IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 34-38
www.iosrjournals.org

Dynamic Routing for Encrypted Data Transmission

Kishor T. Mane[1], Vandana G. Pujari[2], Radhika Dhanal[3], Shatakshi Kokate[4]
[1]*Dept. of Information Technology, D. Y. Patil College of Engg. & Tech., Kolhapur, Maharashtra, India*
[2]*Dept. of E&TC, D. Y. Patil Polytechnic, Kolhapur, Maharashtra, India*
[3,4] *Dept. of CSE, D. Y. Patil College of Engg. & Tech., Kolhapur, Maharashtra, India*

ABSTRACT: *The Nowadays, the use of the internet increases either with the help of wired or wireless network. Due to the transfer of valuable information over the network, security becomes a prime issue for the society. As the data transferred on the computer network may not be secure and is vulnerable to many threats. The various security mechanisms have been incorporated in the recent times, which greatly improve the data security.*

This paper focuses on the new way of transferring the information using a dynamic routing algorithm with cryptographic extensions to improve the data security over computer network. This system is very easy to implement and is also compatible with existing network infrastructure. The results of testing are satisfactory.

Keywords -*Blowfish algorithm, Encryption,Data security, Dynamic routing, Static routing.*

I. INTRODUCTION

Today, everybody use the internet with the help of wired or wireless network. Using this network the businesses can send their valuable data from one place to other. To do this they require the security mechanisms. Although lot of security algorithms are exists but they generates lot of overheads in the transmission. Another way of transferring the information is use of routing techniques while transferring the information. There are two routing techniques as static and dynamic routing. Static routing [1] provides one way of configuring path selection of routers in computer networks. It is the type of routing characterized by the absence of communication between routers regarding the current topology of the network. This is achieved by manually adding routes to the routing table. But,static routes do not dynamically adapt to network topology changes or equipment failures. Static routing does not scale well in large networks. Static routing allows routing tables in specific routers to be set up in a static manner so network routes for packets are set. If a router on the route goes down the destination may become unreachable. Dynamic routing [1] performs the same function as static routing except it is more robust. It allows routing table in routers to change as the possible routes change. There are several protocols used to support dynamic routing. For example, Routing Information Protocol helps routers for adapting dynamical changes of network connections by communicating information about networks each router can reach and how far away those networks are.

Each routing algorithm must specify the following requirements:

i) A procedure for passing reachability information about networks to other routers.
ii) A procedure for receiving reachability information from other routers
iii) A procedure for determining optimal routes based on the reachability information it has and for recording this information in a route table
iv) A procedure for reacting to, compensating for and advertising topology changes in an internetwork.

If security is not provided in the network then an unauthenticated user can do the following activities,

i. Disable the router & network
ii. Compromise other routers
iii. Bypass firewalls, IDS systems
iv. Monitor and record all outgoing and incoming traffic

v. Redirect whatever traffic they desire

So, to keep our data safe form all these activities this paper focuses on the secure transfer of data over the network using dynamic routing.

II. LITERATURE SURVEY

From many years various security-enhanced measures have been implemented to improve the security of data transmission over public networks. Existing systems for security-enhanced data transmission includes the designs of cryptographic algorithms and system infrastructures and security-enhanced routing methods. The common objective of these systems is 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) [2] and the Secure Socket Layer (SSL) [2] are popularly supported and implemented in many systems and platforms. Although IPSec and SSL greatly improve the security level for data transmission, they unavoidably introduce substantial overheads, especially on gateway or 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.[4][5] The discovery of paths in an offline fashion might not be suitable to networks with a dynamic changing configuration which is used in existing system.

An alternative way of security-enhanced data transmission is to dynamically route packets between each source and 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. 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, the dynamic routing algorithm approach is used to provide security enhanced data delivery without introducing any extra control messages.

The proposed system fulfills the following challenges as –

1. To provide guarantee of secure data transmission over computer networks.
2. To provide data security over network without introducing any network traffic overhead while data transmission.
3. To provide system in which user should not worry about the security of data transmitted over network.
4. To provide easy way to end user for transferring confidential data.

III. SYSTEM ARCHITECTURE

The present work is to explore a security enhanced dynamic routing technique based on distributed routing information widely supported in existing wired and wireless networks. In this delivery paths for data transmission have been selected randomly. The block diagram of this system is shown in fig. 1.

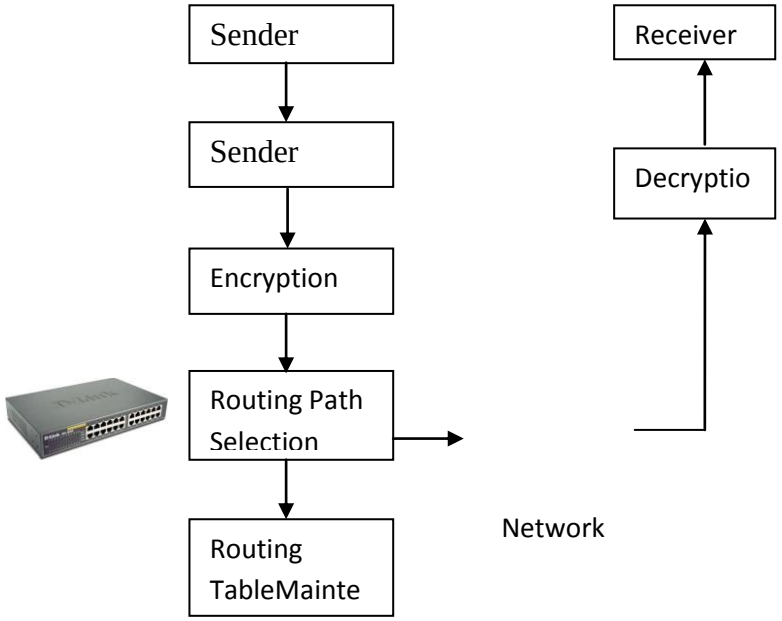

Fig. 1:System Architecture

The design and development of this system is divided into three modules as –

3.1 Constructing Desired LAN Structure

Client-server networking is a distributed architecture that partitions tasks or workloads between service providers and service requesters, called clients. Often clients and servers operate over 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. A client also shares any of its resources; Clients therefore initiate communication sessions with servers which await incoming requests. Depending upon the number of nodes and the links between them, a LAN structure is designed for which possible path was calculated using inter domain packet filtering. The sample LAN structure which is to be taken in account for the process is shown below.

3.2 Cryptographic Algorithm

This module is implemented for encryption of user's data and makes it available for transferring to destination. Encryption is done at sender side and decryption is done at receiver side. The presented system uses a symmetric encryption algorithm known as Blowfish algorithm.

The blowfish algorithm has been developed as a symmetric cryptographic standard for general use by public. Blowfish is a keyed, symmetric block cipher. Blowfish has a 64-bit block size and a variable keylength from 32 up to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. The Blowfish function uses a function which splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The outputs are added modulo 232 and XORed to produce the final 32-bit output.Blowfish algorithm was chosen because of following objectives:

i. High level of security

ii. Completely specified and easy to understand
iii. Cryptographic security does not depend on algorithm secrecy.
iv. Adaptable to diverse Applications
v. Economical hardware implementation
vi. Efficient
vii. Fast encryption and decryption

3.3 Dynamic Routing

A distance vector based algorithm [1] is used for dynamic routing to improve the security of data transmission. Distance information exchanged among neighboring node is used for the seeking of routing paths. In distance-vector-based implementation, each node Ni maintains a routing table. Each entry in routing table represents some unique destination node, an estimated minimal cost to destination, and the next node information.It includes following steps as –

i) *Data Fragmentation* – In this, user data is divided into the number of equal sized subparts where each subpart is known as fragment. User data is divided on the basis of size of user data. Each fragment of user data is identified by the unique fragment number within all fragments of user data. A control information header is added to each fragment. This header contains the fields such as source address, destination address, fragment number, total fragments.

ii) *Packet Forwarding Service* – The main function of this service is extract the destination address from the received packet or fragment of user data and forward the packet or data fragment to the node which claims as destination node.

iii) *Virtual Routing Table* – On the completion of user data fragmentation, next activity is generating of virtual routing table. Virtual routing tables have the different structure than the basic or traditional routing table structure. Structure of virtual routing table is shown in the following fig. 2.

SA	DA	N	FN	T	User Data	A	AD

Fig. 2: Structure of virtual routing table

Where,
S – Source Address D – Destination Address
N – Next Node Address F – Fragment number
T – Total Fragments Data – User Data
A – Acknowledgement from Next node
AD – Acknowledgement from Destination

3.4 Randomization Process

In order to minimize the probability of eavesdropping of packets over a specific link, a randomization process for packet delivery is implemented. The process randomly picks up a neighboring node excluding the neighboring node used for last packet transmission as the next hop for the current packet transmission. The exclusion of neighboring node used for last packet transmission ensure that no two consecutive packets are transferred from same link. The routing table has been maintained to get all information of nodes and paths.

IV. EXPERIMENTAL setup

Our experimental platform includes each node having Intel core to duo processor, 2GHz with 4GB RAM connected to each other via switch. On each node, windows operating system has been installed. The implementation has been done using JAVA language with oracle 10g as the database. The multithreading concept has been used for implementing above system.

The above system has been tested by considering different cases as –

1. Verifying outputfor encryptionanddecryptionfunction.
2. Fragmentationof UserInputData
3. Tocheckwhetherconsecutivepacketsaretransferredornottransferred fromsamenetworklink
4. Tocheckwhetherunavailablenodesareincludedor notincludedinvirtual routingtable.
5. Tocheckforlostpacketsandretransmissionof packets Numberof neighbornodesis equaltonumberof fragments
6. Totestwhetherdatabaseacceptsduplicatevalues
7. Consider networkdelaywhiletransferringpackets.
8. To checkwhethertheintermediatenodecanhandlemultipleusers.

V. RESULTS

The results obtained so far can be summarized as follows,

a. Improved data transmission speed.
b. Easy to use.
c. No extra network traffic overhead is generated.
d. Secure transfer of data.

VI. CONCLUSION AND FUTURE WORK

A security-enhanced dynamic routing algorithm based on distributed routing information widely supported in existing networks. This system is easy to implement and compatible with popular routing protocols, such as RIP and DSDV, over existing infrastructures. This system has advantage such as, improved data transmission speed, improved security over traditional systems. Further it can be applied to wireless network. It can be extended to prevent entry/exit point attack of third person.

REFERENCES

[1] Chin-Fu Kuo, Ai-Chun Pang and Sheng-Kun Chan, "Dynamic Routing with Security Considerations", *IEEE Transactions on Parallel and Distributed System, VOL. 20,* NO. 1, January 2009
[2] G. Apostolopoulos, V. Peris, P. Pradhan, and D. Saha, "Securing Electronic Commerce: Reducing the SSL Overhead,"*IEEE Network*, 2000
[3] J. Yang and S. Papavassiliou, "Improving Network Security byMultipath Traffic Dispersion," Proc. *IEEE Military Comm. Conf.(MilCom)*, 2001.
[4] S.-H. Liu, Y.-F.Lu, C.-F.Kuo, A.-C.Pang, and T.-W. Kuo, "The Performance Evaluation of Dynamic Configuration Method over IPSEC," Proc. 24th *IEEE Real-Time Systems Symp.: Works in Progress Session (RTSS WIP)*, 2003.
[5] Secure Sockets Layer (SSL), http://www.openssl.org/, 2008.
[6] W. Lou and Y. Fang, "A Multipath Routing Approach for Secure Data Delivery," *Proc. IEEE Military Comm. Conf. (MilCom)*, 2001.
[7] Book: Herbert Schildt, "*Java Complete Reference*"
[8] Book: Michael Blaha, James Rambaugh. "*Object Oriented Modeling and Design with UML*"
[9] Book: Ian Sommerville, "*Software Engineering*", Seventh Edition,