draft-struik-6tisch-security-architecture-elements-01

Subir Das,

Yoshihiro Ohba,

René Struik

Status

- Status:
  - Second version published on October 27, 2014
- Intent:
  - Work-in-progress document capturing security architectural design considerations, including the join process; fit with 802.15.4e/TSCH specification; gap analysis; identification of outstanding issues that need to be addressed; contributions towards addressing these.
  - Current version: concepts only, no specifications (yet)
- Security not yet part of current 6TiSCH charter

Device Roles

Node. May move in and out of networks (that may be alien to it), with little network management functionality on board.

Router. May be more tied into a relatively stable infrastructure, with more support for network management functionality or reliable access hereto (e.g., via a back-end system).

Server. Provides stable infrastructure and network management support, either intra-domain or inter domain (thereby, offering homogeneous or even heterogeneous functionality).

CA. Vouches for trust credentials, usually in offline way.

Protocols involving a third party assume these communications to take place via the access point (which is tied into infrastructure).

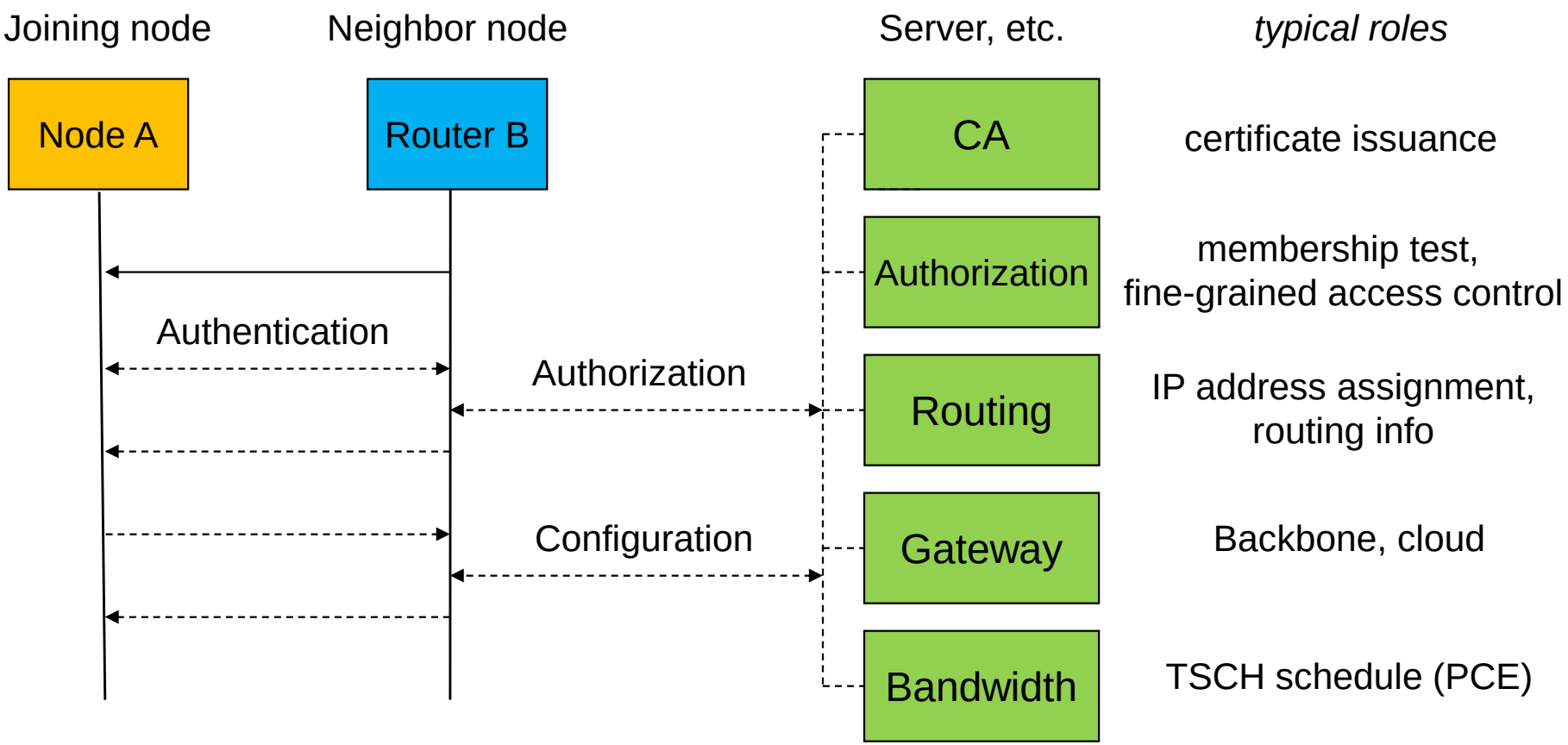
Device Enrolment Steps

Device authentication. Node A and Router B authenticate each other and establish a shared key (so as to ensure on-going authenticated communications). *This may involve server KDC as third party.*

Authorization. Router B decides on whether/how to authorize device A (if denied, this may result in loss of bandwidth). *Authorization decision may be delegated to server KDC or other 3rd-party device.*

Configuration/Parameterization. Router B distributes configuration information to Node A, such as ♦ IP address assignment info; ♦ Bandwidth/usage constraints; ♦ Scheduling info (including on re-authentication policy details). *This may originate from other network devices, for which it acts as proxy.*

Networking Joining (1)



NOTE: in some existing applications, Router B acts as relay only and third-party provides both authentication and authorization.

Desired Properties

Security:

- Authenticated key agreement (incl. PFS)
- Mitigation DoS attacks (both re computation, communication)
- End-to-end security (joining node vs. server (PCE, JCE, etc.))

Privacy:

- Hiding of device identity joining node

Communication:

- Minimization of non-local flows*

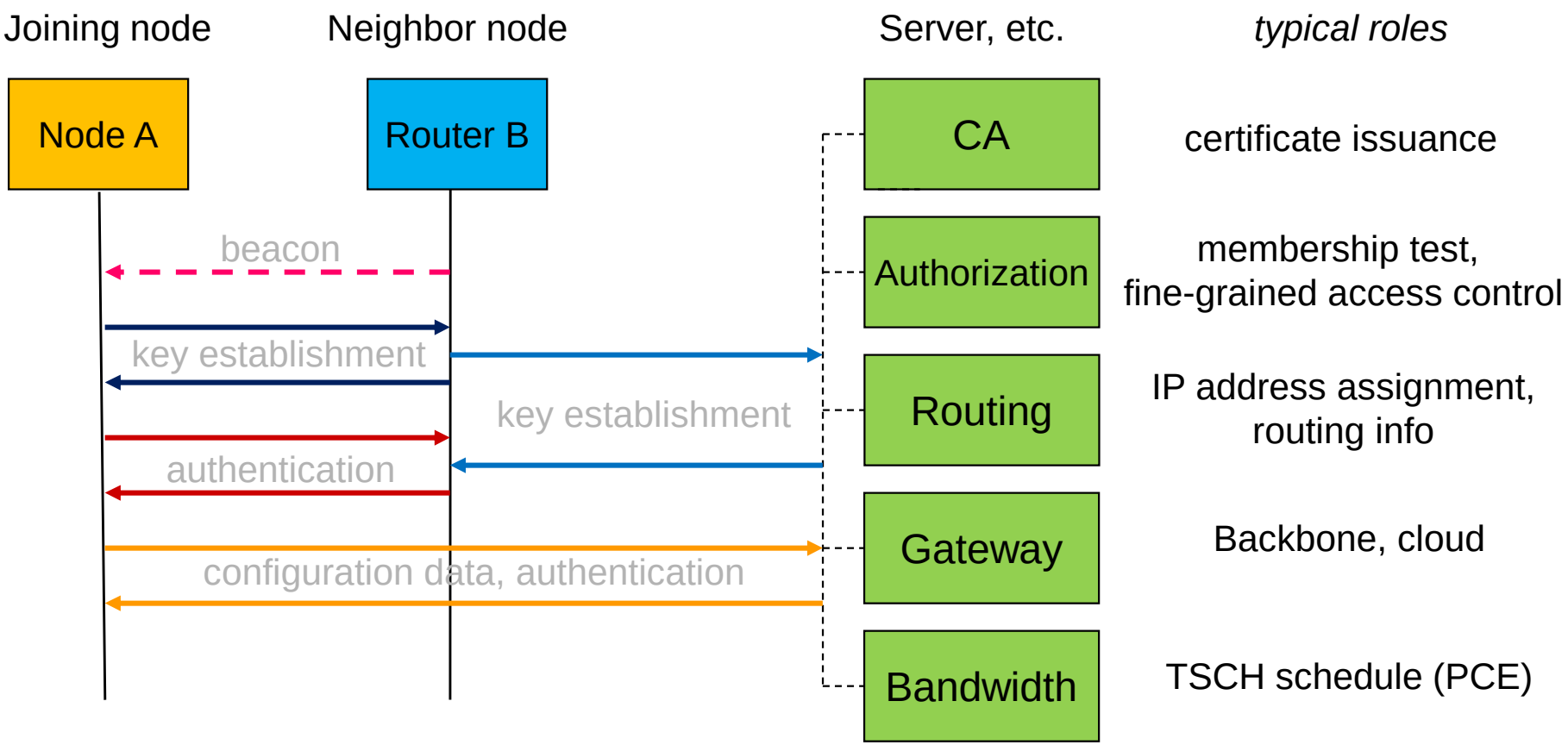
Computation:

- Shift from constrained node to less constrained node

General:

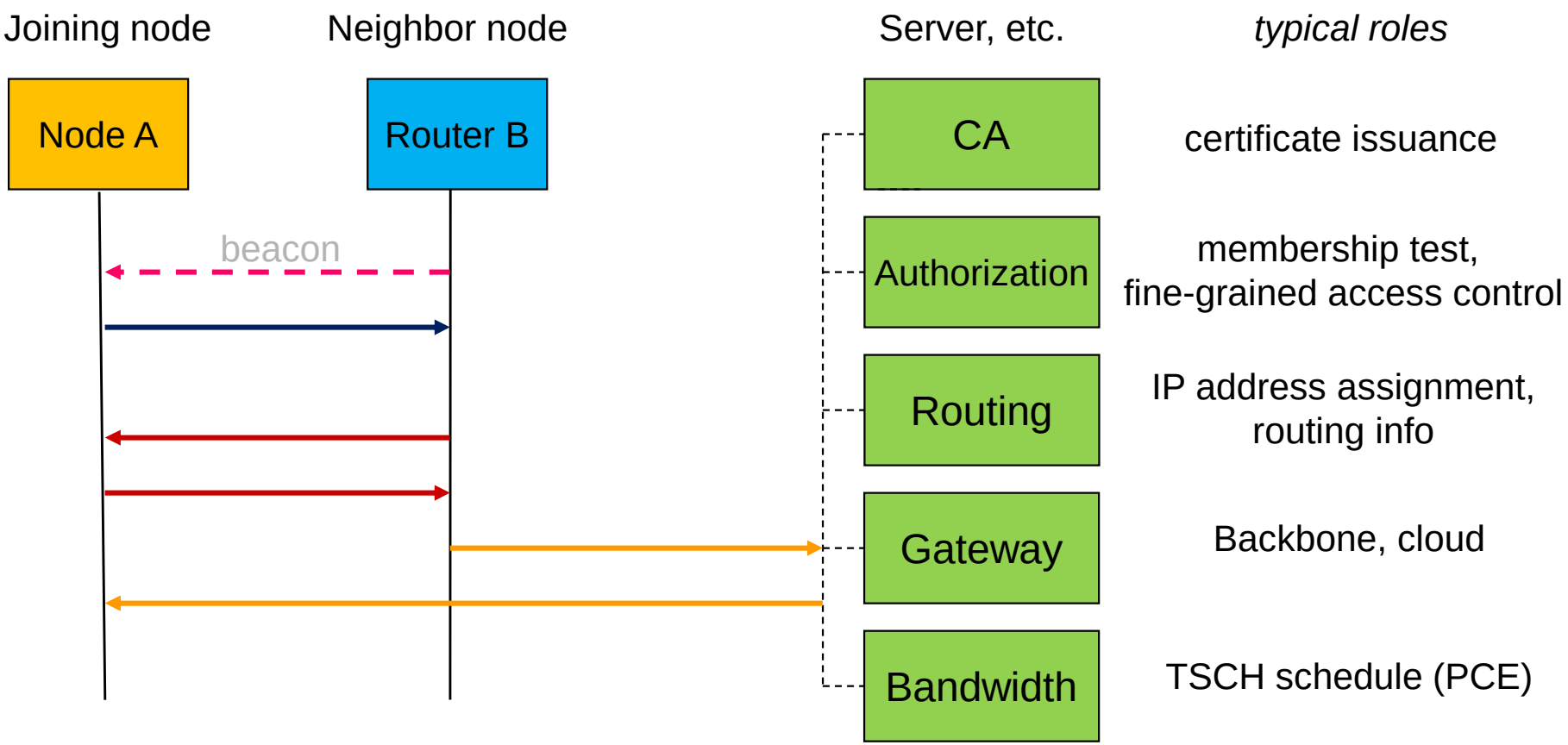
- “Separation of concerns”
- Minimization of dependencies

Networking Joining (2)



NOTE: Router B may transfer configuration data to Node A as part of its authentication to Node A.

Networking Joining (3)



NOTE: Optimized flows, based on caching of server-side information on Router B (this would benefit from secure multicast…)

Realized Properties

Security:

- Authenticated key agreement (incl. PFS)
- Mitigation DoS attacks (both re computation, communication)
- End-to-end security (joining node vs. server (PCE, JCE, etc.))

Privacy:

- Hiding of device identity joining node

Communication:

- Minimization of non-local flows*

Computation:

- Shift from constrained node to less constrained node

General:

- "Separation of concerns"
- Minimization of dependencies

Security and 802.15.4e aspects:

- No "default" keys (or other fake keys)
- No need to trust ASN in beacon for security

Security vs. status information:

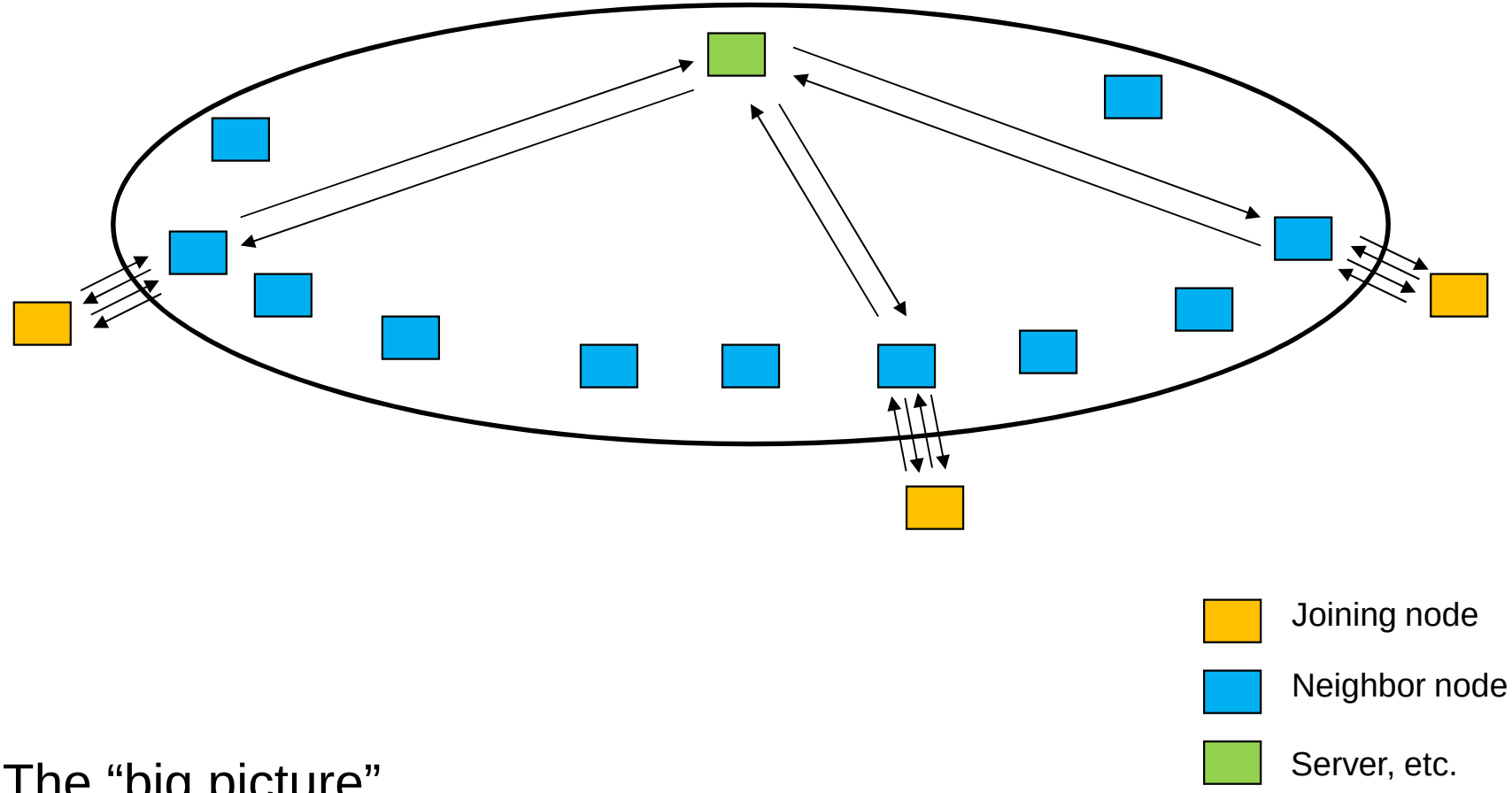
- Prioritization of DoS attack prevention

Separation of concerns:

- 802.15.4e: no need for other beacon
- Routing: no need for "tweaks" (e.g., joining node can use link local address)
- Extensibility: fits with semi-automatic network management concepts and provisioning/configuration concepts

Protocol easy to analyze by security and crypto community (no short cuts)

Networking Joining (4)



The “big picture”...

Outstanding Issues (1)

- Packet sizes:
  - TODO: get more insight on packet sizes configuration parameters (e.g., as w/HART does).
- Device Ids:

  With industrial control, network manager looks up “tag name” device in pre-configured database.
  - TODO: details on tag name syntax, how assigned, and how bound to, e.g., EUI-64.

Outstanding Issues (2)

- Join process impact on network:
  - Status: Minimize non-local communication flows between joining node and network manager to
    - Pass join information from joining node to network manager and back
    - Pass configuration parameters from network manager to joining node (keys, links, frame links) and neighbor report from joining node to network manager.
  - Status: analysis impact Router B as relay, e.g., in terms of time latency, overheads, and DoS attacks.
  - TODO: negotiation of local schedule with neighbor node for execution of join protocol.
  - TODO: more analysis on time latencies due to TSCH

Outstanding Issues (3)

- Crypto protocol details:
  - Status: Crypto properties well-understood
  - Status: mitigation DoS attacks, reducing overheads
- Authorization/trust management:
  - TODO: further discussion lifecycle aspects, certificate issuance (ACE could play role here)

Outstanding Issues (4)

- Fit with 802.15.4e/TSCH:
  - TODO: first join message cannot use ASN from Enhanced Beacon, since not trusted (and may differ from ASN of network manager). More analysis needed. {Analysis completed}
  - TODO: current 802.15.4e does not allow mixing of unsecured and secured traffic.

Next Steps:

- Confirm desired properties
- Work out full details in small “tiger team”