



Generic node identifiers for ID/locator separated network architecture

Ved Kafle, Kiyohide Nakauchi, Masugi Inoue

Network Architecture Group
New Generation Network Research Center
National Institute of Information and Communications Technology
(NiCT)
Tokyo, Japan

Nov 19, 2007

Contents

- Introduction
- Node identifying architecture
- Architectural components
- Name configuration
- Locator assignment
- Communication initialization
- Summary and further work

Introduction

■ AKARI Project

- NICT initiated new generation network research project (started in April 2006)
- Clean-slate design
- Aims to implement a new network by 2015
- <http://akari-project.nict.go.jp>
- Includes research on **node identifying and locating architectures**

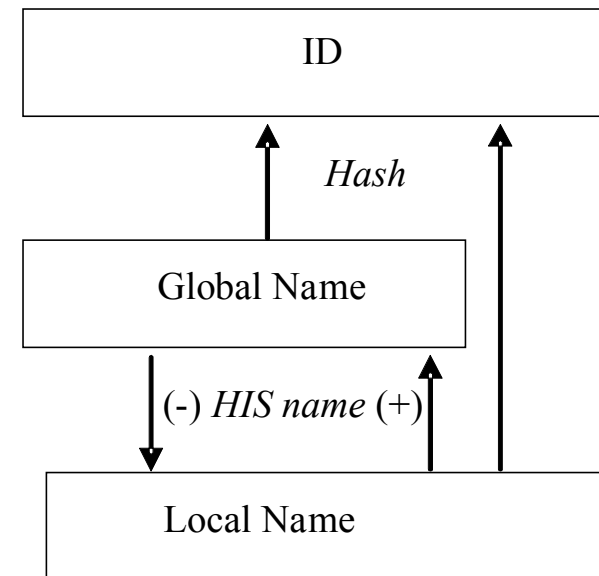
Motivation

- In the current Internet, IP addresses act as both node identifiers and locators
 - Problematic in terms of
 - Mobility management
 - Multihoming and network renumbering
 - Security and privacy
 - Scalable routing
 - Traffic engineering
 - QoS assured end-to-end connectivity
- To overcome these problems, separate node identifiers from its locators

Node identifying architecture (1/3)

A node identifier collectively represents the node name and its ID

- **Node Name:** local or global
 - **Local name**
 - Unique in the local network
 - Generated using feature words
 - Character string format
 - e.g., my.pc, home-phone, tempsensor, etc.
 - **Global name**
 - Local name + home identity server name
 - HIS name is globally unique, may be in domain name format
 - e.g., my.pc#mynetwork.com, tempsensor#hisname.net, etc.
 - (we do not use @ sign in a node name, as it's for a user name)
 - Human readable and rememberable



Node identifier structure

Node identifying architecture (2/3)

■ Node ID

- Bit stream derived from a name using a hash function
- Name to ID has an 1-to-N relation, i.e., one name may correspond to many IDs
- IDs are derived from names, the reverse is not possible
- It is possible to verify whether an ID belongs to a name only by knowing the name-to-ID deriving functions/relations
- Unique in a name/ID/LOC mapping scope

Node identifying architecture (3/3)

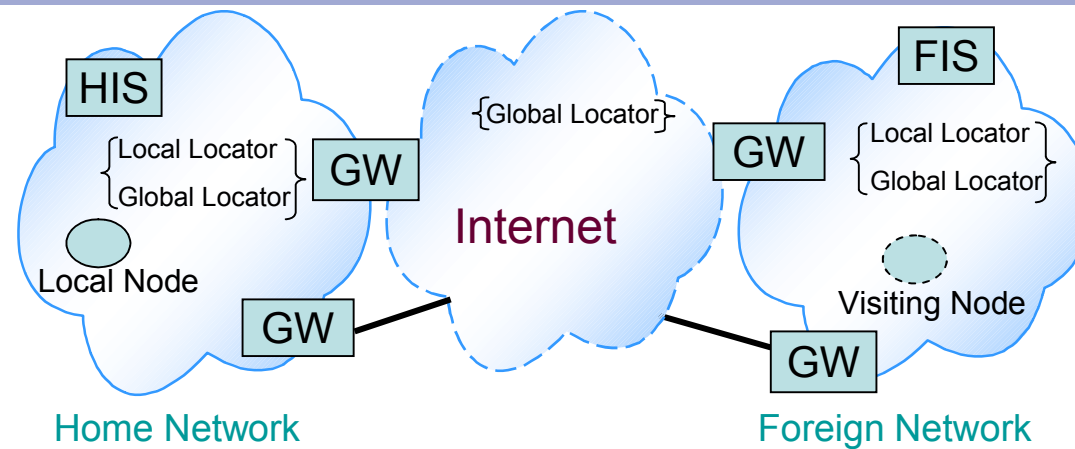
■ Use of name

- Identify nodes for communication initialization
- Network management

■ Use of ID

- In packet headers to identify end nodes
- For ID-to-LOC mapping at indirection points

Architectural components (1/2)



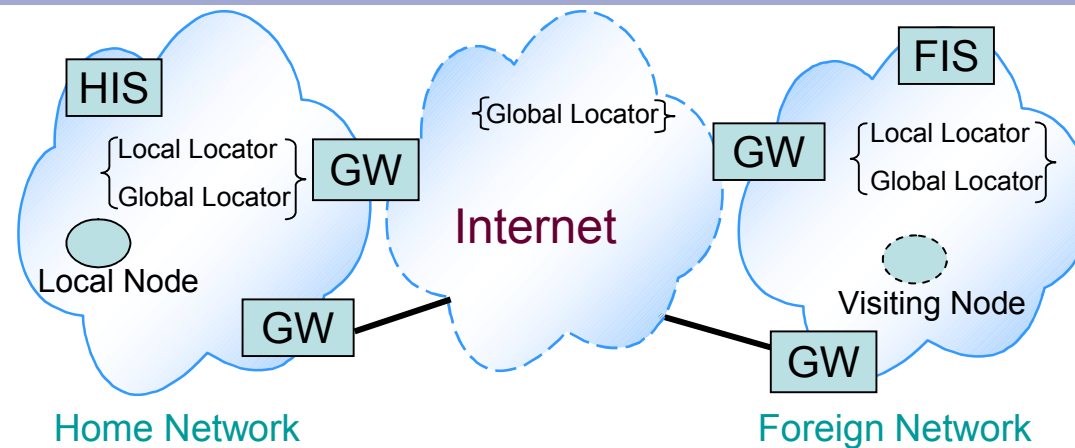
■ Gateway (GW)

- A router located at the border
- Interact with HIS to verify node identity (identifier, authentication info)
- Implement two types of locators: local locators and global locators
- Assign locators/provide info to allow nodes to configure locators
- Unique local locators; unique or shared global locators

■ Home Identify Server (HIS)

- Store node identity and locators
- Verify node identity when requested by GWs
- Assist in ID/LOC mapping retrieval
- Interact with FIS

Architectural components (2/2)

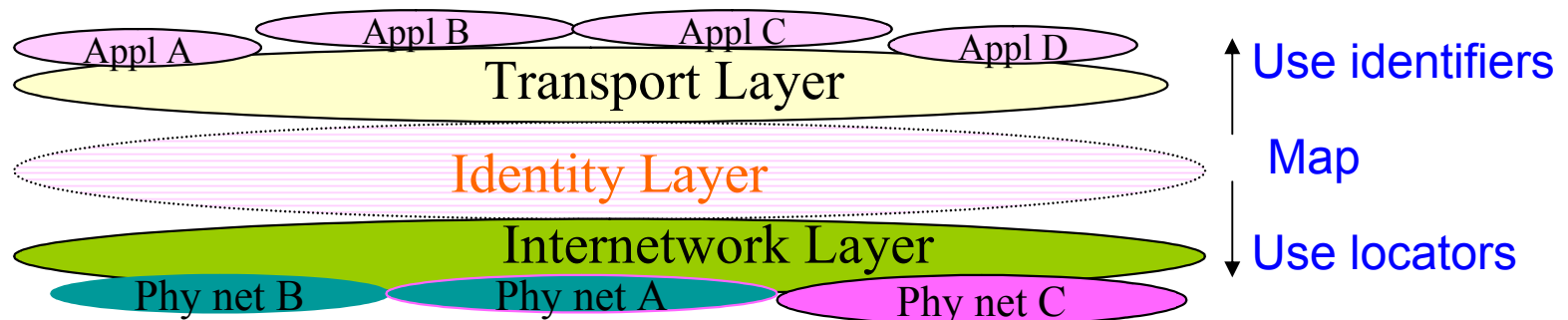


- **Foreign Identity Server (FIS)**
 - Like HIS, but in a foreign network
 - Verify visiting nodes' identity, store identifier/locator mapping
- **Node**
 - Local node: located in its home network
 - Visiting node: located in a foreign network

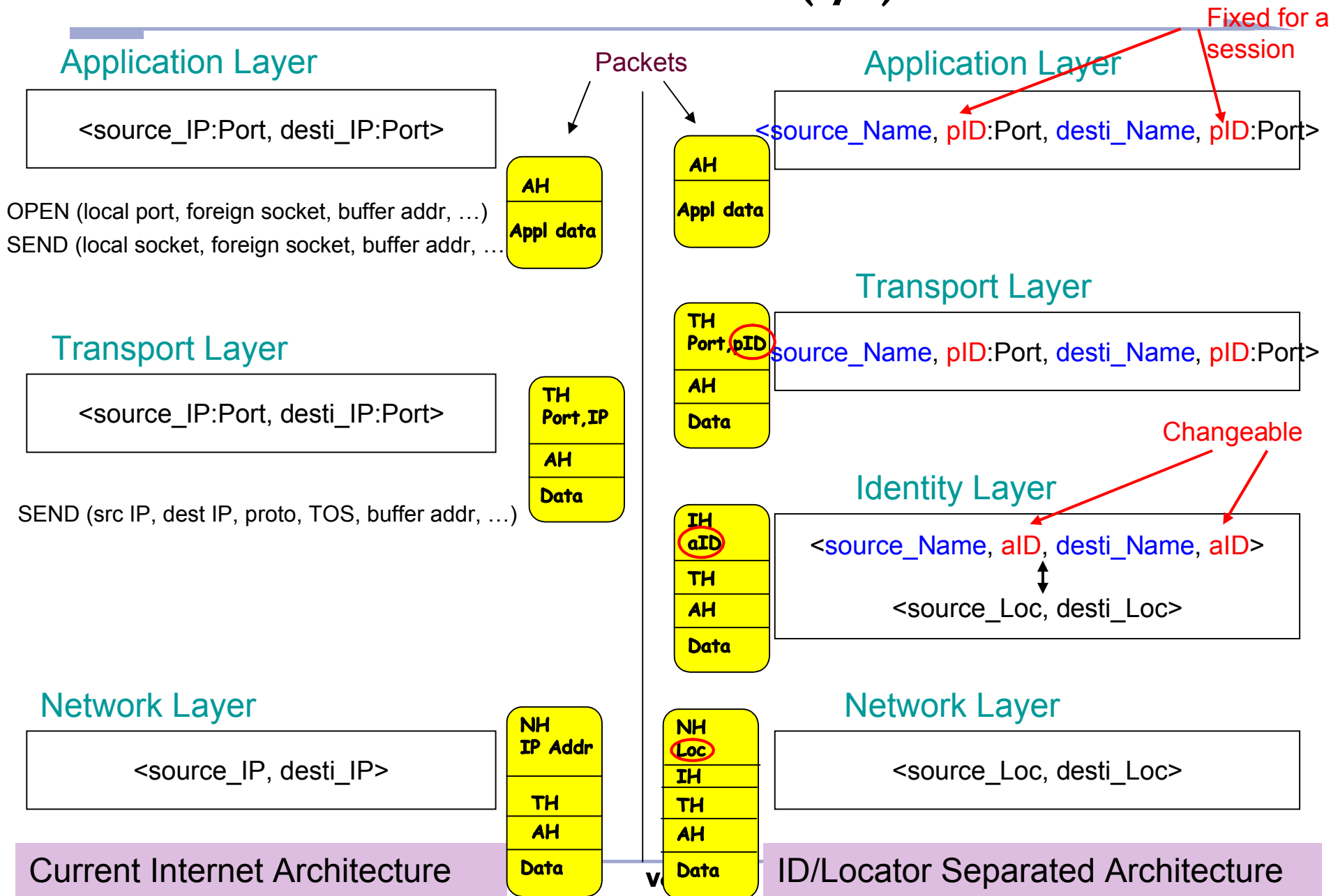
Protocol stack (1/4)

■ Identity layer –

- is inserted below transport and above internetwork layer
- handles both identifiers and locators; maps identifiers to locators
- hides visibility of identifiers and locators from lower and upper layers, respectively



Protocol stack (2/4)



Protocol stack (3/4)

- aID update method
 - Settle during communication initialization

- Two possible methods:
 - Regular
 - e.g., after every n packet exchange
 - On demand
 - (a) inform the other node before updating aID, update on getting acknowledgement
 - (b) inform the other node along with updated aID

Protocol stack (4/4)

Idea: use different **node identifiers** at **protocol stacks** and in **packet headers**, but derive the latter from the former

■ Pros:

- Node identifiers hidden from outsiders in packet headers
 - Better privacy and security
- End-to-end semantic preserved thru IDs

■ Cons:

- Additional commutation overhead at Identity layer
 - Due to tag generation and comparison
- Tag update overhead

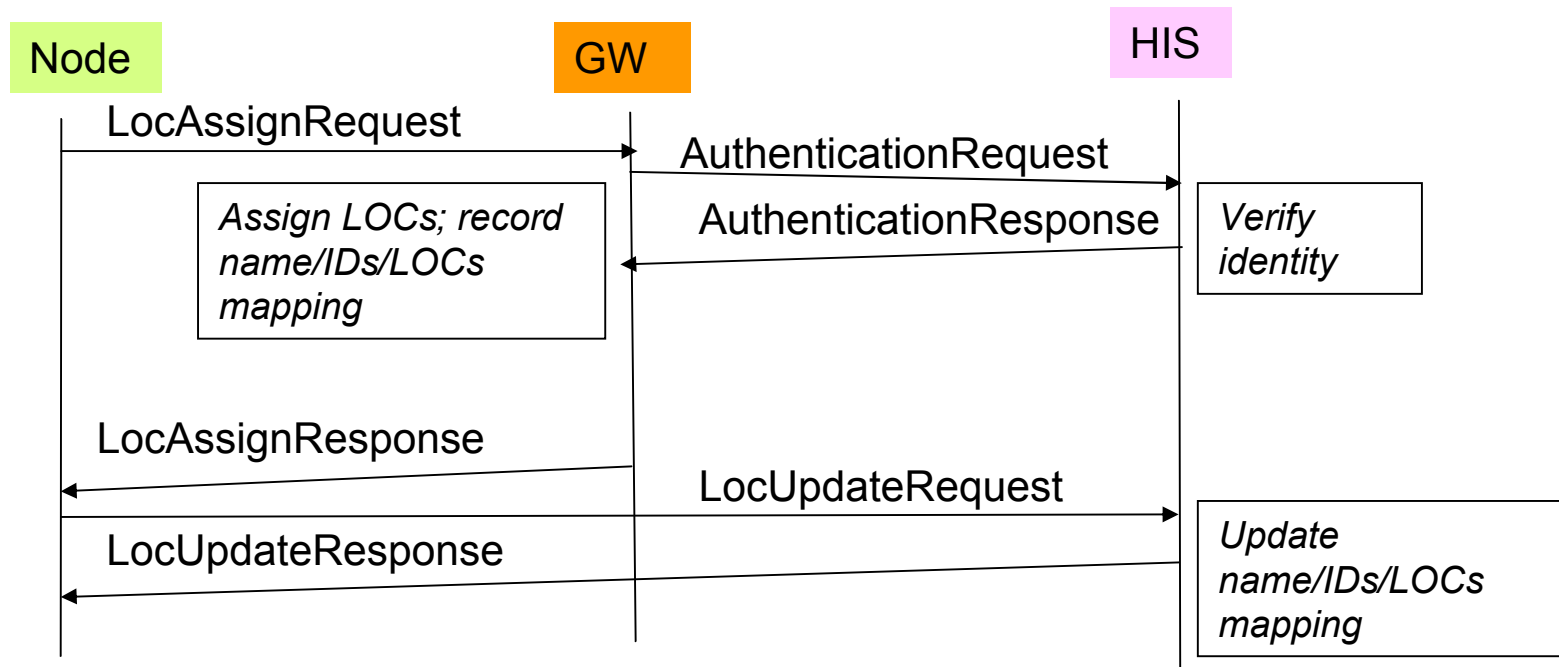
■ Developing testbed to evaluate these overhead

Name configuration

- Nodes generate local names combining feature words
 - e. g., node's usage, owner, location, serial number, installation date and time, etc.
 - kafle-pc, temp-sensor-room-202, ...
- Nodes register names with HIS
 - HIS checks uniqueness
 - In case of conflict
 - HIS may suggest names
 - kafle-pc-2007-nov-20
 - Nodes accept suggestions or regenerate new names
 - kafle-pc-room-502
 - Nodes reregister new names
- Nodes get HIS name to form global names
 - kafle-pc-room-502#mynetwork.org

Locator assignment mechanism (1/2)

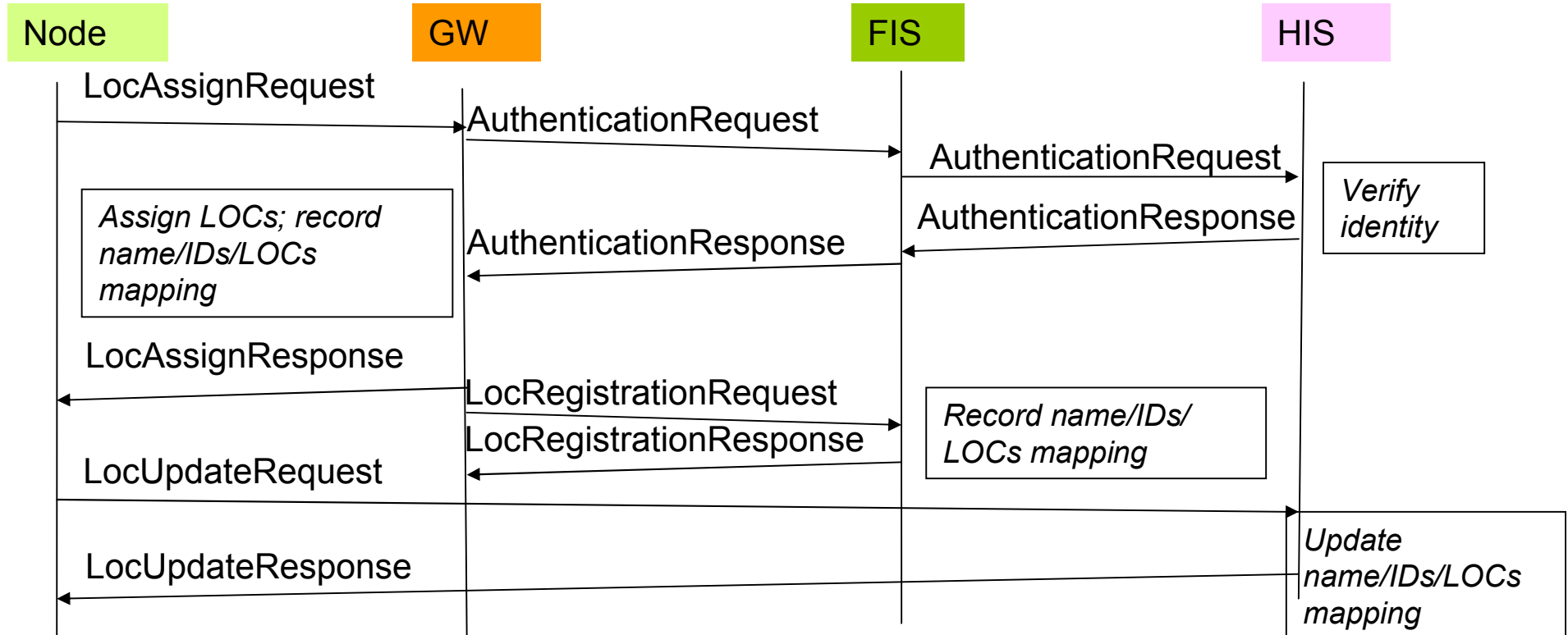
- When Node is in its home network



- Authentication before locator assignment
- Authentication detail in future work

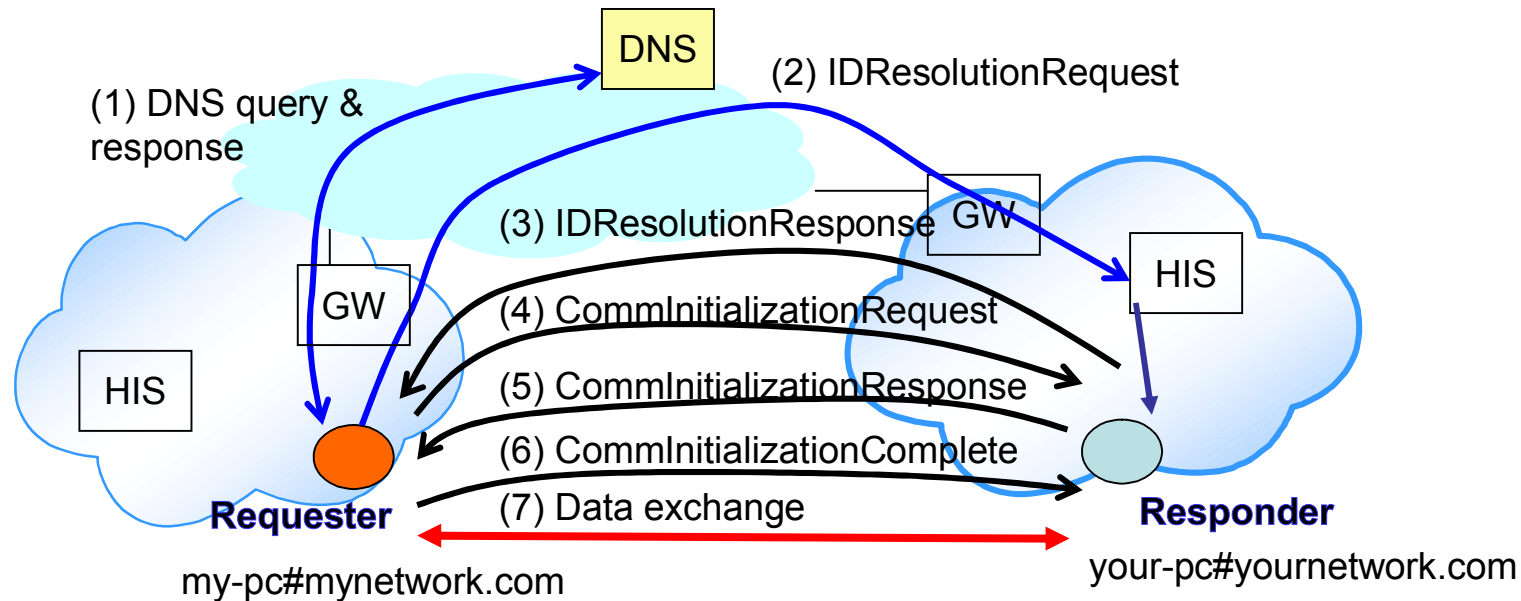
Locator assignment mechanism (2/2)

■ When Node is in a foreign network



- Authentication via FIS
- ID/ LOC mappings stored at both FIS and HIS
- HIS also stores FIS's locator

Communication initialization



- (1) perform a DNS lookup to resolve Responder's HIS name
- (2) query Responder's HIS name to get Responder's locator
- (3-6) establish communication states in Requester and Responder
 - Settle pIDs
 - Settle aIDs
 - Settle ID update algorithm
- (7) exchange packets using aIDs and locators

Session tracking avoidance and privacy protection

- pID does not appear whole in packets
- aID updated regularly
- => session tracking avoided if communication initialization is via a secured channel

- Two possible methods:
 - (1) network-provided secured channel
 - Multiple segments of security association
 - Node-GW; GW-HIS; HIS-HIS; ...
 - (2) end-to-end secured channel using a public-private key pair or a shared key
 - End nodes exchange public keys; encrypt communication initialization messages

Summary and future work

- Identifiers are simple to form and independent of internetwork technology
- Network connectivity only after authentication
- Hiding end node identity from outsiders

- Future work
 - aID update algorithm
 - Scalable routing leveraging ID/LOC split architecture
 - Mobility and multihoming support
 - Evaluation and optimization



Thank you !!!

Contact Information

Ved Kafle

(Researcher)

Network Architecture Group
National Institute of Information and
Communications Technology (NiCT)

Email : kafle@nict.go.jp
Tel: +81-42-327-5471