Onion Routing in Predictable Delay Tolerant Networks

Adrian Antunez-Veas and Guillermo Navarro-Arribas

Department of Information and Communications Engineering,
Universitat Autònoma de Barcelona (UAB), 08193 Cerdanyola, Spain
{aantunez, gnavarro}@deic.uab.cat

Abstract Abstract goes here

Keywords: Onion Routing, Delay-tolerant Network, Anonymous networking, Privacy, Security

1 Introduction

Delay Tolerant Networks (DTNs) are a class of networks aimed to provide end-to-end communication into environments lacking continuous connectivity or with long delays. DTNs can also be used as a communication alternative when the internet internet network can not be trusted, e.g: unknown Wi-Fi hotspots.

DTNs use the store-carry-and-forward principle, i.e: the node stores the message (bundle) received , carrying it if is needed and forwarding it when a connection opportunity occurs.

Due to the nature of the DTNs the routing decision has been challenging since the beginning.

The main problem w this kind of networks is mainly the routing and the security of the data exchanged. On the one hand due to the nature of the nodes of the DTN could be under continuous movement making the routing of the data a difficult task. On the other hand . . .

Onion routing is used to protect the communications online allowing to hide the origin or the source of the information as well as the data itself to the rest of the nodes that forwards the information.

DTN Oracle: Information of the network as contact information (time of the contact and duration) and the public key of every single node of the network, in order to be able to do the Onion Routing.

2 Related work

Aim of this section: Show the existing research about this topic. Identify his flaws and explain briefly what we do to solve (or improve) them.

3 Proposal

Aim of this section: Brief introduction of what are we going to talk about in this section.

3.1 Onion routing overview

Aim of this section: As the onion routing is quite important in this research, explain briefly how it works.

First, we provide a high-level description of how the onion routing works ...

3.2 Oracle networks overview

Aim of this section: As the oracle network is used, explain briefly how it works.

First, we provide a high-level description of how the onion routing works ...

3.3 Key Management in DTNs

Aim of this section: In DTNs the Key Management is challenging, explain how we get rid of this problem: pre-shared keys as in public transportation networks nodes are known in advance.

3.4 Path choosing

Aim of this section: Explain what we did to get some useful paths according to a set of given parameters. Is important to explain the dynamic graph part, the algorithm itself, etc. **All theoretically!**

Put some example showing the graph or the tree?

Important to remark!: Non efficient algorithm, needs to be improved but it is just a prove of concept of deterministic choosing.

4 Security analysis

Aim of this section: Brief introduction of what are we going to talk about in this section.

4.1 Threat model

Aim of this section: Define against who we try to defend our data. What the attacker may or may not do. Define some considerations such as sufficient strong cryptographic algorithms with sufficiently long keys to prevent practical cryptanalysis attacks.

4.2 Passive adversaries

Aim of this section: Needs to be defined. I am not even sure if this kind of adversaries will be in our proposed model.

4.3 Active adversaries

Aim of this section: Needs to be defined. I am not even sure if this kind of adversaries will be in our proposed model.

5 Evaluation

Aim of this section: Brief introduction of what are we going to talk about in this section.

In this section the security of our proposal is evaluated using a realistic scenario providing information about the devices and other parameters used in the evaluation.

5.1 Scenario: Campus buses

Aim of this section: Explain a bit how the campus scenario works and how can be this useful in practice.

In order to test our proposal we considered a very little public transportation network that works inside the Autnonomous University of Barcelona (UAB) composed by 5 buses that makes different routes around the UAB campus.

Each bus has a DTN node achieving secret communications as well as source anonymity using this network. There are several applications that can take profit of such networks like anonymous reporting systems.

5.2 Mobility Model

Aim of this section: explain how we get this scenario: open street maps -> sumo -> ns-3...

We obtained the mobility model going along different stages. First, we exported the UAB Campus map from OpenStreetMaps into SUMO [?] software, filtering some unnecessary items with the Java OpenStreetMap editor [?] tool.

Once the campus roads was imported in SUMO, we recreated the bus movements of each bus taking into consideration the official bus schedule of the UAB public transportation network [?]. In addition, we tuned some bus characteristics like acceleration and deceleration parameters in order to get coherent travel times.

Finally, we exported the model to a the NS-2 mobility trace as is explained in [?]. The NS-2 mobility trace can be used with the well-known Network Simulator NS-3. We used the simulator to obtain important contact related data of the campus network, i.e: information about the duration of the contacts as well as the instant of time when they occurred.

5.3 Simulation setup

Aim of this section: Explain and define the values used in the simulation itself as well as how we know that there is a neighbour able to contact with.

5.4 Simulation results

Aim of this section: Explain the results of this simulation. What we get and explaining why.

6 Conclusions and future work

Aim of this section: There are two parts:
The first one the conclusions of this project. What we can extract from our research. Could be useful? Important things that needs to be remarked, etc.
The second one the future work. What needs to be done in the future to solve some undesired behaviours, explore unresearched lines of this work, etc.

[Conclusions part]

[Future work]

Search and analyse efficient ways of path choosing, being able to use the algorithm in resource-constrained computers.

In the network could exist black holes, i.e: nodes that drop all the traffic. In order to mitigate the impact of such nodes in the whole network a reputation system could be used. By this way the reputation value will be shared among all the nodes in the network. The path choosing algorithm should be modified too to take this value into consideration in the choosing process. Finally this will lead into another security analysis due to the more reputation a node has, most probable is to be one of the chosen.

The simulation model could be adapted to consider traffic modifications, generating the enough information to decrease the number of failed contacts due to a bad contact prediction.

Acknowledgments Acknowledgments go here.

References

All links were last followed on June 13, 2015.