An Improved Link Encryption Protocol for Secure Data Transmission over Public Network

N.Kannan, K.Ramkumar

***Abstract*— Nowadays security is a major problem in around the world. Particularly in communication area, data is transmitting over public networks, these networks have lack security and are vulnerable. Cryptography is important technologies that are used to preserve data security and integrity. Encrypt and decrypt are important security technologies in data transmission through the public networks. These technologies used to preserve data security and privacy then reduce information theft in the public networks. The existing routing protocol is incapable of providing secure data transmission over public networks.**

Our research team to implement Group Key Management Protocol (GKMP). In this paper to create validate group member and distribute the key to all the member of groups. We propose a group key management protocol, these protocol only allows the validate group member to access data in public networks and then create and distribute the key.

A secure key management protocol needs a number of supporting functions for example military environment. The major support functions are security management and network group management. The group member function interacts with other management function in the network to provide the GKMP with group membership lists and group controller. We implement a prototype of Group key management protocol on the NS-3 simulator.

***Index Terms*— Cryptography, Encryption, Decryption, Group Key Management Protocol (GKMP), NS-3**

I. INTRODUCTION

The internet is a major communication media in around the world. Infact public networks are less secure than private networks. The transmitting secure data over public network having lack security and data privacy. This networks is allows hacker to read and modify original data.

Because secure data travels through the public networks. People are demand data security and data privacy for their sensitive data. In other hand to use various security protocols such as MACsec [1], Point to Point Tunneling protocol (PPTS) [2], Secure Socket Layer (SSL) [3], Internet Protocol Security (IPSec) [4], this types of protocols implemented to provide data security. These methods can provide data security only in end to end hosts.

Because the internet comprises millions of networks that are connected by routers. Most of the data travels through these networks routers. Regular routers are incapable of providing data security. Our research team to implemented link encryption protocol by using group router .there router to solve the problem of key distribution and reduce information hacking in public networks. group member function it's consists of following manner, first one is validate group member, then create key for group member using group controller and then routing and replication.

Manuscript received March 20, 2015.

N.KANNAN (PG Scholar) is pursuing final year M.TECH in Computer Science and Engineering at Bharathiyar College of Engineering And Technology

K.RAMKUMAR working Assistant Professor in Department of Computer Science And Engineering at Bharathiyar College of Engineering And Technology

II. PRIOR WORK AND MOTIVATION

Our knowledge there is no proper scheme to issue of security solution is implemented in public networks. Because secure data travels through the internet's. To this end, various security protocols to implement such as MACsec [1], Point to Point Tunneling protocol (PPTS) [2], Secure Socket Layer (SSL) [3], Internet Protocol Security (IPSec) [4], these types of protocols implemented to provide data security. These methods can provide data security only in end to end hosts. The prior link layers are explicitly of public network and very inefficient. In other hand TCP/IP is the major concept used in internet data transmission protocol. The TCP/IP was introduce to provide a connection between two end hosts .when multiple data buffering mechanism lead to time delays.

The proposed protocol to perform a link encryption with help of group member function. These functions to check validate group member and create and distribute the key to validate group member. This protocol in order to generate the key among neighbors and exchange key through public networks.

III. LINK ENCRYPTION AND GROUP ESTABLISHMENT

Link encryption is an approach to security that encrypts and decrypts all traffic at each end hosts of a communication lines. Each vulnerable communication link is equipped on both with a Encryption Devices. Link encryption is the data security process of encrypting data as it is transmitting between two points. Information, which is original text in the host server, is encrypted when it leaves the next, decrypt at the next link. Each and every link having same key in validate group member .this process repeat until the data has reached the recipient.

3.1 Group Establishment

To establishment group member of host that share a key must validate all intended recipients have permission to join the group and distribute the key to all validate group member. The group establishment is consists of following manner.1.Create group and maintaining the validate group member.2. Create and distribute the key through the group controller.

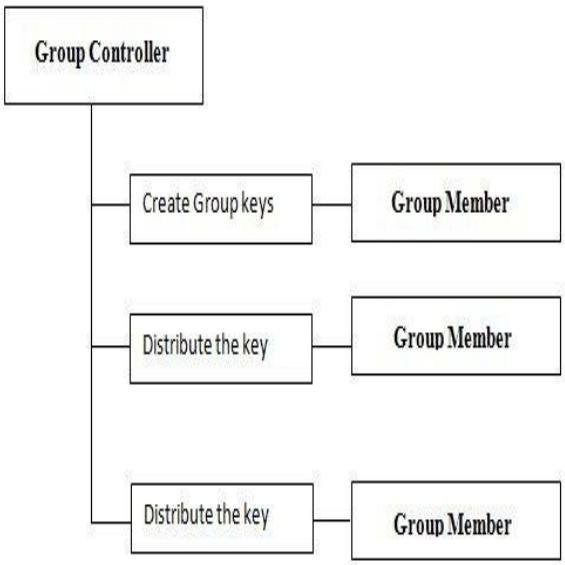

Fig: 1 Group Establishment

IV. SYSTEM ARCHITECTURE

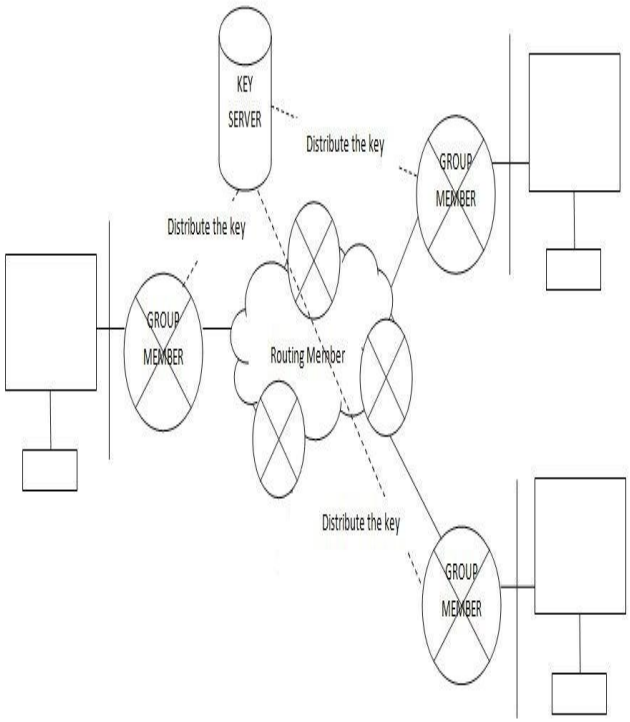

Fig: 2 Architecture of Group Establishment

The system architecture is a process of establish a members of group, that share a key and verify that all neighbors and Recipients have permission to join the group. Distribute the key to all validate members of group. This process consists of two phases, such as creation and distribution of the key through the key server. Group establishes is a process of "Create group".

The group controller verify all are the group member have a validate Group membership. Next then controller to create a key. Then that key to distribute to the group member. After they distribute the group member to process either in encrypt and decrypt the devices. After creation of key, other end members contact the group controller, a key is created, member permissions are validate.

V. DATA FLOW DIAGRAM

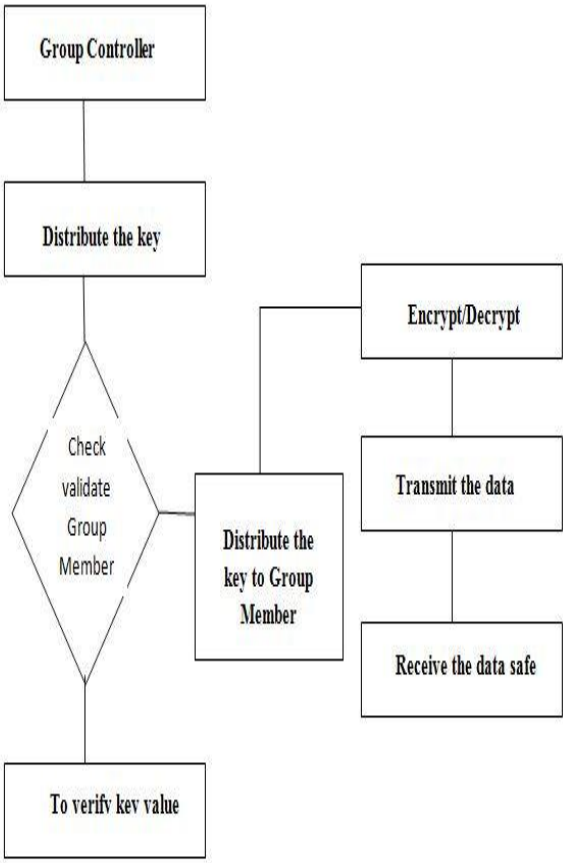

Fig: 3 Data Flow Diagram

The Fig: 3 Data flow Diagram for to establish the group member and distribution of key to validate group member through group controller. The Group controller is an approach to distribute the keys to validate group member. Each and every Group member of the communication link is either encrypted or decrypted the devices for secure data communication in public networks.. Then send secure data to validate group member. Other wise to block the unauthorized member in communication lines and verify the key values.

VI. CONCLUSION AND FUTURE WORK

In this paper we presented a secure authenticated group key exchange algorithm that operates for large group member. We have extended the work encrypted/decrypted each group member .The advantages of this algorithm is consists of following. First one is to create validate group member and then distribute the key to authorized group member. It is a provide secure Algorithms for data transmission through public networks.

Our future work will focus on researching security mechanisms that allow greater scability, extended network life time and dynamic node joining.

Acknowledgments

We are very grateful to Krishnakumr for his helpful discussion with us and his suggestions that helped improved the paper. We would also like to thanks the anonymous reviewers for their comments and suggestions.

REFERENCES

[1]. J.Alves-Foss "*An Efficient Secure Group Key Exchange Algorithm For Large And Dynamic Group".* Technical Report CSDS-99-08, center for secure and dependable software, University of Idaho, 1999.
[2]. Hadia M.S, Hennatoy, AlaaE.A.Omar "*Link Encryption Algorithm Proposed Stream Cipher Algorithm*", Research development center, Cairo, Eggpt, 2014.
[3]. Ragitha Tennekoon "*Per Hop Data Encryption Protocol For Transmitting Data Securely Over Public Networks"*. Department of system design, Keio University, 2014
[4]. Freier, A.Karlton,p.,and kocher.,"*The Secure Sockets Layer Protocol Version 3.0"*,IETFRFC 6101,2011
[5]. Dierks,T," *Transport Layer Security Protocol", Version1.2",*IETF RFC 5246,2008.
[6]. Hamzeh, k.et al*," Point-To-Point Tunneling Protocol",* IETF RFC 2637, 1999
[7].Ylonen.T *"The secure shell Transport layer protocol*",IETF RFC 4253,2006
[8].Harris.S, CISSP All-in-one Exam Guide, McGraw-Hill Companies,2008
[9].DARPA Internet program,"*Transmission Contro; Protocol*",IETF RFC 793,1981:http://www.ietf.org/rfc/rfc793.txt

.

N.KANNAN (PG Scholar) is pursuing final year M.TECH in Computer Science and Engineering at Bharathiyar College of Engineering And Technology

K.RAMKUMAR working Assistant Professor in Department of Computer Science And Engineering at Bharathiyar College of Engineering And Technology