ID/Locator split for IoT-A
FIA 2012

P. Giacomini

May 7, 2012
IoT-A?

- IoT-A is not a middleware
- IoT-A promotes an IoT reference architecture
- IoT-A aims to enable IoT vertical solutions - not reinvent the wheel!
Currently IP addresses act as:

- Endpoint Identifiers (EIDs)
- Routing Locators (RLOCs)

IP addresses were/are used for access control:

- 1985ish: rsh, rcp, rexec;
- 1990-200x: tcpwrapper
- 200x: HTTP proxys;
- July 4th 2011: host based ACL: 294000 results on google

Issues - Check Informational RFC4984 (Scalability of DFZ Routing Information Base, etc...): non-efficient routing (endpoint constraints), bloating ”core” routers (DFZ RIB), multihoming, un-trustable identification

IPs are not IDs: mobility (by design), conflicts (by accident), spoofing (by will)

the fix: ID/locator split (map-encap, HIP)
The good:
- Encryption has low power consumption compared to Radio Activity
- ECC effective with "small" keys
- Few primitives required (on chip?)
- 6lowpan interaction?
- no big infrastructure impact

The bad:
- Memory constraints (implementation challenges and key size)
- Packet size (key size)
- Bandwidth overhead?
- Security Association setup overhead
- Infrastructure interaction?

The ugly: what about RFID technology? HIP support for RFIDs
draft-irtf-hiprg-rfid-05 (limitations?)
mobility?

multihoming?

opportunistic connection?

ID, host == application?

growing number of connected objects, deployment, and so on?

deployment models

communication unification? (bridging non-IP networks)

relationship with application layer IDs? (ONS/EPCglobal, uID, etc...)

Identity Management is orthogonal to application design