Australian Journal of Basic and Applied Sciences, 9(11) May 2015, Pages: 47-53

ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Trust based Group Key Agreement in MANET using Broadcast Encryption

[1]Shunmuga Priya, S and [1]Prasanna, S, [2]Dr. Balaji, N

[1]*Department of Computer Science and Engineering, Thiagarajar College of Engineering, Madurai-15, India*
[2]*Department of Information Technology, K.L.N College of Engineering, Madurai, India*

ARTICLE INFO

Article history:
Received 12 March 2015
Accepted 28 April 2015
Available online 5 May 2015

Keywords:
Group communication, Key agreement, MANET, Trust, Broadcast encryption, Security, Computational time.

ABSTRACT

Mobile Ad hoc Network (MANET) is an infrastructure less wireless network where the nodes are self configuring and movable. Security in MANET is one of the major challenges and it is concentrated here. Group communication in MANET plays a vital role in the flourishing research world. Group communication is transmitting the same content to the members of the group. The group members are free to join or leave the group at any time instant. Secure group key agreement paves way for secure group communication. Secure group key agreement in MANET is challenging and is focused here. In this paper, secure and time efficient group key agreement based on trust calculation and identity based broadcast encryption is proposed. Group Key (or session key) is generated and agreed among the group members using bilinear mapping. Added, Private and Public keys are initially generated for encompassing the key-encryption-key technique. The intended group key is encrypted by the public key at the sender and decryption is by users own private key. Trust is calculated for every node in the network. Ahead of distributing the key to the user, the trust value is verified to be greater than the fixed threshold so that security is safeguarded. The scheme is implemented in C using PBC library. The network traces are obtained from NS2. The results obtained focus on proving the optimal time complexity with constant computation time, even though the group size varies. The computational time is reduced by having minimal interaction among the group members during key generation and by having only one bilinear pairing during key agreement. Correctness of the key agreement is mathematically proved. Security is ensured using trust evaluation. Forward and backward secrecy is pondered in the algorithm which can facilitate the key update and key revocation in future. Communication overhead remains minimal even when the group size varies. This scheme is more secure and advantageous due to optimal time complexity.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: Shunmuga Priya, S and Prasanna, S, Dr. Balaji, N, Trust based Group Key Agreement in MANET using Broadcast Encryption. ***Aust. J. Basic & Appl. Sci.,*** *9(11): 47-53, 2015*

INTRODUCTION

In today's world MANET is evolving due to intensive research and substantial use of handheld devices. MANET is a dynamic network with the absence of infrastructure, centralized control and access point. The nodes in it are mobile and self configuring as they can join or leave the network any time. Every node is capable to take the role of source or destination and router. MANET has a massive application comprising military, rescue operations, internet of things, tactical networks (Corson and Macker,1999). Resource constrained feature in MANET creates many challenges in routing process, power management, topology management, security and so forth. The secure data transfer in MANET is also risky due to the presence of malicious node.

A serious necessity for security exists in MANET. Identity management is one of the best solutions for enhancing security. The increasing identity theft (Rebecca Mercuri, 2006) has earned immense consideration towards identity management. Key management is a premium preference for achieving Identity management. Key management is applicable for peer to peer communication and group communication. The latter one faces several difficulties than the former one (Yang Yang, 2014). Group communication delivers same information among the intended group members who are dynamic. The users in military, pay TV, commercial entertainment, software protection, encrypted email system are some of the beneficiaries of Group communication.

Prior to data communication, the secret group key must be agreed among the group members to preserve security. With this agreed group key, secure message exchange can be progressed using encryption techniques. Many challenges are to be

Corresponding Author: Shunmuga Priya, S, Department of Computer Science and Engineering, Thiagarajar College of Engineering, Madurai-15, India.

addressed in group key distribution. The join and leave event requires periodic key refreshment. The forward and backward secrecy should be pondered while designing the Key management algorithm. Optimum time complexity and indirect transfer of key should be achieved. Also the capture of the group key must be difficult for malicious nodes. Trust evaluation ensures this, thereby improving security. Trust value is evaluated based on some trust parameters and calculated for every node present in the network. A threshold value is predefined to filter out malicious nodes. To ensure the security, the trust value must be greater than the fixed threshold value. When this trust evaluation is performed the malicious nodes or malicious users can be detached from the group and secure group communication can be carried out.

MATERIALS AND METHODS

Related work:

Several approaches such as key pre-distribution, certificate based scheme, contributory scheme, public key cryptography scheme, etc. have been proposed. A brief glimpse of the task accomplished in each of the approach is discussed below.

In key pre-distribution scheme, the distribution of key takes place at the time of deployment ahead of data communication. A good example is an institution or organization distributing the key to the users during their registration. Chan *et al*. (2004) recommended a method based on probability, in which a key is chosen from a key pool and established among the participants. This method suffers stored keys exposure problem. Another method by Ramkumar and Memon (2006) uses one way hash function and public key generation function. This scheme lags since a trade-off between security and complexity exists. Added, stored keys exposure problem and outage probability exists. The Key pre-distribution method is inappropriate for MANET due to dynamic nature.

The alternate method is certificate based scheme that involves a centralized certificate Authority (CA) or a Trusted Third Party (TTP). In one such scheme, the certificates are provided for resource constrained sensor nodes. Pair wise keys for mutual node communication are established. Implicit certificates are used for key generation. Due to absence of centralized authority in MANET, some other good solution replacing the use of certification authority is required. Let us probe through the Contributory scheme where all the participants contribute some entity for key generation. Bresson and M. Manulis (2003) present the contributory scheme in presence of malicious nodes using a generic solution and a special compiler. Despite many benefits, the key update and revocation becomes tedious. It is chaotic to achieve optimal time complexity.

Public Key Cryptography is another method for Key management, essentially discussed in this paper. In TS-RSA by Kong *et al*., a variant of RSA, uses threshold cryptography. This scheme is pointed to fail in verifiability and security by Jarecki *et al*. (2004). Broadcast Encryption scheme is one of the effective methods in the field of Pairing based cryptography, introduced by Fiat and Naor (1994), in which encryption involves usage of ID and decryption is with private keys. The significance of Identity based broadcast encryption is avoiding message exchange. In the first identity based broadcast encryption scheme (Delerablee, 2007), the size of public key is linear and smaller. 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 by Delerablee (2007) for asymmetric group key agreement is proposed. The complexity in both communication and computation is required. Only partial forward secrecy property is met out. A trust based key management scheme by Lei zhang *et al*. (2011), performs key management based on trust evaluation. The performance should be maximized and vulnerability should be reduced. Another task by Echo *et al*. (2013), organizes the network into clusters in which trust is the clustering criterion. Here malicious nodes from the session are evicted. From the analysis the research findings and the problem identified is that the group key generation and distribution require substantial computation time and have security issues. The motivation from the analysis is to construct a time efficient and secure Group Key agreement that possess constant cipher text size.

Preliminaries:

The preliminaries for key agreement are briefly discussed below.

A. Bilinear maps:

Let G and G1 be two cyclic (multiplicative) groups of prime order p and let g be a generator of the group G.

A bilinear map e (also called bilinear pairning) is a map $e: G \times G \rightarrow G1$ has the following properties: (Drira, 2010)

1. Bilinearity : for all $u, v \in G$ G and $a, b \in Z_p$, we have $e(u^a, v^b) = e(u, v)^{ab}$.
2. Non-degeneracy :$e(g, g) \neq 1$. The map does not allow all pair in $G \times G$ to identity in G. Also, if g is a generator of G then the generator of $G1$ is$e(g, g)$.
3. Computability : there exists an efficient computational procedure or algorithm for $e(u, v)$, for all $u, v \in G$.

Weil pairing and Tate pairing are admissible maps (Tatsuaki Okamoto, 2006).

B. 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 (Gentry,2006).

Definition: Given a group G with prime order q, the generators g, h are randomly chosen from G and choose α such that $\alpha \in Z_q$. Given a tuple $T = \left(g', g'_{q+2}, g, g1, \ldots, g_q\right)$ and $Z \in G_1$, where g_i and g'_i denotes g^{α^i} and $g'^{(\alpha^i)}$, the truncated decisional q-ABDHE problem is to decide whether Z equals to $e(g', g_{q+1})$ or to a random element of G_1.

C. 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 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 $1/2 + \varepsilon$ (Boneh *et al*., 2005).

Proposed work:

The objective of the proposed scheme is to establish a common group key (session key) among the group members by having minimal interaction to ensure time efficiency and by using trust evaluation to ensure security which is depicted in Fig.1.

In the proposed scheme a common group key (session key) is established among the group members. For every node present, trust value is evaluated. Private Key Generator (PKG) sets the required system public parameters and constructs private keys from a randomly generated Master key. They are used for establishing the common session key among the group and they are not our intended group key. The private key is generated for every user and issued to all the authorized users after ensuring the security using the trust value. This key is used for decrypting our session key. Session key is generated and encrypted using the system public parameter. The intended receiver set of the group is also appended to it. The broadcaster of the group performs this task. Any node or member in the group which sends the message can act as broadcaster. The session key available in the medium can be decrypted only with receiver's own private key.

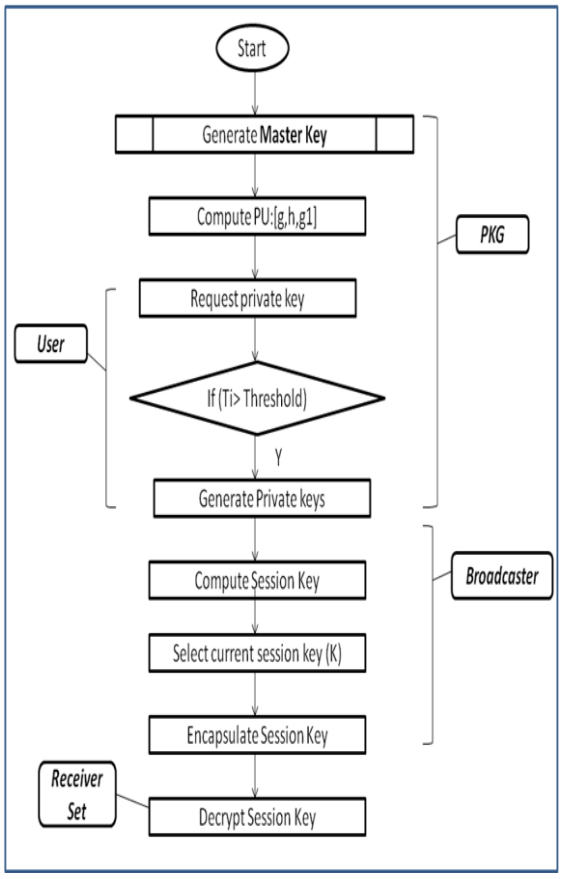

Fig. 1: Flow diagram for Group Key Agreement scheme.

A. Component:

Let the MANET members be $\{ID_1, ID_2, \ldots, ID_n\}$. The PKG generates public parameters and private key for all users. It is made offline and is not needed by any users who require setting MANET. There are five modules.

1) Setup module:

The focus of this module is to generate the master secret key (msk) and required public parameters (PU). Given security parameter k and maximum number of nodes present in MANET N, the PKG selects a group G with prime order p where $p \leq k$. It randomly selects generators g, h of G, master key that belongs to Z_p that is maintained secret. It computes $g1 = g^{msk}$ and the public parameter $PU = [g, g1, h]$.

2) Trust Evaluation module:

Trust value for every node in the network is calculated based on its behavior. The parameters used for trust calculation are Intimacy and Truthfulness. Intimacy refers to the average count of interactions between any two nodes and is calculated between every node pairs in the same radio range.

$T_{intimacy_{i,j}}$ gives intimacy value of node i calculated by j. It is the count of interaction made

between i and j for the given interval of time. $T_{intimacy_i}$ is the average value of all $T_{intimacy_{i,j}}$ node pairs. This evaluation determines the malicious node in the following way. The malicious node does not interact with all nodes present in the same radio range in the same manner. It tends to interact more often with the compromised node. Calculation of $T_{intimacy}$ determines the presence of malicious node based on its interactive behavior.

$$T_{intimacy_i} = \frac{\sum T_{intimacy_{i,j}}}{n} \quad (1)$$

$T_{Truthfulness}$ refers to legitimate and straightforward behavior of any node. Set of anomaly detection rules are used to compute it. The malicious activities(MA_i) such as dropping of packet, repletion, delay of packet are scrutinized and their count is recorded. If count of a malicious activity crosses the threshold then $T_{Truthfulness_i}$ becomes 0. Else it is the ratio of count to the threshold and is given by

$$T_{Truthfulness_i} = Avg\ of\ \frac{count\ of\ MA_i}{MA_i threshold} \quad (2)$$

The overall trust value of a node is given by

$$T_i = (w1.T_{intimacy_i} + w2.T_{Truthfulness_i})/2 \quad (3)$$

The values $w1, w2$ are the weight values which decide which part (intimacy or truthfulness) should dominate the trust value and this can be chosen by system. The trust value calculated lies in the range (0,1). Trust value is evaluated for all nodes present thereby estimating the security level of it. A threshold value is fixed.

3) Extraction module:

The private key of each user is generated by PKG after ensuring their security. The user is considered to be secure if the trust value higher than the predefined threshold value. If the user is valid then the private keyPR_{ID_i} is created using the user's ID, generator value of the group and master secret key. PKG randomly selects $r_{ID_i} \in Z_p$. If ID_i and msk are equal then the PKG aborts. Else, it calculates ID_i's private key PR_{ID_i}.

$$PR_{ID_i} = (PR_{i,0}, PR_{i,1}) = (r_{ID_i}, (hg^{-r_{ID_i}})^{1/(msk-ID_i)}) \quad (4)$$

4) Encryption Phase:

The session key is encapsulated by the Broadcaster and broadcasted. Broadcaster selects receiver set $R = \{ID_1, \dots, ID_n\}$ where $n \leq N$. It chooses a random session key $K \in G1$. It randomly picks $\alpha \in Z_p$ and encapsulates the session key to form encapsulation header. It computes the encapsulation header $EHdr = (E_0, E_1, E_2, E_3)$ as follows

$$E_0 = K.e(g,h)^{-\alpha} \quad (5)$$

$$E_1 = g^{-\alpha.\prod_{j=1}^{n} ID_j} \quad (6)$$

$$E_2 = e(g,g)^{\alpha} \quad (7)$$

$$E_3 = g1^{\alpha} \quad (8)$$

The output $(R, EHdr)$ is broadcasted in the system.

5) Decryption Phase:

The intended user can retrieve session key from the encapsulation header that is available in the broadcast medium. The intended receiver with the identity $ID_i \in R$ can decrypt $(R, EHdr)$ with user's own private key $(PR_{i,0}, PR_{i,1})$ as follows

$$K = E_0.e\left(E_3, E_1^{1/\prod_{j=1, j\neq i}^{n} ID_j}, PR_{i,1}\right) E_2^{PR_{i,0}} \quad (9)$$

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

B. Note:

Any message can be enciphered and deciphered with the session key K to produce the cipher text C using encryption algorithms like AES. Thus a secure group communication can be achieved. As the mobile ad hoc network is dynamic in nature, the receiver set keeps changing in the group. The Encryption phase of the proposed scheme wants to be executed at the time of join or leave events, by including or excluding the ID of the respective user or node. So a new secret key is generated thereby forward secrecy is achieved.

C. Algorithm:

The Algorithmic steps are as follows,

1. Setup Module:

Input: security parameter$k$, Size of MANET N

Output: Public Parameter $PK: [g, h, g1]$

i. Choose a group G with a prime order p such that $p \leq k$.

ii. Randomly choose generators g, h of G; master secret key $msk \in Z_p$.

iii. Compute $g1 = g^{mk}$ and output the public parameter.

2. Trust Evaluation module:

Input: weight values w1,w2

Output: Trust value of each node

Initialize: Past history of all nodes

i. Compute $T_{intimacy_i}$ and $T_{Truthfulness_i}$

ii. Compute $Trust_i$

iii. Fix threshold for trust.

3. Extract Module:

Input: $user\ id: ID_i$

i. If $(Trust_i) > threshold$, randomly choose $r_{ID_i} \in Z_p$.

ii. If$(ID_i \neq mk)$, calculate $PR_{ID_i} = (PR_{i,0}, PR_{i,1})$

4. Encrypt Module:

Output: Encapsulation Header $(R, EHdr)$

i. Chooses the receiver set $R = \{ID_1, \dots, ID_n\}$ where $n \leq N$.
ii. Selects session key $K \in G1$ and randomly choose $\alpha \in Z_p$
iii. Compute Encapsulation header $EHdr = (E_0, E_1, E_2, E_3)$and output $(R, EHdr)$ where

$E_0 =$

$K.e(g,h)^{-\alpha} \quad E_1 g^{-\alpha \prod_{j=1}^{n} ID_j}$

$E_2 = e(g,g)^{\alpha} \quad E_3 = g1^{\alpha}$

5. *Decrypt Phase:*

Input: (S, EHr)

Output: Session Key K

If($ID_i \in S$),retrieve

$K =$

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

D. Implementation Details:

The proposed group key distribution scheme has been implemented in C language. The past history details required for trust calculation is taken from the trace file of sample MANET environment using NS2. To perform key generation and distribution, PBC library (Pairing-based Cryptography) by Lynn, a dedicated library for cryptography is used. The needed pairing functions and mathematical operations can be effectively implemented when using PBC library. This library is built on the top of GMP library. The type-A elliptic curve parameter is chosen which provides 1024-bit discrete log security strength. The group order is generally preferred to be 160-bit. The execution time for all the modules with different group sizes (n values) that varies from 10 to 100 is computed and is deliberated in section 5.2.

RESULTS AND DISCUSSIONS

In this paper, we propose a Secure Group Key Distribution method using identity based broadcast encryption which provides an effective key distribution solution in MANET with very minimal interaction among the nodes. Security is also met out. The bilinear map is used only once and it improves the scheme. Optimal time complexity is achieved.

The benefits of our scheme are as follows

Minimal communication overhead:

Minimal interaction between the broadcaster and the receiver set during key establishment, use of bilinear pairing computation only once reduces the overhead. If the values in Encrypt phase are pre-computed and cached, the requisite of pairing operations is removed. It is obvious that decryption requires only one pairing operation.

Since, unique identity is assigned for each member in the group, the need for public key creation and distribution is avoided. Authentication over digital signatures with certificate issued by a trusted Certificate Authority (CA) is also eluded. So, the communication overhead is appreciable.

Constant size:

The size of the public parameters, private key and cipher text are stable.

Dynamic:

Any join or leave event requires only the execution of Encrypt and Decrypt module instead of the entire modules. The broadcaster needs to include or exclude the ID corresponding to the member change. This facilitates the Key update and Key revocation to be very simple.

Forward secrecy:

On join or leave events, a new key can be established among the group that will be unpredictable by the left out members of the group.

Backward secrecy:

The non-members of the group will be unable to predict session key of current session.

Confidentiality:

The group key is distributed confidentially to the group members. It is tricky for any non-member to retrieve the session key since private key for decrypting the session key is absent.

Security:

The key generation and key distribution process is secure enough. The trust evaluation helps to eliminate the involvement of malicious node in group communication.

A. Correctness:

The substantiation of correctness of our scheme is as follows:

Session key retrieval in decryption module is

$$E_0 . e\left(E_3 . E_1^{1/\prod_{j=1, j\neq i}^{n} ID_j}, PR_{i,1}\right) E_2^{PR_{i,0}} \quad (10)$$

Simplifying after substituting the values for E_3 and E_1, we get

$$E_0 . e(g1^{\alpha} . g^{-\alpha . ID_i}, PR_{i,1}) E_2^{PR_{i,0}} \quad (11)$$

Substitute the values for private keys and E_2

$$E_0 . e(g1^{\alpha} . g^{-\alpha . ID_i}, (h g^{-r_{ID_i}})^{1/(msk - ID_i)}) e(g,g)^{\alpha r_{ID_i}} \quad (12)$$

Substitute the value $g1$ and simplify further

$$E_0 . e(g^{\alpha}, (h g^{-r_{ID_i}})) e(g,g)^{\alpha r_{ID_i}} \quad (13)$$

On further simplification we get

$$E_0 . e(g,h)^{-\alpha} \quad (14)$$

Comparing the equation (8) in encryption module with (14),

K is retrieved.

B. Efficiency:

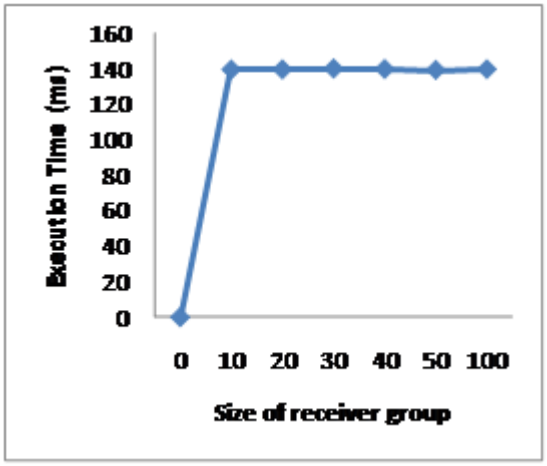

Fig. 2: Time complexity analysis of the scheme.

The execution time for various receiver group sizes is plotted in Fig.2 that gives a linear graph. It is observable from the graph that, as the receiver group size increases, the execution time remains constant which gives an optimal time complexity of $O(1)$. The execution time (in mille seconds) for various group sizes is shown in Table1.

Table 1: Execution Time for the proposed scheme.

Nodes in each group	Execution Time (ms)
10	139.658
20	139.711
30	140.202
40	139.910
50	139.424
100	139.815

C. Comparative Analysis:

The proposed scheme is compared with other broadcast schemes and IBBE schemes below. Let the size of the receiver set be represented by n. Table 2 compares our scheme with other scheme on regarding public parameter, private key and cipher text sizes. Comparisons regarding number of pairings used in encrypt and decrypt phase, Security check before issuing private key is given in Table 3.

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	Constant size
Park *et al*. (2008)	Varies with n	Constant	Constant size
Gentry and Waters(2009)	Varies with n	Varies with n	Constant size
Boneh, and Waters (2006)	Varies with $\sqrt{n}$	Varies with $\sqrt{n}$	Varies with $\sqrt{n}$
Zhang *et al*. (2012)	Varies with n	Constant	Constant size
Our Scheme	Constant	Constant	Constant size

Table 3: Analysis of required pairing and presence of authentication.

IBBE Scheme	Encrypt (pairing)	Decrypt (pairing)	Security check during issuing of key
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

D. Security Analysis:

The role of PKG is offline after the Extract module that prevents the PKG compromise. The intruders or malicious nodes will never get a chance to generate the private key for any identity by compromising the PKG, since it is offline before the encrypt phase. The private key is issued to the users only after checking the security level of the users using trust evaluation. A malicious user is incapable to obtain private key. So, the session key is unavailable for unauthorized entities. Due to the order of the key size chosen, the brute force attack is also unfeasible.

E. Conclusion and future work:

This paper presents a communication effective secure Key distribution scheme for mobile ad hoc network based on identity based broadcast encryption. A desirable property of the proposed scheme is that, it only needs to add or remove the respective member's ID in the encryption process for generating the new group key when group membership changes. The communication overhead is unchanged for any group size and the group key encapsulation remains constant, which strengthen the proposed mechanism. The experimental results illustrates that the proposed work is time efficient and secure due to trust evaluation.

In future, the proposed scheme can be improved by enhancing PKG that results in increased availability. The algorithm can be extended by developing key update and key revocation procedures. The scheme can be implemented in any real time scenarios. Added, the authentication for the users and broadcaster can be guaranteed by verifying digital signatures or through some analogous mechanisms.

REFERENCES

Boneh, D., B. Waters, 2006. A Fully Collusion Resistant Broadcast, Trace, And Revoke System. Proceedings of the 13th ACM Conference on Computer and Communications Security, pp: 211–220.

Boneh, D., C. Gentry, B. Waters, 2005. Collusion Resistant Broadcast Encryption with Short Ciphertexts And Private Keys. Proceedings of Crypto'05 ,in:Lecture Notes in Computer Science, 3621: 258–275.

Bresson, E., M. Manulis, 2003. Contributory Group Key Exchange In The Presence Of Malicious Participants. IET Information Security, 2(3): 85-93.

Chan, A.C.F., 2004. Probabilistic Distributed Key Pre Distribution for Mobile Ad Hoc Networks. IEEE International Conference on Communications, 6: 3743–3747.

Cho, J.H., Kevin chan, Ing ray chen, 2013. Composite Trust based public key management in mobile ad hoc networks. In Proceedings of the 28th Annual ACM Symposium on Applied Computing, pp: 1949-1956.

Corson, S. and J. Macker, 1999. Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. IETF RFC 2501.

Delerablee, C., 2007. Identity based Broadcast Encryption with Constant Size Ciphertexts and Privatekeys. Proceedings of Asiacrypt'07, Lecture Notes in Computer Science, 4833: 200–215.

Drira, K., H. Seba, H. Kheddouci, 2010. ECGK: An efficient clustering scheme for group key management in MANETS, 33(9): 1094-1107.

Du, X.J., Y. Wang, J.H. Ge, Y.M. Wang, 2005. An ID- Based Broadcast Encryption Scheme For Key Distribution. IEEE Transactions on Broadcasting, 51(2): 264–266.

Fiat, A., M. Naor, 1994. Broadcast Encryption, Proceedings of CRYPTO'94, Lecture Notes in Computer Science, 773: 480–491.

Gentry, C., 2006. Practical identity-based encryption without random oracles. Proceedings of 25th Annual International Cryptology Conference, pp: 445-464.

Gentry, C., B. Waters, 2009. Adaptive Security In Broadcast Encryption Systems (With Short Ciphertexts). Proceedings of Eurocrypt'09, in: Lecture Notes in Computer Science, 5479: 171–188.

Jarecki, S., N. Saxena and J.H. Yi, 2004. An Attack on the Proactive RSA Signature Scheme in the URSA Ad Hoc Network Access Control Protocol. In Proceedings of ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '04), pp: 1-9.

Kong, J., P. Zerfos, H. Luo, S. Lu and L. Zhang, 2001. Providing Robust and Ubiquitous Security Support for Mobile Adhoc Networks. In Proceeding of IEEE International Conference on Network Protocols.

Lei zhang, Qianhong wu, Bo qin, Josep domingo-Ferrer, 2011. Provably Secure One-Round Identity Based Authenticated Asymmetric Group Key Agreement. Elsevier, Information sciences, 181(19): 4318-4329.

Lynn, B., The PBC library, http://crypto.stanford.edu/pbc/.

Park, J., H. Kim, M. Sung, Lee, 2008. Public Key Broadcast Encryption Schemes With Shorter Transmissions. IEEE Transactions on Broadcasting, 3(54): 401–411.

Ramkumar, M. and N. Memon, 2006. An Efficient Random Key Pre-Distribution Scheme. IEEE Journal on Selected areas in Communications, 23(3): 611-621.

Rebecca Mercuri, T., 2006. Scoping Identity Theft. ACM Communication, 49: 17-21.

Tatsuaki Okamoto, 2006. Cryptography Based On Bilinear Maps. Springer, AAECC, of Lecture Notes in Computer Science, 3857: 35-50.

Yang Yang, 2014. Broadcast Encryption Based Non-Interactive Key Distribution In Manets. Journal of Computer System Science, 80(3): 533-545.

Zhang, L., Y. Hu, Q. Wu, 2012. Adaptively Secure Identity- Based Broadcast Encryption With Constant Size Private Keys And Ciphertexts From The Subgroups. Mathematical and Computer Modelling, 55(1–2):12–18.