PrivoSDBC is the best choice, otherwise it is PrivoMTTE

E-Poster Gains Table

Scenarios/Mobility		Key Sizes		
		512 bits	1024 bits	2048 bits
	Shortest-path Map-Based Movement	-0.08	-0.01	1.01
	Working Day Movement	1.11	4.77	21.73
	CRAWDAD Haggle-one-infocom2005	0.00	-0.21	-0.09
	CRAWDAD Taxicabs in Rome	-0.11	-0.06	-0.88