Asian Journal of Information Technology 15 (20): 4002-4010, 2016
ISSN: 1682-3915

Group Key Distribution Using Authentication Based Broadcast Encryption

[1]S. Prasanna, [1]S. Shunmuga Priya and [2]N. Balaji
[1]Department of Computer Science and Engineering,
Thiagarajar College of Engineering, Madurai, Tamil Nadu, India
[2]Department of Information Technology, K.L.N College of Engineering
Madurai, Tamil Nadu, India

Abstract: Group communication is crucial in today's contemporary world. Secure exchange of group key is essential to have secure group communication. Group key exchange in MANET is a great challenge and is the focus here. In this study, secure sroup key distribution in MANET based on identity based broadcast encryption is proposed. The group key can be generated by having minimal interaction among the group members. This reduces the computational time for group key generation. Only one bilinear pairing is required during key exchange which reduces the execution time. Authentication of the user is ensured before transferring the key. Forward and backward secrecy is guaranteed. The communication overhead remains minimal as the group size increases. This scheme is secure and more beneficial due to optimal time complexity.

Key words: Group communication, key distribution, MANET, identity based, broadcast encryption, authentication

INTRODUCTION

Network is the backbone of telecommunication. Due to vast use of handheld devices, MANET evolves as a blooming technology. MANET is an infrastructure less wireless network without centralized control and access point. The nodes are free to move. They are self configuring in nature as they join or leave the network at anytime. The network can be formed dynamically. Each node can perform either as source or destination or as a router. Nodes in the MANET have dynamic topology. MANET has an extensive application in military, rescue and recovery operations, tactical networks etc. as proposed by Corson and Macker Now a days MANETs are deployed in airport and internet of things as said by Veltri *et al.* (2013).

MANET with great flexibility and versatility faces many challenges. The resources such as bandwidth, power, memory, processing capability etc. are limited. According to Arabo *et al.* (2008) due to resource constrained feature, the routing process, power management, topology management, security becomes challenging. The MANET has access over air medium. So, it is prone to several security attacks. Brief classification of MANET security is given in Fig. 1.

A great demand for defense exists. One way to enhance security is to have good Identity management. Identity management has acquired its attention in the current era due to tremendous increase in identity theft as proposed by Mercuri (2006). One way of achieving security in information transfer and identity management is via Key management. Key management for group communication in focused here.

Group communication is distributing the same content or message among the intended group members who can vary with time. Group communication faces major problems compared to point to point communication as discussed by Yang (2014). Secure group communication involves agreeing of group key in a secure manner among the group members ahead of data communication. In order to improve the security, numerous keys are given to the users. Using the keys, the users generate encrypted messages and send it secretly. Group key management is widely used in Military, pay TV, commercial entertainment, software protection, encrypted email system internet of things, transmission of video and audio, updating software, applications, video games etc and so on surveyed by Ranjani *et al.* (2011).

The challenge lies in secure distribution of the key to the participants and managing key. The processes involved in group key management are key generation, key distribution, key updation and key revocation.

Since, the environment is dynamic the group participant's membership is also dynamic. Any member

Corresponding Author: S. Prasanna, Department of Computer Science and Engineering, Thiagarajar College of Engineering, Maduria, India

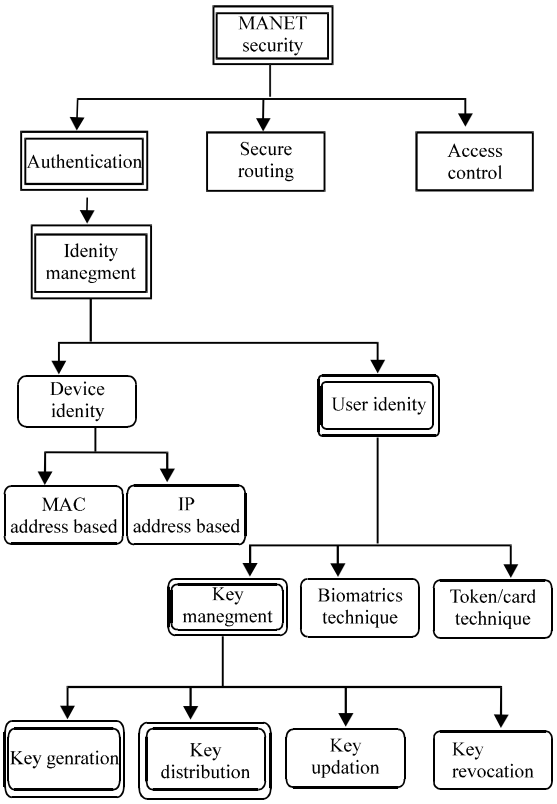

Fig. 1: Classification of MANET security

can leave the group or join the group at any time. So the group key must be updated. Certain parameters are considered to have efficient key management. The keys must be issued only to authorized entities. The key must be transferred in an indirect way. Forward secrecy and backward secrecy has to be obtained. Forward secrecy certifies that the members who were present in previous sessions but departed in the current session is unable to guess the current session key. Backward secrecy certifies that the non-members of the current session should be unaware of the current session key. The computation time for key generation and distribution must be optimum and constant as the group size varies. So, the criteria such as secure key exchange, authentication indirect transfer of key, time complexity, forward and backward secrecy plays a vital role in secure group key distribution.

The objective is to generate and distribute secret group key with minimum interaction among the group members for establishing secure group communication. Authentication must be ensured. The time complexity must be optimum with less overhead. Forward and backward secrecy should be pondered.

Literature review

Related works: Transfer of key among the communicating parties in a confidential way is more important for establishing secure communication. Due the constraints of MANETs key distribution in MANET is typically a critical task than in other networks as discussed by Yang (2014). Several approaches such as key pre-distribution, certificate based scheme, contributory scheme, public key cryptography scheme, etc. have been proposed. A brief description of each approaches and the task carried out in each approach is discussed as follows.

In key pre-distribution scheme, the key is distributed at the time of deployment before the data communication starts. It is similar to an institute or organization distributing the key to the users at the time of their registration. Many approaches for key pre-distribution have been put forward by Chan (2004). Ramkumar and Memon (2004). Ramkumar (2005) and Castelluccia *et al.* (2005). Chan (2004) recommended a method based on probability in which a key is chosen from a pool of keys and it is established among the participants. This method experiences stored keys exposure problem. Another method by Ramkumar and Memon (2004) uses one way hash function and public key generation function. This scheme lags since there is a trade-off between security and complexity. This scheme also suffers stored keys exposure problem and also outage probability exists. In an alternate method proposed by Ramkumar (2005). the random key pre-distribution is applied to broadcast encryption. But there is limitation in number of nodes being revoked. Threshold key pre-distribution proposed by Castelluccia *et al.* (2005) can also be employed. The Key pre-distribution method is inappropriate for MANET which is dynamic in nature.

The alternate method is certificate based scheme which involves a centralized Certificate Authority (CA) or a Trusted Third Party (TTP). In one such scheme as proposed by Porambage *et al.* (2013), the certificates are provided for the resource constrained sensor nodes and pair wise link keys for mutual node communication is established. Implicit certificates are used to generate the key. Wu *et al.* (2007) presents how the view of CA is created among the entire server group and the key management is performed. Moreover, the CA can be distributed based on threshold cryptography as discussed by Kravets. Due to the absence of centralized authority in MANET, some other good solution replacing the use of certification authority is required.

Next, let us probe through the contributory scheme in which all the participants contribute some entity for generating the key. Bresson and Manulis (2008) deals

with the contributory scheme and its role in presence of inspection of malicious nodes. A generic solution and a special compiler are proposed. Amir *et al*. (2004) proposed a robust scheme which is based on Group Diffie-Hellman (GDH) protocol by Steiner *et al*. (2000). key agreement and semantics provided by the GCS. Though there are many benefits in these methods, the key updation and key revocation becomes tedious. It is hectic to achieve optimal time complexity.

Public key cryptography is another method for key management which is essentially discussed in this study. Kong proposed TS-RSA a variant of RSA which is based on threshold based key allocation. This scheme is noticed to fail in verifiability and security which is discussed by Stanislaw *et al*. (2004). Another variant of RSA scheme proposed by Sun *et al*. (2007) is dual RSA. Though, it is storage efficient, the system's security must be scrutinized more. One more scheme proposed by Boldyreva *et al*. (2010) suggested a minor change of the well-known RSA-OAEP encryption scheme as proposed by Fujisaki *et al*. (2001). Achieving optimal time complexity is required.

Broadcast encryption scheme is one of the efficient schemes in the field of pairing based cryptography that was introduced by Fiat and Naor (1994). In this method the broadcaster or the sender chooses group members with their ID. Encryption involves usage of ID and decryption is with private keys. The significance of identity based broadcast encryption is avoiding message exchange. In a different method the users are arranged in leaves of binary tree and a common key for all subset of users is generated. This scheme needs more focus on time and space complexity. Then the first identity based broadcast encryption scheme was proposed by Delerablee (2007). The size of public key is linear and smaller than the number of possible users in the system. This author posts an interesting open problem to construct IBBE system with constant size cipher texts and private keys with security under more standard assumptions.

An efficient identity based batch multi signature scheme for asymmetric group key agreement is proposed by Zhang *et al*. (2011). The complexity in both communication and computation is required. Only partial forward secrecy property is met out. Dual system encryption is combined with IBBE scheme by Zhang *et al*. (2012) to improve the security using a normal key and a semi-functional key. From the analysis of the related work done so far, to have an efficient IBBE scheme, optimal time complexity, constant cipher text size and security needs to be addressed.

MATERIALS AND METHODS

Prerequisites: The preliminaries required are briefly discussed below.

Bilinear maps: Bilinear map is one of the best tools to pairing based cryptography as proposed by Okamoto (2006). Let G and G1 be two cyclic (multiplicative) groups of order p where p is prime and let g be a generator of the group G. A bilinear map e (also called ê) is a map e: G × G → G1 with the following properties:

- Bilinearity for all $\mu, v \in G$ G and α b $\in Z_p$ have e (μ^a, v^b) = e $(\mu, v)^{ab}$
- Non-degeneracy, e.g., g)≠1 (The map does not send all pair in G, G to identity in G Also, if g is a generator of G then is generator of G1
- Computability; there exists an efficient computation for e (μ, v) for all $\mu, v \in G$

Weil pairing and tate pairing are admissible maps as proposed by Boneh and Franklin (2003).

Hardness assumption : q-ABDHE problem: The security of the proposed scheme will be reduced to the hardness of the truncated q-ABDHE problem in the group in which the scheme is designed. A brief definition of truncated q-ABDHE problem proposed by Gentry (2006) is given below:

Definition: Given a group G which is of prime order, the generators g, h are randomly chosen from G and choose at random, α such that $\alpha \in Z_q$. Given tuple T = (g' g' $_{q+2}$ g' g'1 ,...α) and Z $\in G_1$ where: g_1 and g'^{i} denotes $g^{\alpha i}$ and g' $^{(\alpha i)}$ the truncated decisional q-ABDHE problem is to decide whether Z equals to e (g' $g^{\alpha+1}$) or to a random element of G_1.

Security model of IBBE: The security of our scheme predominantly relies on the underlying IBBE security. A simulation game between the challenger and adversary reduces the security of IBBE scheme to a mathematical hardness problem.

Let us assume that there exists an adversary A for whom all the messages in the network are available to it. The aim of is to attack the scheme and to decrypt any message which was intended to other set of users except him. *A* is successful if the following interactive game is won. The scheme can be proved to be secure IND-ID-CPA if the probability of guess of the adversary is greater than or equal to by Boneh *et al*. (2005).

Proposed scheme: The proposed scheme establishes a common group key called session key among the group members. Private Key Generator (PKG) exists which sets the necessary system parameters and generate private keys for the authorized users after authenticating them. The system parameter (public parameter) and private keys are generated from a master secret key and they only help to establish the common session key among the group. Using the system parameters the broadcaster of the group generates the session key and encapsulates it. The intended receiver set of the group is appended to it by the broadcaster and broadcasted. Only the authorized intended receiver can decrypt the session key with their own private key.

Components: Let the members in mobile ad hoc network $\{ID_1, ID_2,..., ID_n\}$ be . The role of PKG is only to generate system parameters and private key for all the users. Hence, the PKG can be made offline after the completion of the above procedures and not required by any users who want to setup a mobile ad hoc network. There are totally five phases in our scheme which is explained below. Work flow of the proposed scheme is illustrated above in Fig. 2.

Setup phase: The public parameter (PK) and the secret master key (m k) are generated in this phase. Given the security parameter k and the maximal size N of the members present in MANET, the PKG chooses a group G with prime order p where p≤ k . It randomly chooses the generators g h of G and master key randomly which belongs to Z_p. The master key is kept secret. It computes $g1 = g^{mk}$. It outputs the public parameter PK = [g' g1,h].

Authentication phase: The user who requests for private key is authenticated by PKG before issuing the key. A challenge response mechanism is made between the user and PKG which is explicated in the algorithm. Using the ID, nonce, time value, a nonce-based authentication value and authentication Id the user is substantiated to be valid. If the user is authenticated the status value is set to 1.

Extraction phase: The private key of each user is generated by PKG after authenticating the user. If the user is valid then the private key of that user is generated using user's ID, the generator value of the group and the master secret key. The private key is denoted by PR_{ID1i}. PKG randomly selects r_{ID}. The $\in Z_P$. If ID_i = mk, PKG aborts. Otherwise, calculate's ID_i's private key PR_{IDi}:

$$PR_{ID} = \left(PR_{I,0}, PR_{i,1}\right) = \left(r_{ID}, \left(hg^{r_i D_i}\right)^{1/(mk-ID_i)}\right) \quad (1)$$

The role of PKG is over.

Encryption phase: The Broadcaster encapsulates the session key and broadcasts it. The broadcaster chooses the receiver set S = { ID_1,..., IDn where, it n≤N selects a random session key K∈ G1. Then, it randomly chooses $\alpha \in Z_p$. It encapsulates the session key and forms the encapsulation header. It computes the encapsulation header Ehr = (E_0, E_1, E_2, E_3) as follows:

$$E_0 = K.e(g,h)^{-\alpha} \quad (2)$$

$$E_1 = g^{-\alpha \prod_{j=1}^{n} ID_j} \quad (3)$$

$$E_2 = e(g,g)^{\alpha} \quad (4)$$

$$E_3 = g1^{\alpha} \quad (5)$$

The output (S, HEr) is broadcasted in the system.

Decryption phase: The session key is retrieved from the encapsulation header by the intended user. The intended receiver with the identity $ID_i \in S$ can decrypt the received (S,EHr) with the user's own private key ($P R_{i,0}$, $P R_{i,1}$)R as follows:

$$K = E0.e\left(E_3.E_1^{1/\prod_{j=1, j\neq i}^{n} ID_j}, PRi,1\right)E_2^{PRi,0} \quad (6)$$

Now the session key is distributed among all the intended receivers in the group.

Note: With the help of this session key, any message M can be enciphered with K to obtain the cipher text C. The C can be deciphered by the users in the group. Thus secure group communication can be established.

As MANET is dynamic, the receiver set in the group S keeps changing. When there is a join or leave event in the group, the proposed scheme only wants to execute the encryption phase by adding or excluding the ID of that member the so that new session key is established.

Algorithm: The Algorithmic steps are as follows:

Setup phase:

Input: Security parameter k, size of MANET N
Output: Public parameter [g, h,g1]

- Choose a group g with a prime order p such that p≤k
- Randomly choose generators g,h of G
- Randomly choose master secret key, mk such that mk $\in Z_p$.
- Compute $g1 = g^{mk}$
- Make master Key secret and output the public parameter

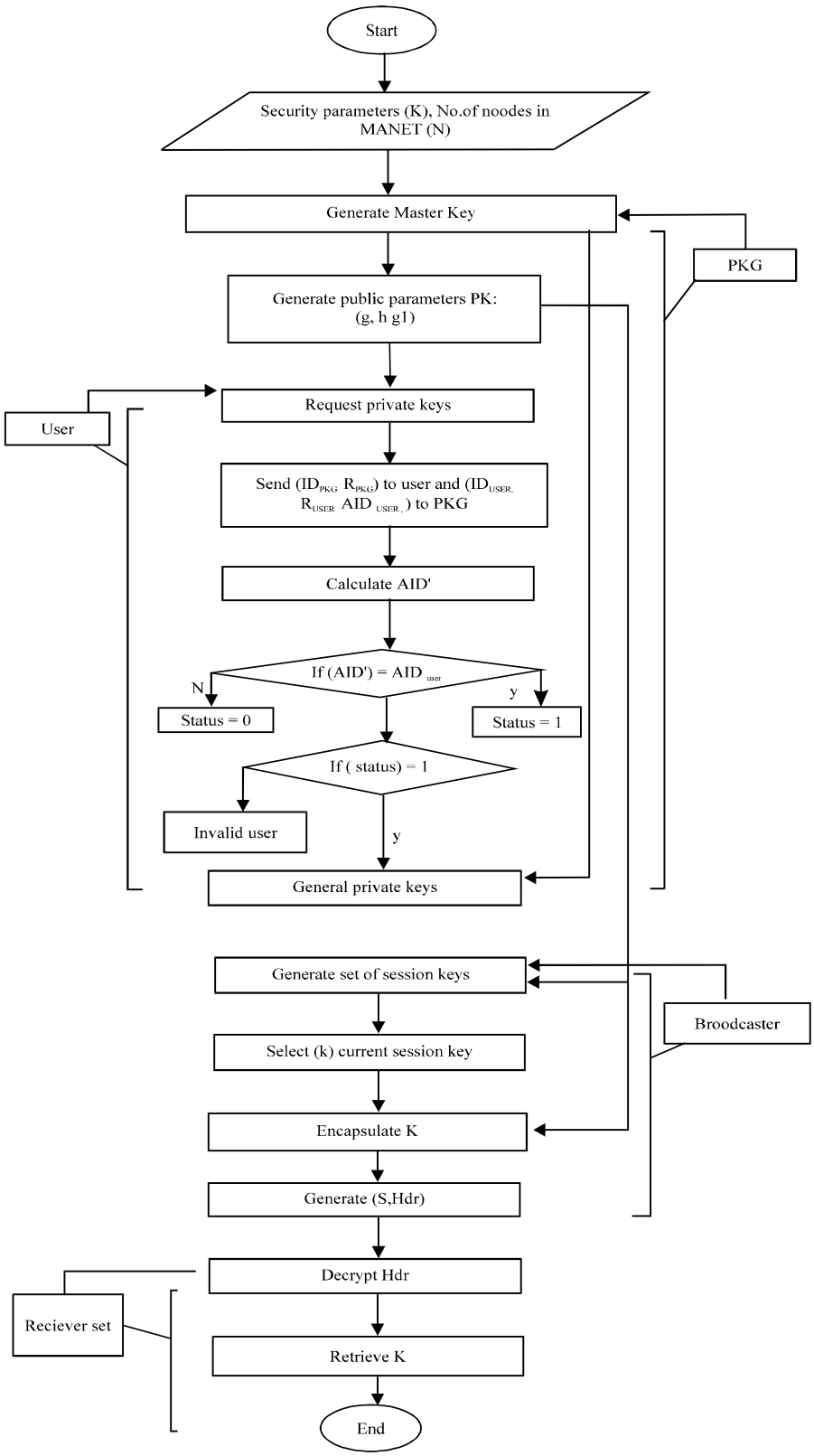

Fig. 2: Flow diagram of the proposed work

Authenticate phase:
Input: secret number of user/device sn.
Output: status //denotes the status of authentication.
Initialize: nonce n, large prime number p, g which is primitive root of p.
Notations: Nonce based authentication value R*,, Authentication_ID AID .

- **PKG:** Calculate ID_{PKG}, R_{PKG} and send to the user

$ID_{PKG} = g_{sn.PKG}$ modp
$R_{PKG} = gn_{PKG.}^{time}$ modp

- **User:** calculate $Id_{user,}$, R_{user} AID_{user} and send to PKG

$ID_{user} = g^{sn}{}_{user}$ modp
$R_{user} = g^{sn\ user}$ modp
$AID_{user} = (R_{user}^{sn.PKG})$ mod p
PKG: Calculate AID_{user} as

- If(aid' = aid)
- Status = 1//authentication success
- Optionally the above step can also be extended by user to authenticate PKG

Extract phase:
Input:
Output: Private key PR, ID_i

- If (status = 1)
- Selects random r $Id_i \in Z_p$
- If ($ID_i \neq mk$)

$$PR_{ID_i} = \left(PR_{i,0}.PR_{i,1}\right) = \left(r_{ID}, \left(hg^{-rID}\right)^{1/(i}\right.$$

Encrypt phase:

Output: Encapsulation header (S, EHR)

- Chooses the receiver set S = $\{ID_1,,,ID_n\}$

where: $n \leq N$

- Selects session key $K \in G1$
- Randomly chooses $\alpha \in Z_p$

Compute Encapsulation header EHR =(E_0, E_1, E_2, E_3)
where:
$E_0 = K.e(g, h)^{\alpha}$ $E_1 =$
$g^{-\alpha \Pi^n_{j=1}} Id_j$ $E_2 = e(g, g)^{\alpha} E^3 g1^{\alpha}$
Outputs (S,EH γ).

Decrypt phase:
Input : (S,EH γ)$\in$ S)
Output: Session key K

- If ($Id_i \in$ S)

K =

$$E_0.e\left(E_3.E_1.^{1/\Pi^n_{j=1,\, j\neq i}\, ID_j}, PR_{i,1}\right)E_2^{\,PR_{i,0}}$$

Implementation details: The proposed group key distribution scheme has been implemented in C language. PBC library (Pairing-Based Cryptography) is proposed by Lynn, a dedicated library for cryptography. The required pairing functions and mathematical operations can be efficiently implemented when using PBC library. This library is built over GMP library. The type-A elliptic curve parameter is chosen that provides 1024-bit discrete log security strength. The order of the group is preferred to be 160-bit. The execution time for all the phases under different group sizes (n values) is deliberated in efficiency 5.2. The execution time of the algorithm is calculated for various receiver set size that varies from 10-100.

RESULTS AND DISCUSSION

Analysis of the proposed scheme: In this study, we propose a group key distribution method using identity based broadcast encryption which provides an efficient key distribution solution in MANET with very minimal interaction among the nodes. Authentication is also met out. The use of bilinear maps only one time improves the scheme. Optimal time complexity is achieved. The benefits of the proposed scheme are as follows.

Less communication overhead: There is no interaction between the broadcaster and the receiver set during key establishment. The requisite is only one bilinear pairing computation. No pairing operations are required in the encrypt phase if the values are pre-computed and cached. It is obvious that decryption requires only one pairing operation.

Apart from this, each member in the group is assigned a unique identity which acts as the public key. This avoids the need for the users to create their own public keys and the process of distributing these public keys is also avoided. Authentication over digital signatures with certificate issued by a trusted Certificate Authority (CA) is also circumvented. So, the communication overhead is appreciable.

Constant size: The size of the public parameters, private key and cipher text are constant.

Dynamic: If any join or leave event occurs instead of executing the entire module, it is sufficient to execute the encrypt and decrypt phase alone. The broadcaster needs to add or remove the ID corresponding to the member change. This facilitates the key updation and Key revocation process to be easy.

Forward secrecy: Whenever the member leaves the current session a new key can be exchanged among the group members efficiently. The newly exchanged key after the leave event of a member will be unpredictable by the members who left the study.

Backward secrecy: The non-members of the group will be unable to guess the current session key.

Confidentiality: The group key is confidentially distributed to the group members. Any nonmember cannot retrieve the session key since private key for decrypting the session key is absent.

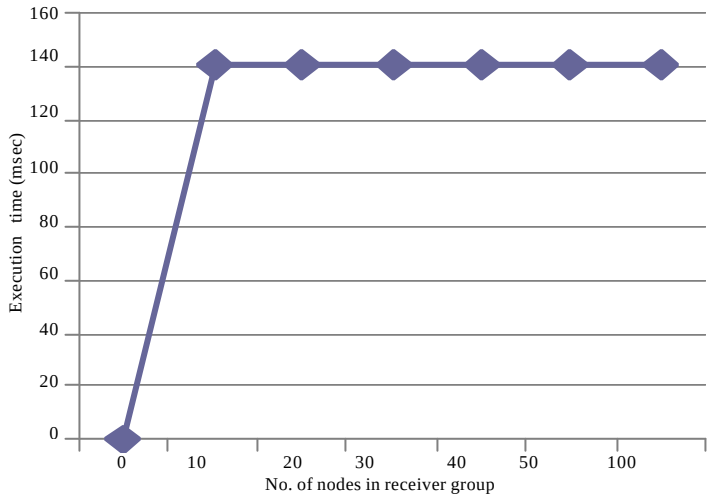

Fig. 3: Analyzing time complexity of the scheme.

Security: The key generation and key distribution process is secure enough.

Authentication: The user is ensured to be valid before issuing the private key.

Correctness: The correctness of the scheme can be substantiated as follows. When performing decryption the session key is retrieved as below:

$$E_0.e(E_3E_1^{1/\Pi_{j=1,j\neq i}^{n} ID_j}, PR_{i,1})E_2^{PR_{i,o}} \quad (7)$$

Substitute the values for and fter simplification, we get:

$$E_0.e\left(g1^{\alpha}.g^{-\alpha.IDi}, PR_{i,1}\right)E_2^{PR_{i,0}} \quad (8)$$

Substitute the values for private keys and E_2:

$$E_0\, e\left(g1^{\alpha}, g^{-\alpha IDi}\left(hg^{-rIDi}\right)^{1/(mk-ID_i)}\right) e(g,g)^{\alpha rID_i} \quad (9)$$

Substitute the value and simplify further:

$$E_0.\left(g^{\alpha}, \left(hg^{-rID}\right)\right)e(g,g)^{\alpha rID} \quad (10)$$

On further simplification we get

$$E_0.(g,h)^{-\alpha} \quad (11)$$

Comparing Eq. 2 in encrypt phase with (Eq. 11), K is retrieved.

Table 1: Execution time for the proposed scheme

No. of nodes in each group	Execution time (ms)
10	140.658
20	140.311
30	141.202
40	140.910
50	140.424
100	140.815

Table 2: Evaluation of public parameter, private key and cipher text size.

IBBE Scheme	Public parameter size	Private key size	Cipher text size
Du *et al.* (2005)	Constant	Constant	Varies with n
Boneh *et al.* (2005)	Varies with n	Constant size	Constant size
Park *et al.* (2008)	Varies with n	Constant size	Constant size
Gentry and Waters (2009)	Varies with n	Varies with n	Constant size
Boneh and Waters (2006)	Varies with	Varies with	Varies with
Zhang *et al.* (2012)	Varies with n	Constant size	Constant size
Our scheme	Constant size	Constant size	Constant size

Table 3: Analysis of required pairing and presence of authentication

IBBE schemes	Encrypt (pairing)	Decrypt (pairing)	Presence ssof Authentication
Du *et al.*(2005)	1	2	No
Boneh *et al.* (2005)	0	2	No
Park *et al.* (2008)	0	2	No
Gentry and Waters (2009)	0	2	No
Boneh and Waters (2006)	0	4	No
Zhang *et al.* (2012)	0	2	No
Our scheme	0	1	Yes

Efficiency: The execution time of our algorithm for various group sizes is measured and is shown in Table 1. The algorithm is run by setting group members from 10-100 and in each trial the execution time is measured and tabulated. The unit for execution time is given in mille seconds.

The execution time for various receiver group sizes is plotted in Fig. 3. A linear graph is obtained. It is obvious from the graph that, as the receiver group size increases, the execution time remains constant. So, an optimal time complexity of 0(1) is obtained.

Comparative analysis: The proposed scheme is compared with other broadcast schemes and IBBE schemes. Let the size of the receiver set be denoted by n. Table 2 compares our scheme with other scheme on the basis of size of public parameter, private key and cipher text size.

Table 3 compares our scheme with other schemes on the basis of number of pairings used in encrypt and decrypt phase. The presence of authenticating the user before issuing the private key is also analyzed.

Security analysis: The role of PKG is made offline after the Extract phase thereby preventing compromise of PKG. The intruders will never get a chance to generate the private key for any identity by compromising the PKG, since it is made offline before the encrypt phase. The private key is issued to the users only after authenticating the users. A malicious user is incapable to obtain private key. So, the session key cannot be captured by the unauthorized entities. Due to the order of the key size chosen, the brute force attack is made impossible.

CONCLUSION

In this study we present a communication effective, authentication ensured Key distribution scheme for mobile ad hoc network based on identity based broadcast encryption. The dynamic group membership change requires the group key to be updated. An appealing property of the proposed scheme is that, it only needs to include or exclude the respective member's ID during the encryption phase for generating the new group key. No matter how the group size varies, the communication overhead is unchanged since the group key encapsulate on remains constant which strengthen the proposed mechanism. The experimental results show that the proposed research is time efficient and secure enough by authentication phase before issuing the keys.

Future work: The proposed scheme can be improved by enhancing PKG that results in increased availability. The scheme can be implemented in any real time scenarios. Added, the authentication for the broadcaster can be guaranteed by verifying digital signatures or through some analogous mechanisms.

REFERENCES

Amir, Y., Y. Kim, C. Nita-Rotaru, J.L. Schultz, J. Stanton and G. Tsudik, 2004. Secure group communication using robust contributory key agreement. IEEE Trans. Parallel Distrib. Syst., 15: 468-480.

Arabo, A., Q. Shi, M. Merabti and J.D. Llewellyn, 2008. Identity management in mobile ad-hoc networks (IMMANets): A survey. Proceedings of the 9th Annual Postrgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting (PGNet 2008), June 23-23, 2008, Liverpool John Moores University, Liverpool, England, UK., ISBN: 978-1-902560-19-9, pp: 23-24.

Boldyreva, A., H. Imai and K. Kobara, 2010. How to strengthen the security of RSA-OAEP. IEEE. Trans. Inf. Theor., 56: 5876-5886.

Boneh, D. and B. Waters, 2006. A fully collusion resistant broadcast, trace and revoke system. Proceedings of the 13th ACM Conference on Computer and Communications Security, October 30-November 3, 2006, ACM, Alexandria, Virginia, USA, ISBN: 1-59593-518-5, pp: 211-220.

Boneh, D. and M. Franklin, 2003. Identity-based encryption from the Weil pairing. SIAM. J. Comput., 32: 586-615.

Boneh, D., C. Gentry and B. Waters, 2005. Collusion Resistant Broadcast Encryption With Short Ciphertexts and Private Keys. In: Advances in Cryptologyâ€“CRYPTO 2005, LNCS 3621, Shoup, V. (Ed.). Springer-Verlag, Berlin, Germany. ISBN: 0302-9743 (Print) 1611-3349 (Online), pp: 258â€“275.

Bresson, E. and M. Manulis, 2008. Contributory group key exchange in the presence of malicious participants. IET. Inf. Secur., 2: 85-93.

Castelluccia, C., N. Saxena and J.H. Yi, 2005. Self-Configurable Key Pre-Distribution in Mobile Ad Hoc Networks. In: NETWORKING 2005. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems, Raouf, B., K. Almeroth, R. Puigjaner, S. Shen and J.P. Black (Eds.). Springer, Berlin, Germany, ISBN: 978-3-540-25809-4, pp: 1083-1095.

Chan, A.F., 2004. Probabilistic distributed key predistribution for mobile ad hoc networks. Proceedings of the 2004 IEEE International Conference on Communications, June 20-24, 2004, IEEE, Ontario, Canada, ISBN: 0-7803-8533-0, pp: 3743-3747.

Delerablee, C., 2007. Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys. In: Advances in Cryptology-ASIACRYPT 2007, Kurosawa, K. (Ed.). Springer, Berlin, Germany, ISBN: 978-3-540-76899-9, pp: 200-215.

Du, X., Y. Wang, J. Ge and Y. Wang, 2005. An ID-based broadcast encryption scheme for key distribution. IEEE. Trans. Broadcasting, 51: 264-266.

Fiat, A. and M. Naor, 1994. Broadcast encryption. Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology, April 19-23, 1993, Springer-Verlag, New York, USA., pp: 480-491.

Fujisaki, E., T. Okamoto, D. Pointcheval and J. Stern, 2001. RSA-OAEP is Secure Under the RSA Assumption. In: Advances in Cryptology-CRYPTO 2001, Kilian, J. (Ed.). Springer, Berlin, Germany, ISBN: 978-3-540-42456-7, pp: 260-274.

Gentry, C. and B. Waters, 2009. Adaptive Security in Broadcast Encryption Systems (with Short Ciphertexts). In: Advances in Cryptology-EUROCRYPT 2009, Antoine, J. (Ed.). Springer, Berlin, Germany, ISBN: 978-3-642-01000-2, pp: 171-188.

Gentry, C., 2006. Practical Identity-based Encryption without Random Oracles. In: Advances in Cryptology, Vaudenay, S. (Ed.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-34546-6, pp: 445-464.

Mercuri, R.T., 2006. Scoping identity theft. Commun. ACM., 49: 17-21.

Okamoto, T., 2006. Cryptography Based on Bilinear Maps. In: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Marc, P.C.F., H. Imai, L. Shu and P. Alain (Eds.). Springer, Berlin, Germany, ISBN: 978-3-540-31423-3, pp: 35-50.

Park, J.H., H.J. Kim, M.H. Sung and D.H. Lee, 2008. Public key broadcast encryption schemes with shorter transmissions. IEEE. Trans. Broadcast., 54: 401-411.

Porambage, P., P. Kumar, C. Schmitt, A. Gurtov and M. Ylianttila, 2013. Certificate-based pairwise key establishment protocol for wireless sensor networks. Proceedings of the 2013 IEEE 16th International Conference on Computational Science and Engineering (CSE), December 3-5, 2013, IEEE, Oulu, Finland, ISBN: 978-0-7695-5096-1, pp: 667-674.

Ramkumar, M. and N. Memon, 2004. An efficient random key pre-distribution scheme. Proceedings of the IEEE Conference on Global Telecommunications GLOBECOM'04, November 29-December 3, 2004, IEEE, arkville, Mississippi, USA., ISBN: 0-7803-8794-5, pp: 2218-2223.

Ramkumar, M., 2005. On Broadcast Encryption with Random Key Pre-Distribution Schemes. In: Information Systems Security, Sushi, J. and C. Mazumdar (Eds.). Springer, Berlin, Germany, ISBN: 978-3-540-30706-8, pp: 304-316.

Ranjani, R.S., D.L. Bhaskari and P.S. Avadhani, 2011. Current trends in group key management. Curr. Trends Group Key Manage., 2: 82-86.

Stanislaw, J., S. Nitesh and H.Y. Jeong, 2004. An attack on the proactive RSA signature scheme in the URSA Ad Hoc network access control protocol. Proceedings of the Workshop on Security of Ad Hoc and Sensor Networks, October 25, 2005, Washington, DC. USA., pp: 1-9.

Steiner, M., G. Tsudik and M. Waidner, 2000. Key agreement in dynamic peer groups. IEEE Trans. Parallel Distrib. Syst., 11: 769-780.

Sun, H.M., M.E. Wu, W.C. Ting and M.J. Hinek, 2007. Dual RSA and its security analysis. IEEE Trans. Inform. Theory, 53: 2922-2933.

Veltri, L., S. Cirani, S. Busanelli and G. Ferrari, 2013. A novel batch-based group key management protocol applied to the internet of things. Ad Hoc Netw., 11: 2724-2737.

Wu, B., J.Wu, E.B. Fernandez, M. Ilyas and S. Magliveras, 2007. Secure and efficient key management in mobile ad hoc networks. J. Network Comput. Appl., 30: 937-954.

Yang, Y., 2014. Broadcast encryption based non-interactive key distribution in MANETs. J. Comput. Syst. Sci., 80: 533-545.

Zhang, L., Q. Wu, B. Qin and F.J. Domingo, 2011. Provably secure one-round identity-based authenticated asymmetric group key agreement protocol. Inf. Sci., 181: 4318-4329.

Zhang, L., Y. Hu and Q. Wu, 2012. Adaptively secure identity-based broadcast encryption with constant size private keys and ciphertexts from the subgroups. Math. Comput. Modell., 55: 12-18.