International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967 *Volume 2 , Issue 1(Jan-Feb 2015), PP1-5*

Locked Communication Using Valid Authentication Group Key Transfer Protocol in Wireless Networks

Nagashetty B Kolar

Bheemanna Khandre Institute of Technology, Bhalki
(kolarnb@gmail.com)

Abstract---Group key transfer protocol is developed to establish the communication path for group of communicating entities. The Key transfer protocols rely on a mutually trusted key generation center to select session keys and transport session keys to all communication entities secretly. Most often, key generation center encrypts session keys under another secret key shared with each entity during registration. In this paper a key transfer protocol for secure communication between group of users in a wireless networks is proposed. Presenting a valid authenticated key transfer protocol based on secret sharing scheme that key generation center can broadcast group key information to all group members at once and only authorized group members can recover the group key; but unauthorized users cannot recover the group key. Also provide authentication for transporting this group key and the confidentiality of this transformation is information theoretically secure. Goals and security threats of proposed group key transfer protocol will be analyzed in detail.

Keywords :-Group key transfer protocol, session key, secret sharing, confidentiality, valid authenticates.

I. INTRODUCTION

IN most secure communication, the following two security functions are commonly considered:
A) Message confidentiality: Message confidentiality ensures the sender that the message can be read only by an intended receiver. The message must be sent to correct receiver end and it is not read by unauthorized end user. This keeps the message secure and confidential to intended receiver.
.B) Message authentication: Message authentication ensures the receiver that the message was sent by a specified sender and the message was not altered en route.
The sender has to valid authenticated the correct receiver so no other unauthorized user alters the message. To provide these two functions, one-time session keys need to be shared among communication entities to encrypt and valid authenticate messages. Thus, before exchanging communication messages, a key establishment protocol needs to distribute one-time secret session keys to all participating entities. The key establishment protocol also needs to provide confidentiality and authentication for session keys.
There are two types of key establishment protocols: *key* ***transfer protocols*** and ***key agreement protocols****.* Key transfer protocols rely on a mutually trusted key generation center to select session keys and then transport session keys to all communication entities secretly. Most often, key generation center encrypts session keys under another secret key shared with each entity during registration. In key agreement protocols, all communication entities are involved to determine session keys. The most commonly used key agreement protocol is Diffie-Hellman (DH) key agreement protocol .In DH protocol, the session key is determined by exchanging public keys of two communication entities. Since the public key itself does not provide any authentication, a digital signature can be attached to the public key to provide authentication.
However, DH public key distribution algorithm can only provide session key for two entities; not for a group more than two members
When a secure communication involves more than two entities, a group key is needed for all group members. Most well-known group key management protocols can be classified into two categories:

- Centralized group key management protocols: a group key generation center is engaged in managing the entire group.
- Distributed group key management protocols: there is no explicit group key distribution center, and each group member can contribute to the key generation and distribution.

The class of centralized group key management protocols is the most widely used group key management protocols.

Harney proposed a group key management protocol that requires *O (n)*, where n is the size of group, encryptions to update a group key when a user is evicted or added if backward and forward secrecy are required. Fiat and Naor proposed a k-resistant protocol, i.e., coalitions of up to k users are secure, with each user storing *O (k log k log n)* keys and the server broadcasting O (k^2 $\log^2$ k log n) messages per rekeying. Eltoweissy proposed a protocol based on Exclusion Basis Systems, a combinatorial formulation of the group key management problem, which allows protocol user to trade-off between the number of keys needed to be stored and the number of messages needed to be transmitted for each key update with no counter collusion solution provided. Most distributed group key management protocols took natural generalization of the DH key agreement protocol, Steiner proposed a natural extension of DH, named the group DH key exchange and later in 2001, it has been enhanced with authentication services and has proved to be secure . In 2006, Bohli developed a framework for robust group key agreement that provides security against malicious insiders and active adversaries in an unauthenticated point-to-point network. Then, in 2007, Bresson constructed a generic valid authenticated group DH Key exchange and the algorithm is provably secure. Also, in 2007, Katz and Yung proposed the first constant-round and fully scalable group DH protocol which is provably secure in the standard model (i.e., without assuming the existence of “random oracles”). The main feature of the group DH key exchange is to establish a secret group key among all group members without relying on a mutually trusted key generation center.

There are other distributed group key management protocols based on non-DH key agreement approach. Tzeng proposed a conference key agreement protocol based on discrete logarithm (DL) assumption with fault tolerance in recent years. The protocol can establish a conference key even if there are several malicious participants among the conference participants. However, the protocol requires each participant to create n-power polynomials, where n is the number of participants; this is a serious encumbrance to efficiency. In 2008, Cheng and Laih modified Tseng’s conference key agreement protocol based on bilinear pairing. In 2009, Huang e proposed a non interactive protocol based on DL assumption to improve the efficiency of Tseng’s protocol. One main concern of key agreement protocols is that since all communication entities are involved to determine session keys, the time delay of setting up this group key may be too long, especially when there are a large number of group members.

Secret sharing has been used to design group key distribution protocols. There are two different approaches using secret sharing: one assumes a trusted offline server active only at initialization and the other assumes an online trusted server, called the key generation center, always active. The first type of approach is also called the key predistribution scheme. In a key pre distribution scheme, a trusted authority generates and distributes secret pieces of information to all users offline. At the beginning of a conference, users belonging to a privileged subset can compute individually a secret key common to this subset. A family of forbidden subsets of users must have no information about the value of the secret. The main disadvantage of this approach is to require every user to store a large size of secrets. The second type of approach requires an online server to be active and this approach is similar to the model used in the IEEE 802.11i standard that employs an online server to select a group key and transport it to each group member. However, the difference between this approach and the IEEE 802.11i is that, instead of encrypting the group temporal key using the key encryption key from the authentication server to each mobile client separately as specified in the IEEE 8-2.11i, the trusted key generation center broadcasts group key information to all group members at once. In 1989, Laih proposed the first algorithm based on this approach using any secret sharing scheme to distribute a group key to a group consisting of (t-1) members. In this paper, proposed a solution based on this approach and provide confidentiality and authentication for distributing group keys. Furthermore, here classifying attacks into insider and outsider attacks separately, and analyze the protocol under these attacks in detail. Following unique features of proposed group key transfer protocol using secret sharing scheme.

- Each user needs to register at key generation center to subscribe the group key transfer service and to establish a secret with key generation center. Thus, a secure channel is needed initially to share this secret with each user. Later, key generation center can transport the group key and interact with all group members in a broadcast channel.
- The confidentiality of group key distribution is information theoretically secure; that is, the security of this transfer of group key to each group member does not depend on any computational assumption.
- The authentication of the group key is achieved by broadcasting a single authentication message to all group members.

II. SYSTEM ARCHETECTURE

The following figure describes the architecture of system. Here every user needs to establish a connection with other user in the network to communicate with each other. This is done by sending request to the kernel for new channel. To start a connection initially each user must be register with the key generation centre. The key generation center is used to generate the private keys to each user. Using these keys key generation center will generate the session key for encryption and decryption. Here every member must register with the key generation center to start the connection; Key generation center generates session keys using all user keys. These session keys are passed to all users to establish the connection. The key generation center will forward the session key to end user these session keys are encrypted and decrypted by using secrete key to achieve the confidentiality and security.

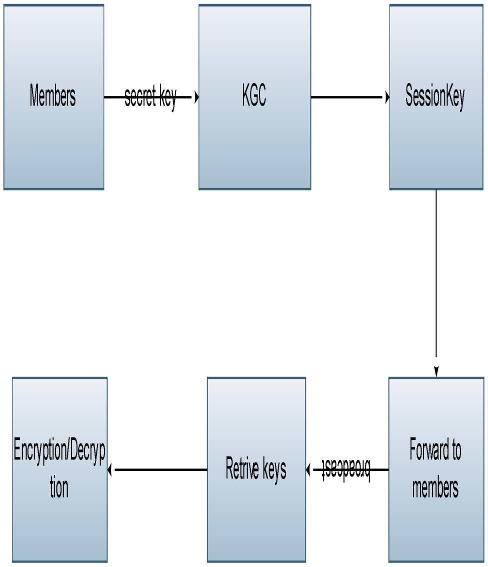

Fig1: System Architecture

The system architecture includes following modules.

- Initialization of key generation center.
- User Registration.
- Session Key Generation and Distribution.

This needs to initialize the key generation center to start the connection establishment so the key generation center will allocate the key to each user and generate the session key.

III. OBJECTIVES

In this section, first describe the model of group key transfer protocol. Then, presenting the security goals for group transfer protocol.

3.1 Model

Group key transfer protocol relies on one trusted entity, key generation center, to choose the key, which is then transported to each member involved. Each user is required to register at key generation center for subscribing the key distribution service. The key generation center keeps tracking all registered users and removing any unsubscribed users. During registration, key generation center shares a secret with each user. In most key transfer protocol, Key generation center encrypts the randomly selected group key under the secret shared with each user during registration and sends the ciphertext to each group member separately. A valid authenticated message checksum is attached with the ciphertext to provide group key authenticity. In this approach, the confidentiality of group key is ensured using any encryption algorithm which is computationally secure. The protocol uses secret sharing scheme to replace the encryption algorithm. A broadcast message is sent to all group members at once. The confidentiality of group key is information theoretically secure. In addition, the authentication of broadcasting message can be provided as a group authentication. This feature provides efficiency of the proposed protocol.

3.2 Goals

The main security goals for group key transfer protocol are:

1) Key freshness 2) key confidentiality and 3) key authentication.

Key freshness is to ensure that a group key has never been used before. Thus, a compromised group key cannot cause any further damage of group communication. Key confidentiality is to protect the group key such that it can only be recovered by authorized group members; but not by any un-authorized user. Key authentication is to provide assurance to authorized group members that the group key is distributed by key generation center; but not by an attacker.

In the defined protocol, the only focus on protecting group key information broadcasted from key generation center to all group members. The service request and challenge messages from users to key generation center are not authenticated. Thus, an attacker can impersonate a user to request for a group key service. In addition, attacker can also modify information transmitted from users to key generation center without being detected. Need to analyze security threats caused by these attacks. In the security analysis, this conclude that none of these attacks can successfully attack to authorized group members since attackers can neither obtain the group key nor share a group key with authorized group members. User/message authentication and key confirmation can be easily incorporated into the protocol since each user has shared a secret key with key generation center during registration. However, these security features are beyond the scope of fundamental protocol. Here briefly discuss ways to provide user authentication, message authentication, and key confirmation in security analysis.

IV. PROTOCOL DESIGN

Valid authenticated group key transfer protocol consists of three processes: initialization of key generation center, user registration, and group key generation and distribution. The detailed description is as follows:

Initialization of key generation center: The key generation center randomly chooses two safe primes p and compute ***n=pq.n*** is made publicly known.

User Registration: Each user is required to register at key generation center for subscribing the key distribution service. The key generation center keeps tracking all registered users and removing any unsubscribed users. During registration, key generation center shares a secret, (x, y) with each user Ui.

Group key generation and distribution: Upon receiving a group key generation request from any user, key generation center needs to randomly selects a group key and access all shared secrets with group members. Key generation center needs to distribute this group key to all group members in a secure and valid authenticated manner. All communication between key generation center and group members is in a broadcast channel

V. SECURITY ANALYSIS

In this section, first consider the two types of adversaries in proposed protocol, insider and outside.

Attacks: Adversaries can be categorized into two types. The first types of adversaries are outsiders of a particular group. The outside attacker can try to recover the secret group key belonging to a group that the outsider is unauthorized to know. This attack is related to the confidentiality of group key. In the proposed protocol, anyone can send a request to key generation center for requesting a group key service. The outside attacker may also impersonate a group user to request a group key service. In security analysis, it shows that the outside attacker gains nothing from this attack since the attacker cannot recover the group key. The second types of adversaries are insiders of a group who are authorized to know the secret group key; but inside attacker attempts to recover other member's secret shared with key generation center. Since any insider of a group is able to recover the same group key, need to prevent inside attacker knowing other member's secret shared with key generation center.

Theorem1:

The proposed protocol achieves the following security goals:
1) Key freshness 2) key confidentiality 3) key authentication.
Proof:1) Key freshness is ensured by key generation center since a random group key is selected by key generation center for each service request. In addition, the polynomial *f(x)* used to recover the group key is a function of random challenge selected by each group member.
2) Key confidentiality is provided due to the security feature of a secret sharing scheme. Key generation center generates a t^{th} degree polynomial f(x) passing through *(t+1)* points, *(o, k)* and (x, y, +R) for i =1 . . . t, and makes t additional points publicly known. For each authorized group member, including the secret shared with key generation center, he/she knows (t+1) points in total on *f(x)*. Thus, any authorized group member is able to reconstruct the polynomial *f(x)* and recover the group key k. However, for any unauthorized member (or outsider), there are only t points on *f(x)* available. Thus, unauthorized member knows nothing about the group key. This property is information theoretically secure since there has no other computational assumption based upon.

3) Key authentication is provided through the value Auth in step 4. Auth is a one-way hash output with the secret group key and all members' random challenges as input. Since the group key is known only to authorized group members and key generation center, unauthorized members cannot forge this value. Any insider also cannot forge a group key without being detected since the group key is a function of the secret shared between each group member and key generation center. In addition, any replay of Pi and Auth of key generation center in step 4 can be detected since the group key is a function of each group member's random challenge.

Theorem 2 (Outsider attack).

Assume that an attacker who impersonates a group member for requesting a group key service, then the attacker can neither obtain the group key nor share a group key with any group member. Proof. Although any attacker can impersonate a group member to issue a service request to key generation center without being detected and key generation center will respond by sending group key information accordingly; however, the group key can only be recovered by any group member who shares a secret with key generation center. This security feature is information theoretically secure. If the attacker tries to reuse a compromised group key by replaying previously recorded key information from key generation center, this attack cannot succeed in sharing this compromised group key with any group member since the group key is a function of each member's random challenge and the secret shared between group member and key generation center. A compromised group key cannot be reused if each member selects a random challenge for every conference.

Theorem 3 (Insider attack).

Assume that the protocol runs successfully v times and the applied factoring instances are intractable, then the secret($x_{i,}$ $y_{i)}$ of each group member shared with key generation center remains unknown to all other group members (and outsiders). Proof: For a group key service request, key generation center generates a t^{th} degree polynomial f(x) passing through points. For each authorized group member, with knowledge of the secret shared with key generation center and t public information, he/she knows (t+1) points on f(x). Thus, any authorized group member is able to reconstruct the polynomial f(x). However, the secret of each group member shared with key generation center remains unknown to outsiders.
In the proposed protocol, group key service requests and challenges from group members are not valid authenticated. An adversary (insider) can make several service requests to key generation center and forge challenges of the target group member. For example, the adversary makes two service requests for a group containing the adversary and the target group member.

VI. ADVANTAGES:

Each user needs to register at key generation center to subscribe the group key transfer service and to establish a secret with key generation center. Thus, a secure channel is needed initially to share this secret with each user. Later, key generation center can transport the group key and interact with all group members in a broadcast channel. The confidentiality of group key distribution is information theoretically secure; that is; the security of this transfer of group key to each group member does not depend on any computational assumption. The authentication of the group key is achieved by broadcasting a single authentication message to all group members.

VII. CONCLUSION

Here proposed an efficient group key transfer protocol based on secret sharing. Every user needs to register at a trusted key generation center initially and preshare a secret with key generation center. Key generation center broadcasts group key information to all group members at once. The confidentiality of group key distribution is information theoretically secure. This provides a group key authentication. Security analysis for possible attacks is included.

VIII. REFERENCES

[1] W. Diffie and M.E. Hellman, “New Directions in Cryptography,” IEEE Trans. Information Theory, Vol. IT-22, no. 6, pp. 644-654, Nov. 1976.

[2] C. Laih, J. Lee, and L. Harn, “A New Threshold Scheme and Its Application in Designing the Conference Key Distribution Cryptosystem,” Information Processing Letters, vol. 32, pp. 95- 99, 1989.

[3] J.C. Cheng and C.S. Laih, “Conference Key Agreement Protocol with Non Interactive Fault-Tolerance Over Broadcast Network,” Int’l J. Information Security, vol. 8, no. 1, pp.37-48, 2009.

[4] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, “Perfectly Secure Key Distribution for Dynamic Conferences,” Information and Computation, vol. 146, no. 1, pp. 1-23, Oct. 1998.

[5] C. Boyd, “On Key Agreement and Conference Key Agreement,” Proc. Second Australasian Conf. Information Security and Privacy (ACISP ’97), pp. 294-302, 1997.

[6] E. Bresson, O. Chevassut, D. Pointcheval, and J.- J. Quisquater, “Provably Authenticated Group Diffie-Hellman Key Exchange,” Proc. ACM Conf Computer and Comm. Security (CCS ’01), pp. 255-264, 2001.

[7] E. Bresson, O. Chevassut, and D. Pointcheval, “Provably-Secure Authenticated Group Diffie-Hellman Key Exchange,” ACM Trans. Information and System Security, vol. 10, no. 3, pp.255-264, Aug. 2007.

[8] J.M. Bohli, “A Framework for Robust Group Key Agreement,” Proc. Int’l Conf. Computational Science and Applications (ICCSA ’06), pp. 355- 364, 2006.

[9] M. Burmester and Y.G. Desmedt, “A Secure and Efficient Conference Key Distribution System,” Proc. Eurocrypt ’94 Workshop Advances in Cryptology, pp. 275-286, 1994.

[10] C. Laih, J. Lee, and L. Harn, “A New Threshold Scheme and Its Application in Designing the Conference Key Distribution Cryptosystem,” Information Processing Letters, vol. 32, pp. 95- 99, 1989.

[11] R. Blom, “An Optimal Class of Symmetric Key Generation Systems,” Proc. Eurocrypt 84 Workshop Advances in Cryptology, pp. 335-338, 1984.

[12] G.R. Blakley, “Safeguarding Cryptographic Keys,” Proc. Am. Federation of Information Processing Soc. (AFIPS ’79) Nat’l Computer Conf., vol. 48, pp. 313- 317, 1979.