Mesh Messaging in Large-scale Protests: Breaking Bridgefy

Martin R. Albrecht

Jorge Blasco

Rikke Bjerg Jensen

Lenka Mareková

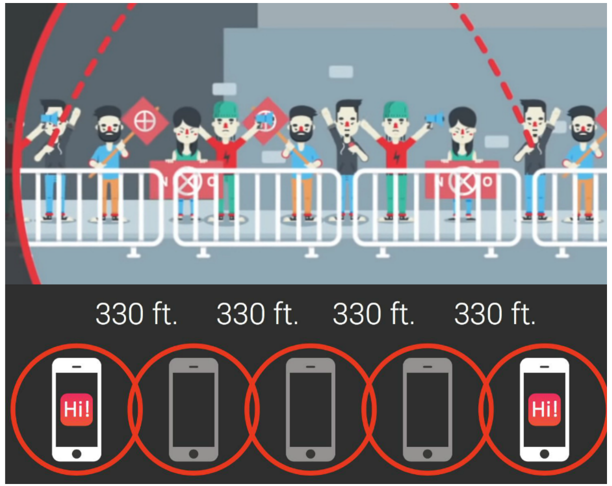
Royal Holloway, University of London

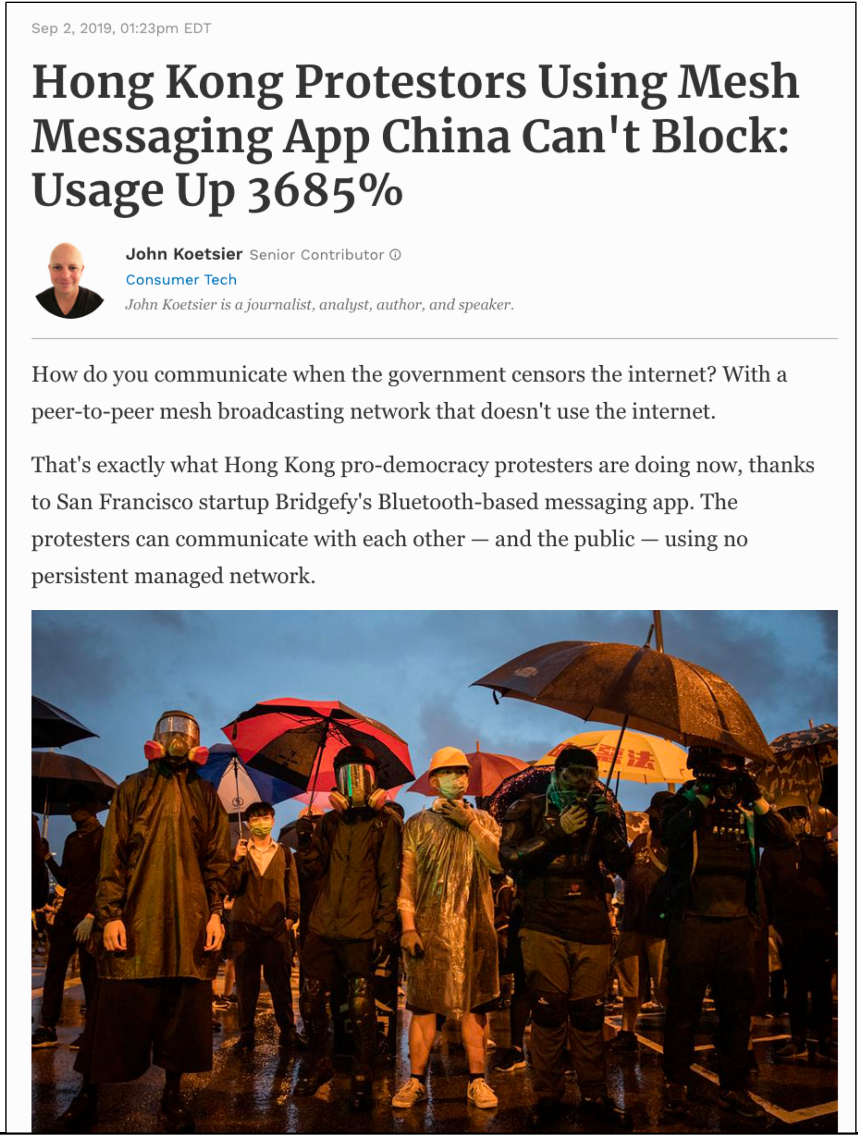
By Studio Incendo - DSCF8925, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=85653507

Context

- Hong Kong Anti-ELAB protests in 2019.
- Media reports on messaging app that works despite an internet shutdown.
- Bridgefy: *secure* mesh messaging via Bluetooth.

bridgefy





Sep 2, 2019, 01:23pm EDT

Hong Kong Protestors Using Mesh Messaging App China Can't Block: Usage Up 3685%

John Koetsier Senior Contributor
Consumer Tech
John Koetsier is a journalist, analyst, author, and speaker.

How do you communicate when the government censors the internet? With a peer-to-peer mesh broadcasting network that doesn't use the internet.

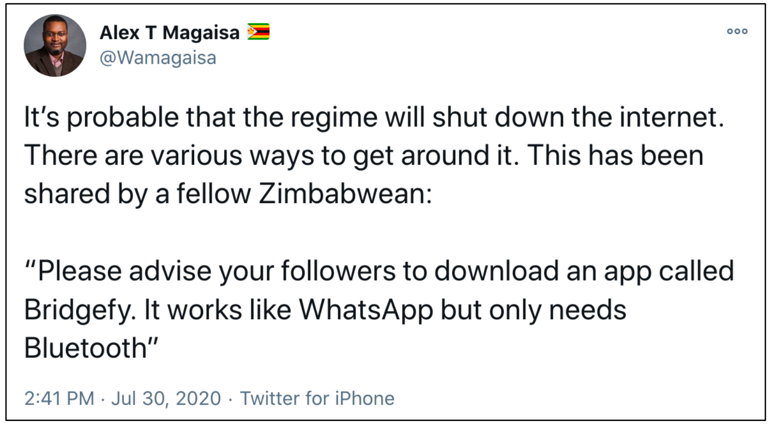
That's exactly what Hong Kong pro-democracy protesters are doing now, thanks to San Francisco startup Bridgefy's Bluetooth-based messaging app. The protesters can communicate with each other — and the public — using no persistent managed network.

forbes.com/sites/johnkoetsier/2019/09/02/hong-kong-protestors-using-mesh-messaging-app-china-cant-block-usage-up-3685/

bridgefy.me

Context

- Knock-on effect in other countries:
  - Citizenship Amendment Act protests in India.
  - Black Lives Matter protests in the US.
  - Protests of opposition activists in Zimbabwe.
  - Protests after the presidential election in Belarus.
  - Monarchy reform protests in Thailand.
- Actual adoption unclear.

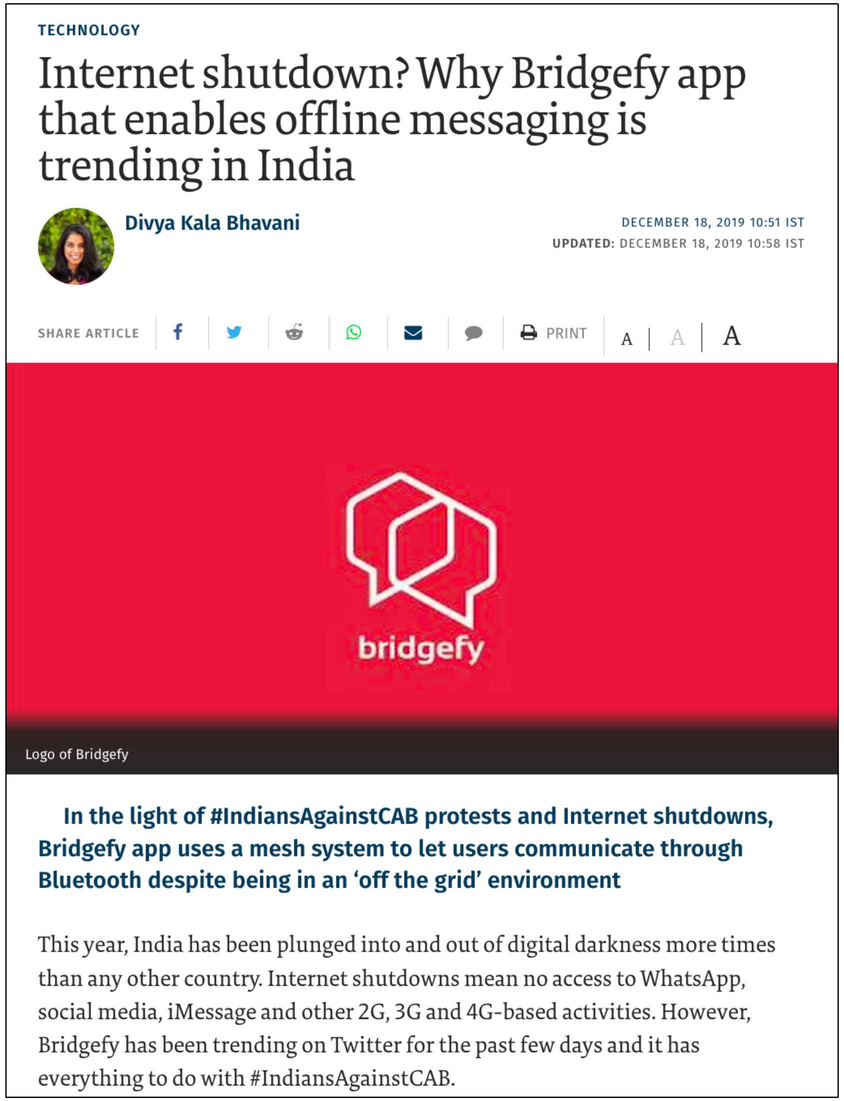


Alex T Magaisa 🇿🇼
@Wamagaisa

It's probable that the regime will shut down the internet. There are various ways to get around it. This has been shared by a fellow Zimbabwean:

"Please advise your followers to download an app called Bridgefy. It works like WhatsApp but only needs Bluetooth"

2:41 PM · Jul 30, 2020 · Twitter for iPhone



TECHNOLOGY

Internet shutdown? Why Bridgefy app that enables offline messaging is trending in India

Divya Kala Bhavani

DECEMBER 18, 2019 10:51 IST
UPDATED: DECEMBER 18, 2019 10:58 IST

Logo of Bridgefy

In the light of #IndiansAgainstCAB protests and Internet shutdowns, Bridgefy app uses a mesh system to let users communicate through Bluetooth despite being in an 'off the grid' environment

This year, India has been plunged into and out of digital darkness more times than any other country. Internet shutdowns mean no access to WhatsApp, social media, iMessage and other 2G, 3G and 4G-based activities. However, Bridgefy has been trending on Twitter for the past few days and it has everything to do with #IndiansAgainstCAB.

thehindu.com/sci-tech/technology/internet-shutdown-why-bridgefy-app-that-enables-offline-messaging-is-trending-in-india/article30336067.ece

twitter.com/wamagaisa/status/1288817111796797440

Security analysis of Bridgefy

- Reverse-engineered Android app v2.1.28 (Jan 20).
- Architecture:
  - Bluetooth Classic or Low Energy used for connections of physically close devices.
  - Mesh is a managed flood-based network with TTL counters and received receipts.
  - BLE messages are Gzipped, then encrypted with RSA with PKCS#1 v1.5 padding in ECB-like fashion.
  - Automatic handshake exchanging public keys between devices in range.

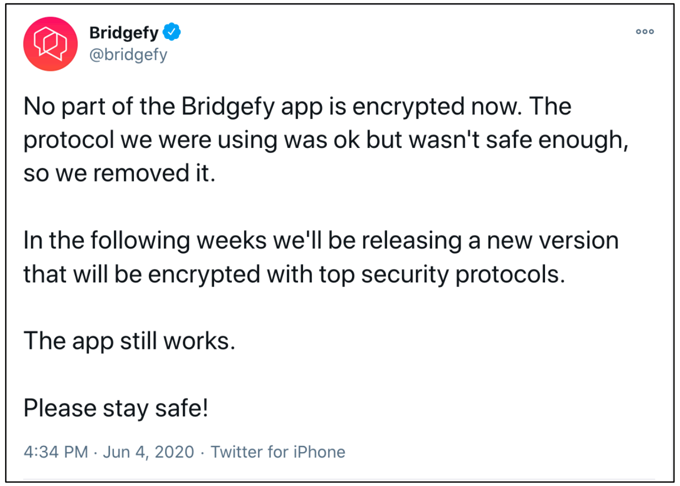
Security analysis of Bridgefy

- Discovered vulnerabilities:
    - Users could be tracked, their social graphs revealed.
    - The handshake was not cryptographically authenticated:
        - Users could be impersonated.
        - A full MITM could be mounted to subvert public-key encryption between two users.
    - Composition of PKCS#1 v1.5 encryption and Gzip compression could be exploited:
        - Confidentiality could be broken using a variant of Bleichenbacher's attack with 2^{17} chosen ciphertexts.
    - A single message “zip bomb” could disable the mesh network.
- Verified attacks in practice with Frida[1].

[1] frida.re, a dynamic instrumentation toolkit.

Disclosure

- Private disclosure to Bridgefy in April 2020.
- Partial disclosure by the developers themselves from June 2020.
- Public disclosure in August 2020 – no fixes yet.
- Bridgefy released an update on 30 October 2020 – switch to the Signal protocol – we did not vet the changes.



Bridgefy
@bridgefy

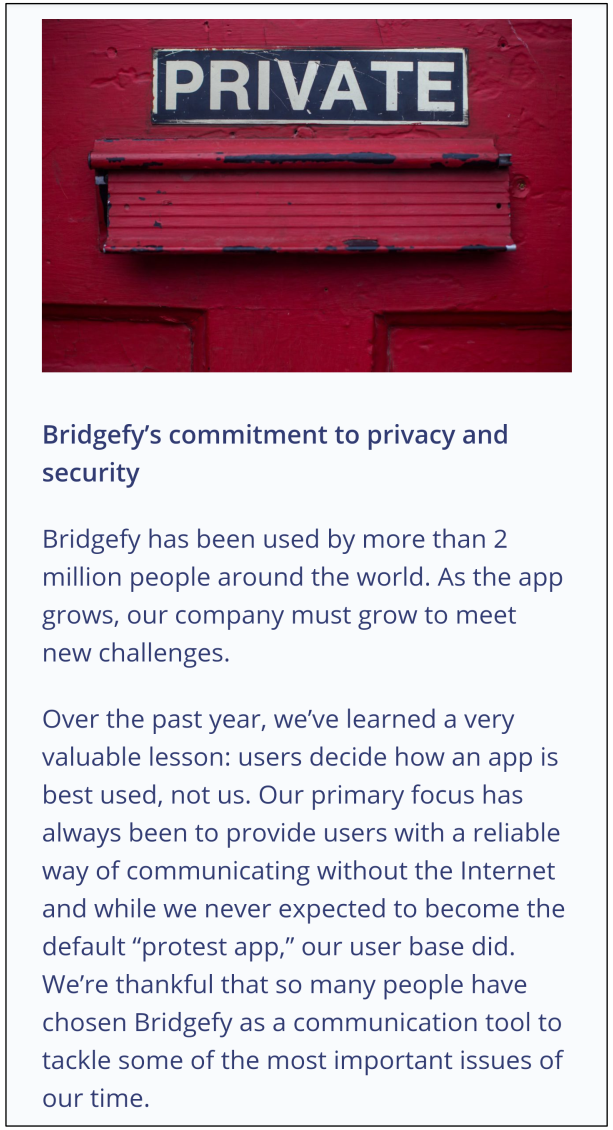
No part of the Bridgefy app is encrypted now. The protocol we were using was ok but wasn't safe enough, so we removed it.

In the following weeks we'll be releasing a new version that will be encrypted with top security protocols.

The app still works.

Please stay safe!

4:34 PM · Jun 4, 2020 · Twitter for iPhone



Bridgefy's commitment to privacy and security

Bridgefy has been used by more than 2 million people around the world. As the app grows, our company must grow to meet new challenges.

Over the past year, we've learned a very valuable lesson: users decide how an app is best used, not us. Our primary focus has always been to provide users with a reliable way of communicating without the Internet and while we never expected to become the default "protest app," our user base did. We're thankful that so many people have chosen Bridgefy as a communication tool to tackle some of the most important issues of our time.

web.archive.org/web/20200826183604/https://bridgefy.me/bridgefys-commitment-to-privacy-and-security/

twitter.com/bridgefy/status/1268551771124834313

Discussion

- Nothing surprising about the attacks given the protocol.
- Users of Bridgefy made it into a “protest app”.
- Applications need to be evaluated under the conditions they are used in.
- Absence of alternatives.
- What security can be achieved in the mesh setting?
- What security needs do protesters have?