Review on Data Transmission using Dynamic Routing and Reverse Encryption Algorithm

Kaustubh Satpute
Dept. of CSE
DMIETR, Wardha, India
kaustubh2008satpute@gmail.com

Charudatt Satpute
P. G. Dept. of CS
SGBAU, Amravati (MH), India
charu861991@gmail.com

Gajanan Tikhe
Dept. of IT
DMIETR, Wardha, India
gajanan_tikhe@yahoo.com

Abstract: In day to day life security has become major issues for data transmission over wired and wireless Network. Due to the transmission of valuable data over the network, security is the big issue for the information technology sector. For the data transmission in network may not be secure and is defenceless to many threats. The various security mechanisms have been incorporated in the recent times, which greatly improve the data security. In this paper the new way of transmission, the information using a routing algorithm such as DSDV or AODV with encryption algorithm (i.e. Reverse Encryption Algorithm (REA)) improve the data security over network.

Keywords: *Routing Protocol, Data Transmission, Encryption, DSDV, AODV.*

*****

I. INTRODUCTION

In last few years, various security mechanism have been proposed to improve the security of data communication over computer networks. In current scenario secure data transmission includes the designs of encryption/decryption algorithms and infrastructures with the help of secured data routing methods.

The alternative for secure 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 and also provide the cryptographic security to hide the original data from the unwanted user.

II. LITERATURE SURVEY

Data transmission

Data transmission is the physical transfer of Data (a digital bit stream) over a point-to-point or point-to-multipoint transmission medium. The exchange of data between two devices through a transmission medium is Data Communication. The data is exchanged in the form of 0's and 1's. The transmission medium used is wire cable or wireless network. In data communication different communication mediums use i.e. fire optical cable, twisted pair cable, radio frequency etc.

Destination-Sequenced Distance Vector routing (DSDV)

Destination-Sequenced Distance-Vector Routing (DSDV) routing Protocol scheme maintain the information in table form based on the Bellman-Ford algorithm for ad hoc mobile networks. Each row in the routing table contains a sequence id, the sequence id are generally even if a link is present; else, an odd number is used. The id is generated by the destination, and the emitter needs to send out the next update with this id. Routing information is distributed between nodes by sending full dumps infrequently and smaller incremental updates more frequently [8, 9].

Ad hoc On Demand Distance Vector (AODV)

The Ad hoc On Demand Distance Vector (AODV) is design for ad hoc mobile networks. It create route when the connection required to communicate by source nodes. AODV uses sequence id to ensure the newness of routes. It

is loop-free, self-starting, and scales to large numbers of mobile nodes [6]

Encryption/Decryption Algorithm

Cryptography is art to hide the original text into coded language. The coded message is called encrypted text it is unintelligible message to outsider. There are various technique to convert or transform the original text into encrypted form.

Encryption algorithm

"Reverse Encryption Algorithm (REA)", because of its simplicity and efficiency. Reverse Encryption Algorithm limits the added time cost for encryption and decryption. In this section we provide a comprehensive yet concise algorithm [10].

Our new Reverse Encryption Algorithm is a symmetric stream cipher that can be effectively used for encryption of data. It takes a variable-length key. The REA algorithm encipherment and decipherment consists of the same operations, except the two operations:

1) Added the keys to the text in the encipherment and removed the keys from the text in the decipherment.

2) Executed divide operation on the text by 4 in the encipherment and executed multiple operation on the text by 4 in the decipherment. We execute divide Operation by 4 on the text to narrow the range domain of the ASCII code table at converting the text [10, 11].

The steps of the Reverse Encryption Algorithm

1. Input the text and the key.
2. Add the key to the text.
3. translate the previous text to ASCII code.
4. translate the obtain ASCII code to binary data.
5. Find out One's complement of the previous binary data.
6. Gather each 8 bits from the previous binary data and obtain the Decimal value from it.
7. Divide the previous Decimal value by 4.
8. Obtain the ASCII code of the previous result divide and put it as one character.
9. Obtain the remainder of the previous divide and put it as a second character.
10. Return encrypted text.

III. SYSTEM ARCHITECTURE

The secure data transmission use routing techniques and cryptography based algorithm to transfer information 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

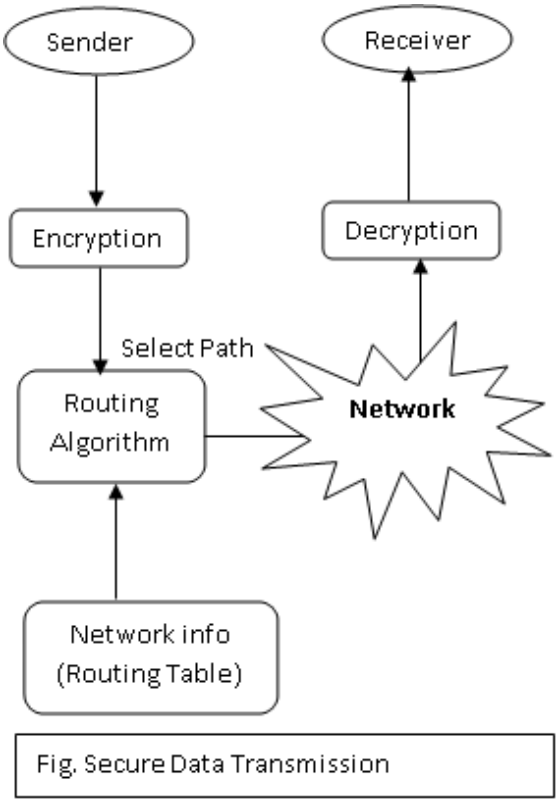

Fig. Secure Data Transmission

IV. CONCLUSION

A secure data transmission using routing algorithm and cryptography widely supported in existing networks. This system is easily implement with popular existing routing protocols, such as AODV and DSDV, over existing infrastructures. This system has advantage such as,

improved data transmission and security over traditional systems. Further it can be applied to wireless network.

REFERENCE

[1] George Aggelou,"Mobile Ad Hoc Networks", 2nd edition, Mc GRAW Hill professional Engineering,2004.

[2] T.H. Cormen, C.E. Leiserson, and R.L. Rivest, Introduction to Algorithms. MIT Press, 1990.

[3] I. Gojmerac, T. Ziegler, F. Ricciato, and P. Reichl, "Adaptive Multipath Routing for Dynamic Traffic Engineering," Proc. IEEE Global Telecommunications Conf. (GLOBECOM), 2003.

[4] C. Hopps, Analysis of an Equal-Cost Multi-Path Algorithm, Request for comments (RFC 2992), Nov. 2000.

[5] C. Kaufman, R. Perlman, and M. Speciner, Network Security—PRIVATE Communication in a PUBLIC World, second ed. Prentice Hall PTR, 2002

[6] Ian D. Chakeres and Elizabeth M. Belding-Royer. "AODV Routing Protocol Implementation Design." Proceedings of the International Workshop on Wireless Ad Hoc Networking (WWAN), Tokyo, Japan, March 2004

[7] H. Brown, Considerations in Implementing A Database Management System Encryption Security Solution, A Research Report presented to The Department of Computer Science at the University of Cape Town, 2003.

[8] Chin-Fu Kuo, Ai-Chun Pang, and Sheng-Kun Chan, Dynamic Routing with Security Considerations, ieee transactions on parallel and distributed systems, vol. 20, no. 1, January 2009

[9] Perkins, Charles E. and Bhagwat, Pravin (1994). "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers"

[10] Ayman Mousa, Elsayed Nigm, Sayed El-Rabaie, Osama Faragallah "Query Processing Performance on Encrypted Databases by Using the REA Algorithm" International Journal of Network Security, Vol.14, No.5, PP.280-288, Sept. 2012

[11] Priti V. Bhagat, Kaustubh S. Satpute, "Reverse Encryption Algorithm - A New Approach For Encryption" SICETE