K. Poorna Surya Teja* et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.4, Issue No.6, October – November 2016, 4412-4417.

A Secure Group Key Agreement With Local Connectivity Using Multicast Key Management

K.POORNA SURYATEJA
M.Tech Student
CNIS,SNIST

K.SREERAM MURTHY
Assistant Professor
Dept of IT,SNIST

Abstract: **In this paper, we study Group key Agreement which mean multiple parties want to create a common secret key to be used to exchange information securely. The group key agreement with an arbitrary connectivity graph, where each user is only aware of his neighbor and has no information about the existence of other users. Further, he has no information about the network topology. We implement the existing system with more efficient manner and provide a multicast key generation protocol. We replace the Diffie-Hellman key exchange protocol by a new multicast key exchange protocol that can work with One to One and One to Many functionality. We also tend to implement a strong symmetric key encryption for improving file security in the system.**

Keywords: **Multicast Exchange Protocol; Group Key Agreement**;

I. INTRODUCTION

In dispersed system, gathering key assertion convention assumes a vital part. They are intended to give a gathering of clients with a common secret key such that the clients can safely speak with one another over an open system. Gathering key understanding means numerous gatherings need to make a typical secret key to be utilized to trade data safely. We think about the gathering key concurrence with a self-assertive network diagram, where every client is just mindful of his neighbors and has no data about the presence of different clients. Further, he has no data about the system topology. In our issue, there is no focal power to instate clients. Each of them can be instated autonomously utilizing PKI (public key infrastructure). A gathering key assertion for this setting is exceptionally suitable for applications, for example, an interpersonal organization. Under our setting, we develop two productive latently secure conventions. We likewise demonstrate lower limits on the round Complexity which shows that our conventions are round proficient.

In specially appointed system, the clients are typically portable. The gathering part is not known ahead of time and the clients may join and leave the gathering much of the time. In such situations, element gathering key understanding conventions are needed. Such plans must guarantee that the gathering session key over upon gathering part changing such that consequent session keys are shielded from the leaving individuals and past session keys are shielded from the joining individuals. There are very much various element gathering key understanding conventions. Client security implies that any leaving part room a gathering can't produce new gathering and joining part into a gathering can't find beforehand utilized gathering key. In this task we actualize the current framework with additional time productive way and give a multicast key era server which is normal in future extension by current creators. We supplant the Diffie- Hellman key trade convention by another multicast key trade convention that can work with balanced and one to numerous usefulness. We likewise tend to execute an in number symmetric encryption for enhancing document security in the framework.

II. SCOPE

A group key agreement in this setting is very suitable for applications such as social networks. We constructed two passively secure protocols with constructiveness and proved lower bounds on a round complexity, demonstrating that our protocols are round efficient. Finally, we constructed an actively secure protocol from a passively secure one. In our work, we did not consider how to update the group key more efficiently than just running the protocol again, when user memberships are changing.

III. EXISTING SYSTEM

Key pre-distribution system (KPS) (a.k.a. non-interactive conference distribution system) can be regarded as a non-interactive group key agreement. In this case, the shared key of a given group is fixed after the setup. If a group is updated, then the group key changes to the shared key of the new group. The drawback of KPS is that the user key size is combinatorial large in the total number of users (if the system is unconditionally secure). Another drawback is that the group key of a given group cannot be changed even if it is leaked unexpectedly (e.g., cryptanalysis of cipher texts bearing this key). The key size problem may be overcome if a computationally secure system is used, while the key leakage problem is not easy. Further, computationally secure KPS is only known for the two party case and the three-party case KPS with a group size greater than 3 is still open.

Disadvantages

The user key size is combinatorial large in the total number of users (if the system is unconditionally secure).The group key of a given group cannot be changed even if it is leaked unexpectedly.

IV. PROPOSED SYSTEM

The group key agreement with an arbitrary connectivity graph, where each user is only aware of his neighbors and has no information about the existence of other users. Further, he has no information about the network topology. Under this setting, a user does not need to trust a user who is not his neighbor. Thus, if one is initialized using PKI, then he need not trust or remember public-keys of users beyond his neighbors

Advantages

To update the group key more efficiently than just running the protocol again, when user memberships are changing. Two passively secure protocols with contributiveness and proved lower bounds on a round complexity, demonstrating that our protocols are round efficient.

V. PRELIMINARIES

Notations: We will use the following notions.

For a set S, x ←S samples x from S uniformly randomly;

Function: N→R is negligible if for any polynomial

$p(x)= \lim_{n\to\infty}\mu(n)\, p(n) = 0$.

X is Alice, Y is bob , a is common prime key.

$X = P^x \bmod(a)$ is the a (prime values), x which indicatives secret integer of alice, x_i which indicatives public key of alice, P primitive root.

Now Alice compute, $(Y)^x{}_i \bmod(a)$

Now he is getting one value that is k

$Y = P^y \bmod(a)$ is the a (prime values) , y which indicatives secret integer of bob, y_i which indicatives public key of bob. P primitive root.

Now Bob compute, $(X)^y{}_i \bmod(a)$

Now he is getting one value that is k.

Alice and Bob now share a secret (the value k)

Indistinguishability

Two ensembles are indistinguishable if no efficient algorithm can tell them apart. This notion was first proposed by Goldwasser and Micali in case of encryption.

Generally, it was due to Yao[15].

Definition 1: Ensembles $X = \{X_\alpha\}_{\alpha \geq 1}$ and $Y = \{Y_\alpha\}_{\alpha \geq 1}$ are indistinguishable if for any Diffie-algorithm D,

$|\Pr[D(X_\alpha) = 1] - \Pr[D(Y_\alpha) = 1]|$ is negligible.

In a cryptographic system, α usually is the security parameter and implicitly defined. For example, in a RSA system, α is the bit length of the modulus N.

Decisional Diffie-Hellman assumption

Consider a (multiplicative) cyclic group G of order p, and with generator g. The DDH assumption states that, given g^x and g^y for uniformly and independently chosen $x,y \in Z_p$ the value g^{xy} looks like a random element in G.

The decisional Diffie-Hellman assumption is as follows.

Definition 2: The decisional Diffie-Hellman assumption

(DDH) holds if (g^x, g^y, g^{xy}) where x and y are randomly and independently chosen from Z_p

$(g^x; g^y; g^z)$ where x,yand z are randomly and independently chosen from Z_p

The subgroup of k th residues modulo a prime a, where (a-1)/k is also a large prime (also called a Schnorr group). For the case of k=constant , this corresponds to the group of quadratic residues modulo a safe prime.

The following lemma can be easily proved by a hybrid reduction and it appeared in[16].

Lemma 1: Let n to N. Then, under the DDH

Assumption, $\{g^{ai,aj}\ 1 \_ i < j \_ n\} \cap \{g, g^{a1}, \ldots., g^{an}\}$

And $\{g^{aij} \mid 1 \leq i < j \leq n\} \cap \{g, g^{a1}, \ldots., g^{an}\}$

Indistinguishable, where a_{ij} $(1 \_ i < j \_ n)$ and $a_{1\ldots\ldots}a_n$; are all uniformly random from Z_q:

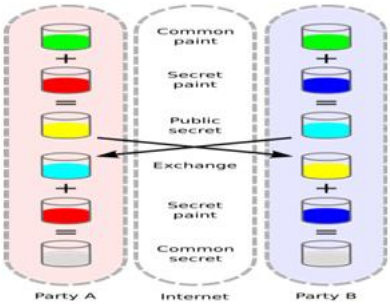

FIG: - Diffie- hellman Key Exchange

Algorithms:

Multicast key Management protocol Algorithm

(Active User)

Stage one.

0. Each $i \in V$ takes $a_i \rightarrow Z_q$ and sets $A_i = g_a i$:

1. Each leaf user s in G (i.e., $N_s = x$) sets $A_s i = 1$ and sends $(A_s i, A_s)$ to i:

2. [**Loop**] Each V does the following.

For i € N, if user has received (A_i ,A_j) from each j € N_n and did not send (A_i , A) to i, then he computes A_i = j €N_n and sends (A_i , A_j) to i.

3. Each user continues stage 2 until he has sent (A_i , A) to user i for each i 2 N`, in which case, he proceeds to Stage two.

Stage two.

1. Each leaf user s (i.e., N_s = x) computes L_si =A and sends C_si = E_si (L_si) to user i:

2. [**Loop**] Each V does the following. For i € N, if user has received Cj from each j € N and did not send C_i to i then he decrypts L_j = D_j (C_j), defines

L_i = (j€N_n f(x)L),(j€N A_j)a and sends C_i = E (L_i) to user i.

3. Each user continues stag 2 until he has sent C_i to user i for each i € N, in which case, he proceeds to Stage three.

Stage three *(group key derivation).*

Upon C_s for all S€ N, user decrypts L_s = D_s (C_s) (if not done before) and calculates group key s_k = Q_s€ N (L_s , A_s) = Q (u.v)=V(g_a).

(Passive user)

Stage one.

Each user (i, v) takes a $_i$; Z $_q$; c $_i$, f(X) and defines Ai = g_a i Then, user i sends A_i to his neighbors N_i and receives A_j from each j € N

Stage two.

1. Each leaf user s (with N_s = X) computes c_si = c_i and sends C_si = E_si (c_si) to i:

2. [**Loop**] Each V does the following.

For i € N, if user has received Cj from all j € N_n X and did not send C_i then he decrypts C_j= D_j(C_j), computes C_i = C_l(C_j€N_n f(x) C_s(i)) and sends C_i = E_i (c_i) to user i:

3. Each user continues stag 2 until he has sent C_i to each i € N in which case, he proceeds to Stage three.

VI. LITERATURE REVIEW

In this paper, a gathering key understanding issue where a client is just mindful of his neighbors while then network diagram is discretionary. In our issue, there is no unified instatement for clients. A gathering key concurrence with these elements is extremely suitable for informal communities. Under our setting, we develop two proficient conventions with detached security[1].

In an element validated gathering key assertion convention is exhibited utilizing blending for impromptu systems. In Join calculation, the quantity of transmitted messages does not increment with the quantity of all gathering individuals, which makes the convention more functional. The convention is provably secure. Its security is demonstrated under Decisional Bilinear Diffie-Hellman supposition. The convention likewise gives numerous different securities property[2].

We are gathering key concurrence with hub confirmation plan has been proposed. It's a changed from which consolidates the components and benefits of both Flexible Robust Group Key Agreement and additionally Efficient Authentication Protocol for Virtual Subnet convention. The fundamental point of preference of proposed plan is that it dispenses with the need to send the different parameters for verification and additionally gathering key commitment[3].

This paper addresses a fascinating security issue in remote specially appointed system: the dynamic Group key Agreement key foundation. For secure gathering correspondence in Ad hoc system, a gathering key shared by all part. In this paper creator proposed a novel secure versatile and powerful Region-based gathering key understanding convention for Ad hoc system[4].

A Group Key Agreement (GKA) convention is an instrument to set up a cryptographic key for a gathering of members in light of every one's commitment, over an open system. The key, along these lines inferred, can be utilized to set up a protected channel between the members. In this paper, Author displays a straightforward, secure and productive GKA convention appropriate to element impromptu systems. We additionally present consequences of our usage of the convention in a model application[5].

This paper exhibits an effective contributory gathering key understanding convention for secure correspondence between the lightweight little gadgets in subjective radio portable specially appointed systems. A Ternary tree based Group ECDH.2 (TGECDH.2) convention that uses a cluster rekeying calculation amid enrollment change is proposed in this paper. This ternary tree is an adjusted key tree in which proper insertion point is chosen for the joining individuals amid rekeying operation. TGECDH.2 joins the computational effectiveness of ECDH convention and the correspondence proficiency of GDH.2 convention. From the execution investigation, it is deduced that the TGECDH.2 beats a current ternary tree based protocol[6].

This paper exhibits a careful execution assessment of five outstanding disseminated key administration methods (for cooperative associate gatherings) incorporated with a solid gathering correspondence framework. An inside and out correlation and investigation of the five procedures is displayed in

light of trial results got in genuine nearby and wide-zone systems. The broad execution estimation analyses led for all routines offer experiences into their adaptability and reasonableness. Besides, our examination of the trial results highlights a few perceptions which are not clear from the hypothetical analysis[7].

In this paper, a verified awry gathering key understanding convention is proposed, which offers security against dynamic and also inactive assaults. Proposed convention utilizes show encryption component without depending on the trusted merchant to circulate the mystery key. A personality based component is incorporated in the convention to give authentication[8].

This paper gives a diagram of conventions utilized as a part of Bluetooth correspondence and security shortcomings and vulnerabilities of the Bluetooth framework. Presently days, Bluetooth is a habitually utilized strategy for information transmission. Bluetooth standard was go under IEEE802.15. It's essential components are specially appointed in nature, low power utilization and minimal effort. It works on radio spread with 2.4GHZ. Different sorts of security conventions are utilized to anticipate listening stealthily and message capture attempt yet at the same time some security shortcomings like no uprightness check, man in center assault, Bluesnarf assault and numerous more are available in Bluetooth transmission[9].

The creators proposed interim based calculations considered in this paper are Batch calculation And the Queue-group calculation. The interim based methodology gives re-keying proficiency to element associate gatherings while saving both conveyed and contributory properties. Execution of these interim based calculations under diverse settings, for example, distinctive join and leave probabilities, is broke down The Queue-bunch calculation performs the best among the interim based calculations.[10]

This paper proposes an effective and contributory gathering key assention convention furthermore bolster dynamic operations like join, leave, combine, and so on by utilizing ECC based Diffie Hellman key trade. This convention utilizes ternary tree like structure rather than twofold tree during the time spent gathering key era. The execution of the proposed plan is contrasted and that of a few others existing plans in writing and it is found that the proposed one is performs well as far as correspondence and calculation cost. Likewise, the formal security approval is done utilizing AVISPA device that showed that the proposed convention is protected against latent and dynamic assaults[11].

This paper takes a gander at how existing examination endeavors the HOKEY WG, Mobile Ethernet and 3GPPframeworks react to this new environment and give security instruments. The examination demonstrates that the exploration's majority had understood the center's openness system and attempted to manage it utilizing diverse routines. These routines will be widely broke down so as to highlight their qualities and weaknesses[12].

It addresses a fascinating security issue in remote impromptu systems: the Dynamic Group Key Agreement key foundation. For secure gathering correspondence in an Ad hoc system, a gathering key shared by all gathering individuals is needed. This gathering key ought to be upgraded when there are participation changes (when the new part joins or current part leaves) in the gathering. In this paper, creator propose a novel, secure, versatile and effective Region-Based Group Key Agreement convention (RBGKA) for specially appointed systems. This is executed by a two-level structure and another plan of gathering key update[13].

In this paper, creator breaks down the as of late secure endorsement less key assention conventions without blending .Author then propose a novel lattice matching free testament less two-gathering validated key understanding (GPC-AKA) convention, giving a more lightweight key administration approach for framework clients. We additionally demonstrate, a GPC-AKA security convention evidence utilizing formal computerized security examination Sycthertool[14].

In this paper, creator propose a protected and productive AKA convention, called SE-AKA, which can fit in with the greater part of the gathering confirmation situations in the LTE systems. In particular, SE-AKA utilizes Elliptic Curve Diffie-Hellman (ECDH) to acknowledge KFS/KBS, and it additionally embraces a lopsided key cryptosystem to ensure clients' security. For gathering validation, it improves the entire confirmation strategy by processing a gathering makeshift key (GTK). Contrasted and other confirmation conventions, SE-AKA can't just give solid security including protection safeguarding and KFS/KBS, additionally give a gathering verification instrument which can viably validate bunch devices[15].

VII. PROPOSED APPROACH

In proposed system we implement the existing system with more time efficient manner and provide a multicast key generation server which is expected in future scope by current authors. We replace the Diffie Hellman key exchange protocol by a new multicast key exchange protocol that can work with one to one and one too many functionality. We also tend to implement a strong symmetric encryption for improving file security in the system.

VIII. RESULT GRAPH

In this screen which represents the graph between Total Group Members and Available Group Members Details.

IX. CONCLUSION

We mulled over a gathering key understanding issue, where a client is just mindful of his neighbors while the network chart is subjective. What's more, clients are instated totally autonomous of one another. A gathering key assertion in this setting is extremely suitable for applications, for example, informal communities. We review distinctive arrangements proposed in this space and reasoned that much work is should have been be done in this understanding conventions. We further propose a voting based convention plan for better protection and security in gathering based situations.

X. REFERENCES

[1]. Shaoquanjiang,"Group key agreement protocol with local connectivity" Dependable and Secure Computing, IEEE Transactions on (Volume:PP ,Issue: 99),03 February 2015.

[2]. Zongyu Song, PengfeiCai, Jie Yang ,"Group key agreement with efficient communication for ad hoc networks" JOURNAL OF SOFTWARE, VOL. 8, NO.10, OCTOBER 2013.

[3]. Anurag Singh Tomar, Gaurav Kumar Tak, Manmohan Sharma"Secure Group Key Agreement with Node Authentication", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3, Issue 4, April 2014.

[4]. k.kumar,j. Nafeesa Begum , Dr V. Sumathy, "Novel Approach towards cost Effective Region Based Key Agreement Protocol for secure Group Communication" in International Journal of Computer and Information Security, vol.8,No. 2,2010.

[5]. D. Augot,R. Bhaskar, V. Issarny and D. Sacchetti, "An Efficient Group Key Agreement Protocol for Ad Hoc Networks", Proc. 6th IEEE Int'l Symp. on a World of Wireless Mobile and Multimedia Networks (WOWMOM 2005), pp. 576-580, 2005.

[6]. N. Renugadevi ,C. Mala "Ternary Tree BaseGroup Key Agreement for Cognitive Radio MANETs" in *I.J. Computer Network and Information Security*, 2014, 10, 24-31 Published Online September 2014 in MECS

[7]. Y. Amir, Y. Kim, C. Nita-Rotaru and G. Tsudik, "On the Performance of Group Key Agreement Protocols", ACM Trans. Inf. Syst. Secur., vol. 7, no. 3, pp. 457-488, Aug. 2004.

[8]. Reddi Siva Ranjani, D.LalithaBhaskari, P. S.Avadhani, "An Extended Identity Based Authenticated Asymmetric Group Key Agreement Protocol", in International Journal of Network Security, Vol.17, No.5, PP.510-516, Sept. 2015.

[9]. TrishnaPanse, Vivek Kapoor, PrashantPanse, "A Review on Key Agreement Protocols used in Bluetooth Standard and Security Vulnerabilities in Bluetooth Transmission", in International Journal of Information and Communication Technology Research, Volume 2 No. 3, March 2012.

[10]. M. Swetha, L. Haritha, "Review on Group Key Agreement Protocol", International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 10, December- 2012.

[11]. Abhimanyu Kumar, SachinTripathi, "Ternary Tree based Group Key Agreement Protocol Over Elliptic Curve for Dynamic Group" ,in *International* Journal of Computer Applications (0975 – 8887) Volume 86 – No 7, January 2104

[12]. Mahdi Aiash, GlenfordMapp and AboubakerLasebae, "A Survey on Authentication and Key Agreement Protocols in Heterogeneous Networks", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.4, July 2012.

[13]. K. Kumar, J. Nafeesa Begum, Dr.V. Sumathy, "A Novel Approach towards Cost Effective Region-Based Group Key Agreement Protocol for Secure Group Communication",in(IJCSIS) International

[14]. Journal of Computer Science and Information Security, Vol. 8, No. 2, 2010. Amr Farouk, Mohamed M. Fouad and Ahmed A. Abdelhafez, "Analysis and Improvement of Pairing-Free Certificate-Less Two-Party Authenticated Key Agreement Protocol for Grid Computing", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 3, No 1, February 2014.

[15]. A Yao, " Theory and Applications of Trapdoor Functions", Proc 23th Ann Symp. Foundations of Computer Science (FOCS'82),pp80-91,1982

[16]. E. Bresson, O. Chevassut and D. Pointcheval, "Dynamic Group Diffie-Hellman Key Exchange under Standard Assumptions",Proc. 21th Int'l Conf. Theory and Application of Cryptographic Techniques
[17]. (Eurocrypt'02), vol. 2332, pp. 321-336, 2002.
[18]. Chengzhe Lai, Hui Li, Rongxing Lu, Xuemin (Sherman) Shen, "A secure and efficient group authentication and key agreement protocol for LTE networks" , Computer Networks 57 (2013) 3492.

