Donar: Anonymous VoIP over Tor

Yérom-David Bromberg, Quentin Dufour, Davide Frey, Etienne Rivière

nsdi'22 - April 4, 2022 - Renton, WA, USA

Univ Rennes, Inria, CNRS, IRISA - UCLouvain, Belgium
Tor’s limitations

High latency hinders Tor’s adoption for interactive applications like VoIP
Our system requirements

Preliminary definitions

- **Interactive call**: 99th-perc delay < 360 ms
- **Call duration**: 5 min avg, up to 90 min

System requirements

- **Interactivity**: interactive calls > 80%
- **Stability**: dropped calls < 2%
- **Anonymity**: both caller and callee

❓ Can Tor satisfy these requirements?
Which Tor configuration should we use?

For 2-way anonymity: Onion Services

Security-first

6 relays, 3-hop circuits

To reduce latency: Reduce circuits length

2-hops circuits have been discussed as a possible optimization²

Performance-first

4 relays, 2-hop circuits

²Kevin Bauer et al. “On the optimal path length for Tor”. In: HotPets in conjunction with PETS 2010
How do we test Tor?

2 Tor Configurations

Simulated Calls
5-minute and 90-minute calls
Each configuration is repeated 64 times

Questions
Do Onion Service meet latency requirements?
Do Onion Service are stable enough?
Do onion services meet latency requirements?

Interactive call definition
99\textsuperscript{th}-perc delay < 360 ms

System interactivity
> 80\% goal, of interactive calls
9\% for 5-minute calls
3\% for 90-minute calls

Calls are not interactive
And what if we use 2-hop circuits?

Interactive call definition
99\textsuperscript{th} perc delay < 360 ms

System interactivity
> 80\% goal, interactive calls
44\% for 5-minute calls
23\% for 90-minute calls

Calls are still not interactive
Are onion services stable enough for calls?

System stability

- **< 2%** goal, dropped calls
- **5%** for 2 hops, 5-minute calls
- **10%** for 3 hops, 5-minute calls
- **10%** for 2 hops, 90-minute calls
- **17%** for 3 hops, 90-minute calls

Calls are not stable
Our contribution: Donar
Our goal

Building a communication abstraction to provide stable low-latency packet delivery over the existing Tor network
Donar Overview

Donar is a **multipath** proxy made of 2 components:

- Link Selection
- Scheduling Policies
We want to schedule only on fastest links
Bob ranks paths and informs Alice that stops using the slowest ones.
Alice selects a new path
Link Selection

Path Ranking
1. F
2. A
3. D
4. B

Ranking is re-computed regularly
Alternate schedule packets across links and leverages Tor’s padding
Scheduling Policy: Double Send

Double Send extends Alternate by adding on-wire duplication.
Multiple paths = less security?

Guards = Fixed relays = Decouple path opening from de-anonimization

Legend

<table>
<thead>
<tr>
<th>Tor Relay</th>
<th>Tor Circuit</th>
<th>Anonymous</th>
</tr>
</thead>
</table>

Icons by RROOK and Juan Pablo Bravo from the Noun Project
Evaluation
Evaluation Setup

Configurations & Goals:
Same as our preliminary analysis

Our 2 Variants

Donar Alternate
Scheduling policy: Alternate (use less bandwidth)

Donar Double Send
Scheduling policy: Double Send (better stability)
Implemented in C, notable API/lib: epoll, gstreamer, glib

Baselines

Simple: Baseline introduced in the preliminary analysis
Torfone: Duplicates packets on 2 paths
Donar on 2-hop circuits

System interactivity

> 80% goal, interactive calls
87% for Donar Alternate
95% for Donar Double Send
25% for Torfone
23% for Simple (our baseline)

- Donar Alternate
- Donar Double Send
Donar on regular circuits

System interactivity
> 80% goal, interactive calls
58% for Donar Alternate
87% for Donar Double Send
31% for Torfone
3% for Simple (our baseline)

Donar Alternate
Donar Double Send
Does Donar maintain calls over time?

System stability

< 2% goal, dropped calls

- 0% Donar Alternate, 2 hops
- 0% Donar Double Send, 2 hops + default

Donar Alternate
Donar Double Send
Conclusion
We contributed Foundations to build a Tor softphone with stable latency over the existing Tor network. Source code: github.com/CloudLargeScale-UCLouvain/Donar

Insights to understand delays on Tor from a real-time perspective
Thanks to the audience for attending this talk.

Our email addresses:

- david.bromberg@irisa.fr
- quentin@deuxfleurs.fr
- davide.frey@inria.fr
- etienne.riviere@uclouvain.be

Source code: github.com/CloudLargeScale-UCLouvain/Donar

Time for questions!