HS SEDI
Homeland Security Systems Engineering and Development Institute

Off-Grid Communications with Android

Meshing the Mobile World

November 2012

Homeland Security

About Us

- Homeland Security Systems Engineering and Development Institute (HS SEDI) is a not-for-profit federally funded research and development center (FFRDC) managed by The MITRE Corporation
- SEDI supports the DHS by providing independent expertise in systems engineering and developing proof-of-concept prototypes
- The Smart Phone Ad-Hoc Networking (SPAN) research project is funded by HS SEDI for use in emergency preparedness and response situations
- MITRE: Jeff Robble, Oliver Chong, Sheldon Durrant, Nick Modly
- Accuvant LABS: Josh Thomas

MITRE

ACCUVANT LABS
Security Assessment and Research

Contact Info

- Jeff Robble (stoker)
  - jrobble@mitre.org
  - mistr.stoker@gmail.com
- Josh Thomas (m0nk)
  - jthomas@accuvant.com
  - m0nk.omg.pwnies@gmail.com

MITRE

ACCUVANT LABS
Security Assessment and Research

Open Source

- SPAN is the collaborative effort of private, public, and independent contributors

- Public release under GPLv3
  - GitHub repository: https://github.com/ProjectSPAN
  - Google Group: https://groups.google.com/forum/#!forum/spandev

- Associated and leveraged projects
  - Wireless Tether for Root Users: http://code.google.com/p/android-wifi-tether/
  - Serval: http://www.servalproject.org/
  - Freifunk: http://start.freifunk.net/
  - OpenWRT: https://openwrt.org/
  - Commotion: https://code.commotionwireless.net/projects/commotion
  - tinc: http://www.tinc-vpn.org/

Motivation

Motivation

- Hurricane Katrina, August 2005
  - Over 3,000,000 phone lines went down, 2000 cell towers knocked out
  - Land Mobile Radio (LMR) communications degraded
  - Ham radio operators assisted 911 dispatchers
  - Field reporters exchanged information between victims and authorities
- Haiti earthquake, January 2010
  - Public telephone service and Digicel and Comcel cell networks went down
  - Haitel cell network quickly overloaded, partially by Red Cross volunteers
  - Fiber-optic networks disrupted
- Tohoku earthquake, March 2011
  - Tsunami lead to Fukushima Daiichi Nuclear Power Plant meltdowns
  - Carriers forced to limit mobile phone traffic by 90-95%
- Hurricane Sandy, October 2012

Motivation

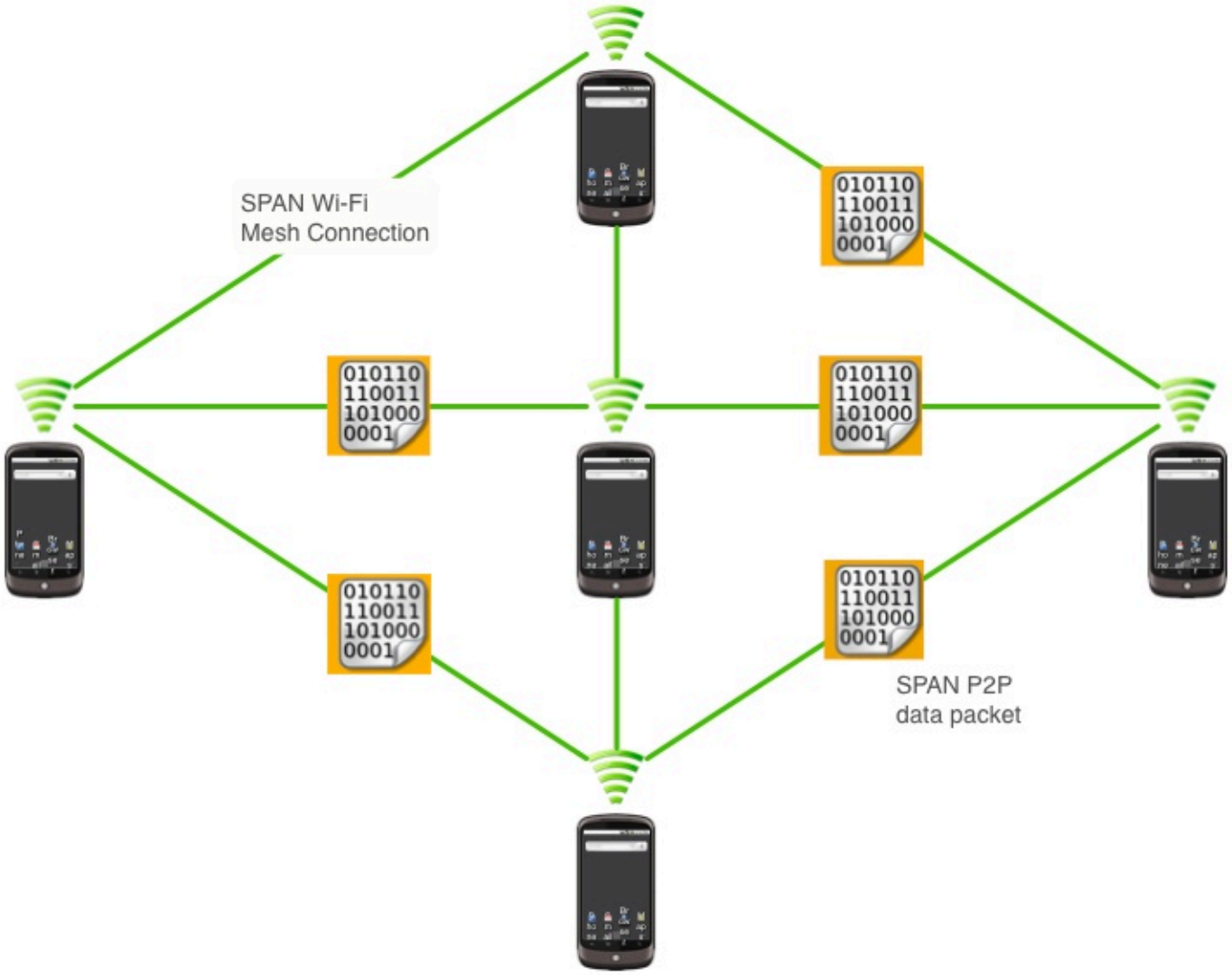
- Cell towers collapse, lose power, or quickly become overloaded
- Landlines become disconnected from PSTN exchange offices
  - Public telephone network and Internet service loss
- Cell towers, PSTN offices, wireless APs, etc. are single points of failure in a centrally managed communications infrastructure
- These single points of failure all provide a convenient mechanism to sniff / filter user traffic and perform MITM attacks
- Egyptian Arab Spring Protests, January 2011
  - Egyptian president Hosni Mubarak suddenly cuts off Internet and cell phone service

Motivation

- Attacks on cellular communication are becoming more common
  - MITM attack launched against 4G and CDMA users at DEFCON 19
  - Commercialization of the IMSI catcher, a device used to spoof a cellular tower and intercept encrypted GSM traffic

- A smart phone without a cell tower or wireless AP is more than a brick!
  - Although service providers might want you to think otherwise

Solution


SPAN Wi-Fi
Mesh Connection
010110
110011
101000
0001
SPAN P2P
data packet

Solution

Solution

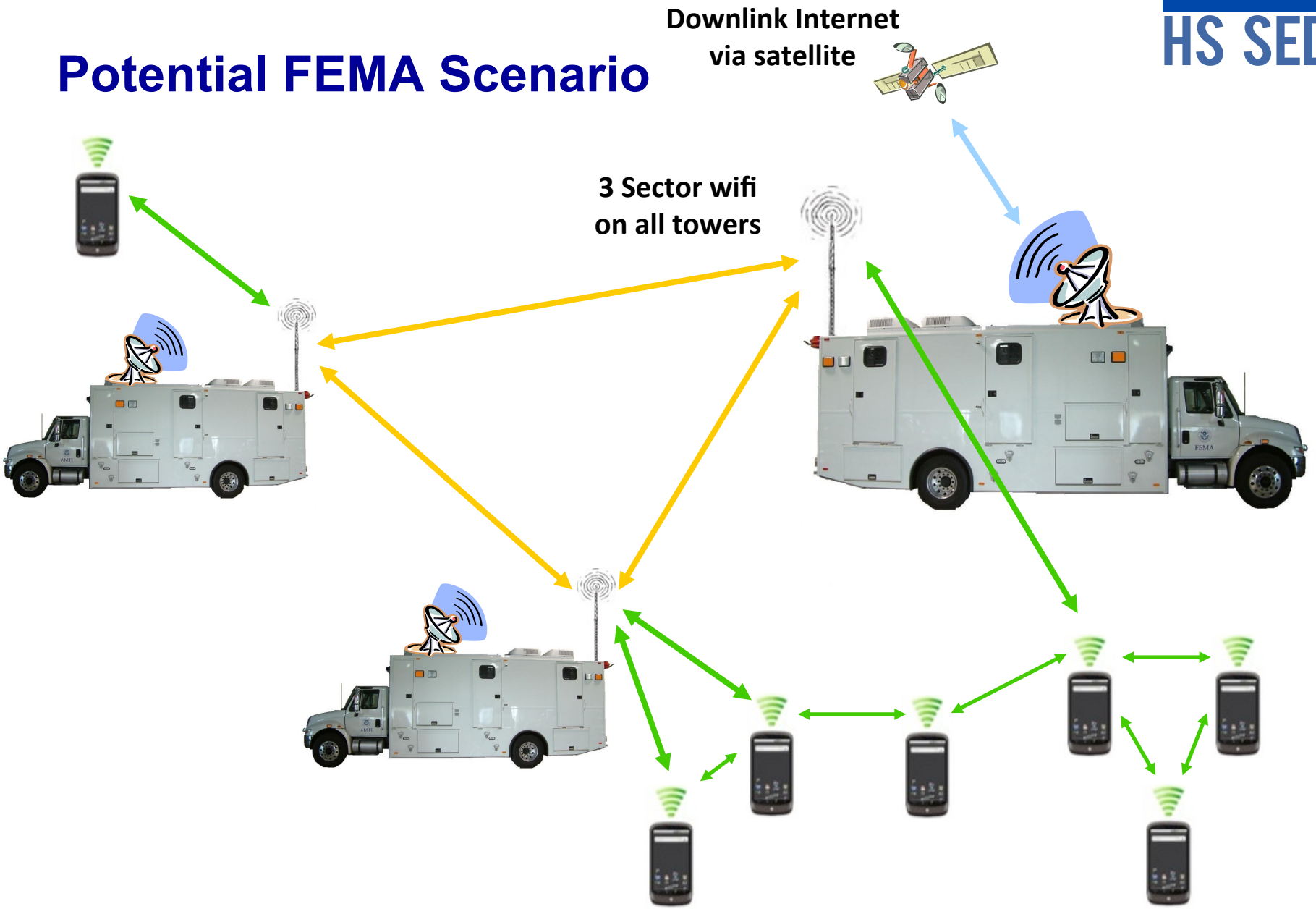
- Leverage the ubiquity of smart phones to create a P2P mesh network
  - 46% of American adults are smart phone users (up 11% from May 2011) [1]
  - Network is headless, does not depend on cell towers or wireless APs
  - Relay messages through peers, forming routing chains
  - Network dynamically expands as more peers join
  - Network is self-healing, peers can leave at any time
- Share information across the Mobile Ad-Hoc Network (MANET) when infrastructure is broken or cannot be trusted
  - Form a P2P VPN over the mesh to secure communications
  - Route data through trusted peer devices
- Nodes can act as gateway devices to connect the mesh to existing infrastructure as it becomes available
  - Share your cell phone service for your specific carrier

[1] http://pewinternet.org/Reports/2012/Smartphone-Update-2012/Findings.aspx

Potential FEMA Scenario

- FEMA deploys Mobile Emergency Response Support (MERS) teams
  - Usually set up within 12 hours near airports
  - Location of MERS communication vehicles broadcast over AM/FM radio
  - Provide free public wifi and an IP voice gateway
- Each MERS vehicle has a tower with 3 sector wifi antennas
  - MERS vehicles form a long-distance wireless mesh network
  - Extend mesh to mobile devices for FEMA, state, local, and public entities
- Individuals set up initial mesh network immediately following or during the emergency situation
  - Broadcast SSID and other information over radio
  - Once MERS mesh network is deployed the range and robustness of the existing mesh is immediately enhanced without reconfiguration
  - Existing mesh users gain access to the Internet, VOIP gateway, information broadcasts, etc.

Potential FEMA Scenario

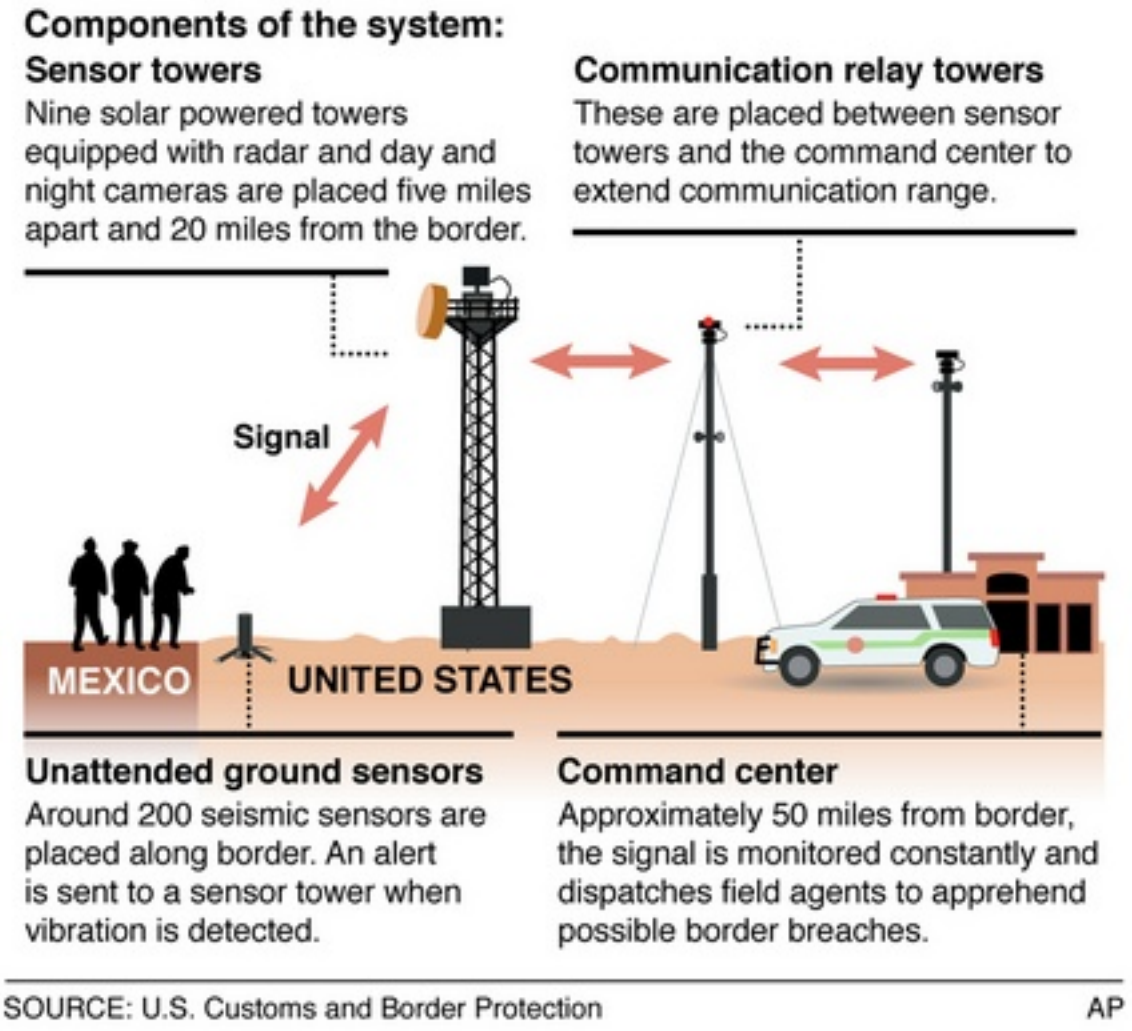


Potential FEMA Scenario

- Load balancing
  - Public use wireless mesh network
  - FEMA, state, and local agencies to use wireless managed network
- Security
  - Obtain keys from trusted Certificate Authority and download to mobile device
  - SPAN app. generates a new key pair, share with others by bumping phones
  - Optionally, only communicate with devices which share symmetric key
- “Citizens as Sensors”
  - Individuals create situational reports using their device’s camera and GPS
  - Information shared across the mesh via an ad-hoc social network app. similar to twitter or tumblr with a map feature
  - Content is tagged with importance/confidence level by creator
  - Content is voted up/down by community and individuals assigned trust levels
  - Content is filtered by trusted FEMA, state, and local authorities

Potential Border Patrol Scenario

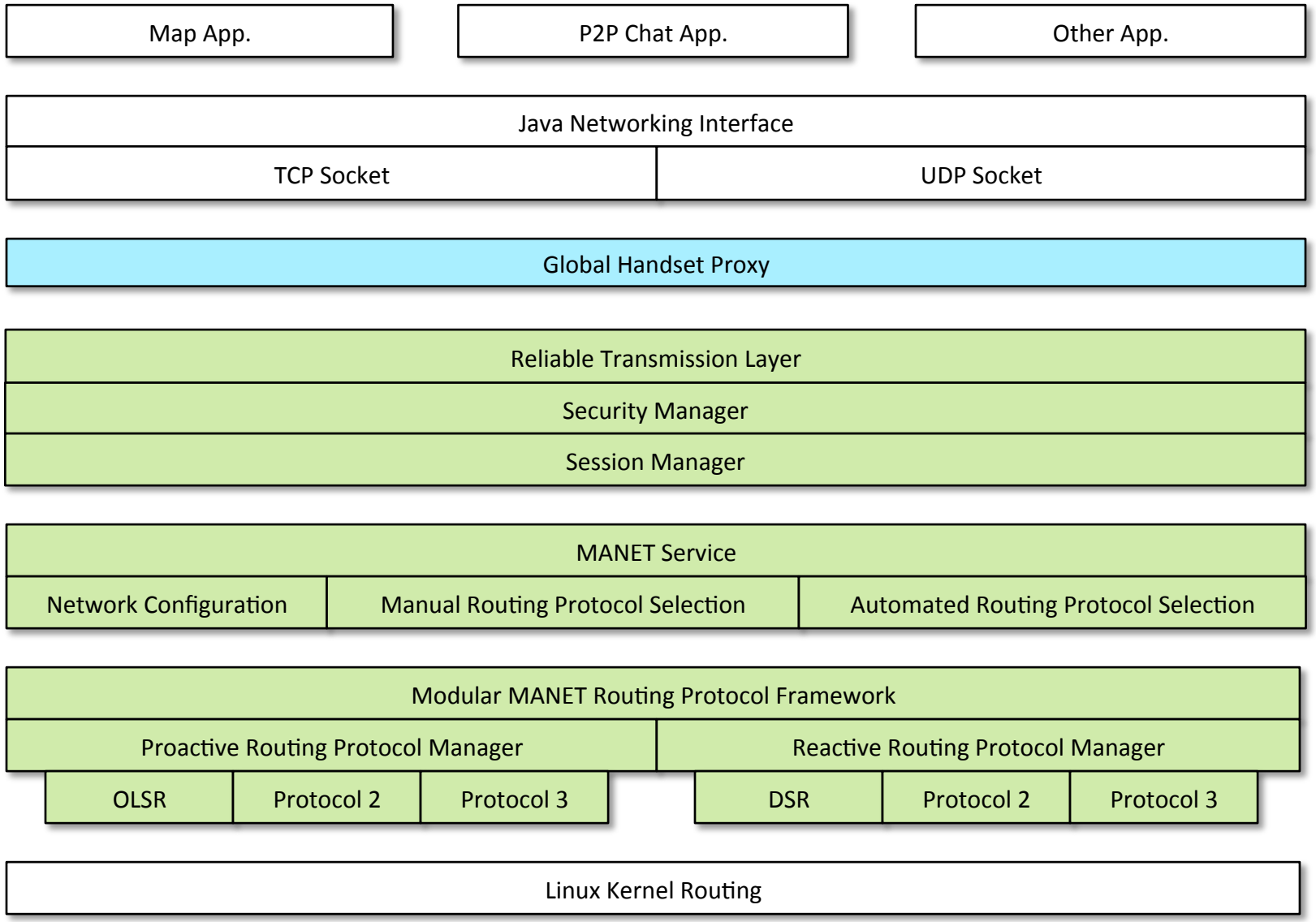
- Cameras on sticks, as well as magnetic, seismic, and acoustic sensors installed along fence line in certain regions
- Boeing Secure Border Initiative network (SBInet) project designed to provide a “virtual fence”
  - Placement of 9 surveillance towers with radar, high-resolution cameras, infrared cameras, wireless networking, etc.
  - Provides a Common Operation Picture (COP)
- Cameras, sensors, towers connected in a mesh?
  - Communication relay towers provide long-distance backbone
  - Extend mesh to mobile devices for agents patrolling the fence line


Components of the system:
Sensor towers
Nine solar powered towers equipped with radar and day and night cameras are placed five miles apart and 20 miles from the border.
Communication relay towers
These are placed between sensor towers and the command center to extend communication range.
Signal
MEXICO
UNITED STATES
Unattended ground sensors
Around 200 seismic sensors are placed along border. An alert is sent to a sensor tower when vibration is detected.
Command center
Approximately 50 miles from border, the signal is monitored constantly and dispatches field agents to apprehend possible border breaches.
SOURCE: U.S. Customs and Border Protection
AP

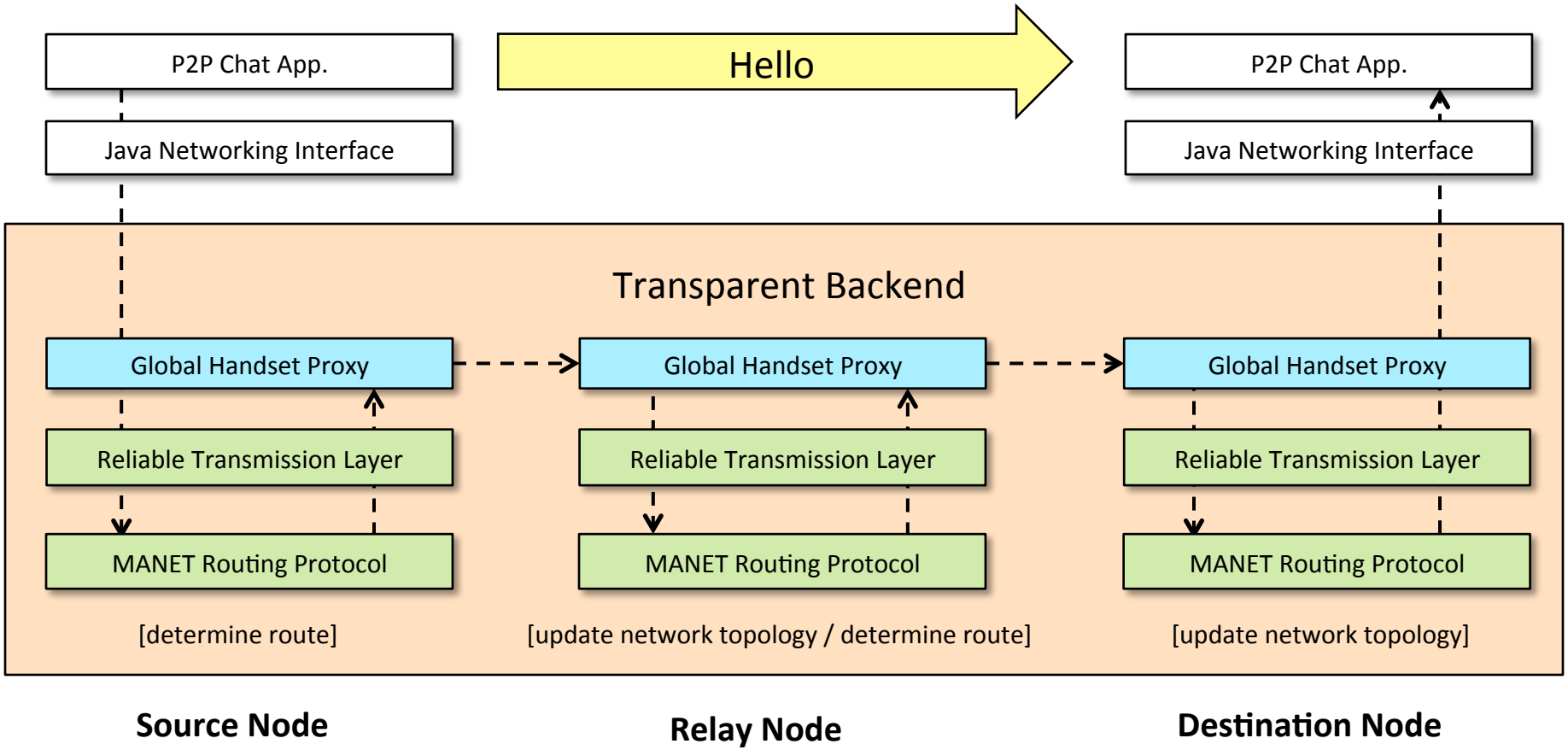
Security Considerations

- Certificate Authority (CA) alternative
  - CA server may not be accessible
  - What if there's no way to get the root certificate to validate signatures?
  - What if root certificate jeopardized?
  - Peers bump phones on the fly to establish a web of trust
- Route data through trusted peers
  - Each peer signs data as it works its was through the mesh
  - Receiver validates each signature
- Split-packet routing
  - Split each packet into two and send them over non-overlapping routes
  - Receiver reconstructs original packet, each half is useless without the other
- Don't request or push an unsigned public key over the air in plain text
  - Can MITM Diffie-Hellmen key exchange without proper authentication

Architecture



Data Flow


P2P Chat App.
Hello
P2P Chat App.
Java Networking Interface
Java Networking Interface
Transparent Backend
Global Handset Proxy
Global Handset Proxy
Global Handset Proxy
Reliable Transmission Layer
Reliable Transmission Layer
Reliable Transmission Layer
MANET Routing Protocol
MANET Routing Protocol
MANET Routing Protocol
[determine route]
[update network topology / determine route]
[update network topology]
Source Node
Relay Node
Destination Node

Ad-Hoc Mode on Android Hardware

- Leveraged Wi-Fi Tether for Root Users app.
  - Edify script for setting up ad-hoc mode using cross-compiled iwconfig
- Some phone wifi drivers don't support ad-hoc mode
  - Wi-Fi Tether app. switched to using softAP
  - softAP: software enabled portable wireless access point
- Needed to compile Wireless Extensions support into kernel
  - Compiled vendor open source software
  - Dumped zImage and drivers to AnyKernel tree
  - Flashed using ClockworkMod Recovery

Ad-Hoc Mode on Android Hardware

- Easy to flip Broadcom chips into ad-hoc mode

Device	Wireless Chip
Samsung Nexus S 4G	Broadcom BCM4329
Samsung Galaxy Tab 10.1	Broadcom BCM4330
Samsung Galaxy S II Epic Touch 4G	Broadcom BCM4330
Samsung Galaxy Nexus	Broadcom BCM4329
ASUS Eee Pad Transformer Prime	AzureWave AW-NH615 (rebranded Broadcom BCM4329)
Motorola Razr Maxx	Texas Instruments WL1285C
iPhone 4S	Broadcom BCM4330
Nokia Lumia 900	Broadcom BCM4329

Ad-Hoc Mode on Android Hardware

- Currently require Wireless Extensions support
- Ad-hoc mode support disabled in some kernels
  - Add NL80211_IFTYPE_ADHOC back into supported interface modes list

Wireless Extensions Support	**No Wireless Extensions Support**
Samsung Nexus S 4G	Samsung Galaxy Nexus
Samsung Galaxy Tab 10.1	ASUS Eee Pad Transformer Prime
Samsung Galaxy S II Epic Touch 4G	Motorola Razr Maxx

Ad-Hoc Mode Support	**No Ad-Hoc Mode Support**
Samsung Nexus S 4G	Samsung Galaxy Nexus
Samsung Galaxy Tab 10.1	ASUS Eee Pad Transformer Prime
Samsung Galaxy S II Epic Touch 4G	Motorola Razr Maxx

Implementation Details

- Android apps and services (Java language)
  - MANET Manager, MANET Service, MANET Logger, MANET Visualizer
- Native code (C language)
  - OLSR daemon, P2P VOIP daemon, netfilter hook, Linux utilities
- Unique IP address assignment without DHCP
  - IPv6 link-local addressing based on network adapter MAC address
- Connect to existing infrastructure
  - Gateway device masquerades connection for devices within mesh
  - Devices within mesh are NATed behind gateway on a subnet
  - VPN through gateway using PPTP

Root vs. Non-Root

- Root required
  - Need root to modify iptables / routing tables
  - Need root to configure wireless driver and put phone in ad-hoc mode
  - Potential security risk for non-technical users
- Root benefits
  - Transparent proxy handles all outgoing / incoming data
  - Existing apps work over mesh without modification
  - Easier to flip in and out of ad-hoc mode without affecting running apps
  - Potentially automate network scanning (cell, wireless AP, ad-hoc)
- Non-root alternative
  - P2P connection over Bluetooth, Wi-Fi redirect, or client and softAP setup
  - Apps send data to mesh daemon running on device via SPAN API
- SPAN API provides access to peer list, routes, keys, etc.

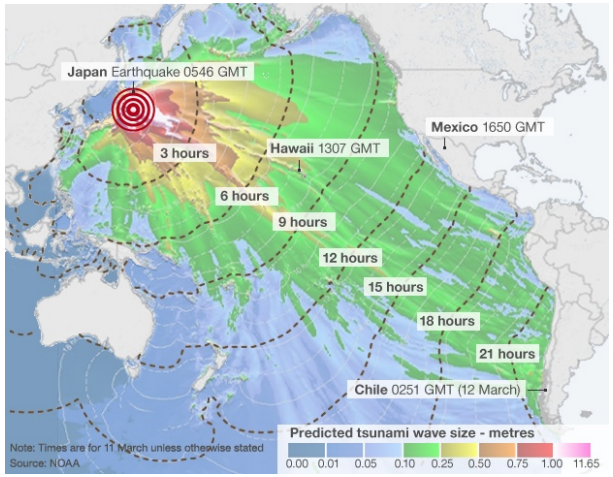
Range Considerations

- Range tests
  - Frequency: 2.412 GHz
  - Transmission power: 32 dBm
- Galaxy S II Epic Touch 4G and Galaxy Nexus
  - Approx. 100-170 ft. range down long narrow indoor hallway
  - Approx. 100-150 ft. line of sight range outdoors in wide open area
- Qualcomm's LTE Direct (previously FlashLinq) part of LTE Release 12
  - Becoming standardized by the 3GPP standards body
  - Release 12 should be approved by 2015
  - OLSR P2P routing protocol
  - Line of sight connections up to 500m (1640 ft.)

Delay-Tolerant Networking

- If intended recipient of an urgent message is not currently reachable, broadcast message to all peers
  - Peers hang onto message and serendipitously pass it on to new peers
  - Eventually the message will reach the intended recipient
  - Peers transparently become couriers of data
  - Leverage highly mobile nature of ad-hoc networks

- Quickly spread word disasters starting from the epicenter and propagate outward
  - “Right-time” information
  - Notification messages can be limited to a georadius or destined for a geolocation



Proactive vs. Reactive Protocols

- Proactive protocols
  - Daemons run autonomously in user space
  - Periodically broadcast “hello” and plan new routes
  - Routes available when you need them
  - OLSR, BATMAN, etc.

- Reactive protocols
  - Lazily plan routes as needed
  - Initial communication between peers takes longer
  - Less processing and CPU usage
  - Less network congestion
  - Dynamic Source Routing (DSR), Ad-hoc On-Demand Distance Vector (AODV) routing, etc.

Sensory Intelligence

- Battery
  - Don’t send packets to devices going dead
  - Send more packets to devices plugged in
- GPS
  - Form routes to devices closer to you
  - Form routes to devices that don’t move often
- Accelerometer
  - Don’t send packets to devices in motion
  - Predict device movement, direct packets to devices along movement vectors
- Develop intelligent routing protocols
  - Consider sensor data, mesh stability and history, node density, etc.
  - Use AI to fine-tune mesh over time, develop hybrid protocols

Strategic Fallback Security Model

- Strategy 1: Use X.509 certs assigned by CA
  - Individual's public key, private key, and cert get loaded on their device
  - Each device loaded with the CA root key for X.509 cert signature validation
  - Peers exchange signed X.509 certs via bump or over the air
  - Peers use asymmetric encryption over a P2P VPN
- Strategy 2: Use self-generated public / private keys
  - Key pair is generated for each device as part of the SPAN first run process
  - Peers exchange public keys by physically bumping phones
  - Peers use asymmetric encryption over a P2P VPN
- Strategy 3: Use common symmetric key
  - One symmetric shared by all users of the mesh as part of the configuration file loaded into SPAN
  - All routing protocol communications encrypted using symmetric key
  - Peers use symmetric encryption, other peers can decrypt

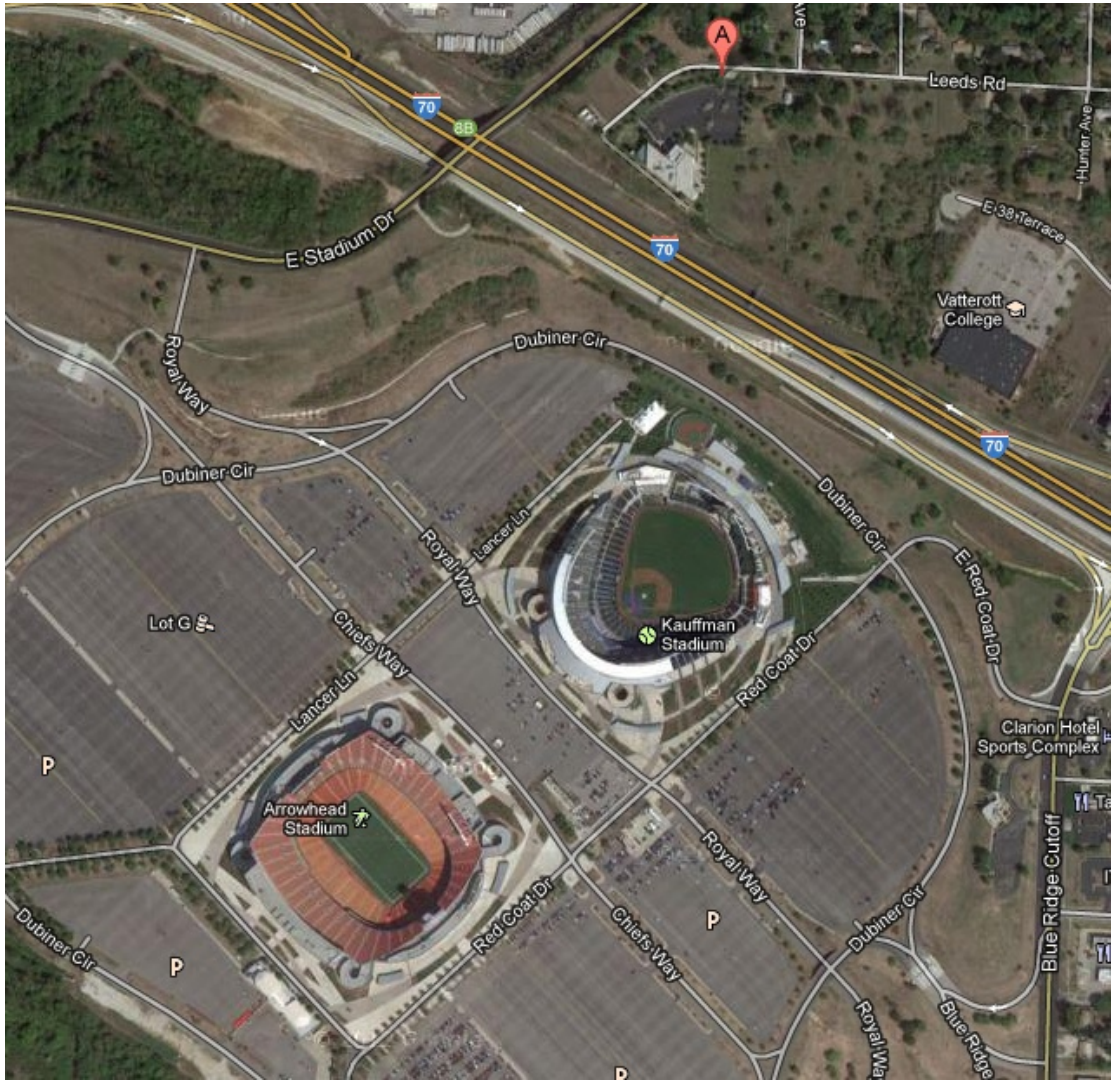
Strategic Fallback Security Model

- Users aware of strategy employed when communicating with peers
- Strategy 1 and Strategy 2 classified as “high” or “true” security
- Strategy 3 classified as “low” or “default” security and
  - Should not be used for sharing confidential information
- Option to limit P2P communications to “high” security (“Trusted Mode”)
- If the symmetric key is compromised
  - User-initiated broadcast propagated out over the network
  - Upon reception, user is notified and the device automatically reverts to “Trusted Mode”
  - User can change mode if desired

Operational Support

- Major League Baseball All Star Game, July 10 2012
  - Provided operational support to the Kansas City Police Dept.
  - Worked with Kansas City Terrorism Early Warning Group
- Officers patrolled parking lots around Royals Kaufman Stadium in Gators
  - Provided with Galaxy Nexus phones running SPAN and Beacon IC.NET app. for reporting GPS position and creating situational reports
  - ASUS Transformer Prime gateway connected mesh to Persistent Systems Wave Relay equipment long-distance radio equipment
  - Data piped from mesh to command center server across the road
  - Provided COP to authorities
- Phone density …

Operational Support



Operational Support

Future Work

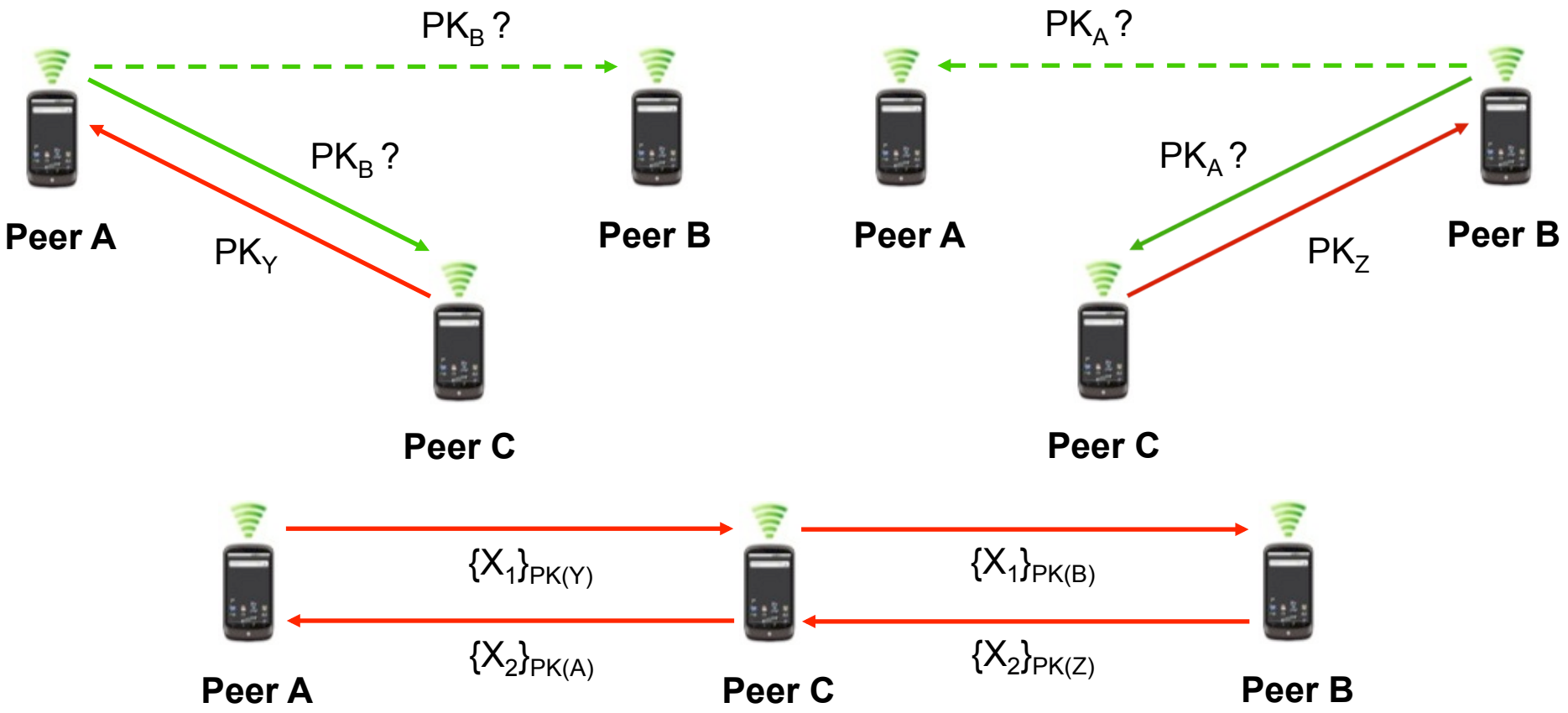
- Applications
  - VOIP connection to Asterisk server
  - Torrent protocol to RAID data across devices
  - Distribute threads and tasks across cloud of unused processors
- Delay-tolerant networking
- Platform support
  - iOS, Windows 8
- Leverage LTE Direct
- Consider integrating with CyanogenMod custom Android ROM
- Sponsor outreach

Questions?

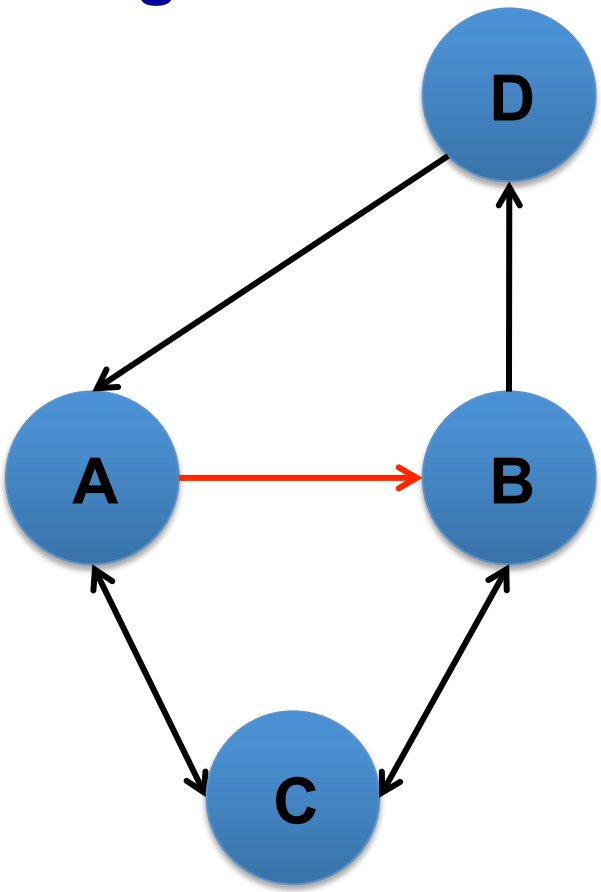
Backup

Security Considerations

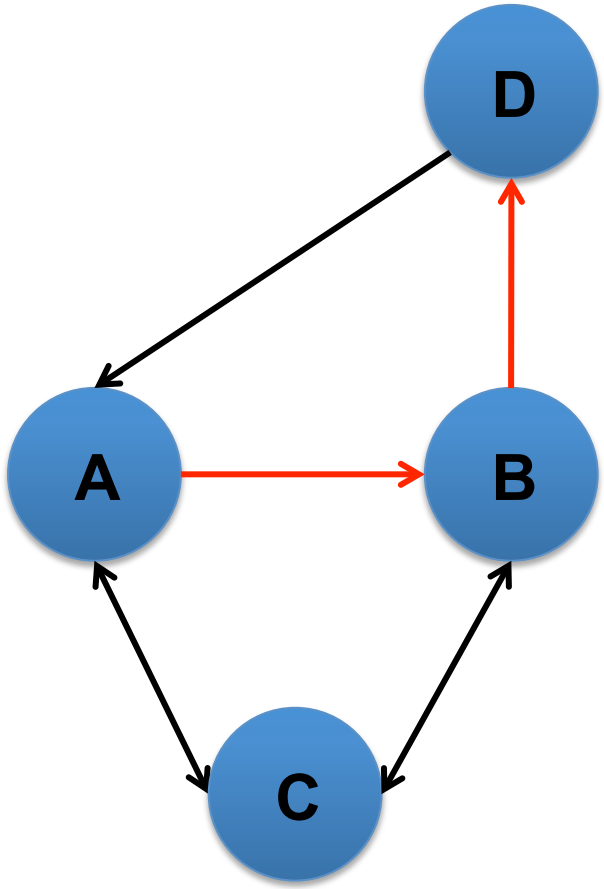
- Don't request or push an unsigned public key over the air in plain text
- Can MITM Diffie-Hellmen key exchange without proper authentication
  - Should be performed over private channel



Routing



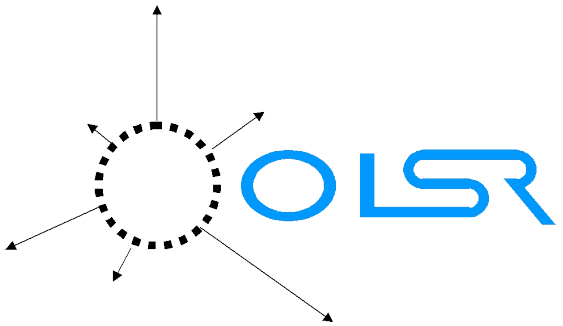
Route to
1-hop neighbor



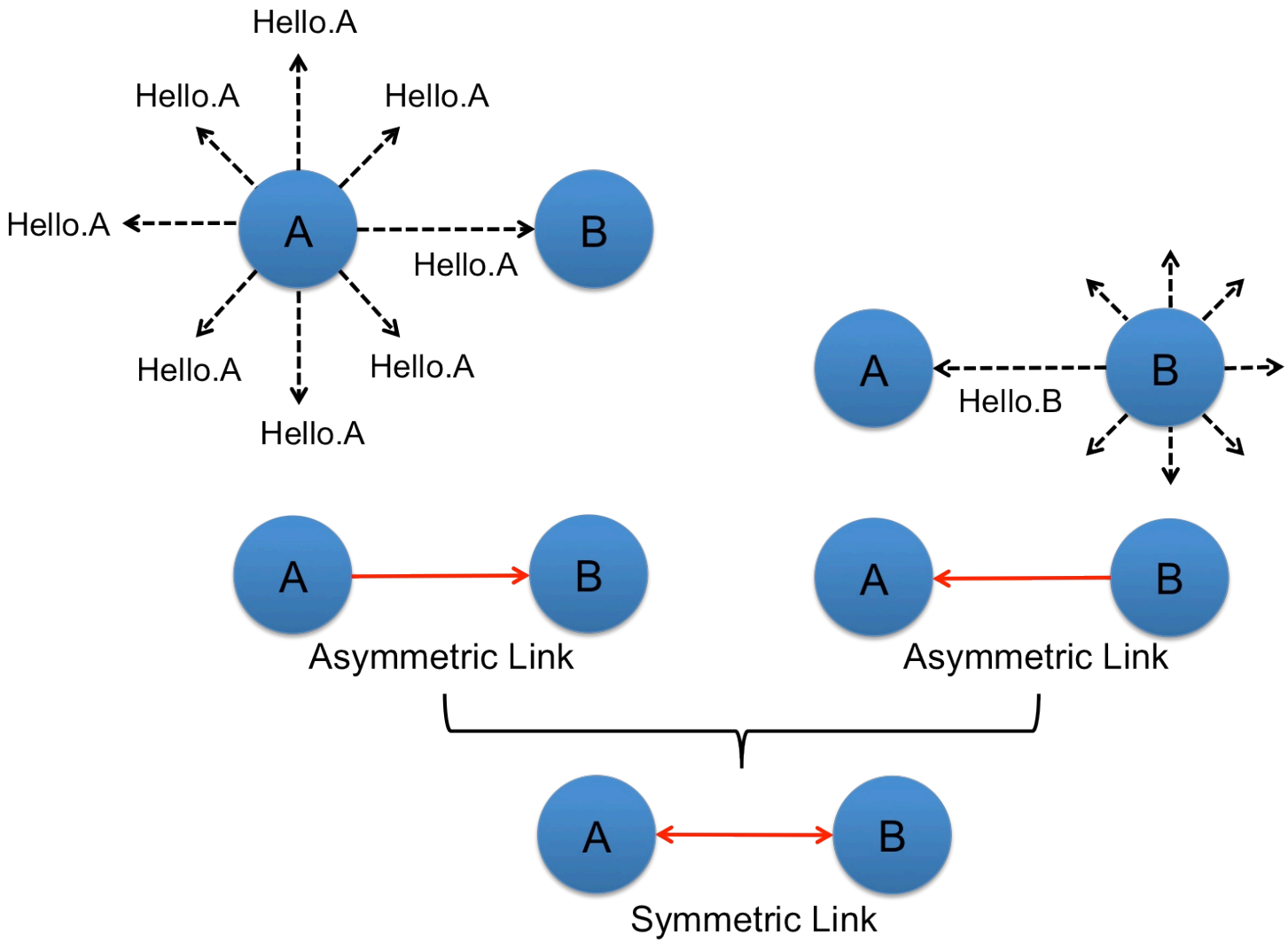
Route to
2-hop neighbor

OLSR

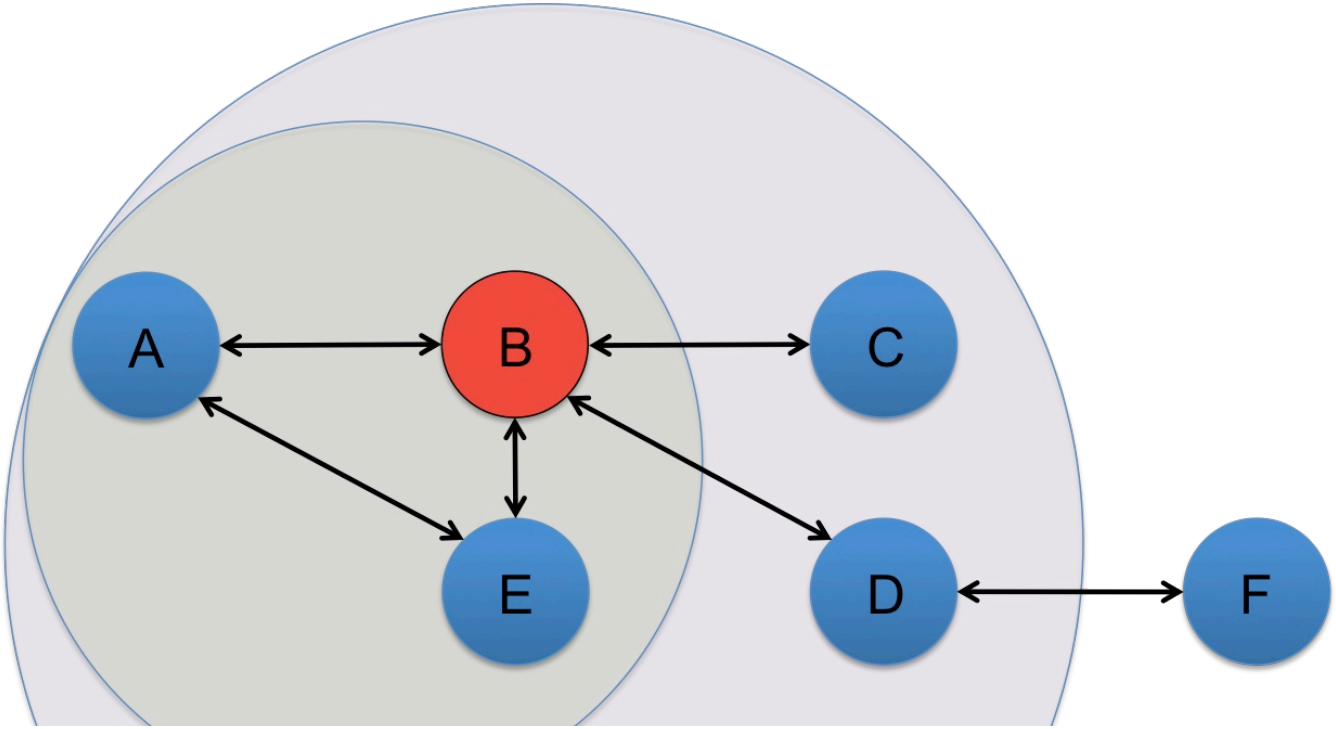
- Optimized Link State Routing Protocol (2003)
- Link-state protocol
  - Nodes know who they can talk to
  - Each node determines entire route to every other node
- Proactive
  - Routes periodically planned in advance
  - Kernel-level routing table modified on-the-fly
- Dijkstra Open Shortest Path First algorithm
- Layer 3 in OSI stack



OLSR: Find 1-hop Neighbors



OLSR: Multi-Point Relay



- A selects B as Multi-Point Relay (MPR)
  - All 2-hop nodes reachable through B
- All > 1-hop routes from A will go through B

OLSR

- Pros
  - Better than everyone sharing everything
  - Topology info dumps only between MPRs
  - Incremental improvements
- Cons
  - MPRs are throughput choke points
  - Entire routes planned in advance, but next hop uses its own route
- Main developers behind OLSR came up with BATMAN
  - Address circular routing, network congestion, and performance issues
- OLSR-NG (Next Generation) fixed fisheye feature (~2008)
  - Performs much better than before with less network congestion
  - Precise view of close neighborhood, approximate view of farther nodes

BATMAN

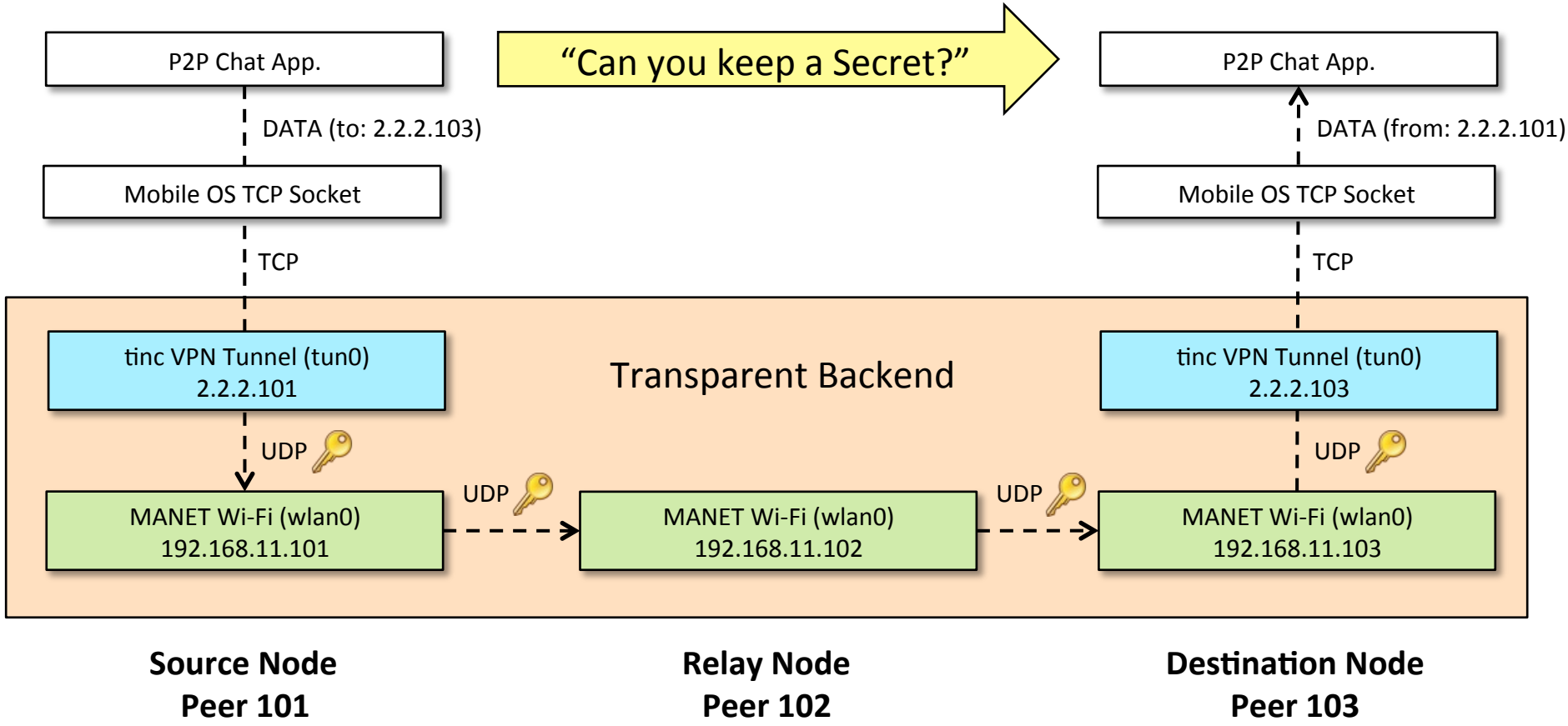
- Better Approach to Mobile Ad-hoc Networking (2006)
- Decentralize: No single point has all the data
  - No MPRs
  - Each node sends out originator messages: “I exist”
  - Every other node keeps track of number of hops an originator message takes to reach them
- Simplify: Only plan first step in route
  - Direct packets along route with lowest originator message hop count
- OLSR still the most popular
- BATMAN gaining traction

Security Considerations

- Serval Mesh Data Protocol (MDP)
  - Each device assigned random IPv4 address
  - Each device generates 256-bit ECC key pairs
  - All outgoing messages are broadcast and contain multiple payloads
  - Payloads may be destined for different peers
  - Each payload contains sender, destination, and next hop public key
  - Public key used to filter and route data between Serval daemons
  - Essentially a custom network stack

- There Is No Cabal (tinc)
  - ”tinc is a self-routing, mesh networking protocol, used for compressed, encrypted, virtual private networks”
  - P2P VPN routing daemon using X.509 certificates
  - Android port

P2P VPN Data Flow



Ad-Hoc Mode on iOS Hardware

- iOS Devices have a history of using Broadcom chips similar to those already supported by SPAN Android devices

iOS Device	Wireless Chip
iPhone 3GS	Broadcom 4325
iPhone 4	Broadcom 4329
iPhone 4S	Broadcom 4330
iPhone 5	Broadcom 4334
iPad	Broadcom 4329
iPad 2	Broadcom 4329
iPad 3	Broadcom 4330
iPad 4	Broadcom 4334
iPad Mini	Broadcom 4334

Ad-Hoc Mode on iOS Hardware

- Apple doesn't expose a public framework method of placing an iOS wireless device in to ad-hoc mode
  - Indicates that jailbreaking (root) is likely necessary
  - IPConfiguration.bundle private framework potentially exposes configuring the device mode
- Cydia Store
  - Provides the capability to distribute applications outside of the Apple App Store to jailbroken devices
  - Could be leveraged to distribute SPAN
  - Apps on Cydia that are configuring the Wireless Device beyond the public framework capabilities
  - MyWi and WiFiFoFum access capabilities beyond the public framework
- Modify firmware to enable ad-hoc mode?

Freifunk

- German for "Free radio”
- Non-commercial open grassroots initiative to support free open radio networks in Germany
- Offers specialized OpenWrt firmware
- Routing based on OLSR or BATMAN
- Freifunk Berlin has 500+ nodes
- http://berlin.freifunk.net/
- http://wiki.freifunk.net/

Serval

- Also known as batphone
- Android ad-hoc network framework

- Implemented features
  - P2P VOIP calls over mesh
  - MeshMS, free mesh-based SMS

- Features under development
  - Serval Rhizome, distributed mesh-based data distribution platform
  - Serval Maps, mesh-based mapping application
  - Serval Morse, distributed micro-blogging service

- Custom Mesh Data Protocol (MDP)

- http://www.servalproject.org/