DYNAMIC BROADCAST ROUTING WITH SECURITY ENHANCEMENT

V. Anil Kumar[1], B.Yakhoob[2] and E.Pradeep[3]

[1&2]Asst. Professor in CSE Department, Kamala Institute of Technology and Science, Huzurabad, Karimnagar, AP, INDIA

[3]Asst. Professor in ECE Department, Kamala Institute of Technology and Science, Huzurabad, Karimnagar, AP, INDIA

anilkumarvbaranam@gmail.com, yakub.7182001@gmail.com, pradeep.e.kumar@gmail.com

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 network security algorithms and system infrastructures, we will propose a dynamic broadcast 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. The simulation results have been verified from the proposed algorithm and it shows the capability of the proposed algorithm.*

KEYWORDS- *Security-enhanced data transmission, dynamic broadcast routing, RIP, DSDV.*

1. INTRODUCTION

In the last years, various security-enhanced measures have been introduced to improve the security of data transmission over public networks. Existing work on security-enhanced data transmission includes the designs of network security 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 network security based systems, the IP Security (IPSec) [23] and the Secure Socket Layer (SSL) [21] are popularly supported and implemented in many systems and platforms. AlthoughIPSec 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 broadcast 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 multiplepath 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 broad cast 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 broadcast routing algorithm to provide securityenhanced data delivery without introducing any extra control messages.

The objective of this work is to explore a securityenhanced dynamic broadcast 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.

2 PROBLEM STATEMENT

The objective of this work is to explore a security-enhanced dynamic broadcast 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 broadcast routing to improve the security of data transmission.

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) ----- $(N_{i,} N_{i+1})$, where $S=N_1$, $N_{i+1}=t$, N_j ε N, and 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 Ps;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 pi and pj, the path similarity Sim(pi,pj) for pi and pj is defined as the number of common links between pi and pj:

$$Sim(pi,pj)=|\{(Nx,Ny)|(Nx,Ny)\ \varepsilon\ pi\ \wedge(Nx,Ny)\ \varepsilon\ pj)\}|,$$

where Nx and Ny are two nodes in the network.

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

The purpose of this research is to propose a dynamic broadcast 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 BROADCAST ROUTING

3.1 Notations and Data Structures

The objective of this section is to propose a distance-vectorbased algorithm for dynamic broadcast 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 ($t,WN_{i,;t}$,Nexthop), where t, $W_{Ni;t}$, 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.

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 Routing Table for the Node N_i

Destination Node(t)	Cost($W_{Ni;t}$)	Nexthop
N_1	7	N_6
N_2	8	N_{21}
N_3	9	N_9
: :	: :	: :

(a)

Destination Node (t)	Cost ($W_{Ni;t}$)	Nexthop Candidates (C_t^{Ni})	History Record for Packet Deliveries to the Destination Node t (H_t^{Nt})
N_1	7	$\{N_6,N_{20},N_{21}\}$	$\{(N_2, N_{21}),(N_3, N_6),\ldots..,(N_{31}, N_{20})\}$
N_2	8	$\{N_6,N_{20},N_{21}\}$	$\{(N_2, N_{21}),(N_3, N_6),\ldots..,(N_{31}, N_{20})\}$
N_3	9	$\{N_6,N_{20},N_{21}\}$	$\{(N_2, N_{21}),(N_3, N_6),\ldots..,(N_{31}, N_{20})\}$
:	:	:	:

(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 broadcast routing algorithm (DDBRA) 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.

3.2 Distributed Dynamic Broadcast Routing Algorithm

The DDBRA 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 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 h_s as the next hop for the current packet transmission. The exclusion of h_s 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.

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 $h_s \varepsilon C_t^{Ni}$ then
3:    if $| C_t^{Ni} |>1$ then
4:       Randomly choose a node x from { $C_t^{Ni}$ - $h_s$} 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 $C_t^{Ni}$ 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 Ni) consists of entries

$\{(N_j,W_{Ni,Nj},C^{Ni}_{Nj}=\{ N_j \},H^{Ni}_{Nj}=0)\}$, where $N_j \varepsilon Nbr_i$ 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 Ni 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 nodeN_j to the destination node t.

4 PERFORMANCE EVALUATION

The purpose of this section is to evaluate the performance of the proposed algorithm, referred to as the DDBRA. We compare the performance of DDBRA 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.

The primary performance metric is the average value [ESimPS]of path similarity for all source-destination pairs in PS. The values of [ESimPS] 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 [ESimPS] can be obtained by averaging the path similarity of all source-destination pairs with the length l of minimal-cost paths.

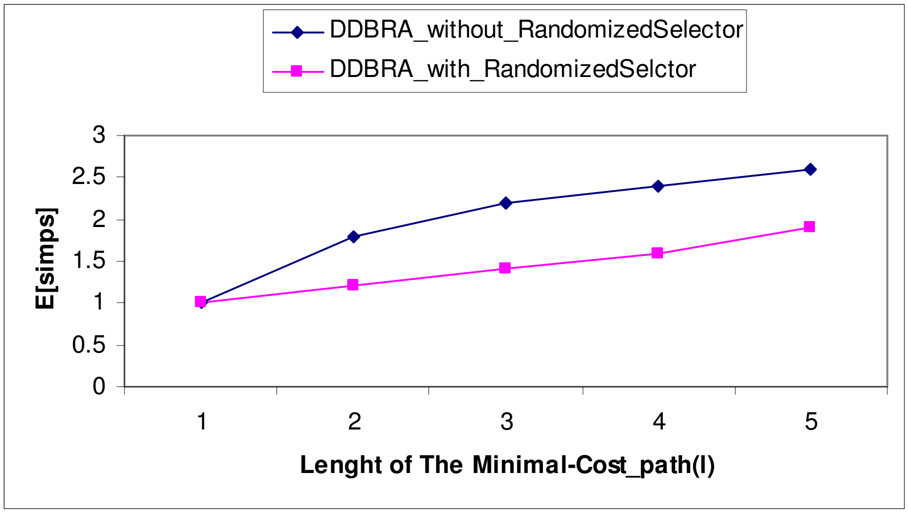

Figure 1. Experimental results

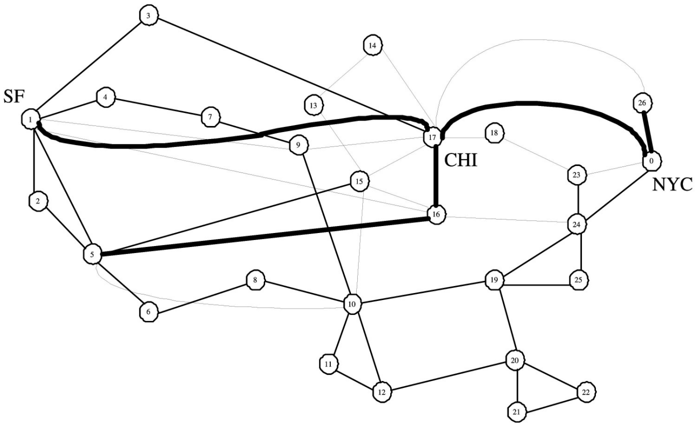

Figure 2.AT&T US topology

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 The simulated traffic is constant bit rate (CBR) over User Datagram Protocol (UDP). The interval time ofCBR is 10msand 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.

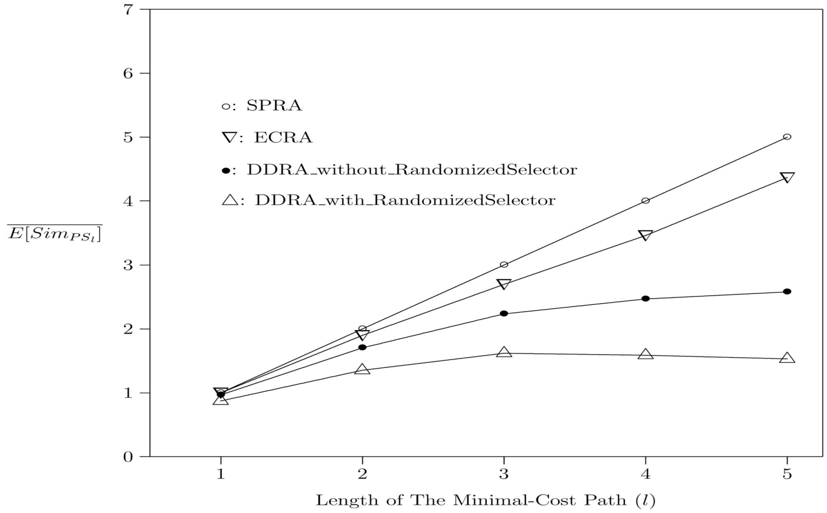

Figure 3. E[Simps] for AT&T US topology.

Fig.3 shows the experimental results of E[Simps] 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 E[simps]values for SPRA, ECRA, and DDRA_without_RandomizedSelector increases. The increasing rates for SPRA and ECRA are much larger than those for DDRA_without_RandomizedSelector especially when l is large. Specifically, the E[simps]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.Onthe other hand,whenl increases, E[simps]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.

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 broadcast 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] 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.

Authors:

V.ANIL KUMAR received B.Tech degree in Computer Science and Engineering from KITS(S), Huzurabad, JNTUH and the M.Tech degree in Computer Science and Engineering from JNTU Hyderabad. He served as an Asst.Professor in Computer Science and Engineering Department at Kamala Institute of Technology and Science, Huzurabad, Karimnagar, Andhra Pradesh, India. His research interests include

Mobile communications, Wireless communications and Network Security. He is a member of ISTE.

B. YAKHOOB received B.Tech degree in Computer Science and Engineering from KITS, Warangal in 2000 and M.Tech degree in Computer Science from JNTU, Anantapur in 2005.He served as an Asst.Professor in Computer Science and Engineering Department at Kamala Institute of Technology and Science, Huzurabad, Karimnagar, Andhra Pradesh, India. His research interests in Data Mining, Wireless communication and network security.

E. PRADEEP received M.Sc degree in Electronics from Osamania University in 2007 and M.Tech degeree in Computer Science and Engineering from JNTU in 2010. He served as an Asst.Professsot in ECE Department at Kamala Institute of Technology and Science, Huzurabad, Karimnagar, Andhra Pradesh,India. His research interests in Mobile communications, Wireless networks and Network security.