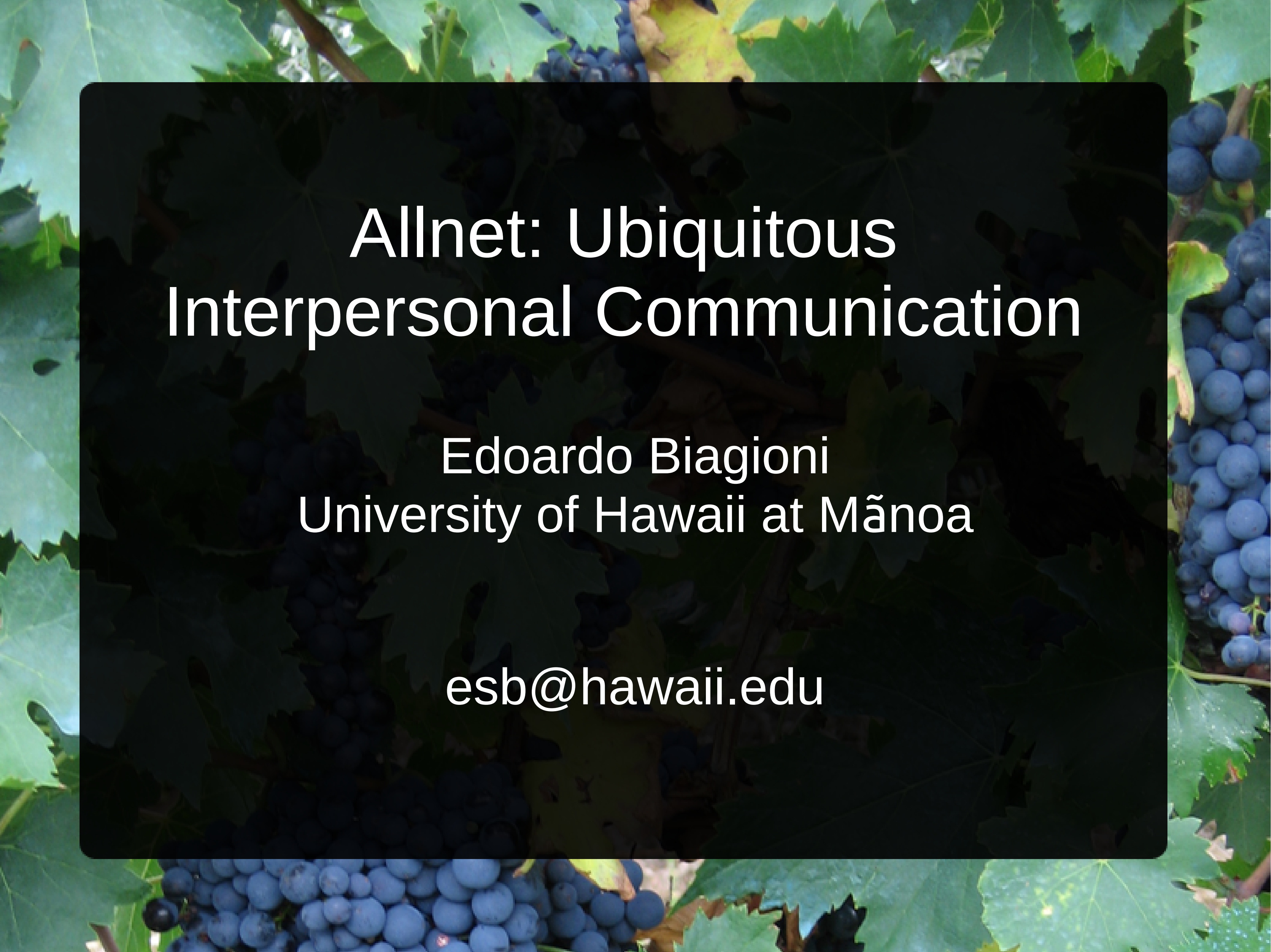


Allnet: Ubiquitous Interpersonal Communication

Edoardo Biagioni
University of Hawaii at Mãnoa

esb@hawaii.edu

Basic Idea

- The radio in my cellphone can talk to the radio in your cellphone
- There is no software in my cellphone to talk to the software in your cellphone
- Why not?
- What can such ad-hoc communication be useful for?

Observations

- Useful interpersonal communication do not require much bandwidth
  - Ubiquitous connectivity from 1% each
- Phones are actually computers
- Any centralized system has a central point of failure

=> distributed system to deliver small amounts of data (text messages)

Outline

- Introduction and Motivation
- Basic Design
- Forwarding and Routing
- Social Network
- Resource Control
- Status and Summary

Basic Design of AllNet

- Designed to work well with few bits and few round-trips
- Untrusted network components require pervasive encryption
- Broadcasting is a backup to Routing
  - And maybe better in transient networks
- Message prioritization solves many ills

Low bandwidth communication

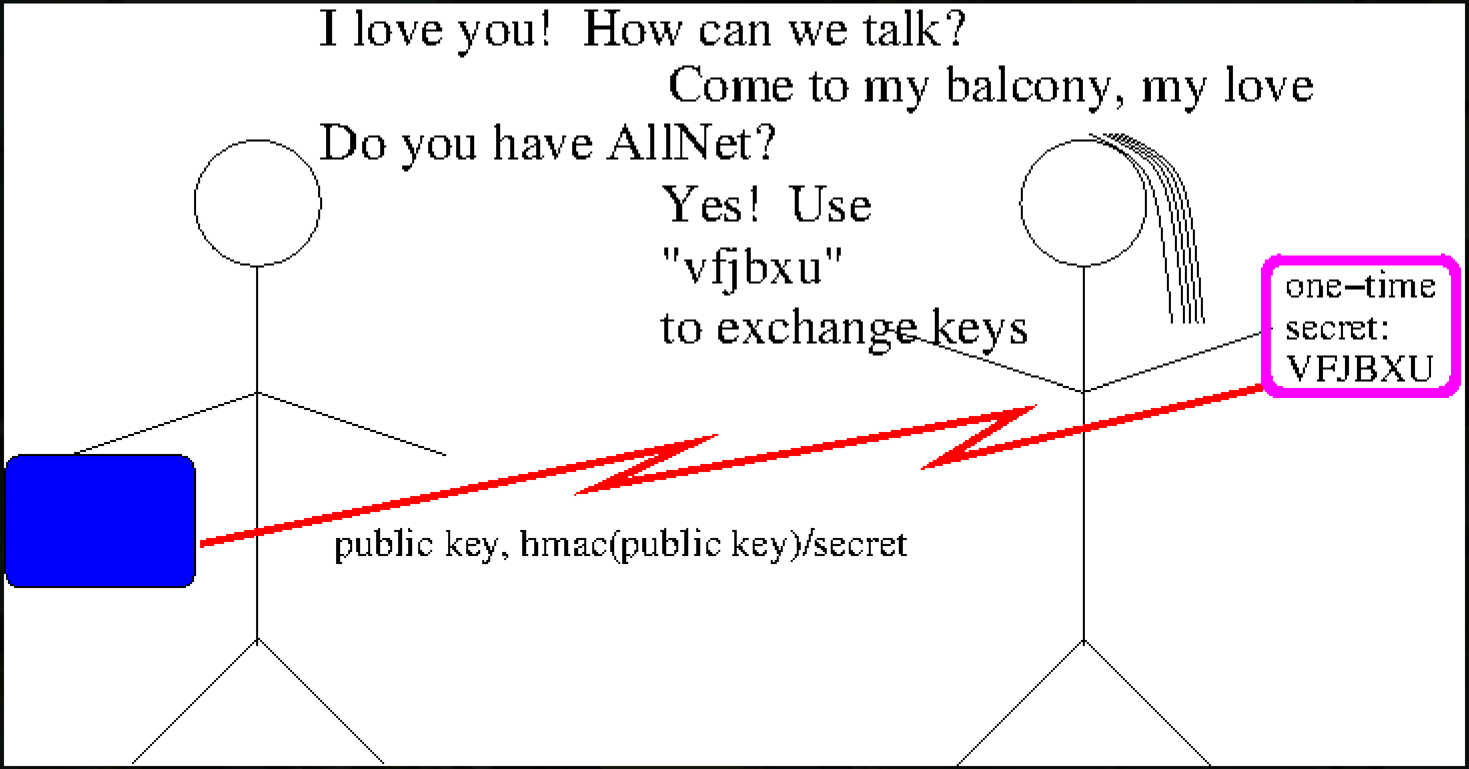
- Short text messages
- Sent best-effort over UDP, WiFi, other technologies (cognitive), and Internet
- Stored permanently at sender
- Stored at intermediate nodes until acked or displaced by higher-priority messages

Security Assumptions

- My device is under my control
- Public-Key cryptography is secure
- Verifying signatures is fast

- Security should work in a high-school classroom
  - must be simple and effective

Romeo meets Juliet



I love you! How can we talk?

Come to my balcony, my love

Do you have AllNet?

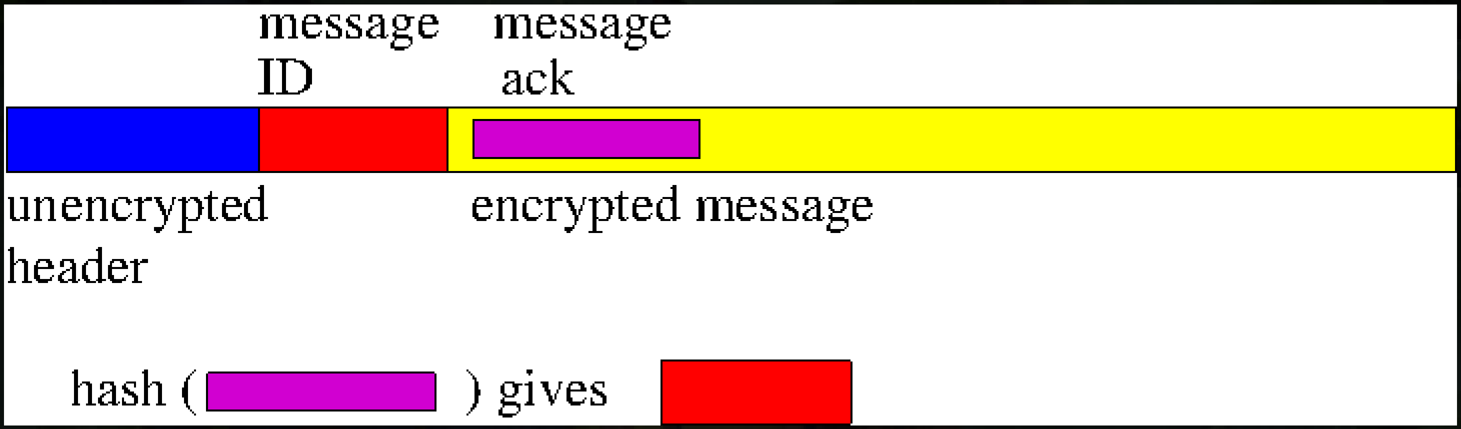
Yes! Use "vfjbxu" to exchange keys

Encryption and Authentication

- Messages between individuals who know each other's public key are:
  - Encrypted (RSA, + AES for long msgs)
  - Then digitally signed
- I only decrypt if I can verify the signature
- Everything else is “from unknown”/spam

Secure Acknowledgements

- Encrypted payload has bytes of ack
- Only a recipient that can decrypt the payload can generate a valid ack



Message Caching

- Intermediate nodes keep message until ack is seen
- Or until they need to reuse the space
- Recipient can request cached messages
  - Lets recipient be online intermittently
  - Data Mules work like intermediate nodes

xchat

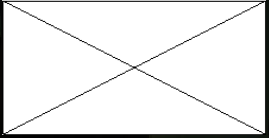
- Distributed chat over AllNet
- Key exchange
- Exchange of encrypted messages
  - Sequence numbers and timestamps
  - Same seq, newer time is correction
- Pidgin (http://pidgin.im/) as user interface

Outline

- Introduction and Motivation
- Basic Design
- Forwarding and Routing
- Social Network
- Resource Control
- Status and Summary

Message Delivery

- Across the Internet
  - To Rendezvous Points, if known
  - To Distributed Hash Table nodes
  - Directly to destination, if possible
- Broadcast on all attached LANs
- Hop count limits distribution
- Low hop limit gives higher priority



Addressing and Routing

- Addresses are self-selected 64-bit strings
  - e.g. the hash of “edo using AllNet”
  - can use fewer than 64 bits
- Addresses identify parts of the network:
  - Distributed Hash Table (DHT)
  - Configured Rendezvous Points (Rps)
- Routing uses broadcast locally
  - On LANs+for Delay Tolerant Networking

Related work: BitMessage

- In principle, every message broadcast to every node
- Every message kept for two days
- If too many messages, messages are stored on only part of the network
- Recipients know which part of the network has their messages

AllNet Routing Considerations

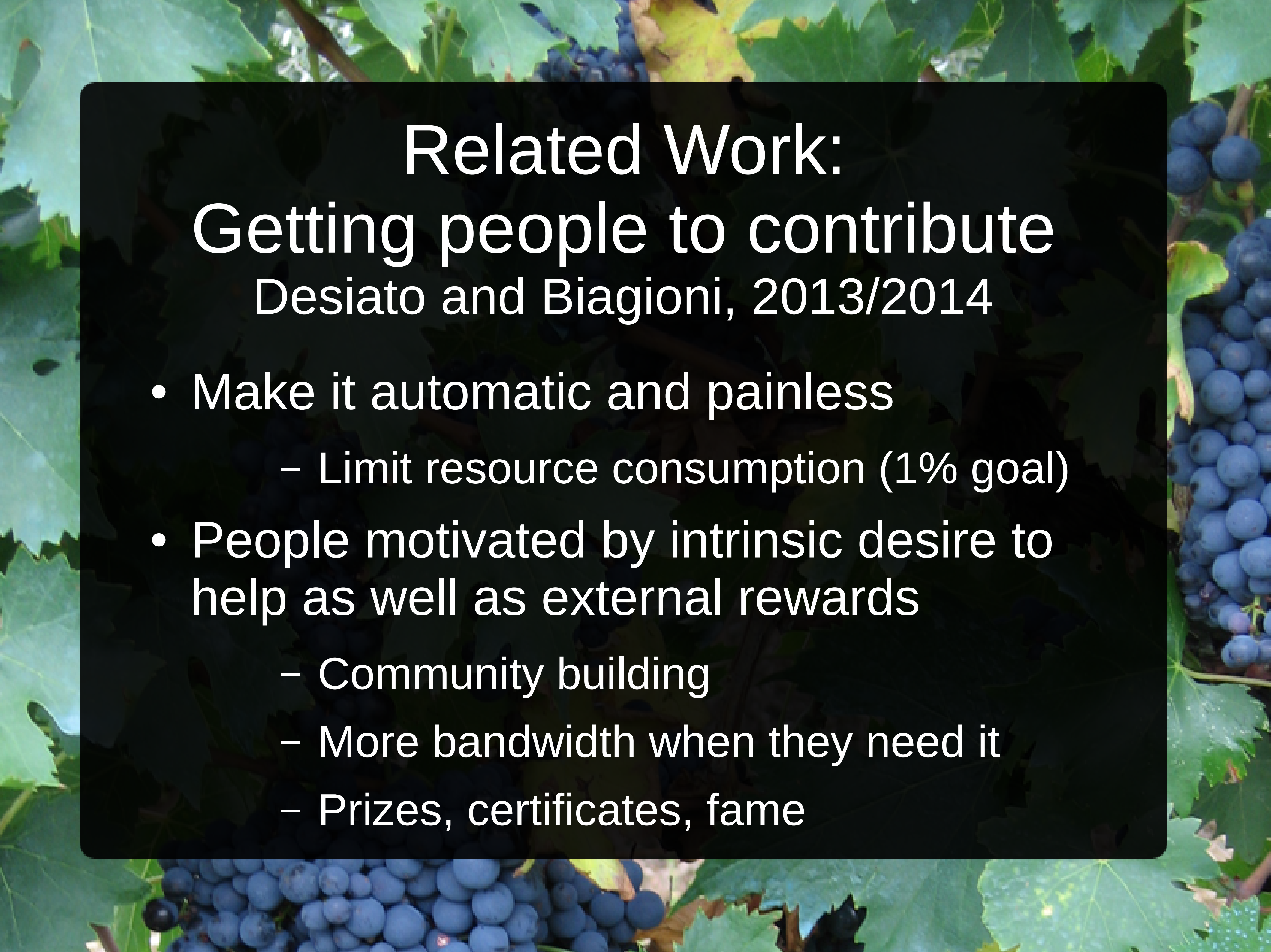
- When traffic is low, OK to forward everything everywhere
- When traffic is high, only forward high priority messages
- With prioritization, limited broadcast OK
- Pure broadcast lessens the effectiveness of traffic analysis

Outline

- Introduction and Motivation
- Basic Design
- Forwarding and Routing
- Social Network
- Resource Control
- Status and Summary

Distributed Social Network

- I can give you my friends' public keys
- If they match yours, we have friends in common
- You can introduce me to your friends
  - Messages won't go to the spam box
- You can recognize my friends' messages
  - and give them higher priority



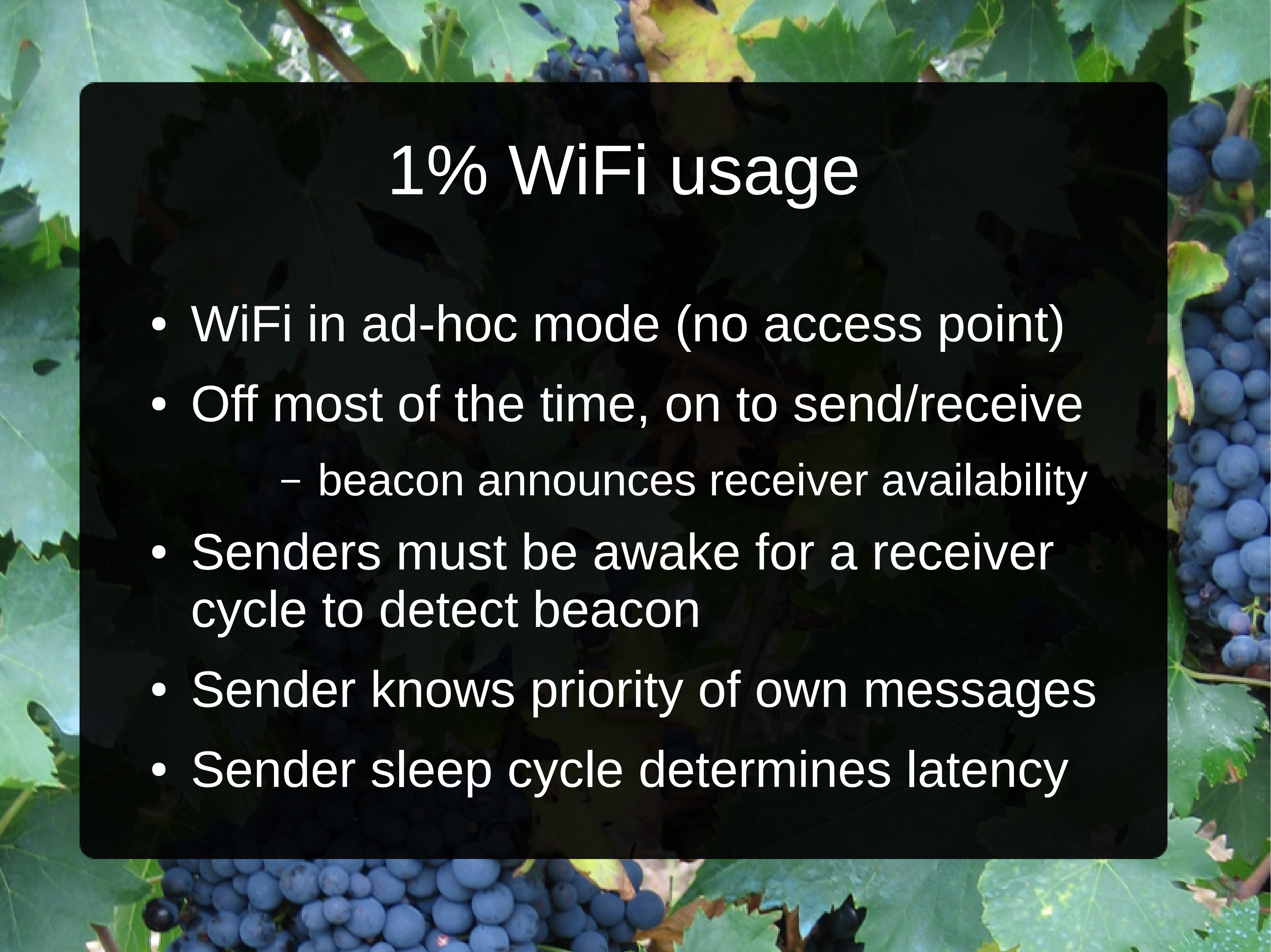
Related Work: Getting people to contribute

Desiato and Biagioni, 2013/2014

- Make it automatic and painless
  - Limit resource consumption (1% goal)
- People motivated by intrinsic desire to help as well as external rewards
  - Community building
  - More bandwidth when they need it
  - Prizes, certificates, fame

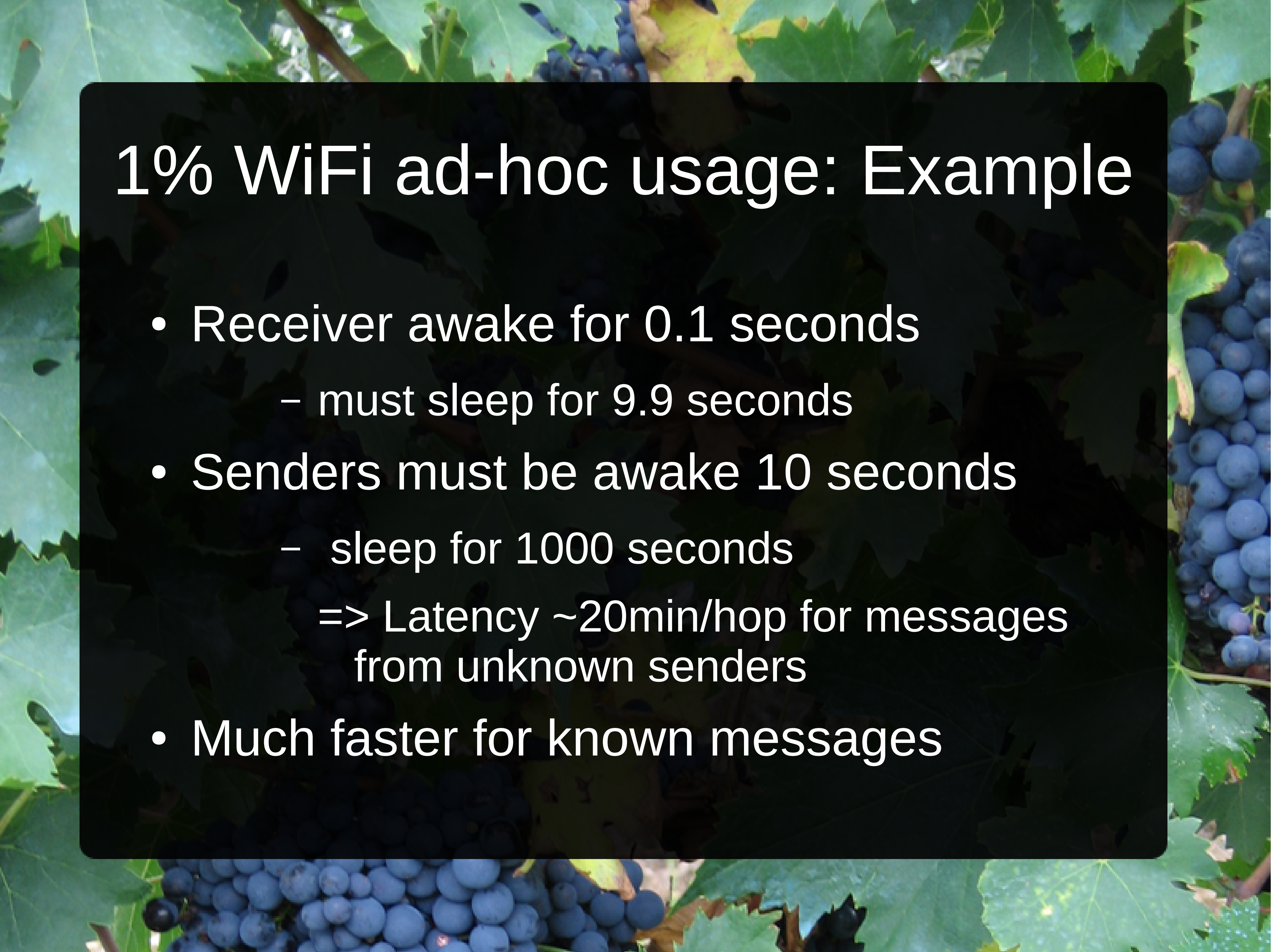
Outline

- Introduction and Motivation
- Basic Design
- Forwarding and Routing
- Social Network
- Resource Control
- Status and Summary



1% WiFi usage

- WiFi in ad-hoc mode (no access point)
- Off most of the time, on to send/receive
    - beacon announces receiver availability
- Senders must be awake for a receiver cycle to detect beacon
- Sender knows priority of own messages
- Sender sleep cycle determines latency



1% WiFi ad-hoc usage: Example

- Receiver awake for 0.1 seconds
  - must sleep for 9.9 seconds
- Senders must be awake 10 seconds
  - sleep for 1000 seconds

    => Latency ~20min/hop for messages from unknown senders
- Much faster for known messages

Outline

- Introduction and Motivation
- Basic Design
- Forwarding and Routing
- Social Network
- Resource Control
- Status and Summary

AllNet Status

- Version 2 released, tested
  - xchat application with pidgin as GUI
  - time broadcast server
  - key exchange and security
- Version 3 under development
  - Distributed Hash Table
  - streaming, larger messages for multimedia

Summary

- Key exchange is less difficult with portable wireless devices => easier security
- Conventional addresses not very good for mobile devices – some broadcasting required
- Basic connectivity need not require big expensive resources

`http://www.alnt.org/`

Usage Scenario I

- Internet-connected host with public IP address
- Contributes to DHT, stores others' data
- Immediate delivery of data from other DHT nodes that it listens to
- May give senders its IP address for direct delivery

Usage Scenario II

- Mobile Device intermittently connected to Internet
- Carries data (Data Mule) and forwards it based on priority
- Tries to deliver data over ad-hoc network
- May use others to deliver its data

Usage Scenario III

- Group separated from the Internet
- Supports communication within the group
- High data rates supported with direct communication
- May use ad-hoc communication over unrelated devices