

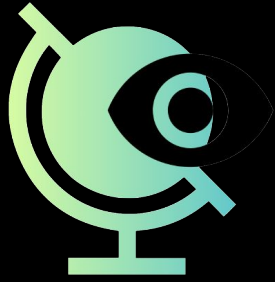


Advancing the Science of Shutdown Circumvention



Piyush Kumar Sharma





Detecting Censorship with Side Channels

The Art of Censorship Data Analysis

FOCI 2023

Measurement Methods for Locating & Examining Censorship Devices

CoNEXT 2023 🏆 IRTF Applied Networking Research Prize winner

Censored Planet: An Internet-wide, Longitudinal Censorship Observatory

ACM CCS 2020

Measuring the Deployment of Network Censorship Filters at Global Scale

NDSS 2020

Quack: Scalable Remote Measurement of Application-Layer Censorship

USENIX Security 2018

Internet-Wide Detection of Connectivity Disruptions

IEEE S&P (“Oakland”) 2017 , [Invited to appear in the IEEE S&PMagazine](#)

Global Measurement of DNS Manipulation

USENIX Security 2017 [Invited to appear in USENIX ;login;](#), Winter 2017 Issue

Analyzing the Great Firewall of China Over Space and Time

PETs 2015

Detecting Intentional Packet Drops on the Internet via TCP/IP Side Channels

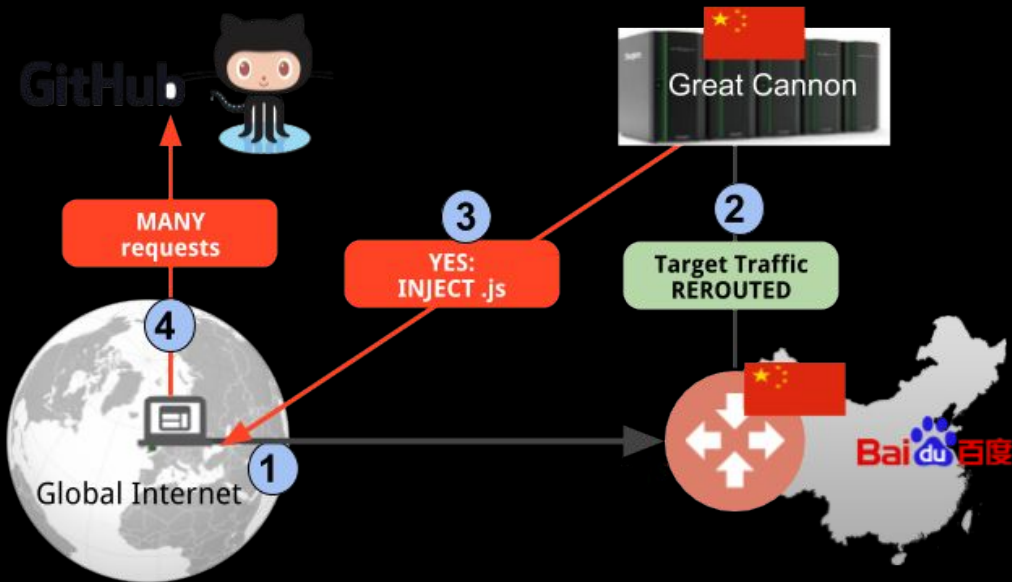
Passive and Active Measurement (PAM), 2014

Idle Scanning and Non-interference Analysis of Network Protocol Stacks

Using Model Checking

USENIX Security 2010

Understanding the Technology of Interference



TSPU: Russia's Decentralized Censorship System

In: ACM IMC , October 2022

Measurement Methods for Locating & Examining Censorship Devices

CoNEXT 2023 🏆 IRTF Applied Networking Research Prize winner

Throttling Twitter: An Emerging Censorship Technique in Russia

In: ACM IMC, November 2021

Decentralized Control: A Case Study of Russia

In: NDSS, February 2020

Censorship in Russia

Report: <https://censoredplanet.org/russia>

Examining How the Great Firewall Discovers Hidden Circumvention Servers

ACM Internet Measurement Conference (IMC), October 2015

IRTF (IETF) Applied Networking Research Prize winner

Analyzing the Great Firewall of China Over Space and Time

Privacy Enhancing Technologies Symposium (PETS), July 2015

An Analysis of China's Great Cannon

USENIX FOCI, August 2015



Safeguarding the consumer VPN ecosystem

"All of them claim to be the best": Multi-perspective study of VPN users and VPN providers

R. Ramesh, A. Vyas, R. Ensafi
USENIX SECURITY, August 2023

OpenVPN is Open to VPN Fingerprinting

D. Xue, R. Ramesh, M. Kallitsis, J. Halderman, J. Crandall, R. Ensafi

USENIX Security, August 2022



Distinguished paper award



Won First Prize in the 2022 Internet Defense Prize

VPNalyzer: Systematic Investigation of the VPN Ecosystem

R. Ramesh, L. Evdokimov, D. Xue, R. Ensafi
NDSS, April 2022

Internet Shutdowns

- Recently, a new and extreme form of censorship at play.
- The Internet is completely cut-off also known as *Internet shutdown*.

TARGETED, CUT OFF, AND LEFT IN THE DARK



Number of countries where shutdowns occurred



** Shutdowns were imposed by external forces during armed conflict in Ukraine and Yemen.

Impact of Internet Shutdowns

- High dependency on Internet
 - Healthcare, Education, Banking
 - Rapid shift due to COVID

Switching off the internet causes incalculable damage: UN report

27 June 2022

- Lack of Internet leaves people crippled for basic tasks.
 - Accessing news (info about Covid in Myanmar delayed by months)
 - Sending important emails

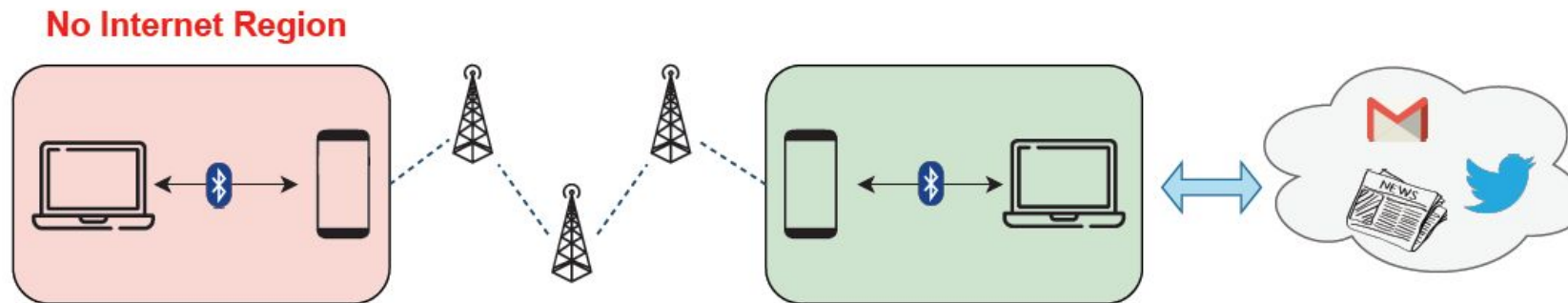
Goals

- Enabling access to light-weight and delay-tolerant internet services in shutdown regions
- Easy to setup and use
 - Can be run on standard devices users already possess



Solution: Dolphin

- Utilize cellular voice channel:
 - Directly encode data as voice.
- Assumption : Cellular services are working.
 - Observed in multiple recent shutdowns.



Challenges

I: Various **background processing** (VAD, AGC etc.) in the cellular network can limit data transmission.

- The cellular channel is highly bandwidth constrained.

II: Cellular channel is **lossy** and prone to errors. However, Internet applications require reliability.

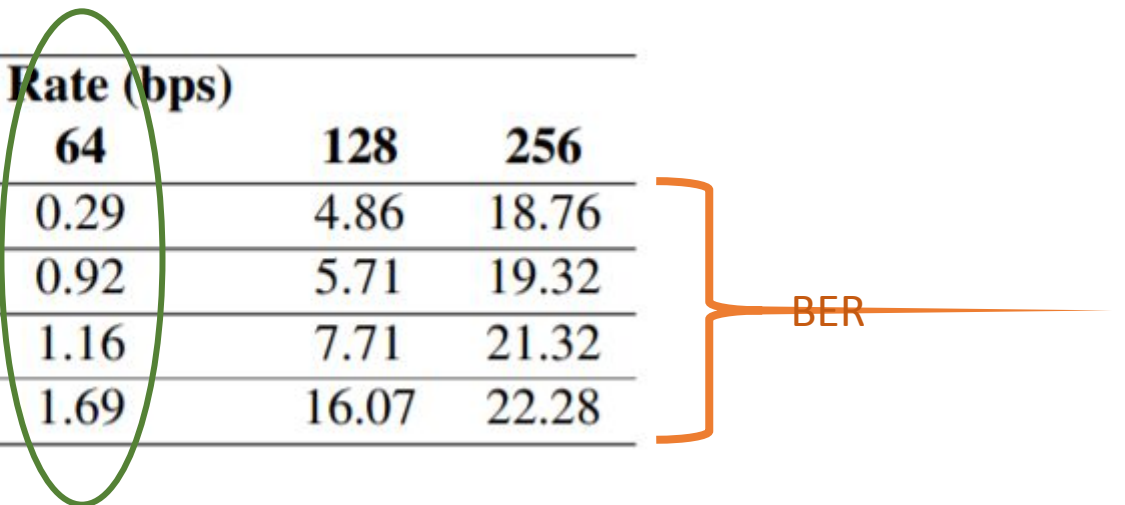
III: Cellular voice channel is **not end to end encrypted**.

IV: Undetectability of Dolphin usage.

Solution: Data Encoding

- Developed a custom modulator
 - Performed feasibility tests of possible data encoding rates.
 - Varied the cellular technology (2G/3G/4G), provider, location etc.

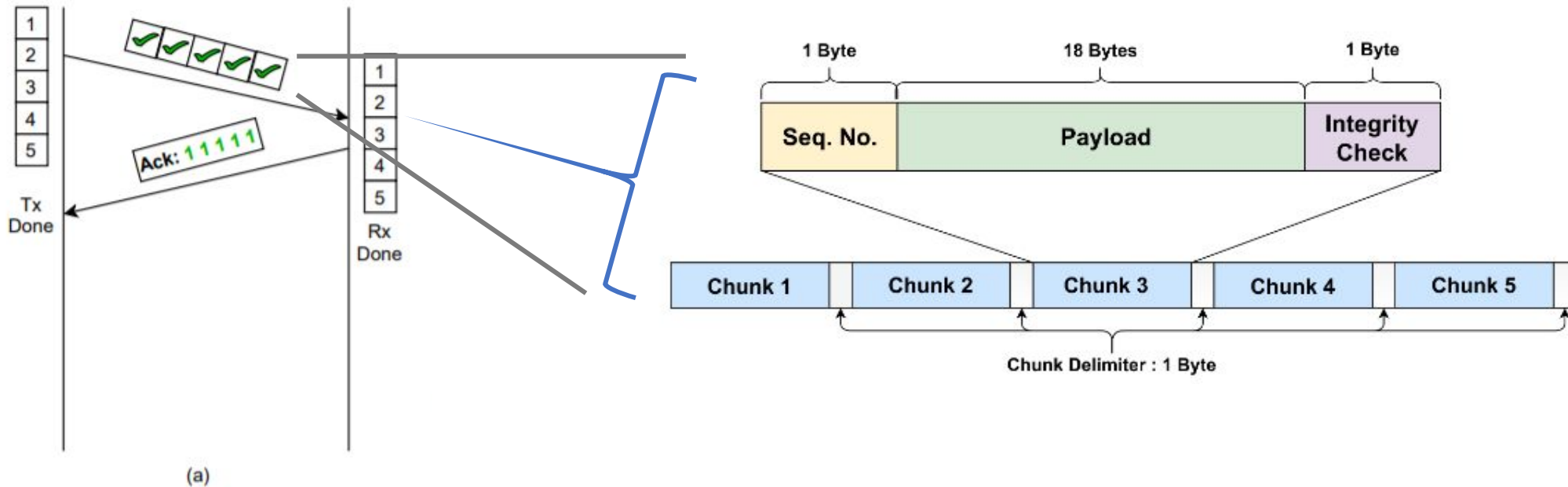
Size (Bytes)	Bit Rate (bps)				
	16	32	64	128	256
100	0.01	0.15	0.29	4.86	18.76
500	0.61	0.9	0.92	5.71	19.32
1000	0.92	1.23	1.16	7.71	21.32
5000	0.97	1.8	1.69	16.07	22.28



Even by varying different parameters, observed similar Bit Error Rates (BER)

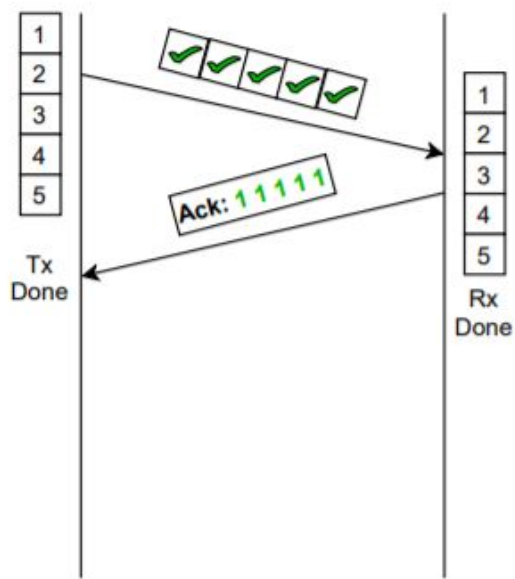
Solution: Reliability

- Built a custom *TCP style* reliability layer capable of working with any underlying modulation scheme
 - Minimizes the overhead (e.g., 1 bit per chunk for ack)

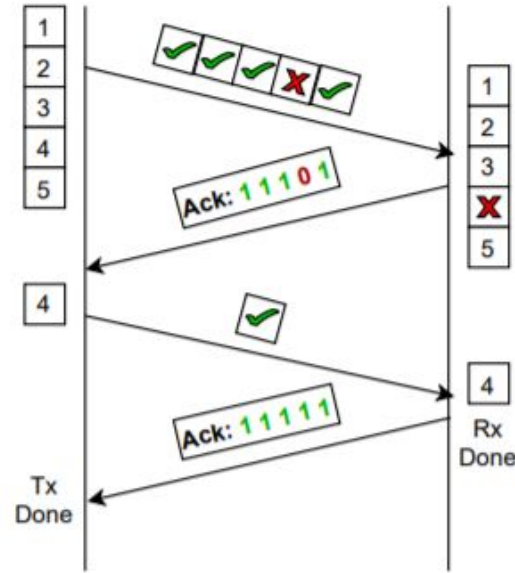


Solution: Reliability

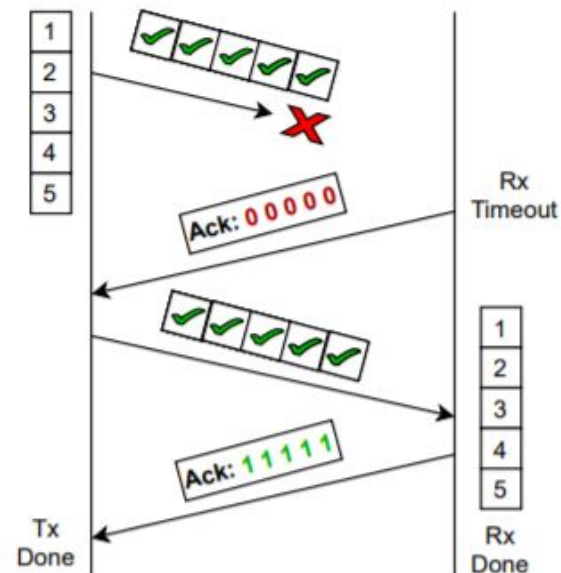
- Built a custom *TCP style* reliability layer capable of working with any underlying modulation scheme
 - Minimizes the overhead (e.g., 1 bit per chunk for ack)



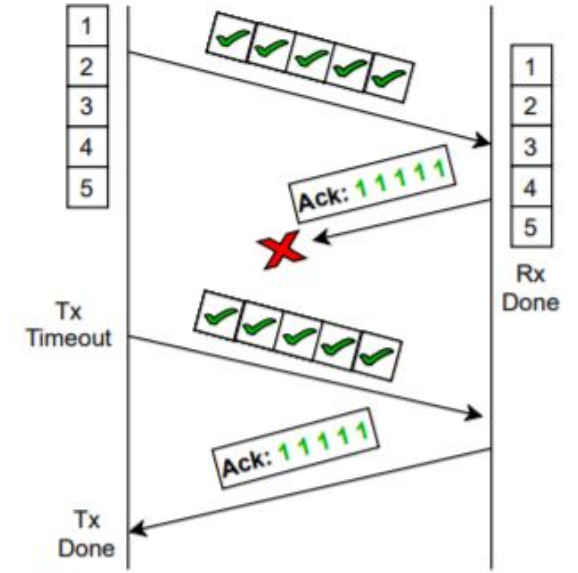
(a)



(b)



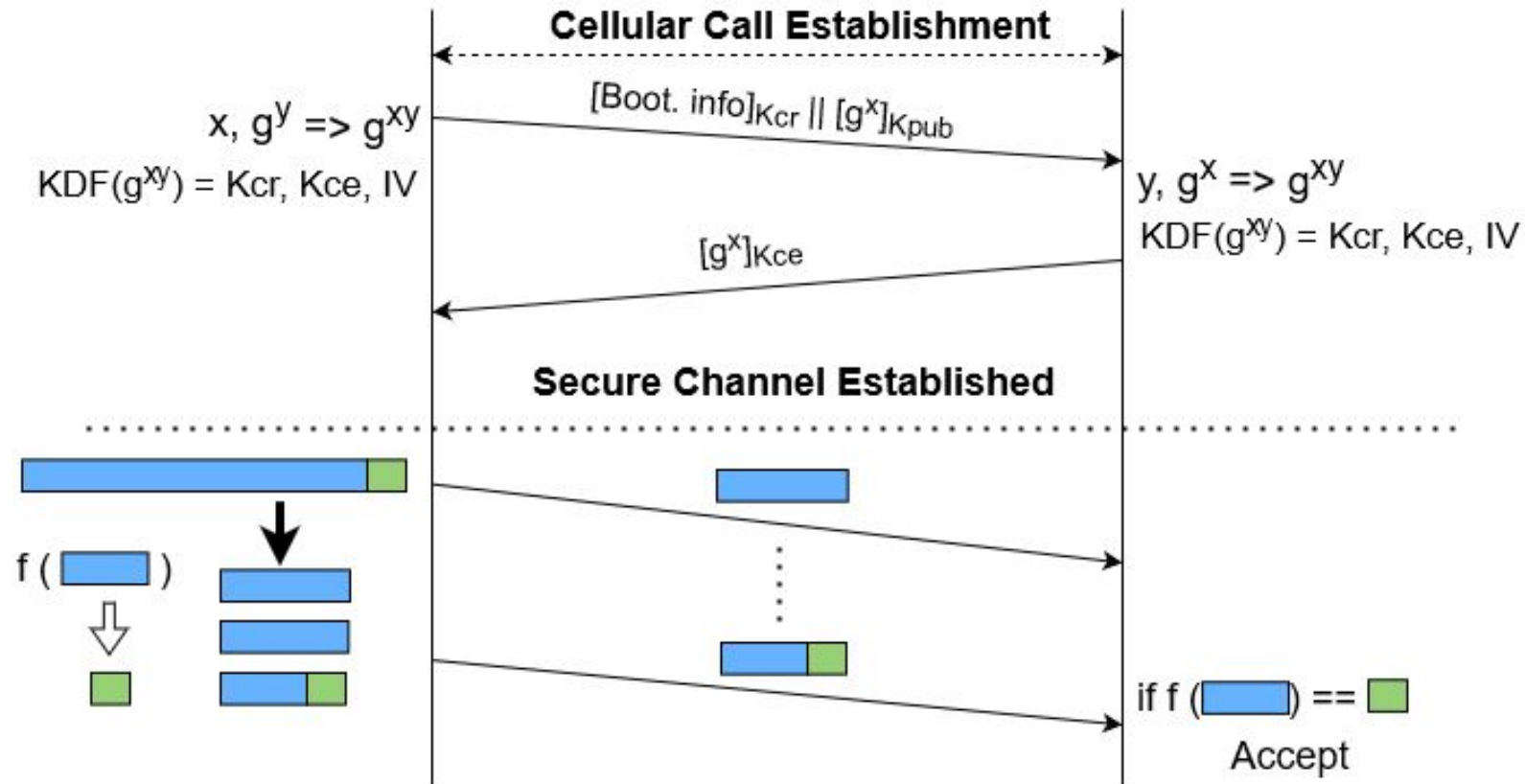
(c)



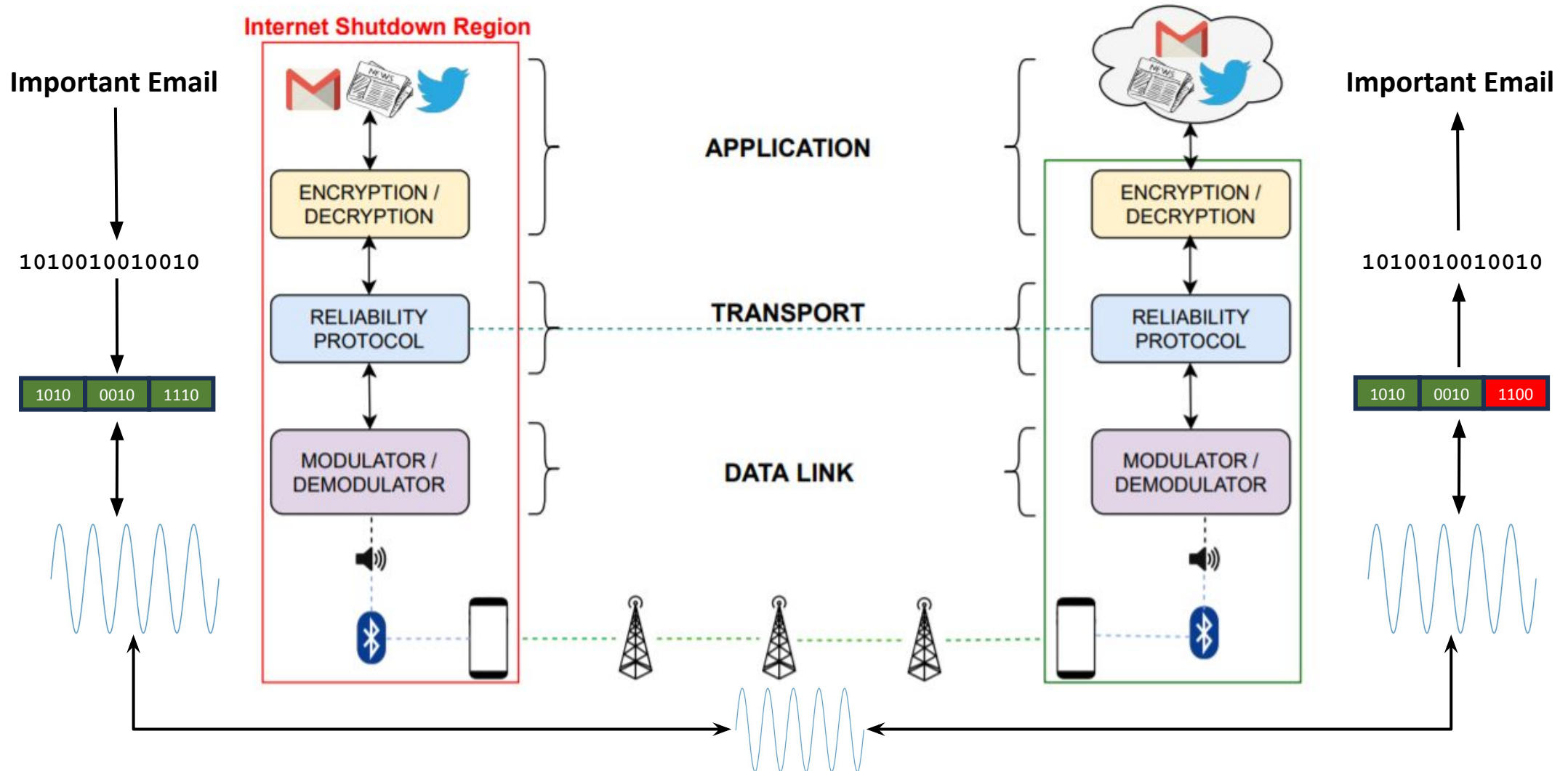
(d)

Solution: End-to-end Confidentiality

- Designed a security protocol to establish secure and encrypted channel.

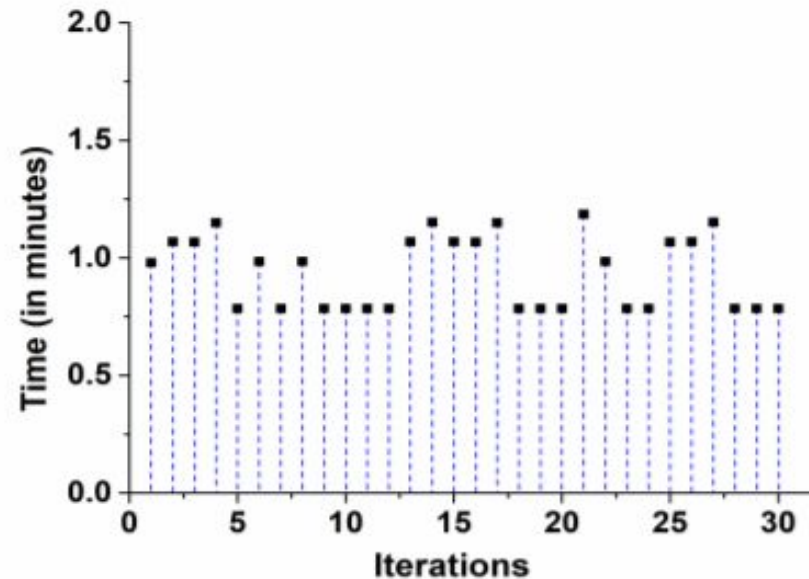
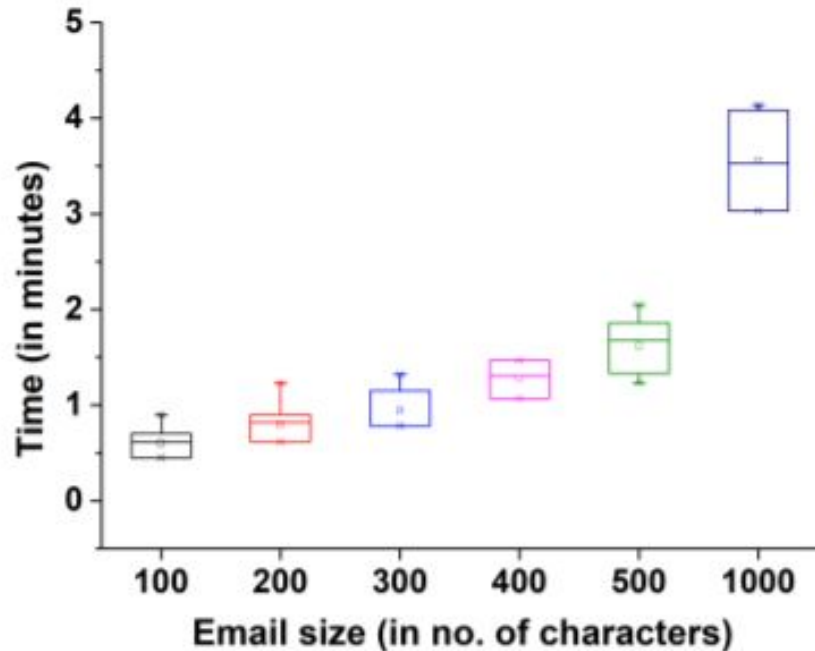


Dolphin end-to-end System



Accessing Internet Application

- Recorded time taken to **tweet** a 280 character message (max single tweet size).
- Sent **Email** of varying sizes (100, 200, 300, 500, 1000 characters).



- 10 **news snippets**, 60 characters each (total = 600); Average time: ~2 minutes

Dolphin Security Analysis

- **Threat Model:** Difficult to define precisely for cellular providers.
 - Less explored for censorship capabilities.
 - Well known for surveillance capabilities.
 - Censor can: downgrade mode (2G/3G/4G), eavesdrop, alter/modify voice data.
 - Censor cannot: disable voice calling, hamper voice quality

Possible attacks

- Perturbation
 - Can try to introduce perturbations so that Dolphin is hampered, but cellular calls not impacted much.
- Active enumeration (probing) of Dolphin servers.
- Traffic or signal analysis (offline and real-time).

Possible attacks

- Perturbation
 - Can try to introduce perturbations so that Dolphin is hampered, but cellular calls not impacted much.
- Active enumeration (probing) of Dolphin servers.
- Traffic or signal analysis (offline and real-time).

Perturbation Attacks

- Case I: Introduce perturbations after **random intervals**.
 - Dolphin's reliability protocol would recover.
- Case II: Introduce perturbations such that **all chunks get corrupted**.
 - Renders cellular channel unusable for regular callers with PESQ < 2.
- Case III: Introduce perturbations to **corrupt all acknowledgements**.
 - Could disrupt Dolphin without drastically impacting the call quality.
 - Simple mitigation: Send ack after each chunk.

Comparison

- Satellite (Starlink, Amazon Kuiper)
 - Infrastructural needs, starlink+t-mobile?
- Ad hoc networks (Moby, Rangzen, Briar, Ceno etc)
 - Dense connectivity among users
- SMS, RF communication

Towards potential future solutions

- Long road ahead
- Local vs global solutions
- Simple to use (Dolphin) vs complex technologies (satellite)
 - Easier to block vs harder to block

Please sign up

- Our upcoming steps would require support of people from this audience.
- Please use the QR code and signup.
 - <https://forms.gle/aZoPfdUsQ6BPqCTV9>
- Mailing list: CensoredPlanet-shutdown@umich.edu



Thank you!

