Dynamic Routing with Security Considerations

Chin-Fu Kuo, *Member*, *IEEE*, Ai-Chun Pang, *Member*, *IEEE*, and Sheng-Kun Chan

Abstract—Security has become one of the major issues for data communication over wired and wireless networks. Different from the past work on the designs of cryptography algorithms and system infrastructures, we will propose a dynamic routing algorithm that could randomize delivery paths for data transmission. The algorithm is easy to implement and compatible with popular routing protocols, such as the Routing Information Protocol in wired networks and Destination-Sequenced Distance Vector protocol in wireless networks, without introducing extra control messages. An analytic study on the proposed algorithm is presented, and a series of simulation experiments are conducted to verify the analytic results and to show the capability of the proposed algorithm.

Index Terms—Security-enhanced data transmission, dynamic routing, RIP, DSDV.

1 Introduction

In the past decades, various security-enhanced measures have been proposed to improve the security of data transmission over public networks. Existing work on security-enhanced data transmission includes the designs of cryptography algorithms and system infrastructures and security-enhanced routing methods. Their common objectives are often to defeat various threats over the Internet, including eavesdropping, spoofing, session hijacking, etc.

Among many well-known designs for cryptography-based systems, the IP Security (IPSec) [23] and the Secure Socket Layer (SSL) [21] are popularly supported and implemented in many systems and platforms. Although IPSec and SSL do greatly improve the security level for data transmission, they unavoidably introduce substantial overheads [1], [7], [13], especially on gateway/host performance and effective network bandwidth. For example, the data transmission overhead is 5 cycles/byte over an Intel Pentium II with the Linux IP stack alone, and the overhead increases to 58 cycles/byte when Advanced Encryption Standard (AES) [10] is adopted for encryption/decryption for IPSec [7].

Another alternative for security-enhanced data transmission is to dynamically route packets between each source and its destination so that the chance for system break-in, due to successful interception of consecutive packets for a session, is slim. The intention of security-enhanced routing is different from the adopting of multiple paths between a source and a destination to increase the throughput of data transmission (see, e.g., [8] and [9]). In particular, Lou et al. [14], [15] proposed a secure routing protocol to improve the security of end-to-end data transmission based on multiple-path deliveries. The set of multiple paths between each source and its destination is determined in an online fashion, and extra control message exchanging is needed. Bohacek et al. [2] proposed a secure stochastic routing mechanism to improve routing security. Similar to the work proposed by Lou et al. [14], [15], a set of paths is discovered for each source and its destination in an online fashion based on message flooding. Thus, a mass of control messages is needed. Yang and Papavassiliou [25] explored the trading of the security level and the traffic dispersion. They proposed a traffic dispersion scheme to reduce the probability of eavesdropped information along the used paths provided that the set of data delivery paths is discovered in advance. Although excellent research results have been proposed for security-enhanced dynamic routing, many of them rely on the discovery of multiple paths either in an online or offline fashion. For those online path-searching approaches, the discovery of multiple paths involves a significant number of control signals over the Internet. On the other hand, the discovery of paths in an offline fashion might not be suitable to networks with a dynamic changing configuration. Therefore, we will propose a dynamic routing algorithm to provide security-enhanced data delivery without introducing any extra control messages.

The objective of this work is to explore a security-enhanced dynamic routing algorithm based on distributed routing information widely supported in existing wired and wireless networks. We aim at the randomization of delivery paths for data transmission to provide considerably small *path similarity* (i.e., the number of common links between two delivery paths) of two consecutive transmitted packets. The proposed algorithm should be easy to implement and compatible with popular routing protocols, such as the Routing Information Protocol (RIP) for wired networks [16] and Destination-Sequenced Distance Vector (DSDV) protocol for wireless networks [20], over existing infrastructures. These protocols shall not increase the number of control messages if the proposed algorithm is

- C.-F. Kuo is with the Department of Computer Science and Information Engineering, National University of Kaohsiung, Taipei 106, Taiwan, R.O.C. E-mail: chinfukuo2006@nuk.edu.tw.
- A.-C. Pang is with the Graduate Institute of Networking and Multimedia, Department of Computer Science and Information Engineering, National Taiwan University, Taipei 106, Taiwan, R.O.C. E-mail: acpang@csie.ntu.edu.tw.
- S.-K. Chan is with Chunghwa Telecom (CHT) Co., Ltd. Taiwan. E-mail: r92002@csie.ntu.edu.tw.

Manuscript received 18 Mar. 2007; revised 9 Sept. 2007; accepted 22 Apr. 2008; published online 6 May 2008.
Recommended for acceptance by Y. Oruc.
For information on obtaining reprints of this article, please send e-mail to: tpds@computer.org, and reference IEEECS Log Number TPDS-2007-03-0089.
Digital Object Identifier no. 10.1109/TPDS.2008.73.

1045-9219/09/$25.00 © 2009 IEEE Published by the IEEE Computer Society

adopted. An analytic study will be presented for the proposed routing algorithm, and a series of simulation study will be conducted to verify the analytic results and to show the capability of the proposed algorithm.

The rest of this paper is organized as follows: Section 2 formally defines the problem under investigation. In Section 3, we propose a security-enhanced dynamic routing algorithm to randomize the data delivery paths. An analytic study on the proposed algorithm is conducted. Section 4 summarizes our experimental results to demonstrate the capability of the proposed algorithm. Section 5 is the conclusion.

2 Problem Statement

The objective of this work is to explore a security-enhanced dynamic routing algorithm based on distributed routing information widely supported in existing networks. In general, routing protocols over networks could be classified roughly into two kinds: distance-vector algorithms and link-state algorithms [11]. Distance-vector algorithms rely on the exchanging of distance information among neighboring nodes for the seeking of routing paths. Examples of distance-vector-based routing algorithms include RIP and DSDV. Link-state algorithms used in the Open Shortest Path First protocol [19] are for global routing in which the network topology is known by all nodes. Our goal is to propose a distance-vector-based algorithm for dynamic routing to improve the security of data transmission. Before we proceed with further discussions, our problem and system model shall be defined.

A network could be modeled as a graph $G = (N, L)$, where N is a set of routers (also referred to as nodes) in the network, and L is a set of links that connect adjacent routers in the network. A path p from a node s (referred to as a *source node*) to another node t (referred to as a *destination node*) is a set of links $(N_1, N_2)(N_2, N_3) \cdots (N_i, N_{i+1})$, where $s = N_1$, $N_{i+1} = t$, $N_j \in N$, and $(N_j, N_{j+1}) \in L$ for $1 \leq j \leq i$. Let $P_{s,t}$ denote the set of all potential paths between a source node s and a destination node t. Note that the number of paths in $P_{s,t}$ could be an exponential function of the number of routers in the network, and we should not derive $P_{s,t}$ in practice for routing or analysis.

Definition 1 (path similarity). *Given two paths p_i and p_j, the path similarity $\mathrm{Sim}(p_i, p_j)$ for p_i and p_j is defined as the number of common links between p_i and p_j:*

$$\mathrm{Sim}(p_i, p_j) = \left|\left\{(N_x, N_y) | (N_x, N_y) \in p_i \wedge (N_x, N_y) \in p_j\right\}\right|,$$

where N_x and N_y are two nodes in the network.

The path similarity between two paths is computed based on the algorithm of Levenshtein distance [12].

Definition 2 (the expected value of path similarity for any two consecutive delivered packets). *Given a source node s and a destination node t, the expected value of path similarity of any two consecutive delivered packets is defined as follows:*

$$E[\mathrm{Sim}_{s,t}] = \sum_{\forall p_i, p_j \in P_{s,t}} \mathrm{Sim}(p_i, p_j) \cdot \mathrm{Prob}(p_j | p_i) \cdot \mathrm{Prob}(p_i),$$

where $P_{s,t}$ is the set of all possible transmission paths between a source node s and a destination node t. $\mathrm{Prob}(p_j|p_i)$ is the conditional probability of using p_j for delivering the current packet, given that p_i is used for the previous packet. $\mathrm{Prob}(p_i)$ is the probability of using p_i for delivering the previous packet.

The purpose of this research is to propose a dynamic routing algorithm to improve the security of data transmission. We define the *eavesdropping avoidance problem* as follows:

Given a graph for a network under discussion, a source node, and a destination node, the problem is to minimize the path similarity without introducing any extra control messages, and thus to reduce the probability of eavesdropping consecutive packets over a specific link.

3 Security-Enhanced Dynamic Routing

3.1 Notations and Data Structures

The objective of this section is to propose a distance-vector-based algorithm for dynamic routing to improve the security of data transmission. We propose to rely on existing distance information exchanged among neighboring nodes (referred to as routers as well in this paper) for the seeking of routing paths. In many distance-vector-based implementations, e.g., those based on RIP, each node N_i maintains a *routing table* (see Table 1a) in which each entry is associated with a tuple $(t, W_{N_i,t}, Nexthop)$, where t, $W_{N_i,t}$, and $Nexthop$ denote some unique destination node, an estimated minimal cost to send a packet to t, and the next node along the minimal-cost path to the destination node, respectively.

With the objective of this work in the randomization of routing paths, the routing table shown in Table 1a is extended to accommodate our security-enhanced dynamic routing algorithm. In the extended routing table (see Table 1b), we propose to associate each entry with a tuple $(t, W_{N_i,t}, C_t^{N_i}, H_t^{N_i})$. $C_t^{N_i}$ is a set of *node candidates* for the nexthop (note that the candidate selection will be elaborated in Procedure 2 of Section 3.2), where one of the nexthop candidates that have the minimal cost is marked. $H_t^{N_i}$, a set of tuples, records the history for packet deliveries through the node N_i to the destination node t. Each tuple (N_j, h_{N_j}) in $H_t^{N_i}$ is used to represent that N_i previously used the node h_{N_j} as the nexthop to forward the packet from the source node N_j to the destination node t. Let Nbr_i and w_{N_i,N_j} denote the set of neighboring nodes for a node N_i and the cost in the delivery of a packet between N_i and a neighboring node N_j, respectively. Each node N_i also maintains an array (referred to as a *link table*) in which each entry corresponds to a neighboring node $N_j \in \mathrm{Nbr}_i$ and contains the cost w_{N_i,N_j} for a packet delivery.

The proposed algorithm achieves considerably small path similarity for packet deliveries between a source node and the corresponding destination node. However, the total space requirement would increase to store some extra routing information. The size of a routing table depends on the topology and the node number of a network under discussions. In the worst case, we have a fully connected network. For each entry in the routing table shown in Table 1b, the

TABLE 1
An Example of the Routing Table for the Node N_i

Destination Node (t)	Cost ($W_{N_i,t}$)	Nexthop
N_1	7	N_6
N_2	8	N_{21}
N_3	9	N_9
$\vdots$	$\vdots$	$\vdots$

(a)

Destination Node (t)	Cost ($W_{N_i,t}$)	Nexthop Candidates ($C_t^{N_i}$)	History Record for Packet Deliveries to the Destination Node t ($H_t^{N_i}$)
N_1	7	$\{\hat{N_6}, N_{20}, N_{21}\}$	$\{(N_2, N_{21}), (N_3, N_6), \cdots, (N_{31}, N_{20})\}$
N_2	8	$\{N_9, \hat{N_{21}}\}$	$\{(N_1, N_9), (N_3, N_9), \cdots, (N_{31}, N_{21})\}$
N_3	9	$\{\hat{N_9}\}$	$\{(N_1, N_9), (N_2, N_9), \cdots, (N_{31}, N_9)\}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

(b)

(a) The routing table for the original distance-vector-based routing algorithm. (b) The routing table for the proposed security-enhanced routing algorithm.

additional spaces required for recording the set of node candidates (as shown in the third column of Table 1b) and for recording the routing history (as shown in the fourth column of Table 1b) are $O(|N|)$. Because there are $|N|$ destination nodes at most in each routing table, the additionally required spaces for the entire routing table for one node are $O(|N|^2)$. Since the provided distributed dynamic routing algorithm (DDRA) is a distance-vector-based routing protocol for intradomain systems, the number of nodes is limited, and the network topology is hardly fully connected. Hence, the increase of the total space requirement is considerably small. However, the impact of the space requirement on the search time will be analyzed in the following section.

3.2 A Distributed Dynamic Routing Algorithm

The DDRA proposed in this paper consists of two parts: 1) a randomization process for packet deliveries and 2) maintenance of the extended routing table.

3.2.1 Randomization Process

Consider the delivery of a packet with the destination t at a node N_i. In order to minimize the probability that packets are eavesdropped over a specific link, a *randomization process* for packet deliveries shown in Procedure 1 is adopted. In this process, the previous nexthop h_s (defined in $H_t^{N_i}$ of Table 1b) for the source node s is identified in the first step of the process (line 1). Then, the process randomly pick up a neighboring node in $C_t^{N_i}$ excluding h_s as the nexthop for the current packet transmission. The exclusion of h_s for the nexthop selection avoids transmitting two consecutive packets in the same link, and the randomized pickup prevents attackers from easily predicting routing paths for the coming transmitted packets.

Procedure 1 RANDOMIZEDSELECTOR (s, t, pkt)

```
 1: Let $h_s$ be the used nexthop for the previous packet
    delivery for the source node $s$.
 2: if $h_s \in C_t^{N_i}$ then
 3:     if $|C_t^{N_i}| > 1$ then
 4:         Randomly choose a node $x$ from $\{C_t^{N_i} - h_s\}$ as a
            nexthop, and send the packet $pkt$ to the node $x$.
 5:         $h_s \leftarrow x$, and update the routing table of $N_i$.
 6:     else
 7:         Send the packet $pkt$ to $h_s$.
 8:     end if
 9: else
10:     Randomly choose a node $y$ from $C_t^{N_i}$ as a nexthop,
        and send the packet $pkt$ to the node $y$.
11:     $h_s \leftarrow y$, and update the routing table of $N_i$.
12: end if
```

The number of entries in the history record for packet deliveries to destination nodes is $|N|$ in the worst case. In order to efficiently look up the history record for a destination node, we maintain the history record for each node in a hash table. Before the current packet is sent to its destination node, we must randomly pick up a neighboring node excluding the used node for the previous packet. Once a neighboring node is selected, by the hash table, we need $O(1)$ to determine whether the selected neighboring node for the current packet is the same as the one used by the previous packet. Therefore, the time complexity of searching a proper neighboring node is $O(1)$.

3.2.2 Routing Table Maintenance

Let every node in the network be given a routing table and a link table. We assume that the link table of each node is constructed by an existing link discovery protocol, such as the *Hello* protocol in [18]. On the other hand, the construction and maintenance of routing tables are revised based on the well-known Bellman-Ford algorithm [4] and described as follows:

Initially, the routing table of each node (e.g., the node N_i) consists of entries $\{(N_j, W_{N_i,N_j}, C_{N_j}^{N_i} = \{N_j\}, H_{N_j}^{N_i} = \emptyset)\}$, where $N_j \in \mathrm{Nbr}_i$ and $W_{N_i,N_j} = w_{N_i,N_j}$. By exchanging distance vectors between neighboring nodes, the routing table of N_i is accordingly updated. Note that the exchanging for distance vectors among neighboring nodes can be based on a predefined interval. The exchanging can also be triggered by the change of link cost or the failure of the link/node. In this paper, we consider cases when N_i receives a distance vector from a neighboring node N_j. Each element of a distance vector received from a neighboring node N_j includes a destination node t and a delivery cost $W_{N_j,t}$ from the node N_j to the destination node t. The algorithm for the maintenance of the routing table of N_i is shown in Procedure 2, and will be described below.

```
Procedure 2 DVPROCESS($t, W_{N_j,t}$)
 1: if the destination node $t$ is not in the routing table then
 2:   Add the entry $(t, (w_{N_i,N_j}+W_{N_j,t}), C_t^{N_i}=\{N_j\}, H_t^{N_i}=\emptyset)$.
 3: else if $(w_{N_i,N_j} + W_{N_j,t}) < W_{N_i,t}$ then
 4:   $C_t^{N_i} \leftarrow \{N_j\}$ and $N_j$ is marked as the minimal-cost
      nexthop.
 5:   $W_{N_i,t} \leftarrow (w_{N_i,N_j} + W_{N_j,t})$
 6:   for each node $N_k \in \mathrm{Nbr}_i$ except $N_j$ do
 7:     if $W_{N_k,t} < W_{N_i,t}$ then
 8:       $C_t^{N_i} \leftarrow C_t^{N_i} \cup \{N_k\}$
 9:     end if
10:   end for
11:   Send $(t, W_{N_i,t})$ to each neighboring node $N_k \in \mathrm{Nbr}_i$.
12: else if $(w_{N_i,N_j} + W_{N_j,t}) > W_{N_i,t}$ then
13:   if $(N_j \in C_t^{N_i})$ then
14:     if $N_j$ was marked as the minimal-cost nexthop then
15:       $W_{N_i,t} \leftarrow \mathrm{MIN}_{N_k \in \mathrm{Nbr}_i}(w_{N_i,N_k} + W_{N_k,t})$
16:       $C_t^{N_i} \leftarrow \emptyset$
17:       for each node $N_k \in \mathrm{Nbr}_i$ do
18:         if $W_{N_k,t} < W_{N_i,t}$ then
19:           $C_t^{N_i} \leftarrow C_t^{N_i} \cup \{N_k\}$
20:         end if
21:       end for
22:       Send $(t, W_{N_i,t})$ to each neighboring node $N_k \in \mathrm{Nbr}_i$.
23:     else if $W_{N_j,t} > W_{N_i,t}$ then
24:       $C_t^{N_i} \leftarrow C_t^{N_i} - \{N_j\}$
25:     end if
26:   else if $(N_j \notin C_t^{N_i}) \wedge (W_{N_j,t} < W_{N_i,t})$ then
27:     $C_t^{N_i} \leftarrow C_t^{N_i} \cup \{N_j\}$
28:   end if
29: end if
```

First, for the elements that do not exist in the routing table, new entries for the corresponding destination nodes will be inserted (lines 1 and 2). Otherwise, $w_{N_i,N_j} + W_{N_j,t}$ is compared with $W_{N_i,t}$ saved in the routing table of N_i, and the following four cases are considered:

1. $(w_{N_i,N_j} + W_{N_j,t}) < W_{N_i,t}$ (lines 3-11). The corresponding minimal cost is updated in the routing table, and N_j is marked as the minimal-cost nexthop. Any neighboring node N_k which has an estimated packet delivery cost from N_k to t (i.e., $W_{N_k,t}$) no more than $(w_{N_i,N_j} + W_{N_j,t})$ joins the candidate set $C_t^{N_i}$. It is to aggressively include more candidates for the nexthop to t with reasonable packet delivery cost (i.e., $W_{N_k,t} < W_{N_i,t}$). Compared to the Bellman-Ford algorithm, more than one neighboring node can be selected as the nexthop candidates in this step (lines 6-10) to accommodate multiple packet-delivery paths to the destination node t. Also, the selection policy described above can prevent the algorithm from generating the routing loops, and the proof will be shown in Theorem 1.
2. $(w_{N_i,N_j} + W_{N_j,t}) > W_{N_i,t}$, and N_j is in the set $C_t^{N_i}$ of nexthop candidates (lines 13-25). Based on whether N_j is marked as the minimal-cost nexthop in the routing table of N_i, the following two cases are further considered.
   - N_j was marked as the minimal-cost nexthop (lines 14-22). For all neighboring nodes of N_i, the minimal cost to the destination node t is recomputed according to the distance vectors received from the neighboring nodes. Also, the nexthop candidates for the destination node t are reselected, and the selection policy is the same as lines 7-9 for Case 1.
   - N_j was not marked as the minimal-cost nexthop (lines 23 and 24). If $W_{N_j,t} > W_{N_i,t}$, N_j is removed from $C_t^{N_i}$.
3. $(w_{N_i,N_j} + W_{N_j,t}) > W_{N_i,t}$, and N_j is not in the set $C_t^{N_i}$ of nexthop candidates (lines 26 and 27). If $W_{N_j,t} < W_{N_i,t}$, N_j is inserted into $C_t^{N_i}$.
4. Otherwise, nothing is done.

When a node N_i receives a distance vector from a neighboring node, Procedure 2 is used to maintain the nexthop candidates for each entry in the routing table of N_i. The time complexity of Procedure 2 maintaining the nexthop candidates is $O(|N|)$. Furthermore, in the routing table of N_i, there are $|N|$ entries in the worst case. Hence, the time complexity of maintaining the routing table is $O(|N|^2)$.

Based on Procedures 1 and 2, our security-enhanced dynamic routing can be achieved without modifying the existing distance-vector-based routing protocols such as RIP and DSDV. Also, the properties for the proposed algorithms are summarized as follows:

Theorem 1. *The proposed algorithm would not result in any routing loop during the run time, given a fixed routing table for each router.*

Proof. It can be proven by contradiction. Given any source-destination pair (s, t), consider the set $P_{s,t}$ of possible paths for packet deliveries. Suppose that a path $p \in P_{s,t}$ with a loop $(N_1, N_2)(N_2, N_3) \cdots (N_{k-1}, N_k)(N_k, N_1)$ could be resulted, where k is a positive integer, and routers are renumbered for the simplicity of presentation. As a result, we have $N_2 \in C_t^{N_1}, N_3 \in C_t^{N_2}, \ldots, N_k \in C_t^{N_{k-1}}$, and $N_1 \in C_t^{N_k}$. In other words, $W_{N_2,t} < W_{N_1,t}, W_{N_3,t} < W_{N_2,t}, \ldots, W_{N_k,t} < W_{N_{k-1},t}$, and $W_{N_1,t} < W_{N_k,t}$. Thus, $W_{N_1,t} < W_{N_k,t} < W_{N_{k-1},t} < \cdots < W_{N_3,t} < W_{N_2,t} < W_{N_1,t}$. Because $W_{N_1,t}$ could not be smaller than $W_{N_1,t}$, a contradiction is found. □

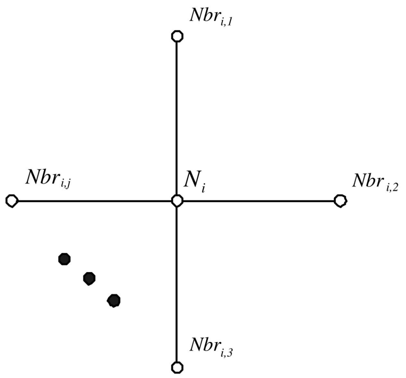


Fig. 1. Illustration of a node N_i with its neighboring nodes ($\mathrm{Nbr}_{i,1}$, $\mathrm{Nbr}_{i,2}, \ldots$, and $\mathrm{Nbr}_{i,j}$).

3.3 An Analytic Study

In this section, we propose an analytic model to analyze path similarity for our security-enhanced DDRA. The goal is to provide an analytic framework for the proposed algorithm and to quantify the "degree" of security possibly achieved.

Fig. 1 shows an illustration for the node N_i with its neighboring nodes denoted as $\mathrm{Nbr}_{i,1}, \mathrm{Nbr}_{i,2}, \ldots$, and $\mathrm{Nbr}_{i,j}$. Let t be a destination node, and the node N_i has a set $C_t^{N_i}$ of nexthop candidates and a minimal cost $M_{N_i,t}$ for the destination node t. The minimal cost $M_{N_i,t}$ can be derived as

$$M_{N_i,t} = \sum_{\forall (x,y) \in \mathrm{MCP}_t^{N_i}} w_{x,y},$$

where $\mathrm{MCP}_t^{N_i}$ is the set of all links along the minimal-cost path from the node N_i to node t. Note that $\mathrm{MCP}_t^{N_i}$ can be derived by a single-source shortest path algorithm, such as the Dijkstra's algorithm [4].

Since the neighboring nodes of N_i whose minimal delivery costs to the destination node t are less than $M_{N_i,t}$ will be included in $C_t^{N_i}$, $C_t^{N_i}$ can be defined as

$$C_t^{N_i} = \{N_j | M_{N_j,t} < M_{N_i,t} \quad \text{and} \quad N_j \in Nbr_i\}.$$

Let $P_{s,t}$ denote a path set containing all possible delivery paths from a source node s to a destination node t. Let p, a sequence of links $(s, N_2)(N_2, N_3) \cdots (N_m, t)$, denote one of the paths in $P_{s,t}$, where m is the number of links that the packet goes through over the path p. The probability that the path p is selected for transmitting a packet from the source s to the destination t can be derived as follows:

$$\mathrm{Prob}(p) = \frac{1}{|C_t^s|} \times \frac{1}{|C_t^{N_2}|} \times \frac{1}{|C_t^{N_3}|} \times \cdots \times \frac{1}{|C_t^{N_m}|}.$$

Based on Definition 2 in Section 2, the expected value $E[\mathrm{Sim}_{s,t}]$ of path set $P_{s,t}$ can be

$$E[\mathrm{Sim}_{s,t}] = \sum_{\forall p_i, p_j \in P_{s,t}} \big(\mathrm{Sim}(p_i, p_j) \cdot \mathrm{Prob}(p_j|p_i) \cdot \mathrm{Prob}(p_i)\big).$$

For any two paths p_i and p_j in $P_{s,t}$, the derivation of $\mathrm{Prob}(p_j|p_i)$ can be classified into the following three cases:

1. For each link $(N_x, N_y) \in p_j$, if $(N_x, N_y) \in p_i$, and more than one candidate exists in the nexthop set of the routing table of N_x, p_j will not be selected as the following path of p_i for delivering the packets from the source s to the destination t. Then, we have $\mathrm{Prob}(p_j|p_i) = 0$.
2. For each link $(N_x, N_y) \in p_j$ where $|C_t^{N_x}| > 1$, if (N_x, N_y) is not in p_i and there exists a link (N_x, N_z) such that $(N_x, N_z) \in p_i$ and $N_z \in C_t^{N_x}$, then the probability that N_y will be selected as the nexthop of N_x for the path p_j is $\frac{1}{|C_t^{N_x}|-1}$.
3. Otherwise, $\mathrm{Prob}(p_j|p_i) = \frac{1}{|C_t^{N_x}|}$. It occurs when the path p_i does not go through the node N_x or when $|C_t^{N_x}| = 1$.

Based on the above discussions, we have

$$\mathrm{Prob}(p_j|p_i) = \prod_{\forall (N_x,N_y) \in p_j} \begin{cases} 0, & \text{if } |C_t^{N_x}| > 1 \text{ and } (N_x, N_y) \in p_i, \\ \frac{1}{|C_t^{N_x}|-1}, & \text{if } |C_t^{N_x}| > 1 \text{ and } \exists (N_x, N_z) \in p_i, \\ & \text{such that } N_z \in C_t^{N_x} \text{ and } N_z \neq N_y, \\ \frac{1}{|C_t^{N_x}|}, & \text{otherwise.} \end{cases}$$

Note that if the previously selected nexthop is not recorded in Procedure 1, the adoptions of the paths p_i and p_j are independent, and $\mathrm{Prob}(p_j|p_i)$ equals to $\mathrm{Prob}(p_j)$.

Furthermore, let PS_l be a source-destination pair set that includes all delivery paths from some source node s to some destination node t, and all included source-destination pairs have the minimal-cost path length l. Then, the average value $\overline{E[Sim_{PS_l}]}$ of $E[\mathrm{Sim}_{s,t}]$ for all source-destination pairs (s, t) in PS_l can be derived as follows:

$$\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]} = \frac{1}{|\mathrm{PS}_l|} \cdot \sum_{\forall (s,t) \in \mathrm{PS}_l} E[\mathrm{Sim}_{s,t}],$$

where $|\mathrm{PS}_l|$ is the number of source-destination pairs in PS_l, and (s, t) is a source-destination pair.

By using $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$, the "degree" of security for different kinds of routing protocols can be quantified. The above analytic model can be applied to any network topology, and the mathematical analysis for $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$ has been validated against the simulation experiments, which will be shown in Section 4. Also, we shall show that in the experiments, the proposed algorithm greatly outperforms the existing routing algorithms in terms of $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$.

3.4 Implementation Remarks

The original cost-assignment strategy of RIP assigns an equal cost value (i.e., 1) to each link. If the proposed algorithm is implemented over RIP with equal cost links, then the resulted path set would be the same as that generated by an equal-cost multipath protocol based on RIP (which maintains more than one nexthop if they all have the minimal cost). However, links could have different costs in practice. For example, the default cost value of a link (N_i, N_j) in OSPF could be derived as follows:

$$\mathrm{OSPF\_Cost}_{(N_i,N_j)} = \frac{10^8}{\mathrm{Interface\_Speed\_in\_bps}},$$

where Interface_Speed_in_bps is the minimal bandwidth of the connected interfaces between N_i and N_j. The setting for the link-cost value in another popular distance-vector-based routing protocol, Enhanced Interior Gateway Routing

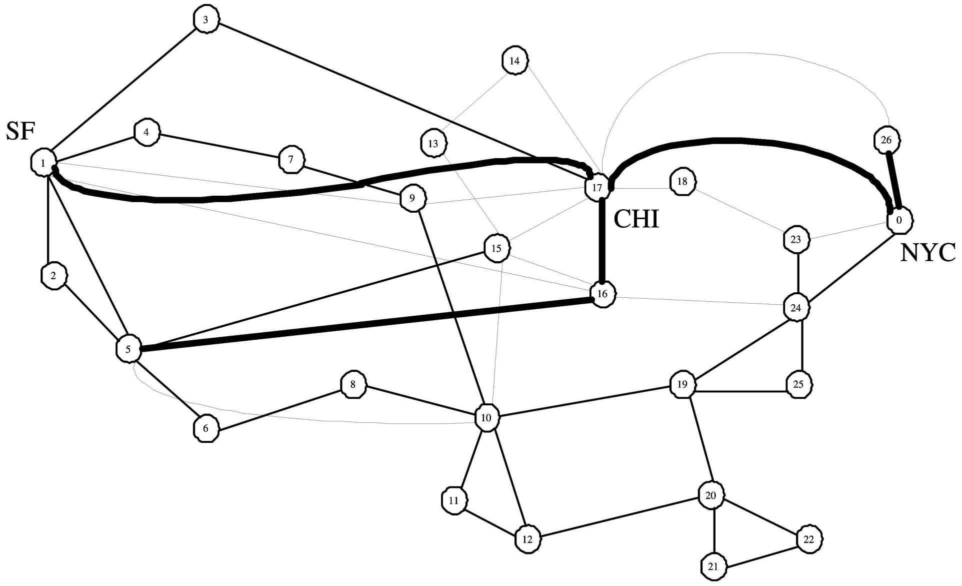


Fig. 2. AT&T US topology.

Protocol, can be found in [22], and the details are omitted. We shall show that, in the experiments, an equal-cost link strategy could have a more average on the path similarity.

4 Performance Evaluation

The purpose of this section is to evaluate the performance of the proposed algorithm, referred to as the DDRA. A simulation model is constructed to investigate the performance of the proposed methodology with the ns-2 network simulator [24]. In the simulation model, the AT&T US topology and DANTE Europe topology shown in Figs. 2 and 3 for backbone networks are used [17]. Note that with the self-similar characteristic for Internet topologies [6], the behavior for backbone networks could be applied to that for corporate/enterprise networks. In addition to AT&T US and DANTE topologies, we generate some random topologies based on random graphs [5] for the experiments. A random graph is a graph with a fixed set of vertices, and a link between any two nodes occurs with a given probability. In our experiments, the numbers of nodes in the random topologies are 40, 50, and 60. The link probabilities are 0.1, 0.2, 0.3, and 0.4.

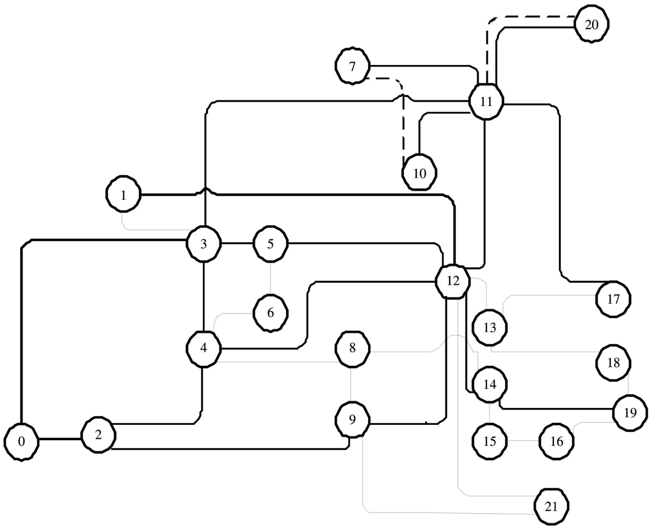


Fig. 3. DANTE Europe topology.

We compare the performance of DDRA with the popular Shortest-Path Routing Algorithm (SPRA) and the Equal-Cost Routing Algorithm (ECRA) used in RIP. In SPRA, only one path with the minimal cost is derived for each source-destination pair. On the other hand, more than one path can be accommodated in ECRA if their delivery costs are the same as that of the minimal-cost path. Note that in the remainder of this section, we use "DDRA_with_RandomizedSelector" to represent the situation where both Procedures 1 and 2 are used, and "DDRA_without_RandomizedSelector" to denote the situation where only Procedure 2 is adopted. Though multipath routing protocols, e.g., [14] and [15], could also provide multiple paths for source-destination pairs, the control messages of the online multipath routing protocols will be significantly increased. Also, the offline multipath routing protocols cannot reflect the changing of the topology. Therefore, the multipath routing protocols will not be compared with our distance-vector-based dynamic routing algorithm.

The primary performance metric is the average value $\overline{E[Sim_{PS_l}]}$ of path similarity for all source-destination pairs in PS_l. The values of $\overline{E[Sim_{PS_l}]}$ is calculated by the following procedure: For each source-destination pair with the length of the minimal-cost path equal to l, a considerable number of packets are transmitted from the source node to the corresponding destination node. The average path similarity of the source-destination pair is calculated by summing the path similarity of each two consecutive packets divided by the packet number minus 1. The same operation is done for the rest of source-destination pairs. Finally, the value of $\overline{E[Sim_{PS_l}]}$ can be obtained by averaging the path similarity of all source-destination pairs with the length l of minimal-cost paths.

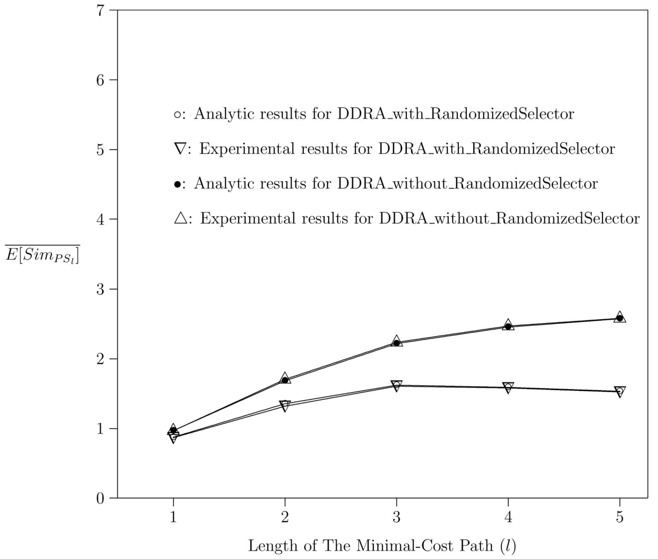


Fig. 4. Analytic and experimental results of $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$ for AT&T US topology.

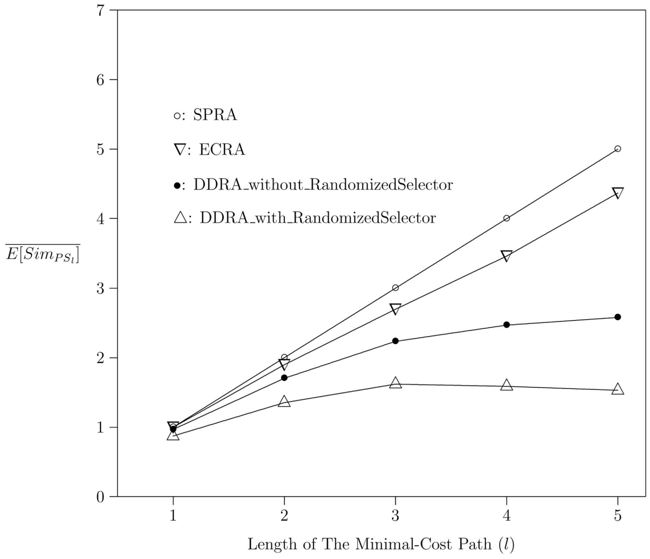


Fig. 5. $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$ for AT&T US topology.

In the AT&T US topology, the cost of each link is set as 1 or 4, depending on the bandwidth of each link. The bold lines in Fig. 2 represent the links with 9.6-Gbps bandwidth. The bandwidth of any other links is equal to 2.4 Gbps. In Fig. 3, three costs (1, 2, and 4) are set for links in the DANTE Europe topology. The bold lines and the dash lines represent the links with 10-Gbps bandwidth and with 5-Gbps bandwidth, respectively. For any other links in Fig. 3, the bandwidth is equal to 2.5-Gbps bandwidth. In the random topologies, the cost of each link is uniformly set from 1 to 5 with the bandwidth values (10, 8, 6, 4, and 2) Gbps, respectively. The simulated traffic is constant bit rate (CBR) over User Datagram Protocol (UDP). The interval time of CBR is 10 ms and the packet size is 1,000 bytes. The simulation time is set to 100 seconds. In addition to path similarity, the performance of the proposed algorithm will be further investigated in terms of average single-trip time (i.e., end-to-end delay) and interpacket jitter (the definition of jitter will be described in the following section) caused by the varying delays resulting from our multipath packet deliveries.

In order to investigate the effect of traffic load on throughput for our proposed DDRA, the traffic is also generated based on variable-bit-rate applications such as file transfers over Transmission Control Protocol (TCP). The average packet size is 1,000 bytes, and source-destination pairs are chosen randomly with uniform probabilities.

4.1 Effect of l on $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$

The purposes of this section are to verify the correctness of the analytic study and to compare the performance of DDRA, ECRA, and SPRA for AT&T US topology and DANTE Europe topology.

Fig. 4 shows the analytic results of $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$ derived by the analytic study in Section 3.3 and its experimental results by simulating the proposed algorithm over ns-2. The x-axis is for the length l of the minimal-cost path for source-destination pairs, and the y-axis is for $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$. From this figure, the analytic results match the experimental results pretty well, which indicates that our mathematical analysis is validated against the simulation experiment.

Fig. 5 shows the experimental results of $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$ for DDRA_with_RandomizedSelector, DDRA_without_RandomizedSelector, ECRA, and SPRA under the AT&T topology. From this figure, we observe that our DDRA-based methodologies greatly outperform SPRA and ECRA for all l values under investigation,[1] which indicates that our DDRA provides larger path variation and, thus, more secure packet routing. Also, the $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$ values for SPRA, ECRA, and DDRA_without_RandomizedSelector increase as l increases. The increasing rates for SPRA and ECRA are much larger than those for DDRA_without_RandomizedSelector especially when l is large. Specifically, the $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$ value for SPRA is the same as the length of minimal-cost path because all packets always go through the minimal-cost path between source-destination pairs. On the other hand, when l increases, $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$ for DDRA_with_RandomizedSelector increases and then decreases. For all l values, the performance of DDRA_with_RandomizedSelector is better than that of DDRA_without_RandomizedSelector. The RandomizedSelector can prevent from selecting the previous nexthop for the current packet delivery and therefore avoids that consecutive packets are transmitted to the same nexthop.

Fig. 6 shows the experimental results of $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$ for the DANTE Europe topology. In this figure, a similar phenomenon as Fig. 5 is observed, i.e., the values of $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$ for our DDRA-based methodologies are smaller than those for SPRA and ECRA. Also, the $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$ values of ECRA and SPRA in this figure are much similar to those in Fig. 5. However, the performance of DDRA_with_Randomized Selector and DDRA_without_RandomizedSelector for the DANTE Europe topology is not as good as that for the AT&T US topology. The reason is that there are less nodes and links in the DANTE Europe topology than those in the AT&T US topology, which results in less path variation for our DDRA-based methodologies.

Note that in Figs. 5 and 6, we just show the experimental results for the case where the length of the minimal-cost path

[1] For the AT&T US and DANTE Europe topologies, the cases for $l \geq 5$ hardly occur and the results for these cases are not shown in the figure.

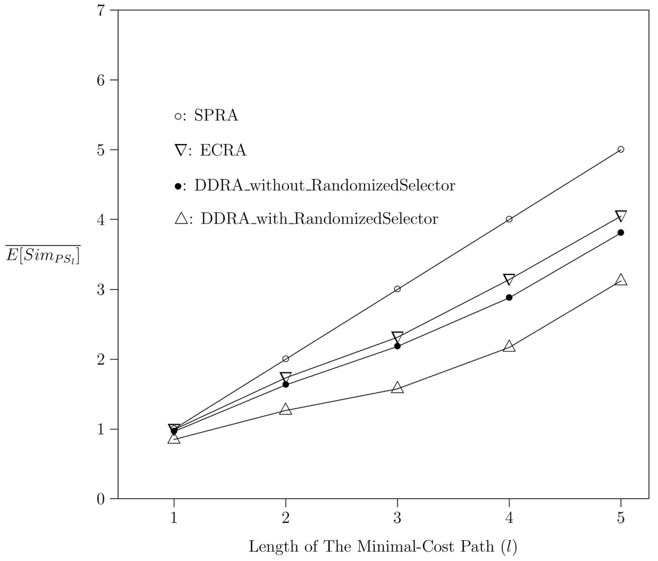


Fig. 6. $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$ for DANTE Europe topology.

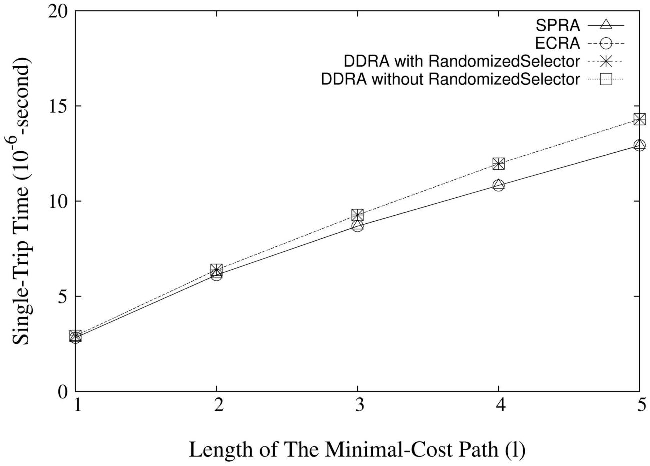


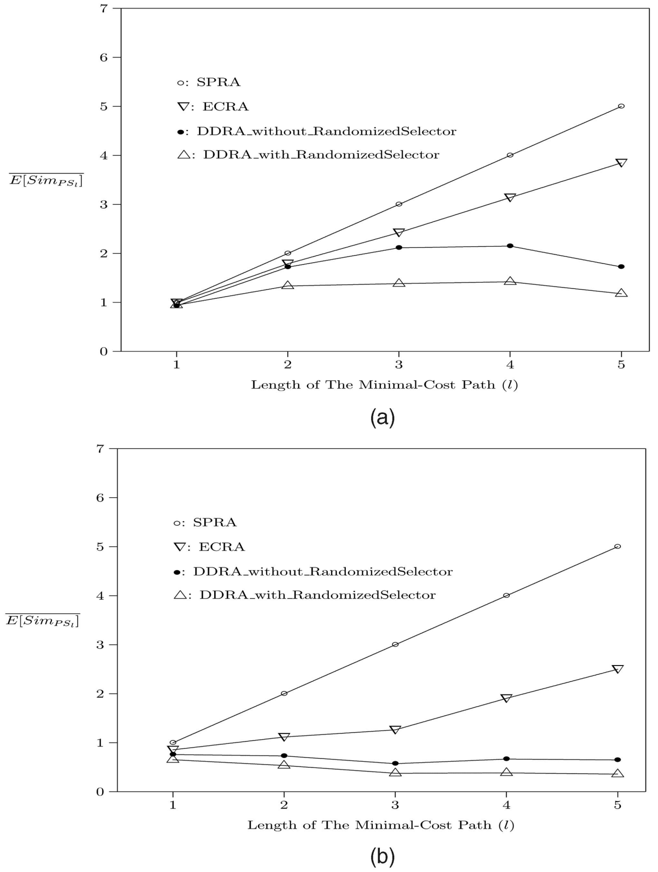
Fig. 8. Effect of l on single-trip time for AT&T US topology.

is equal or less than 5. The reason for this is as follows: First, the number of source-destination pairs with the length of minimal-cost path larger than 5 in the AT&T and DANTE Europe topologies is too few to sufficiently indicate anything. Furthermore, our dynamic routing algorithm is designed based on a distance-vector routing protocol for intradomain systems, the number of nodes is limited and, thus, the length of minimal-cost paths for source-destination pairs is bound. However, we must emphasize that when the length of the minimal-cost path is larger than 5, the trends of the curves of $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$ for DDRA_with/without_RandomizedSelector, ECRA, and SPRA are similar to those for the path length equal to or less than 5.

Fig. 7 shows the experimental results of $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$ for the random topologies where the node number $|N|$ is equal to 60. Specifically, Figs. 7a and 7b, respectively, indicate the results when the link probabilities are 0.1 and 0.4. From these figures, it is obvious that a similar phenomenon for $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$ is shown as that of Fig. 5. That is, the values of $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$ for our DDRA-based methodologies are much smaller than those for SPRA and ECRA when l is larger. For all l values, the performance of DDRA_with_RandomizedSelector is better than that of DDRA_without_RandomizedSelector. Note that the experimental results for the link probabilities 0.2 and 0.3 and for the node numbers 40 and 50 are similar to those of Figs. 7a and 7b, and are omitted in this paper.

4.2 Effect of l on Single-Trip Time and Jitter

Figs. 8 and 9 show the experimental results of the average single-trip time under the proposed DDRA, ECRA, and



(a)

(b)

Fig. 7. $\overline{E[\mathrm{Sim}_{\mathrm{PS}_l}]}$ for random topologies, where $|N| = 60$. (a) Link Probability $= 0.1$. (b) Link Probability $= 0.4$.

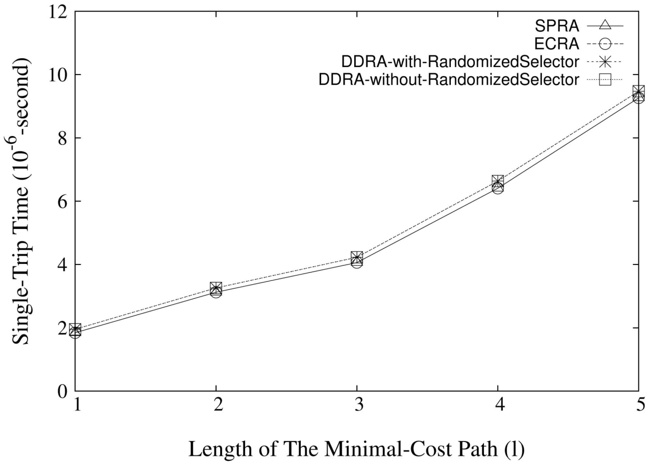


Fig. 9. Effect of l on single-trip time for DANTE Europe topology.

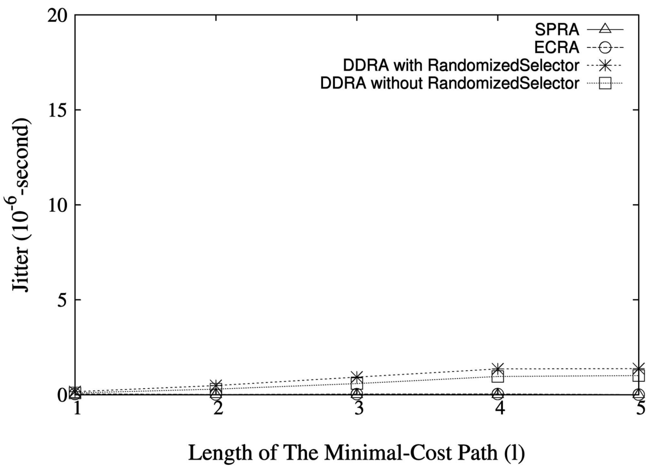


Fig. 10. Effect of l on jitter for AT&T US topology.

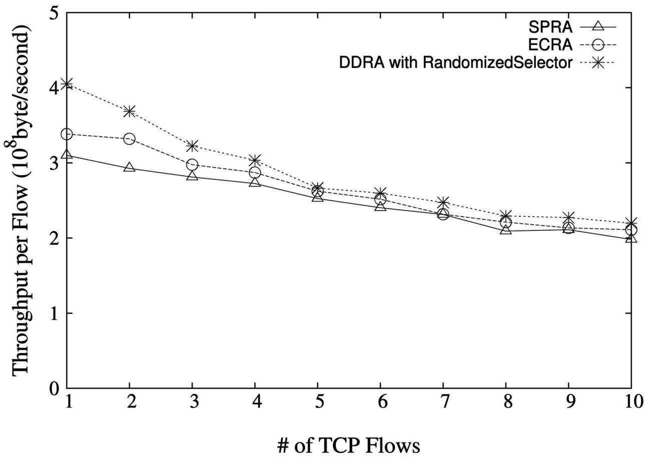


Fig. 12. Effect of traffic load on throughput for AT&T US topology.

SPRA for the AT&T US and DANTE Europe topologies, respectively. These figures indicate that the DDRA does not result in much longer single-trip-time compared with SPRA and ECRA. Furthermore, since DDRA_with_RandomizedSelector and DDRA_without_RandomizedSelector would have the same delivery-path set, the single-trip times of the DDRA-based methodologies are much similar. Also, the single-trip times for ECRA and SPRA are similar because ECRA and SPRA always send their packets through the minimal-cost paths with the same bandwidth.

For a network, "Jitter" is defined as the variation of single-trip times between the transmitted packets, and can be formulated as

$$J(i) = J(i-1) + (|D(i-1,i)| - J(i-1))/16.$$

This equation is used to calculate the jitter for cumulatively receiving i packets, where $D(i-1,i) = STT_{i-1} - STT_i$, STT_i is the single-trip time used to transmit the ith packet, and $J(0) = 0$ [3].

Based on the above equation, Figs. 10 and 11 show the experimental results of the jitters caused by our DDRA-based methodologies, SPRA and ECRA. From the figures, we observe that the jitter value of SPRA is nearly equal to zero, and ECRA has a relatively small jitter. On the other hand, the jitter values for DDRA_with_RandomizedSelector and DDRA_without_RandomizedSelector increase as the length l of the minimal-cost path increases. The reason is that the packet-delivery paths by using DDRA would be more diverse, which results in a larger jitter.

4.3 Effect of Traffic Load on Throughput

This section elaborates on the effect of traffic load on throughput for SPRA, ECRA, and our DDRA. Note that since the performance of DDRA with RandomizedSelector and without RandomizedSelector is similar in this case, the curve for DDRA_without_RandomizedSelector will not be plotted. Figs. 12 and 13 show the experimental results of the throughput under different traffic loads for DDRA_with_RandomizedSelector, ECRA, and SPRA. From these figures, we can observe that the throughput would be degraded when the number of TCP flows increases (i.e., the traffic load increases). Furthermore, for all values of traffic loads under investigation, the performance of DDRA_with_RandomizedSelector on the throughput is superior as compared with that of ECRA and SPRA. This phenomenon implies that our security-enhanced dynamic routing can provide more path variation against security

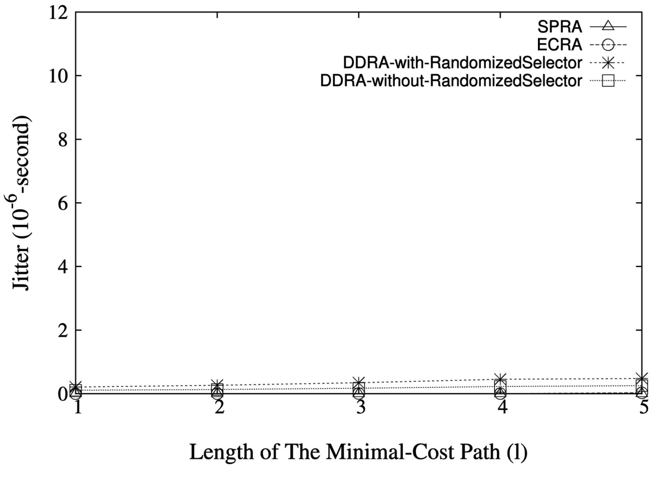


Fig. 11. Effect of l on jitter for DANTE Europe topology.

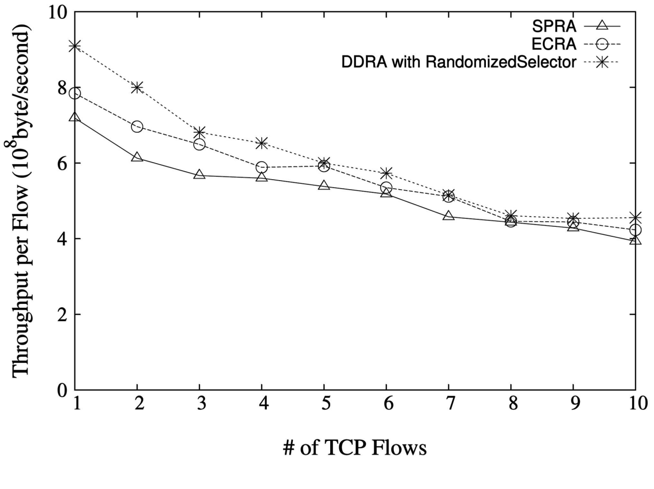


Fig. 13. Effect of traffic load on throughput for DANTE Europe topology.

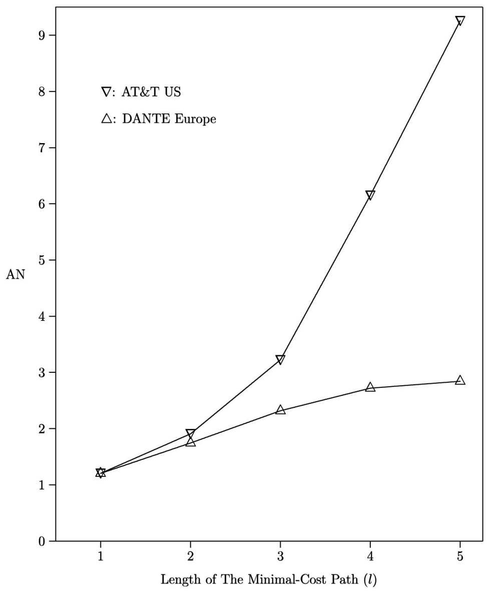


Fig. 14. Effect of l on available paths for AT&T US and DANTE Europe topologies.

threats without sacrificing the end-to-end transmission performance on the throughput.

4.4 Effect of l on Available Paths

Fig. 14 shows the impact of l on the average number (AN) of available paths for each source-destination pair in AT&T US and DANTE Europe topologies. The figure indicates that AN increases as l increases. Also, we observe that for a fixed l, there are more available paths in the AT&T US topology that those in the DANTE Europe topology. The reason is that the average number of links between the nodes in the AT&T US topology is larger than that in the DANTE Europe topology. Thus, more nexthop candidates can be selected in the AT&T US topology than in the DANTE Europe topology while packets are transmitted over the network by using our proposed security-enhanced dynamic routing algorithm.

5 Conclusion

This paper has proposed a security-enhanced dynamic routing algorithm based on distributed routing information widely supported in existing networks. The proposed algorithm is easy to implement and compatible with popular routing protocols, such as RIP and DSDV, over existing infrastructures. An analytic study was developed for the proposed algorithm and was verified against the experimental results. A series of simulation experiments were conducted to show the capability of the proposed algorithm, for which we have very encouraging results. We must point out that the proposed algorithm is completely orthogonal to the work based on the designs of cryptography algorithms and system infrastructures. Our security-enhanced dynamic routing could be used with cryptography-based system designs to further improve the security of data transmission over networks.

Acknowledgments

This work was sponsored in part by the Excellent Research Projects of National Taiwan University under Contract 95R0062-AE00-07, National Science Council under Contracts NSC96-2221-E-390-010, NSC96-2219-E-002-004, and NSC95-2221-E-002-096-MY3, Institute of Information Industry, Information and Communications Research Lab/Industrial Technology Research Institute.

References

[1] G. Apostolopoulos, V. Peris, P. Pradhan, and D. Saha, "Securing Electronic Commerce: Reducing the SSL Overhead," *IEEE Network,* 2000.

[2] S. Bohacek, J.P. Hespanha, K. Obraczka, J. Lee, and C. Lim, "Enhancing Security via Stochastic Routing," *Proc. 11th Int'l Conf. Computer Comm. and Networks (ICCCN),* 2002.

[3] D. Collins, *Carrier Grade Voice over IP.* McGraw-Hill, 2003.

[4] T.H. Cormen, C.E. Leiserson, and R.L. Rivest, *Introduction to Algorithms.* MIT Press, 1990.

[5] P. Erdös and A. Rényi, "On Random Graphs," *Publicationes Math. Debrecen,* vol. 6, 1959.

[6] M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On Power-Law Relationships of the Internet Topology," *Proc. ACM SIGCOMM '99,* pp. 251-262, 1999.

[7] *FreeS/WAN,* http://www.freeswan.org, 2008.

[8] I. Gojmerac, T. Ziegler, F. Ricciato, and P. Reichl, "Adaptive Multipath Routing for Dynamic Traffic Engineering," *Proc. IEEE Global Telecommunications Conf. (GLOBECOM),* 2003.

[9] C. Hopps, *Analysis of an Equal-Cost Multi-Path Algorithm,* Request for comments (RFC 2992), Nov. 2000.

[10] C. Kaufman, R. Perlman, and M. Speciner, *Network Security—PRIVATE Communication in a PUBLIC World,* second ed. Prentice Hall PTR, 2002.

[11] J.F. Kurose and K.W. Ross, *Computer Networking—A Top-Down Approach Featuring the Internet.* Addison Wesley, 2003.

[12] V.I. Levenshtein, "Binary Codes Capable of Correcting Deletions, Insertions, and Reversals," *Soviet Physics Doklady,* vol. 10, no. 8, pp. 707-710, 1966.

[13] S.-H. Liu, Y.-F. Lu, C.-F. Kuo, A.-C. Pang, and T.-W. Kuo, "The Performance Evaluation of a Dynamic Configuration Method over IPSEC," *Proc. 24th IEEE Real-Time Systems Symp.: Works in Progress Session (RTSS WIP),* 2003.

[14] W. Lou and Y. Fang, "A Multipath Routing Approach for Secure Data Delivery," *Proc. IEEE Military Comm. Conf. (MilCom),* 2001.

[15] W. Lou, W. Liu, and Y. Fang, "SPREAD: Improving Network Security by Multipath Routing," *Proc. IEEE Military Comm. Conf. (MilCom),* 2003.

[16] G. Malkin, *Routing Information Protocol (RIP) Version 2 Carrying Additional Information,* Request for comments (RFC 1723), Nov. 1994.

[17] *October 2004 Map Poster of the GEANT Topology,* http://www.geant.net/upload/pdf/topology_oct_2004.pdf, 2004.

[18] D.L. Mills, *DCN Local-Network Protocols,* Request for comments (RFC 891), Dec. 1983.

[19] J. Moy, *Open Shortest Path First (OSPF) Version 2,* Request for comments (RFC 1247), July 1991.

[20] C. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," *Proc. ACM SIGCOMM '94,* pp. 234-244, 1994.

[21] *Secure Sockets Layer (SSL),* http://www.openssl.org/, 2008.

[22] Cisco Systems, *White Paper: EIGRP,* Sept. 2002.

[23] R. Thayer, N. Doraswamy, and R. Glenn, *IP Security Document Roadmap,* Request for comments (RFC 2411), Nov. 1998.

[24] *The Network Simulator-ns2,* http://www.isi.edu/nsnam/ns/, 2008.

[25] J. Yang and S. Papavassiliou, "Improving Network Security by Multipath Traffic Dispersion," *Proc. IEEE Military Comm. Conf. (MilCom),* 2001.

Chin-Fu Kuo received the BS and MS degrees from National Chung Cheng University, Chiayi, Taiwan, R.O.C., in 1998 and 2000, respectively, and the PhD degree in computer science and information engineering from National Taiwan University, Taipei, in 2005. He joined the Department of Computer Science and Information Engineering (CSIE), National University of Kaohsiung (NUK), Kaohsiung, Taiwan, as an assistant professor in 2006. His research interests include real-time process scheduling, resource management, network QoS, and system security. He is a member of the IEEE.

Ai-Chun Pang received the BS, MS, and PhD degrees in computer science and information engineering from National Chiao Tung University, Hsinchu, Taiwan, in 1996, 1998, and 2002, respectively. She joined the Department of Computer Science and Information Engineering (CSIE), National Taiwan University (NTU), Taipei, as an assistant professor in 2002. From August 2004 to July 2005, she served as an assistant professor in the Graduate Institute of Networking and Multimedia (INM) and as an adjunct assistant professor in CSIE, NTU. She is currently an associate professor in INM and CSIE, NTU. Her research interests include design and analysis of personal communications services network, mobile computing, voice over IP, and performance modeling. She has served as a program cochair and as a committee member of many international conferences/workshops. She was a guest editor of the *IEEE Wireless Communications*. She is currently an associate editor of the *International Journal of Sensor Networks* and *ACM Wireless Networks*. She was a recipient of the Teaching Award at NTU in 2005, 2006, and 2007, the Investigative Research Award from the Pan Wen Yuan Foundation in 2006, the Wu Ta You Memorial Award from National Science Council (NSC) in 2007, the Excellent Young Engineer Award from the Chinese Institute of Electrical Engineering, and the K.T. Li Award for Young Researchers from ACM Taipei/Taiwan Chapter in 2007. She is a member of the IEEE.

Sheng-Kun Chan received the BS degree from National Taiwan University of Science and Technology (NTUST), Taipei, in 2003, and the MS degree from National Taiwan University (NTU), in 2005. He is currently an engineer in Chunghwa Telecom (CHT) Co., Ltd. in Taiwan.