ISSN : 2231-0711

IJCSET | May 2011 | Vol 1, Issue 4,176-179

A Novel Approach for Security Enhancement in Dynamic Routing

P.Nagamalleswari , P.Srinivasulu, G.Kranthi Kumar , J.Rangarao
V. R Siddhartha Engineering College,Vijayawada,Andrapradesh, India

***Abstract* -In this project we deal fully about the security which 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. 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. The main objective of the project is to propose a dynamic routing algorithm to improve the security of data transmission.**

1. INTRODUCTION

In the past decades, various security-enhanced measure shave 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) 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, 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 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. 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. proposed a secure stochastic routing mechanism to improve routing security. Similar to the work proposed by Lou et al. 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.

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 and Destination-Sequenced Distance Vector (DSDV) protocol for wireless networks, 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.

2.PROBLEM STATEMENT

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) and the Secure Socket Layer (SSL) are popularly supported and implemented in many systems and platforms.

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 and DSDV. Link-state algorithms used in the Open Shortest Path First protocol 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.

3.OBJECTIVE

In the proposed system is 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. Our goal is to propose a distance-vector-based algorithm for dynamic routing to improve the security of data transmission.

4. METHODOLOGY

In the proposed system using two algorithms.Security Enhanced Dynamic routing and Distributed Dynamic Routing algorithm.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. The DDRA proposed in this paper consists of two parts: a randomization process for packet deliveries and maintenance of the extended routing table.

5. HYPOTHESIS

The objective of this work is to explore 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 and Destination-Sequenced Distance Vector (DSDV) protocol for wireless networks, 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.

6. ALGORITHM USED:

- An updated version of the distance-vector-based routing algorithm called Security-Enhanced routing algorithm.
- This algorithm has the terms as in DSV algorithm with a updated column which holds the history of the path through which the packet traversed.

Algorithm / Technique used:

Distance Vector based Algorithm for Dynamic Routing.

Algorithm Description:

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 in which each entry is associated with a tuple and Next hop 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.

7. 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 ðt;WNi ;t;NexthopÞ, where t, WNi;t, and Next hop 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.

7.1.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.

7.2Randomization 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 nexthop hs (defined in HNi t 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 CNi t excluding hs as the nexthop 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. The number of entries in the history record for packet deliveries to destination nodes is jNj 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 Oð1Þ 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.

7.3Routing Table Maintenance

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 fðNj;WNi;Nj; CNi Nj ¼ fNjg;HNi Nj ¼ ;Þg, where Nj 2 Nbri and WNi;Nj ¼ wNi;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 Nj. Each element of a distance vector

received from a neighboring nodeNj includes a destination node t and a delivery costWNj;t from the nodeNj to the destination node t.

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

7.4 Performance and Evaluation

The purpose of this section is to evaluate the performance of the proposed algorithm, referred to as the DDRA. 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 ðNi;NjÞ in OSPF could be derived as follows:

OSPF-Cost(ni,nj)=10^8/Interface Speed in bps

where Interface_Speed_in_bps is the minimal bandwidth of the connected interfaces between Ni and Nj. The setting for the link-cost value in another popular distance-vector-based routing protocol, Enhanced Interior Gateway Routing We shall show that, in the experiments, an equal-cost link strategy could have a more average on the path similarity.

Figures 1 and 2 show 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 DRA_with_R anodized 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, 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 is the single-trip time used to transmit the jth packet. This equation is used to calculate the jitter for cumulatively receiving i packets, where STTi is the single-trip time used to transmit the ith packet, and Based on the above equation, Figure 3 and 4 show the experimental results of the jitters caused by our DDRAbased 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.

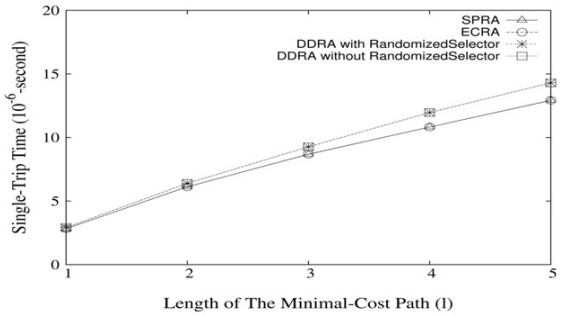

Figure.1 Effect of l on single-trip time for AT&T US topology

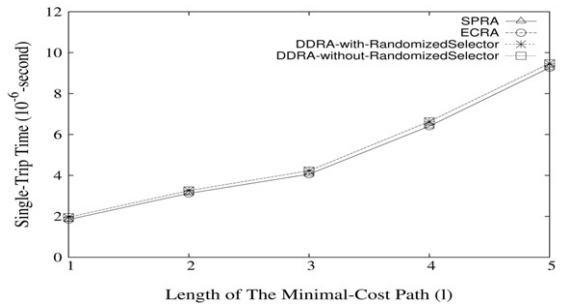

Figure.2 Effect of I on single-trip time for DANTE Europe topology

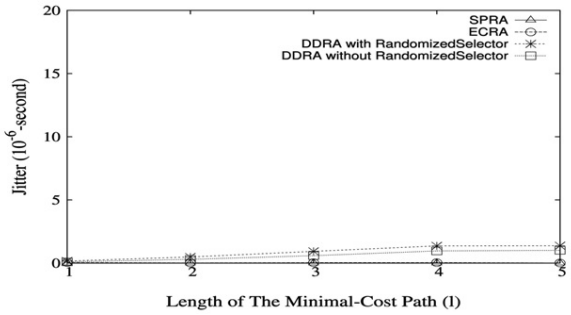

Figure.3 Effect of l on jitter for AT&T US topology

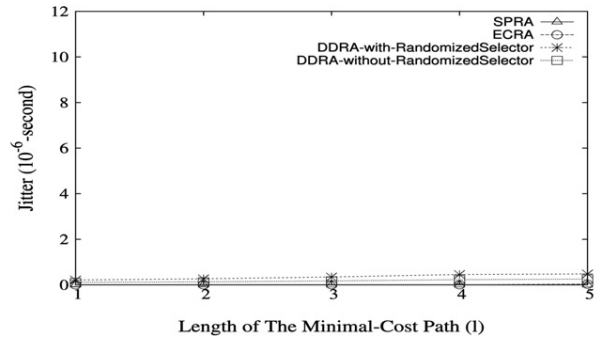

Figure.4 Effect of l on jitter for DANTE Europe topology

7.5 Distributed computing

Distributed computing utilizes a network of many computers, each accomplishing a portion of an overall task, to achieve a computational result much more quickly than with a single computer. In addition to a higher level of computing power, distributed computing also allows many users to interact and connect openly. Different forms of distributed computing allow for different levels of openness, with most people accepting that a higher degree of openness in a distributed computing system is beneficial. The segment of the Internet most people are most familiar with, the World Wide Web, is also the most recognizable use of distributed computing in the public arena. Many different computers make everything one does while browsing the Internet possible, with each computer assigned a special role within the system. A home computer is used, for example, to run the browser and to break down the information being sent, making it accessible to the end user [17]. Client-server computing or networking is a distributed application architecture that partitions tasks or workloads between service providers (servers) and operate over service requesters, called clients. Often clients and servers a computer network on separate hardware. A server machine is a high-performance host that is running one or more server programs which share its resources with clients [20].

8.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.

9. FUTURE SCOPE

Satellite network capacity, adaptability, and responsiveness are enhanced with onboard capabilities for packet switching, bandwidth allocation, and spot-beams which facilitate uplink and downlink spectral reuse. A recent over-the-air (OTA) test of the SPACEWAYTM system, a Ka-band regenerative satellite mesh network supporting IP packet services, provides definitive demonstration of key capabilities in the areas of quality-of-service, routing for unicast and multicast (both best-effort and guaranteed service) traffic, dynamic bandwidth resource allocation, security, and configurable satellite uplink and downlink components. Leveraging SPACEWAY system technologies and operational capabilities serves as a pragmatic step toward the development of future multi-satellite networks with more advanced features including onboard packet routing, multi-mode radio transmission, and inter-satellite links, which are now being considered for transformational satellite 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.