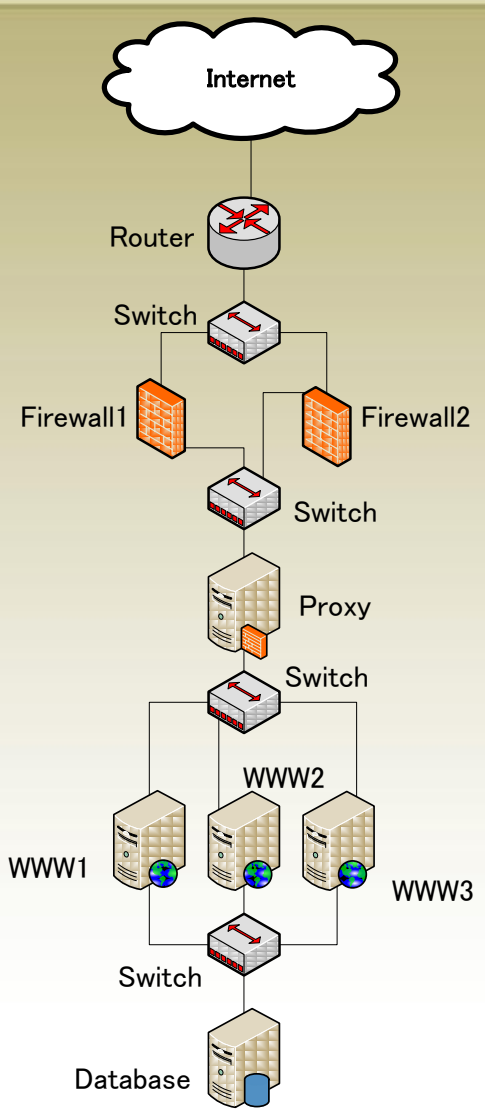
Networked System Modeling and its Access Control Characteristic Analysis

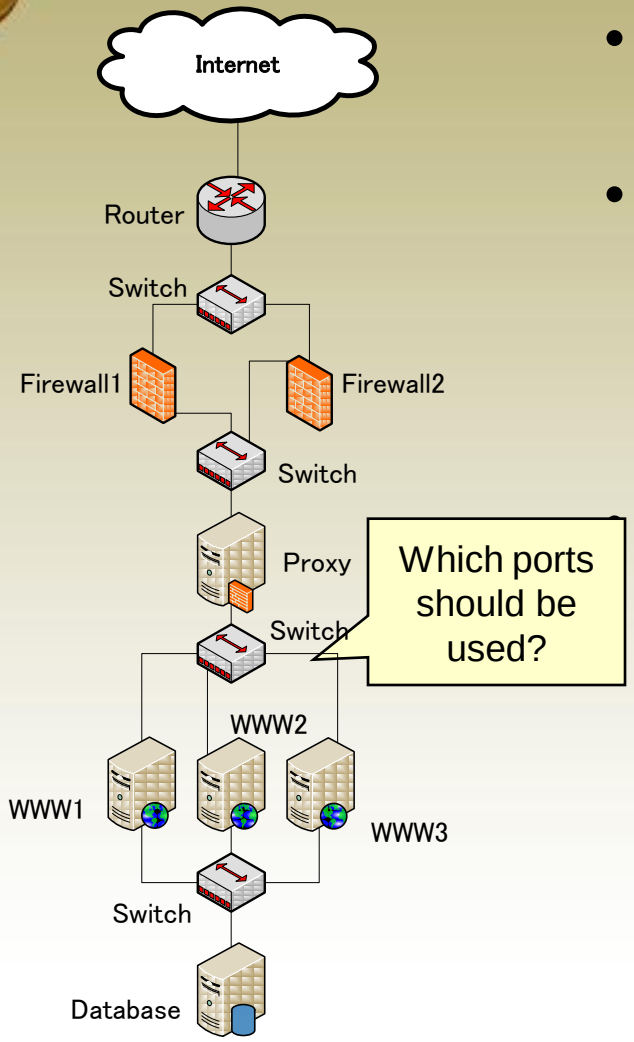
A. Kanaoka (University of Tsukuba, Japan)
M. Kato (IIJ Technology, Inc., Japan)
N. Todo (University of Tsukuba, Japan)
E. Okamoto (University of Tsukuba, Japan)

Networked System

- The service provided through the Internet, is rarely provided by only one server.
  - Various network equipments
  - Hub, Switch, Router, Firewall, IDS, Proxy….
- Networked System (NS)
  - Network equipments
  - LAN technology



Designing Networked System (NS) : Problem statement



- Consideration Point to Design
  - Cost, Throughput, Scalability, Access Control, Availability, Vulnerability Impact
- Difficulty for Optimized Design
  - Complex, even small NS
  - Depending professional knowledge of designer
  - No theoretical Approach and Methodology

Problem on existing NS design

- Lack of Sufficient information on blueprint
- Need more data (ex., Excel spreadsheet file FW rules)

Because of only one level expression for multiple function

NSQ (Networked-system Security Quantification) Model

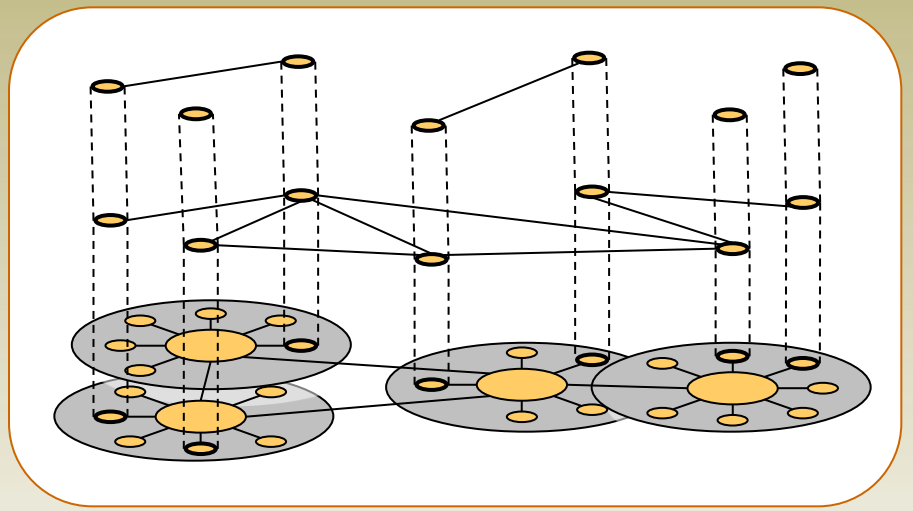
Basic Strategy of Modeling NS

Existing Model

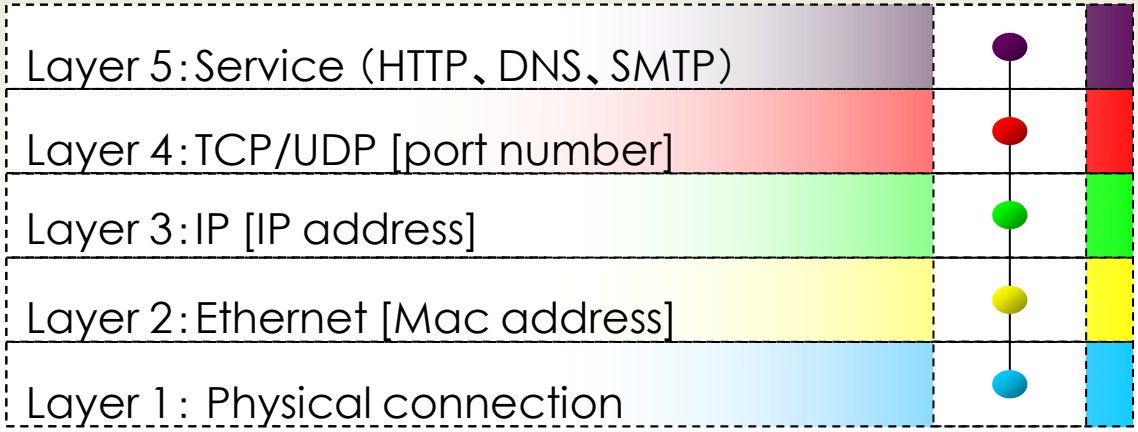
Only physical connection relationship

Proposed Model

Logical Networks of each TCP/IP Layer
+
Connection between each Layer Networks

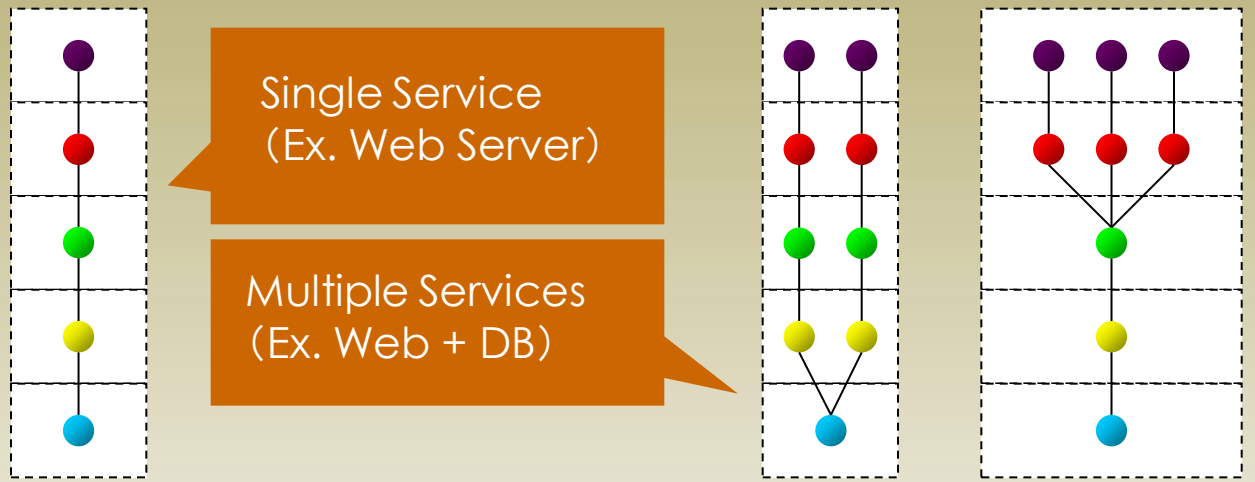


Layer Definition

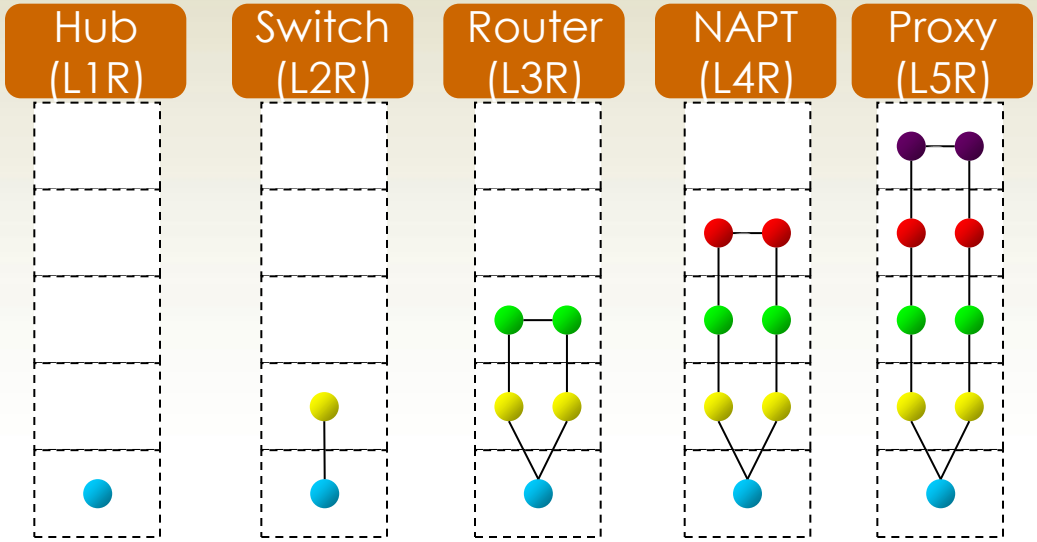


Module Examples

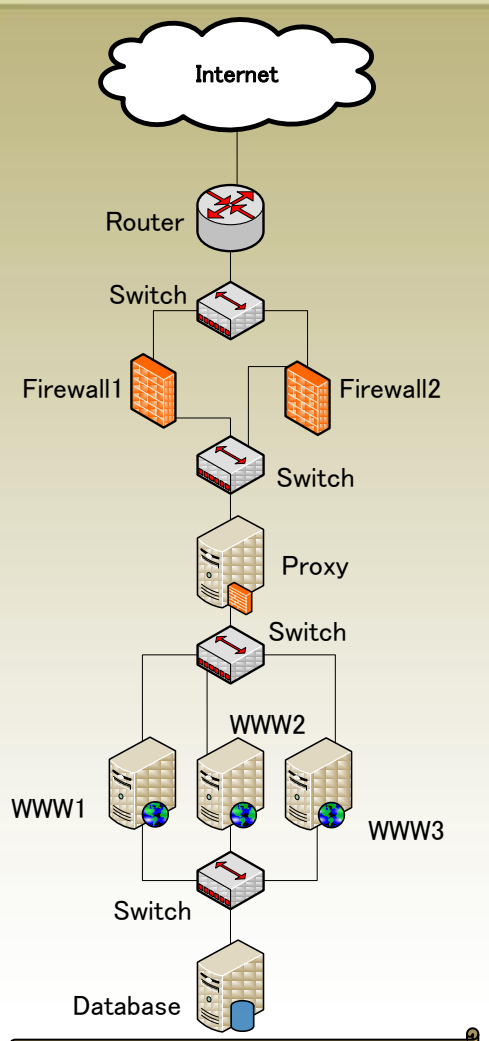
Servers



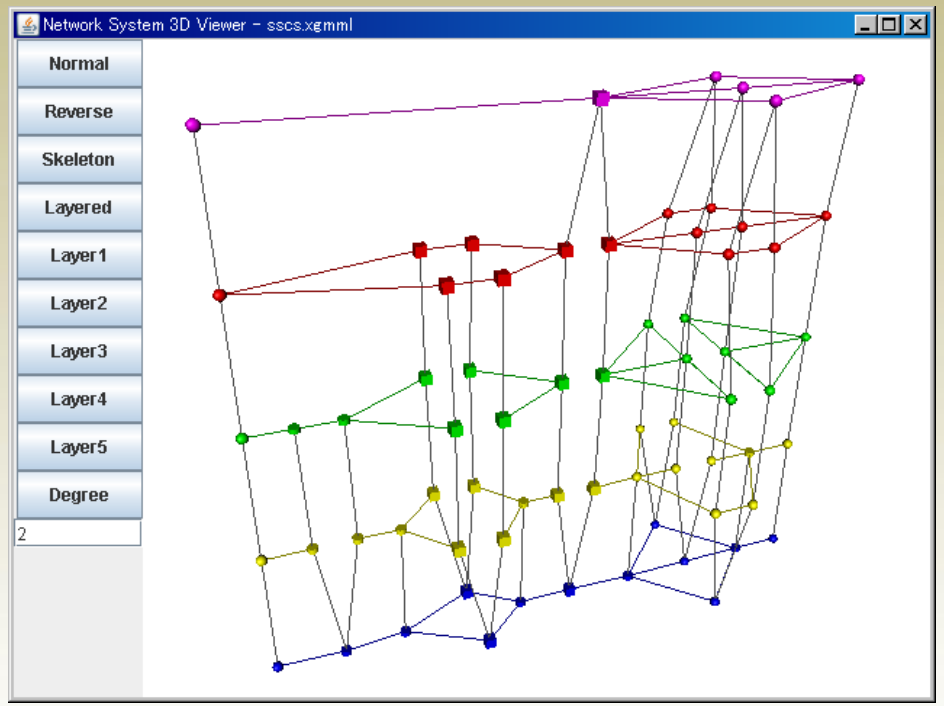
Relay



Example of Proposed Model Expression



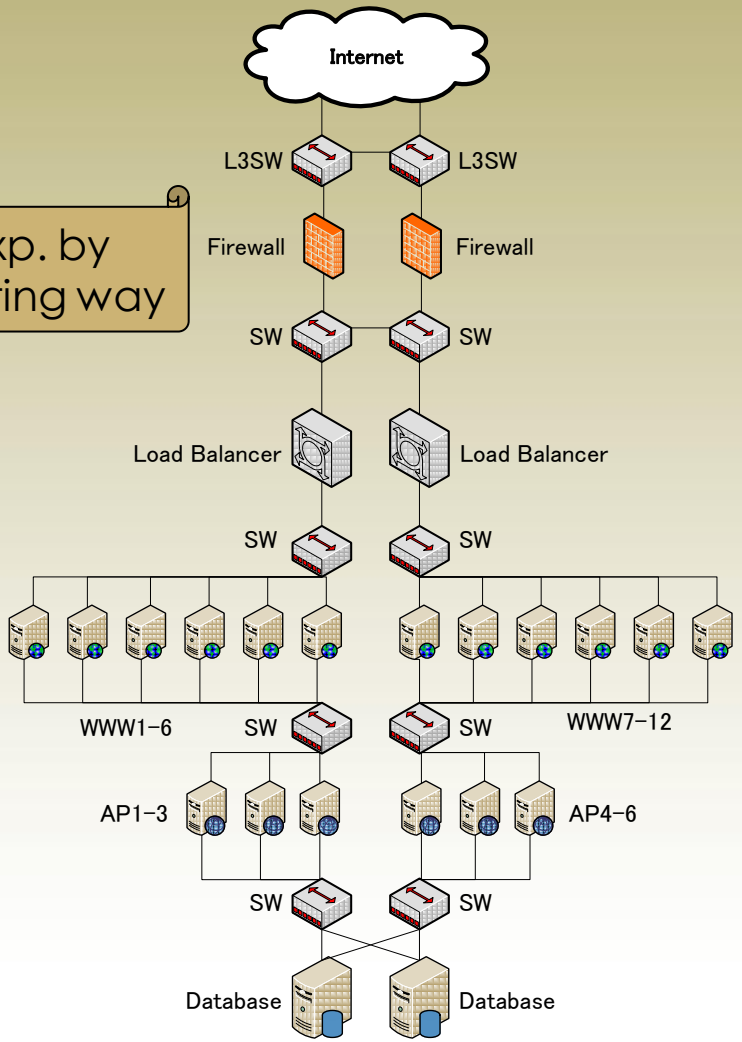
Existing Expression



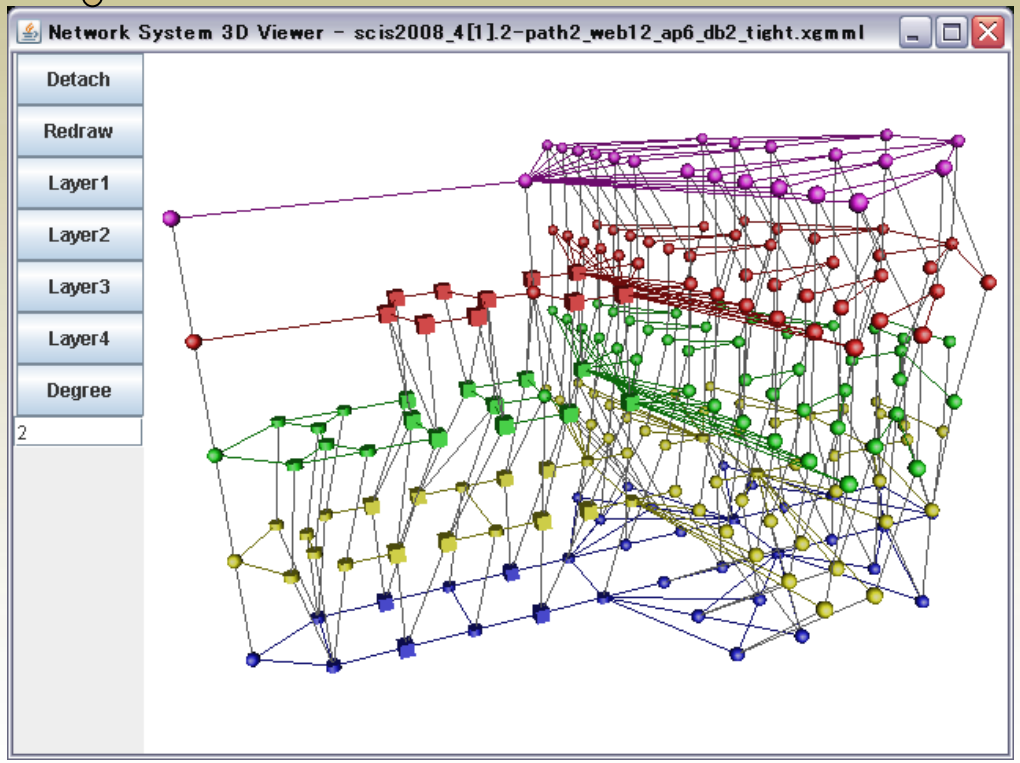
Proposed Expression

Finding Characteristics of Well-designed NS

Exp. by Existing way



Exp. by Proposed Model



Dataset for Characteristic Analysis

- Need to extract common characteristic of NS
- Ideal
  - Whole NS patterns
- Problem
  - **Enormous** number of patterns
  - Only L1 network patterns

Type of Nodes :
S/Ss(Service)、
L1R(Hub)、L2R(Switch)、L3R(Router)、
L4R(NAPT)、L5R(Proxy)

Restriction:
At least 2 nodes which have only one link.

Patterns of L1 Network

# of Nodes	# of Networks (Before isomorphic check)	# of Networks
2	1	1
3	6	6
4	42	27
5	474	294
6	12606	7121
7	470742	283482
8	26364210	N/A
9	2181981354	N/A
10	**292914780702**	N/A

Connection Restriction between Modules

- Most of modules are usually connected to L2R (switch) in existing systems
- Restriction rules
  - At least 2 nodes which have only one link.
  - Connection restriction between nodes
    - Each modules except L2R are connected to L2R

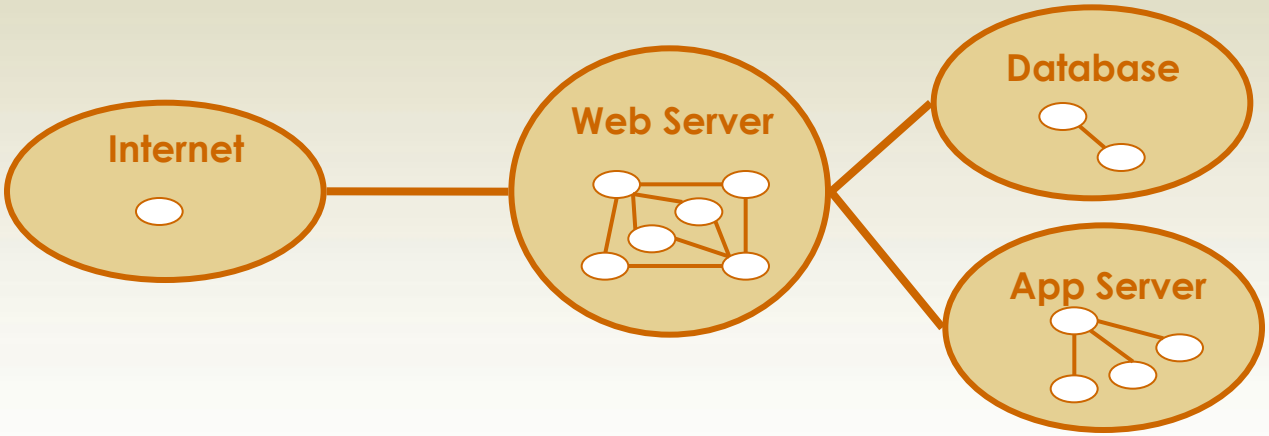
	S	Ss	L1R	L2R	L3R	L4R	L5R
S	×	×	×	○	×	×	×
Ss	×	×	×	○	×	×	×
L1R	×	×	×	○	×	×	×
L2R	○	○	○	×	○	○	○
L3R	×	×	×	○	×	×	×
L4R	×	×	×	○	×	×	×
L5R	×	×	×	○	×	×	×

- Types of module
  - # of link : 1
    - S
  - # of link : multiple
    - L1R, L2R, L3R, L4R, L5R, Ss

# of Nodes	# of Networks (before isomorphic check)	# of Networks
2	0	1
3	1	6
4	1	27
5	6	294
6	21	7121
7	121	283482
8	1061	N/A
9	**10782**	N/A
10	N/A	N/A

Partial L1 Network by L5 Node

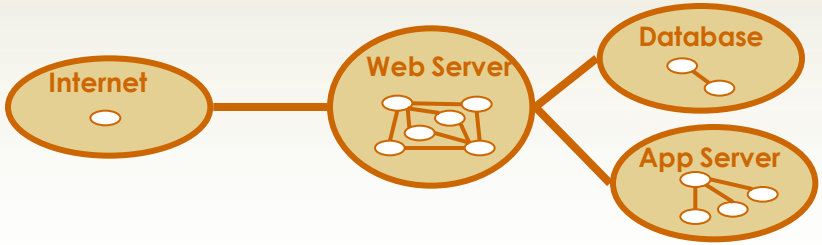
- Based on L5 network (Requirements of function)
  - Each L5 nodes are made by multiple L1



Structure of L1	# of Patterns
• • •	
1-1-5-5	7520
1-3-5-5	140
1-3-4-5	205
1-3-5-5	18020
1-4-4-5	140
1-4-5-5	18170
• • •	

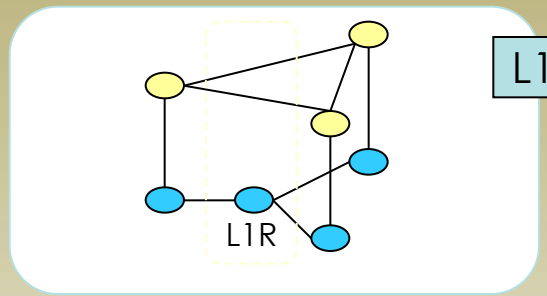
Each Layer Network

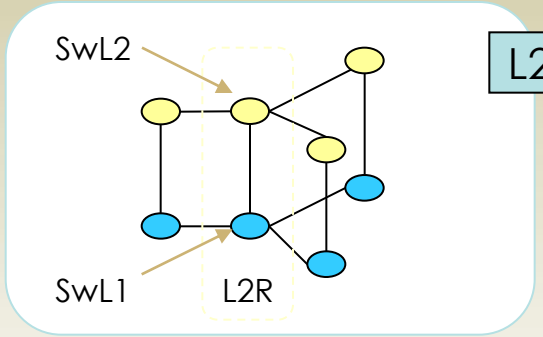
- L5 network
  - 4 services : Internet, Web Server, Database, Application Server
  - 27 patterns (after isomorphic check)
- L1 network
  - Partial networks for each 4 L5 services
  - Connection according to L5 connection
  - # of nodes on L1 networks is 1 to 5
- L2、L3、L4 networks
  - L2 network
    - Decided by L1 network
  - L3、L4 network
    - Decided by
      - L5 network
      - **Access Control Rule**

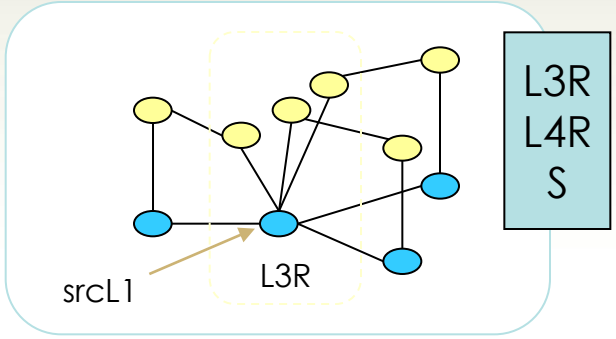


Each Layer Network: L1-L2

- L1R (Hub)
  - Extract L1 nodes connected to L1R
  - Make complete graph among L2 nodes connected by L1 nodes above
- L2R (Switch)
  - Extract L1 nodes connected to SwL1
  - Connect L2 nodes connected by L1 nodes to SwL2
- L3R、L4R、S
  - Extract L1 nodes connected to srcL1
  - Connect each L2 node to L2 node of L3R



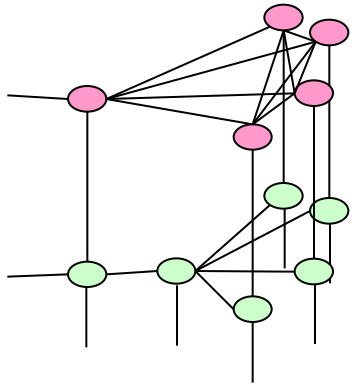




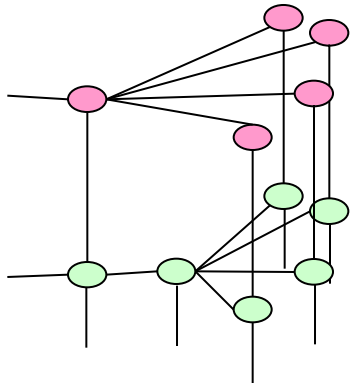
L3, L4 network : Access Control Rules

- L3, L4 network
  - Depends on access control rules
- Access Control Rules on Datasets
  - No control (Case: Loose)
    - All modules in a same segment are able to communicate (has links)
    - Complete graphs in the segment
  - Well-Managed (Case: Efficient)
    - Only necessary communication paths
    - “Optimum” is “Minumum number of links” in this paper

Case: Loose



Case: Efficient



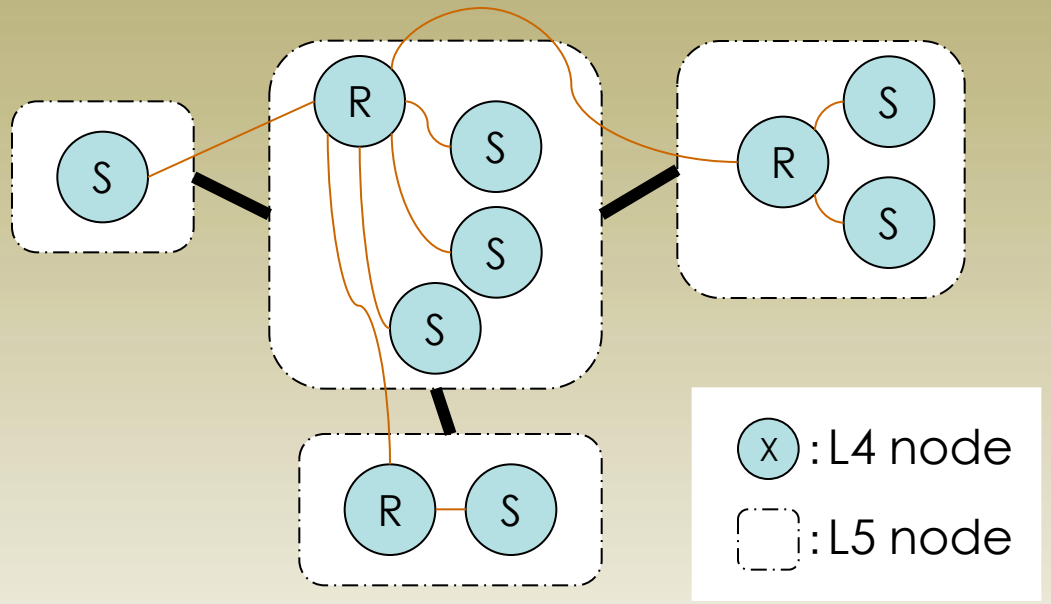
Number of Links Reduction Algorithm (Efficient connection algorithm)

Basic Idea

Depends on Links of Upper Layer

• If there is relay modules on lower layer

-only nodes of the relay module on lower layer, are connected to nodes of outside



Algorithm

Connection between node A and B on layer x

1: Extract candidates on layer x-1 of A

- if LxR exists inside A, nodes of LxR are candidates
- else, all nodes are candidates

2: Extract candidates on layer x-1 of B

3: Connect candidates between A and B

Degree Distributions

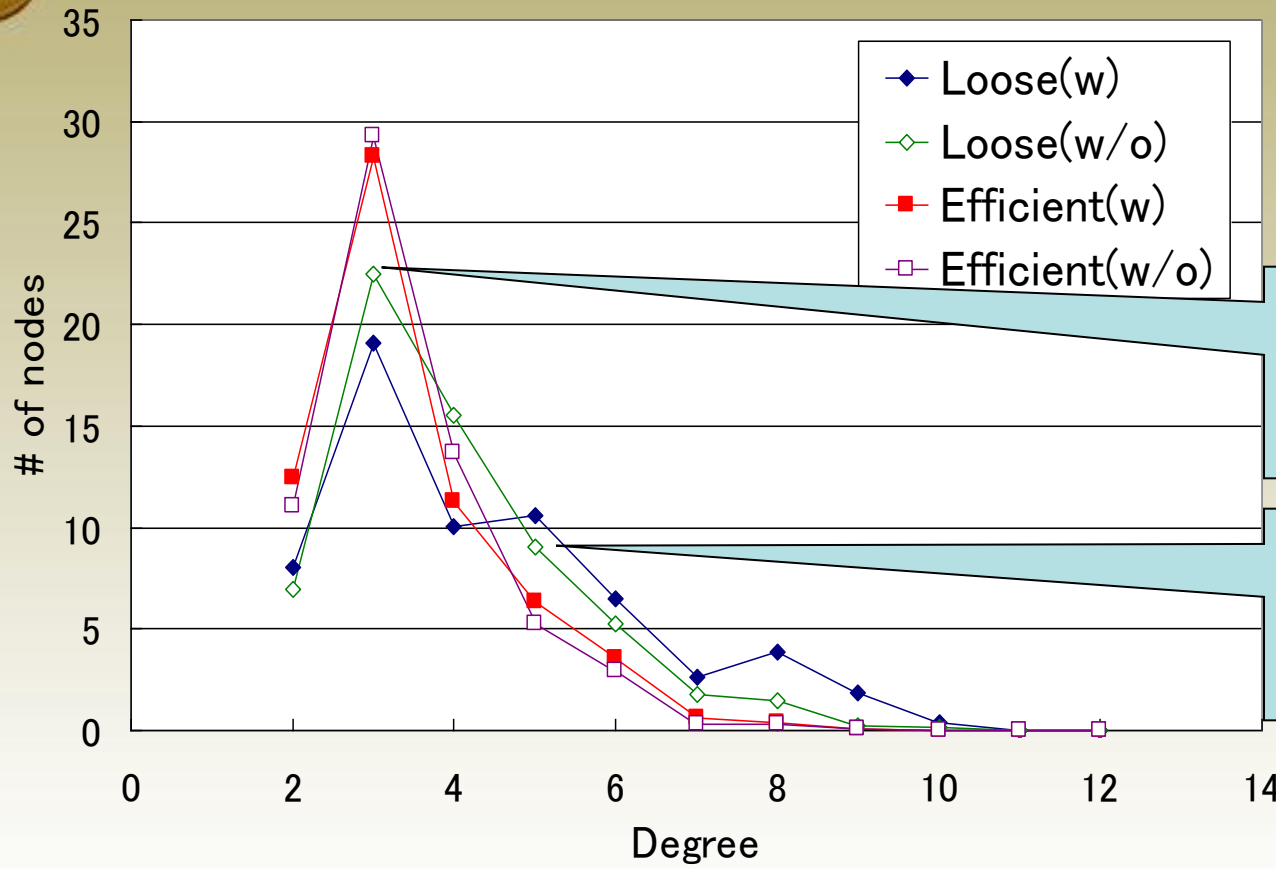
- Comparison target
  - Distributions between loose and efficient access control algorithm
  - Distributions between ones with/without a particular module

- Comparison
  - Between groups
    - Dataset are divided into groups
    - group : number of nodes
  - Extract groups of which patterns are more than 300

Hypothesis
from out result

If an NS is connected efficiently
from an access control point of view,
the link distribution is fixed
regardless of the restriction on the module connection.

Particular module effect (L1R)
of node: 63



Little difference between efficient cases

NS with L1R has flatter distribution in loose case

Similar result on other cases

the link distribution is fixed regardless of the restriction on the module connection

→ Support our hypothesis

Conclusion

- Propose new model of networked system
  - NSQ (Networked-system Security Quantification) model
- Build dataset for analysis
  - Networked system construction algorithms
- Analysis by degree distribution
  - Difference between Loose and Efficient
  - Difference between distribution with/without a particular module
- Hypothesis from result
  - If an NS is connected efficiently from an access control point of view, the link distribution is fixed regardless of the restriction on the module connection
- Future works
  - Approximation of fixed distribution and extract parameters
  - Evaluation method using parameters