AllNet

Ubiquitous secure shared connectivity

over existing hardware

E. Biagioni
University of Hawaii at Manoa
Information and Computer Sciences
January 2012

“twitter revolutions”

- arab spring revolutions – Tunisia and Egypt, Libya and Syria
- using social media to organize protests against authoritarian governments
- twitter and facebook are centralized, relatively easy to block
- peer-to-peer networking is notoriously hard to block

Emergency Communications

- Cellphones provide excellent emergency communication capabilities, including SMS
- But what if the infrastructure is not available?
- Cellphone to cellphone communication should still be possible
- How to train users and install software?

Low-resource Internet Sharing

- Most of the time that I have an internet connection, I am not using it
- I could make a small fraction of that bandwidth available to others
- Who could send and receive SMS-like and twitter-like short messages
- To achieve this, cellphones could automatically form a peer-to-peer network that is independent of any infrastructure

Secure Distributed P2P

- Any authenticated transmission can be intercepted or jammed, but attacks are harder on pseudonymous communication
- I can have as many identities as I like: one for each of my friends, one for a group of friends, and another for my government
- Encrypt everything using public keys
- Exchange pseudonyms and keys personally, when within range, or through friends/acquaintances

Why should I help?

Motivations range from selfish to altruistic:

- more “points” from helping others
- helping my friends communicate
- letting my friends’ friends communicate
- believing in free and unfettered communication
- wanting to help others

Practical examples of Collaboration

- Ham and CB radio networks, especially in emergencies
- TCP congestion control is collaborative
- Cooperatives and Credit Unions
- People who take first aid courses
- Hypothesis: many people are willing to be altruistic if the cost and risk are low, the potential benefit widespread, and there is little or no abuse of the system

Challenges

- How can this work in practice?
  - technology: protocols, addressing, software
  - incentives: game theory, rewards
  - security: encryption, key validation, anonymity
- No central control – abuse prevention must be distributed, similar to wikipedia and P2P nets
- How do I prove that I have been very helpful to others and deserve credit for that?
- How can we revolutionize the world?

Protocol Ideas

- With low bandwidth, intermittent connectivity, do limited broadcast in the ad-hoc network
- Packets/senders that require fewer resources have priority
- If I get a packet for destination D, and I have been in range of D before, I store the packet, and deliver it if I see them again
  - Delay Tolerant Networking, data mule

Addressing

- Deliver to this IP address
- Deliver to geographical area A
- Deliver to my immediate neighborhood
- Deliver to pseudonym X
- Deliver to anyone who can decrypt this
  - or any combination of these

Required Software

- Communication software for a variety of mobile and fixed platforms: Iphone, Android, BB, Windows, Mac, Linux
- user-level software
  - SMS-like service
  - twitter- or chat-like service
  - multimedia supported with low priority

Motivations to Participate

- AllNet is more useful the more people participate
- So how do we get people to use AllNet?
- Basic usefulness:
  - low-rate Internet access as a backup to the usual Internet access
  - walkie-talkie equivalent
  - geographically-limited social network

Motivations to Participate, II

- As long as AllNet is perceived to be socially beneficial, many will be proud to support it
- Game theory: I am more likely to help you if I can be affected by your actions in the future
  - how to leverage this?
  - can we automate keeping track of who helped whom, when and how?
- Increased security, safety

AllNet Security

- Public Key cryptography requires knowing the public key of at least one of the parties
  - certificates are used to provide assurance of ownership of public keys
  - but this fails sometimes (e.g. DigiNotar)
- Identity verification is hard online
  - currently mostly tied to domain names, credit cards, email addresses, passwords
- Interpersonal communication can establish identity and communicate public keys

Pseudonymous Communication

- With a computer to store keys, there is no reason to be limited to a single identity
- One identity can be used for each peer, and one for each group of peers
- The public key identifies the recipient
- If I can decrypt a message, it is for me
- If you don’t know my public key, your message is not for me
- Unless you use my “junk mail” public key

Secure Communication

- With mutually available public keys, all communications can be encrypted and signed
- If the message falls into the wrong hands, it is secure – as long as the pseudonyms are not known, it is hard to even do traffic analysis
- To send me a message, you must authenticate with your public key (or risk going into my spam folder)

Related Work

- AllNet is based on much previous work in:
  - P2P networks
  - Ad-hoc wireless networks
  - Cryptography and security
  - Game theory and human motivation
- “Universal” propsed networks failed due to:
  - limited bandwidth
  - lack of recruitment

can AllNet do better?

Summary

- A network to support free low-bandwidth or short-range communications:
  - text messaging and social networking
  - walkie talkies
  - delay tolerant communications
- Secure
- Ubiquitous as long as others are in range
- Useful whenever the infrastructure fails