IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Group Key Distribution using Self Healing Property for Peer to Peer System

D. Shilpaa[1], M. Vidhya[2], T. Packia Lakshmi[3]

[1, 2] **Department of Information Technology, AIHT**

[3]**Department of Information Technology, Anand Institute of Higher Technology**

Abstract

Self healing schemes for group key distribution have been an active research area. It is a method that enables dynamic group of users to establish secure group keys over untrustworthy network for secure communication. The functionality of the scheme is divided into three main building blocks- secret data management, predistributed data management, self healing mechanism. The SKD algorithm is tightly coupled with self healing property. If a GM wants to transmit a message to a user to ensure secure communication the GM uses group keys by randomly selecting them. The keys are updated and act as one time password(OTP). The keys are generated using SHA-HMAC algorithm. This decreases workload on the GM as well as user exposure and thus prevents hacking of files on networks.

Keywords- selective key distribution, Group Manager, secure hash algorithm, message authentication code, one time password

I. INTRODUCTION

In network communication, messages that are intended for more than one user should be delivered through multicasting to save network resources. There is a need to control access to the content of such messages, and to restrict them to authorized users only. However, the group of authorized users can vary periodically thus it becomes difficult to prevent from hacking.

Computer networks were used by researches for sending e-mail, sharing data and by corporate employees for sharing printers. Under these conditions, security did not get a lot of attention. Now millions of people are using networks for banking, shopping etc. Effective network security targets threats and stops them from entering into the network. Security protects the network as well as oversees the operations.

Secure key distribution schemes for group communications allow establishing a secure communication between a group manager and group members through an unreliable broadcast channel. Attention is paid to the self-healing property. Self healing is a good property for key distribution in wireless networks. A self healing key distribution schemes allows a large group of users to establish secure keys dynamically over a lousy or an unreliable wireless networks.

Existing solutions use group keys to implement such control, but face problems in dealing with changes in the group of authorized users. As the group size grows larger, scalability becomes an issue and more efficient protocols are required to provide a desired level of security without trading away performance.

Existing work on communication security suffer from hacking through SKD algorithm. The SKD algorithm is tightly coupled with self healing mechanism where the secure keys get frequently updated and acts as one time password (**OTP**).

The keys are generated using SHA-HMAC (Secure Hash Algorithm-Hash Message Authentication Code). So the hacker cannot recognize the key pattern as the keys change dynamically for each set of users. For instance, once the authorized user login, a set of ten secure keys will be generated by using SHA and these keys are unique for every user. The user randomly selects a key and attaches it with the file that is to be sent to the destination. Once the key is used, the same key becomes invalid. This is the process of self healing technique.

This technique can be applied in the broadcast transmission systems, including cable and satellite television, pay-per-view TV and information services. Packet losses are expected in these applications, so they can significantly benefit from the self-healing mechanism. We introduce an abstract model that uses self healing technique to decrease collision and workload of the sender as well as the user exposure on the network through thorough security and efficiency analysis.

II. RELATED WORK

An efficient self-healing scheme with group key distribution is proposed for communications in wireless networks. The most prominent characteristic of the scheme is resisting collusion between the new joined users and the revoked users, which is fatal weakness of hash function based self-healing key distribution schemes.[1]

Security of group communication for large mobile wireless sensor network hinges on efficient key distribution and key management mechanism. As the wireless medium is characterized by its loss nature, reliable communication cannot be assumed in the key distribution schemes. In such conditions, self-healing is a good property for key distribution in wireless applications. The main idea of self-healing key distribution scheme is that even if during a certain session some broadcast messages are lost due to network faults, the users are capable of recovering lost session keys on their own, without requesting additional transmission from the group manager. The only requirement for a user to recover the lost session keys is its membership in the group both before and after the sessions in which the broadcast packets containing the keys are sent. [2]

Self-healing approach of key distribution is stateless in the sense that a user who has been off-line for some period is able to recover the lost session keys immediately after coming back on-line. In this paper, we propose two constructions for scalable self-healing key distribution with t revocation capability. The novelty of our constructions are that we apply a different and more efficient self healing mechanism compared to the ones in the literature using one-way key chain.[1]

The objective of self-healing key distribution is to enable group users to recover session keys by themselves, without requesting additional transmissions from the group manager (GM), even when they miss some broadcast messages. One major benefit of the self-healing key distribution mechanism is the reduction of energy consumption due to the elimination of such additional transmission. Also in some applications, e.g., uni-directional broadcast channel from the GM, the self-healing key distribution mechanism seems to be the ideal solution. Desired features of self-healing key distribution schemes include energy awareness, short broadcast message, efficient users addition, revocation and so on. [3]

A primary challenge is managing the trade-off between providing an acceptable level of security and conserving scarce resources in particular energy which is critical for wireless network operations. Over a decade, a great number of self-healing key distribution schemes have been proposed for establishing a group key amongst a dynamic group of users over an unreliable, or lossy network. In this paper a comprehensive survey is conducted on the state-of-the-art in the field of self-healing key distribution. First, we clarify the security requirements of self-healing key distribution scheme for their special application environment. [4]

III. SELF HEALING APPROACH

We introduce the basic idea and the most important characteristics of the self healing approach to the group key distribution.

A. NETWORK MODEL

Self-healing group key distribution schemes are used in various network scenarios thus to make analysis easier.

The network consists of a single Group Manager (*GM*) and a Group Users (*U*). Group Manager is a resource rich node with high computational power, large memory space, and unlimited energy resources. User nodes, on the other hand, have limited computational power, limited memory and limited energy resources. *GM* communicates with nodes in *U* through an unreliable broadcast channel. She transmits broadcast messages which are received by all users. Because of nodes mobility and channel communications errors, some messages can be lost. Message retransmission should be avoided, if possible, since it is costly and requires feedback connection from receiver nodes to *GM*, which may not be available.

The main goal is to establish secure multicast communication between *GM* and members of a group of nodes $G \subseteq U$, which is a subset of *U*. Group *G* is dynamic, user nodes can join and leave. Communications security is achieved by message encryption and authentication using shared symmetric secret group key *K*. A shared key is convenient, but it can be disclosed by nodes leaving the group, or by group members intercepted by an adversary. To achieve high security level the key shall be changed frequently throughout the group lifetime and thus keys acts as OTP.

List of contents

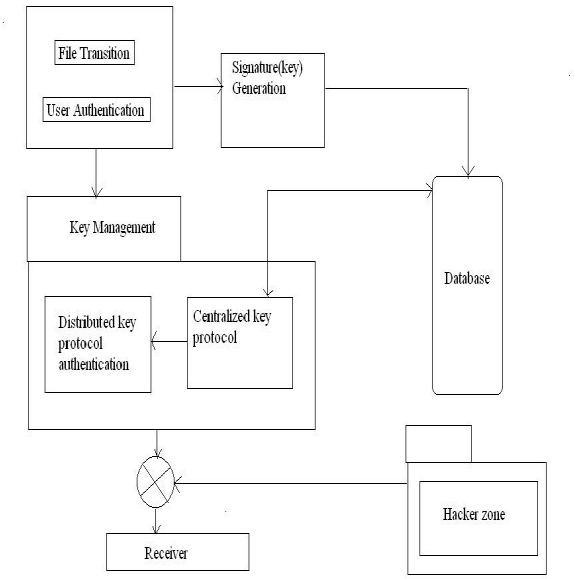
Terms	Abbreviations
GM	Group Manager
GU	Group Users
K	Group key
OTP	One Time Password

B. USER ENROLLMENT

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 during the login process.

When the user has been registered with the database, a set of keys will be generated for more authentications. These keys will provide more security while sending the data from one system to another system. 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. The keys which have generated in the database will act as a onetime password while data transfer.

SYSTEM ARCHITECTURE



C. SIGNATURE (KEY) GENERATION

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 and reaches the destination(receiver).

The keys are generated using SHA-HMAC.
The SHA encryption algorithm specifies a Secure Hash Algorithm (SHA1), which can be used to generate a Condensed representation of a message called a message digest.

The SHA is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest. Any change to a message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify. SHA1 is used to compute a message digest for a message or data file that is provided as input.

D.SIGNATURE (KEY) MANAGEMENT

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

i. 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 router is responsible for key distribution, to secure the updates. In the key distribution protocols the center node maintains a set of “k” keys.

ii. Centralized Key Distribution:

Where a central authority is responsible for key distribution. In this approach, the cost of signature generation for a router is only one signature, i.e., the route attestation that is added by this speaker. The cost of signature generation is lower.

In this approach, the cost of signature generation is low, that each router only needs to add its own signature to the update.

E .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.

CONCLUSION

In this paper, we make three key contributions. First, we show that the right trade-off between efficiency and security for information could be achieved by adding the little bit of trust on routers. We present a new flexible threat model where for any path of length k, at least one router is trustworthy. Second, we present two new symmetric key approaches to secure information; the centralized key distribution approach and the distributed key distribution approach. Third, we evaluated the efficiency of the two approaches with previous approaches to securing data.

The evaluation results show that our approaches are significantly more efficient than previous approaches. Also, we have discussed the deployment issues and important concerns like key management and interoperability to illustrate the feasibility of our protocols. Secure distribution is a proposed version of key freshness that includes strong authentication and encryption using public key infrastructure.

REFERENCES

[1] Self-Healing Sensor Network Key Distribution Scheme for Secure Communication", Patel Jay Kumar Shantilal Computer Science Department, Kadi Sarva Vishwa Vidyalaya, Gandhinagar, Gujarat, INDIA Received 12th October 2012.

[2] B. Tian, S.Han, S. Parvin, Hu, and S. Das, Self-healing key distribution schemes for wireless networks: A survey,". The Computer Journal, vol.54, no. 4,pp. 549-569, 2011.

[3] R.Dutta, E.C.Chang, S.Mukhopadhyay, "Efficient self-healing key distribution with revocation for wireless sensor networks using one way key chains",Proc.5th international conference on Applied Cryptography and Network Security,2007.

[4] M.Naor and B.Pinkas,"Efficient public trace and revoke schemes", Proc.4th International Conference on Financial Cryptography, ser.FC'00, 2001.