Networked System Modeling and its Access Control Characteristic Analysis

Akira Kanaoka, Masahiko Kato, Nobukatsu Todo, and Eiji Okamoto

***Abstract*—**Integration of a networked system (NS), which consists of various network equipment and uses LAN technology to provide a service, has become increasingly important. However, there have been few studies in on the integration of secure NSs. In this paper, we propose a new model of system expression to realize secure and reasonable NS integration, and analyze the characteristics of the proposed model. The obtained results suggest that a well-designed NS from an access control viewpoint has a fixed link distribution, regardless of connection restriction.

***Keywords*—**Networked system, access control, modeling, security.

I. Introduction

When we want to provide a service through the Internet, the service is rarely provided by only one server. Usually, various network equipment is assigned to the system, and LAN technology is used to maintain redundancy, scalability, and security. We call such a system a Networked System (NS).

It is complicated to integrate an NS if it is a small system. Thus, recent business growth through the Internet requires higher these characteristics to NS. Although integration of an NS is increasingly important, it depends on professional experience, and there has been little research on NS integration.

Since an NS consists of several network devices such as servers, routers, and switches, most previous studies considered single function networks [HST05][SSK06] [Chekuri07] [LNSS07][Wolf07]. We cannot apply this research to the integration of NS for network and system design.

In this paper, we propose a new model of system expression to realize secure and reasonable NS integration. To include several functions of network devices in one system expression, we adopt logical networks of layers and connect these networks. The proposed model realizes the representation of most network devices, even advanced devices such as virtual IPs, load balancers, and VRRP.

We also analyze the proposed model from an access control point of view, using a simple NS construction algorithm. These algorithms are also proposed in this paper.

In Section 2, we outline previous studies on network and system design. The NS model is proposed in Section 3, and NS construction algorithms are proposed in Section 4. In Section 5, we analyze the characteristics of the NS from an access control point of view. We then conclude the paper in Section 6.

Akira Kanaoka, Nobukatsu Todo and Eiji Okamoto are with University of Tsukuba, Japan, email: {kanaoka,okamoto}@risk.tsukuba.ac.jp, toudou@cipher.risk.tsukuba.ac.jp. Masahiko Kato is with IIJ Technology Inc., Japan, email:masa@iij-tech.co.jp

II. Network and System Design

Most of these studies realize an effective solution of throughput or optimized network architecture, including design restrictions and requirements [HST05] [SSK06] [Chekuri07] [LNSS07] [Wolf07]. Although these studies acquire solutions using such restrictions and requirements appropriately, most of these studies focused on single function networks. From a graph theoretical point of view, nodes that form an edge or relay point of a network consist of only one function.

On the other hand, networks of a NS consist of various functions, including Hub, Switch, Router, Firewall, Load Balancer, Server, Database, and Proxy. If there are several nodes with various functions in a graph, the meanings of edge and graph change. We cannot directly apply previous studies to achieve optimized NS for a different meaning of graph.

III. NS Model Definitions

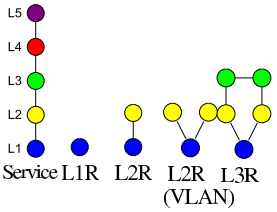
Networked systems consist of various types of network equipment, including hubs, switches, routers, and servers. We first define the Module as the element that provides network function. The Module is composed of several services and network relays.

Second, we define the Layers used to distinguish modules. Each layer is defined in Table I, which is sufficient to express all modules for a NS.

TABLE I
Layer Definitions

Layer 5	Abstracted service (WWW, DNS, etc.)
Layer 4	Services by port number (80, 53, etc)
Layer 3	IP
Layer 2	MAC address space
Layer 1	Physical object

TABLE II
Module Examples



Six modules are defined by layer definition. The service module (S) provides a service such as WWW, e-mail, or DNS. The Internet module (I) provides Internet service and is the source of communication with the system. The Layer 1 Relay (L1R), Layer 2 Relay (L2R), Layer 3 Relay (L3R), and Layer 4 Relay (L4R) modules are the relay modules at each layer.

A module has several nodes for each layer, according to its function. For example, the router module has several layer 3 (L3) nodes and no nodes above layer 4 (L4).

The node is the source, destination, and relay point of communication in its layer. In L1, both ends of a cable are the

source and destination of communication. In addition, MAC addresses are both sources and destinations of communication in L2. The relay node relays communication data from a source to a destination based on the address information of its layer.

A module has only one node in L1 and several nodes above L2, depending on the function. For example, L1R does not provide any services above L2. There are no nodes above L2. L2R has several nodes in L2 based on the number of VLANs, and there are no nodes above L3. L3R has several nodes in L2 based on the number of IP, and several nodes in L2 according to L3 nodes.

Each node is connected by a link. There are two types of connections: links between nodes of different modules and the same layer, and links between nodes of the same module and a different layer. The first type expresses the possibility of direct communication of its layer. The second type expresses the relationship between nodes in the module and indirect communication by intermediation of nodes. Table II shows example modules in the proposed model.

For these definitions, the NS, which is a set of modules, is expressed by a set of logical networks realized by the connection of nodes from each module. Figure 2 shows an example of the NS using the proposed model. The same NS is expressed at present as shown in Figure 1.

In this paper, node and link correspond to vertex and edge, respectively, in graph theory.

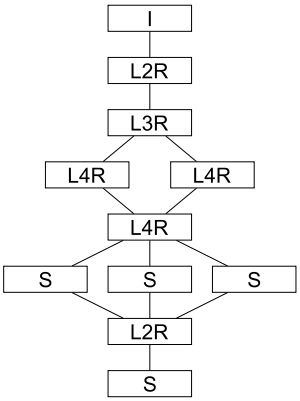


Fig. 1. Current expression of NS

IV. NS Construction

To realize a secure NS, it is not sufficient to model the NS. A method by which to construct a secure NS and a method by which to measure security for the NS are also necessary.

First, we must analyze the networked system using the proposed model in order to find common characteristics for security measurement. In order to find common characteristics for security measurement, the analysis of several examples of NS is undesirable. Comprehensive analysis is necessary in order to achieve common characteristics.

In this section, we describe how to collect patterns of an NS without lack of comprehensiveness.

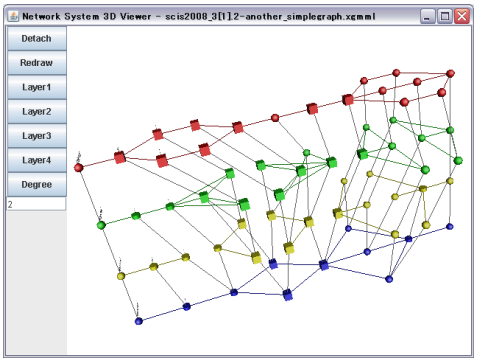


Fig. 2. Expression of NS by the proposed model

TABLE III
NUMBER OF L1 NETWORKS: EDGE NODES

# of node	Before iso. check	After iso. check
2	1	1
3	6	6
4	42	27
5	474	294
6	12,606	7,121
7	470,742	283,482
8	26,364,210	N/A
9	2,181,981,354	N/A
10	292,914,780,702	N/A

A. Restriction of Node Connection

To collect comprehensive patterns of NSs, the simplest method of collection is an exhaustive search. We first consider connection between modules, which is L1 connection. Modules are classified into two styles based on the position on the network, namely, modules that are end points of communication, such as I and S, and modules that are joint points of communication, such as L1R, L2R, L3R, L4R, and S. End point modules are connected to only one module, and joint modules are connected to several modules. The NS must at least include two end points (I and S).

We classify the L1 network pattern under this condition. In Table III, we show the numbers of patterns before and after isomorphism check. We could not show the numbers of patterns from eight to ten nodes, because of the huge amount of computation time required for an isomorphic check.

If we consider building all patterns of the entire NS by the proposed model, the desirable maximum number of modules is between 20 and 100. Since the number of patterns in the case of seven nodes is 284,482, it is clear that the number of patterns without any restriction is enormous. These patterns contain cases that are rarely used by the real NS. For example, there are five L3R (router) modules between I and S in the patterns of the seven-node case.

There are many cases in which network equipment and servers are connected to switches. That is, firewalls that are a special function of L3R or L4R are rarely connected directly to servers. Even if a firewall is connected directly to servers, such a firewall usually provides the L3R or L4R function and the L2R (switching) function. This firewall can be considered as two modules in one piece of hardware. Based on the

TABLE IV
NUMBER OF L1 NETWORKS UNDER THE RESTRICTION RULES

# of node	Rest. #1	Rest. #2
2	0	0
3	1	1
4	1	2
5	6	14
6	21	111
7	121	1722
8	1,061	39815
9	10,782	N/A
10	N/A	N/A

above situation, we have the following restrictions on module connection.

a) Restriction rule #1:: All modules except L2R must connect to L2R, and L2R cannot connect to other L2R modules.

b) Restriction rule #2:: All modules except L2R must connect to L2R. L2R can connect to other L2R modules.

Table IV shows the numbers of patterns for L1 connection under the above restrictions. The number of patterns is less than in the non-restricted case.

B. Layer 5 Nodes as Functional Requirements

When we consider the maximum number of modules to be 20 or 100, the number of patterns above will still be unrealistic to analyze. We then use another method to reduce the number of patterns using the functional requirements of the NS.

When a business client asks a system integrator to integrate the NS, the system requirements are given by a business client. Such requirements usually include system functions and the relationship between functions.

For example, when a client integrates an e-commerce web system, the system requirements include functions such as front web servers, application servers, and databases. The requirements also include its relationship. Such a relationship also includes front servers passing requests to application servers and application servers collecting appropriate data from a DB. We can draw a functional connection from these requirements and consider this network as an L5 network and functions as L5 nodes.

Function (L5) nodes consist of several L1 nodes, that is, a partial network is built by several modules (Figure 3). Connection patterns of the L1 partial network are obtained by the results from the last section (Table III), and the connection patterns of the L1 nodes between different L5 nodes are decided by L5 connections.

Table V shows an extract of the number of patterns that use L5 nodes as functions. The entire NS is covered by dozens of nodes.

C. Logical Network Connection

L1 and L5 connections are decided by the last section and other layer connections must be decided in order to analyze the proposed model and achieve common characteristics.

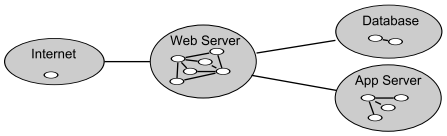


Fig. 3. Four L5 nodes, each of which contains one, six, two, and four L1 nodes

TABLE V
NUMBER OF L1 NETWORKS USING L5 NODES AS FUNCTIONS (EXTRACT)

# of L5 nodes	L1 nodes of each func.	# of patterns
3	1-5-5	3660
	...	
	5-5-5	128235
4	...	
	1-1-5-5	7520
	1-3-3-5	140
	1-3-4-5	205
	1-3-5-5	18020
	1-4-4-5	140
	1-4-5-5	18170
	...	

The following subsection describes L2 connection, and L3 and L4 connections by a different access control method are described in later subsections.

1) L2 network: L2 connection is decided uniquely by L1 connection. The algorithm of L2 connection is shown in Algorithm 1.

Basically, L2 connections are decided by the L1 connection relationship. If L1 nodes a and b are connected, then L2 nodes x and y, which are connected to a and b respectively, are connected to each other. However, if NS has L1R, then the L2 nodes on which L1 nodes are connected to L1R are all connected. Thus, the case of NS having L2R should be considered because of its relay method. The subalgorithms in Algorithm 1 are omitted due to space limitations.

Algorithm 1 L2 connection algorithm

Require: L1 link set L
Ensure: L1 and L2 link set L'
1: $L' \leftarrow L$
2: $L' \leftarrow L' \cup linkByL1R(L')$
3: $L' \leftarrow L' \cup linkByL2R(L')$
4: $L' \leftarrow L' \cup linkByOverL3R(L')$

2) Loose connection on L3 and L4: The L3 and L4 networks are not decided uniquely because they depend on access control rules. In this subsection, we describe L3 and L4 network constructions for the loosest access control case.

The basic strategy of loose access control is to connect all possible nodes. All connectable nodes of L3 or L4 are extracted depending on the lower layer. First, L3 layer connections are decided by L2 connection. Then, L4 layer connections are decided by L3 connection.

The algorithm of loose connection on L3 and L4 is shown in Algorithm 2. The function $compGraph()$ in Algorithm 2 connects all nodes. The details of this algorithm are omitted

due to space limitations.

Algorithm 2 Loose connection algorithm

Require: Link set L, Node set S
Ensure: Link set L'
1: $L' \leftarrow L$
2: **for all** L3 node $x \in S$ **do**
3: $y \leftarrow$ L2 node such that $(x, y) \in L$
4: $V \leftarrow findL3connectable(y, L)$
5: $L' \leftarrow L' \cup compGraph(V, L)$
6: **end for**
7: **for all** L4 node $x \in S$ **do**
8: $y \leftarrow$ L3 node such that $(x, y) \in L$
9: $V \leftarrow findL4connectable(y, L)$
10: $L \leftarrow compGraph(V, L)$
11: **end for**

Algorithm 3 Finding a connectable L3 node: $findL3connectable()$

Require: L2 node x, Link set L
Ensure: L3 node set S
1: $S \leftarrow \phi$
2: $V \leftarrow$ L2 nodes p such that $(x, p) \in L$
3: **for all** L2 node $i \in V$ **do**
4: **if** i is a node of L2R **then**
5: $S \leftarrow S \cup findL3connectable(i, L)$
6: **else**
7: $S \leftarrow S \cup \{$ one of L3 node y such that $(i, y) \in L\}$
8: **end if**
9: **end for**

3) Efficient connection of L3 and L4 networks: To realize optimum access control for NS, the number of links between nodes must be minimized without isolation of the nodes in each layer. However, the optimum access control method seems difficult to realize, and realizing optimum access control method is out of scope in this paper. Therefore, we describe L3 and L4 network constructions with efficient access control, which realizes a reduction in the number of links in this subsection.

We first extract candidate nodes of L4 to be connected according to L5 connection and then connect candidate L4 nodes with a minimum number of links. Candidates are decided by the existence of the L4R module inside L5 node. If an L5 node has an L4R module, L4 nodes of L4R are chosen as candidates. If not, the L4 nodes of all modules inside this L5 node are chosen as candidates. Next, L3 nodes are also connected according to L4 connection.

The algorithm of efficient connection on L3 and L4 is shown in Algorithm 4. The function $connect(S_A, S_B)$ in Algorithm 4 realizes the minimum number of links between S_A and S_B. $candidateL4nodes()$ is the function for the choice candidate of L4 nodes in one of the L5 nodes. The details of this algorithm are omitted due to space limitations.

Algorithm 4 Efficient connection algorithm

Require: Link Set L
Ensure: Link Set L'
1: $L' \leftarrow L$
2: **for all** L5 nodes x, y such that $(x, y) \in L$ **do**
3: $S_A \leftarrow candidateL4nodes(x, L)$
4: $S_B \leftarrow candidateL4nodes(y, L)$
5: $L' \leftarrow L' \cup connect(S_A, S_B)$
6: **end for**
7: **for all** L4 nodes x, y such that $(x, y) \in L'$ **do**
8: $p \leftarrow$ L2 node such that (p, k) and $(k, x) \in L'$ for some L3 node k
9: $q \leftarrow$ L2 node such that (q, l) and $(l, y) \in L'$ for some L3 node l
10: $V \leftarrow searchRoute(p, q)$
11: $L' \leftarrow connectRoute(x, y, V)$
12: **end for**

Algorithm 5 Extract L2 or L3 nodes on the route between L2 nodes x, y: $searchRoute()$

Require: x,y, Link set L
Ensure: Node set V
1: $V \leftarrow \phi$
2: **if** $(x, y) \in L$ **then**
3: $V \leftarrow V \cup \{x, y\}$
4: **else**
5: $V \leftarrow V \cup \{x\}$
6: **for all** L2 or L3 node i **do**
7: **if** $(x, i) \in L$ and $searchRoute(i, y) \neq \phi$ **then**
8: $V \leftarrow V \cup searchRoute(i, y)$
9: return
10: **end if**
11: **end for**
12: $V \leftarrow V / \{x\}$
13: **end if**

Algorithm 6 Connect L3 nodes between x, y using route V: $connectRoute(x, y, V)$

Require: Node x,y, Node set V
Ensure: Link set L
1: $L \leftarrow \phi$
2: $a \leftarrow x$
3: $b \leftarrow$ null
4: **while** $V \neq \phi$ **do**
5: $b \leftarrow$ first node of V
6: $V \leftarrow V / \{b\}$
7: **if** b is L3 node **then**
8: $L \leftarrow L \cup \{(a, b)\}$
9: $a \leftarrow b$
10: **end if**
11: **end while**

V. Model Analysis

A. Differences between Access Control Algorithms for All Cases

The networked system expressed by the proposed model can be analyzed with respect to a number of aspects, such as scalability, cost, throughput, damage potential by vulnerabilities, and access control. It depends on the design requirements for the NS. In this paper, we focus on access control.

When two nodes can communicate, there is a link between those nodes. If the access control policies are different, the link distributions are also different. Therefore, in this section, we compare the link distributions between loose connection and efficient access control connection. The target of the NS is providing Web service, which is the most typical internet service. The requirement of the functions is fixed at four services: Internet, Web server, Application Server, and Database. Four functions are assigned as the L5 node and its possible number of connection types is 27.

The inside number of each node is covered widely from one to five. The maximum number of modules on the NS is 20, i.e., five nodes for each L5 nodes.

The maximum number of nodes is 72, and the minimum number of nodes is 16. The connection between the nodes is decided by Algorithm 2 or Algorithm 4.

1) Comparison between connection algorithms: Figure 4 shows the link distribution of the 51-node case. Figure 5 shows the link distribution of the 58-node case. Figure 6 shows the link distribution of the 63-node case. Figure 7 shows the link distribution of the 66-node case.

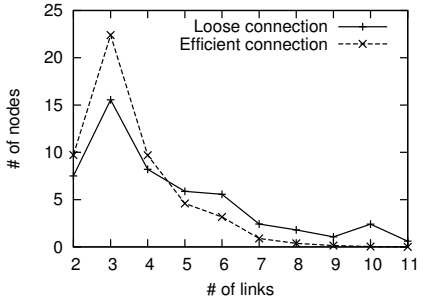


Fig. 4. Link distribution: # of nodes = 51

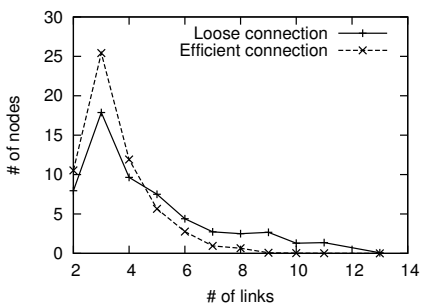


Fig. 5. Link distribution: # of nodes = 58

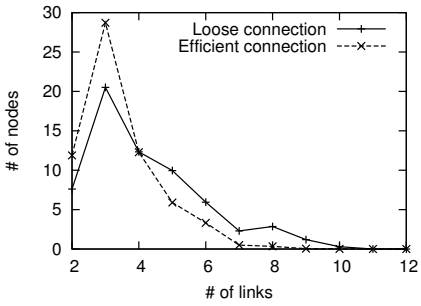


Fig. 6. Link distribution: # of nodes = 63

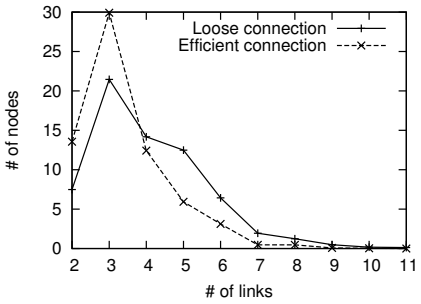


Fig. 7. Link distribution: # of nodes = 66

In this paper, due to space limitations, we present the results for only four cases. However, the results are similar for all cases.

Efficient cases have a smooth link distribution, and loose cases have a rough link distribution.

There are peaks on the number of links with 3 (L=3) in both loose and efficient cases. The efficient access control case has a larger number of nodes in L=3 than that in the loose case. In L=4, the numbers of nodes are similar. Then, L>5, and the loose access control case has a larger number of nodes. The efficient case has a high peak and low skirts, and the loose case has a low peak and relatively high skirts, that is, it is flatter than the efficient case.

The reason on flatter is considered as influences by loose connection. When the connection policy is loose, several links are drawn in one node in Layers 3 and 4.

2) Comparison between connection restrictions: We also compare link distributions for the cases of restrictions #1 and #2.

Figures 8 and 9 compare the link distributions between each restriction for the 63-node case. Figures 10 and 11 compare the link distributions between each restriction for the 66-node case.

Although the basic characteristics of both distributions are as above, the loose case link distribution on restriction #2 is flatter than that on restriction #1.

The difference between efficient cases in both restrictions is interesting in that the distributions are similar. Based on this result, we use the following hypothesis of link distributions.

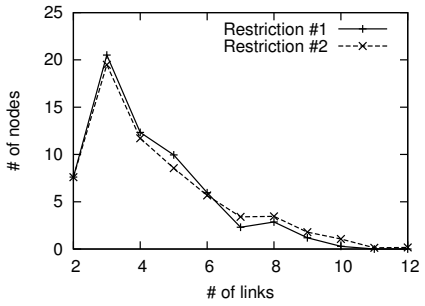


Fig. 8. Link distribution on loose connection: # of nodes = 63

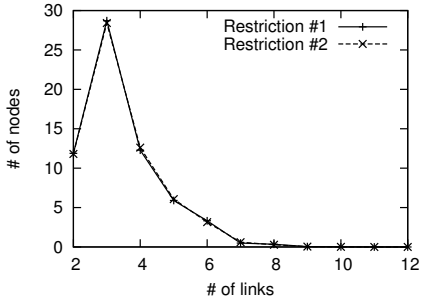


Fig. 9. Link distribution on efficient connection: # of nodes = 63

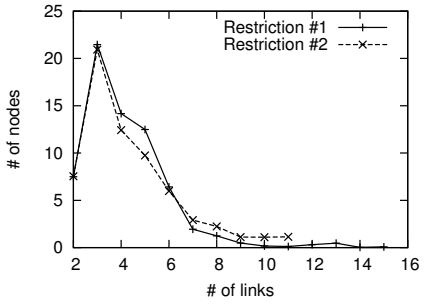


Fig. 10. Link distribution on loose connection: # of nodes = 66

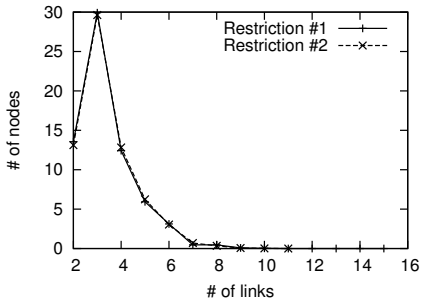


Fig. 11. Link distribution on efficient connection: # of nodes = 66

Hypothesis: 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.

B. Influences of the module with respect to link distribution

In this section, we analyze the influence of the module on the link distribution. Intuitively, an NS that has a large number of L4R or L3R is better than one with a large number of L1R.

We compared the link distribution characteristics between loose connection and efficient access control connection in order to confirm its assumption.

We first analyze the L1R influence of the link distribution on restriction #1. Figures 12 and 13 show the link distribution of the 63-node case of the NS with and without L1R. Figures 14 and 15 show the link distribution of the 66-node case of the NS with and without L1R.

In comparison with loose connection, the distributions of the loose case with L1R are flatter than those without L1R. On the other hand, there is little difference between efficient cases. This result also supports our hypothesis.

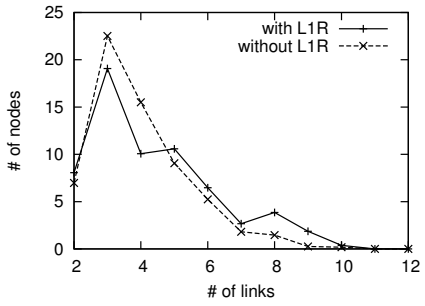


Fig. 12. Link distribution on loose connection: # of nodes = 63

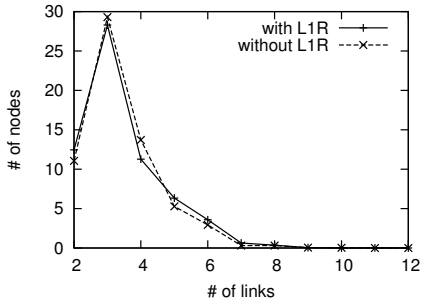


Fig. 13. Link distribution on efficient connection: # of nodes = 63

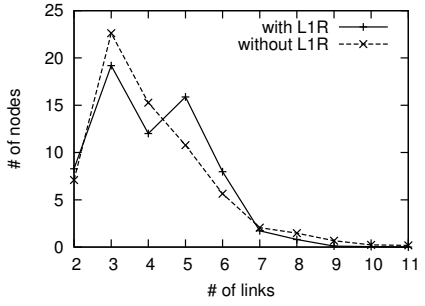


Fig. 14. Link distribution on loose connection: # of nodes = 66

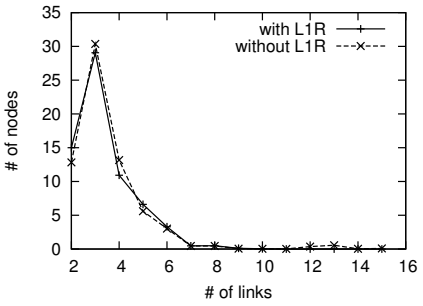


Fig. 15. Link distribution on efficient connection: # of nodes = 66

Next, we analyze L3R influence to link distribution on restriction #1. Figures 16 and 17 show the link distribution of the 63-node case of NS with and without L3R, respectively. Figures 18 and 19 show the link distribution of the 66-node case of NS with and without L3R, respectively.

In comparison with loose connection, the distribution of the loose case with L3R is smooth, whereas the distribution of the loose case without L3R is rough. On the other hand, there is little difference between the distributions for efficient cases. This result supports our hypothesis.

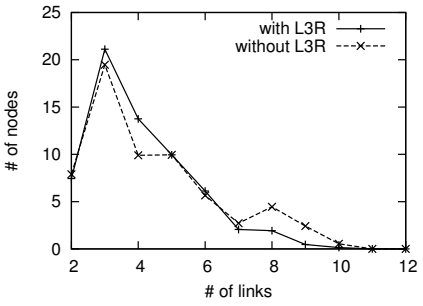


Fig. 16. Link distribution on loose connection: # of nodes = 63

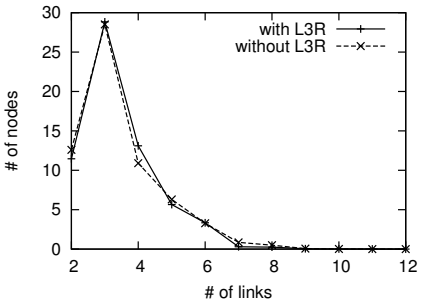


Fig. 17. Link distribution on efficient connection: # of nodes = 63

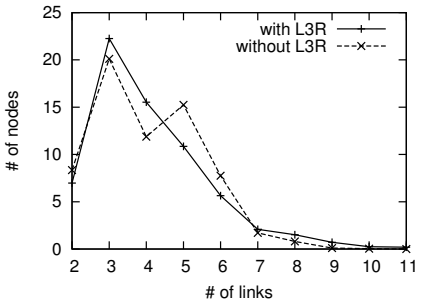


Fig. 18. Link distribution on loose connection: # of nodes = 66

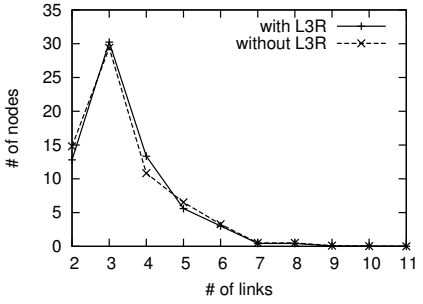


Fig. 19. Link distribution on efficient connection: # of nodes = 66

Finally, we analyze the influence of L4R of the link distribution on restriction #1. Figures 20 and 21 show the link distribution of the 63-node case of NS with and without L4R. Figures 22 and 23 show the link distribution of the 66-node case of NS with and without L4R.

In comparison with loose connection, both distributions have little difference in shape compared to the previous results.

In the L1R and L3R cases, the distributions of efficient cases are also same. However, in L4R cases, there are differences. There is a higher peak and lower skirt in the L4R case. The relay module on the higher layer can be considered to provide effective access control, i.e., relay module raises its distribution peak, lowers its skirt, and reduces the average number of links.

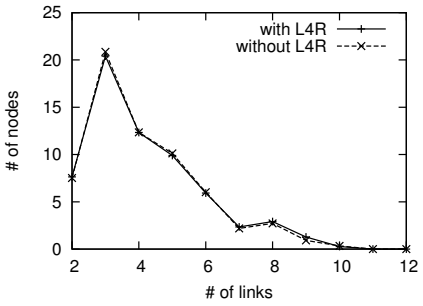


Fig. 20. Link distribution on loose connection: # of nodes = 63

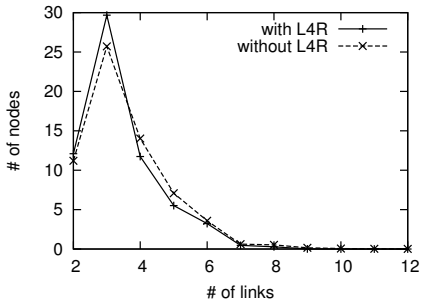


Fig. 21. Link distribution on efficient connection: # of nodes = 63

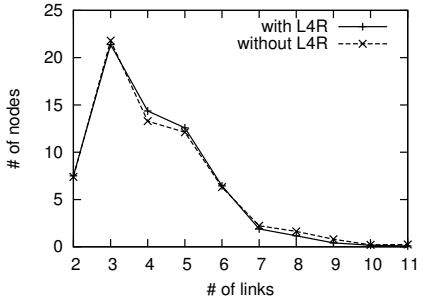


Fig. 22. Link distribution on loose connection: # of nodes = 66

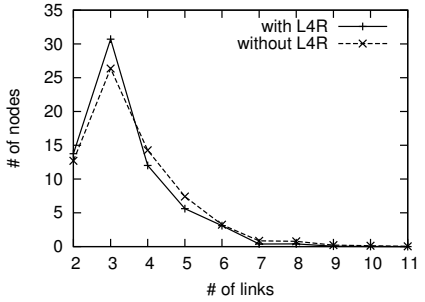


Fig. 23. Link distribution on efficient connection: # of nodes = 66

VI. Conclusion

Networked Systems (NS) are usually integrated by various pieces of network equipment, and its security has been recently become significant. However, at present, there is no NS integration methodology or theory. Although many previous studies on networking and design, including security aspects, have been conducted, these studies focused on single functions of equipment, even though the NS includes several pieces of network equipment.

In this paper, we propose a new NS expression model that enables several pieces of network equipment without loss of its characteristics, toward the establishment of a secure NS integration methodology.

We presented several algorithms to analyze the characteristics of the NS expressed by the proposed model. The results of analysis show similar shapes of link distributions. The results suggest that an effective connection algorithm for access control makes the distribution of links equivalent, regardless of the module component.

Further studies should be conducted to find the parameters of the function for its distribution, to analyze the NS from other points of view, such as throughput or potential damage by vulnerabilities, and to find an optimum NS integration algorithm.

References

[HST05] A. Hayrapetyan, C. Swamy, E. Tardos: Network Design for Information Networks. Proc. of 16th annual ACM-SIAM symposium on Descrete Algorithms, 933-942 (2005)

[SSK06] N. Sadagopan, M. Singh, B. Krishnamachari: Decentralized Utility-based Sensor Network Design. Mobile Networks and Applications 11, 341-350 (2006)

[Chekuri07] C. Chekuri: Routing and Network Design with Robustness to Changing or Uncertain Traffic Demands. ASM SIGACT News, 106-129 (2007)

[LNSS07] L.C. Lau, J. Naor, M. R. Salavatipour, M. Singh: Survivable Network Design with Degree or Order Constraints. STOC'07, (2007)

[Wolf07] T. Wolf: Design of a Network Architecture with Inherent Data Path Security. ANCS'07 (2007)

Akira Kanaoka He received B.S. and M.S. in information science from Toho University in 1998 and 2001 respectively. He received Ph.D in computer science from University of Tsukuba in 2004. He worked for SECOM Co., Ltd. since 2004. From 2007 he worked as a postdoctoral fellow at University of Tsukuba. He is working as an assistant professor at University of Tsukuba. His research interests are network security and electronic authentication.

Masahioko Kato recieved the B.Sc. and M.Sc. degrees in engneering from Toyohashi University of Technology in 1993 and 1995, respectively. He is now working at IIJ Technology since 1998. He is currently interested in security of network system.

Nobukatsu Todo He received B.S degree from University of Tsukuba in 2007. Currently, he is a master course student of the graduate school of systems and information engineering in University of Tsukuba. His current research interest is network security.

Eiji Okamoto Professor Eiji Okamoto received his B.S., M.S. and Ph.D degrees in electronics engineering from the Tokyo Institute of Technology in 1973, 1975 and 1978, respectively. He worked and studied communication theory and cryptography for NEC central research laboratories since 1978. From 1991 he became a professor at Japan Advanced Institute of Science and Technology, then at Toho University. Now he is a professor at Graduate School of Systems and Information Engineering, University of Tsukuba. His research interests are cryptography and information security. He is a member of IEEE and a coeditor-in-chief of International Journal of Information Security.

