COLLEGE OF SOCIAL & BEHAVIORAL SCIENCES
School of Information

Privacy and Decentralization III: B.A.T.M.A.N. and Briar

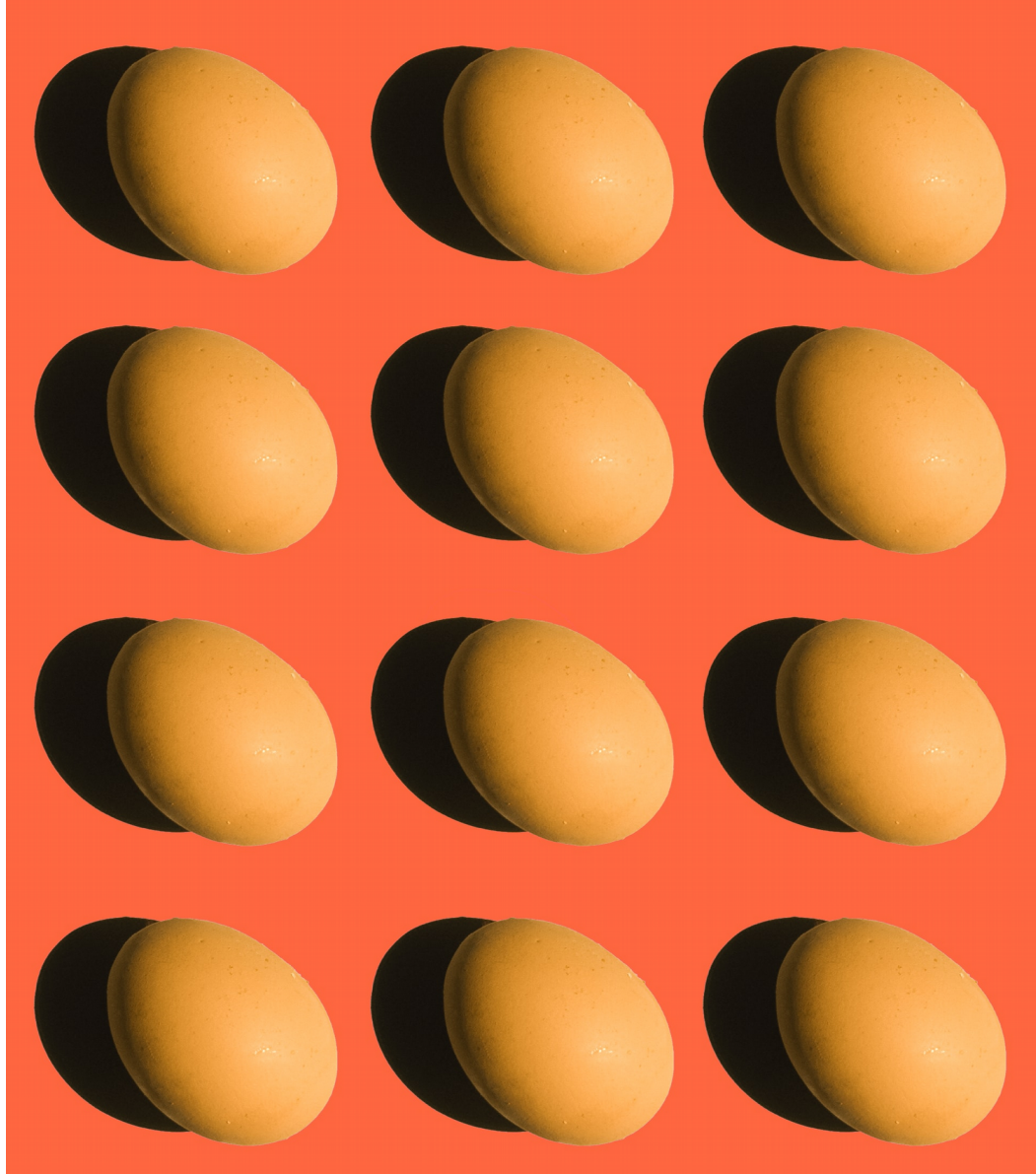
Information Privacy with Applications

David Sidi (dsidi@email.arizona.edu)

From last time:

unmarked “users”

identifying specific stakeholders and their roles in the platform



Abstract modeling of lived experience is a poor substitute for participation

- personas
- threat modeling driven by asset modeling/attacker modeling
- iterative feedback and redesign with real-world users after product launch

Abstract modeling of lived experience is a poor substitute for participation

- **personas**
- threat modeling driven by asset modeling/attacker modeling
- iterative feedback and redesign with real-world users after product launch

Pronouns
He/Him

Role
LGBTQ+ Activist

Location
Kampala, Uganda

Languages
Luganda, English

Jelani, the human rights defender

Jelani lives in Kampala, Uganda. He works for a human rights organisation, publishing the stories of LGBTQ+ people who live in fear of their sexuality or gender identity being discovered and the discrimination that follows.

Anonymity is paramount for Jelani and the LGBTQ+ community in Uganda. The government have repeatedly sought extreme penalties for homosexuality, and newspapers have publicly outed members of the LGBTQ+ community in the past – leading to violent and brutal homophobic attacks often perpetrated by the authorities themselves.

Motivation

Jelani wants to minimise his risk of arrest from collating and publishing LGBTQ+ information in his home country.

Pain points

- Jelani lacks the technical knowledge to differentiate trustworthy apps from others.
- Low bandwidth and unreliable power make it difficult for Jelani to download Tor Browser.
- Jelani's ISP blocks public relays, however a default bridge works instead.
- Jelani is suspicious of being tracked, even when using Tor Browser.

Risk level
HIGH

Trust level
LOW

Technical proficiency
NOVICE

Income
LOW

Bandwidth
V. LOW

Tor censorship
Tor partially blocked

Abstract modeling of lived experience is a poor substitute for participation

- personas
- **threat modeling driven by asset modeling/attacker modeling**
- iterative feedback and redesign with real-world users after product launch

What to model

- Assets
- Attackers
- Software

}

- experts
- less technical input to your project
- prioritization

What to model

- Assets
- Attackers
- Software

- usually: what attackers want, that you want to protect
- Stepping stones really requires understanding attackers and software

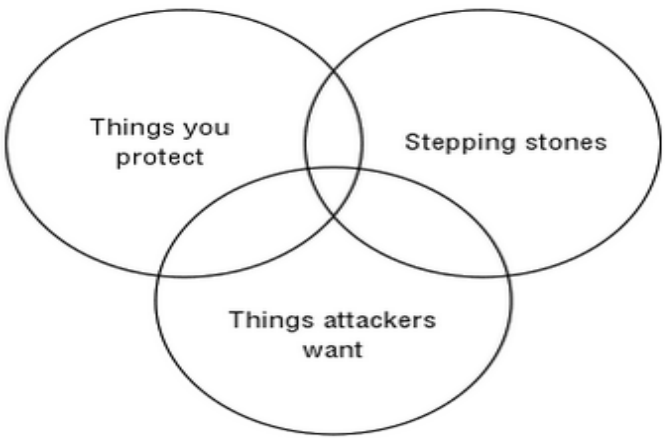


Figure 2-2: The overlapping definitions of assets

What to model

- Assets
- Attackers
- Software

- what kinds of attackers do we face?

- Competitor
- Data miner
- Radical activist
- Cyber vandal
- Sensationalist
- Civil activist
- Terrorist
- Anarchist
- Irrational individual
- Government cyber warrior
- Organized criminal
- Corrupt government official
- Legal adversary
- Internal spy
- Government spy
- Thief
- Vendor
- Reckless employee
- Untrained employee
- Information partner
- Disgruntled employee

What to model

- Assets
- Attackers
- Software

- what kinds of attackers do we face?
- A space of attacker features: personas

1. Identify behavioral variables.
2. Map interview subjects to behavioral variables.
3. Identify significant behavior patterns.
4. Synthesize characteristics and relevant goals.
5. Check for completeness and redundancy.
6. Expand descriptions of attributes and behaviors.
7. Designate persona types.

Abstract modeling of lived experience is a poor substitute for participation

- personas
- threat modeling driven by asset modeling/attacker modeling
- **iterative feedback and redesign with real-world users after product launch**

“real users” vs. potential users

- Which users to design for, and be accountable to, is exclusive
- Costanza-Chock says this is not necessarily a problem, but the choice of who is centered should be explicit.
- *Why is it not a problem? What is the alternative to choosing a specific group of users? Why is transparency about this choice important?*

Inclusive practices of design: how, in the real world, does participation with a community work? Who do you talk to?

Governance

involving a community in design: identifying collective information practices

vs.

involving design in a community: identifying where design contributes to community-defined problems

duh-nuh-nuh-nuh-nuh-nuh-nuh-nuh...

B.A.T.M.A.N.

B.A.T.M.A.N. *Advanced*

“B.A.T.M.A.N. advanced (often referenced as batman-adv) is an implementation of the B.A.T.M.A.N. routing protocol [...]”

wireless routing protocol for mesh networks

Wireless ad-hoc networks

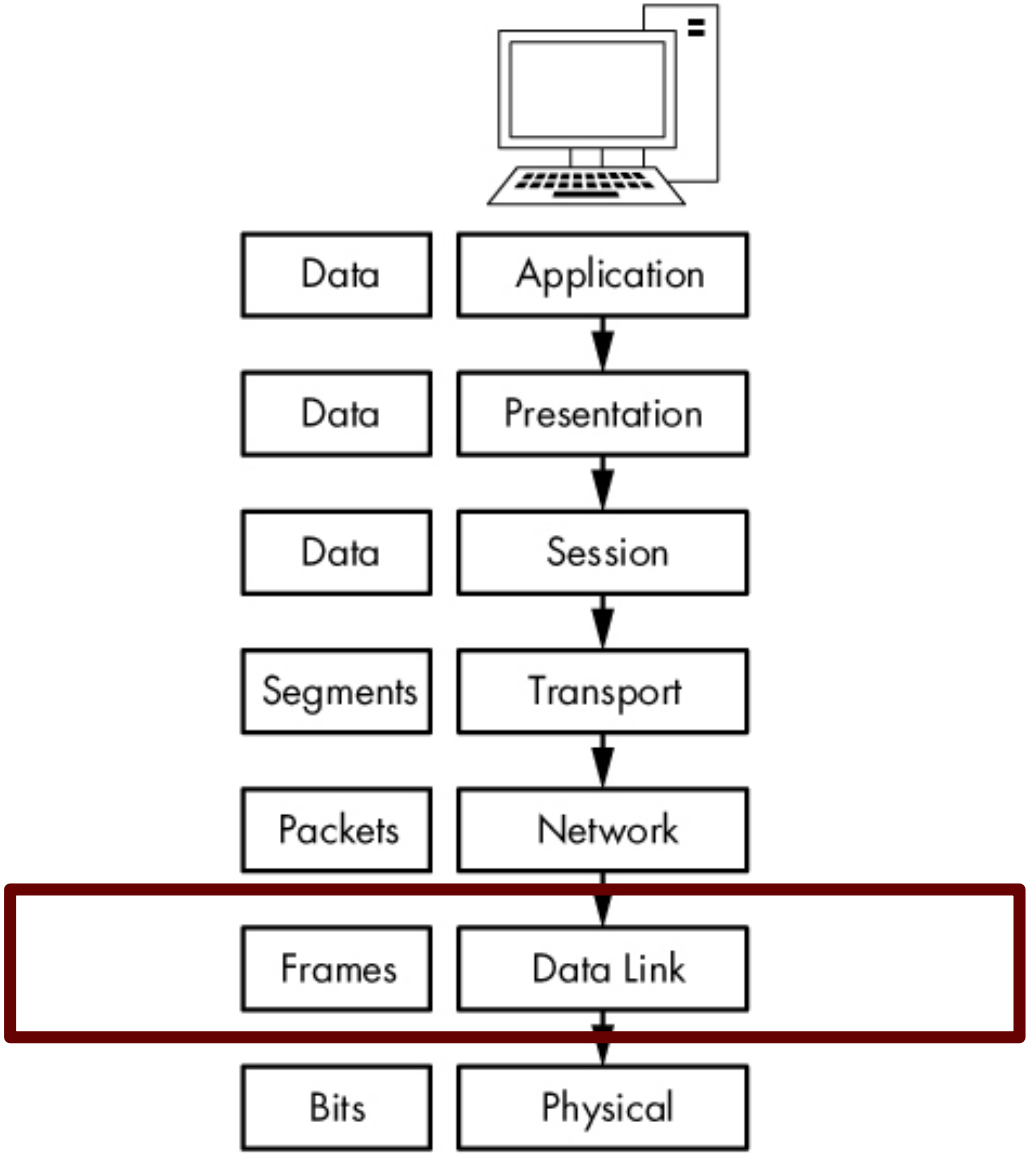
- unreliable links
- change topology

high-latency

unreliable connections

distributed

Old school concerns
UUCP, Usenet...


Data
Application
Data
Presentation
Data
Session
Segments
Transport
Packets
Network
Frames
Data Link
Bits
Physical

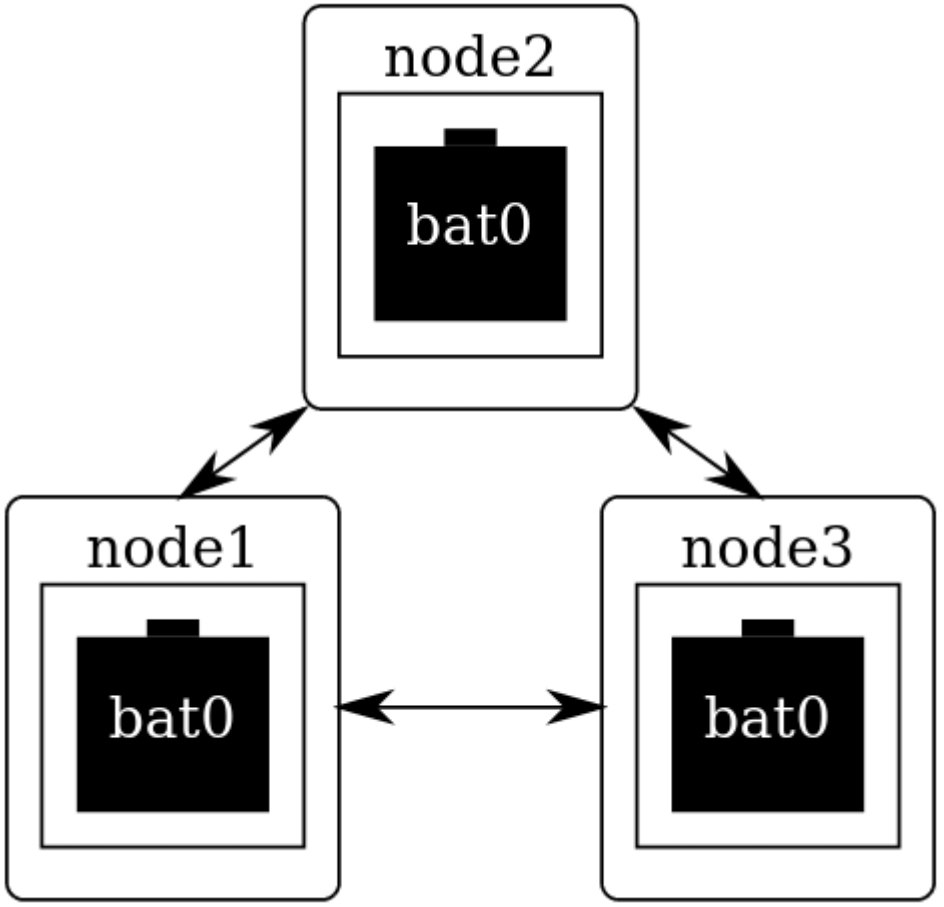


image credit: https://www.open-mesh.org/projects/batman-adv/wiki/Wiki

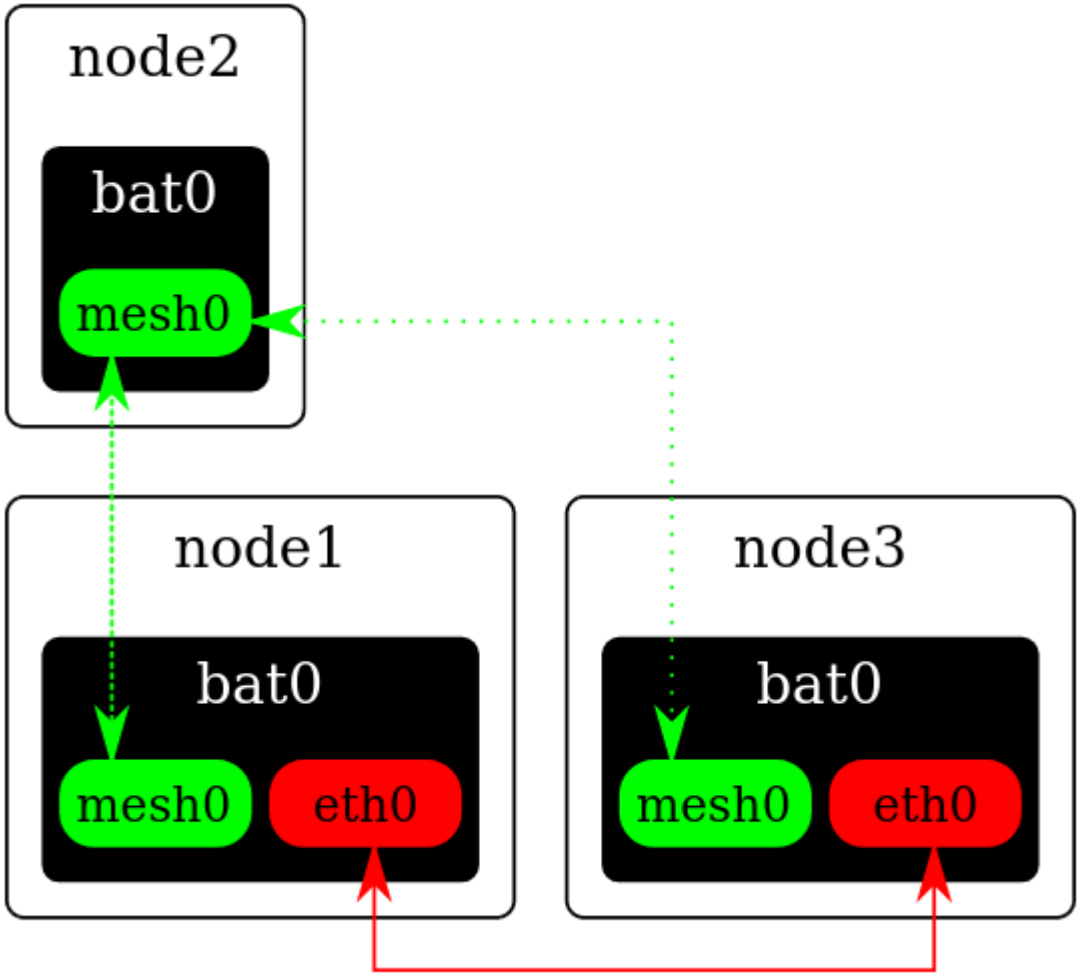
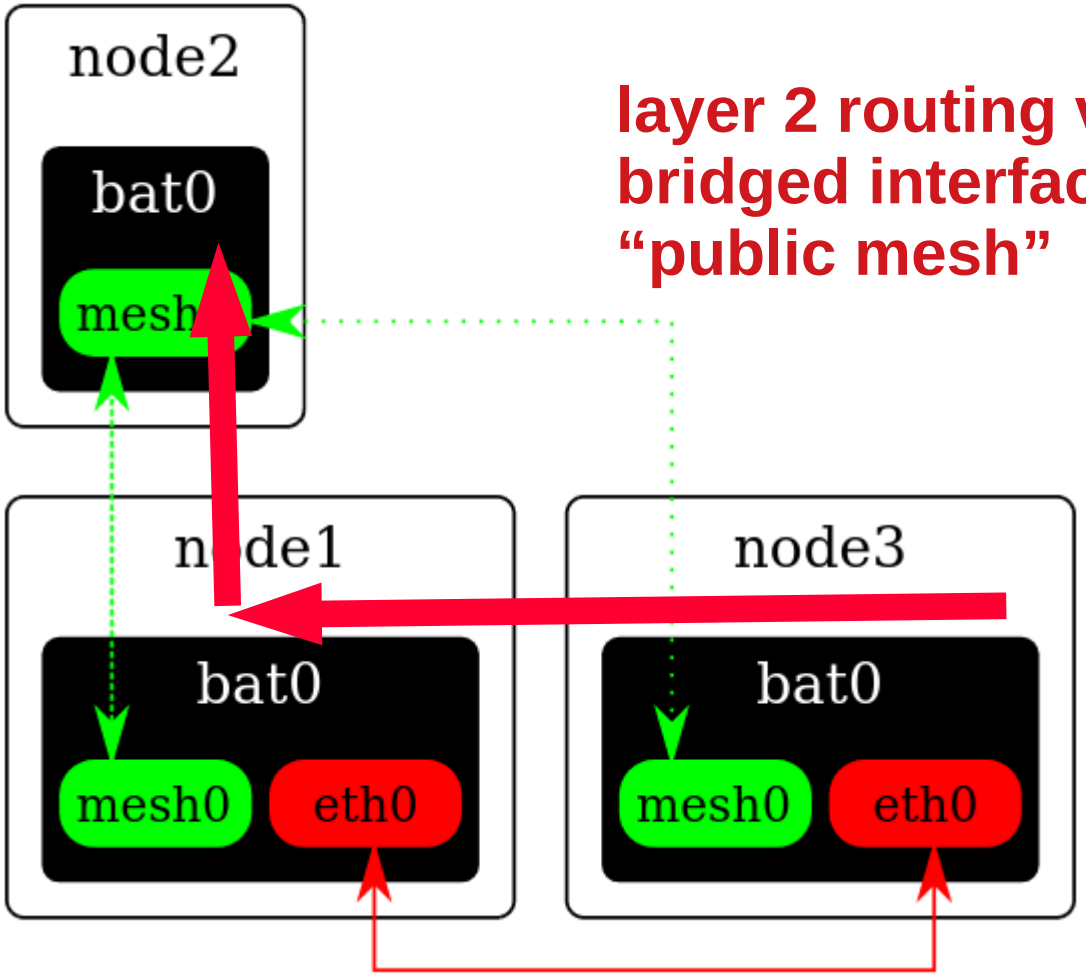
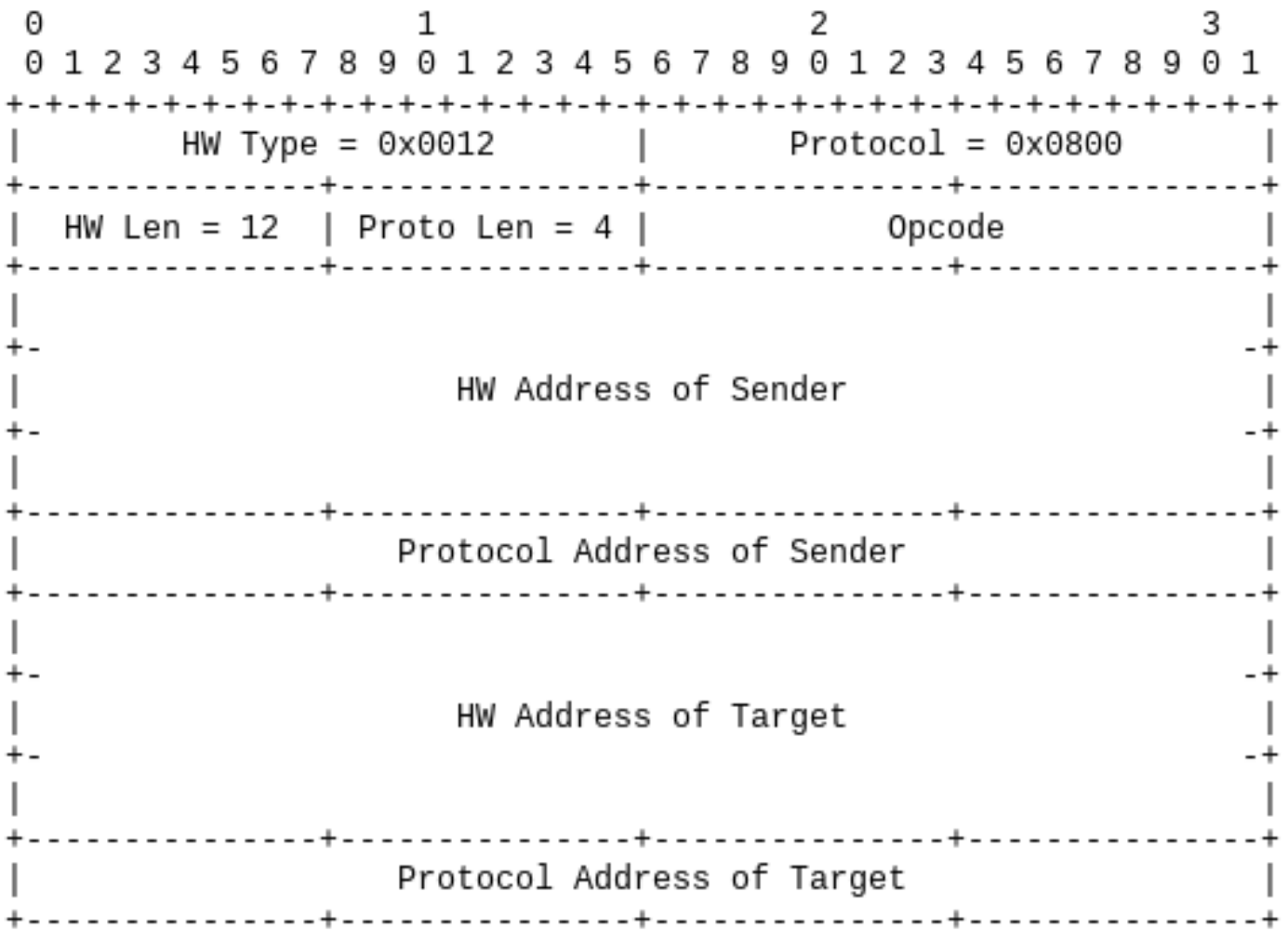


image credit: https://www.open-mesh.org/projects/batman-adv/wiki/Wiki



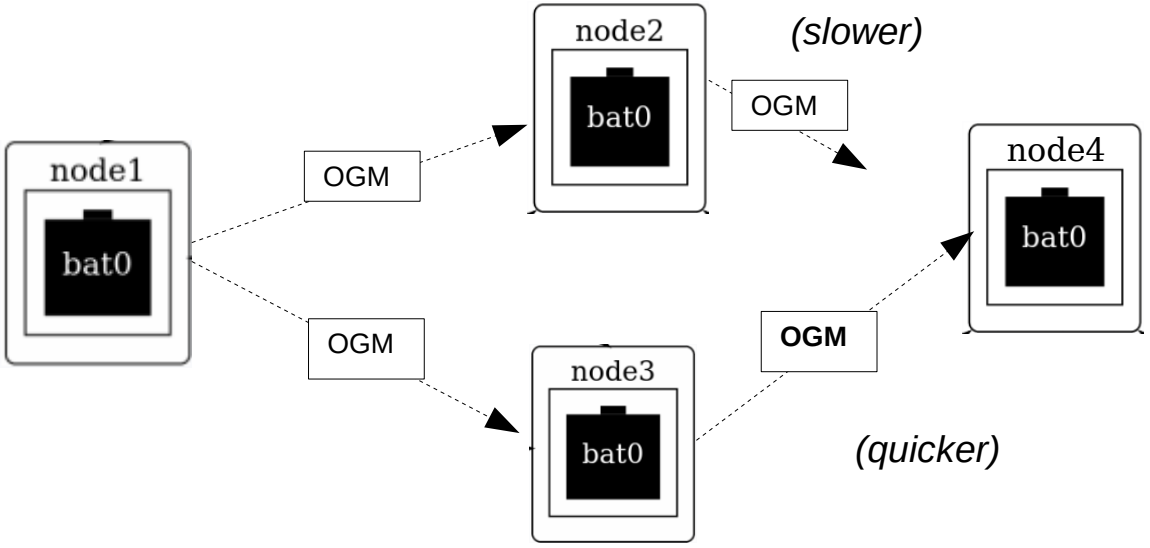
layer 2 routing via bridged interfaces -- “public mesh”

image credit: https://www.open-mesh.org/projects/batman-adv/wiki/Wiki


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
HW Type = 0x0012
Protocol = 0x0800
HW Len = 12
Proto Len = 4
Opcode
HW Address of Sender
Protocol Address of Sender
HW Address of Target
Protocol Address of Target

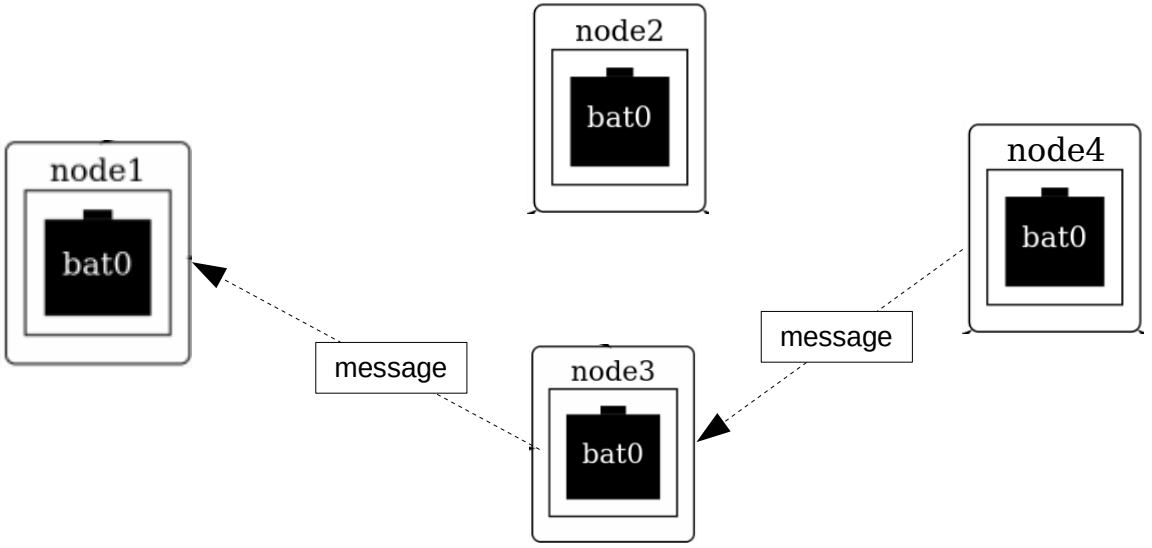
OGM

- address of the originator
- address of the node transmitting the packet
- TTL
- sequence number



OGM

- address of the originator
- address of the node transmitting the packet
- TTL
- sequence number



which nodes send OGMs faster and more reliably is used to decide which route node4 chooses for packets going back to node1.

But why?

- *Which view of privacy does BATMAN (Advanced) serve, and which does it not? Encryption, authentication?*
- Connectivity: poor availability of communications subnets as an access issue (e.g., rural communities) or as a censorship/social control issue (gov’t shutdown, denial of service attacks). Mesh networks make hosts gateways.

- During the Arab Spring protests in Egypt, the government security services shutdown access to the Internet
- Some protesters hacked Toyota in Cairo, took over the satellite uplink, and connected to an ISP. If you were on that ISP, you were connected again. That required hackers, and didn’t work for long

- An alternative would be to use a system that doesn’t rely on the communications subnet controlled by the gov’t, like B.A.T.M.A.N.
- Whoever succeeds in getting a satellite connection out is connected via a mesh to many, many people
- A more specific response for communication among protesters is to use a messenger like Briar

Centralized Model

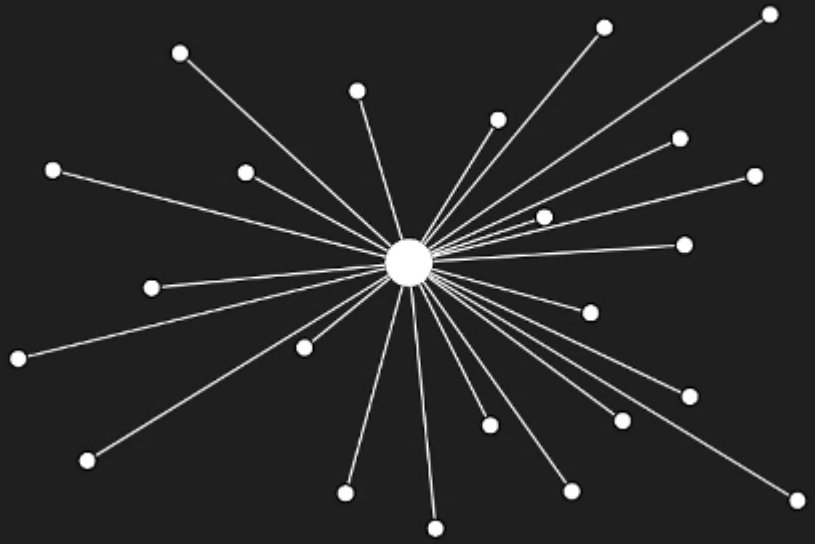


image credit: Nico Alt, https://nico.dorfbrunnen.eu/de/posts/2021/diving-at-xmpp/

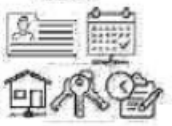
FEDERAL BUREAU OF INVESTIGATION

LAWFUL ACCESS

(U//FOUO) FBI's Ability to Legally Access Secure Messaging App Content and Metadata

(U//LES) As of November 2020, the FBI's ability to legally access secure content on leading messaging applications is depicted below, including details on accessible information based on the applicable legal process. Return data provided by the companies listed below, with the exception of WhatsApp, are actually logs of latent data that are provided to law enforcement in a non-real-time manner and may impact investigations due to delivery delays.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

App	iMessage	Line	Signal	Telegram	Threema	Viber	WeChat	WhatsApp	Wickr
Information Accessed									
Legal Process & Additional Details	• **Message Content: Limited** • **Subpoena:** can render basic subscriber information • **18 U.S.C. §2703(d):** can render 25 days of iMessage lookups to and from a target number[1] • **Pen Register:** no capability[1] • **Search Warrant:** can render backups of a target device; if target uses iCloud backup, the encryption keys should also be provided with content return; can also acquire iMessages from iCloud returns if target has enabled Messages in iCloud	• **Message Content: Limited*** • Suspect's and/or victim's registered information (profile image, display name, email address, phone number, LINE ID, date of registration, etc.) • Information on usage *Maximum of seven days' worth of specified users' text chats (Only when E2EE has not been elected and applied and only when receiving an effective warrant; however, video, picture, files, location, phone call audio and other such data will not be disclosed)	• **No Message Content** • Date and time a user registered • Last date of a user's connectivity to the service	• **No Message Content** • No contact information provided for law enforcement to pursue a court order. As per Telegram's privacy statement, for confirmed terrorist investigations, Telegram may disclose IP address and phone number to relevant authorities	• **No Message Content** • Hash of phone number and email address, if provided by user • Push Token, if push service is used • Public Key • Date (no time) of Threema ID creation • Date (no time) of last login	• **No Message Content** • Provides account (i.e. phone number) registration data and IP address at time of creation • Message History: time, date, source number and destination number	• **No Message Content** • Accepts preservation letters and subpoenas, but cannot provide records for accounts created in China • For non-China accounts, they can provide basic information (name, phone number, email, IP address), which is retained for as long as the account is active	• **Message Content: Limited*** • **Subpoena:** can render basic subscriber records • **Court Order:** Subpoena return as well as information like blocked users • **Search Warrant:** Provides address book contacts and WhatsApp users who have the target in their address book contacts • **Pen Register:** Sent every 15 minutes, provides source and destination for each message *If target is using an iPhone and iCloud backups enabled, iCloud returns may contain WhatsApp data, to include message content	• **No Message Content** • Date and time account created • Type of device(s) app installed on • Date of last use • Total number of messages • Number of external IDs (email addresses and phone numbers) connected to the account, but not plaintext external IDs themselves • Avatar image • Limited records of recent changes to account setting such as adding or suspending a device (does not include message content or routing and delivery information) • Wickr Version Number

SUBSCRIBER DATA	MESSAGE SENDER–RECEIVER DATA	DEVICE BACKUP	IP ADDRESS	ENCRYPTION KEY(S)	DATE/TIME INFORMATION	REGISTRATION TIME DATA	USER'S CONTACTS
							

(U) Prepared by Science and Technology Branch and Operational Technology Division

7 January 2021

[1] (U//LES) Apple provided logs only identify if a lookup occurred. Apple returns include a disclaimer that a log entry between parties does not indicate a conversation took place. These query logs have also contained errors.

Federated Model

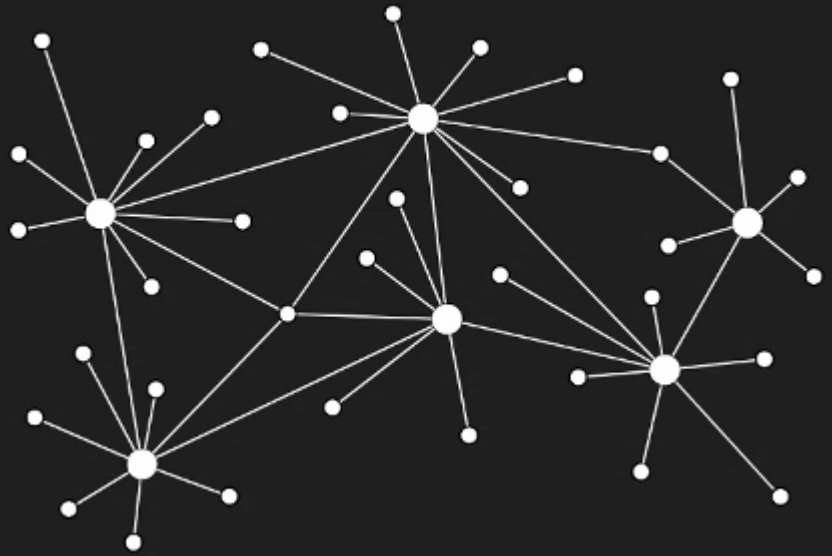


image credit: Nico Alt, https://nico.dorfbrunnen.eu/de/posts/2021/diving-at-xmpp/

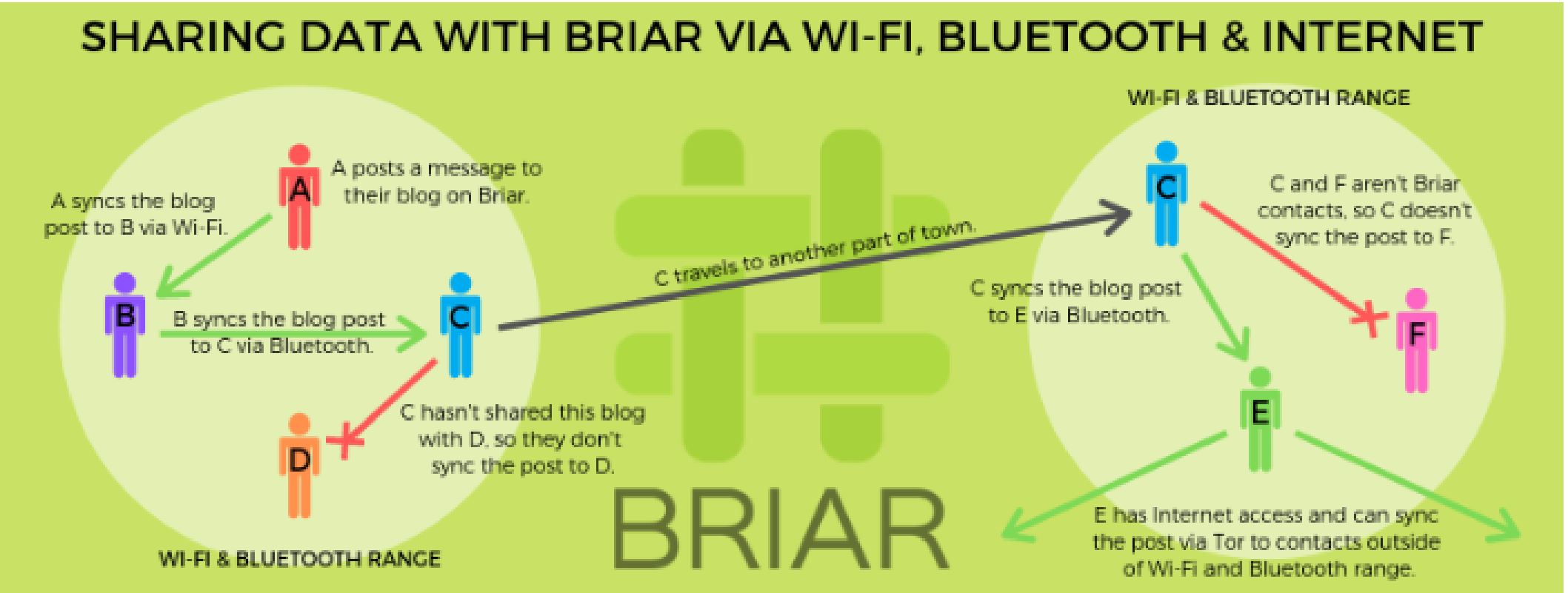
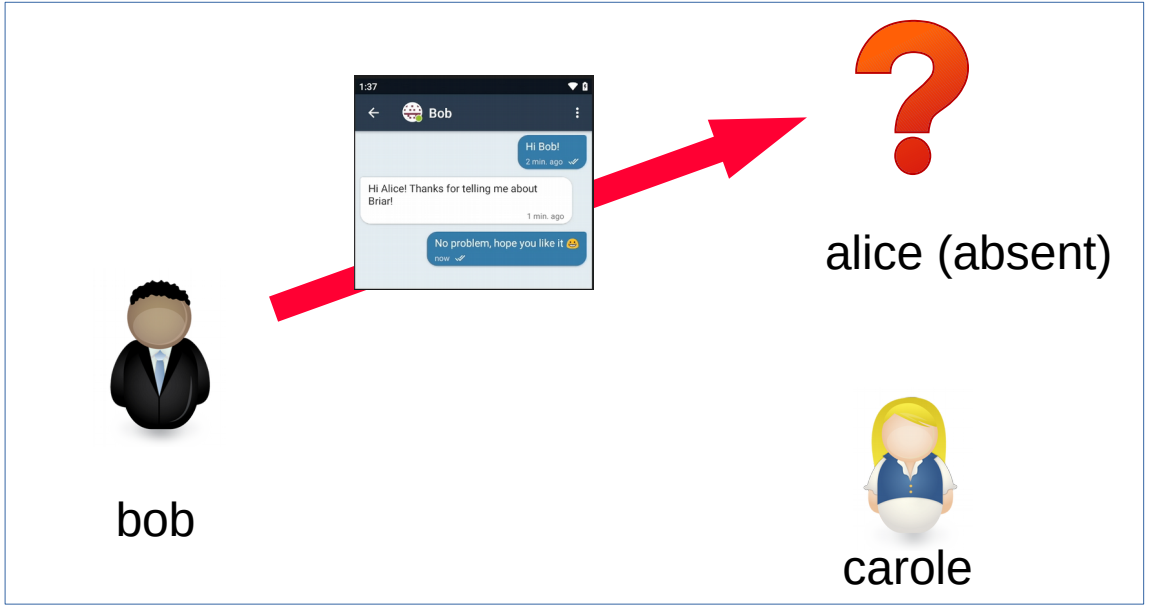
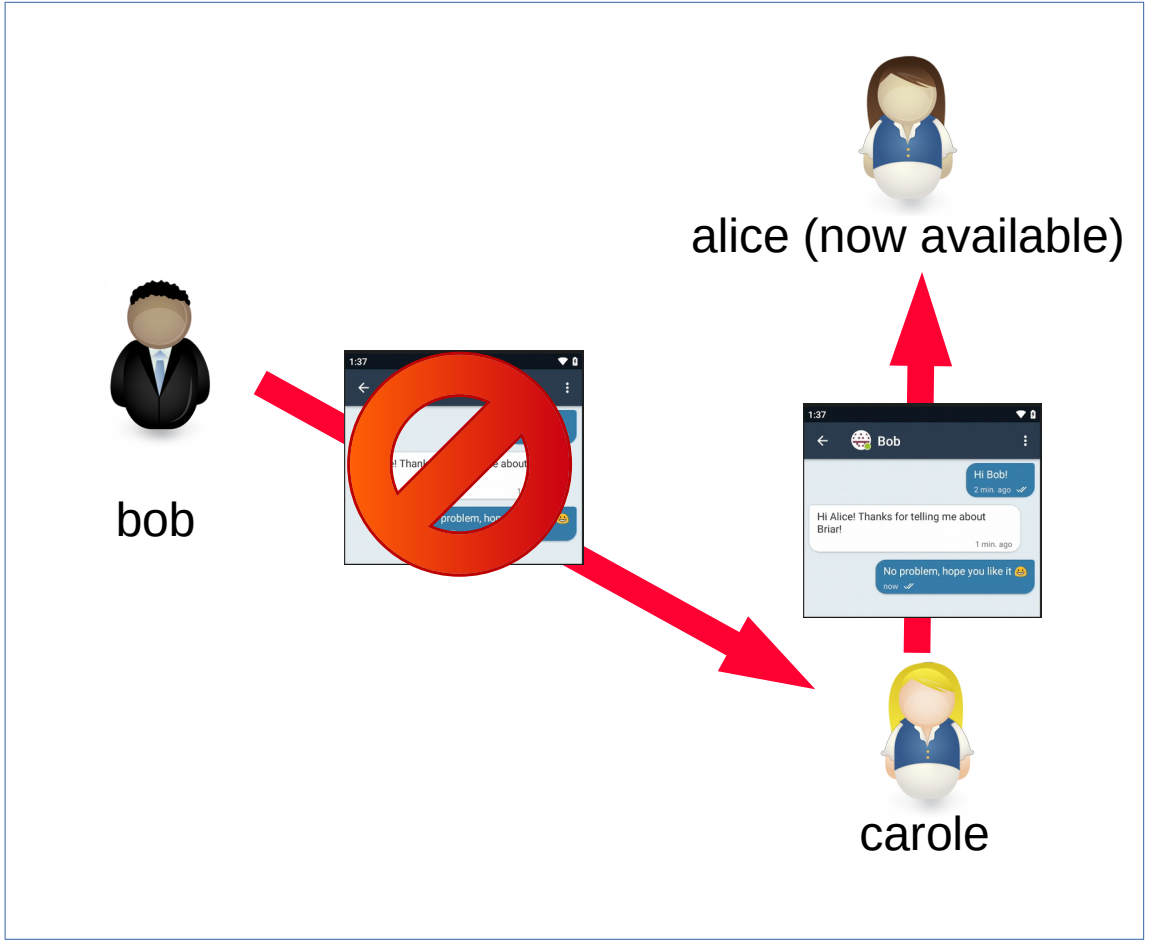


Image credit: https://briarproject.org/how-it-works/

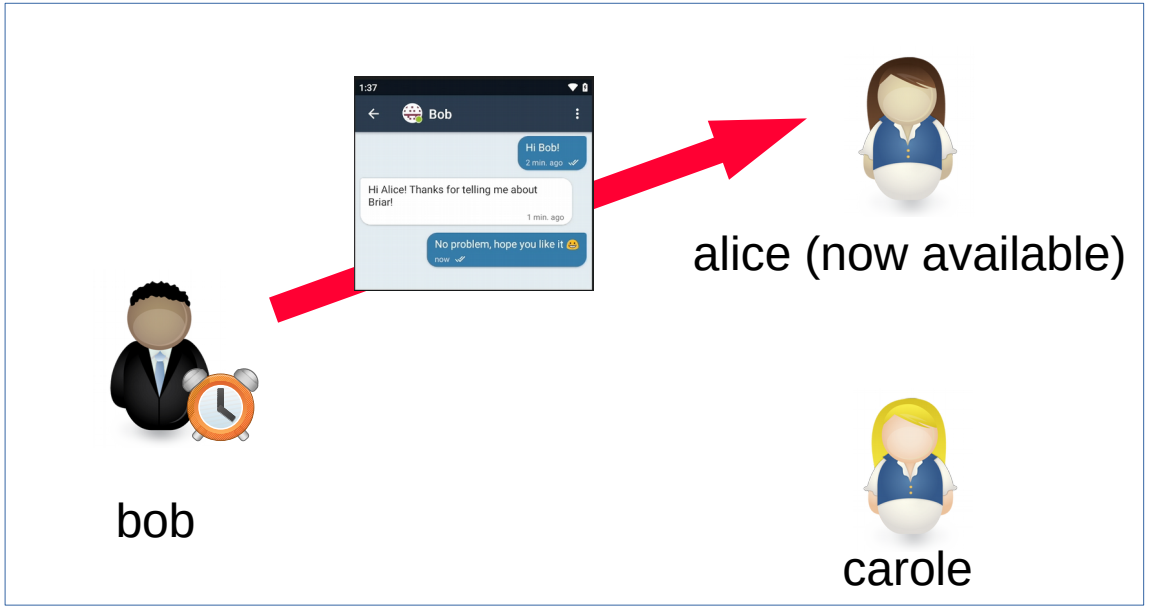
in a peer group of three,
direct messages to alice
go directly to alice



in a peer group of three,
direct messages to alice
go directly to alice

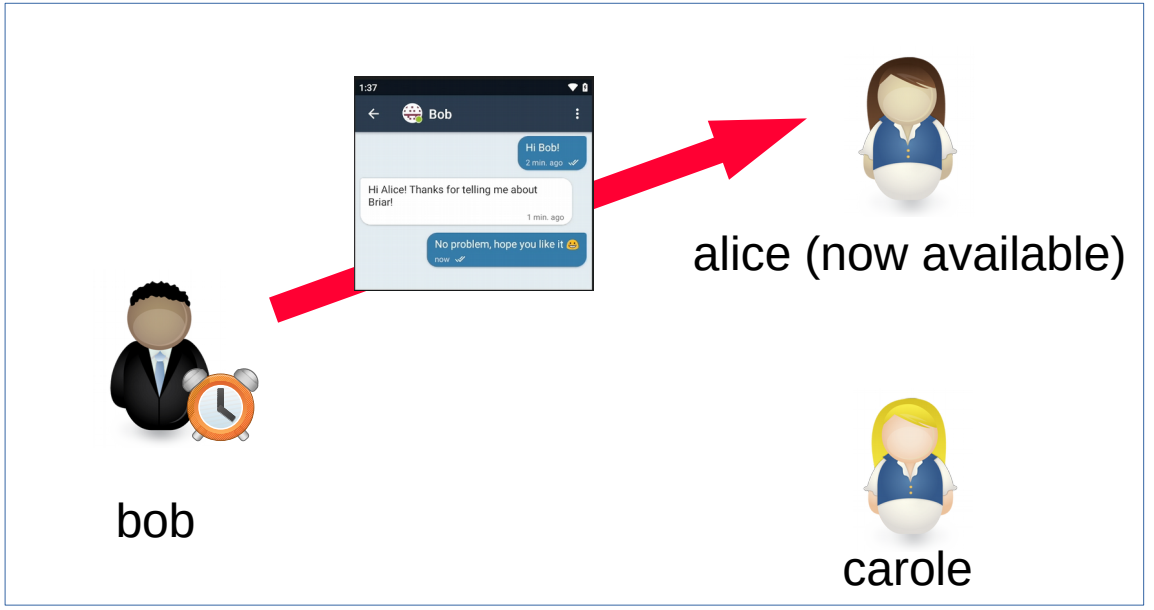


in a peer group of three,
direct messages to alice
go directly to alice, waiting
until she becomes available.
Not shared with all your
contacts, or all Briar users.



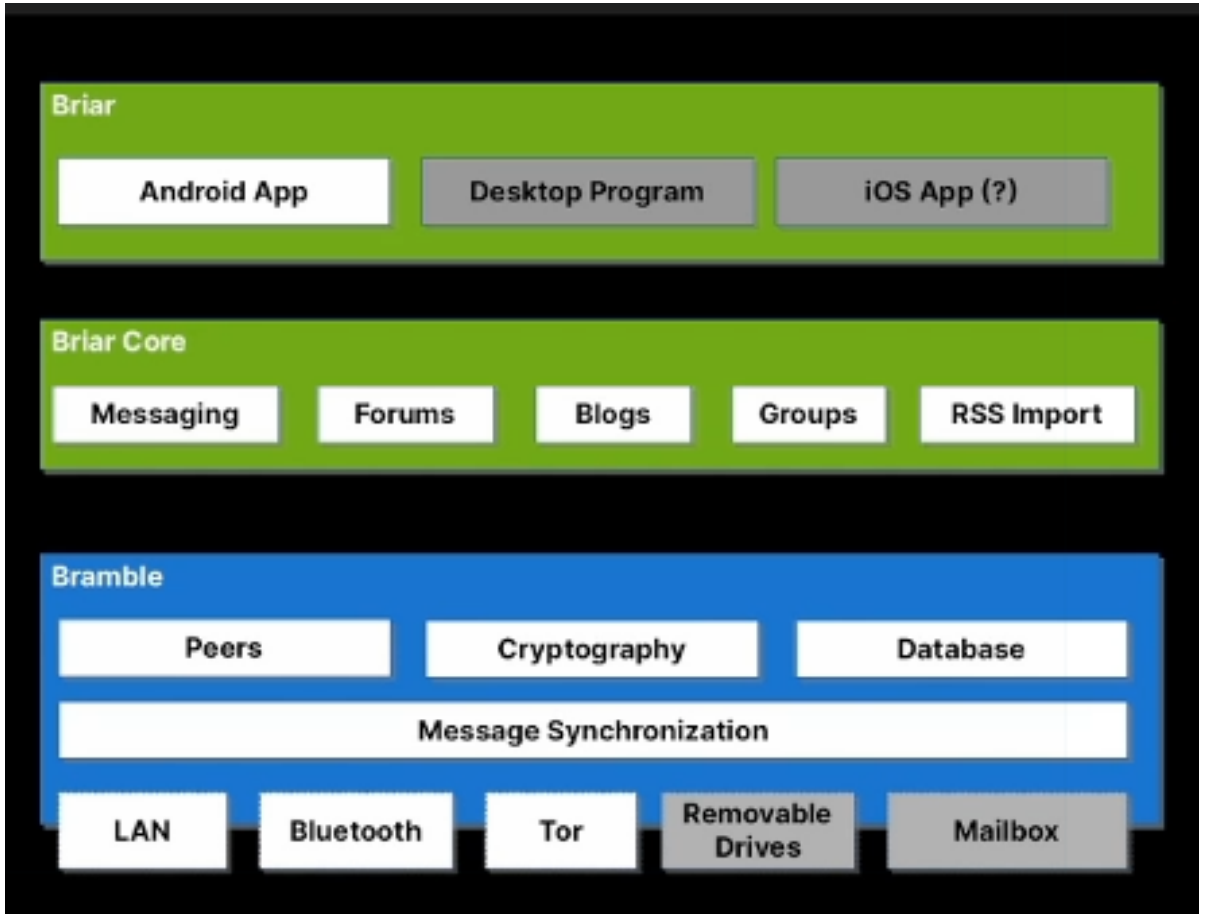
“Single-hop social mesh”

in a peer group of three, direct messages to alice go directly to alice, waiting until she becomes available. Not shared with all your contacts, or all Briar users.



“Single-hop social mesh”

Think about why BATMAN did flooding, and which view of privacy it served. What is traded-off with Briar’s alternative approach?


Briar
Android App
Desktop Program
iOS App (?)
Briar Core
Messaging
Forums
Blogs
Groups
RSS Import
Bramble
Peers
Cryptography
Database
Message Synchronization
LAN
Bluetooth
Tor
Removable Drives
Mailbox