Distributed Dynamic Routing Algorithm to Enhance- Security in Wired and Wireless Networks

P Kiran Kumar[1] G Yedukondalu[2] R Praveen Kumar[3]

[1]M.Tech Scholar, Vignan Institute of Technology and Science, Hyderabad
[2]Assoc.Prof, CSE Dept, Vignan Institute of Technology and Science, Hyderabad
[3]Asst.Prof, CSE Dept, Vignan Institute of Technology and Science, Hyderabad

Abstract: Security has become one of the major issues for data communication over wired and wireless networks. The existing algorithms supported stationary delivery paths for data transmission over the wired and wireless networks. In this paper we are introducing a Distributed Dynamic Routing Algorithm that could randomize delivery paths for data transmission. The algorithm is easy to implement and congenial 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 objective of this work is to explore a security-enhancement in wired and wireless networks with Distributed Dynamic Routing Algorithm based on distributed routing information with small path similarity.

Key Words: Security-enhanced data transmission, dynamic routing, RIP, DSDV, DDRA, path similarity.

1. ITNTRODUCTION

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 [1].

[1]Among many well-known designs for cryptography based systems, the IP Security (IPSec) [7] and the Secure Socket Layer (SSL) [13] 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 6 cycles/byte over an Intel Pentium II with the Linux IP stack alone, and the overhead increases to 68 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 [1].

2. LITERATURE SURVEY

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 [16] 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 [1].

3. SECURE SOCKET LAYER

In Secure Socket Layer we concern with the implementation of the client and server entities and the SSL transaction between respective client and server. This transaction comprises of the authentication, key exchange and large data transfer. Our implementation ensures secure and reliable communication (message exchange) and data transfer (files) between the two entities. Now-a-days Information is one of the most valuable resources in the world. Whether it is a personal letter or an industrial secret, all information or data has a worth to someone. This considers issues of security and privacy for such information or data that is stored. It discusses the reasons for wishing to provide security for the data and the methods available for doing so.

For secure transferring of information between the sockets at distant places which mainly requires security so that the message or data may not be tampered while it has been transferred. When a client and server communicate with each other, SSL ensures that the connection is private and secure by providing authentication and encryption. Authentication confirms that the server and the client are trustworthy. Encryption then creates a secure “tunnel” between the two, which prevents any unauthorized system from reading the data. SSL enabled clients (such as a Netscape or Microsoft browser) and SSL-enabled servers (such as Apache or IIS) confirm each other’s identities using digital certificates. Digital certificates are issued by trusted third parties called Certificate Authorities (or CAs) and provide information about an individual’s claimed identity, as well as their public key. By validating digital certificates both parties can ensure that an imposter has not intercepted a transmission [2],[9].

4. EXISTING SYSTEM

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 6 cycles/byte over an Intel Pentium II with the Linux IP stack alone, and the overhead increases to 68 cycles/byte when Advanced Encryption Standard (AES) is adopted for encryption/decryption for IPSec.

5. PROPOSED SYSTEM

We will propose a distributed 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 Dynamic Routing Information Protocol in wired and wireless networks and Destination-Sequenced Distance Vector protocol in wireless networks, without introducing extra control messages.

6. 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 [14] 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.

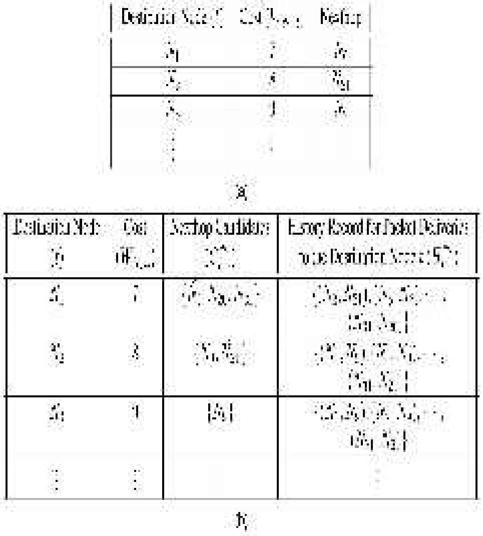
A network could be modeled as a graph G =(N,L), where N is a set of routers (also referred to as nodes) in the network, and L is a set of links that connect adjacent routers in the network. A path p from a node s (referred to as a source node) to another node t (referred to as a destination node) is a set of links (N1,N2), (N2,N3)….(Ni,Ni+1), where s=N1, Ni+1= t, Nj € N, and (Nj,Nj+1) € L for 1≤ j ≤ 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[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) € pi ^ (Nx, Ny) € pj}|, where Nx and Ny are two nodes in the network.

7. SECURITY-ENHANCED DYNAMIC ROUTING

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 [1].



Destination Node (t)	Cost ($W_{N_i,t}$)	Nexthop
N_1	7	[illegible]
N_2	[illegible]	[illegible]
N_3	[illegible]	[illegible]
⋮	⋮	

a

Destination Node (t)	Cost ($W_{N_i,t}$)	Nexthop Candidates ($C_t^{N_i}$)	History Record for Packet Deliveries to the Destination Node ($H_t^{N_i}$)
N_1	7	[illegible]	[illegible]
N_2	8	[illegible]	[illegible]
N_3	1	[illegible]	[illegible]
⋮	⋮		⋮

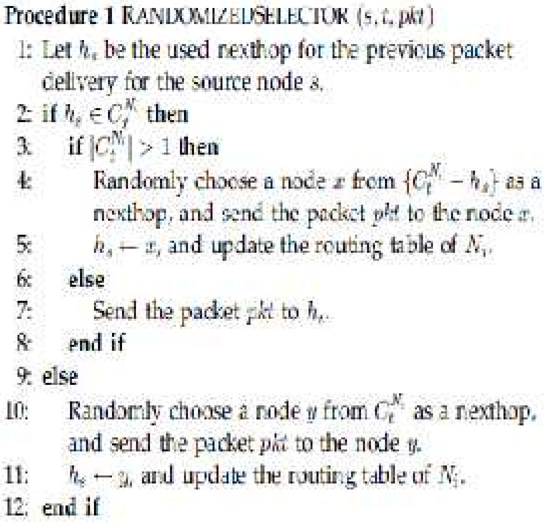
b

Table 1(a) and 1(b)

8. DISTRIBUTED DYNAMIC ROUTING ALGORITHM

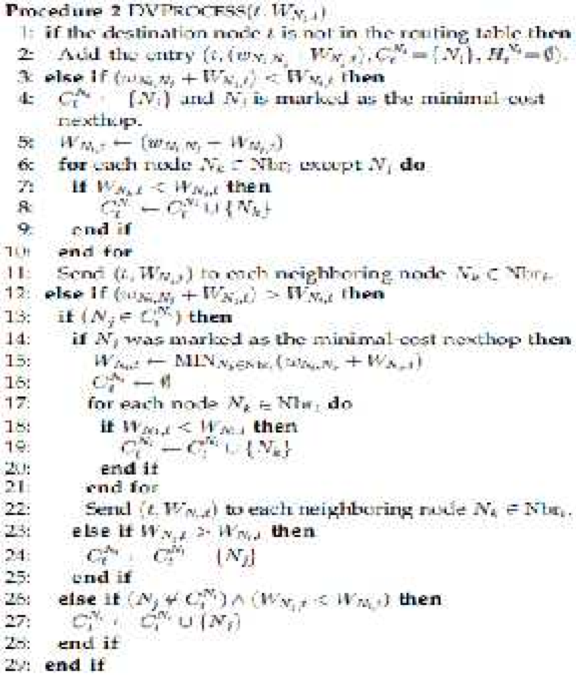
A Distributed Dynamic Routing Algorithm The DDRA proposed in this paper consists of two parts: 1) a randomization process for packet deliveries and 2) maintenance of the extended routing table.

Randomization Process



```
Procedure 1 RANDOMIZEDSELECTOR (s, t, pkt)
Let $h_s$ be the used nexthop for the previous packet
  delivery for the source node $s$.
if $h_s \in C_t^{N_i}$ then
  if $|C_t^{N_i}| > 1$ then
    Randomly choose a node $x$ from $\{C_t^{N_i} - h_s\}$ as a
    nexthop, and send the packet $pkt$ to the node $x$.
    $h_s \leftarrow x$, and update the routing table of $N_i$.
  else
    Send the packet $pkt$ to $h_s$.
  end if
else
  Randomly choose a node $y$ from $C_t^{N_i}$ as a nexthop,
  and send the packet $pkt$ to the node $y$.
  $h_s \leftarrow y$, and update the routing table of $N_i$.
end if
```

Routing Table Maintenance



```
Procedure 2 DVPROCESS($t, W_{N_j,t}$)
if the destination node $t$ is not in the routing table then
  Add the entry $(t, (w_{N_i,N_j} + W_{N_j,t}), C_t^{N_i} = \{N_j\}, H_t^{N_i} = \emptyset)$.
else if $(w_{N_i,N_j} + W_{N_j,t}) < W_{N_i,t}$ then
  $C_t^{N_i} \leftarrow \{N_j\}$ and $N_j$ is marked as the minimal cost
  nexthop.
  $W_{N_i,t} \leftarrow (w_{N_i,N_j} + W_{N_j,t})$
  for each node $N_k \in Nbr_i$ except $N_j$ do
    if $W_{N_k,t} < W_{N_i,t}$ then
      $C_t^{N_i} \leftarrow C_t^{N_i} \cup \{N_k\}$
    end if
  end for
  Send $(t, W_{N_i,t})$ to each neighboring node $N_k \in Nbr_i$.
else if $(w_{N_i,N_j} + W_{N_j,t}) > W_{N_i,t}$ then
  if $(N_j \in C_t^{N_i})$ then
    if $N_j$ was marked as the minimal-cost nexthop then
      $W_{N_i,t} \leftarrow MIN_{N_k \in Nbr_i}(w_{N_i,N_k} + W_{N_k,t})$
      $C_t^{N_i} \leftarrow \emptyset$
      for each node $N_k \in Nbr_i$ do
        if $W_{N_k,t} < W_{N_i,t}$ then
          $C_t^{N_i} \leftarrow C_t^{N_i} \cup \{N_k\}$
        end if
      end for
      Send $(t, W_{N_i,t})$ to each neighboring node $N_k \in Nbr_i$.
    else if $W_{N_j,t} > W_{N_i,t}$ then
      $C_t^{N_i} \leftarrow C_t^{N_i} - \{N_j\}$
    end if
  else if $(N_j \notin C_t^{N_i}) \wedge (W_{N_j,t} < W_{N_i,t})$ then
    $C_t^{N_i} \leftarrow C_t^{N_i} \cup \{N_j\}$
  end if
end if
```

Routing Information Protocol (RIP): The Routing Information Protocol (RIP) is a distance-vector routing protocol, which employs the hop count as a routing metric. The hold down time is 180 seconds. This protocol prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 13. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 14 is considered an infinite distance and used to deprecate inaccessible, inoperable, or otherwise undesirable routes in the selection process. RIP implements the split horizon, route positioning and hold-down mechanisms to prevent incorrect routing information from being propagated. These are some of the stability features of RIP. It is also possible to use the so called RMTI (Routing Information Protocol with Metric-based Topology Investigation) algorithm to cope with the count-to-infinity problem. With its help, it is possible to detect every possible loop with a very small computation effort [2].

RIP Version2 Carrying Additional Information: The Routing Information Protocol (RIP) is a Distance-vector protocol that uses hop count as its metric. RIP is widely used for routing traffic in the global Internet and is an interior gateway protocol (IGP), which means that it performs routing within a single autonomous system. Exterior gateway protocols, such as the Border Gateway Protocol (BGP), perform routing between different autonomous systems [2].

1). **Routing Updates***:* RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by one, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send [2].

9. 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. 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. 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 50, 60, and 70. The link probabilities are 0.2, 0.3, 0.4, and 0.5.

10. CONCLUSION AND ENHANCEMENT

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.

11. REFERENCES

1. Dynamic routing with security Considerations IEEE Transactions on Parallel and Distributed Systems VOL.20, NO.1, January2009 Chin fu kuo , Member, IEEE , Ai-Chun Pang , Member , IEEE .
2. Dynamic routing with security Considerations, D Pavan et al, Int. J. Comp. Tech. Appl., Vol 2 (6), 1790-1794, ISSN:2229-6093.
3. G. Apostolopoulos, V. Peris, P. Pradhan, and D. Saha,“Securing Electronic Commerce: Reducing the SSL Overhead,” IEEE Network, 2000.
4. 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.
5. 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.
6. P. Erdo¨s and A. Re´nyi, “On Random Graphs,” Publicationes Math. Debrecen, vol. 6, 1959.
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.
8. J.F. Kurose and K.W. Ross, Computer Networking—A Top-Down Approach Featuring the Internet. Addison Wesley, 2003.
9. Secure Sockets Layer (SSL), http://www.openssl.org/, 2008.
10. Cisco Systems, White Paper: EIGRP, Sept. 2002.
11. R. Thayer, N. Doraswamy, and R. Glenn, IP Security DocumentRoadmap, Request for comments (RFC 2411), Nov. 1998.
12. The Network Simulator-ns2, http://www.isi.edu/nsnam/ns/, 2008.
13. Secure Sockets Layer (SSL),http://www.openssl.org/, 2008.
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. J. Yang and S. Papavassiliou, “Improving Network Security by Multipath Traffic Dispersion,” Proc. IEEE Military Comm. Conf.(MilCom), 2001.