A non-technical Overview of the RiseApp Project

Leonardo Maccari
September 1st, 2014

Motivation

*The goal of the **RiseApp** project (www.riseapp.org) is to help people that are rising up against regimes and want the whole world to witness their protest. RiseApp will be an open source mobile phone application to share and publish media contents in risky situations (such as protests and riots) when Internet connectivity is filtered, censored or temporarily blocked. RiseApp is still in its early stages of design; the goal of this document is to gather contributions to shape RiseApp in a way that will make it useful in real world scenarios. The idea will be described with a non-technical language conceived for activist wishing to help improve the project. Using the feedback I receive to this document, I will design the application and apply for funding to the CHEST open call (www.chest-project.eu) in order to gather the resources needed to realize it.*

If you're interested and you think you can contribute, please read on, in the last section you can find ways to contact me and send me your opinions and feedback. You are also encouraged to share this document with whoever you think may be interested.

1 Introduction

The freedom to assemble peacefully is being increasingly violated in many countries around the world. Many peaceful protests are treated as riots by authorities, violently repressed and silenced by the media. In these cases it is extremely important to shed light on violation of human rights and distribute the evidence that repression is really happening. Pictures, video, audio and any other media can let the world know that there is a protest, and that authorities are trying to silence it with violence. We have recently witnessed in several cases how the spread of information played a role in such situations. Anyway, to achieve this goal is not as easy as it would seem, for many reasons, among which:

Forced disconnections:

In many critical situations authorities try to shut down the access to the Internet, or filter the access to social networks. When Internet is filtered it is hard to publish media on social networks or any other platform.

Media can be seized:

Police often seizes mobile phones and cameras when people is arrested or simply stopped. All the media are lost before they can be published.

Surveillance of Social Media:

Authorities are always monitoring the social networks and there are many pieces of evidence of people being arrested or intimidated for their on-line activity. In many countries service providers are forced by law to cooperate with authorities and are subject to strong pressure to reveal private information. The NSA scandal in the U.S.A. is an example of how this daily happens also in liberal democracies.

The goal of RiseApp is to support people fighting for their rights increasing the visibility of the protests (and their repression). RiseApp will be based on technologies that enable two key features: the circumvention of filters and temporary disconnections and the preservation of the users' anonymity.

2 The Building Blocks

RiseApp will have two main features. The first is the possibility of uploading media on the internet using the Tor network in an anonymous and secure way. The second is the ability to direct exchange media between mobile phones without the need of any infrastructure (so-called, *ad-hoc networking*). Before entering the details of how RiseApp will work I need to briefly describe these two technologies.

2.1 The Tor Network

Tor (The Onion Router) is a complex network of servers that is used by activists in all the world to escape censorship and anonymously publish their information online[1].

When you use Tor to navigate the web, instead of taking a direct route from source to destination, data packets take a random pathway through several relay servers on the Tor network. This covers your tracks so no observer at any single point can tell where the data came from or where it's going. To create a private network pathway Tor incrementally builds a circuit of encrypted connections through relays on the network. No individual relay or eavesdropper ever knows the complete path that a data packet has taken. Figure 3 shows how a mobile phone outside of the Tor network can use Tor to anonymously and safely browse any web server.

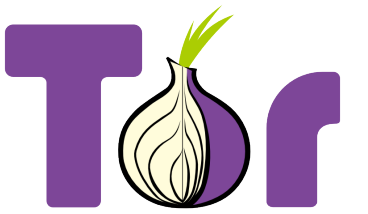


Figure 1: The Onion Router logo.

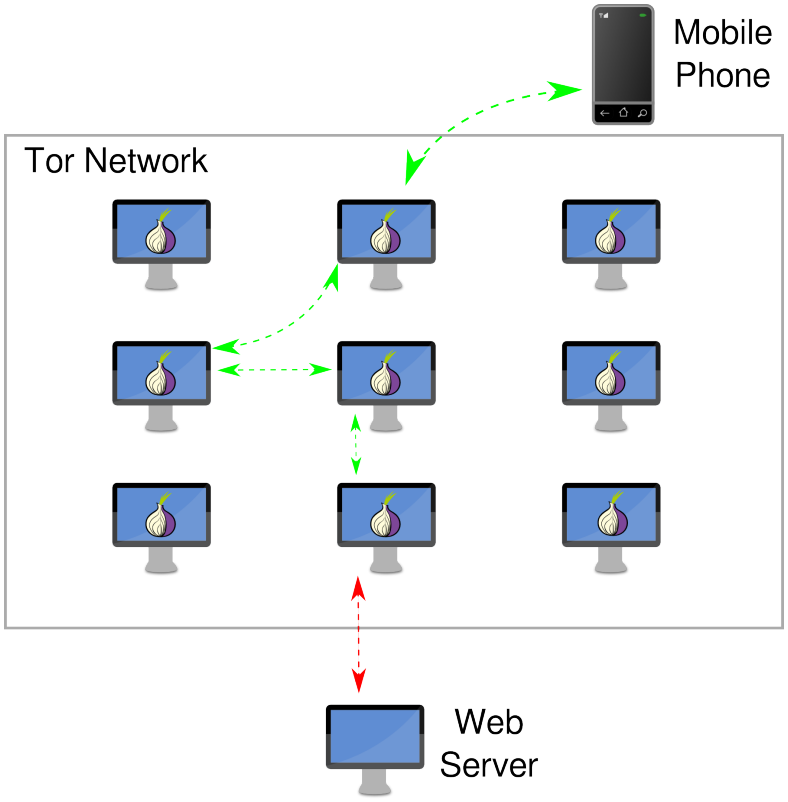


Figure 2: How Tor works, green links are encrypted, red ones may not be.

[1]Most of the text from this section comes from the Tor website, www.torproject.org

This means that your network provider can not filter your traffic or spy on you, because he can not access unencrypted data, including the address of the website you are navigating to.

Tor also makes it possible for users to hide their locations (their IP address) while offering various kinds of services, such as web publishing. A *hidden service* is a web server hidden in the Tor network, nobody would be able to determine who is offering the site, and nobody who offered the site would know who is visiting it. This hidden service functionality allows Tor users to set up a website where people can anonymously publish material that is extremely hard to censor.

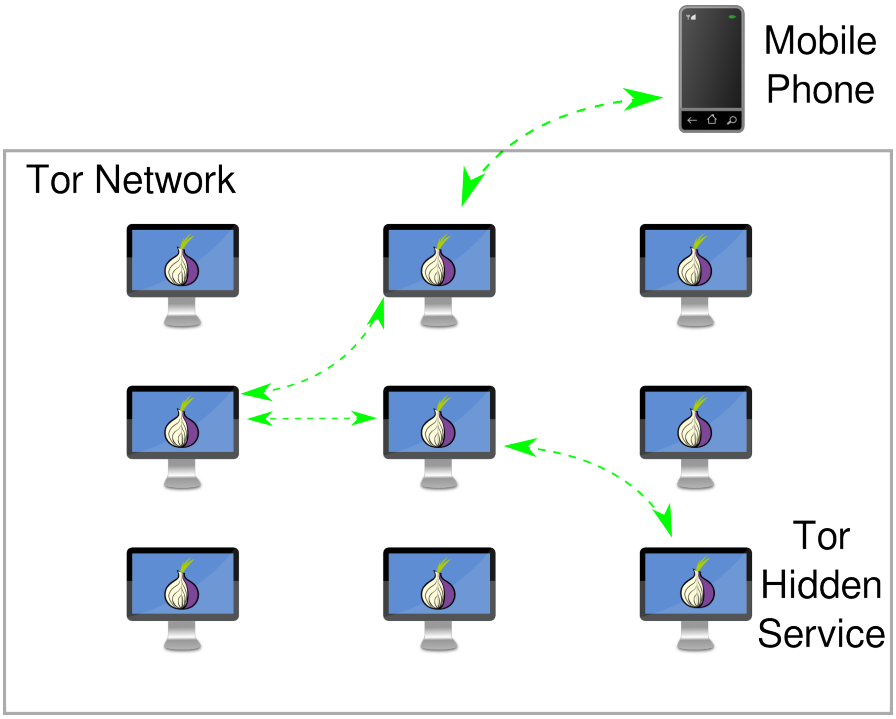


Figure 3: How hidden services works, green links are encrypted.

To date Tor has been subject to various kinds of attacks, even by the NSA, but there is no evidence that its overall security has been compromised.

2.2 Ad-hoc Networking

Mobile phones, and computer in general do not need an infrastructure to communicate with each other. Even outside a Wi-Fi hotspot or without an available cellular network they can communicate over short distance via wireless, creating an ad-hoc network. This feature is largely unused, mostly because the vendors do not have interest in giving full support to it, but recent applications are starting to use it.

Imagine that several people use RiseApp in a public demonstration to shoot photos and videos. RiseApp will let users directly exchange their media during protests so that media don't get lost if a mobile phone is seized or destroyed. The goal of this exchange is that at the end of the demonstration the media will be spread over the highest number of mobile phones without relying on any fixed infrastructure. If a device is seized or destroyed, not all its content is lost with it.

During that event there are three possible modes for the exchange of media based on ad-hoc networking:

1. Two people will intentionally share media when they meet. This involves approaching the mobile phones and enabling the share of selected media. The exchange is bi-directional.
2. In the area of the event there will be a set of wireless collection points, that are access points that are running RiseApp. When users get close to such collection point they will intentionally upload the media they have in the collection point and receive other content in return.
3. People will exchange media in an automatic and unplanned way. Each mobile phone will sense the presence of another mobile phone equipped with RiseApp in the vicinity and exchange media whenever possible. No voluntary interaction is needed from the owners.

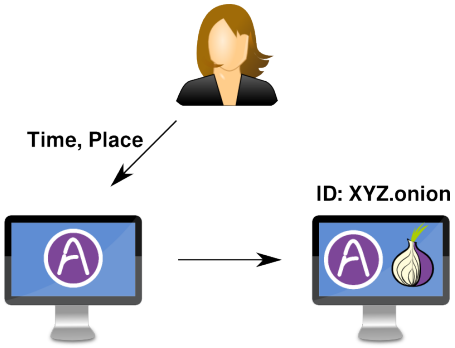
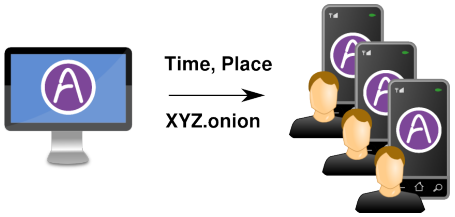
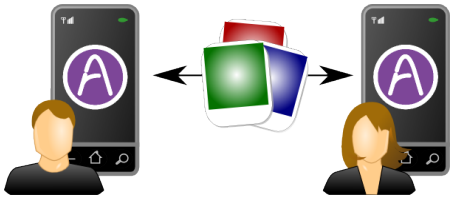
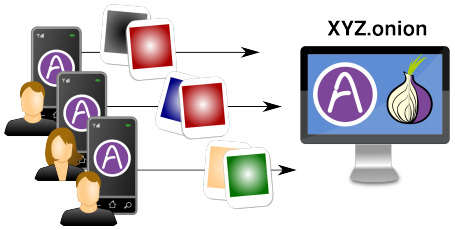
Whenever a mobile phone or collection point reaches internet connection it will upload the media it contains on the internet using Tor, so that the majority of the media will reach a large audience. The three modes for the exchange of media can be composed. At the current state of design, the first two seem technically feasible, further study is needed to assess the feasibility of the third one.

3 How RiseApp Will Work

This section describes how RiseApp will use Tor and ad-hoc networks to fulfill its purpose. Please keep in mind that this is an extreme simplification and that the design may change with time. RiseApp will be made of three components:

The public website www.riseapp.org available via any browser, (with or without using Tor).	
A web service to collect all the media related to a specific event. An instance of this service is activated for each running event. This software runs as a hidden service in the Tor network so it is hard to censor and can be browsed anonymously. It is a public service, anyone with its address can reach it using Tor.	
The mobile application	

The workflow to use RiseApp is made of a few steps:

I	An activist visits riseapp.org and creates a new hidden service for an upcoming event, specifying the time and place of the event. The service is generated automatically with a new ID.	
II	riseapp.org will periodically update all the instances of the RiseApp application with the list of the upcoming events. Users will select the one that they will participate to.	
III	During the event people will share media, in order to minimize the chance that media gets lost or doesn't reach the Internet	
IV	Whenever any RiseApp application reaches Internet connection, it will upload all the stored media to the hidden service. Tor guarantees that this will happen in an anonymous way, hard to filter.	
V	The hidden service is a public resource from which the media can reach any other Internet website for maximum diffusion, such as mainstream social networks.	

Step I and II are not mandatory. Everybody will be able to install its own hidden service and configure the application to use it. Of course, RiseApp will be released with a Free/Open Source license and all its documentation with a copyleft license so that anybody will be able to use, copy and inspect the internals of the hidden service and the mobile application.

4 Feedback

This initial design of RiseApp is the result of a small grant that I have received from the CHEST project [2]. CHEST has another open call for larger grants that will allow me to implement a first version of RiseApp. Before applying I need feedback to validate the RiseApp idea (is it really useful?) and improve its design in order to prepare a solid proposal to gather funds to realize it.

RiseApp needs feedback from human rights activists working in different contexts in order to design an application that really fits the needs of those that will use it on the field, avoiding a technology-driven approach. Since I'm a technologist and my social activism is limited to the Italian context, I need as more feedback as possible to avoid pitfalls. Note that this document is not intended to receive feedback on the technical details. There will be more time and more documentation to discuss technical aspects in the future. In this phase I need the feedback on the concept, based on your experience. Note also that I hope RiseApp can be useful in many different situations, so if you think it can help, share your experience whether you come from the Arab Spring, the Occupy Movement or anything else.

Feedback on any aspects of the proposal are highly appreciated. Below are a few questions to help guide your input.

1. The relationship between communication technology and activism has received great attention, and in some cases it has been highly overrated. **Do you think the goal of RiseApp is a useful one?**
2. **Would you use RiseApp?** Please justify why you would be interested in it or the concerns not to use it.
3. **Are there specific situations in which you could have used RiseApp?** Do you have any examples of a situation in which RiseApp would have been useful to you? what are the features you think you would have needed more?
4. **What are the criticalities you can forcast?** Are there some wrong assumptions, or missing ones?
5. **Are there some features that RiseApp misses?** Can you imagine some added features that could make RiseApp more useful to your cause?

[2] www.chest-project.eu

If you are part of any public organization that is directly involved in activism or that supports actions in an indirect way, there are a few more questions I'd like to ask. Note that I'm not asking to take an official position for the organization, just your feeling about what the orientation could be.

1. **Do you think your organization could encourage the use of RiseApp?** Does your organization have direct contacts with people that can use it? do you think it could advice its use?
2. **Does your organization use any similar software?** For instance, Tor-based browsers, or secure mobile applications to communicate or record media.
3. **Is your organization involved in the development of similar projects?**
4. **Do you think your organization could support the development of RiseApp?** Support does not mean only directly funding, there can be many forms of direct or indirect support such as testing, advocating etc... Writing a letter of support can be extremely useful to show that RiseApp tackles a real problem in the context of the CHEST call, for instance.
5. **Do you think your organization can be involved in the development of RiseApp?** Does your organization have experience in software development or fund-raising? Would it be interested in a joint participation to any future project calls?

4.1 How and When to contact me

If you want to send me a feedback, first of all, thank you. Please add as much information as you feel. In particular I'm interested in the place and the period you were involved in the activism, what happened, the association you belong to (if any). **It is really important that you specify if you allow me to consider the information you give as public**. In case I may anonymously quote it in the website, presentations, projects etc.

The more details you give about your situation, the more it helps situating your contribution. If you include personal data (name, email to be recontacted etc.) I will treat them with care and respect your privacy, but please, give me as few as you think is needed. Anonymous feedback is perfectly ok.

You can write your answers to leonardo.maccari@unitn.it.

You can also use PGP to encrypt your emails, with the following key:

```
pub   4096R/AABE2BD7 2013-11-02 [expires: 2015-11-02]
Key fingerprint =
  567C B5B1 65A3 5295 ED83  1732 B425 3D8A AABE 2BD7
```

The deadline for CHEST open call for project is September 30th, 2014. It would be extremely good to receive feedbacks at least a week before that date, so I can use them to shape the proposal. Anyway, even after that date, all the feedback will be evaluated and will contribute to future activities.

4.2 Who Am I

I'm a research fellow at the Department of Information Engineering and Computer Science at the university of Trento. I hold a Master and a Ph.D in Computer Science and I was awarded with a Marie Curie grant for the period 2011-2013.

My research focuses on security and privacy in distributed networks, and I'm currently working on Wireless Community Networks. I'm the author of about 30 publications on these themes. You can find more details of my work in my personal page[3].

I am a hacktivist of the Ninux Wireless Community Network [4], and a long-time open source and copy-left supporter. You can find more about my hacktivism in my personal blog [5].

You can get in contact with me on twitter as @leobowski.

5 Copyright

[3] See www.disi.unitn.it/maccari
[4] See www.ninux.org
[5] See www.leonardo.ma, in Italian
[6] See http://creativecommons.org/licenses/by/4.0/ for details