Overview of Secure Conference Scheme for Mobile Communications

Nilesh M. Shidurkar
Student,M.E.(C.S.E.)
Jagadambha College of Engineering & Technology
Yavatmal- 445001(M.S.)
INDIA

Mangesh M. Ghonge
Assistant Professor
Jagadambha College of Engineering & Technology
Yavatmal- 445001(M.S.)
INDIA

M.V.Sarode, Ph.D
Head of Department
Jagadambha College of Engineering & Technology
Yavatmal- 445001(M.S.)
INDIA

ABSTRACT
A Secure digital conference scheme allows a group of people to communicate safely in different way. Dynamic participation is a key feature of the secure conference schemes that allows new conferees to join and the old conferees to leave. The conference key distribution scheme (CKDS) enables three or more parties to derive a common conference key to protect the conversation content in their conference. In this paper we study a conference scheme for mobile communications and find that the scheme is insecure against the replay attack. With our replay attack, an attacker with a compromised conference key can cause the conferees to reuse the compromised conference key, which in turn completely reveals subsequent conversation content.

Keywords— Mobile communications, conference scheme , security, dynamic participation.

1. INTRODUCTION

A Portable communication device that are low power, low cost , and small in size with mobile networking capabilities are mostly preferable by user. During mobile teleconference it is necessary for all conferees to be connected to mobile switching center (MSC) via wireless communication. Wireless communications transmit conversations via radio,

making them more susceptible to eavesdropping and unauthorized access than are conversations carried via wires. Therefore, it is crucial to ensure confidentiality and authenticity in mobile teleconferences.

Dynamic participation is a key feature of the secure conference schemes that allows new conferees to join and the old conferees to leave. The confidentiality of the conference communication must be achieved among the current conferees. The conferees who have left should not be able to participate the secure conference communication anymore, i.e., they should not have the updated secret key. This is the basic security requirement for dynamic participation; otherwise, dynamic participation makes no sense.

A secure conference scheme with dynamic participation was proposed in [4], which is an improved version of [3] that has no dynamic participation feature. Later it was pointed out that the scheme in [4] has a security weakness due to the attack. A countermeasure against the attack was also proposed to secure the scheme.

In this paper two more powerful attacks proposes that breaks both the original scheme and the improved scheme. The countermeasure of [4] cannot resist our attacks.

The first attack is conducted by a group of colluding conferees. They first set up a conference session and discover NC's (network center) session secret by an active attack, i.e., selecting special session secrets for themselves. After that they invite other people to join while they gradually leave the conference. Finally the conference is going on with a completely different group of people without any of the attackers. However, the attackers still keep the NC's session secret and are able to decrypt the conference communication.

The second attack works conditionally when the number of the conferees is large. The attack is successful with a probability which grows with the number of the conferees. The probability is close to 1 when there are over several thousand conferees. The attack is passive since the attacker is not necessarily to join the conference. What he needs to do is just to intercept the communication and conducts some computation.

Let's describe briefly the scenario and the security goals of the protocol before discussing the weaknesses.

The network center (NC) is a trusted central authority responsible for authenticating the participants and generating and distributing session keys. The participants are U1, the chairperson initiating the conference, and U2; . . .; Um. Each user Ui is assumed to be in secure possession of a terminal Ti, which has a reliable clock. Each Ui shares a secret si = f(IDi) with the network center NC, where f is a secret one-way function known only to NC. The network center NC has a unique identity IDNC, while user Ui has unique identity IDi. The users are also assumed to have a reliable copy of NC's RSA public key (n; e). The public exponent e is assumed to be small.

The paper is organized as follows. The Hwang's Conference Key Distribution Protocol is presented in Section 2. The Attack is presented in Section 3. Security analysis in Section 4 and Section 5 concludes the paper.

2. PREVIOUS WORK

2.1 Hwang's Conference Key Distribution Protocol

Hwang proposed a new secure conference service for mobile communication. Their scheme establishes a common secret key for the valid conferee to hold a teleconference. In

1999, Hwang [4] further proposed a modified secure teleconference scheme, which allows the active participant to join or to exit an in-progress conference. In particular, both user authentication, as well as session key distribution are simultaneously included in Hwang's conference key distribution protocol. Next just review Hwang's scheme.

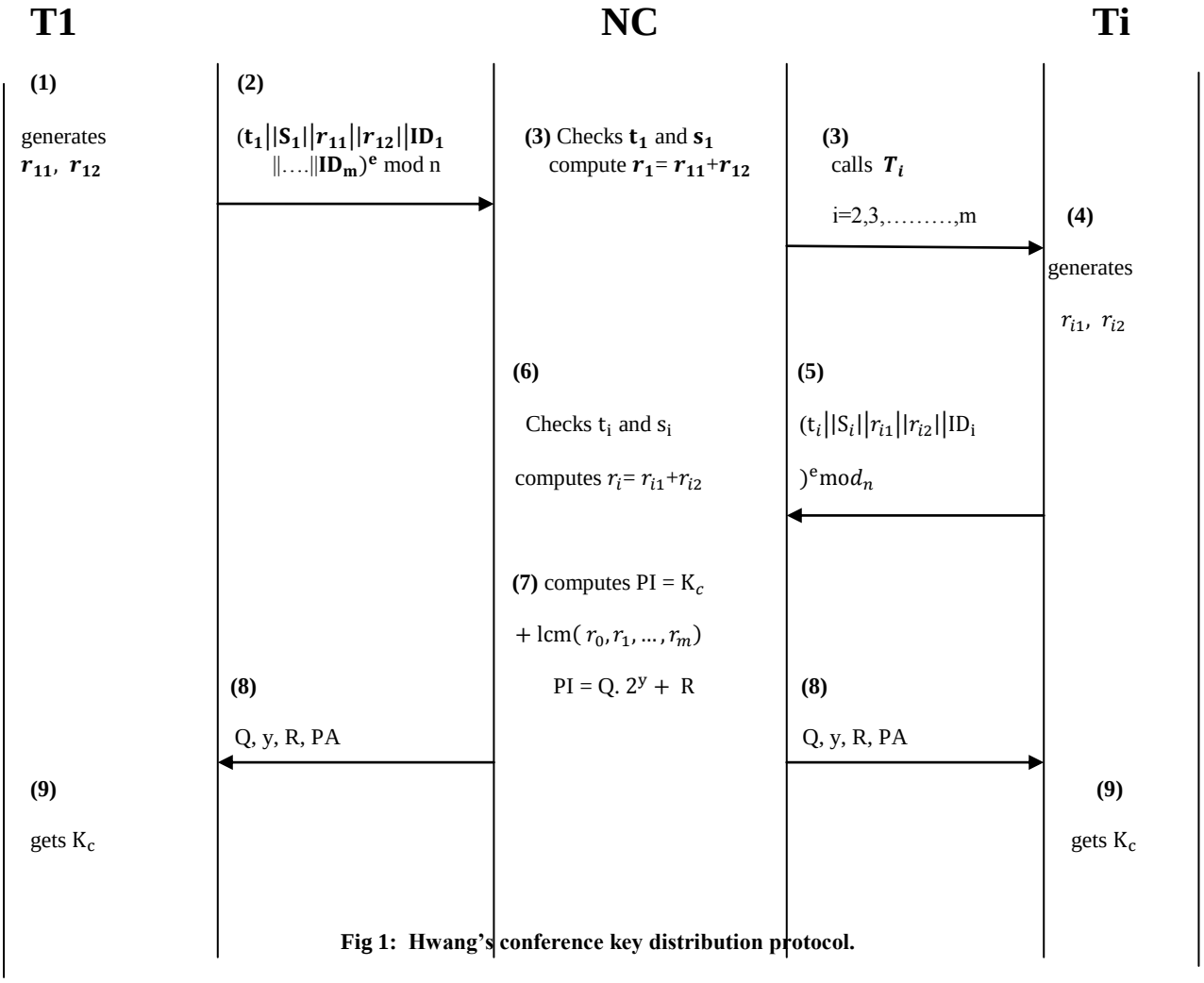

Fig 1: Hwang's conference key distribution protocol.

Step 1: The initial conference participant, say T_1 , selects two random numbers r11 and r12. Note that for an authorized participant T_i , the session key-decryption key r_i is formed by $r_{i1}+r_{i2}$.

Step 2: U1 sends (t1||s1||r11||r12|| IDi , for i=1,2,…,m)$^e \bmod d_n$ to the trusted network center (NC). Here, t_1 denotes the current date and time (timestamp), S_1 denotes T_1's authentication key which is generated by NC, such as $S_i = f(\text{IDi})$, where f is a secret one-way function held by NC. Moreover, NCs public key is denoted as , and IDi , i=1,2,…,m, represents the identity of users who are invited to join the conference.

Step 3: NC decrypts the encrypted data using its private key d , and then verifies whether is equal to f (ID1) and the validity of t_1. Then, NC calls the other mobile terminals' IDi 's, i=2,3,…,m .

Step 4: Each participant T_i , for i=2,…,m selects two random numbers r_{i1} and r_{i2} . Afterward, the session key-decryption key is obtained by $r_{i1}+r_{i2}$.

Step 5: T_i sends $(t_i||S_i||r_{i1}||r_{i2}||\text{IDi})^e \bmod d_n$ to NC, for i=2,3,…,m.

Step 6: NC decrypts the encrypted data and then verifies whether S_i is equal to $f(\text{IDi})$ and the validity of timestamp t_i.

Step 7: NC selects two nonzero random numbers K_c and r_0. Here, K_c denotes the session key of the secret conference. Next, NC calculates PI = $K_c + \text{lcm}(r_0, r_1, \ldots, r_m)$ and PA =$E K_c(ID_{NC})$. Here, lcm( ) denotes the least common multiple function.

Step 8: NC broadcasts Q, y , R , and PA to T_i, i=1,2,…,m. Here Q, y , and R are computed by the equation PI = Q. 2^y + R .

Step 9: Each participant T_i obtain K_c = (Q. 2^y + R) mod r_i , and then verifies the validity of K_c by checking whether PA is equal to $E K_c(ID_{NC})$.

When a participant Um+1 joins a conference in progress of the protocol are executed as follows except that Q. 2^y + R =

PI = K_c +rm+1. In this case, K_c remains unchanged for all other current participants.

When a participant Uj quits a conference in progress, NC chooses new random numbers K_c' and r_0' and computes $PI' = K_c' + lcm(r_i', i = 0,1,\dots,m, i \neq j)$ where $r_i' = r_i + t'$, with t' being the current timestamp. New Q', R', y' such that $PI' = Q' \cdot 2^{y'} + R'$ are computed and broadcast to T_i, i = 1,…,m,i ≠ j , together with t' .The T_is then obtain K_c' by computing $(Q' \cdot 2^{y'} + R') \bmod (r_i + t_i) = K_c'$.

3. ATTACK

The protocol used in [4] is insecure against eavesdropping once a participant joins a conference in progress. Before that, we examine the representation of PI by Q, y and R. Each r_i is a sum of two 256-bit numbers r_{i1} and r_{i2}. Therefore, r_i is a 257-bit number and PI = K_c + lcm(r0,….,rm) has at most 257(m+1) bits, not 256(m+1) bits, as claimed in [1]. Now, since Q and R are both 256-bit numbers, there will be cases when PI cannot be represented by Q, y, and R as claimed in the paper. However, since the representation of PI has no bearing on the security of the protocol, suppose that PI is broadcast as it is to the participants, and we show that the protocol is insecure nonetheless.

For ease of notation and without loss of generality, suppose that U1, U2, and U3 are already in conference using the session key K_c when U4 joins in the conference. When U4 joins, NC sends PI = K_c +r4 to U4, which is observed by U1, U2, and U3. Now, U1, U2, and U3 all know K_c and hence can obtain r4 by computing PI - K_c. If U3, say, should quit the conference after U4 joined, NC would broadcast a new session key K_c' + lcm(r_0', r1 + t', r2 + t', r4 + t') and t'. However, U3 would then be able to compute K_c' because he knows t' and r4 and hence would be able to eavesdrop on the conference that he has just left. Similarly, a new participant U5 may also follow the same line of attack by waiting for a participant to join before joining the conference himself and leaving immediately while continuing to be able to eavesdrop. This attack works because the new participant's secret is only masked by an entity K_c, which is known to all other current participants. One way of stopping this attack is to send $K_c + r_i . k_i$ for some random number k_i.

4. SECURITY ANALYSIS

In this section, analyze the security of the modified key distribution protocol, as well as discuss its performance. Hwang [4] pointed out that there are five security objectives for the secure conference service. We list these objectives as follows:

1)allowance for any active participant to join or to exit a conference;
2) prevention of fraud;
3) prevention of replaying attack;
4) privacy of conversation content;
5) privacy of participant's location information.

Since only the authentication mechanism has been altered in the modified key distribution protocol, the first objective remains. The second objective is achieved by verifying the correctness of the participant's identity IDi and its secret key s_i . A timestamp has been used here to resist the replaying attack. Thus, the modified protocol remains the third objective. Certainly, once the conference key has been successfully established, i.e., only the valid participants hold the correct conference key, the conversation content of the conference will be protected by a cryptosystem. The modified protocol also achieves the fourth objective, because the key distribution mechanism remains unchanged.

Finally, the last objective ensures that the information about participants' locations cannot be intercepted. In other words, any participant's identity IDi cannot be obtained by an intruder during the teleconference. Hwang's scheme uses a public-key cryptosystem to prevent the participant's identity from being revealed. Nevertheless, the modified protocol removes the public-key cryptosystem in order to simplify the complexity of mobile equipment. Therefore, the participant's identity IDi has to be revealed to the network center in order to obtain the corresponding secret key s_i . In other words, the information about participants' locations will be intercepted by an intruder. However, location-aware applications for the mobile user have been proven to have significant relevance for future telecommunication. That is to say, location-aware services and applications will become more popular in the future. Therefore, the importance of protecting the information about participants' locations is decreasing. Although the modified key distribution protocol may disclose information about the participant's location, it is still practical thanks to the location-aware service that has been increasingly used.

5. CONCLUSION

The conference key distribution protocol of [4] is designed to be dynamic. Therefore, it is important that the participants currently in conference should be known to all the participants. However, the only entity with this knowledge is K_c . The participants are authenticated by NC, and two participants U_i , U_j accept each other as authorized participants on the grounds that only authenticated participants know the session key K_c . However, because of the attack described above, this premise does not hold, and hence this conference scheme is insecure against impersonation as well as eavesdropping. So one way to prevent all these threats is to send $K_c + r_i . k_i$ for some random number k_i , so that r_i is never known by another participant.

REFERENCES

[1] H. C.Williams, "A modification of the RSA public key encryption procedure," *IEEE Trans. Inform. Theory*, vol. 26, pp. 726–729, Nov. 1980.

[2] I. Ingemarsson, D. T. Tang, and C. K. Wong, "A conference key distribution system," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 714–720, Sept. 1982.

[3] K. Koyama and K. Ohta, "Identity-based conference key distribution system," in *Proc. CRYPTO'87*, Santa Barbara, CA, Aug. 1987, pp. 194–202.

[4] M. J. Beller, L. F. Chang, and Y. Yacobi, "Privacy and authentication on a portable communications system," *IEEE J. Select. Areas Commun.*, vol. 11, pp. 821–829, Aug. 1993.

[5] M. S. Hwang andW. P. Yang, "Conference key distribution schemes for secure digital mobile

communications," *IEEE J. Select. Areas Commun.*, vol. 13, pp. 416–420, Feb. 1995.

[6] M. S. Hwang, "Dynamic participation in a secure conference scheme for mobile communications," *IEEE Trans. Veh. Technol.*, vol. 48, pp. 1469–1474, Sept. 1999.

[7] D K. F. Hwang and C. C. Chang, "A self-encryption mechanism for authentication of roaming and teleconference services," *IEEE Trans. Wireless Commun.*, vol.2, no. 2, pp. 400-407, Mar. 2003.

[8] X. Yi, C. K. Siew, and C. H. Tan, "A secure and efficient conference scheme for mobile communications," *IEEE Trans. Veh. Commun.*, vol. 52, pp. 784-793, July 2003.

[9] X. Yi, C. K. Siew, C. H. Tan, and Y. Ye, "A secure conference scheme for mobile communications," *IEEE Trans. Wireless Commun.*, vol. 2, pp. 1168-1177, Nov. 2003.

[10] Feng Bao, "Analysis of a secure Conference Scheme for mobile communication," *IEEE Trans. Wireless Commun.*, vol.5, no. 8, Aug. 2006.