International Journal of Communication Networks and Security

Volume 1 | Issue 4 Article 6

April 2012

ACP BASED ANONYMOUS SECURE GROUP COMMUNICATION

NIRMALA C. G
Dept of ECE , Reva Institute of Technology and Management, Bangalore, Karnataka,,
nirmala.cg@gmail.com

HEMALATHA N
Dept of ECE , Reva Institute of Technology and Management, Bangalore, Karnataka,,
hemaharish15@gmail.com

ACP BASED ANONYMOUS SECURE GROUP COMMUNICATION

NIRMALA C.G[1] & HEMALATHA.N[2]

[1,2]Dept of ECE , Reva Institute of Technology and Management, Bangalore, Karnataka,
E-mail : nirmala.cg@gmail.com & hemaharish15@gmail.com

Abstract – -Anonymous secure group communication is a new research and application paradigm. In this paper Anonymity between two-party communication, Access control polynomial to multi-part group communication, group key management for secure group communication and secure set concepts has been proposed. Newly extended scheme enforces Anonymous group membership, group size, Anonymous group communication and group message broadcasting. The experimental results and comparisons with existing system show that the ACP scheme is elegant, flexible, efficient and practical.

Keywords*-Secure Group Communication (SGC), Anonymity, Anonymous Secure Group Communication, Secret Set, Secret Set Access Control Polynomial (ACP.*

I. INTRODUCTION

There is a high importance in providing secure group communication in networking. The existing system generally uses secure lock which provides anonymous secure group communication. This lock is, in fact, a single value computed from the multiple encrypted keys using the Chinese Remainder Theorem (CRT). Secure Lock implements anonymous secure group communication, but it suffers from an efficiency problem .SAM (Secure Anonymous and multicast) tries to provide an architecture for anonymous secure group communication, but fails in providing rigorous anonymity.

Traditionally, the research on anonymity has been focused on two-party communication. Further, three typical anonymities have been extensively studied. Anonymity is not only an issue in two-party communication environments, but also in multi-party computing environments. Some preliminary work on privacy and anonymity in VANETs has been initiated such as Traceable Anonymous Certificate (TAC) recently proposed by the IEEE Internet Engineering Task Force and group-based anonymous communication schemes.

There are some challenges that make the design of anonymous secure group communication a tough task. Firstly, in secure lock implements anonymous secure group communication, but it is inefficient. SAM tries to provide architecture for anonymous secure group communication, but fails in providing rigorous anonymity. Secondly, Secret Set schemes can implement anonymous group membership and group size, but cannot support secure group communication.ACP (Access control polynomial) can be exposed to provide anonymous multi-party communication, which enforces both anonymous group (membership and size) and secure communication among the members of the anonymous group.

II. EXISTING SYSTEM

Let us discuss some of the existing scheme used in group communication.

1. Secure lock:

This lock is a single value computed from the multiple encrypted keys using the Chinese Remainder Theorem (CRT). The Secure Lock scheme works as follows: Suppose each member mi in the universal group G has its public and private key pair (Pi, Si) Suppose each member mi in the universal group G has its public and private key pair (Pi, Si). A central entity (e.g. a server) determines a sequence of n = |G| pairwise relatively prime numbers N1, N2, N3, Nn. These numbers are assigned to group member's m1, m2, m3, mn respectively. All the Ni are made public. When a group of members § = {mi1, m2, miℓ} wants to form an anonymous secure communicating group, the central server selects a random key k and first establishes the following congruence's:

$$Ł \equiv EPi1\ (k)\ (mod\ Ni1)$$

...

$$Ł \equiv EPiℓ\ (k)\ (mod\ Ni\ ℓ)$$

Then, the server computes Ł by applying the CRT. Integer Ł will be the lock for the encrypted keys EPij (k), and is sent along with the random key k as (Ł, {k} k). When a receiver, such as mij, receives the above packet, he/she can compute EPij (k) = Ł mod Nij, then obtains k = DSij (EPij (k)) using his/her private key and finally decrypts the random key k using k. If the decryption discloses k, then mij knows that he is in the group and the group key is k. Otherwise, the member is not in the group .Once group members get to know they are in the group and get the group key k, they can perform group communication which is securely protected by the group key k. It is clear that the CRT value Ł hides group membership by introducing decoys and group size is also hidden (group size means exact size).the attacker will actually know the upper bound of the group size. Due to the involvement of public key

systems and the Chinese Remainder Theorem the Secure Lock scheme is inefficient and not scalable.

The Drawback of the Secure Lock scheme is inefficient and not scalable because it is only applicable to small group, if number of member increases, time required computing the lock is more. In this scheme any user can check their membership only but cannot check membership of other group members and group size.

III. PROPOSED SYSTEM

Secret Set is defined a group of members in which any user can test their membership in the group but can determine neither the other group members nor the size of the group. Secret Set provides a fundamental structure for mutually suspicious entity group communication.

1. Secret Set Based ACP- Anonymous Secure Group Communication Scheme:

From the above descriptions, Secure Lock implements anonymous secure group communication, but it is inefficient. SAM tries to provide architecture for anonymous secure group communication, but fails in providing rigorous anonymity. Secret Set schemes can implement anonymous group membership and group size, but cannot support secure group communication. First introduce an innovative construction of an Access Control Polynomial (ACP). Then we extend the ACP mechanism to anonymous multi-party communication, which enforces both anonymous group (membership and size) and secure communication among the members of the anonymous group.

2. Access Control Polynomial

As in the above secret key-based Secret Set scheme, we assume that every valid member mi in the system is assigned a secret key Si (a random positive integer less than *q*). This secret is only known to the member and the central server. We also assume that *q* is a large prime from which a finite field Fq is formed and f: {0, 1} €→ {0, 1} ℓ (where ℓ = ⌈log (q) ⌉) is a cryptographic hash function. An Access Control Polynomial (ACP) is a polynomial over Fq[x] and defined as follows. A(x) =$\prod_{I \in §}$ (x – f (Si, z)) where § denotes the Secret Set under consideration and z is a random integer from Fq and made public. In addition, *z* is changed every time *A*(*x*) is computed. It is evident that A(x) is equated to 0 when x is substituted with f (Si, z) by a valid user with Si in set §; otherwise, A(x) is a random value if other numbers or invalid users' secret keys are used in the substitution.

Advantages of ACP:

1. It is elegant, simple, easy to understand and implement.
2. It is flexible and easy to adapt to (any) different kinds of key management and (any) different kinds of access control relations.
3. It is able to enforce access control and secure group communication in any scale and any granularity.
4. It is able to implement seamless integration of heterogeneous data sources and systems without much modification of the existing components.
5. It is able to protect against any kind of attacks, not only external attacks, but also internal attacks, even when attackers and/or malicious users collude.
6. It supports highly dynamic environments; in particular, the revocation of members/resources is simple and efficient. It also supports temporary suspension of membership.
7. It does not require member serialization or synchronization and does not disclose membership.
8. Users only need to store a secret value. Furthermore, the key computation and key derivation are executed by the same efficient procedure. This makes the scheme applicable to various devices including those with low computing powers such as PDAs, sensors.
9. It is able to offer the capability of hiding the entities in groups and even group size.

IV. COMPARISONS AND DISCUSSIONS

1. Comparisons

Secret Set schemes: From the above description, the Secret Set is only used for anonymous membership and set size, but the new ACP based mechanism can also distribute the secret key. In contrast, the new ACP-based scheme allows for a random number of members and there is no need for such ordering.

Anonymous membership broadcasting schemes (AMB): The new ACP-based scheme can also support AMB if only the intended receiver's ID is included in the construction of A (x). In particular, the new ACP-based scheme is secure against collusion of any number of users.

Anonymous secure group communication schemes: As for Secure Lock, it is based on public key cryptosystems. In contrast, the new ACP-based mechanism employs polynomial and secret key cryptosystems. Thus, the ACP-based scheme can use a 128-bit number to get stronger security than Secure Lock using at least 1024-bit numbers. This is because 80-bit symmetric systems, 160-bit hash functions, and 1024-bit RSA all have comparable security. In this sense, the new ACP-based scheme will be more efficient than Secure Lock.

Table 1.Complexities of Secure Lock and ACP

	Secure Lock	ACP
Generation of Ł or $P(x)$	$O(n^2B_1^2)^* + O(nB_1^3)^\#$	$O(n^2B_2^2)$
Given $B_1 = 1024$, $B_2 = 128$	$O(2^{20}n^2) + O(2^{30}n)$	$O(2^{14}n^2)$
Key computation	$O(nB_1^2)^\% + O(B_1^3)^\$$	$O(nB_2^2)$
Given $B_1 = 1024$, $B_2 = 128$	$O(2^{20}n) + 2^{30}$	$O(2^{14}n)$
Message length	$O(nB_1)$	$O(nB_2)$
Given $B_1 = 1024$, $B_2 = 128$	$O(2^{10}n)$	$O(2^7n)$

The time complexity for generating P(x) is O (n^2) multiplications (with modulus) and the key computation time is O (n) multiplications. The complexity for modular multiplications is O (B^2) bit operations, where B is the bit length of the operands. As for Secure Lock, the complexity for public key encryption is O (B^3). Since there are n public key encryptions, the total running time for public key encryptions are O (nB^3) (in bit operations).The complexity for CRT computation is O (n^2B^2). Thus, the total running time for computing Ł (which is nB bits) is O (nB^3) + O (n^2B^2). As for computing the key from Ł, its complexity is O (nB^2) + O (B^3). Ignoring the key and membership verification (which is the same for both methods), the complexities are summarized in Table 1.

2. Experiments

To demonstrate the performance of our scheme, implemented both the ACP-based scheme and the Secure Lock scheme. A java program was developed to measure the computation time of the core message generation and key computation.

For the ACP-based scheme, we generate a 128-bit random prime q to form the field Fq in which to perform our polynomial arithmetic. The one way function is chosen as z mod q where z is a primitive root of q. We use the typical square and multiply technique for exponentiation. In the experiments, the program generates 10, 000 random numbers less than q as keys S for 10, 000 users. For each experiment, the program selects different group sizes and then m random values S1, S2, Sm from the pre-generated keys for the users in the group such as U1, Um. Then a random number less than q is generated as z. S1, Sm and z, together with a random session key, are used to calculate the coefficients of the polynomial P(x).

For the Secure Lock scheme, we select RSA public key cryptosystem and use RSA classes contained in bcprov-jdk16-138.jar. The package is a Java implementation of cryptographic algorithms from Bouncy Castle Crypto. We generate 10,000 public primes and RSA objects. The primes are 1024 bits long and generated randomly. We use a random 128-bit number as session key K.

Table 2. Experimental results of Secure Lock and ACP

Group Size	Generation of Ł or $P(x)$ (ms)		Key Computation (ms)	
	Secure Lock	ACP	Secure Lock	ACP
10	22.122448	3.607294	32.548145	0.160141
50	334.4157	11.172215	35.519367	0.2505174
100	1248.3452	25.149284	35.745132	0.48382694
150	2715.346	45.294716	37.36742	0.7251202
200	4739.1973	71.207054	38.873844	0.96511495
250	7328.6416	102.26748	40.622406	1.2320576
300	10508.015	138.02417	42.16938	1.4394373
350	14244.455	187.28809	44.092808	1.6779447
400	18545.045	225.84566	45.835262	1.9190532
450	23349.342	278.32162	47.28901	2.161534
500	28807.654	336.43692	48.277184	2.4009411

The experimental results are shown in Table 2 and also in Figures 1, 2, and 3 from the table and figures, it can be observed that the experimental results validate theoretical analysis in Table 1 and prove the ACP-based mechanism is more efficient than the Secure Lock scheme approximately 100 times faster in term of membership representation generation (i.e. Ł or P(x)) and approximately 10 times better in terms of key computation and message length.

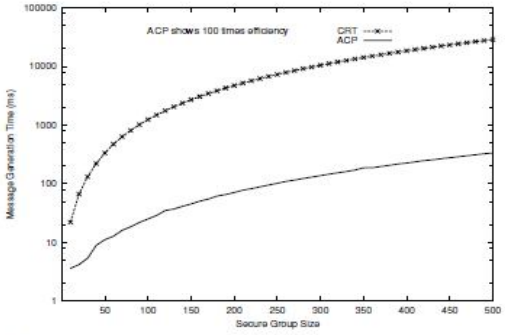

Figure 1. Membership representation generation time.

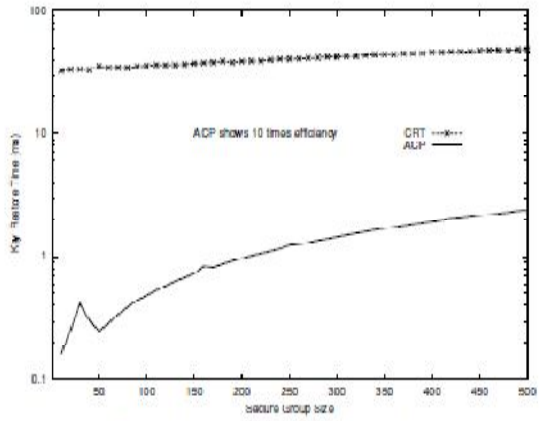

Figure 2. Key computation time.

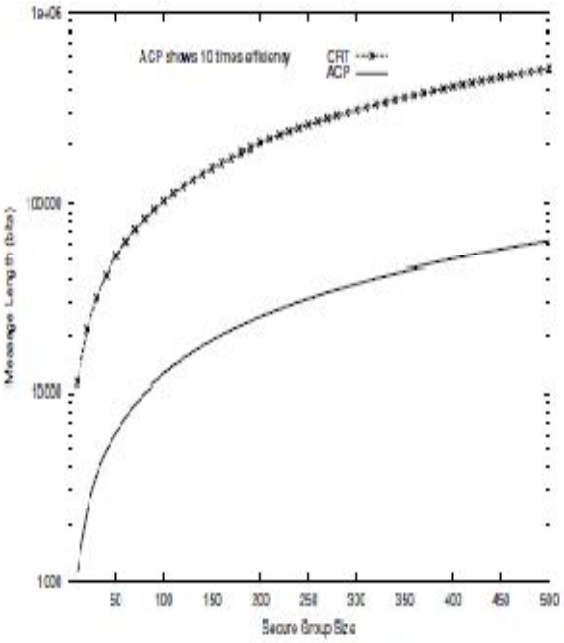

Figure 3. Communication complexities in terms of message length in bits.

V. APPLICATIONS

ACP based extended secure group communication is used in Trusted Collaborative Computing (TCC) is a new research and application paradigm. Two important challenges in such a context are represented by secure information transmission among the collaborating parties and selective differentiated access to data among members of collaborating groups. Addressing such challenges requires, among other things, developing techniques for Secure Group Communication (SGC), Secure Dynamic Conferencing (SDC), Differential Access Control (DIF-AC), and Hierarchical Access Control (HAC) and also used in securing Distance Education and Video Conference.

VI. CONCLUSION AND FUTURE WORK

Secret set supports anonymous secure group communication. Furthermore, the new scheme also supports anonymous secure group communication and offers many desirable features. The experiment and comparison showed ACP-based scheme is generic, flexible, efficient, dynamic, practical, invulnerable and easy to implement.

Secure group communication protocols used in particular multi-party key agreement and update algorithms, help promote traditional and new Internet multi-party applications such as video conferencing or distance education. We propose a framework for managing such approaches with access management mechanisms and applications in real environments. Furthermore, we extend this framework with anonymisation techniques for the sake of the individual's privacy. Our solution combines traditional unicast based approaches for privacy with authenticated and encrypted group communication. Thereby, we are able to build closed groups in which the members are not disclosed to outsiders. The introduced secure and anonymous multicast (SAM) framework can be employed as scalable, ones, malicious replays or masquerading, because of missing access control mechanisms.

REFERENCES

[1] E.Bach and J. Shallit, "Algorithmic number theory", *The MIT Press*, 1996

[2] Mira Belenkiy, Melissa Chase, Markulf Kohlweiss, and Anna Lysyanskaya.,"Non-interactive anonymous credentials" , Cryptology ePrint Archive, Report 2007/384, 2007.

[3] Matt Bishop, Rick Crawford, Bhume Bhumiratana, Lisa Clark, and Karl N. Levitt. "Some problems in sanitizing network data", In 15th IEEE International Workshops on Enabling Technologies Infrastructures for Collaborative Enterprises (WETICE 2006), 26-28 June 2006, Manchester, 2006.