ISSN:0975-9646

Secure Dynamic Routing Using DDRA

NAGAMALLESWARA RAO.A,ADILAKSHMI.Y
Department of Computer Science and Engineering
Gudlavalleru Engineering College
Gudlavalleru—521356

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.

Keywords: Security-enhanced data transmission, dynamic routing, RIP, DSDV.

I. 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 cryptographybased systems, the IP Security (IPSec) and the Secure Socket Layer (SSL) 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], [6], [5], 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) is adopted for encryption/decryption for IPSec [6].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. 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. [7], [8], 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 [13] 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 pathsearching 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 rovide 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 [9] and Destination-Sequenced Distance Vector (DSDV) protocol for wireless networks [11], over existing infrastructures. These protocols shall not increase the number of control messages if the proposed algorithm is adopted. We propose a security-enhanced dynamic routing algorithm to randomize the data delivery paths.

II.PROBLEM STATEMENTS

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. 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 andDSDV. Link-state algorithms used in the Open Shortest Path First protocol [10] 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 **(N1,N2) (N2,N3)…(N_I,N_{I+}1)**, where **S=Ni,N_{i+1}=t,N_j∈N, and (N_J,N_{i+1})∈L for 1≤ j≤ i** .Let Ps,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 Ps,t could be an exponential function of the number of routers in the network, and we should not derive Ps,t in practice for routing or analysis .

Definition 1 (path similarity). Given two paths pi and pj, thepath similarity Sim (pi, pj) for pi and pj is defined as the number of common links between pi and pj:
Sim (pi, pj)= $\left| \{(N_x,N_y) \mid (N_x,N_y) \in p_i \wedge (N_x,N_y) \in p_j\} \right|$, 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:

$$E[Sim_{s,t}]=\sum_{\forall p_i, p_j \in P_{s,t}} sim(p_i p_j) \cdot prob(p_j \mid p_i) \cdot Prob(p_i),$$

Where Ps, t is the set of all possible transmission paths between a source node s and a destination node t. Prob (pi | pj) is the conditional probability of using pj for delivering the current packet, given that pi is used for the previous packet. Probo ((pi), is the probability of using pi for delivering the previous packet.

III.OBJECTIVE

The objective of this work is to explore a security-enhanceddynamic routing algorithm based on distributed routing information widely supported in existing networks. Our goal is to propose a distance-vector-based algorithm for dynamic routing to improve the security of data transmission. The purpose of this research is to propose a dynamic routing algorithm to improve the security of data transmission
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 next hop hs (defined in HNit of Table 1b) for the source node s is identified inthe first step of the process (line 1). Then, the process randomly pick up a neighboring node in CNit excluding hs as the next hop for the current packet transmission. The exclusion of hs for the next hop 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.

IV. PROPOSED METHOD

We will propose a dynamic routing algorithm to improve the security of data transmission.

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.
Randomization Process Consider the delivery of a packet with the destination t at a node Ni. 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 next hop hs (defined in H_t^{Ni} of Table 1b) for the source node s is identified in the first step of the process (line 1). Then, the process randomly picks up a neighboring node in C_t^{Ni} excluding hs as the next hop for the current packet transmission. The Exclusion of hs for the next hop 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.

Procedure1RANDOMIZEDSELECTOR (s,t, pkt)

1: Let hs be the used next hop for the previous packet delivery for the source node s.
2: if hs ∈ $C_t^{N}{}_i$ then
3: if $\left| C_t^{N}{}_i \right| > 1$ then
4: Randomly choose a node x from { $C_t^{N}{}_i$ - hs} as a next hop, and send the packet pkt to the node x.
5: hs ←x, and update the routing table of Ni.
6: else
7: Send the packet pkt to hs.
8: end if
9: else
10: Randomly choose a node y from $C^{N}{}_i$ t as a next hop, and send the packet pkt to the node y.
11: hs← y, and update the routing table of Ni.
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).

TABLE A
An Example of the Routing Table for the Node Ni

Destination Node(t)	Cost ($w_{Ni,t}$)	Nexthop Candidates (C^{Ni}_t)	History Record for Packet Deliveries to The Destination Node t(H^{Ni}) t
N_1	9	{ N_6, N_{21}, N_9}	{(N_2, N_{21}),(N_3, N_6),…,(N_{31}, N_{20})}
N_2	10	{ N_9, N_{21}}	{(N_1, N_9),(N_3, N_9),…,(N_{31}, N_{21})}
N_3	11	{ N_9}	{(N_1, N_9),(N_2, N_9),…,(N_{31}, N_9)}
:	:	:	:

Destination Node(t)	Cost($W_{Ni,t}$)	Nexthop
N_1	9	N_6
N_2	10	N_{21}
N_3	11	N_9
:	:	:

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

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 Ni) consists of entries $\{(N_J, W_{Ni\,Nj}, C^{Ni}_{Nj}=\{N_j\}, H^{Ni}_{Nj}=\emptyset)\}$ where $Nj \in Nbr_i$ and $W^{Ni}_{,Nj} = w^{Ni}_{Nj}$. By exchanging distance vectors between neighboring nodes, the routing table of Ni 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 $W_{Nj,\,t}$ 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, WNj, t)

1: if the destination node t is not in the routing table then
2: Add the entry (t, ($W_{Ni;\,NJ+WNjt)}$, C^{N}_{i} t = {NJ}; HNi_t =Ø).
3: else if ($W_{Ni,\,Nj}$ +$W_{Nj,\,t}$<WNi, t then
4: $C^{N}_{t\,i} \leftarrow \{N_J\}$ and N_J is marked as the minimal-cost next hop.
5: WNi, t ← ($W_{Ni,\,Nj}$ +$W_{Nj,}$ t)
6: for each node $N_k \in$ Nbri except N_J do
7: if $W_{Nk,\,t} < W_{N,\,t}$ then
8: $C^{N}_{t\,i} \leftarrow C^{N}_{t\,i} \cup \{N_k\}$
9: end if
10: end for
11: Send {t, WNi, t) to each neighboring node Nk ∈ Nbri.
12: else if ($w_{Ni,\,NJ+}W_{Nj,\,t}$)>WNi, t then
13: if (Nj ∈ $C^{N}_{t\,i}$) then
14: if NJ was marked as the minimal-cost next hop then
15: $W_{Ni,\,t}$ MIN $_{Nk \in Nbri}$ ($w_{Ni,\,Nk}$ +$W_{Nk,\,t}$)
16: $C^{N}_{t\,i} \leftarrow \emptyset$
17: for each node Nk ∈ Nbri do
18: if $W_{Nk,\,t} < W_{Ni,\,t}$ then
19: $C^{N}_{t\,i} \leftarrow C^{N}_{t\,i} \cup \{N_k\}$
20: end if
21: end for
22: Send (t, WNi, t) to each neighboring node $N_k \in Nbr_i$.
23: else if $W_{Nj,\,t} > W_{Ni,\,t}$ then
24: $C^{N}_{t\,i} \leftarrow C^{N}_{t\,i}$ _ {NJ}
25: end if
26: else if (NJ ∉ $C^{N}_{t\,i}$ t) ^ ($W_{Nj,\,t} < W_{Ni,t}$) then
27: $C^{N}_{t\,i} \leftarrow C^{N}_{t\,i} \cup \{N_j\}$
28: end if
29: end if

V.PERFORMANCE EVALUTION

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 .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 inECRA 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 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 experimental results of the average single-trip time under the proposed DDRA, ECRA, and 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_Randomized_Selector 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.experimental results of the jitters caused by our DDRAbasedmethodologies, 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 otherhand, the jitter values for DDRA_with_Randomized Selector and DDRA_without_RandomizedSelector increases 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.

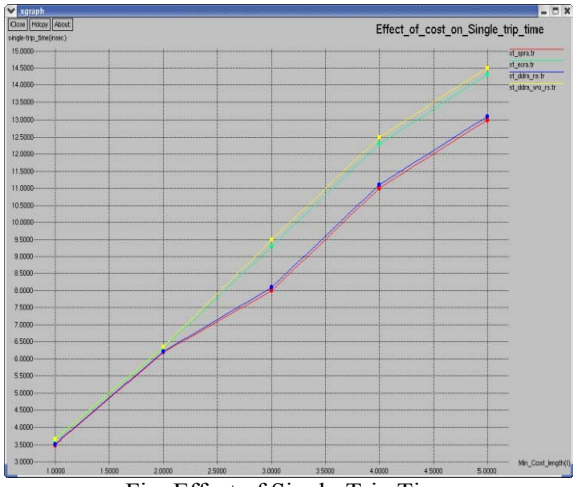

Fig. Effect of Single-Trip Time

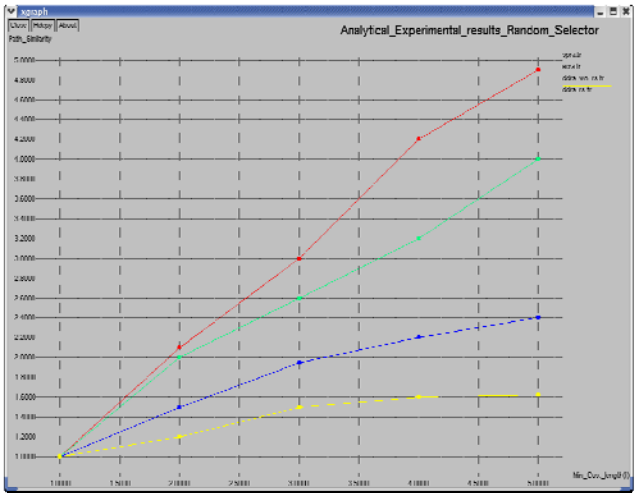

Fig. Analytical Experimental Results Random Selector

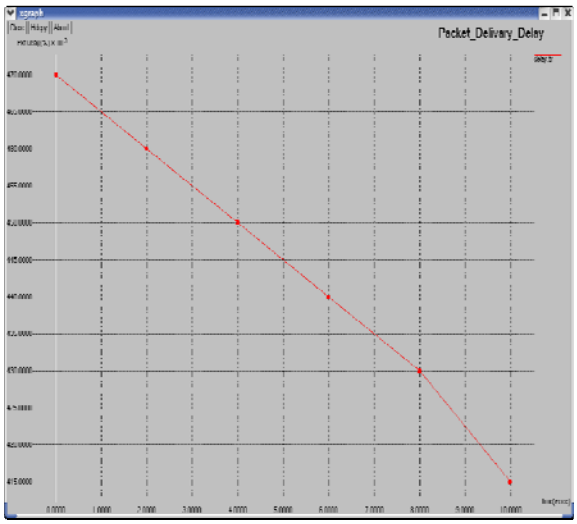

Fig. Packet Delivary Delay

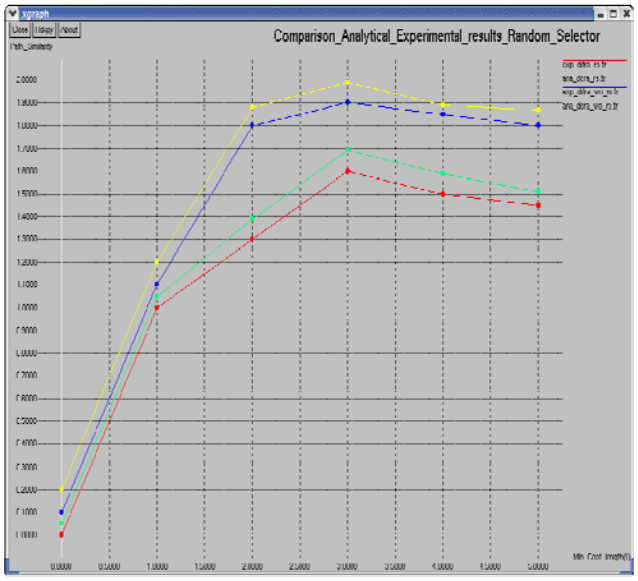

Fig. Comparison Analytical Experimental Results Random Selector

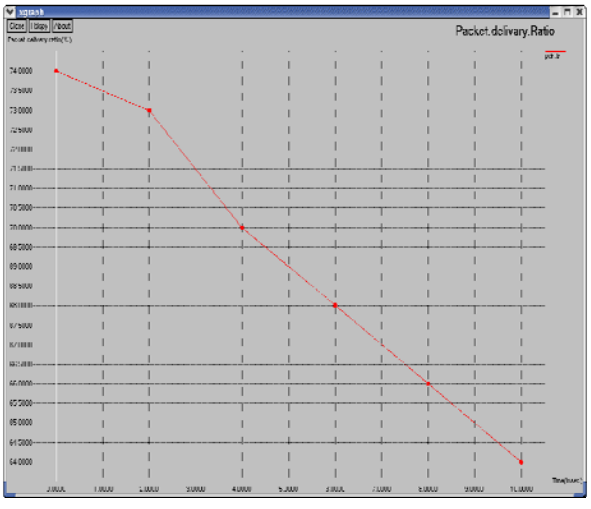

Fig. Packet Delivary Ratio

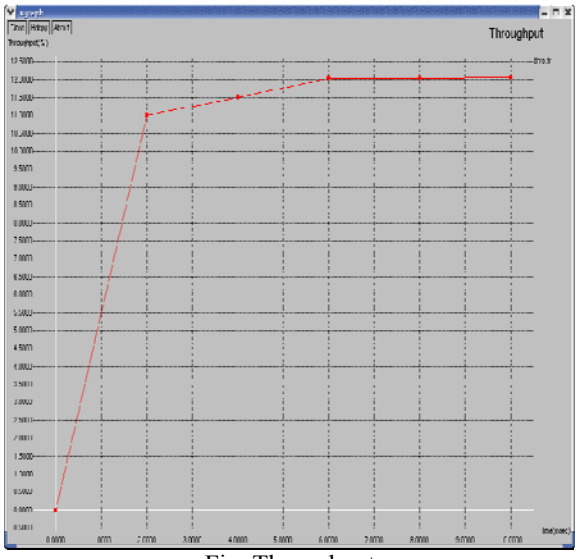

Fig. Throughput

VI.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.

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]I. Gojmerac, T. Ziegler, F. Ricciato, and P. Reichl, "Adaptive Multipath Routing for Dynamic Traffic Engineering,"Proc. IEEEGlobalTelecommunicationsConf. GLOBECOM),

[4] C. Hopps, Analysis of an Equal-Cost Multi-Path Algorithm, Request for comments (RFC 2992), Nov. 2

[5] 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 ProgressSession (RTSS WIP), 2003.

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

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

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

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

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

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

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

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