ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Discriminating the Outside Attacks Probabilistic Method Using Trusted Mechanism with Sharing Key Support of Authentication

Alluri Lakshmi Lavanya
Assistant Professor,
SRKR Engineering College.
E mail: allurilavanya111@gmail.com

Abstract:
In wireless sensor networks, secure group communication, one-time session keys need to be shared among group members in a secure way and authenticated manner. The earliest Harn and Lin existing a authenticated group key transfer protocol that a jointly trusted key generation center (KGC) can broadcast the group key information to all group members at once and verify only authorized group members can be recover the group key at a time. The existing system as Harn and Lin's protocol cannot avoid the outsider's attack and describes the reasons and detailed processes that the group key is progressed by the active attacker who is not included in the member list of that particular group member. we propose a trusted mechanism with sharing process of keys then upload and set the information into network. Here we set the rules of network process and apply for the probabilistic method of attacks based then discriminate the problems.

1 INTRODUCTION:

CONFIDENTIALITY and AUTHENTICATION are two basic requirements in secure group communication. Specifically, confidentiality ensures the transmitted message is only recognizable for an intended receiver, and authentication guarantees that the communication entity is an authorized member. To provide these two basic functions, key establishment protocols are deployed to share a common one-time session key among group members, which are often classified into key agreement protocols and key transfer protocols. The former involves all members' participation to generate a session key without a trusted third party, but the process of authentication may take a long time, especially when the number of members is large. The latter relies on a trusted key generation center (KGC) to firstly select session keys, and then securely distribute these session keys to all communication members.Key transfer protocols[1,3,4] and key agreement protocols[5-7] are two types of key establishment protocols. Key transfer protocols rely on a mutually trusted key generation center (KGC) to select session keys and then transport session keys to all communication entities secretly. Most often, KGC 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[2]. In DH protocol, the session key is determined by exchanging public keys of two communication entities. Most key transfer protocols take natural generalization of the DH key agreement protocol. There are other key transfer protocols based on non-DH key agreement approach as well. Secret sharing schemes were introduced by both Blakley[8] and Shamir [5] independently in 1979 as a solution for safeguarding cryptographic keys and have been studied extensively in the literatures.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In this paper, we show that the attacker, who is not included in the list of a particular group, can impersonate any group member to join in that group only if the attacker outside of that group is allowed to request for group key service in their protocol. This condition is a basic feature to everyone who wants to make use of their protocol. The analysis shows the users who have subscribed the key distribution service but not are included in a particular group can gain the access of the group . The rest of this paper is organized as follows. Section 2 briefly reviews Harn and Lin's key transfer protocol[1]. Section 3 provides security analysis to the original protocol and the proposed attack is described in Section 4 . A conclusion is made in section 5.

2 Brief Introduction of Harn Lin's Protocol:

Harn Lin.′s authenticated group key transfer protocol consists of three processes:

Initialization of KGC:

The KGC randomly chooses two primes p and q and computes n= p×q. n is published.

User Registration:

Each user is required to register at the KGC for subscribing the key distribution service. The KGC keeps tracking all the registered users and removing any unsubscribed users. During registration, KGC shares a secret, (x_i, y_i), with each user, U_i, where $x_i, y_i \in Z_n^*$.

Group Key Generation and Distribution:

Upon receiving group key generation request from any user, KGC needs to randomly select a group key and access all the shared secrets with the group members. KGC needs to distribute this group key to all the group members in a secure and authenticated way. All the communications between KGC and group members are in a broadcast channel. For example, we assume that a group consists of t members, $\{U_1,U_2, \cdots ,U_t\}$, and shared secrets are (x_i, y_i), for i = 1, · · · , t.

The key generation and distribution process contains five steps.

Step1. The initiator sends a key generation request to KGC with a list of group members as $\{U_1,U_2, \cdots ,U_t\}$.

Step2. KGC broadcasts the list of all the participating members, $\{U_1,U_2, \cdots ,U_t\}$,, as a response.

Step3. Each participating group member needs to send a random challenge, $R_i \in Z_n^*$, to KGC.

Step4. KGC randomly selects a group key, k, and generates an interpolated polynomial f (x) with degree t to pass through (t +1) points, (0, k) and $(x_i, y_i \oplus Ri)$, for i = 1, · · · , t. KGC also computes t additional points, $P_1, \cdots ,P_t$, on f(x) and Auth = $h(k, U_1,U_2, \cdots ,U_t ,R_1,R_2, \cdots ,R_t ,P_1,P_2, \cdots ,P_t)$, where h is a one-way hash function. All the computations on f (x) are over Z_n^* . KGC broadcasts $\{Auth,P_1, \cdots ,P_t\}$ to all the group members. All the computations are performed in Z_n^*

Step5. For each group member U_i, knowing the shared secret, $(x_i, y_i \oplus Ri)$, and t additional public points, P_i, for i = 1, · · · , t, on f (x), he is able to compute the polynomial f (x) and recover the group key k = f (0). Then, U_i computes $h(k, U_1,U_2, \cdots ,U_t ,R_1,R_2, \cdots ,R_t ,P_1,P_2, \cdots ,P_t)$ and checks whether this hash value is identical to Auth. If these two values are identical, U_i authenticates the group key sent from KGC.

3. Security Analysis:

Harlin's provide the following theorem that avoids the outsiders attack.

Theorem (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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Proof. Although any attacker can impersonate a group member to issue a service request to KGC without being detected and KGC 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 KGC. This security feature is information theoretically secure. If the attacker tries to reuse a compromised group key by replaying previously recorded key information from KGC, 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 KGC. A compromised group key cannot be reused if each member selects a random challenge for every conference.

4. Praposed Attack:

In above protocol that we will study, simultaneous broadcasts are intensively used. However it is actually a multi-cast, in which the attacker may delay, modify, or cancel the message sent to each recipient independently . Suppose an attacker want to make an active attack to impersonate a group member. His aim is to obtain the group key and attend their secret conference. he has the ability to intercept messages between the KGC and normal group members and can forge a new one as well. To abide by the protocol, he should get the published parameter n and subscribe the key distribution service of the KGC before the attack. Suppose his general identity is U_e and the shared secret between the KGC and her is (x_e, y_e), where $x_e, y_e \in Z_n^*$. Note that his general identity is not included in the list of the group members, who want to start a conversation. That is $e \notin [1, t]$.Attack processes are described as follows:

1. U_e intercepts the key generation request, which contains a list of group members as$\{U_1,U_2, \cdots ,U_t\}$ to the KGC. Then U_e deletes any one, such as U_i where $i \in [1, t]$, in the list $\{U_1,U_2, \cdots ,U_t\}$, and replaces U_i with her identity U_e in the forged list. Finally, she unicasts the forged list $\{U_1, \cdots ,U_{i-1},U_e,U_{i+1}, \cdots ,U_t\}$ to the KGC.

2. U_e intercepts the response, $\{ U_1, \cdots ,U_{i-1},U_e,U_{i+1}, \cdots ,U_t \}$, from the KGC, and broadcasts the original list $\{U_1,U_2, \cdots ,U_t\}$ to all the participating members.
After the two steps above, the KGC believes the participating members are $\{ U_1, \cdots ,U_{i-1},U_e,U_{i+1}, \cdots ,U_t \}$, but group members consider $\{ U_1, \cdots ,U_{i-1},U_i,U_{i+1}, \cdots ,U_t \}$ are going to start a new conversation.

3. U_e intercepts $R_i \in Z_n^*$ from Ui and unicasts her random challenge $R_e \in Z_n^*$ to the KGC. At the same time, U_e records all the R_j s to the KGC, where j = 1, $\cdots$, t, $j \neq i$. In the step4 of riginal protocol, KGC will compute f (x) with the t +1 points $(x_i, y_i \oplus R_j)$, where j = 1, $\cdots$, t, $j \neq i$, $(x_e, y_e \oplus R_e)$ and (0, k). Then KGC computes t additional points $P_1, \cdots ,P_t$ on f (x), computes Auth = $h(k,U_1, \cdots ,U_{i-1},U_e,U_{i+1}, \cdots ,U_t ,R_1, \cdots ,R_{i-1},R_e, R_{i+1}, \cdots ,R_t ,P_1,P_2, \cdots ,P_t)$ and broadcasts $\{Auth,P_1,\cdots ,P_t\}$.

4. U_e intercepts $\{Auth,P_1, \cdots ,P_t\}$ sent from the KGC, where Auth = $h(k, U_1, \cdots ,U_{i-1},U_e,U_{i+1}, \cdots ,U_t ,R_1, \cdots ,R_{i-1},R_e, R_{i+1}, \cdots ,R_t ,P_1,P_2, \cdots ,P_t)$ Then he computes $(x_e, y_e \oplus R_e)$ with her challenge R_e and her own secret value (x_e, y_e). The group key k can be computed with the t +1 points $(P_1, \cdots ,P_t)$ and $(x_e, ye \oplus R_e)$. Finally, he forges the signature Auth′ = $h(k,U_1, \cdots ,U_{i-1},U_i,U_{i+1}, \cdots ,U_t ,R_1, \cdots ,R_{i-1},Ri,R_{i+1}, \cdots ,Rt ,P_1,P_2, \cdots ,P_t)$, and broadcasts {Auth′ ,P1, $\cdots$,Pt} to all the group members except U_i.

In the step 5 of the original protocol, each group member U_j , where j = 1, $\cdots$, t, $j \neq i$, is able to compute the group key k with $(P_1, \cdots ,P_t)$ and $(x_i, y_i \oplus R_j)$. Then U_j computes the hash value $h(k, U_1, \cdots ,U_{i-1},U_i,U_{i+1}, \cdots ,U_t ,R_1, \cdots ,R_{i-1},Ri,R_{i+1}, \cdots ,R_t ,P_1,P_2, \cdots ,P_t)$ with the member list that he reserves in the step1 and compares it with the received Auth′ . Since these two values are identical, U_j accepts the group key k. As a result, $U_1, \cdots ,U_{i-1},U_e,U_{i+1}, \cdots ,U_t$

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

will start a new conversation and U_i cannot obtain the group key. In the end of the Harn lin.′s protocol, they claim their protocol does not focus on user authentication n and messages authentication that from group members toKGC. But they suggest that the following two additional steps can achieve above two features. First, in step3 of the original protocol, each user U_i attaches an authentication value, $h((x_i, y_i),R_i)$, along with the challenge message R_i. Then KGC can authenticate R_i. Second, after step5 of the original protocol, each user U_i sends a key confirmation, $h((x_i, y_i), k)$, to KGC. Then, after receiving all key confirmations, KGC sends a group key confirmation, $h((x_i, y_i), k,U_1, \cdots ,U_t)$, to each group member. As the result, each user U_i can confirm the group key.

It seems that the protocol with the additional key confirmation steps can prevent our man-in-the-middle attack, because the key confirmation $h((x_i, y_i), k,U_1, \cdots ,U_t)$ contains the user list $\{U_1, \cdots ,U_t\}$ and the shared secret between each user and the KGC. The attacker U_e can not forge valid key confirmation $h((x_i, y_i), k,U_1, \cdots ,U_{i-1},U_e ,U_{i+1}, \cdots ,U_t)$ without the shared secret (x_i, y_i). However, actually, these steps not only do not enhance the security of the original protocol, but also lead their protocol suffers from more serious attacks. Suppose KGC sends a group key confirmation $h((x_1, y_1), k,U_1, \cdots ,U_{i-1},U_e, U_{i+1}, \cdots ,U_t)$ to a user U_1 after step5. The attacker U_e intercepts it and does not forward it to U_1 immediately.

Since the group key k has been computed and the user list$\{U_1, \cdots ,U_{i-1},U_e,U_{i+1}, \cdots ,U_t\}$ is known to him, he can guess a pair of number (x'_1, y'_1) and verify whether it is U_1's secret by the equation $H \stackrel{?}{=} h(x'_1, y'_1, k,U_1, \cdots ,U_{i-1}, U_e,U_{i+1}, \cdots ,U_t)$ in an offline manner. $H = h((x_1, y_1), k, U_1, \cdots ,U_{i-1},U_e,U_{i+1}, \cdots ,U_t)$ is the intercepted key confirmation. As the result, U_e will get U_1's secret and thus he can impersonate U_1 directly. It means that adding these additional steps may lead the user′s secret reveals . Actually, these two additional steps are just a suggestion at the last of the original paper.

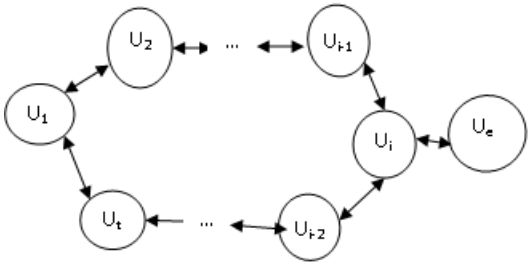
After four steps attack, the outside attacker U_e can impersonate U_i to participate in the new conversation w ith other group members and U_i will be kicked out off the group. Since U_i may be any one of the group member, U_e can impersonate any one he wants to replace. However, if the attacker is not familiar with others, he may not have enough knowledge to talk with each others.Even if he owns the group key, other members may fin d he is not U_i by the content in the conversation. To overcome this shortage, the attacker can continue the attacking process as follows:

5.U_e unicasts a new key generation request to the KGC with the group members $\{U_e,U_2, \cdots ,U_i, \cdots ,U_t\}$.

6. U_e intercepts the response $\{U_e,U_2, \cdots ,U_i, \cdots ,U_t\}$ from the KGC. For the response has been sent to U_i, U_e does not need to unicast another list.

7. U_e unicasts the challenge $R_e \in Z_n^*$ and R_j , where j = 2, · · · , t, to the KGC. Note, R_j is the original challenge intercepted from U_j in the step3. In the step4 of original protocol, KGC will compute f (x) with the t +1 points $(x_j, y_j \oplus R_j)$, where j = 2, · · · , t, $(x_e, y_e \oplus R_e)$ and $(0, k_e)$. Then KGC will compute t additional points $P_1, \cdots ,P_t$ on f (x), computes $Auth = h(k, U_e,U_2, \cdots ,U_i, \cdots ,U_t ,R_e,R_2, \cdots ,R_i, \cdots ,R_t ,P_1,P_2,\cdots ,P_t)$ and broadcasts $\{Auth,P_1, \cdots ,P_t\}$.

8. U_e intercepts $\{Auth,P_1, \cdots ,P_t\}$ sent from the KGC, where $Auth = h(k,U_e,U_2, \cdots ,U_i, \cdots ,U_t ,R_e,R_2, \cdots ,R_i, \cdots ,R_t ,P_1,P_2, \cdots ,P_t)$. Then she computes the group key k_e with the t+1 points $(P_1, \cdots ,P_t)$ and $(x_e, y_e \oplus R_e)$.



ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Finally, he generates a new signature Auth′ = h(k_e,U_1, · · · ,U_i, · · · ,U_t ,R_1, · · · ,R_i, · · · ,R_t ,P_1,P_2, · · · ,P_t) and unicasts {Auth′ ,P_1, · · · ,P_t} to U_i. After receiving the signature Auth′ and the points P_i, U_i can compute k_e with (P_1, · · · ,P_t) and (x_j, $y_j \oplus R_j$). Then he computes the hash value h(k_e,U_1, · · · ,U_i, · · · ,U_t ,R_1, · · · ,R_i, · · · ,R_t ,P_1,P_2, · · · ,P_t) with the member list that he reserves in the step1 and compares it with the received Auth′ . Since these two values are identical, U_i accepts the group key k_e. As a result, {U_i,U_e} will start a new conversation and U_e can gain enough knowledge to talk with other t-1 participators. As the result of all 8 steps, U_e participates in two conversations at the same time. One is with U_1, · · · ,U_{i-1},U_{i+1}, · · · ,U_t , another is with U_i. The result can be described as Fig. 3. When someone in the group1 talks something that the attacker does not know, he can send this message to U_i and give back U_i's response as his response. In addition, if he believes U_i's response doesn't meet her needs, he can also forge another one based on U_i's response.

For Example:

A company has 10 departments, each department owns 9 employees and 1 supervisor. If the company uses this protocol to distribute group keys, all 90 employees and 10 supervisors should subscribe the key distribution service and each department can form a regular group and use the group key to deal with their own vocational work confidentially. However, when the supervisors want to form a group and talk some secrets, any employee can eavesdrop or tamper on it with above method. Finally, a conclusion can be made that anyone who has established a shared secret with KGC can obtain the group key; he does not need to be a member of that group.

6.Conclusion:

In this paper, due to the attack methods described and, Harn lin′s authenticated group key transfer protocol based on the secret sharing doesn't achieve their goals. Here, we proposed a proposed attack includes anyone outside of a particular group can gain the group key without being detected.

Hence we demonstrated that original protocol does not resist against outsider attacks and apply to network process. we compare proposed with existing its better performance.

References:

[1] Lein Harn and Changlu Lin, Authenticated Group Key Transfer Protocol Based on Secret Sharing, IEEE Trans. Computers, **59**, 842 (2010).

[2] W. Diffie and M. E. Hellman, New Directions in Cryptography, IEEE Trans. Information Theory, **22**, 644 (1976).

[3] N. W. Lo, Kuo-Hui Yeh, Cryptanalysis of two three-party encrypted key exchange protocols, Computer Standards & Interfaces, **31**, 1167 (2009).

[4] V. A. Ustimenko, Y. M. Khmelevsky, Walks on graphs as symmetric or asymmetric tools to encrypt data, The South Pacific Journal of Natural and Applied Sciences, **20**, 34-44 (2002).

[5]A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612-613, 1979.

[6] Xianfeng Guo, Jiashu Zhang, Secure group key agreement protocol based on chaotic Hash, Information Sciences, **180**,
4069 (2010).

[7] Wei Yuan, Liang Hu, Hongtu Li, Jianfeng Chu, An Efficient Password-based Group Key Exchange Protocol Using Secret Sharing, applied mathematics & information sciences, **7**,145 (2013).

[8] G. R. Blakley, "Safeguarding cryptographic keys," in Proceeding American Federation of Information Processing Society, vol. 48, pp. 313- 317, 1979.