INTRODUCTION

Locha Mesh: A Decentralized Mesh Network powered by RIOT

$ whoami

- I Am: Jean Pierre Dudey
- Do work as: Embedded Software Developer

$ whois locha.io

Domain: LOCHA.IO
Registrant Organization: Bitcoin Venezuela Non-Profit Organization

@Locha_io @jeandudey
WHY LOCHA MESH

- A network that could be used at any time, without depending on central infrastructure
- A fallback network in case someone presses a big red button and the Internet shuts down

Psst: Did you now the "Locha" name comes from an old coin in Venezuela that had little value?
NATIONAL BLACKOUT

2019, MARCH 7 - 2019, MARCH 8

Credits to: NASA EOSDIS Worldview

https://go.nasa.gov/3maG1Nf
THE SOLUTION

- Small hand held device
- Battery powered
- Efficient
- Easily replicated using spare parts (DIY)
SO... HOW RIOT HELPS?

- Powerful network stack!
- Supports a wide range of MCUs
- Easily extendable
- Of course, a great community
HOW DOES IT WORK?
THE STACK

On the CC1312

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AODVv2</td>
<td>Routing Algorithm</td>
</tr>
<tr>
<td>UDP</td>
<td>Transport</td>
</tr>
<tr>
<td>6LoWPAN - IPv6</td>
<td>Network</td>
</tr>
<tr>
<td>ICMPv6</td>
<td>PHY</td>
</tr>
<tr>
<td>IEEE 802.15.4g</td>
<td></td>
</tr>
</tbody>
</table>
WHAT'S UP WITH A MANET?

- Stands for Mobile Ad Hoc Network
- Been in research for a loooong time
- As the name says, allows mobile communications
- Generally do not require Internet to work
  (and by design is hard to provide Internet on a MANET)
AND WHAT ABOUT AODVV2?

- Not the same as the original AODV (it's IPv4 only)
- Finds routes by flooding "Route Requests"
- Once a route is found a "Route Response" is sent to the node that asked about the route
- We ask for a route only when we need it
- When multiple "Route Response" arrive, we select the one with the less hops to the destination
- Built on top of RFC 5444
TAKING A LOOK AT THE ROUTING
JOHN WANTS TO SEND A MESSAGE TO JANE
JOHN PROCEEDS TO FLOOD ROUTE REQUESTS

All nodes participate by re-sending the request, and verifying whether it isn't a duplicate request.
JANE ONCE FINDING THIS REQUEST, GIVES A RESPONSE TO JOHN
OKAY... BUT HOW DOES THIS WORK WITH RIOT?

- Each network interface (gnrc_netif_t) on RIOT provides a callback for providing routing information: `gnrc_netif_t::route_info_cb`
- It informs us when the GNRC IPv6 stack doesn't have a valid route to a destination.
- Along with informing the need of a route, also provides the packet that is going to be sent for us to "buffer" it and send it later when the route is found.
HOW IPV6 ADDRESSES ARE USED?

- Each node generates a random unique address, saved for later usage.
- All addresses use a fc00::/16 prefix or in other words an Unique Local Address.
- Unique Local Address aren't routable on the public Internet.
- These addresses however can be routed on a private network.
- In general terms it's sort of (with exceptions) equivalent to the IPv4 private address range (192.168.0.0/16).
SECURITY CHALLENGES FOR THE FUTURE

- Security on a public network is somewhat difficult
- Jamming is an issue on the radiospace, even interference could be problematic
- Impersonation attacks are possible, although can be solved using cryptography (e.g.: generating an address out of an ECC public key, and incorporate validation on the routing protocol)
- Validation of AODVv2 messages
AND MAYBE A WORKING PROTOTYPE?

Yes! Still being worked and details being polished :-)
FINALLY

Thanks for hearing me, and very much thanks to all of the RIOT Summit 2020 organizers.

Project main repository can be found at:

https://github.com/btcven/locha

Made with love using Reveal.js and Inkscape

100% Open Source

#LaLuchaPorLaLochaLibre