International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 4, April - 2014

Long Lived Self-Healing Group Key Distribution Scheme.

E. Kamalapriya
Computer Science Engineering
Saveetha University

J. Kavipriya
Computer Science Engineering
Saveetha University

Guide: Mrs. Rathi
Assistant Professor,Sse.

***Abstract*— Long lived self-healing group key group key distribution scheme is for one-to-one communication to establish privacy in communication between one manager and any one of the group members in a single network. Selective key distribution algorithm is used to select one particular key from the set of keys by which we can send our information to the receiver. In this we are using SHA-1 and Hash based technique and Self-healing technique. The Self-healing technique is used to retrieve the key and to generate the new key when the key is misplaced. Group key distribution is a scheme that is used to select a particular key in which we want to send our message.**

Keywords*— *Safety, Unicast communication, Cryptographic Protocol, Key distribution, Self-Healing.

I. INTRODUCTION

Long lived Self-healing distribution scheme is mainly used for the greatly personal communication between one team member and the other one in a much secured way. It is the secured unicast communication within the systems in single network.Each members or users in a group will be given a common key through which the message will be send to each individual in the group.

Every user belong to the group reckon the group key using the information or Private message. If they have lost the transmitted message means the user can still retrieve the group key by using the information or a message that arrives at the beginning with the need of additional transmission from the sender. This kind of approach reduces the gash or damage of the personal information in a unicast communication and also the network traffic.

A. Our Contribution

The main aspiration of this paper is to give clarity to our readers about the betterment in the field of Long lived self-healing key distribution scheme.It will be chiefly useful for the users as it describes about the basic building blocks of the system which are not been done in the paper. It also enclose a deep Security and efficiency critique and also point out the issues which are not been solved by the authors in the paper. We introduce a three-dimensional classification, based on each aspect of the scheme separately, which allows for more flexibility.Communications security in this schemeis achieved by encrypting the message and authentication using shared symmetric secret group key. There are two keys used in this type of communication. In this scheme, public key is used for encryption of the message and the private key is used for decryption of the message.We were also include the description of few broken schemes which are been explained in the original papers to explain about the insecure mechanism in that papers. We trust that researchers can avoid getting repeating mistakes in their upcoming research.

This scheme describe about the property of self-healing group key distribution scheme and also tells how data is send in a secured way. That is this scheme describes about how the secured communication is done in a network. Many schemes are introduced before based on the security for the communication, but almost none of the scheme is used for the very large scale, but this scheme is suitable for very large Wireless Sensor networks in the large scale.

***B**.Applications:*

This Long lived self-healing group key distribution scheme is used in the unicast commnication in the single network over a broadcast channel such as in wireless sensor networks, machine-to-machine

systems and also in systems connected in single network.

This scheme is used in the place where the keys are used for short period of time or to reduce the amount of the cipher text during the transmission and when there is a need of frequent changes in the group structure in a network. Military applications can be get benefit from this self-healing group key distribution scheme.

C.Organization of the Paper:

This paper is organized as follows, Section I describes about the introduction of the model , Section II describes about basic idea of self-healing group key distribution schemes.

II. SELF-HEALING APPROACH

This Long lived self-healing group key distribution scheme is been studying by the many research developers in recent no of years. In this scheme we described about how the self-healing property is used in the key distribution schemes.Self-healing schemes for key distribution has become a good research in this century.

In this concept we have introduced a distribution and generationSelf-healing group key distribution keys have used in various local area networks these network consist of one group manager who have send the data to another manager or group members these messages or information can be send with the help of keys where these keys are used to transmit the messages the main goal of this model is to build the idea of securing one to one communication. The secrecy of sending messages can be achieved by Encryption and authentication by the help of secret group key N. of keys for transmission purpose.

A Group key should have the following methods:

Authorization: This method should prevent unauthorized user which are not in group.

Key freshness: This technique has been used to get different set of new keys for different logins.

Capability:Self–healing mechanism property is efficient for good communication between sender and receiver.

Scalability: Scalability is defined as the size of the network and nodes it has been ranges up to different levels.

Communication scenario:This scenario describes how communication is achieved in a secured way in the systems in the local area networks.

III. FILE TRANSMISSION USING GROUP KEYS:

A. Login & New User:

In this module, the login process itself has lots of security. Usually the user account name and appropriate password of that account is enough to do the validation and login process, but here some more actions are given to make more security to the login process and get it the next action. The file search process is used to select the file to be sent. New User Creation process entitled that to collect some of the details to maintain the file transfer/Key Management.

B. Sender/file transmission:

Sender holds the key values (signature) which has been generate by key generation. The keys are in two categories private, public to give more security to the data transmission. The private key allows sending the selected data to the particular location or system. The public key allows sending to all users whom all are currently available in the network and the file transmission can be able, to process through Routers (BGP Speakers) and reached the destination (receiver).

C. Signature (Key) Generation:

In the signature Generation module, a random key is generated for each action. This generated key is stored in the database. Using this key field this is connected to the Access Specifier module. This key can be categorized to public or private to the user access. A new method is used to generate the key randomly, by using the SHA-1+HMAC (or) RSA method. SHA hash to make an Asymmetric approach accept a forged signature requires such signatures combination of HMAC (Hashed Message Authentication Code) algorithm Symmetric approach with 512-bit keys to generate.

D. Signature(Key) Management :

We present two new symmetric key approaches to securing BGP: Pre-key distribution approach, centralized key distribution approach.

1. Pre-Key distribution :

The users are given a substantial number of keys to avoid frequent key update. Periodic rekeying method, the keys are changed at the beginning of each period which is sufficiently long.Where the individual BGP router is responsible for key distribution, to secure the BGP updates. In the key

distribution protocols the center node maintains a set of "k" keys.

2. Centralized Key Distribution:In SBGP, the Central authority is responsible for key distribution. In SBGP, the cost of signature generation for a BGP speaker (BGP router) is only one signature, i.e., the route attestation that is added by this speaker. The cost of signature generation is lower. In SBGP, the cost of signature generation is low, that each BGP speaker only needs to add its own signature to the update.

Hackers Zone

The node which is present in the different network or individual system accessing the data in the false name of a node which is present in the router network is called as hackers. The randomly generated key is not allocated to the hacker system.

Monitoring Access

Monitoring Access module takes care of the data sending through the network using the key. It accesses the database to check the validation for proper and improper user. It also monitors the hackers if anybody accessing the data, which does not belong to the network.

Receiver :

Some of the node is acting as a sender and all the remaining nodes are the receivers.

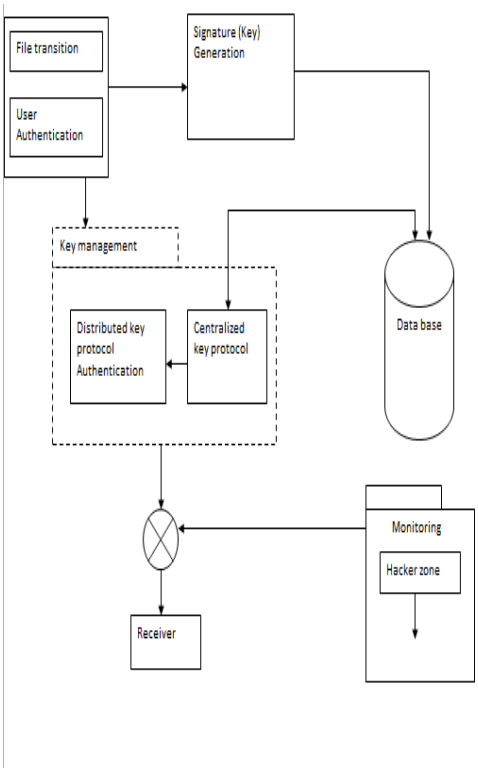
If a node sends a message that includes a signature from each of the keys it has and the receiver verifies the signatures based on the common keys then it can conclude that the message is authentic.

IV. THREE APPROACHES USED IN SELF-HEALING

There are three approaches used in self-healing approach for the distribution of keys they are

- Selective key distribution mechanism
- Predistributed secret data management
- Self-healing mechanism

The selective key distribution has been used to select the particular key from the group of keys with that key we can send our information .



SIMPLE ARCHITECTURE DIAGRAM OF SELF-HEALING SCHEME

Secret data management has been used to send our information secretly in the encrypted form and the self-healing mechanism has been used for the generation of different set of keys and for retrieving the keys which have been misplaced in the selective key distribution polynomial based algorithm and exponential based algorithm has been used to select particular key.

REFRENCES

1) Y. Jiang, C. Lin, M. Shi, and X. S. Shen, "Self-healing group keydistribution with time-limited node revocation for wireless sensornetworks," Ad Hoc Networks, vol. 5, no. 1, pp. 14 – 23, 2007,security Issues in Sensor and Ad Hoc Networks. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870506000448

2) R. Dutta, S. Mukhopadhyay, and T. Dowling, "Trade-off betweencollusion resistance and user life cycle in self-healing key distributionswith t-revocation," in Applications of Digital Information and Web Technologies, 2009. ICADIWT '09. Second International Conference on the, aug. 2009, pp. 603 –608.

3) B. Tian, S. Han, and T. Dillon, "An efficient self-healing key distribution scheme," in New Technologies, Mobility and Security, 2008. NTMS '08., nov. 2008, pp. 1 –5.

4) Daza, J. Herranz, and G. S´aez, "Flaws in some selfhealing key distribution schemes with revocation," Inf. Process. Lett., vol. 109, pp. 523–526, May 2009. [Online]. Available: http://portal.acm.org/citation.cfm?id=1519558.1519948

5) R. Dutta, S. Mukhopadhyay, and T. Dowling, "Enhanced access polynomial based self-healing key distribution," in Security in Emerging Wireless Communication and Networking Systems, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, O. Akan, P. Bellavista, J. Cao, F. Dressler, D. Ferrari, M. Gerla, H. Kobayashi, S. Palazzo, S. Sahni, X. S. Shen, M. Stan, J. Xiaohua, A. Zomaya, G. Coulson, Q. Gu, W. Zang,

and M. Yu, Eds. Springer Berlin Heidelberg, 2010,vol.42,pp.13–24,10.1007/978-3-642-11526-4 2. [Online].
Available: http://dx.doi.org/10.1007/978-3-642-11526-4 2

6) B. Tian, S. Han, and T. Dillon, "A self-healing and mutual-healingkey distribution scheme using bilinear pairings for wireless networks,"in Embedded and Ubiquitous Computing, 2008. EUC '08. IEEE/IFIP International Conference on, vol. 2, dec. 2008, pp. 208 –215.