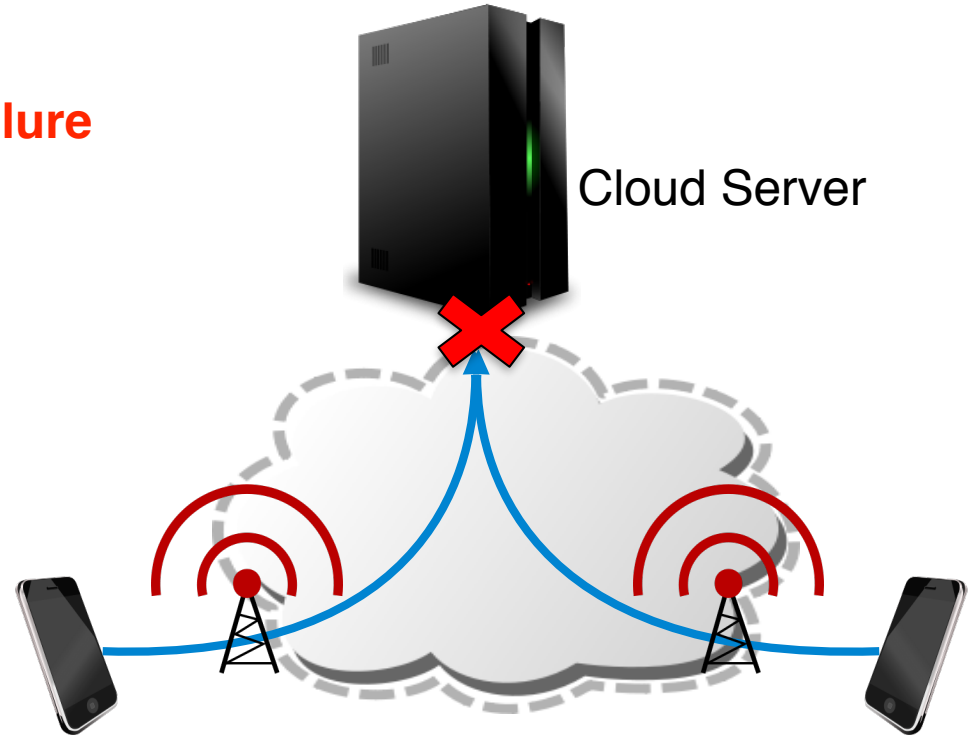
# Background & Motivation: Issues with Traditional Communication cont.

**Central point of failure**

**IP Blacklisting**




**Congestion**

**Kill Switch**

60% of the world has mobile devices

50% of the world is without Internet access

[1] Digital in 2017: Global Overview We Are Social

# Background & Motivation: Issues with Traditional Communication cont.

How Egypt did (and your government could) shut down the Intern

By Iljitsch van Beijnum | Published about a year ago


How hard is it, exactly, to kill the Internet? Egypt seems to have been able to do it. But Egypt's situation isr exactly the same as that in the Western world. And even though Egypt only has four big ISPs, the fact that everything went down after midnight local time suggests that it took considerable effort to accomplish the 'N shut-off. After all, it seems unlikely that President Hosni Mubarak ordered the Internet to be shut down as h went to bed; such a decision must have been made earlier in the day, and then taken hours to execute.

http://arstechnica.com/tech-policy/2011/01/how-egypt-or-how-your-government-could-shut-down-the-internet/

FireChat Prepares Encryption Feature As It Drives Hong Kong Protests

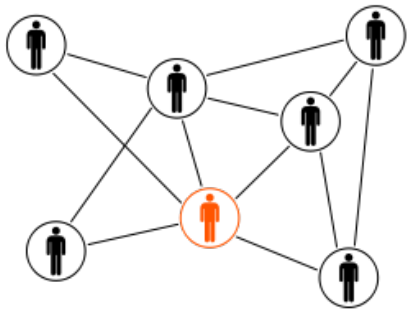
+ Comment Now + Follow Comments

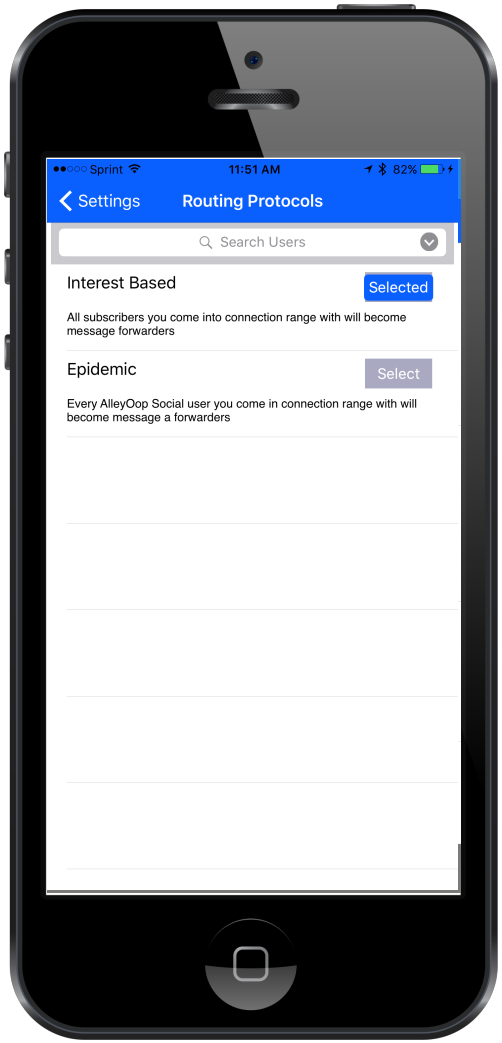
FireChat powered protests at the Burning Man festival, allowing users to communicate off-the-grid when Internet connections were sluggish and/or nonexistent. FireChat was downloaded over 100,000 within a 24 hour period

http://www.forbes.com/sites/parmyolson/2014/09/29/firechat-prepares-encryption-feature-as-it-drives-hong-kong-protests/

# AlleyOop Social Research Platform

- A Low Latency Evaluation sYstem for ad-hOc Opportunistic Passing (AlleyOop Social)
- No jailbreak needed
- Capabilities
  - Online/offline social network
  - Publish/subscribe system
  - Disseminate messages using D2D connections
  - Secure message delivery
  - Can run multiple DTN wireless protocols
  - Link Facebook & Twitter accounts



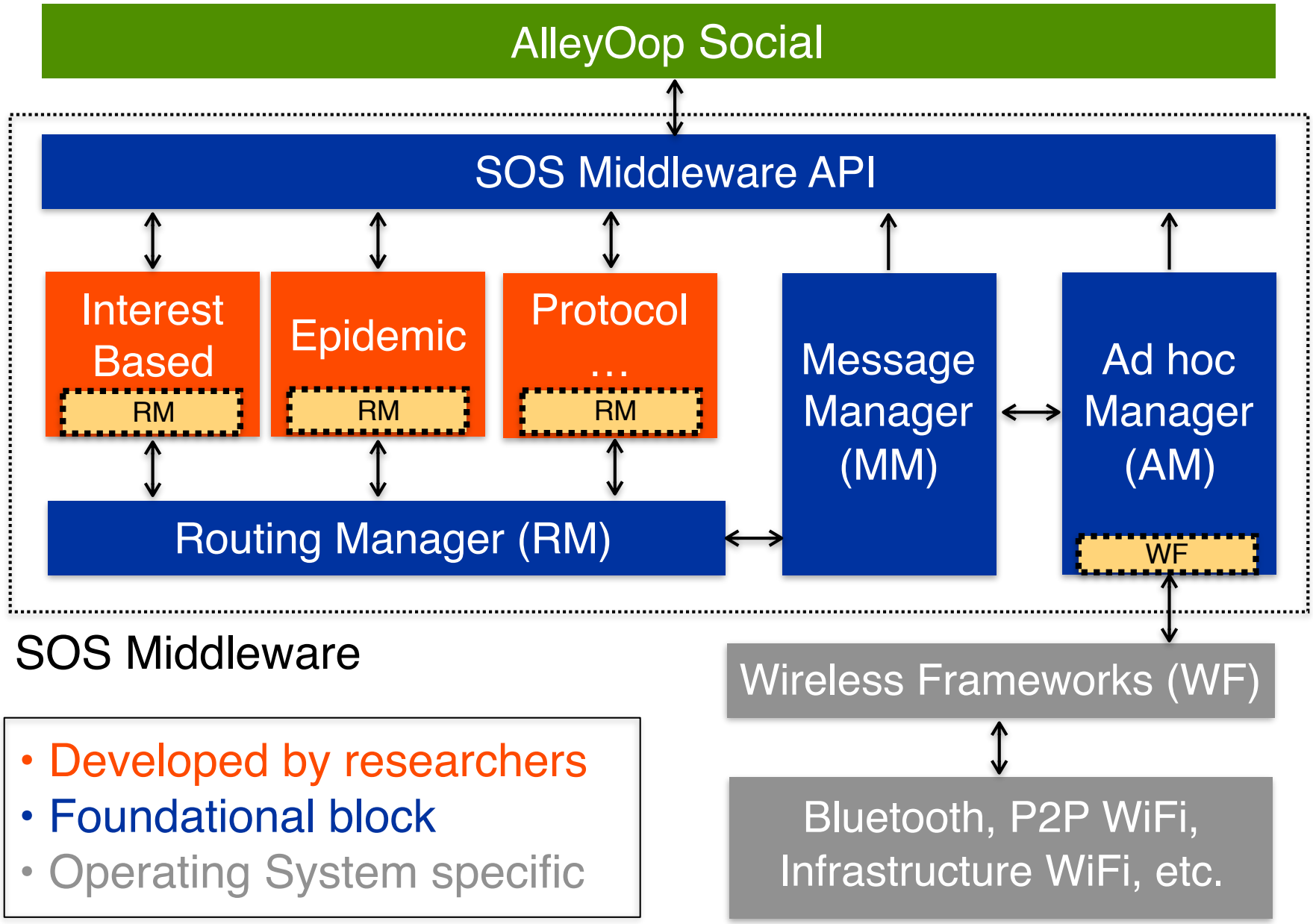




[1] **Baker CE** et. al, “In vivo evaluation of the secure opportunistic schemes middleware using a delay tolerant social network” 2017 IEEE ICDCS

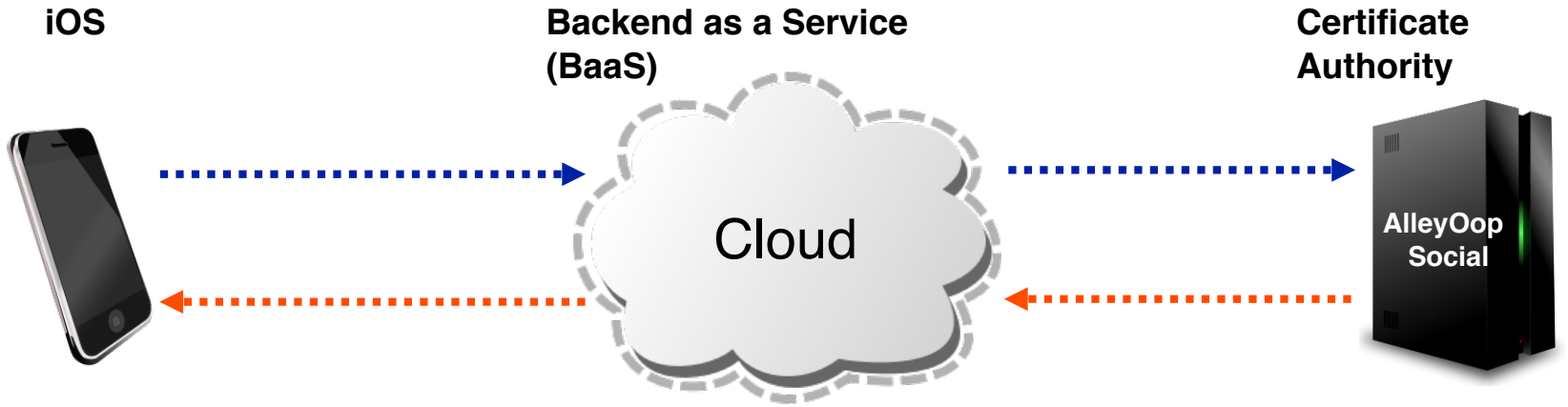
[2] **Baker CE** et. al, “A research platform for real-world evaluation of routing schemes in delay tolerant social network” 2017 IEEE INFOCOM

# AlleyOop Social & Secure Opportunistic Schemes Middleware




- Developed by researchers
- Foundational block
- Operating System specific

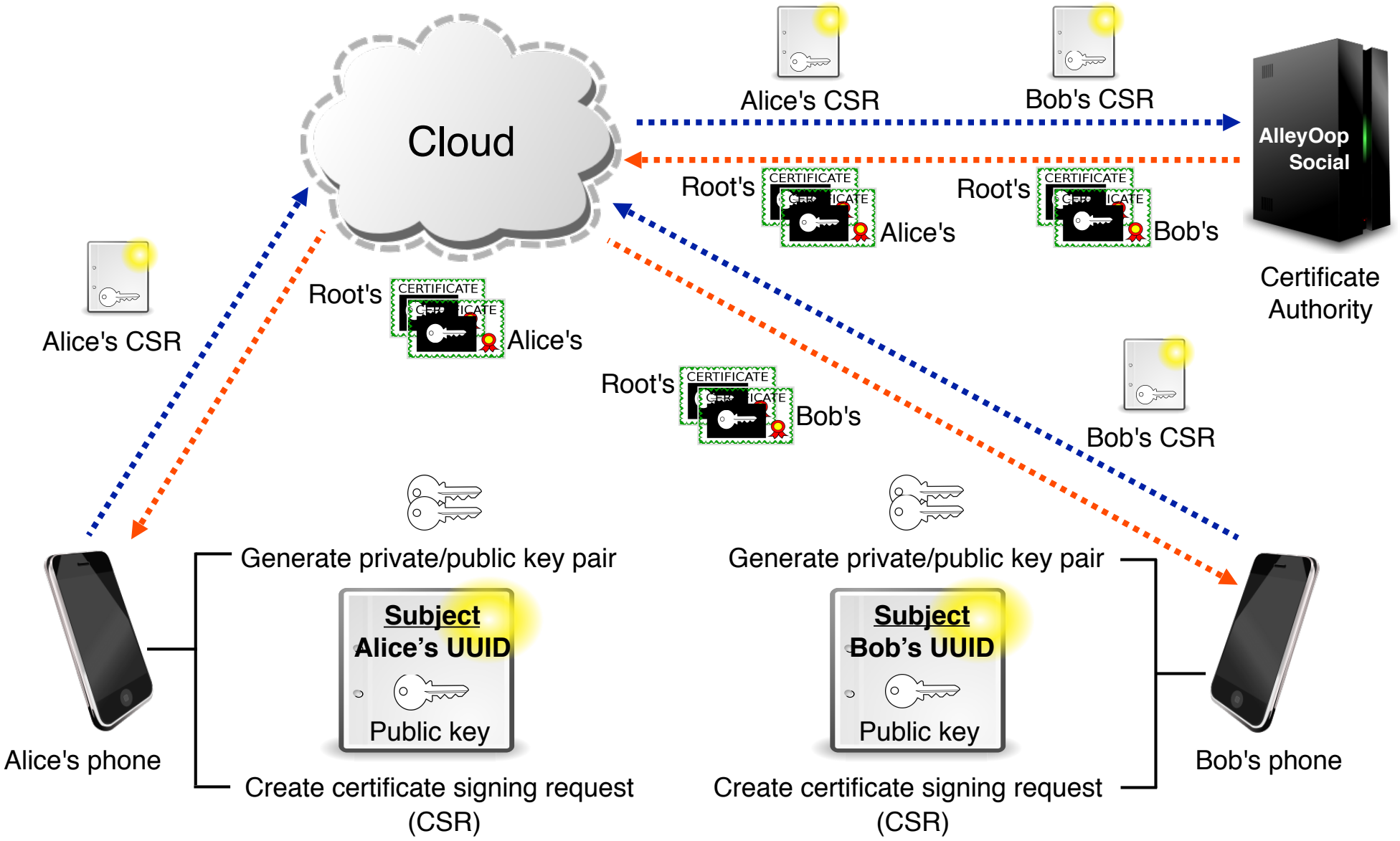
# AlleyOop Social Architecture



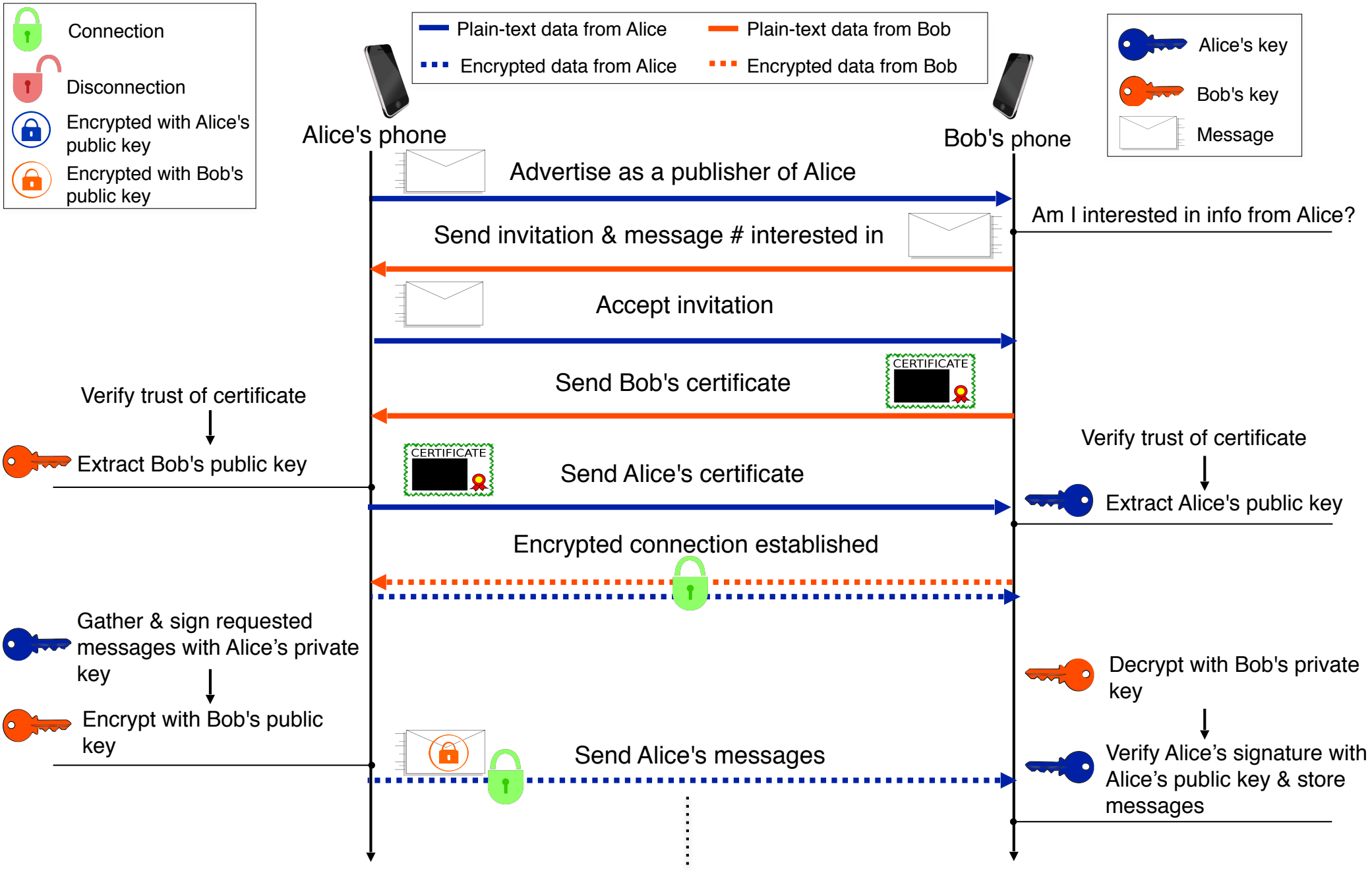

## Architecture & Capabilities

| | | |
|---|---|---|
| • iPhone, iPad, and iPod<br>• Swift<br>• SOS Middleware | • Cloud database management<br>• Push notifications<br>• App tracking analytics<br>• Javascript | • Powered by nodejs<br>• RESTfull API's<br>• Openssl<br>• Mysql<br>• Javascript |
| **Functionality** | | |
| • D2D: Bluetooth, P2P WiFI, Infrastructure WiFi<br>• DTN Routing<br>• Generate private/public keys & certificate signing requests<br>• 16 simultaneous connections<br>• Communicates directly to other mobile devices & BaaS | • Handles account creation for all users<br>• Store all user info when cloud is available<br>• Facilitates certificate creation and revocation<br>• Communicates directly to mobile devices and AlleyOop Social Certificate Authority | • Creates certificates from certificate signing request<br>• Stores certificate for each users mobile device<br>• Communicates directly to BaaS |

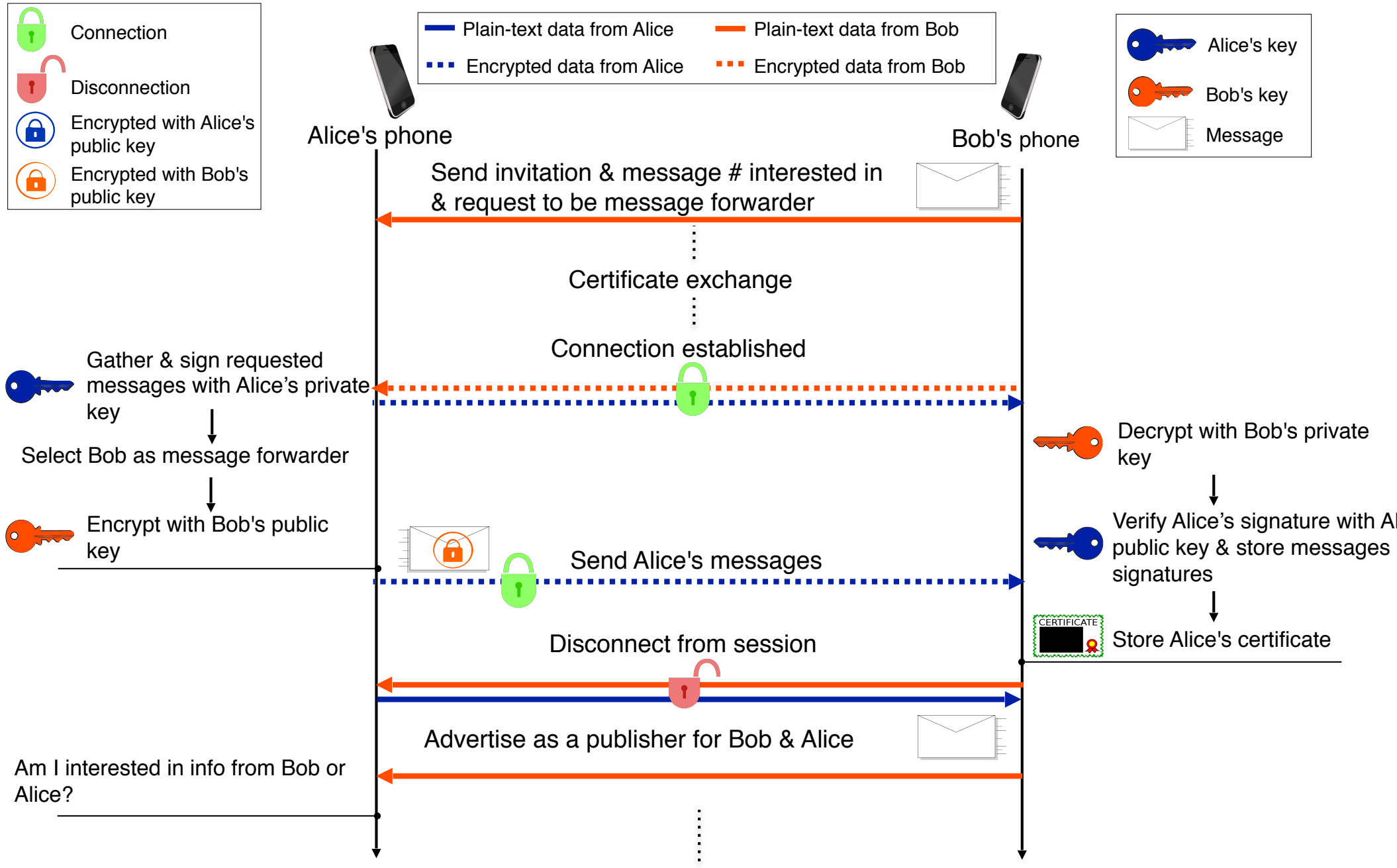
# Enabling Offline Security: One-time Infrastructure Requirement



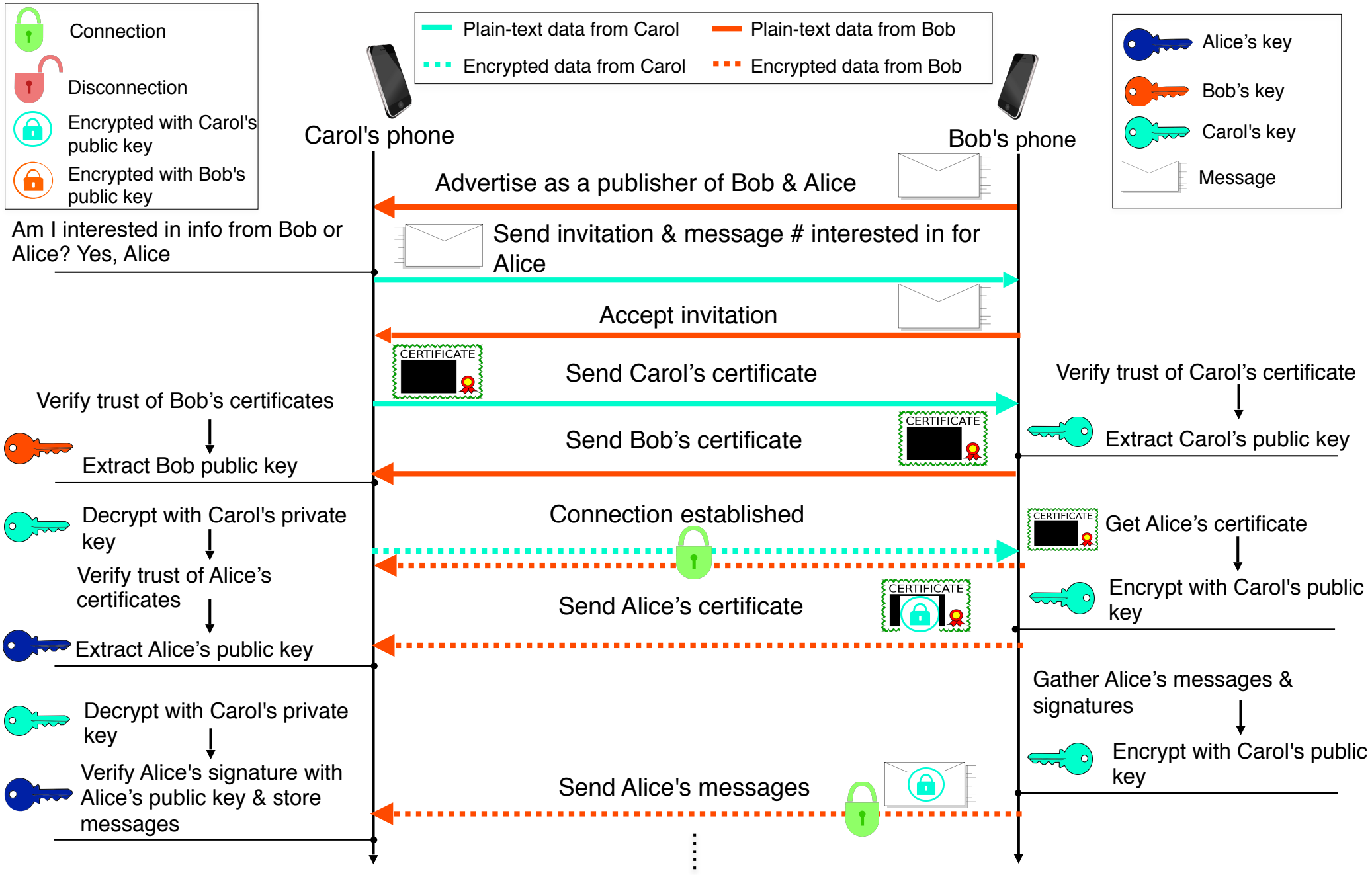
# AlleyOop Social Decentralized Communication



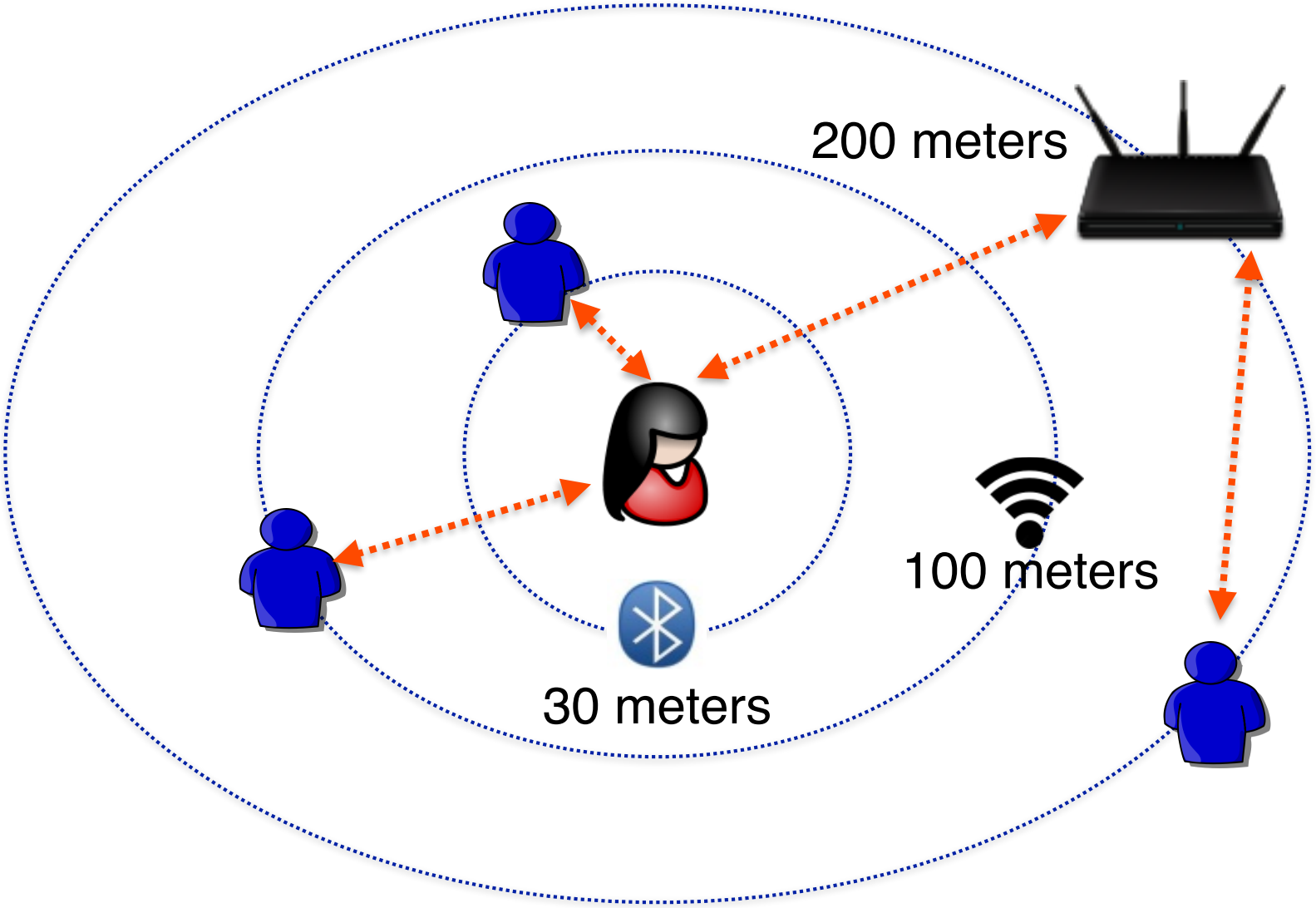
# AlleyOop Message Forwarder Selection



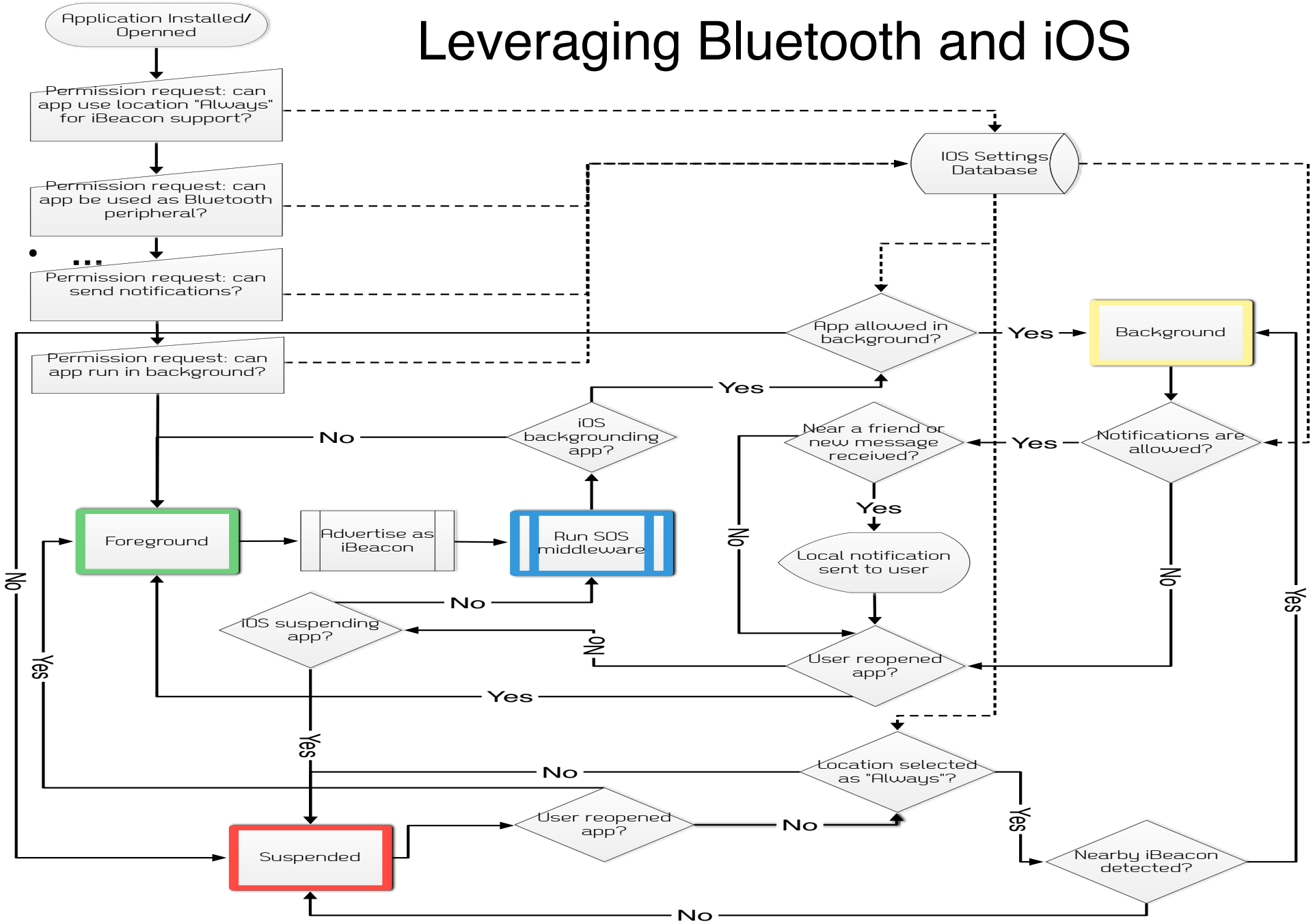
# AlleyOop Message Forwarder Dissemination



# Wireless Communication Range



# Leveraging Bluetooth and iOS



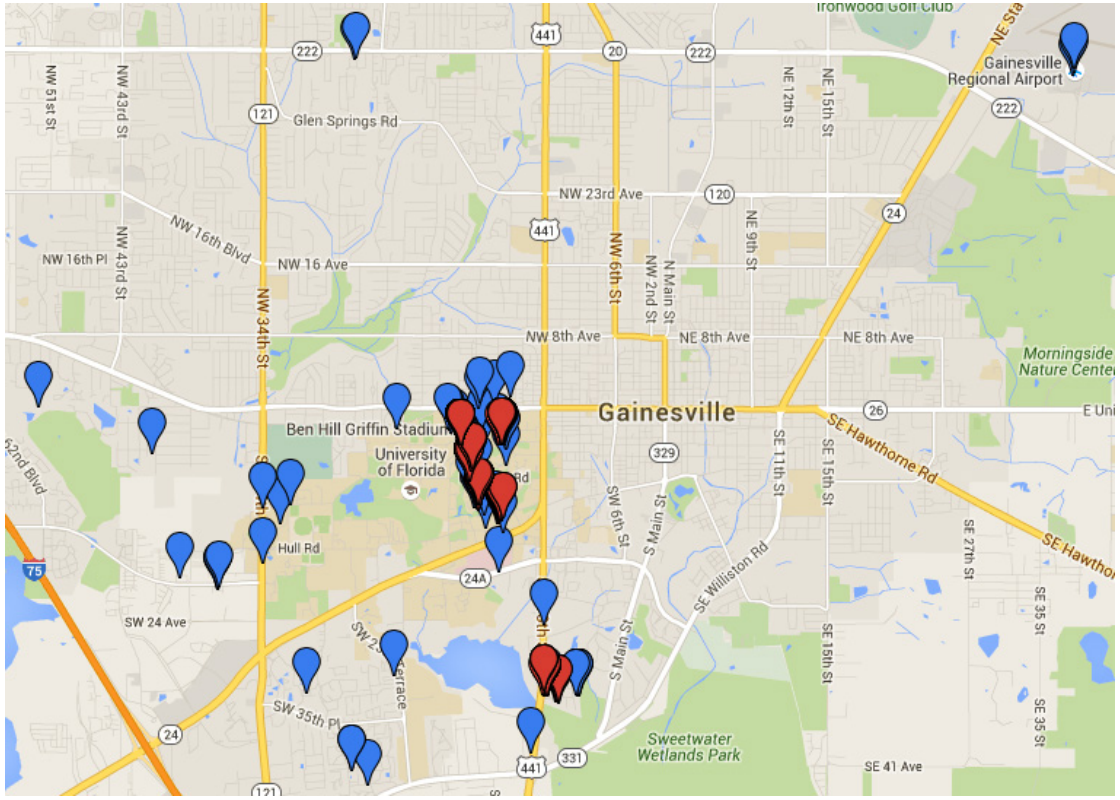
# SOS Middleware Security

| | **Values** |
|---|---|
| Key type | Elliptic curve (EC), RSA |
| Key size (bits) | **EC: 256**<br>RSA: 512, 1024, 2048 |
| Hashing algorithms | **SHA-256**, SHA-512,<br>SHA-1024, SHA-2048 |

**Note: bold is default**

# Preliminary Results

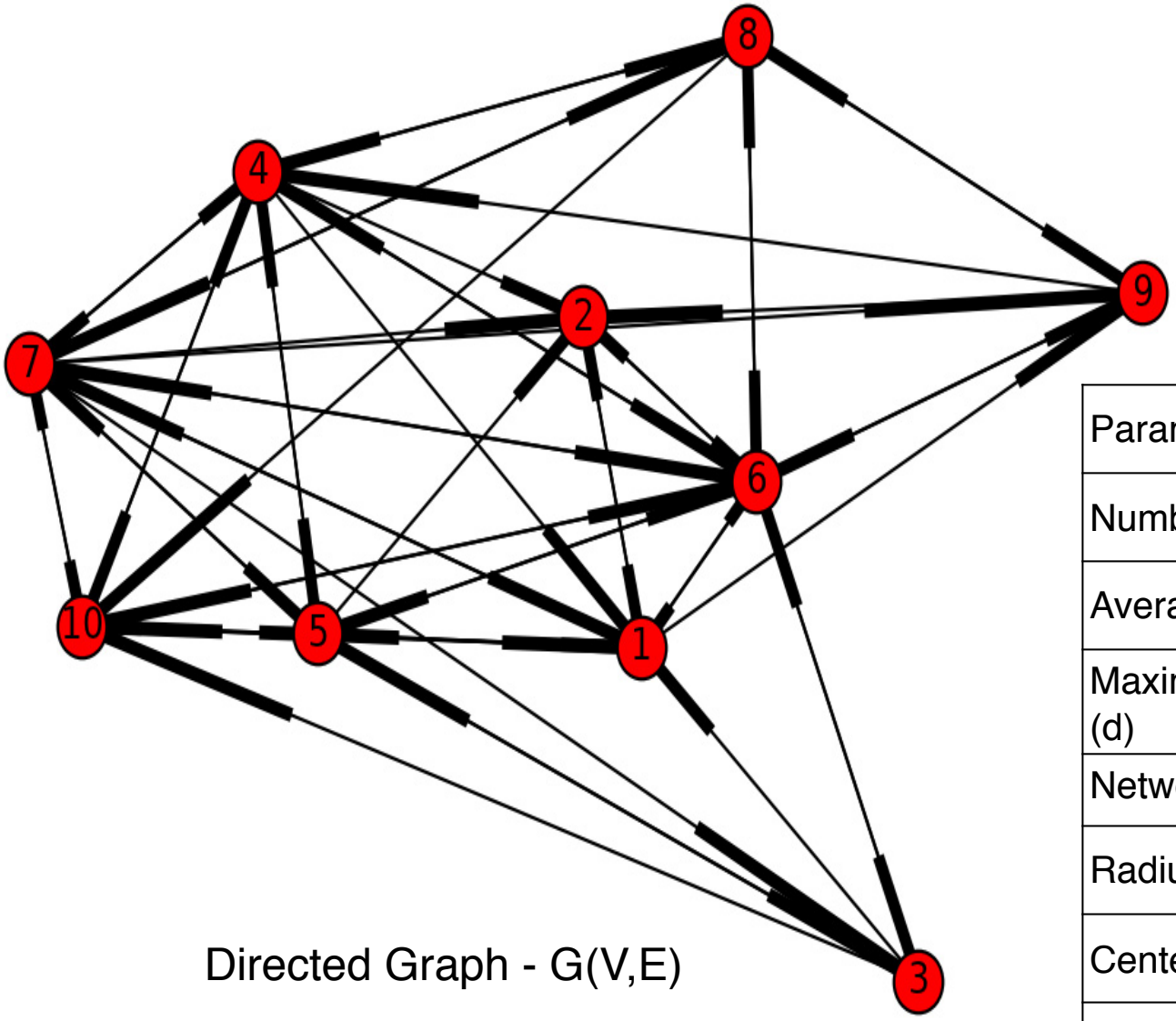
# *In Vivo* Evaluation: Environment




Gainesville, FL
Area: 11km x 8km

| Parameters | **Active** |
|---|---|
| Number of nodes (n) | 10 |
| Duration (days) | 7 |
| Total messages created | 259 |
| Total messages disseminated (1-hop) | 796 |
| Total messages disseminated (>1-hop) | 167 |

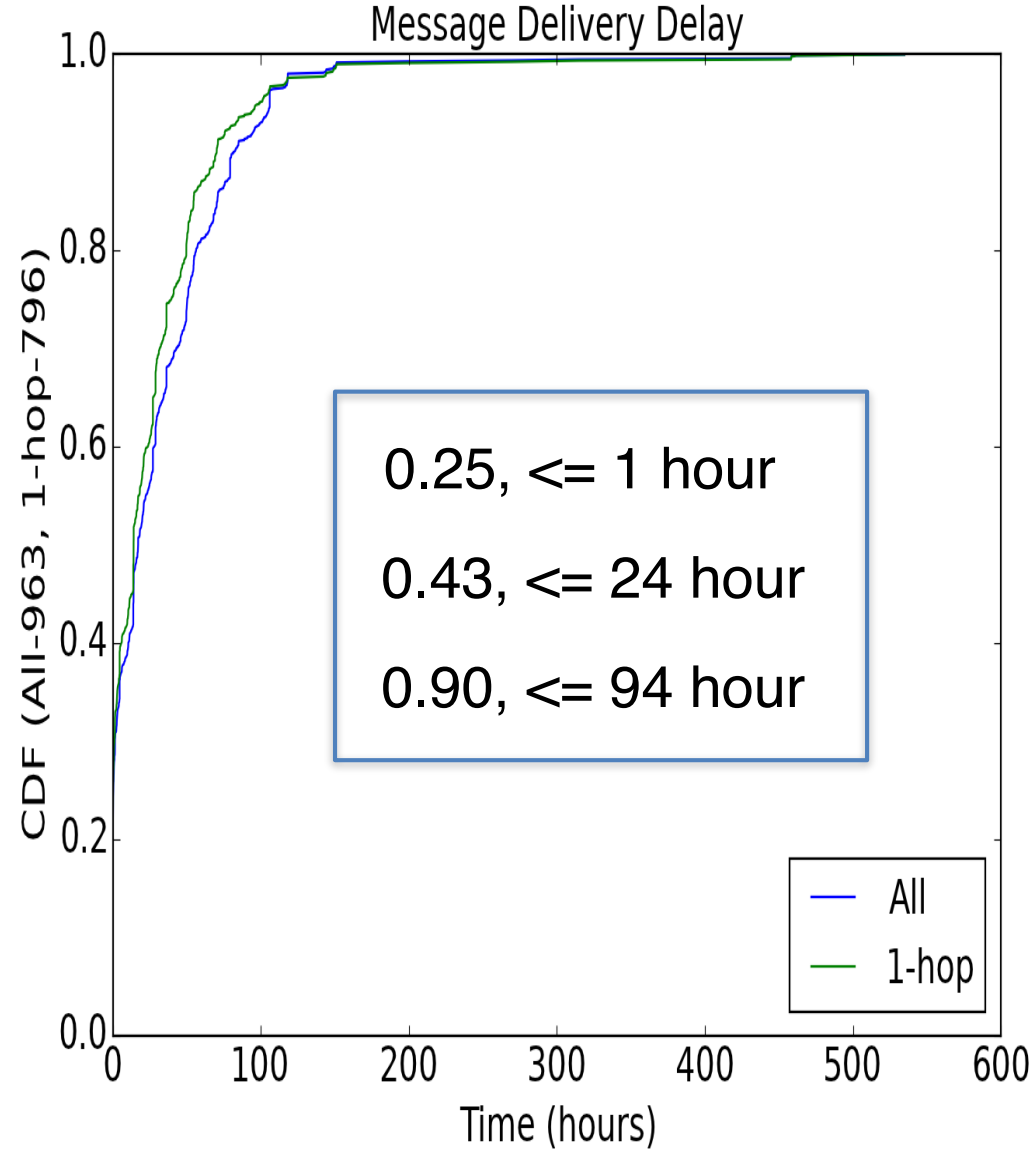
# *In Vivo* Evaluation: Social Relationships

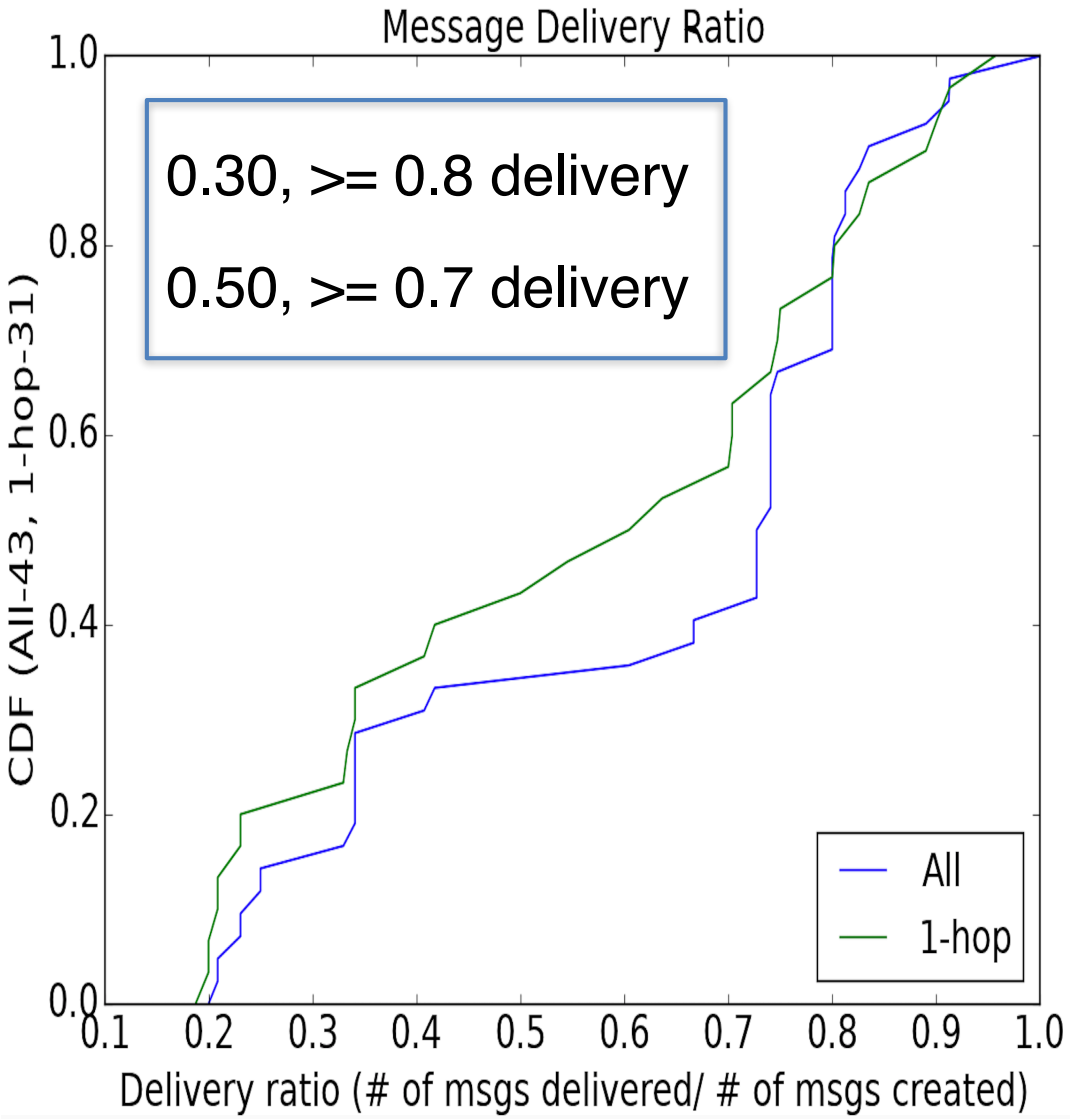



Directed Graph - G(V,E)

| Parameters | **Values** |
|---|---|
| Number of nodes (n) | 10 |
| Average shortest path length | 1.3 |
| Maximum shortest path length (d) | 2 |
| Network density | 0.64 |
| Radius | 1 |
| Center nodes | 6 and 7 |
| Transitivity | 0.80 |

# *In Vivo* Evaluation: Results



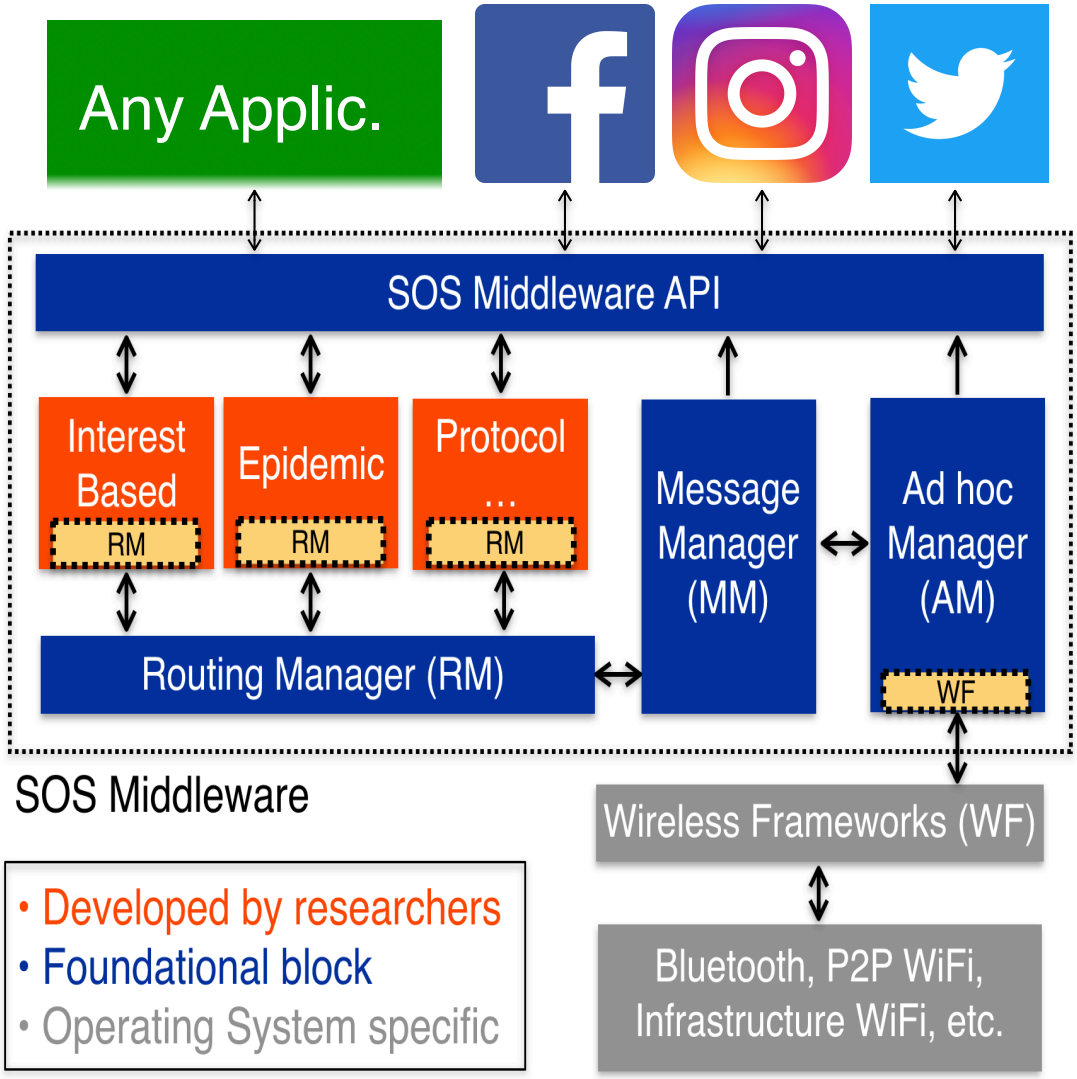
# Protocols Evaluated in Simulation

| Protocol | **Nodes** | ***Transmission Range*** | ***Area*** |
|---|---|---|---|
| Interest based routing (Baker et al. 2017) | 10 | 5m - 50m | 88km$^2$ |
| Epidemic routing (Vahdat et al. 2000) | 50 | 25m | .45km$^2$ |
| PRoPHET (Lindgren et al. 2004) | | 50m | 4.5km$^2$ |
| | | 100m | |
| CAR (Musolesi et al. 2009) | | 200m | 1km$^2$ |
| SocialCast (Costa et al. 2008) | 100 | | 16km$^2$ |
| CAR (Musolesi et al. 2000) | | 250m | 2km$^2$ |

[1] **Baker CE** et. al, “Efficient routing using evolving community structures in mobile delay tolerant social networks” (In-progress)

# Future Work

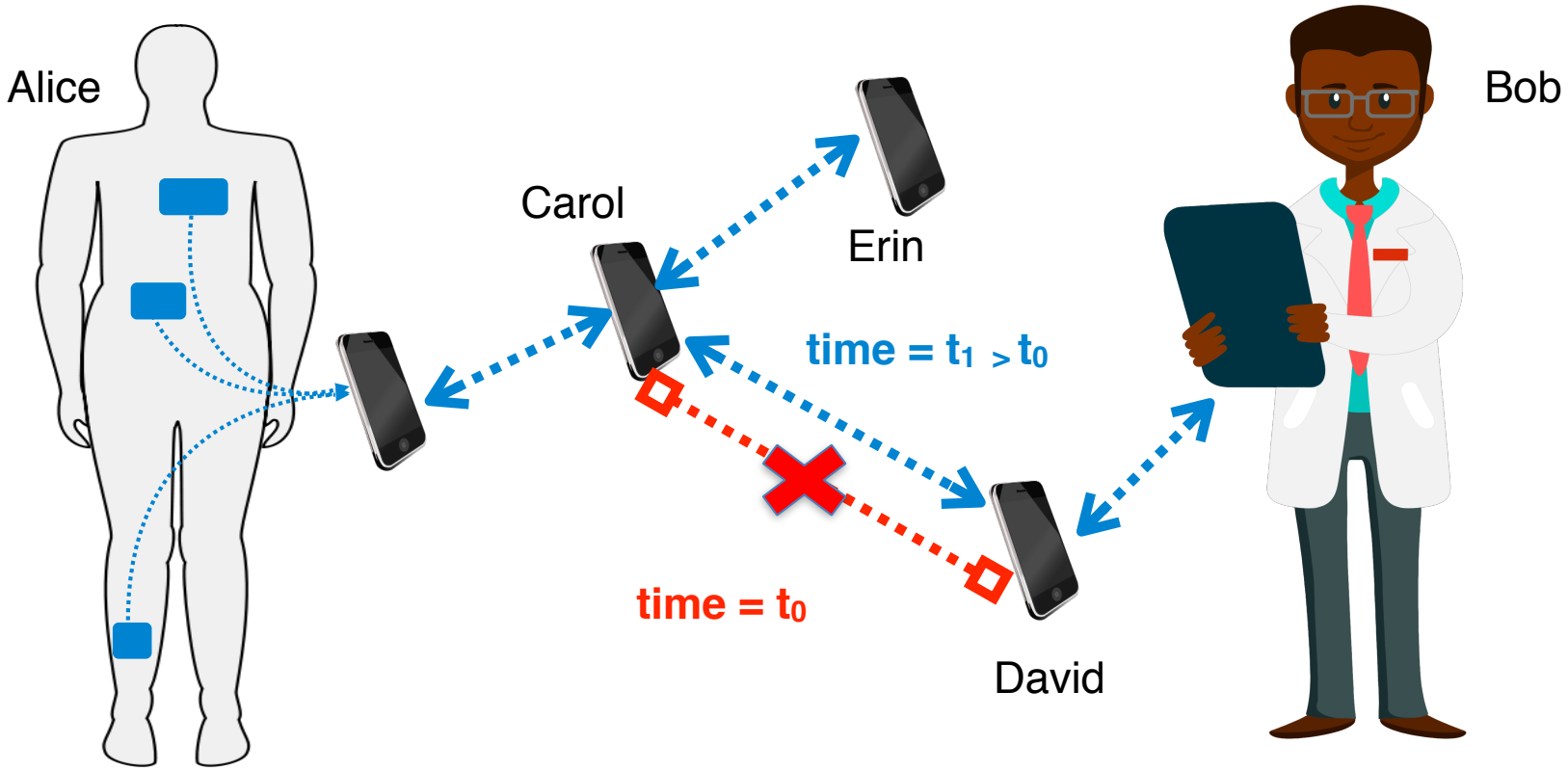
# Future Work




- 1 patent
- 3 employees
- 1 angel invester
- Part of Qi at UCSD

TECHNO 1 GIES

# Future Work: Opportunistic Medical Patient Monitoring




# Related Work

Related

- Haggle Project[1]
- OS: Linux, Android (rooted), iOS (partially)
- Runs system wide
- Conceptually discusses security (no claim framework is secure)
- Captures node interaction times

AlleyOop Social / SOS Middleware

- OS: iOS
- Runs as a framework in any application
- Easy incorporation of many routing schemes (<100 lines of code)
- Captures node interaction along with ability to leverage OS

[1] Su et. al, “Haggle: Seamless networking for mobile applications”, Springer 2017, https://code.google.com/archive/p/haggle/