

Mobility and Address Freedom in AllNet

Edoardo Biagioni

University of Hawai'i at Mānoa

esb@hawaii.edu

<http://www.alnt.org>

ICUFN 2017

Mobility is a headache

- Mobile providers must keep a Home Location Register to record a device's location
 - often also keep a Visitor Location Register
- the problem: addresses (and phone numbers) no longer correspond to the point-of-attachment
- a layer of indirection is always required

Addresses are (almost) obsolete

- unless your computer happens to be permanently connected to a wire
- Challenge: addresses are what makes routing manageable
 - how can we manage routing without point-of-attachment addresses?

Non-point-of-attachment addresses

- Indirection is needed to support mobility
- So an address is really an identifier
 - it identifies the device, not the location
- The location is obtained by doing a lookup in a global, usually distributed database
- <https://xkcd.com/1129/>



So the question really is

- How do we build this global, distributed database?
 - without any central points of failure
- The answer is different for:
 - the Internet (hint: use a Distributed Hash Table)
 - ad-hoc networks (hint: broadcast)
- if possible, combine the two!

The rest of this talk

- the AllNet protocol
 - for communication among humans
 - whenever possible! e.g. Internet, Ad-hoc
- self-selected identifiers
 - what about duplicates?
- leveraging encryption

But first: isn't broadcast evil?

- Yes and No
- ARP uses broadcasts on local networks, and is not evil as long as the network is small
- most ad-hoc networks are small
 - as they grow, likely someone is on the Internet
- BitCoin and BitMessage broadcast
 - but require proof-of-work to avoid DoS

AllNet overview

- started with the question:
why can't my phone talk to your phone?
- and the answer: they should!

- with mobile devices, it is easy to exchange keys
 - authentication and encryption become easy

AllNet applications

- xchat: everyday chat over AllNet
 - had security before WhatsApp!
 - useful in emergencies and offline (hiking)
- exchange pictures directly, without relying on the cellphone service
- cellphone walkie-talkie
- unfortunately, not all of this is implemented yet

AllNet networking

- send to every network you are connected to
- send to (and participate in) Distributed Hash Table/DHT when on the internet
 - (DHTs map bitstrings to content)
- data messages carry a messageID
 - message ack hashes to the messageID, and is sent encrypted as part of the message
 - so ack can only be issued by final receiver

Yes, but what about addressing?

- AllNet addresses are self-selected bitstrings
 - length of bitstring is also selectable (≤ 64 bits)
- addresses are used to decide what messages to try to verify and decrypt
- duplicate addresses are OK!
 - just mean I will verify a few more packets
 - and signature verification is quick

Summary

- AllNet addresses are used:
 - to decide which signed packets to verify
 - to decide where in the DHT to save and retrieve packets
- neither of these requires unique addresses

Locating an address in AllNet

- AllNet doesn't actually locate addresses
 - only forwards packets
- send to the DHT node corresponding to the address
- broadcast on attached local area networks
- broadcast within ad-hoc networks

a related topic: AllNet

Human-Readable Addresses

- Suppose I do want a unique address, similar to an email or a web address
 - [edo@something](#) (*edo* is Personal Name/PN)
- generate lots of keys, encrypt *edo* with each
 - the last 16/32/48/64 bits of the cyphertext must be found in the hash of the PN (that's why lots of keys)
 - these bits map to *something*, represented as word pairs: [daily_time@go_car.for_computer.do_future](#)

Human Readable Addresses

- it is relatively easy to generate AHRAs
 - though many keys must be generated for each
- and select one that is memorable
- it is much harder to generate a key to match an existing AHRA
- e.g. with 3 word pairs, attackers must generate 68,719,476,736 more keys than the owner

AHRA summary

- for now, AHRAs are used only to decide which broadcast packets to display
- e.g. to get a daily time message, subscribe to daily_time@go_car.for_computer.do_future
- or just remember daily_time@go_car
 - shorter is easier to remember, but easier to spoof

AllNet status

- Ad-Hoc communications and Voice-over-AllNet (VOA) available for Linux only
 - ad-hoc in android only available on rooted devices
 - but anyway, android is not yet available (10/2017?)
- iOS is available! allnet-xchat
- no picture exchange yet, and can still be slow
- AHRAs work for broadcasts

Summary:

Mobility and Address Freedom

- Pick your own address!!
- mobility requires a global database anyway
- you might as well choose your own address
 - and keep it forever
 - or discard it after 10 minutes
 - <https://10minutemail.com>
- for both AllNet addresses and AHRAs

Why read the paper? (contributions)

- self-selected addresses are useful
 - can choose your own
 - less need for central authority
 - sometimes, unique addresses are not required
- user choice of the lifetime of the address
 - stability vs. anonymity
- AllNet Human Readable Addresses

A more formal summary

- Current addresses require uniqueness and hierarchical topology
 - and have poor support for mobility
- Mobility requires a global mapping of addresses to locations, for any kind of address
 - so, hierarchical topology is not as useful
- Signed packets: uniqueness not required

AllNet Trace

- AllNet Trace helps us see who else is on the network

```
0.002253s rtt, 0 d3.8f/16
0.159654s rtt, 1 00.00/16
0.215810s rtt, 1 dd.99/16
0.337738s rtt, 1 80.00/16
0.489997s rtt, 1 c0.00/16
```

```
$ bin/trace -i
1:      0.000723s timestamp,    0.002281s rtt,  0 d3.8f/16
1:      0.133257s timestamp,    0.164316s rtt,  1 00.00/16
1:      0.164257s timestamp,    0.214654s rtt,  1 dd.99/16
1:      0.352748s rtt,          1 c0.00/16
1:      0.353152s rtt,          1 80.00/16
sent 1 packet, received 5, rtt min/mean/max is 0.002281/0.217430/0.353152s
```