Onion Routing in Predictable Delay Tolerant Networks

Adrián Antúnez Veas

dEIC, Universidad Autónoma de Barcelona

Julio, 2015

1. Background
2. Motivation and objectives
3. Proposal
4. Security Analysis
5. Evaluation
6. Conclusions

DTNs overview

Definition

Delay and disruption tolerant networks.

Based on the *store-carry-and-forward* principle.

Some applications...

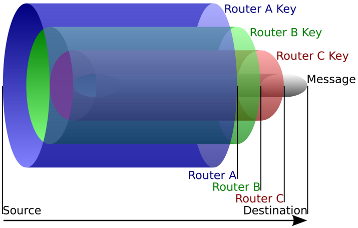
- Lacking continuous connectivity.
- Long or variable delays.
- Achieve independent network.

Onion routing overview

Source S wants to send an anonymous message to C (destination).

Onion routing phases

1. S chooses a path $p = (S), A, B, C$ from source to destination.
2. S encrypts the message with the pre-shared key of C, B and A.
3. S sends the message.



Oracle schemes overview

Definition

Oracle schemes have knowledge of the network and its evolution.

Contacts oracle

Contacts oracle can answer any contact related question between two nodes in any point in time.

Predictable (deterministic) DTNs

Networks where the behaviour is known in advance or where a repetitive action occurs over time.

Motivation and objectives

Main objective

Achieve anonymous communications over an independent network.

Onion routing along with predictable DTNs

- Find a way to represent the contacts of the network.
- Find a method to perform the previous path selection step.
- Security analysis of our proposal.
- Show how this method performs in a real scenario.

Contact representation

Structure used

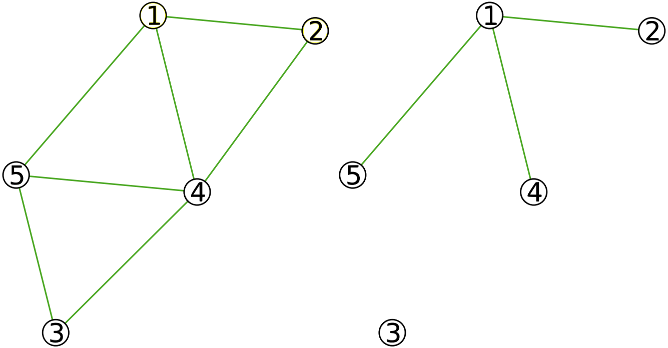
A dynamic graph $G = (V, E)$ as a way of contact representation.

- *G:* Dynamic graph representing the evolution of the network.
- *V:* Each node of the network is represented by vertices.
- *E:* Each contact between nodes is represented by edges.

Each edge will have two attributes

- Instant of time when the contact began.
- Duration of the contact.

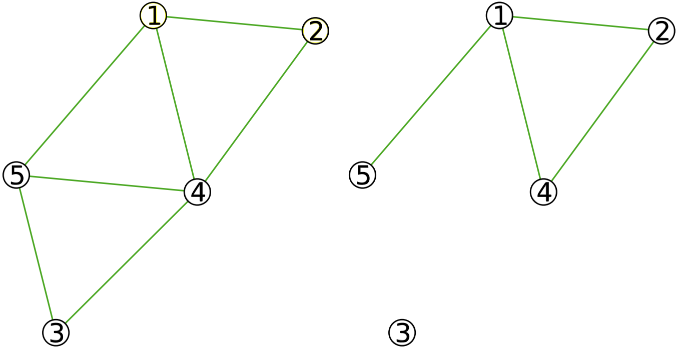
Dynamic graph example



(a) Complete graph

(b) t=0

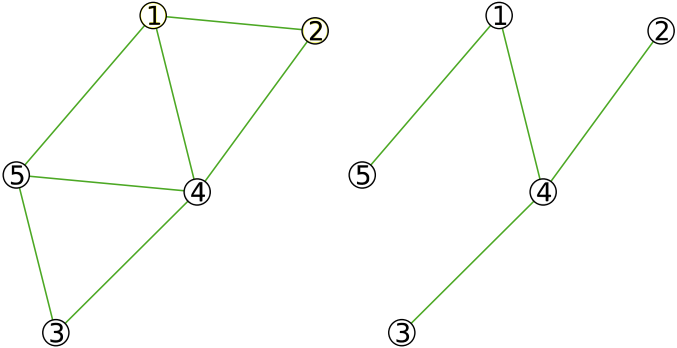
Dynamic graph example



(a) Complete graph

(c) t=1

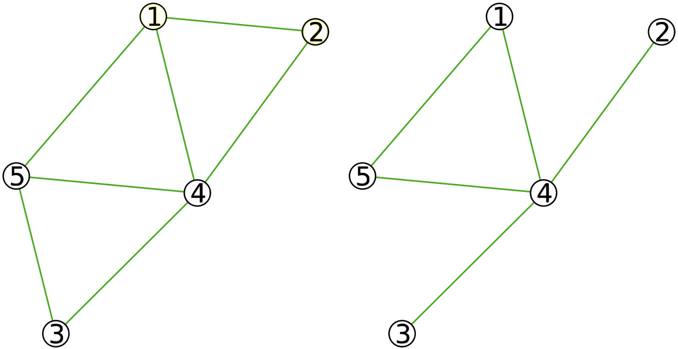
Dynamic graph example



(a) Complete graph

(d) t=2

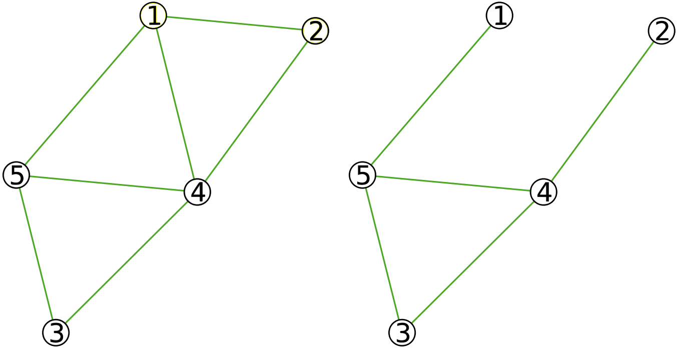
Dynamic graph example



(a) Complete graph

(e) t=3

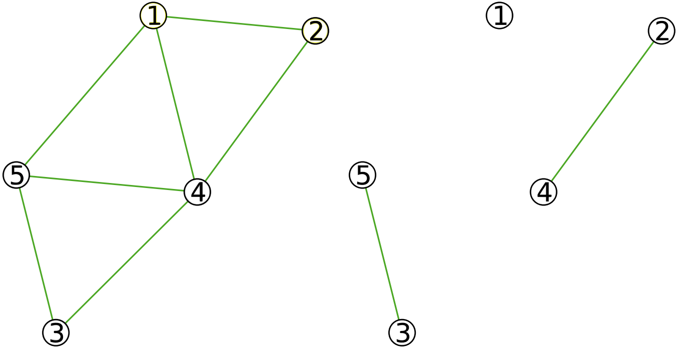
Dynamic graph example



(a) Complete graph

(f) t=4

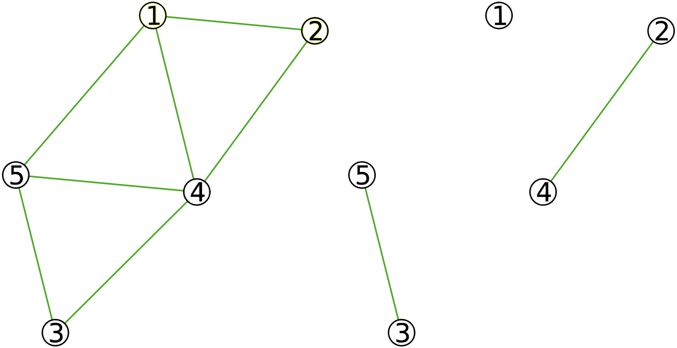
Dynamic graph example



(a) Complete graph

(g) t=5

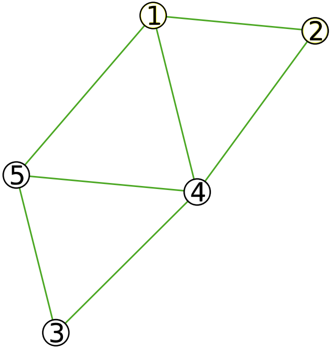
Dynamic graph example



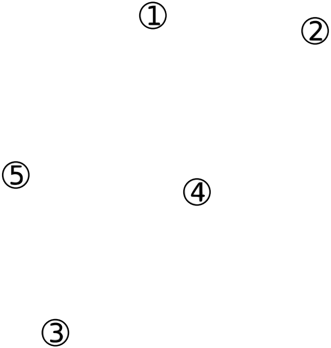
(a) Complete graph

(h) t=6

Dynamic graph example



(a) Complete graph



(i) t=7

Path selection

The necessity

In onion routing a path to perform the layering process is needed.

The method

A deterministic method *f(s, d, t, n, k, tt)* is defined.

- *s*: Source node.
- *d*: Destination node.
- *t*: Time when the message is sent.
- *n*: Number of nodes in each path.
- *k*: Maximum number of paths to be returned.
- *tt*: Transmission time.

Security Analysis

Goal

Reveal who sent the message (uncover the source).

Attack types

Can be divided in two groups:

- Active: Actions against nodes or message modifications.
- Passive: Just observing user traffic patterns from nodes.

Active attacks

- Denial of Service (DoS) attacks to neighbour nodes.
- Message modifications.
- Masquerading (nodes pretending to be others).

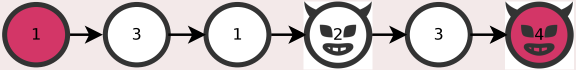
Passive attacks

Passive attacks

- Learn from the content of the message.
- Sending node periodicity analysis.
- Set of compromised nodes working together.

Example

- Node 1 sent an anonymous message to node 4.
- Node 1 message's contains a timestamp.
- Nodes 2 and 4 have been compromised.
- Node 5 never has sent or has forwarded a message yet.



NS-3 simulation scenario

NS-3 definition

NS-3 is a discrete-event simulator targeted primarily for research.

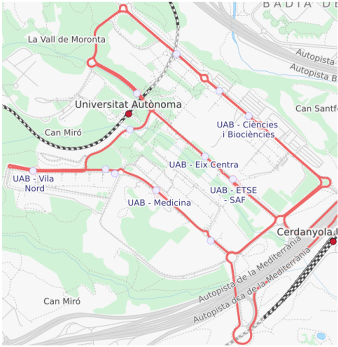
Implementation details

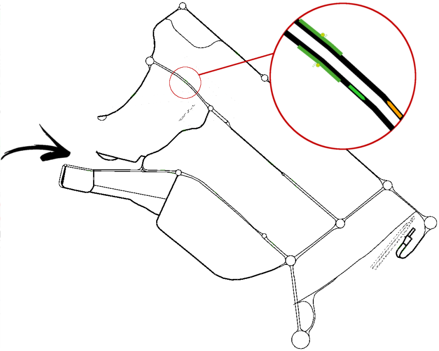
- Implemented neighbour discovery on the application layer.
- The app polls every second to find new contact opportunities.
- If contact is missing for 2 seconds, contact has been lost.

Mobility model

UAB campus buses

- Very small public transportation network (5 buses).
- Every single bus makes the same route daily (deterministic).
- Each bus 802.11b Wi-Fi hotspot with a range up to 100m.





Simulation results

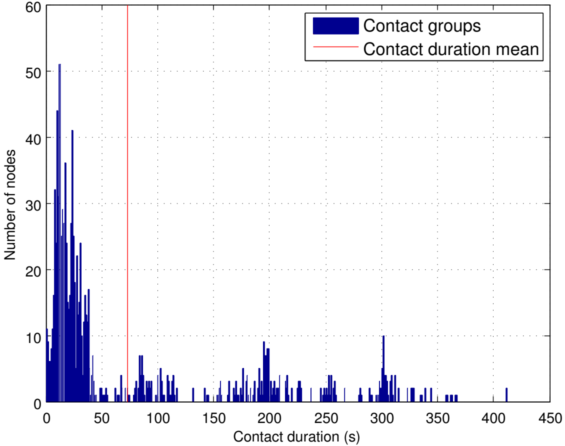


Figure: Contacts duration.

Simulation results (II)

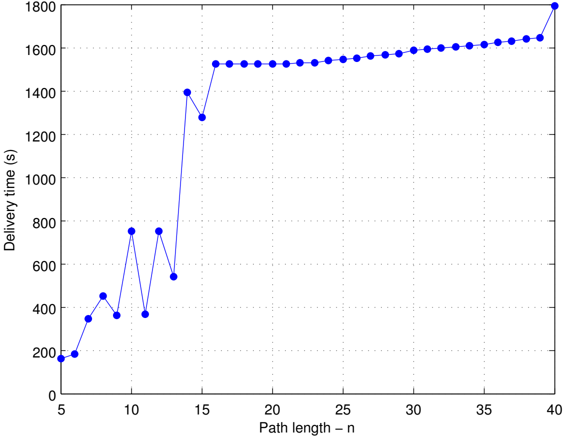


Figure: Average delivery time considering the variation of the path length (k=10 was fixed).

Simulation results (III)

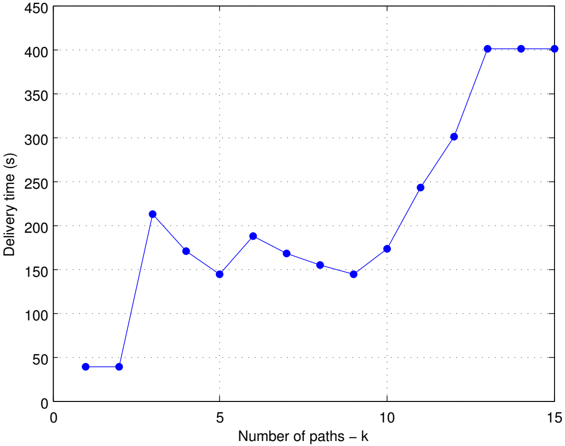


Figure: Average delivery time considering the variation of the number of paths (n=5 was fixed).

Conclusions

Conclusions

- We proposed a method to use onion routing in DTNs.
- In DTNs not always the shortest paths are the quickest ones.
- In our method, new paths selection are not correlated to time.

Future work

- Search and analyse efficient ways of path selection.
- Decrease the number of attacks using reputation systems.
- Adapt contact representation to consider traffic modifications.