A Privacy Preserving Prediction-based Routing Protocol for Mobile Delay Tolerant Networks

Omar Hasan, Jingwei Miao, Sonia Ben Mokhtar, Lionel Brunie

University of Lyon, CNRS, INSA-Lyon, LIRIS, UMR5205, F-69621, France
E-mail: {omar.hasan, jingwei.miao, sonia.benmokhtar, lionel.brunie}@insa-lyon.fr

October 18, 2013

Motivation

Probability that Alice will Encounter another User

User	Probability
Bob	20%
Carol	80%
Dave	0%
Eve	90%
Frank	50%

Outline

Mobile Delay Tolerant Networks (MDTNs)

Characteristics

- Nodes are mobile
- Nodes communicate via short range wireless communication technologies, e.g., Bluetooth
- Fixed communication infrastructure is not utilized
- An end-to-end routing path may not exist between the source node and the destination node of a message

Routing in MDTNs

Store-Carry-and-Forward

- A message is stored by intermediary nodes and forwarded to nodes closer and closer to the destination node until it is eventually reached

Direct Delivery

- The source node forwards the message only to the destination node
- Low delivery ratio and latency
- Low delivery cost: only one message copy

Epidemic

- A node forwards a copy of the message to every other node that it encounters
- High delivery ratio and latency
- High delivery cost: large number of message copies

Routing in MDTNs

Prediction-Based Routing Protocols

- Try to predict the shortest path based on the mobility patterns of nodes

Routing Mechanism

- A node u forwards the message to a node v if the probability of v encountering the destination node d is higher than the probability of u encountering d
- The probability that a node with a copy of the message will encounter the destination node continues to rise until the message is delivered

Literature

- Bubble [Hui et al. 2011], Habit [Mashhadi et al. 2009], PRoPHET [Lindgren et al. 2003]
- Prediction-based routing protocols perform better than other protocols when nodes exhibit well known mobility patterns [Chaintreau et al. 2007]

The Privacy Challenge

Loss of Private Information

- Prediction-based routing protocols compromise the privacy of nodes by revealing their mobility patterns
- Nodes must divulge the probability that they will encounter the destination

Our Objective

- Take advantage of prediction-based routing, however, reduce the loss of private information

Privacy Preserving Prediction-based Routing (3PR)

Communities

- 3PR is intended for environments in which nodes belong to communities
- Assumption: the nodes in a community are frequently physically collocated and thus the probability of successful message delivery within the community is high

Basic Ideas of 3PR

- 3PR hides the probability that a node will encounter the destination node
- Nodes compare the maximum of probabilities that nodes in their communities will encounter the destination node instead of comparing individual probabilities

Privacy Preserving Prediction-based Routing (3PR)

Intra-Community Routing

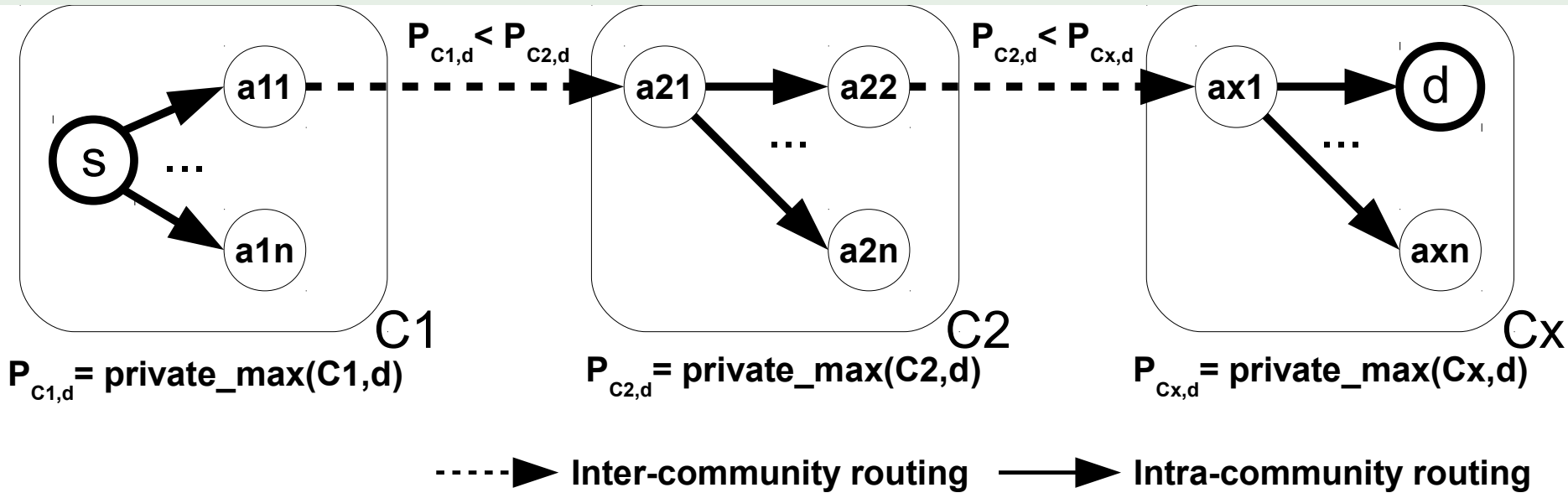
- 3PR disseminates messages inside a community using the epidemic protocol
- Preserves the privacy of nodes by construction
- Efficient for small communities

Inter-Community Routing

- Nodes from different communities compare the **maximum probability in their community** that a given node will encounter the destination
- The maximum probability in a community is periodically computed by the nodes that belong to that community using our Private Maximum protocol

Privacy Preserving Prediction-based Routing (3PR)

Example



Privacy Preserving Prediction-based Routing (3PR)

Loss of Private Information bounded by the Maximum

- The adversary learns that node u's probability of encountering the destination node is no higher than the maximum
- However, the adversary can learn whether node u is the one who has the maximum, no better than a random guess with probability $1/h$, where h is the number of honest nodes in the community

Private Maximum

Private Maximum

- Take a private input from each node and find the **maximum** without revealing any of the private inputs

Example

- Private inputs: **90, 92, 79**
- Maximum: **92**

Private Maximum

Literature for Private Maximum and Private Sum

- Kreitz et al. 2010
- Sheikh and Mishra 2010
- Hasan et al. 2012

Challenges

- No Trusted Third Parties (TTPs) can be assumed
- Nodes have no prior knowledge of connected nodes (the nodes that they will encounter)
- Messages may arrive after long and variable delays

Private Maximum

Protocol: Step 1

1. Each node represents its private number in binary form

Example

Node	**Private Number**	**Binary**
u	90	1011010
v	92	1011100
w	79	1001111

Private Maximum

Protocol: Steps 2–7

2. Compute the sum of the Most Significant Bits (MSBs)
3. A node u does not have the maximum if its MSB is zero but the sum is not zero
4. Node u submits zero to all subsequent sums
5. Compute the sum of the next MSBs
6. Continue until the least significant bit
7. The node with the maximum learns this fact

Example

Node	**Private**	**Binary**	**Most Significant Bit Submitted**						
			6^{th}	**5^{th}**	**4^{th}**	**3^{rd}**	**2^{nd}**	**1^{st}**	**0^{th}**
u	90	1011010	1	0	1	1	0	0	0
v	92	1011100	1	0	1	1	1	1	0
w	79	1001111	1	0	0	0	0	0	0
		Sum of Bits:	3	0	2	2	1	1	0

Private Maximum

Protocol: Steps 8–10

8. Compute the sum of the private numbers; the node with the maximum submits its true input
9. Compute the sum of the private numbers; the node with the maximum submits zero
10. Compute the difference of the two sums to obtain the maximum

Example

Node	**Private Number**
u	90
v	92
w	79
Sum Round 1 (Node v inputs the maximum):	261
Sum Round 2 (Node v inputs 0):	169
Difference = Maximum:	$261 - 169 = 92$

Private Sum

Private Sum

- Take a private input from each node and compute the **sum** without revealing any of the private inputs

Example

- Private inputs: **90, 92, 79**
- Sum: **261**

Private Sum

Protocol: Steps 1–3

1. The initiating node floods an *init* message to all nodes in the community
2. When a node u encounters another node v in its community, u sends a random number r_{uv} to v, and u receives a random number r_{vu} from v
3. After node u has encountered k nodes, the node computes the sum of its private number and all random numbers received minus all random numbers sent

Node u's Individual Sum

$$\sigma_u = p_u + \sum_{j=1}^{k} r_{vu} - \sum_{j=1}^{k} r_{uv}$$

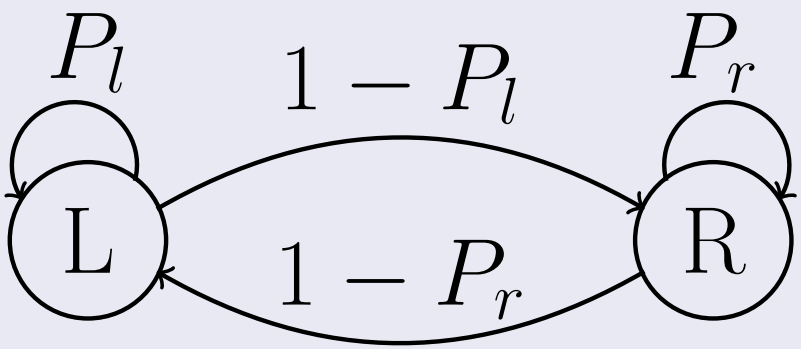
Protocol: Steps 4–6

4. Node u sends σ_u to the initiating node
5. The initiating node waits for individual sums from all nodes in the community
6. The initiating node computes the final sum

Mobility Model

- Simulations based on a well established community-based mobility model [Spyropoulos et al. 2006, Dang et al. 2010]
- Each community is associated with a geographical area
- The movement of a node consists of a sequence of *local* and *roaming* epochs

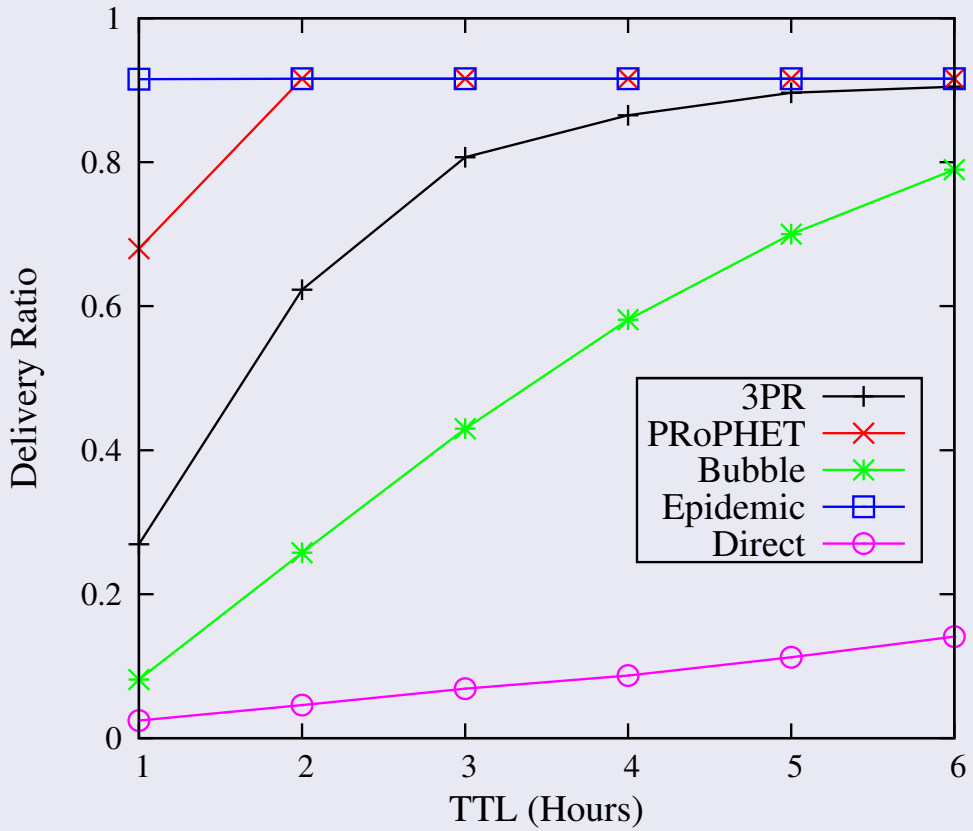
State Transition between Local and Roaming Epochs



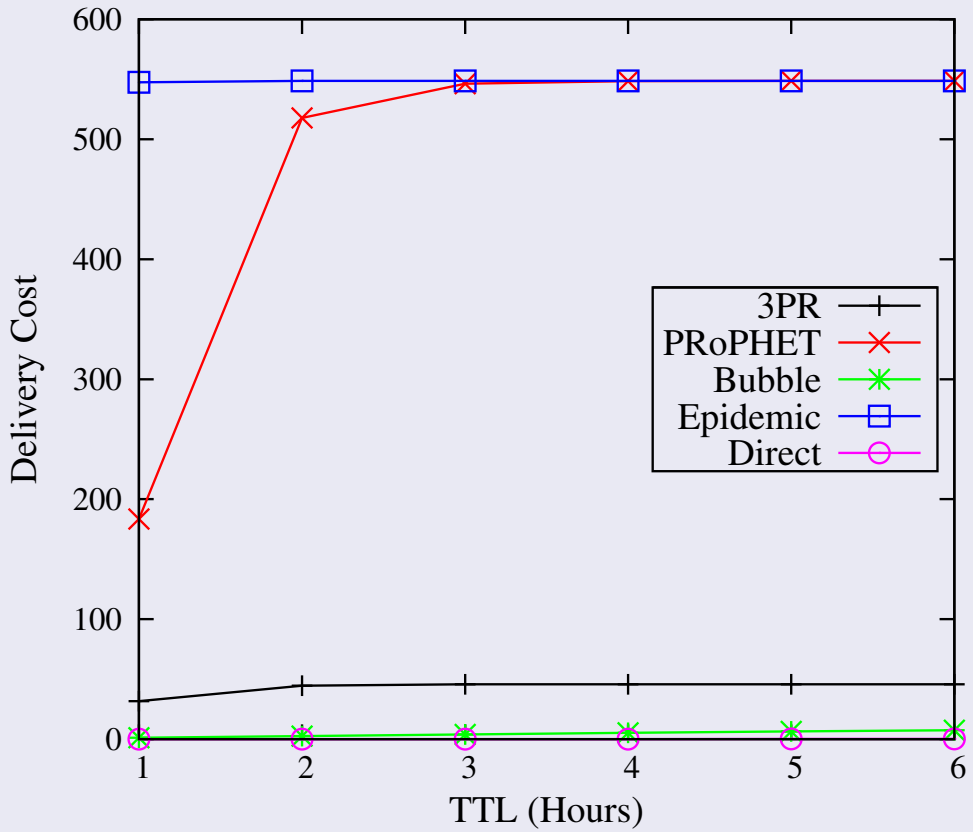
Simulation Settings

Parameter	**Value**
Simulation area	3000×1500 m^2
Transmission range	10 m
Simulation duration	12 hours + TTL
Message generation rate	1 message every 30 seconds
Number of communities	12
Number of nodes in a community	Between 10 and 50
Node speed	1.34 m/s
P_l	0.8
P_r	0.2

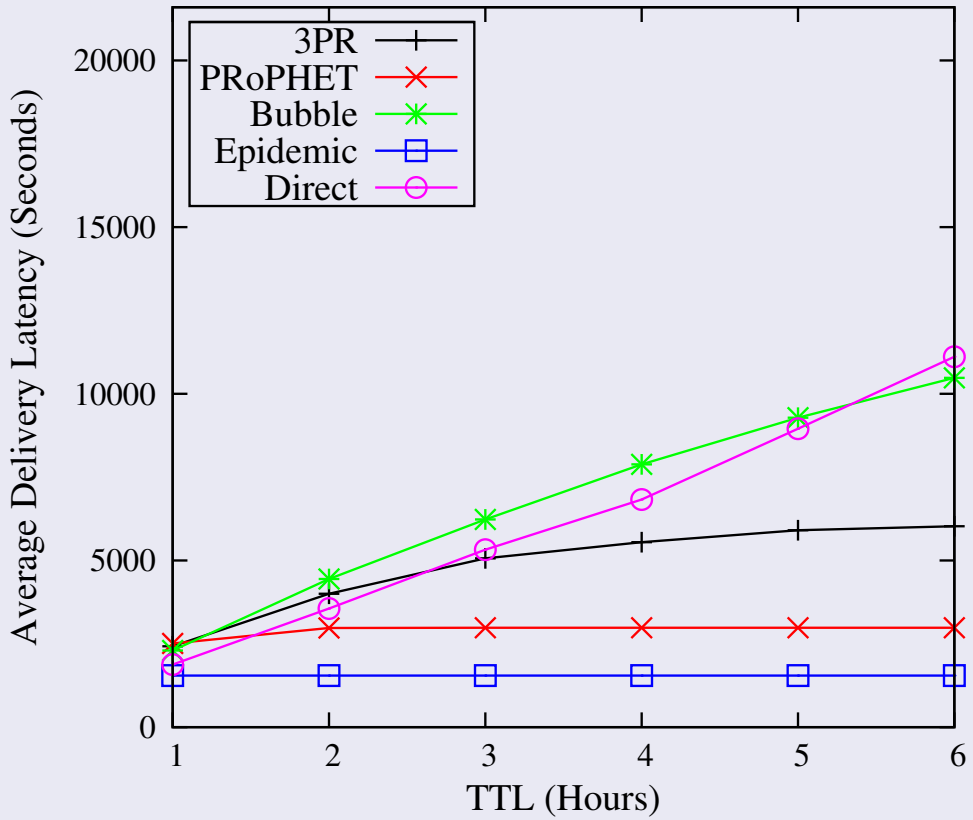
Delivery Ratio



Delivery Cost



Delivery Latency



Conclusion and Future Work

Conclusion

- Nodes compare the maximum probabilities that nodes in their communities will encounter the destination node instead of comparing individual probabilities
- Private Maximum and Private Sum protocols that do not rely on trusted third parties, do not assume prior knowledge of neighbor nodes, and assume long and variable message delays
- Comparable performance to existing prediction-based routing protocols

Future Work

- Analysis of the house keeping costs
- A protocol that hides even the maximum probability
- A protocol that compares the probability that any given node in a community will encounter the destination node