Volume 3, Issue 5, May 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Dynamic Routing with Security Consideration Using DES Algorithm

Monisha M P[1], Priyanka C A[2] , Gayathri P N[3],T.Suresh[4]

[1,2,3,4]*Department of Computer Science & Engineering, BITM, Bellary, India.*

[5]*Asst. Prof Department of Computer Science & Engineering, BITM, Bellary, 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, 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. The Algorithm used is Data Encryption Standard(DES).

Keywords— Cryptography, Dynamic routing, Routing information protocol and Distance vector protocol

1.INTRODUCTION

Earlier technologies used static routing mechanisms there was no reliability of delivering the data. Project proposes a distance vector based algorithm for dynamic routing to improve data transmission with security. Data Encryption Standard algorithm can randomize delivery paths and choose the best path for data transmission. It avoids transmitting two consecutive packets on the same link. Algorithm randomizes delivery paths and chooses the best path for data transmission.

II.RELATED WORK

The following are the related works.

Becker et al. [1]. Derived lower bounds for contributory key generation systems for the gossip problem and proved them realistic for Diffie-Hellman (DH) based protocols.

Steiner et al. [2]. Proposed the basic DH distribution [3] extended to groups from the work. Where three new protocols are presented: GDH.1-2-3.

Ingemarsson et al. [4] Presented another efficient DH-based KA scheme, “ING”, logically implemented on a ring topology.

Burmester et a. [5]. Introduced a new GDH protocol, denoted as BD (very efficient in terms of round complexity)

Kim et al. [6]. Proposed another hybrid DH-based KA scheme is TGDH introduced is an efficient protocol that blends binary key trees with DH key exchanges.

Katz et al. [7] Proposed to improve on existing KA schemes either by rendering them more scalable or by enhancing their security against various kinds of attacks. Still, the described algorithms are implemented on logical graphs or address wire-line networks.

Lou et al. [11] 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.

III. PROPOSED WORK

- Dynamic routing algorithm that could randomize delivery paths for data transmission.
- The objective of this work is to explore a security enhanced dynamic routing algorithm based on cryptography algorithms and 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.
- Overhead is minimized, because dynamic routing mechanism is implemented here, there is no fixed path, router dynamically selects next minimum cost path if current path fails

Figure 1 shows the relationship between different components of system. The overall logical structure of the project is divided into processing modules and conceptual data structure is defined as Architectural Design. It shows a Top-down approach.

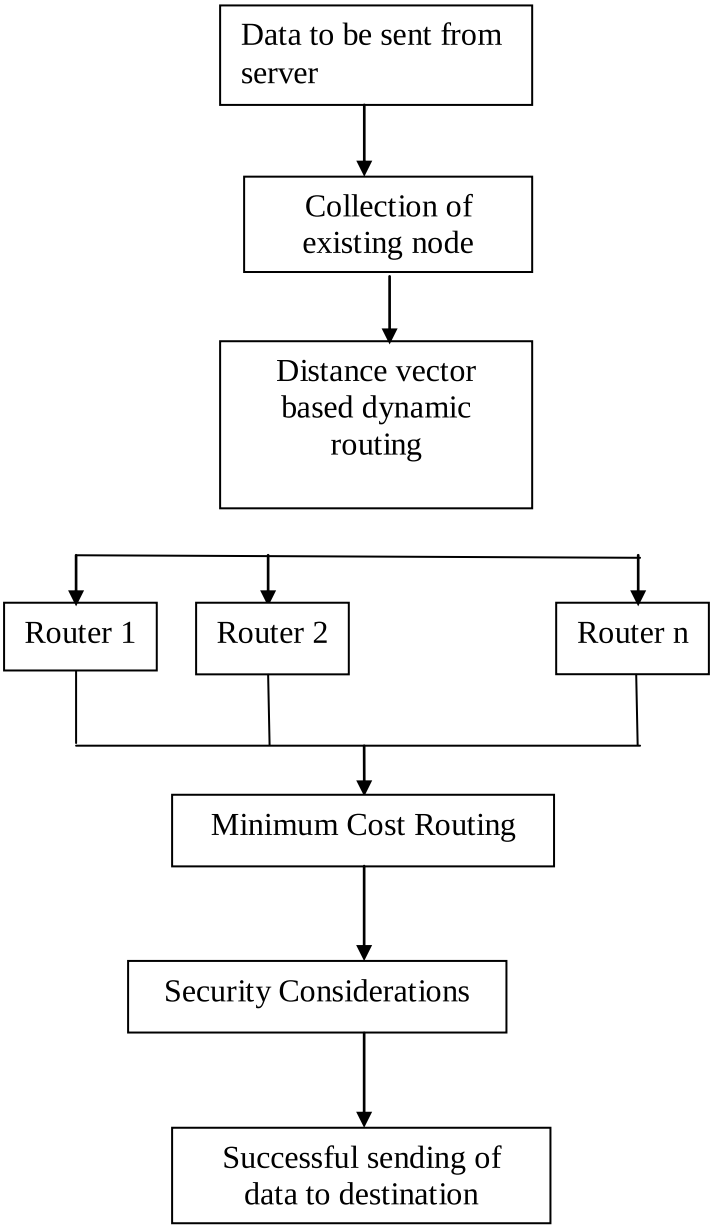

Data to be sent from server
Collection of existing node
Distance vector based dynamic routing
Router 1
Router 2
Router n
Minimum Cost Routing
Security Considerations
Successful sending of data to destination

Figure 1: Basic block diagram

DES Algorithm:
DES takes on input a 64-bit plaintext data block and 56-bit key (with 8 bits of parity) and outputs a 64-bit cipher text block.

1. The plaintext block is subject to an Initial Permutation to shift the bits around.
2. The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
3. The plaintext and key are processed in 16 rounds consisting of:
    1. The key is split into two 28-bit halves.
    2. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
    3. The halves are recombined and subject to a Compression Permutation to reduce the key from 56 bits to 48 bits. This Compressed Key is used to encrypt this round's plaintext block.
    4. The rotated key halves from step 2 are used in next round.
    5. The data block is split into two 32-bit halves.
    6. One half is subject to an Expansion Permutation to increase its size to 48 bits.
    7. Output of step 6 is exclusive-OR'ed with the 48-bit compressed key from step 3.
    8. Output of step 7 is fed into an S-box, which subsitutes key bits and reduces the 48-bit block back down to 32-bits.
    9. Output of step 8 is subject to a P-box to permute (scramble) the bits.
    10. The output from the P-box is exclusive-OR'ed with the other half of the data block.
    11. The two data halves are swapped and become the next round's input.

4. After 16 rounds, the resultant chipertext is subject to a Reverse Initial Permutation. The output is the cipher text block.

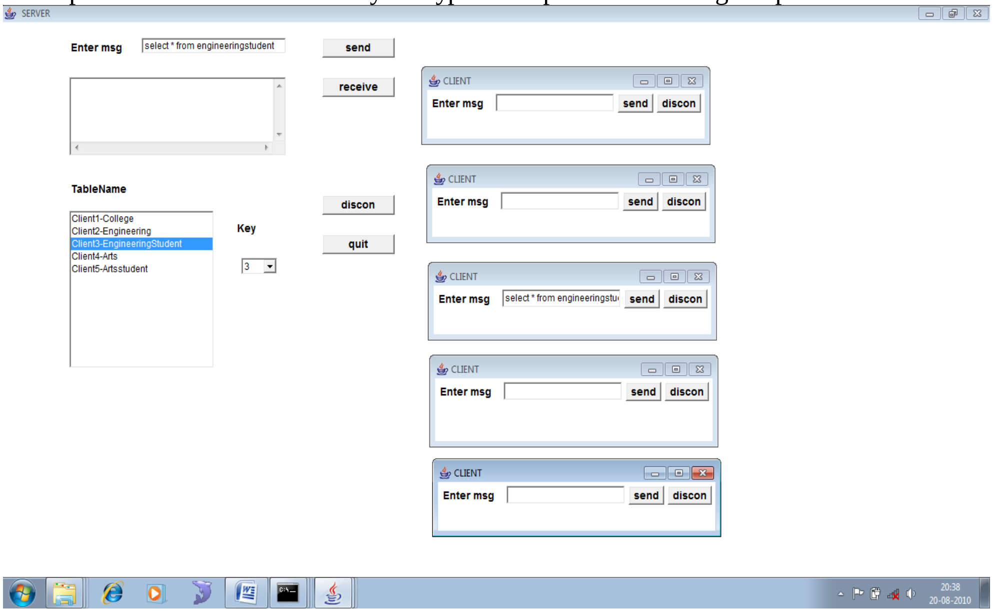
IV.EXPERIMENTAL RESULTS

INPUT:

We considered a data and few tables those are stored in a database. Each table had some data which was given to client from server which includes few queries which are sent to client in encrypted form with secret key.

OUTPUT:

Server process the query receive in server window. The process of decryption starts after getting the cipher text from server. It takes the cipher text and same secret key decrypt it and produces the original plain text



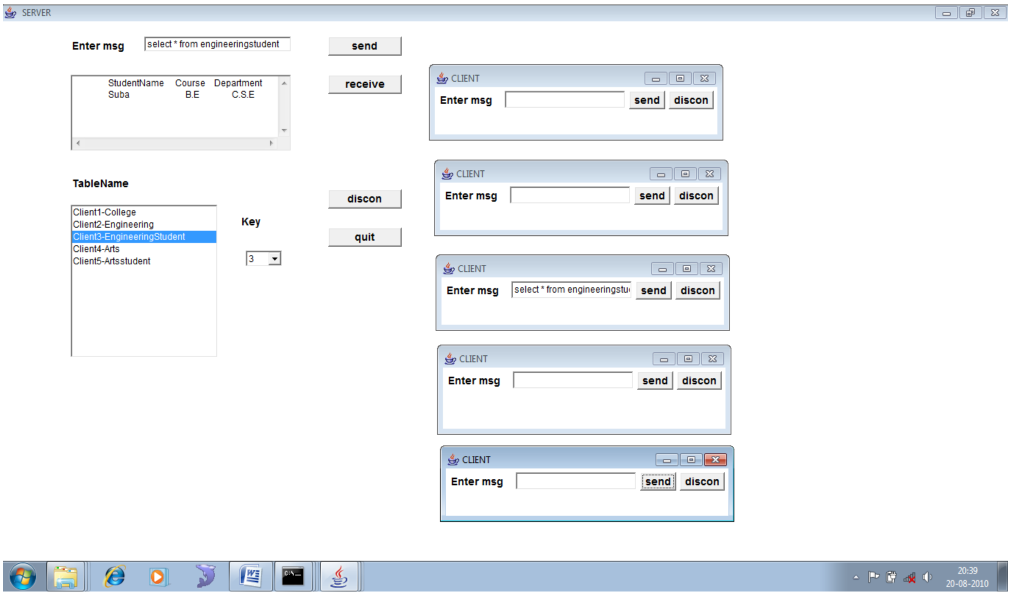
Enter msg: select * from engineeringstudent

TableName:
Client1-College
Client2-Engineering
Client3-EngineeringStudent
Client4-Arts
Client5-Artsstudent

Key: 3

CLIENT — Enter msg: select * from engineeringstu

20:38
20-08-2010



Enter msg: select * from engineeringstudent

StudentName Course Department
Suba B.E C.S.E

TableName:
Client1-College
Client2-Engineering
Client3-EngineeringStudent
Client4-Arts
Client5-Artsstudent

Key: 3

CLIENT — Enter msg: select * from engineeringstu

20:39
20-08-2010

V. CONCLUSIONS AND FUTURE SCOPE

This project proposed a security-enhanced dynamic routing algorithm based on distributed routing information widely supported in existing wired and wireless networks. The main aim was the randomization of delivery paths for data transmission to provide considerably small path similarity of two consecutive transmitted packets. The proposed algorithm is easy to implement and compatible with popular routing protocols such as the Routing Information Protocol (RIP) for wired and Destination Sequenced Distance Vector protocol(DSDV) for wireless networks, over existing infrastructures. We proposed a distance vector based algorithm for dynamic routing chooses all the possible paths to reach the destination. Among these paths it chooses the best path and sends the packets through router in different paths randomly. So that it improves the security of data transmission over networks. We implemented DES algorithm to provide security for data transmission.

ACKNOWLEDGMENT

We wish to thank Asst.Prof.T.Suresh for many insightful discussions that contributed to the ideas of this paper.

REFERENCES

[1] K. Becker, U. Wille, “Communication Complexity of Group Key Distribution,” *Proc.5th ACM Conference on Computer & Communicatios Security*, pp. 1-6, San Francisco, CA, November 1998.

[2] M. Steiner, G. Tsudik, M. Waidner, “Diffie-Hellman Key Distribution Extended to Groups,” *3rd ACM Conference on Computer & Communication Security*, pp. 31-37 ACM Press, 1996.

[3] W.Diffie, M.Hellman,”New directions in cryptography”, *IEEE Trans. On Information Theory*, 22(1976), 644-654.

[4] I. Ingemarsson, D.Tang, C.Wong. “A Conference Key Distribution System”, *IEEE Trans. on Information Theory*, 28(5): 714-720, Sept. 1982

[5] M.Burmester, Y.Desmedt. “A Secure and Efficient Conference Key Distribution System”, *Advances in Cryptology–EUROCRYPT’94, Lecture Notes in Computer Science.* Springer – Verlag, Berlin, Germany.

[6] Y. Kim, A. Perrig, G. Tsudik, “Simple and Fault Tolerant Key Agreement for Dynamic Collaborative Groups,” *Proc. 7th ACM Conf. on Computer and Communication Security (CCS 2000),* pp. 235-244

[7] J. Katz, M.Yung, “ Scalable Protocols for Authenticated Key Exchange“, *Advances in Cryptology - EUROCRYPT’03, Springer-Verlag,* LNCS Vol 2729, pp. 110-125, Santa Barbara, USA

[8] W. Lou and Y. Fang, “A Multipath Routing Approach for Secure Data Delivery,” *Proc. IEEE Military Comm. Conf. (MilCom),* 2001.