On the Security of an Efficient Group Key Agreement Scheme for MANETs

Purushothama B R[1,*], Nishat Koti

Department of Computer Science and Engineering
National Institute of Technology Goa
Farmagudi, Ponda-403401, Goa, INDIA.
Email: {puru}@nitw.ac.in

Abstract

Yang et al. have proposed an efficient group key agreement scheme for Mobile Adhoc Networks. The scheme is efficient as only one bilinear computation is required for group members to obtain the session key. The scheme is analyzed for security without random oracle model. However, we prove that their scheme is not secure. In particular, we show that any passive adversary (or non-group member) can compute the session key without having access to the individual secret keys of the group members. Hence, Yang et al. scheme cannot be used for secure group communication. We also show that, the scheme cannot be used for secure group communication unless there exists a central entity, and hence cannot be used for secure communication in mobile adhoc networks.

Keywords: Key agreement, MANET, Cryptanalysis, Group Communication.

1. Introduction

Secure group communication among the set of users can be achieved by encrypting the group message with a key known as *group key*. The members of the group who possess the group key can obtain the message. The primary challenge in secure group communication is key management; to distribute

*Corresponding Author: Email: puru@nitgoa.ac.in, Phone: +91 9404882132

the group key efficiently among the group users. Group communication is also used in Mobile Adhoc Networks (MANET). MANETs have diverse applications ranging from small, static networks that are constrained by power sources to large-scale, mobile, highly dynamic networks. Security is a major concern for MANETs. For group communication among the MANET users, it should be ensured that only the intended receivers get the message and no adversary has access to the group message. An energy efficient group key agreement scheme is a demand in MANET, as devices in MANETs are battery operated and become unusable after the battery dies out. Therefore, energy of the nodes need to be used optimally. Also, MANETs are decentralized (there is no central server managing the group communication). This property of MANETs poses a challenge on group key agreement research for wireless mobile ad-hoc networks.

Group key management schemes may vary for different scenarios. There are centralized group key management schemes [1] which have the inherent problem of a single point of failure. Decentralized schemes [2] also exist with a few number of controllers for the users. However, these schemes would not prove efficient in MANETs. Diffie-Hellman protocol [3] can be used on a one-to-one basis for group key exchange. The two-party Diffie-Hellman protocol has been extended to multi-party protocols [4, 5, 6, 7]. In these protocols, one of the users has to carry out heavy computation, and hence it is not suitable for ad-hoc networks because of the extensive power requirements.

Yang et al. [8] have proposed an efficient group key management for MANET. The scheme is efficient and any group user need to perform only one bilinear operation to obtain the session key for the group communication. Yang et al. have compared their scheme with some of the existing secure key agreement schemes in [9, 10, 11, 12, 13, 14] and shown that their scheme is efficient. Also, they have analyzed the scheme for security and provided the proof of security under $q - BDHI$ assumption. However, we show that the scheme by Yang et al. [8] is not secure. Precisely, we show that any non-group user can get the session key of the group.

Rest of the paper is organized as follows. In Section 2 we briefly explain the Yang et al. [8] scheme. In Section 3, we comment on the security of their scheme and show that their scheme is insecure followed by conclusion.

2. Yang et al. Scheme [8]

In this section, we elaborate the group key agreement scheme proposed by Yang et al. [8] based on Identity Based Encryption System (IBES).

2.1. Bilinear maps

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two multiplicative cyclic groups of prime order p and g be a generator of $\mathbb{G}_1$. The bilinear map, $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ has the following properties:

1. *Bilinearity:* For all $u, v \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_p$, $e(u^a, v^b) = e(u, v)^{ab}$ is easily computable.
2. *Non-degeneracy:* $e(g, g) \neq 1$,
3. *Symmetric:* $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$.

2.2. System Model

Let $U = \{id_1, id_2, \ldots, id_N\}$ be the group of all N possible ad-hoc members that can form MANETs. There is a Private Key Generator (PKG) whose job is to set up the system parameters, authenticate the identity of the users, generate the private key for each authorized user, and distribute securely the generated private keys to their respective users. The scheme consists of four phases: *Setup, Extract, Encrypt* and *Decrypt*.

1. *Setup*: The PKG will generate the Master Secret Key MK and the public parameter PK for the system.
2. *Extract*: The PKG will first verify the identity of the user id_i and then will generate the corresponding private key s_{id_i}, if the verification of the user id_i is successful.
3. *Encrypt*: Consider a situation in which a group of users $S = \{id_1, \ldots, id_n\}$ have been selected to be the receivers using their wireless devices. There is a need to establish a session key (or group key) K for this group. The broadcaster will generate an encapsulation header Hdr for the group key K, after knowing the identities of the receivers. Then, the broadcaster will broadcast (S, Hdr).
4. *Decrypt*: After receiving (S, Hdr), the intended user with the identity $id_i \in S, i = 1, \ldots, n$, will be able to compute the group key K with his/her corresponding private key s_{id_i}. Any user with identity $id_i \notin S$, will not be able to get any information about K.

After the group key K is set up for the dynamic ad-hoc group, the message M will be encrypted using K to obtain ciphertext C by using an efficient symmetric encryption algorithm like AES or DES. The ciphertext C can be decrypted by the users who has the key K.

2.3. Yang et al. Scheme

1. **Setup**: Security parameter k is chosen along with N, which is the maximum number of MANET members of the system. PKG chooses the group $\mathbb{G}_1$ with order p. Also defines bilinear map as defined in section 2.1. Let the hash function be $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_p$. Randomly chooses a generator g of $\mathbb{G}_1$ and $\beta, \lambda \in \mathbb{Z}_p^*$. And, computes $U = g^\beta, V = g^\lambda$. PKG output the public parameter $PK = (g, U, V)$. PKG keeps secret the master secret key $MK = (\beta, \lambda)$.
2. **Extract:** PKG authenticates a user with identity id_i and computes the private key for the corresponding user. PKG chooses randomly $r_i \in \mathbb{Z}_p^*$ such that $H_1(id_i) + \beta + r_i\lambda \neq 0 \mod p$. PKG computes the private key $s_{id_i} = (s_{i,0}, s_{i,1}) = (r_i, g^{\frac{1}{H_1(id_i)+\beta+r_i\lambda}})$, and securely gives to user with identity id_i.
3. **Encrypt**: W.l.o.g, suppose the set of receivers is $S = \{id_1, \ldots, id_n\}$, $n \leq N$. The broadcaster chooses randomly a session key $K \in \mathbb{G}_1$ and randomly chooses $\tau \in \mathbb{Z}_p^*$. Broadcaster computes $Hdr = (C_0, C_1, C_2, C_3)$ where,

$$C_0 = Ke(g,g)^\tau, C_1 = g^\tau \prod_{j=1}^{n} H_1(id_j), C_2 = U^\tau, C_3 = V^\tau$$

   and broadcasts (S, Hdr).
4. **Decrypt**: The user with the identity $id_i \in S$ receives (S, Hdr) and computes as below to get the group key K.

$$K = \frac{C_0}{e(C_1^{\frac{1}{\prod_{j=1, j\neq i}^{n} H_1(id_j)}}.C_2.C_3^{s_{i,0}}, s_{i,1})}$$

3. Comment on the security of Yang et al. Scheme

In this section, we show that the scheme of Yang et al. [8] is not secure. Precisely, we show that the non-member of the group can get the session key of the group without possessing the private key of any of the group member.

Suppose, w.l.o.g let $S = \{id_1, id_2, \ldots, id_n\}$, $n \leq N$ want to form a group. The broadcaster chooses a session key $K \in \mathbb{G}_1$ and randomly chooses $\tau \in \mathbb{Z}_p^*$. Broadcaster computes $Hdr = (C_0, C_1, C_2, C_3)$ where,

$$C_0 = Ke(g,g)^\tau, C_1 = g^{\tau \prod_{j=1}^{n} H_1(id_j)}, C_2 = U^\tau, C_3 = V^\tau$$

and broadcasts (S, Hdr). By following the Decrypt method given in the previous section, the user with identity in S can get the session key K.

Now consider any non-member (any user of U such that the identity of the user is not part of S) of the group or any outsider (passive adversary $\mathcal{A}$). The adversary $\mathcal{A}$ has access to (S, Hdr). $\mathcal{A}$ does not have private keys of any of the user in S. However, $\mathcal{A}$ can obtain the session key K as below.

$$\begin{aligned} K &= \frac{C_0}{e(C_1^{(\prod_{i=1}^{n} H_1(id_i))}, g)} \\ &= \frac{K.e(g,g)^\tau}{e(g^{\frac{\tau \prod_{j=1}^{n} H_1(id_j)}{\prod_{i=1}^{n} H_1(id_i)}}, g)} \\ K &= \frac{K.e(g,g)^\tau}{e(g^\tau, g)} \\ &= \frac{K.e(g,g)^\tau}{e(g,g)^\tau} \end{aligned}$$

So, adversary $\mathcal{A}$ can obtain the session key K without possessing any of the private key of the users with the identity in S.

This scheme cannot be used for the group communication. The problem is in the design of the scheme. Any broadcaster (obviously who is a part of the MANET), will not have a public component which is the function of private keys of the users in S. Unless, there is a PKG involvement in broadcasting the session key, the scheme cannot be secure. If PKG is brought into the system, then it violates the basic idea of MANET. Also, PKG has to communicate with each user after every join and leave activity in the group which makes the scheme inefficient. Also, this scheme for obvious reasons does not support forward and backward secrecy requirement of the group communication scheme.

4. Conclusion

In this paper, we have commented on the security of the group key agreement scheme proposed by Yang et al. We have shown that any non-member or passive adversary may have access to the session key of the group, making the scheme insecure.

References

[1] V. Ayyadurai, R. Ramasamy, Internet connectivity for mobile ad hoc networks using hybrid adaptive mobile agent protocol, Int. Arab J. Inf. Technol. 5 (2008) 25–33.

[2] J. Hur, Y. joo Shin, H. Yoon, Decentralized group key management for dynamic networks using proxy cryptography, in: H.-H. Chen, L. Bononi (Eds.), Q2SWinet, ACM, 2007, pp. 123–129.

[3] W. Diffie, M. E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory 22 (1976) 644–654.

[4] I. Ingemarsson, D. T. Tang, C. K. Wong, A conference key distribution system, IEEE Transactions on Information Theory 28 (1982) 714–719.

[5] M. Steiner, G. Tsudik, M. Waidner, Diffie-hellman key distribution extended to group communication, in: L. Gong, J. Stearn (Eds.), ACM Conference on Computer and Communications Security, ACM, 1996, pp. 31–37.

[6] M. Steiner, G. Tsudik, M. Waidner, Cliques: A new approach to group key agreement, in: ICDCS, IEEE Computer Society, 1998, pp. 380–387.

[7] M. Steiner, G. Tsudik, M. Waidner, Key agreement in dynamic peer groups, IEEE Trans. Parallel Distrib. Syst. 11 (2000) 769–780.

[8] Y. Yang, Y. Hu, C. hui Sun, C. Lv, L. Zhang, An efficient group key agreement scheme for mobile ad-hoc networks, Int. Arab J. Inf. Technol. 10 (2013) 10–17.

[9] D. Boneh, C. Gentry, B. Waters, Collusion resistant broadcast encryption with short ciphertexts and private keys, in: CRYPTO, 2005, pp. 258–275.

[10] D. Boneh, B. Waters, A fully collusion resistant broadcast, trace, and revoke system, in: ACM Conference on Computer and Communications Security, 2006, pp. 211–220.

[11] C. Delerablée, Identity-based broadcast encryption with constant size ciphertexts and private keys, in: ASIACRYPT, 2007, pp. 200–215.

[12] X. Du, Y. Wang, J. Ge, Y. Wang, An id-based broadcast encryption scheme for key distribution, Broadcasting, IEEE Transactions on 51 (2005) 264–266.

[13] C. Gentry, B. Waters, Adaptive security in broadcast encryption systems (with short ciphertexts), in: EUROCRYPT, 2009, pp. 171–188.

[14] J. H. Park, H. J. Kim, H.-M. Sung, D. H. Lee, Public key broadcast encryption schemes with shorter transmissions, TBC 54 (2008) 401–411.