Advances in Wireless and Mobile Communications.
ISSN 0973-6972 Volume 10, Number 2 (2017), pp. 251-259

http://www.ripublication.com

Group Authentication and Key Agreement with Dynamic Policy Updation: A Review

Amandeep Singh[1] and Charanjit Singh[2]

[1]Department of Electronics and Communication Engineering, Punjabi University, Patiala, Punjab, India.
[2]Department of Electronics and Communication Engineering, Punjabi University, Patiala, Punjab, India.

Abstract

Group authentication and key agreement plays an important role in security. The key agreement protocols must ensure confidentiality and integrity of message. Key Agreement Protocol provides significant development in security to protect integrity, user anonymity and confidentiality of data. The environment of existing key agreement protocol has been presented in this paper. The network security tools are studied in order to establish key agreement between two party or multi party communications, various techniques and algorithms for implementation are discussed. Also, various methods of key agreement have been presented which were developed for mutual authentication among group members. In recent era, more and more applications are built that rely on peer to peer communication. The suggested protocol can be applied on wireless network to condense the security, performance requirement and cost of computation.

Keywords: Group Authentication, Key agreement, Third party, Complexity, Communication Overhead, Signaling Overhead

1. INTRODUCTION

As a result of the increased popularity of group-oriented applications and protocols, group communication occurs in many different settings i.e. from network layer multicasting to application layer and tele-communication to video-conferencing. Regardless of the application environment, security services are necessary to provide communication privacy and integrity.

While peer-to-peer security is a mature and well developed field, secure group communication remains relatively unexplored. Contrary to a common initial impression, secure group communication is not a simple extension of the secure two-party communication. There are two important differences. First, protocol efficiency is of greater concern due to the number of participants and distances among them. The second difference is due to group dynamics [1]. Two-party communication can be viewed as a discrete phenomenon, i.e. it starts, lasts for a while, and ends. Group communication is more complicated: it starts, the group mutates (members leave and join) and there might not be a well-defined end. This complicates the attendant security services among which key agreement is the most important. In the following, we specifically focus on the requirements of Dynamic Peer Groups (DPGs). DPGs are common in many layers of the network protocol stack and many application areas of modern computing.

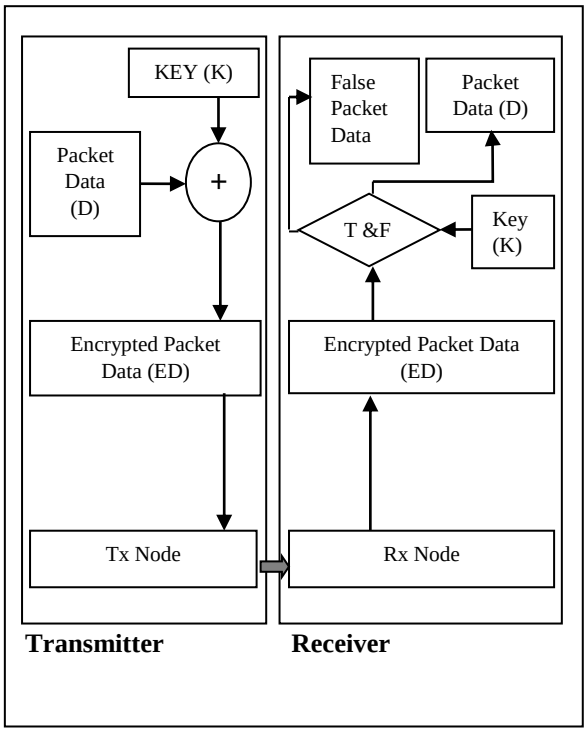

Figure 1: Key Transport Approach

In contrast to large multicast groups, DPGs tends to be relatively small in size, on the order of a hundred members. (Larger groups are harder to control on a peer basis and are typically organized in a hierarchy of some sort.) DPGs typically assume many-to-many communication pattern, rather than one-to-many that commonly found in larger, hierarchical groups [2].

Figure 1 shows, the Key Transport Approach for the authentication of packet data. In figure, there are two sections first is Transmitter and second is Receiver. In

Transmission section, we have created encrypted packet data ED with the help of packet data D with a secret key K and after that transmit using transmitter node.
We start Section 2, by discussing the contributory key agreement and the requirement in supporting the dynamics of groups.

2. DIMENSIONS OF KEY AGREEMENT

All of the protocols are based on contributory key agreement. This means that a group key K is generated as:

$$f.Ni;\ \ldots;Nn.,$$

Where, f is some one-way function and Ni is an input (or key share) randomly chosen by the ithparty. The method of computing group keys must guarantee that each party contributing one Ni, can calculate K; no information about K can be extracted from a protocol that runs without knowledge of at least one of the Ni. All inputs Ni are kept secret, i.e., if party is honest, then even a collusion of all other parties cannot extract any information about Ni from their combined view of the protocol.

Each part must calculate the value of K because K is a group key and all inputs of Ni must kept secret. The last property ensures that the inputs Ni,can be reused for subsequent key agreements. Several contributory schemes key agreement has been proposed in the literature [3], [4], [5], [6], [7], [8], and [9]. However, none have been widely used. These actually transport the key or do key distribution, not key agreement. While the centralized approach works reasonably well for static groups or very large groups, it turns out that the contributory key agreement is superior for DPGs, i.e., flat (non-hierarchical) groups with dynamically changing membership.
A permanently fixed group leader is a potential performance bottleneck and a single point of failure. Some DPG environments (such as ad hoc wireless networks) are highly dynamic and no group member can be assumed to be present all the time. This is also the case in wired networks, when high availability is required. Therefore, our view is that the fault tolerance (such as handling network partitions and other events) can be best achieved by treating all parties as peers.

2.1 Initial Key Agreement

IKA takes place at the time of group genesis. This is the time, when protocol overhead should be minimized, since, key agreement is a prerequisite for secure group communication. On the other hand, for highly dynamic groups, certain allowances can be made, for example, extra IKA overhead can be tolerated in exchange for lower AKA (subsequent key agreement operations) costs.

2.2 Auxiliary Key Agreement

Initial group key agreement is only a part, though a major one, of the protocol suite needed to support secure communication in dynamic groups. Thesecurity property crucial to all AKA operations is key independence.

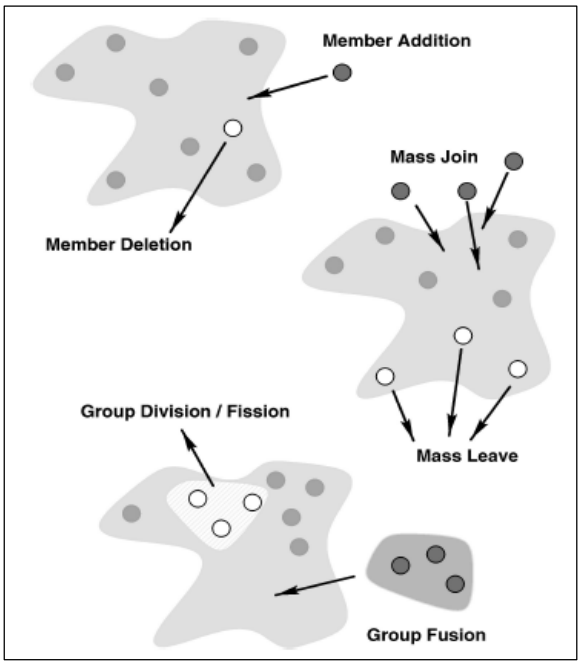

Figure 2: AKA Operations

Informally, it encompasses the following two requirements:

- Old, previously used group keys must not be discovered by new group member(s). In other words, a group member must not have the knowledge of keys used before it joined the group.
- New keys must remain out of the reach of former group members.

3. RELATED WORK

The earliest attempt to provide contributory key agreement and to extend DH (Diffie Hellman) is file exchange parameters to groups are due to the protocol requires synchronous startup and executes in (n-1) rounds. The members must be arranged in a logical ring. In a given round, every participant raises the previously-received intermediate key value to the power of its own exponent and forwards the result to the next participant. After (n-1) rounds, everyone computes the same key Kn.

We note that this protocol falls into the class of natural DH extensions as defined in [7]. It is, thus, suitable for use as an IKA protocol. However, because of its symmetry,

(no natural group leader) it is difficult to use it as a foundation for auxiliary key agreement protocols.

Another DH extension geared towards teleconferencing was proposed by Steer et al., in [4]. This protocol requires all members to have broadcasting facilities and takes n rounds to complete. In some ways, STR is similar to IKA.1. Both take the same number of rounds and involve asymmetric operation. Also, both accumulate keying material by traversing group members one per round. However, the group key in STR has a very different structure:

$$K8 = \propto^{\propto^{\frac{N1}{N2,}}\propto^{\frac{N3}{N4,}}\propto^{\frac{N5}{N6,}}\propto^{\frac{N7}{N8,}}}$$

$N_{1\ to}\ N_{8:}$ No. of Nodes

$K_{8:}$ Key

One notable result is due to Burmester and Desmedt [5]. They construct a very efficient protocol (BD) which executes in only three rounds:

1. Each Mi generates its random exponent Ni and broadcasts Zi= $\propto^{Ni}$.
2. Each Mi computes and broadcasts Xi = (Zi +1/ Z- 1). ^{Ni}

In the recent work, Becker and Wille [9] systematically analyze the communication complexity of contributory group key agreement protocols. The authors have proved lower bounds for the number of messages, exchanges, simple and synchronous rounds and, e.g., confirmed that IKA.1 is optimal in respect to the number of messages and exchanges. Additionally, they also describe a novel protocol, 2d-octopus, which reaches the lower bound for simple rounds $(d\,.\,dlog2\,ne)$. Their main idea is to arrange the parties on a d-dimensional hypercube, i.e., each party is connect to d other parties. The protocol proceeds through d rounds, 1 . . . d. In the jth round, each player performs a two party. Discrete logarithms are logarithms defined with regard to multiplicative cyclic groups. It is defined below:

3.1 Discrete Logarithm Problem

This is the logarithms that are defined on multiplicative cyclic groups. Let Γ is a multiplicative cycle group and g is a generator of G , then the elements r of the cyclic group are in the form mod t g n for some n t $*\in'$.

Definition 1

Discrete logarithm to base g of r in the group Γ is defined to be t. The discrete logarithm problem is defined as:

Given a group G, a generator g of the group and an element h of G, to find the discrete logarithm to the base g of h in the group G. Discrete logarithm problem is not always hard. The hardness of finding discrete logarithms depends on the groups.

3.2 Elliptic Curve Discrete Logarithm Problem

In cryptographic context, it is a curve over a finite area, which consists of points satisfying the following equation:

$$y2 = x3 + ax + b$$

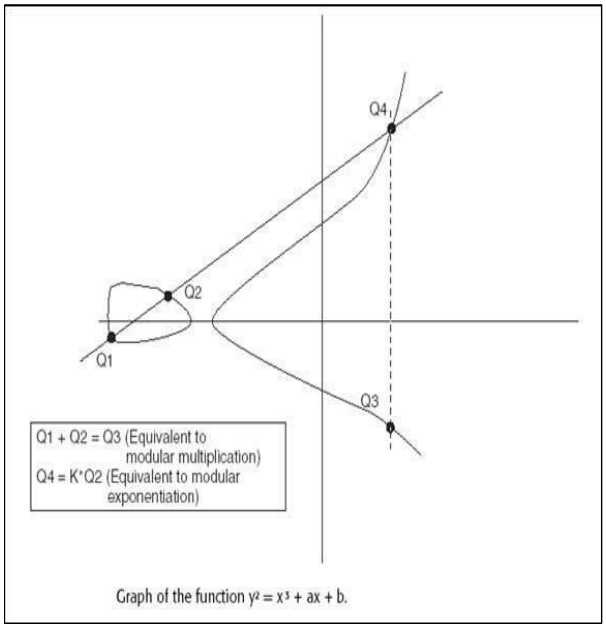

Figure 3: Elliptic Curve Discrete Logarithm

Definition 2
Given an elliptic curve E defined over a finite field Φp , a point ( ) P ∈ E Φp of order n , and a point Q P ∈ , find the integer l n ∈ − [0, 1] such that Q = lP . The integer l is called discrete logarithm of Q to base P, denoted = p l log Q [10].

Table 1: Comparison Table of Group Key Management Protocols [21]

Scheme/ Feature	Secrecy		Secure Against Coll.	Message			Storage	
	back	fore		Join		leave	KDC	member
				multicast	unicast			
Simple	Y	Y	Y	nK	K	nK	nK	K
GKMP	Y	N	Y	$2K$	$2K$	—	$2K$	$2K$
LKH	Y	Y	Y	$(2d-1)K$	$(d+1)K$	$I + 2d\,K$	$(2n-1)K$	$(d+1)K$
OFT	Y	Y	Y	$(d+1)K$	$(d+1)K$	$I + (d+1)K$	$(2n-1)K$	$(d+1)K$
OFCT	Y	Y	Y	$d\,I$	$(d+1)K$	$I + (d+1)K$	$(2n-1)K$	$(d+1)K$
Clusters	Y	Y	Y	$m-1+$ $a\log_a(\frac{n}{m})$	$\log_a(\frac{n}{m})$ 2	$m-1$ $a\log_a(\frac{n}{m})$	$\frac{n \quad a}{m\ a_{\underline{n}}}-1+$ m	$\log_a(\frac{n}{m})+$ 2
FT	Y	Y	N	$2I\,K$	$(I+1)K$	$2I\,K$	$(2I+1)K$	$(I+1)K$
ELK	Y	Y	Y	0	$(d \quad 1)K$	$I \quad d(n_1 \quad n_2$	$(2n \quad 1)K$	$(d \quad 1)K$

4. SECURITY PURPOSE

Let k be a security parameter. All algorithms run in probabilistic polynomial time with k and n as inputs and induction representation is shown below:

- An: ($view\big(n-1,(N1,X)\big),K\ (n-1),(N1,K)$
$view\big(n-1,(N2,X)\big),K\ (n-1),(N2,K)$
$\big(view(N1,N2,X)\big),y)$
- Bn: ($view\big(n-1,(N1,X)\big),K\ (n-1),(N1,K)$
$view\big(n-1,(N2,X)\big),K\ (n-1),(N2,K)$
$\big(view(c,X)\big),y)$
- Cn: ($view\big(n-1,(N1,X)\big),K\ (n-1),(N1,K)$
$view\big(n-1,(N2,X)\big),K\ (n-1),(N2,K)$
$\big(view(c,X)\big),yK\ (n-1),(c,K)$
- Dn: ($view\big(n-1,(N1,X)\big),K\ (n-1),(N1,K)$
$view\big(n-1,(N2,X)\big),K\ (n-1),(N2,K)$
$\big(view(N1,N2,X)\big),y\ K\ (n-1),(N1,N2,K)$

The above result allows us to construct a number of specific protocols belonging to the natural DH extensions family without worrying about their individual security. The key agreement scheme defined in the standard [1-16] has three main categories, such as two parties, one party, and no temporary key participation. In addition, desired security features and implementation requirement parameters to be considered are Mutual Authentication, on-repudiation of Service, Confidentiality, Anonymity of User, Physical Requirements, and Terminal Security as shown in Table 2.
The table is divided into properties on the basis of
AKA [10], AKA [15], AKA [14], AKA [17], AKA [18], AKA [19] and AKA [20] for the comparative analysis of key agreement protocols for efficiency.

Table 2: Efficiency comparison analysis of key Agreement Protocols

PROPERTIES	**AKA[10]**	**AKA[15]**	**AKA[14]**	**AKA[17]**	**AKA[18]**	**AKA[19]**	**AKA[20]**
Mutual Authentication	Yes	Yes	Yes	Provided	Provided	Provided	Provided
Key agreement	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Certification computation	Yes	No	No	No	No	No	No
Parings computations	No	No	No	Yes	No	No	No
Computation Cost(user side)	3PM+2PA +1MM	1PM+2PA	3PM+2 PA	12PM	10PM	10PM	6PM
Communication rounds	3	2	2	3	2	2	2
Bandwidth	2P+2p	2P	2P+2p	2P+2p	2P	2P	P+H

5. CONCLUSION

As a result of the increased popularity of group-oriented applications and protocols, group communications occur in many different settings that is, from network multicasting to application layer and from, telecommunication to videoconferencing. Regardless of the application environment, security services are necessary to provide communication privacy and integrity. This paper considers the problem of key agreement in dynamic peer groups. (Key agreement, especially in a group setting, is the stepping stone for all other security services.

REFERENCES

[1] W. Diffie and M. Hellman, 1976, "New Directions in Cryptography", IEEE Trans. Information Theory, vol. 22, no. 6, pp. 644-654.

[2] G, Ateniese, M. Steiner, and G. Tsudik, 2000, "New Multiparty Authentication Services and Key Agreement Protocols", IEEE J. Selected Areas in Comm., vol. 18, no. 4.

[3] I. Ingemarsson, D. Tang, and C. Wong,1982, "A Conference Key Distribution System", IEEE Trans. Information Theory, vol. 28, no. 5, pp. 714-720.

[4] D. Steer, L. Strawczynski, W. Diffie, and M. Wiener, 1988, "A Secure Audio Teleconference System", Proc. Advances in Cryptology ĐCRYPTO, pp. 520-528.

[5] M. Burmester and Y. Desmedt, 1995, "A Secure and Efficient Conference Key Distribution System", Proc. Advances in Cryptology DEUROCRYPT .

[6] M.K. Just, 1994, "Methods of Multiparty Cryptographic Key Establishment", MS thesis, Computer Science Dept., Carleton Univ., Ottawa, Ontario.

[7] M. Steiner, G. Tsudik, and M. Waidner, 1996, "Diffie-Hellman Key Distribution Extended to Groups", Third ACM Conf. Computer and Comm. Security, pp. 31-37.

[8] M. Just and S. Vaudenay, 1996, "Authenticated Multi-Party Key Agreement", Proc. Advances in Cryptology ĐEUROCRYPT.

[9] K.Becker and U.Wille, 1998, "Communication Complexity of Group Key Distribution", Proc. Fifth ACM Conf. Computer and Comm. Security, pp. 1-6.

[10] He Debiao, Padhye Sahadeo, and Chen Jianhua, 2012, "An efficient certificate less two-party authenticated key agreement protocol", Computers& Mathematics with Applications, 64(6), pp. 1914–1926.

[11] Tianhua Liu, Hongfengzhu, 2010, "An ID based multi-server authentication with key agreement scheme without verification table on elliptic curve cryptosystem", International conference on computational aspects of Social Networks,978-7695-4202/10, IEEE.

[12] S. H. Islam and G. P. Biswas, 2011, "A more efficient and secure id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem", Journal of Systems and Software, vol. 84, no. 11, pp. 1892–1898.

[13] R.W.Zhu,G.Yang,R.Sun, 2007, "An efficient identity-based key agreement protocol with KGS forward secrecy for low-power devices", Theoretical Computer Science,no.378,pp. 198-207.

[14] X. Cao, W. Kou, Yyu, R. Sun,2008, "Identity-based authentication key agreement protocols without bilinear pairings", IEICE tran. Fundamental.vol.E91-a, No.12, pp. 3833-3836.

[15] X. Cao, W. Kou, 2010, "A pairing –free identity-based authenticated key agreement protocol with minimal message Exchanges", Information sciences, Doi:10.1016/j.ins.2010.04.002.

[16] Debiao He,jianhuachen,JiN Hu, 2010, "A New Provably Secure authenticated Key agreement protocol without Bilinear pairings", Journal of information & Computational science Vol. 7, No: 5, pp. 1089-1096.

[17] M.Zhang,Y.Fang,2004"Security analysis and enhancements of 3GPP authentication and key agreement protocol", IEEE Trans, Wirel. Commun. Vol. 4(2), pp. 734–742.

[18] Y.L.Huang,C.Y.Shen,S.W.Shieh,2011,"S-AKA: approvable and secure authentication key agreement protocol for UMTS networks", in IEEE Transactions on Vehicular Technology, Vol.60 No. 9, pp. 4509–4519.

[19] J. Cao, M. Ma, H. Li, 2012, "A group-based authentication and key agreement for MTC in LTE networks", in the Proceedings of IEEE Global Communication Conference (Globecom), pp.1017–1022.

[20] Chengzhe Lai, 2016, "GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications", Computer Networks.

[21] Sandro Rafaeli, 2003, "A Survey of Key Management for Secure Group Communication", ACM Computing Surveys, Vol. 35, No. 3, pp. 309–329.

[22] Sonali Nimbhorkar, 2015, "Comparative Analysis of Authenticated Key Agreement Protocols Based on Elliptic Curve Cryptography", ELSEVIER, International Conference on Information Security & Privacy (ICISP2015), 11-12, Nagpur, India