IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DYNAMIC ROUTING FOR DATA INTEGRITY IN WIRELESS SENSOR NETWORKS

CHEDALAVADA MICHAEL JOSEPH RAJA [#1], K.RAMBABU [#2]

[#1] MSC Student, Master of Computer Science,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Head & Assistant Professor, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, 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, 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 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.

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.Among many well-known designs for cryptography based systems, the IP Security and the Secure Socket Layer are popularly supported and implemented in many systems and platforms.

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. The set of multiple paths between each source and its destination is determined in an online fashion.

Although excellent research results have been proposed for security-enhanced dynamic routing, many of them rely on the discovery of multiple paths.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 a dynamic routing algorithm to provide security enhanced data delivery without introducing any extra control messages\.

PROBLEM STATEMENT

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. Hence there is no proper method which can give guarantee for the data under dedicated path.

PURPOSE

Security has become one of the major issues for data communication over wired networks. Different from the past work on the designs of cryptography algorithms and system infrastructures, 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 without introducing extra control messages. An analytic study on the proposed

OBJECTIVE

- The objective of this work is to explore a security enhanced dynamic routing algorithm based on distributed routing information widely supported in existing wired networks.
- 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.
- DDR Algorithm should be easy to implement and compatible with popular routing protocols, such as the Routing Information Protocol (RIP) for wired networks.

SCOPE

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. Here we try to avoid the paths which is having any infected node and try to send the data in a alternate path which is not having any failed node.If this is implemented we can able to provide data integrity as well reduce a lot of delay in transmission.

2. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool, it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, ten next steps are to determine which operating system and language used for developing the tool. Once the programmers start building the tool, the programmers need lot of external support. This support obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into for developing the proposed system.

1) Efficient packet marking for large-scale IP traceback

AUTHORS: M. T. Goodrich

We present a new approach to IP traceback based on the probabilistic packet marking paradigm. Our approach, which we call randomize-and-link, uses large checksum cords to "link" message fragments in a way that is highly scalable, for the checksums serve both as associative addresses and data integrity verifiers. The main advantage of these checksum cords is that they spread the addresses of possible router messages across a spectrum that is too large for the attacker to easily create messages that collide with legitimate messages. Our methods therefore scale to attack trees containing hundreds of routers and do not require that a victim know the topology of the attack tree a priori. In addition, by utilizing authenticated dictionaries in a novel way, our methods do not require routers sign any setup messages individually.

2) Dynamic probabilistic packet marking for efficient IP traceback

AUTHORS: J. Liu, Z.-J. Lee, and Y.-C. Chung

Recently, denial-of-service (DoS) attack has become a pressing problem due to the lack of an efficient method to locate the real attackers and ease of launching an attack with readily available source codes on the Internet. Traceback is a subtle scheme to tackle DoS attacks. Probabilistic packet marking (PPM) is a new way for practical IP traceback. Although PPM enables a victim to pinpoint the attacker's origin to within 2–5 equally possible sites, it has been shown that PPM suffers from uncertainty under spoofed marking attack. Furthermore, the uncertainty factor can be amplified significantly under distributed DoS attack, which may diminish the effectiveness of PPM. In this work, we present a new approach, called dynamic probabilistic packet marking (DPPM), to further improve the effectiveness of PPM. Instead of using a fixed marking probability, we propose to deduce the traveling distance of a packet and then choose a proper marking probability. DPPM may completely remove uncertainty and enable victims to precisely pinpoint the attacking origin even under spoofed marking DoS attacks. DPPM supports incremental deployment. Formal analysis indicates that DPPM outperforms PPM in most aspects.

3) Detection and Localization of Network Black Holes

AUTHORS : J.Yates,A.Greenberg,A.C.Snoren

Internet backbone networks are under constant flux, struggling to keep up with increasing demand. The pace of technology change often outstrips the deployment of associated fault monitoring capabilities that are built into today's IP protocols and routers. Moreover, some of these new technologies cross networking layers, raising the potential for unanticipated interactions and service disruptions that the built-in monitoring systems cannot detect. In such instances, failures may cause data packets to be silently dropped inside the network without triggering any alarms or responses (e.g., the failure is not routed around). So-called "silent failures" or "black holes" represent a critical threat to today's rapidly evolving networks. In this paper, we present a simple and effective method to detect and diagnose such silent failures. Our method uses active measurement between edge routers to raise alarms whenever end-to-end connectivity is disrupted, regardless of the cause. These alarms feed localization agents that employ spatial correlation techniques to isolate the root-cause of failure. Using data from two real systems deployed on sections of a tier-I ISP network, we successfully detect and localize three known black holes. Further, we present simulation results demonstrating that our system accurately and precisely (both greater than 80% according to our metrics) localizes a variety of failures classes.

4) Single-link failure detection in all-optical networks using monitoring cycles and paths

AUTHORS: S.Ahuja,M.Krunz

In this paper, we consider the problem of fault localization in all-optical networks. We introduce the concept of monitoring cycles (MCs) and monitoring paths (MPs) for unique identification of single-link failures. MCs and MPs are required to pass through one or more monitoring locations. They are constructed such that any single-link failure results in the failure of a unique combination of MCs and MPs that pass through the monitoring location(s). For a network with only one monitoring location, we prove that three-edge connectivity is a necessary and sufficient condition for constructing MCs that uniquely identify any single-link failure in the network. For this case, we formulate the problem of constructing MCs as an integer linear program (ILP). We also develop heuristic approaches for constructing MCs in the presence of one or more monitoring locations. For an arbitrary network (not necessarily three-edge connected), we describe a fault localization technique that uses both MPs and MCs and that employs multiple monitoring locations. We also provide a linear-time algorithm to compute the minimum number of required monitoring locations. Through extensive simulations, we demonstrate the effectiveness of the proposed monitoring technique

3. EXISTING SYSTEM

In the existing system there was no method which can send the data packets under random path by choosing one packet at a time.All the existing routing algorithms try to follow the single route for sending all the packets from source to destination and one route is failed then it will choose alternate route and all the packets move in that route.Hence in the existing system it is very complicated for the end users to send data under dedicated paths.

LIMITATION OF EXISTING SYSTEM

The following are the main limitations of the existing system. They are as follows:

1. All the existing systems use general routing algorithms for sending the data under dedicated path.
2. The data will be divided into packets and all the data will be send under dedicated path.
3. If there is one path failed the data will be send from alternate path.
4. In the existing system there was huge time delay for sending the data from one system to another system.
5. It is exhaustive

4. PROPOSED SYSTEM

In the proposed system we try to use dynamic routing method under randomization process so that all the data will not be send under single path,they will be send randomly through all the paths.The data will be choose one packet under one path and there will be no traffic or delay during the transfer.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system, they are as follows:

1. It is cost effective
2. This will guarantee the data packets under attack mode also
3. There will be less time delay for sending the packets from source to destination

This is highly secure for sending the data under the multi paths.

5. SOFTWARE PROJECT MODULES

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. The application is divided mainly into following 3 modules. They are as follows:

1. *Topology Construction*
2. *Random Path Selection*
3. *Message Transmission*

Now let us discuss about each and every module in detail as follows:

5.1 TOPOLOGY CONSTRUCTION MODULE

In this module we construct our topology structure. Here we use mesh topology because of its unstructured nature. Here we using sockets for connecting the nodes.

5.2 RANDOM PATH SELECTION MODULE

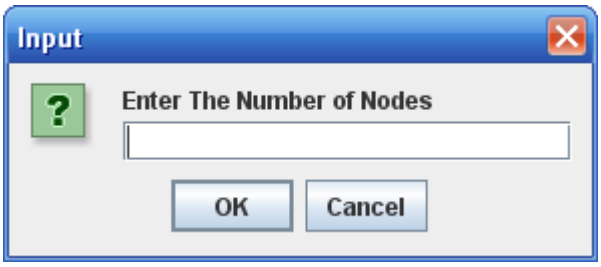
By Applying random selection algorithm we choose a path from routing table.For find a new route here we use DDRA algorithm.Here we try to choose distinct paths for sending data from one node to another node.

5.3 MESSAGE TRANSMISSION MODULE

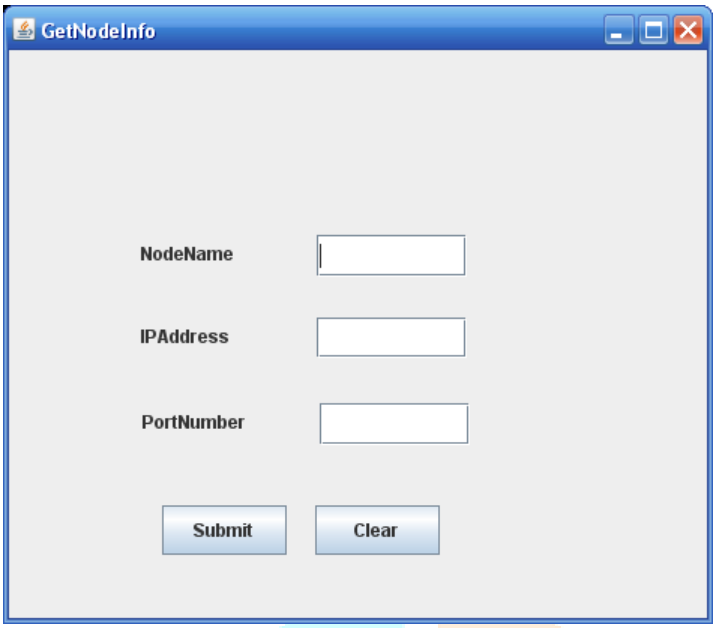
Here we transmit the message from source to destination. For each transmission we choose a random path, in that only the packet is transmitted.

6. RESULTS (OUTPUT SCREENS)

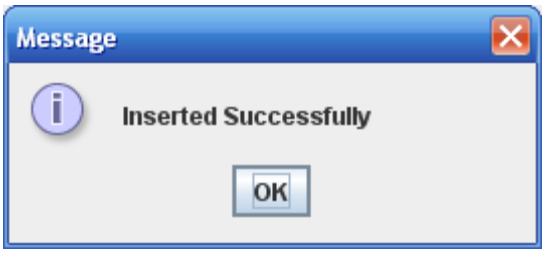
Get Node Number



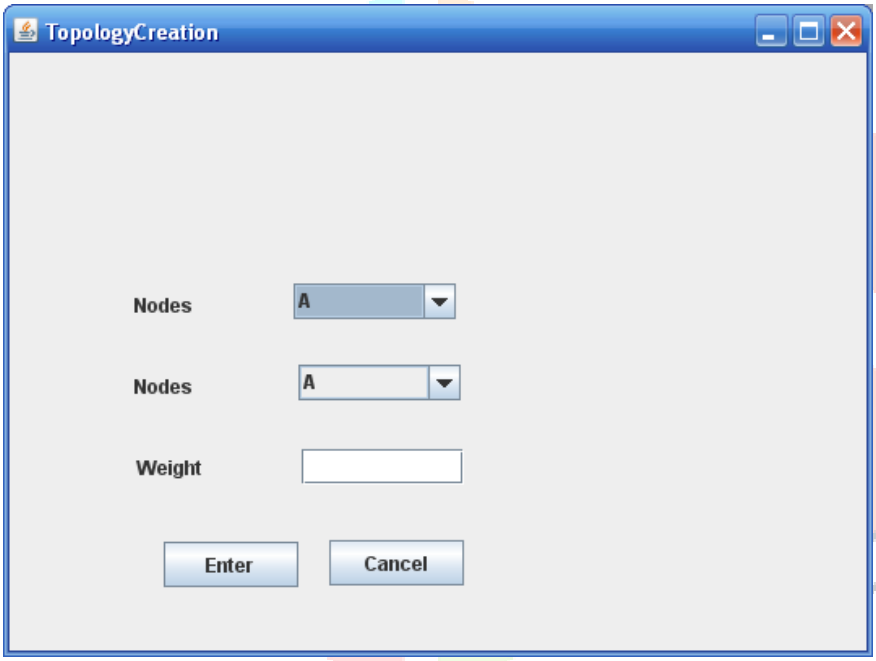
Get Node Detail

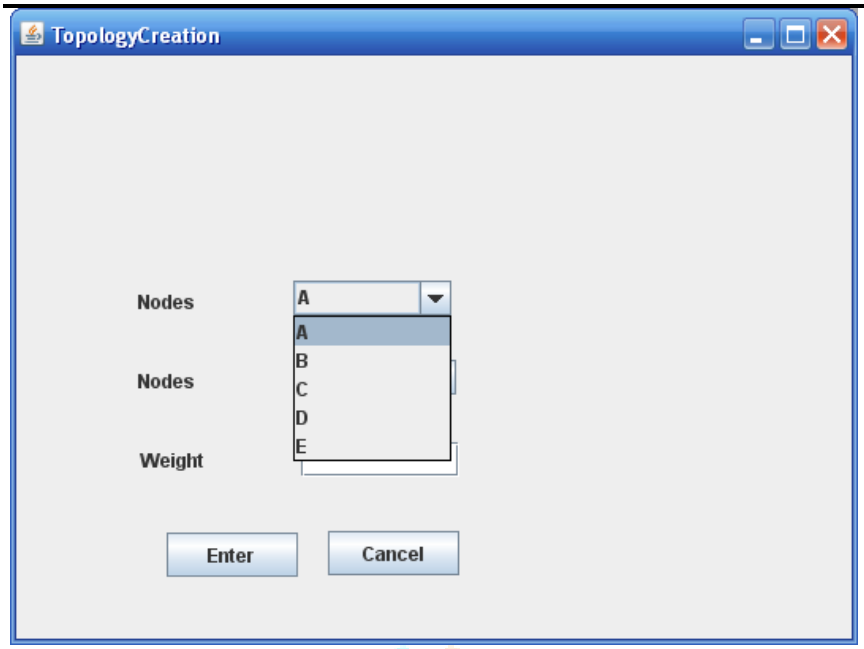


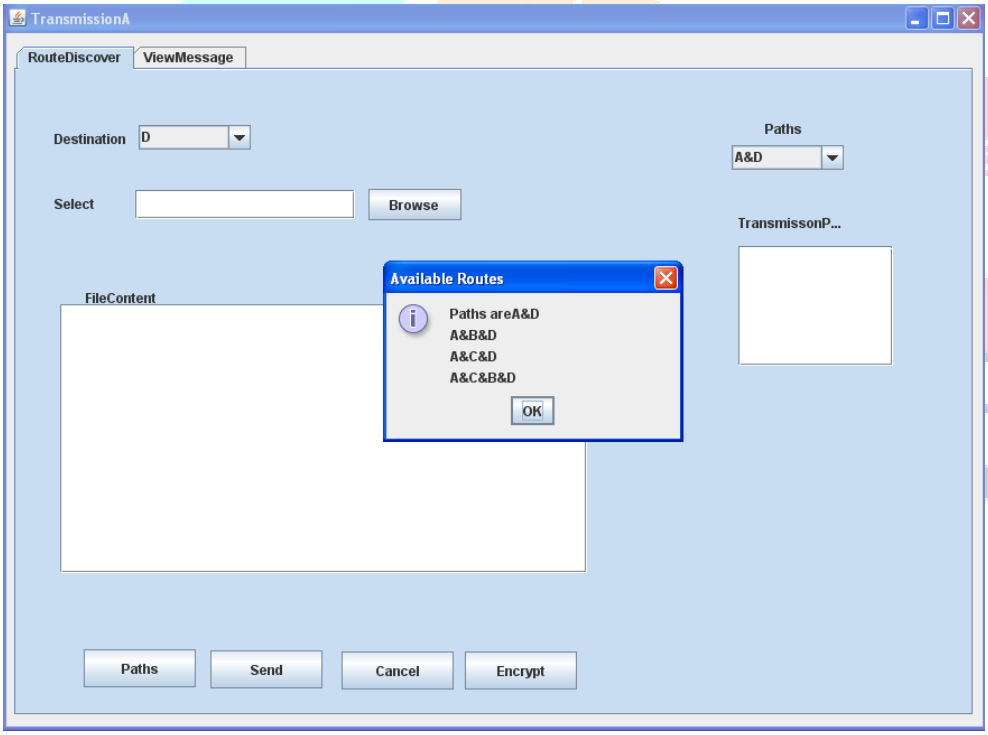
Node registration

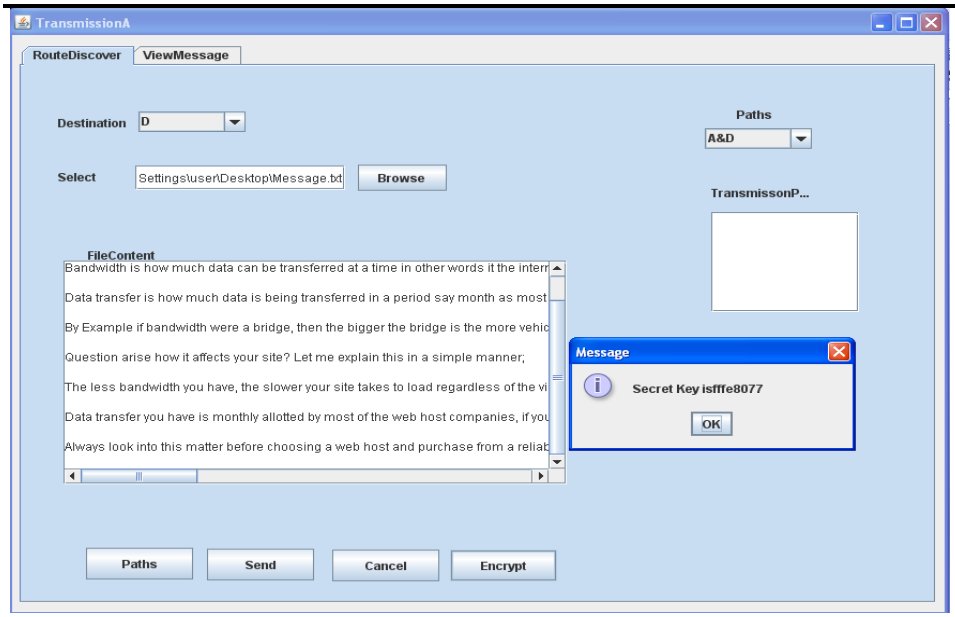


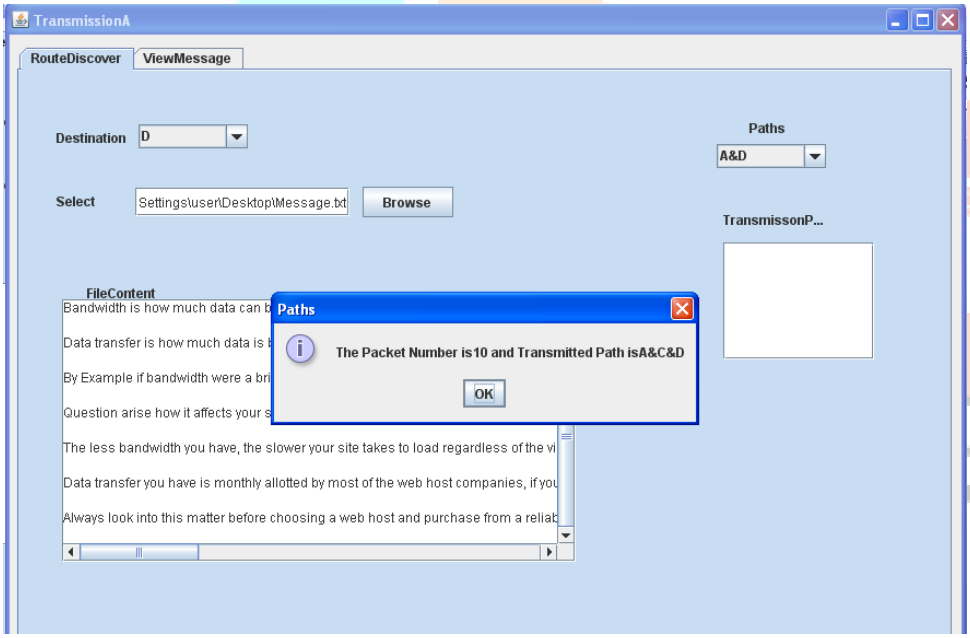
Topology Structure

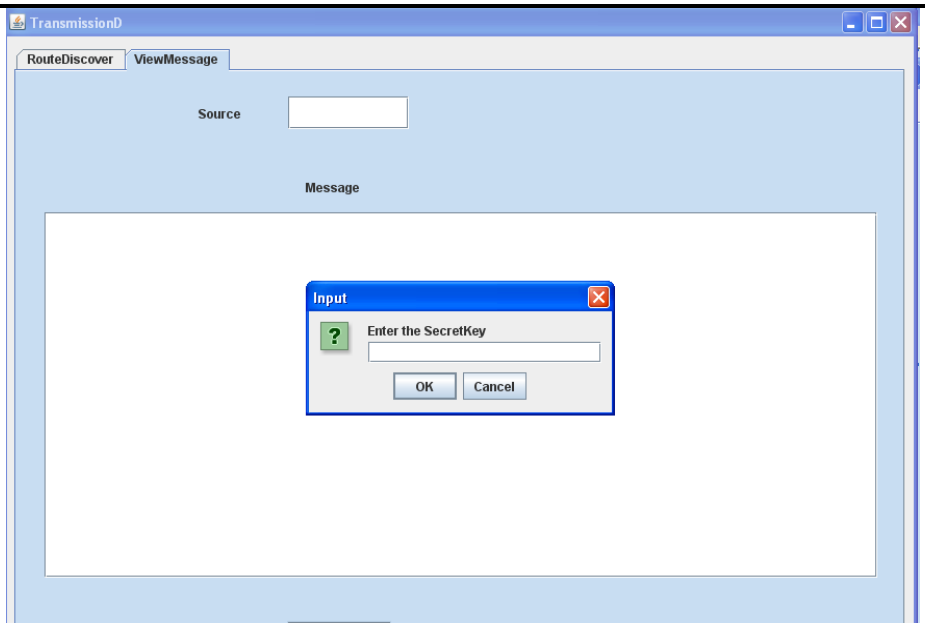


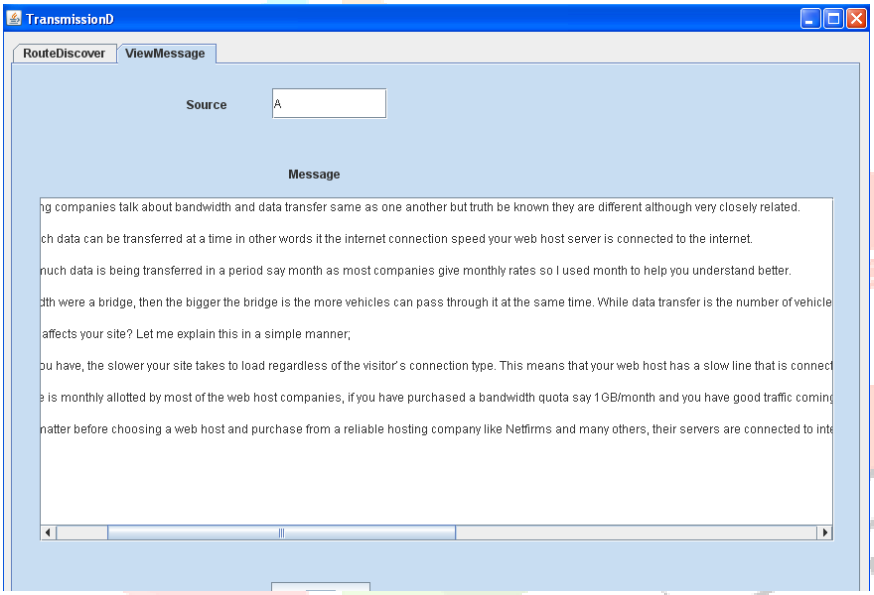

TopologyCreation
Nodes
A
A
B
C
D
E
Nodes
Weight
Enter
Cancel


TransmissionA
RouteDiscover
ViewMessage
Destination
D
Select
Browse
FileContent
Paths
A&D
TransmissonP...
Available Routes
Paths areA&D
A&B&D
A&C&D
A&C&B&D
OK
Paths
Send
Cancel
Encrypt


TransmissionA
RouteDiscover
ViewMessage
Destination
D
Paths
A&D
Select
Settings\user\Desktop\Message.txt
Browse
TransmissonP...
FileContent
Bandwidth is how much data can be transferred at a time in other words it the interr
Data transfer is how much data is being transferred in a period say month as most
By Example if bandwidth were a bridge, then the bigger the bridge is the more vehic
Question arise how it affects your site? Let me explain this in a simple manner;
The less bandwidth you have, the slower your site takes to load regardless of the vi
Data transfer you have is monthly allotted by most of the web host companies, if you
Always look into this matter before choosing a web host and purchase from a reliab
Message
Secret Key isfffe8077
OK
Paths
Send
Cancel
Encrypt


TransmissionA
RouteDiscover
ViewMessage
Destination
D
Paths
A&D
Select
Settings\user\Desktop\Message.txt
Browse
TransmissonP...
FileContent
Bandwidth is how much data can b
Data transfer is how much data is b
By Example if bandwidth were a bri
Question arise how it affects your s
The less bandwidth you have, the slower your site takes to load regardless of the vi
Data transfer you have is monthly allotted by most of the web host companies, if you
Always look into this matter before choosing a web host and purchase from a reliab
Paths
The Packet Number is10 and Transmitted Path isA&C&D
OK





7. CONCLUSION

This proposed work has 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.

8. 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