International Journal of Academic Research
ISSN: 2348-7666 Vol.2, Issue-1(4), January-March, 2015

A Distributed Dynamic Routing with Security Considerations

Kakara Ganesh, M.Tech (Final) Department CSE, Baba Institute of Technology and Sciences (BITS), PM Palem. Madhurawada, Visakhapatnam, A.P, India

T. Anand Kumar, Assistant Professor, Department CSE, Baba Institute of Technology and Sciences (BITS), PM Palem. Madhurawada, Visakhapatnam, A.P, India

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.*

Key words: *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 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, 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 Ni maintains a routing table (see Table 1a) in which each entry is associated with a tuple (t, WNi,t, $Nexthop$) where t, WNi,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, WNi,t, C^{Ni} 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 $(N1,N2)$ $(N2,N3)...(Ni,Ni+1)$, where $s= N1$, $Ni+1=t$, $Nj \in N$ and $(Nj, Nj+1)$ 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 $Sim(P_i, P_j)$ for p_i and p_j is defined as the number of common links between p_i and p_j:*

$$Sim(P_i, P_j) = |\{(N_x,N_y) | (N_x,N_y) \in p_i \wedge (N_x,N_y) \in p_j\}|,$$ *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:*

$$E[Sim_{s,t}] = \sum_{p_i,p_j \in P_{s;t}} Sim(p_i, p_j).Prob(p_i | p_j).Prob(p_i)$$

where $P_{s,t}$ is the set of all possible transmission paths between a source node s and a destination node t. $Prob(p_i | p_j)$ *is the conditional probability of using p_j for delivering the*

current packet, given that pi is used for the previous packet. Prob*(pi,) is the probability of using pi 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.* 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^{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_{Nj}) in $H^{N_i}{}_t$ is used to represent that N_j previously used the node h_{Nj} as the nexthop to forward the packet from the source node N_j to the destination node t. Let Nbr_i and $w_{Ni, Nj}$ 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 Nbr_i and contains the cost $w_{Ni,Nj}$ 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 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 intra domain 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

Table 1: An Example of the Routing Table for the Node Ni

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

(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	$\{N_6, N_{20}, N_{21}\}$	$\{(N_2, N_{21}), (N_3, N_6), \cdots, (N_{31}, N_{20})\}$
N_2	8	$\{N_9, N_{21}\}$	$\{(N_1, N_9), (N_3, N_9), \cdots, (N_{31}, N_{21})\}$
N_3	9	$\{N_9\}$	$\{(N_1, N_9), (N_2, N_9), \cdots, (N_{31}, N_9)\}$
⋮	⋮	⋮	⋮

(b)

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

3.2 A Distributed Dynamic Routing Algorithm

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^{Ni} 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 t. 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).

4 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 network

References

[1] G. Apostolopoulos, V. Peris, P. Pradhan, and D. Saha,"Securing Electronic Commerce: Reducing the SSL Overhead,"IEEE Network, 2000. neighboring node in C^{Ni} excluding h_S as the nexthop for the

[2] S. Bohacek, J.P. Hespanha, K.

Obraczka, J. Lee, and C. Lim,"Enhancing Security via Stochastic Routing," Proc. 11th Int'l Conf. Computer 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

RANDOMIZED SELECTOR (s, t, pkt) 1: Let h_S be the used next hop for the previous packet delivery for the source node s. 2: if h_S C^{Ni}_t **then**

3: if | C^{Ni}_t | > 1 **then**

4: Randomly choose a node x from {C^{Ni}_t - h_S} as a next hop, and send the packet pkt to the node x.

5: h_S 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^{Ni}_t as a nexthop, and send the packet pkt to the $node\ y$.

11: h_S 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, 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. Erdo¨s and A. Re´nyi, "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.