ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)
Organized by
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

A Cost Effective Multicast Key Management Scheme for Secure Group Communication

R Keerthana[1], Dr.N.M Saravana Kumar[2]

PG Scholar, Department of CSE, Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India[1]

Associate Professor, Department of CSE, Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India[2]

ABSTRACT—Problem statement: Key management is the management of cryptographic keys in a cryptosystem. This includes dealing with the key generation, exchange, storage, use, and replacement of keys. Several schemes have been proposed to make key management efficient and usable. This paper proposes a cost effective key management scheme in multicast network for achieving a secure communication between the group members. This scheme gives better results with respect to the key management for multiple members. A secure key management scheme using RSA-CRT coding and Euclidean algorithm for efficient key distribution in multicast network. The keys generated in the network are securely exchanged with the help of RSA-CRT. This paper solves the most security problem by user registration and verification phases in the multicast network. The primary advantages are its large compression rate on the size of the shares and its strong protection of the secrets which avoids many attacks. For a ubiquitous system to be capable of sharing multiple secrets, the scheme can be potentially used for its efficiency, security and reliability. RSA-CRT algorithm is a method to periodically renew n secret shares without modifying the group key values whenever the member leaving in the star topology. The future work towards minimizing the communication cost in various tasks.

KEY WORDS—Group communication, rekeying, secure multicast, key management, RSA-CRT

I. INTRODUCTION

In the modern technology world, network attacks have become more sophisticated and harder to identify the attack. When many applications like scalable chat services and streaming video, are expected to run over the Internet, the security is necessary in computing and communication became a necessity. The internet today provides less security for privacy and authentication of multicast packets. The number of applications using multicast increases day by day and so it need secure multicast services. Multicasts is an internetwork service which provides efficient delivery of data from a source to multiple receivers and also improve the bandwidth efficiency of the network. A common group key is necessary for individual members in the group for secure multicast communication. In general the group key management (Sahar et al., 2010; Abdul-Rahman et al., 2011) can be divided into three consortium (a) centralized key management (b) distributed key management (c) decentralized key management.

In all approaches (Harney and Muckenhirm, 1997; Waldvogel et al., 1999) whenever a member joins or leaves the group or the members are static in nature, the group key has to be changed to achieve forward secrecy which assures that the newly joined members cannot decrypt the multicast data sent earlier before joining the group and assures that the former members cannot decrypt the communication after leaving the cluster. In most of the key management protocol tree topology issued. Tree balancing is another issue when a member joins or leaves. The main drawback of tree topology is that number of overhead and cost for rekeying proportionately increase if the number of member increases. A huge database is necessary for storage and complexity also increases. Scalability is an issue in connection with the dynamic multicast members.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014
Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)
Organized by
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

II. LITERATURE REVIEW

RSA Algorithm Using Modified Subset Sum Cryptosystem by Sonal Sharma (2011) proposed the concept of Subset-Sum cryptosystem (Knapsack Cryptosystem) is also an asymmetric cryptographic technique. The Merkle-Hellman system is based on the subset sum problem (a special case of the knapsack problem): given a list of numbers and a third number, which is the sum of a subset of these numbers, determine the subset. In general, this problem is known to be NP-complete. However, if the set of numbers (called the knapsack) is super increasing, that is, each element of the set is greater than the sum of all the numbers before it, the problem is 'easy' and solvable in polynomial time with a simple greedy algorithm. So in this paper a Modified Subset-Sum over RSA Public key cryptosystem is presented which is secure against Mathematical and brute-force attacks on RSA as well as Shamir attacks. RSA-CRT algorithm provides complete forward and backward security: Newly admitted group members cannot read previous messages, and evicted members cannot read future messages, even with collusion by arbitrarily many evicted members.

III. MATERIALS AND METHODS

The drawback of tree based architecture was overcome in SBMK (Lin et al., 2010) which uses star- based architecture in which the server computes a secret key and unicast to every user separately. But the drawbacks of these kinds of protocols are as follows:

- It increases the load on the server
- Computational and communication complexities are increased
- If private key is computed and sent by a server to all the members then the private component of members may not be used for authentication

  Figure 1 shows the key server only one entity can control the whole group. The central controller does not have to rely on any auxiliary entity to perform access control and key distribution. The group privacy is dependent on the successful functioning of the single server. Furthermore, the group may become too large to be managed by a single party, thus raising the issue of scalability.

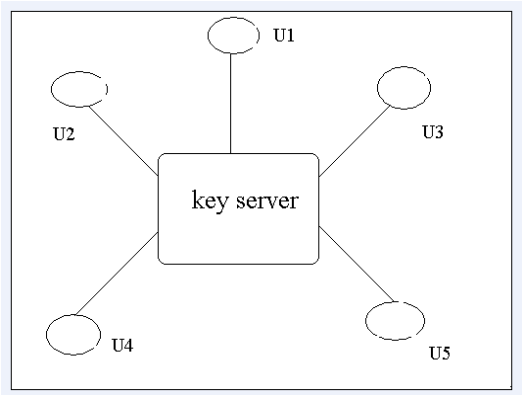

Figure 1

Our star topology based proposed algorithm has overcome the above problem:

- The total load on the server reduces because the private key is computed and sent by each user to server. So it reduces the load on the server
- The private component of members may be used for authentication

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

- It also reduces the computation complexity of server
- It gives a better rekeying performance than that of the key tree and there is no need to balance the tree Moreover our proposed scheme takes care of the important security requirements for secure group communication such as group secrecy, forward secrecy and backward secrecy.

In this study, we propose a Cost Effective Multicast Key Management Scheme for internet pay sites, which is relatively simple to implement. The rest of the study describes the proposed scheme, derives the result with suitable illustration of proposed algorithm, discuss and compare the proposed algorithm with the existing algorithms and finally concludes the study and future work.

IV. PROPOSED SCHEME

In the proposed star topology based algorithm, the individual member joining the group is allowed to choose prime numbers and compute their private key and the secret value of N computed is sent to the server by a secure unicast message.

Thus the burden of server is reduced and also rekeying is totally reduced and also scalable for a large multicast group.

A. RSA Cryptosystem

The steps of key assignment are as listed below:

Step 1: First the server authenticates the user who wants to join the multicast group and also announce public value as e. It is common for the server as well as users.

Step 2: The individual user M_i randomly selects two prime numbers m and n and calculates the product $X_i = m_i \times n_i$ and $(X_i) = (m_i-1) \times (n_i-1)$.

Step 3: The private of key of individual member will be calculated (Rivest et al., 1978; Menezes et al., 1997; Sharma et al., 2011) by the user using the extended Euclidean algorithm to calculate a unique integer d_i such that Eq(1):

$$e \times d_i \equiv 1 \bmod (\quad (Xi) \qquad \text{where, } d_i > \qquad 1$$

(X_i)

Step 4: The authenticated individual members send their X value to the server.

Step 5: The server verifies and accepts the X_i value only if it is unique value from other members and hold the value of X_i as secret.

B. Chinese Remainder Theorem (CRT)

A common math puzzle is to find a positive integer x.which when divided by 2, 3, 5 gives remainder 1 and is divisible by 7. Such questions are formally studied using the Chinese Reminder Theorem. Given a system of congruence to different modulo:

$$x == a1 \bmod m1 ,$$

$$x == a2 \bmod m2 ,$$

...

$$x == ar \bmod mr ,$$

If each pair of modulo are relatively prime: gcd $(m_i, m_j) = 1$ or i = j, has exactly one common solution modulo $M = m1 * m2 * m3 \ldots mr$ and any two solution are congruent to one another modulo M.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

C. Chinese Remainder Theorem In RSA-CRT

In RSA-CRT, it is a common practice to employ the Chinese Remainder Theorem during decryption. It results in a decryption much faster than modular exponentiation. RSA-CRT differs from the standard RSA in key generation and decryption. The value of d, the secret exponent cannot be made short. As soon as d < N0.292, RSA system can be totally broken. Keeping this in mind we make use the following scheme (Rivest et al., 1978; Menezes et al., 1997; Sharma et al., 2011).

D. RSA-CRT Key Generation and Encryption+

1. let p and q be very be two large primes of nearly the same size such that gcd(p − 1, q − 1)= 2.
2. Compute N = p ∗ q.
3. Pick two random integers dp and d_q such that gcd (d_p, p − 1)= 1, gcd(d_q, p −1)= 1 and d_p == d_q mod2.
4. Find d such that d == d_p mod (p − 1) and d == d_q mod (q − 1).
5. Compute **e = d−1 (mod (N))**.

The public key is < N, e > and the private key is < p, q, d_p , d_q >. Since gcd(d_p , p −1)= 1 and d == d_p mod p − 1, we have gcd(d, p − 1)= 1. Similarly, gcd(d, q −1)= 1. Hence gcd(d, (N)) = 1 and by step 5, e can be computed. To apply the Chinese Remainder Theorem in step 4, the respective modulo have to be relatively prime in pairs for a solution to necessarily exist. We observe that (p − 1) and (q − 1) are even and that we cannot directly apply the Chinese Remainder Theorem. However, gcd ((p − 1)/2, (q − 1)/2)= 1. Since gcd(d_p , p − 1)= 1 and gcd(d_q, q − 1)= 1, essentially d_p , d_q are odd integers and d_p − 1, d_q − 1 are even integers. We have gcd(d, p − 1)= 1 which implies that d is odd and (d − 1)is even .To find a solution to d = d_p mod p − 1, and d == d_q mod q − 1We find a solution to d − 1 == (d_p − 1) mod (p − 1). d − 1 == (d_q − 1) mod (q − 1).By applying the cancellation law and taking the common factor 2 out, we have x= d == (d − 1)/2 == (d_p − 1)/2 mod (p − 1)/2, x = d == (d − 1)/2 == (d_q − 1)/2 mod (q − 1)/2,Using Chinese Remainder Theorem we find d such that d = (2 ∗ d)+ 1.

E. RSA-CRT Decryption

Let M be the plaintext and C the cipher text. If C is not dividable by p and d_p == d mod p − 1, then C^{dp} == C^d mod p. For decryption we find

1. M_p = C^{dp} (mod p)= C^d (mod p) and. M_q = C^{dq} (mod q)= C^d (mod q).
2. Then using Chinese Remainder Theorem, we find a solution. M=M_p (mod p)= C^d (mod p), M=M_q = C^{dq} (mod q)= C^d (mod q).

F. Member Joining

When a new member Mn+1 want to join the group, the key server repeats the procedures similar to key assignment.

Step 1: First the server authenticates the user who want to join the multicast group and also announce public value as e .It is common for the server as well as users.

Step 2: The individual user M_i+1 select two prime numbers m and n and calculate the product X_i+1 = m_i+1 x n_i+1 and (X_i+1) = (m_i+1-1) x (n_i+1-1).

Step 3: The private of key (Rivest et al., 1978; Menezes et al., 1997; Sharma et al., 2011) of individual member will be calculated by the user using the extended Euclidean algorithm to calculate a unique integer d0 such that Eq :(2)

e ∗d_i+1 =1 mod ((X_i+1) 2

Step 4: The newly joined member send their X_i+1 value to the server

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014
Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)
Organized by
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Step 5: The server verify the X_i+1 and accept the X_i+1 only if it is unique value from other members and hold the value of X as secret

G. Members Leaving

When a member Xi leaves the group, the key server just deletes the secret information X_i. Therefore, in the cipher text computation (Rivest et al., 1978; Menezes et al.,1997; Sharma et al., 2011) in Formula (2) removes the modulus operations with respect to X_i (m_i ,n_i). Member Mi, cannot decrypt the secrete message because X_i is not added in cipher text calculation. Hence both forward and backward secrecy is maintained. The pair of prime numbers of a leaving member cannot be reassigned to new user joining the group. So there is no need for rekeying even if the members of multicast group change.

V. RESULTS

Illustration of the proposed algorithm with suitable examples and the result obtained is discussed in this section. *Key assignment phase:* The steps of key assignment are as listed below:

Step 1: First the server authenticate the user who want to join the multicast group and also announce public value as e = 103. It is common for the server as well as users.

Step 2: The individual user M_i selects two prime numbers mi and n_i randomly and also compute their

Xi = mi x ni and $\phi(X_i) = (m_i\text{-}1) * (n_i\text{-}1)$:

M_1 selects m_1=163 and n_1=227 computes X_1=37001 and ϕ (X_1) =36612

M_2 selects m2=181 and n_2=233 computes X_2=42173 and ϕ (X_2) =41760

M_3 selects m_3=163 and n_3=199 computes X_3=32437 and ϕ (X_3) =32076

M_4 selects m_4=137 and n_4=173computes X_4=23701 and ϕ (X_4) =23392

M_5 selects m_5=223 and n_5=211computes X_5=47053 and ϕ (X_5) =46620

M_6 selects m_6=251 and n_6=191computes X_1=47941 and ϕ (X_6) =47500

Step 3: The private of key of individual member is calculated by each user using the extended Euclidean algorithm used in RSA algorithm:

103 $d_1 \equiv 1 \bmod ((X_1) \equiv 1 \bmod 36612$ and d_1 =16351

103 $d_2 \equiv 1 \bmod ((X_2) \equiv 1 \bmod 41760$ and d_2= 6487

103 $d_3 \equiv 1 \bmod ((X_3) \equiv 1 \bmod 32076$ and d_3 =28339

103 $d_4 \equiv 1 \bmod ((X_4) \equiv 1 \bmod 23392$ and d_4 =6359

103 $d_5 \equiv 1 \bmod ((X_5) \equiv 1 \bmod 46620$ and d_5 =16747

103 $d_6 \equiv 1 \bmod ((X_6) \equiv 1 \bmod 47500$ and d_6 =2767

Step 4: The individual members communicate their X value to the server: X_1=37001, X_2=42173, X_3=32437, X_4=23701, X_5=47053, X_6=47941.

Step 5: Server verifies the secret value X_i of individual users and accepts the X only if it is unique value from other members and hold the value of X_i as secret.

Multicast communication: The steps of the Multicast communication are as listed below

Step 1: Assume there are 6 members X_1, X_2, …X_6 in the multicast group. When the server wants to send a secret message P= 5 to all members in the multicast group, then the server uses its public

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014
Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)
Organized by
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

value e0 as well as the secrets of Members X_1, X_2,… X_6 in the encryption formulae
The encryption of the secret message is computed using the general formulae:

C = 5103 mod (X_1*X_2* X_3 *X_4 *X_5 *X_6) = 5103 mod (37001 42173 32437 23701 47053 47941)= 1749630034980094709227313040

Step2: The server computes cipher text C and sends a broadcast message to all the members of the group

Step3: All six members in the multicast group can decrypt the secret message P from the cipher text received. The secret message is decoded as follows:

$M_1 \rightarrow P=(C \bmod X_1)^{d1} \bmod X_1=(1749630034980094709227313040 \bmod 37001)^{16351} \bmod 37001 = 5$
$M_2 \rightarrow P=(C \bmod X_2)^{d2} \bmod X_2=(1749630034980094709227313040 \bmod 42173)^{6487} \bmod 42173 = 5$
$M_3 \rightarrow P=(C \bmod X_3)^{d3} \bmod X_3=(1749630034980094709227313040 \bmod 32437)^{28339} \bmod 32437 = 5$
$M_4 \rightarrow P=(C \bmod X_4)^{d4} \bmod X_4=(1749630034980094709227313040 \bmod 37001)^{16351} \bmod 37001 = 5$
$M_5 \rightarrow P=(C \bmod X5)^{d5} \bmod X_5=(1749630034980094709227313040 \bmod 47053)^{16747} \bmod 47053 = 5$
$M_6 \rightarrow P=(C \bmod X_6)^{d6} \bmod X_6 = (1749630034980094709227313040 \bmod 47941)^{2767} \bmod 47941 = 5$

Performance analysis based on complexity comparison of various key management schemes: Table 1-2 provides the comparative analysis of the various protocols. It shows that every protocol achieves unique results when applying different techniques. Some protocols achieve exceptionally better results than others do. By comparing the table, we can clearly understand that the bottleneck of server is avoided by reducing total no of keys managed by server in our proposed algorithm. It is also smaller when compared with LKH, OFT and SBMK algorithm (Lin et al., 2010; Abdul-Rahman et al., 2011).Only one multicast message will be send to the group when a member joins and no message is send when a member leaves the group. So there is no need for rekeying when a member leaves also the rekeying overhead is less compared with LKH and OFT (Abdul-Rahman et al., 2011). The proposed algorithm achieves better results for storage, communication, computation and processing on both server and user. The computation cost of server is greatly reduced by allowing the users to calculate their private key and secret values compared with other techniques. The cost of encryption when a member joins the group is 1 and the cost of encryption when a member leaves the group. From the tables we can easily understand that proposed protocol is more suitable for a dynamic users and storage cost of server is reduced (Lin et al., 2010) and distributed to the users.

Table 1: Communication cost

Protocols	Join Multicast	Leave Unicast
LKN 2 LOG -1	Log n	
One way function tree	Log n+1	Log n+1
SBMK	1	0
CEKMS protocol	1	0

Table 2: Computation cost

Protocols	Join Multicast	Leave Unicast
LKN	2 Log n-1	2 Log n
One way function	Log n+1	Log n+1

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014
Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)
Organized by
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

tree		
SBMK	1	0
CEKMS protocol	1	0

VI. OTHER BENEFITS

CEKMS involves E-business security. It is the necessary protection against data theft in IT. This paper proposes a four times faster RSA-CRT algorithm for decryption than RSA using Chinese Remainder Theorem. Also it is found that encryption is more effective by using CRT. This algorithm can be usable for multimedia application. With this we can encrypt and decrypt the media file with high security and it produces the well organized group key management for data communication in multicast network.

VII. CONCLUSION

In this study, A Cost Effective Multicast Key Management Scheme for Secure Group Communication is proposed and implemented which produces better results than the existing protocols in terms of less computational, communication and storage costs. The proposed star based architecture reduces the rekeying overhead. The private key of the users are computed by the individual and so it can be used for authentication also. Theory predicts that the CRT decryption should be four times as faster than RSA .The average decryption time for the normal method is about 0.157 seconds per decryption and for the CRT method is 0.046 second per decryption, giving speedup by a factor of about 3.4The computation complexity of the server is totally reduced in the new protocol. It is also scalable and easy to implement when the number of users are very high and dynamic in nature. As future scope of work, it may be extended for bulk member join and leaves.

REFERENCES

[1] Abdul-Rahman, H., A.M. Alashwal and Z.H.Jamaludin, 2011. Implementation and methods of project learning in quantity surveying firms: Barriers, enablers and success factors. Am. J. Econ. Bus. Admin., 3: 430-438. DOI:10.3844/ajebasp.2011.430.438.

[2] Harney, H. and C. Muckenhirm, 1997. Group Key Management Protocol (GKMP) architecture. SPARTA, Inc.

[3] Lin, I.C., S.S. Tang and C.M. Wang, 2010. Multicast key management without rekeying processes. Comput. J., 53: 940-950. DOI:10.1093/comjnl/bxp060.

[4] Menezes, A.J., P.C.V. Oorschot and S.A. Vanstone,1997. Handbook of Applied Cryptography. 1st Edn., CRC Press, Boca Raton, Fla., ISBN: 0849385237, pp: 780.

[5] Rivest, R.L., A. Shamir and L. Adleman, 1978. A method for obtaining digital signatures and public- key cryptosystems. Mag. Commun. ACM., 21:120-126. DOI: 10.1145/359340.359342

[6] Sahar, N.B.M., S. Ardi, S. Kazuhiko, M. Yoshiomi and M. Hirotsugu, 2010. HAZOP analysis management system with dynamic visual model aid. Am. J. Applied Sci., 7: 943-948. DOI:10.3844/ajassp.2010.943.948.

[7] Sharma, S., P. Sharma and R.S. Dhakar, 2011. RSA algorithm using modified subset sum cryptosystem. Proceedings of the 2nd International Conference on Computer and Communication Technology (ICCCT), Sep. 15-17, IEEE Xplore Press, Allahabad, pp:457-461. DOI:10.1109/ICCCT.2011.6075138.

[8] Waldvogel, M., G. Caronni, D. Sun, N. Weiler and B.Plattner, 1999. The versakey framework: Versatile group key management. IEEE J. Selected Areas Commun., 17: 614-1631. DOI:10.1109/49.790485.

[9] Zhu, S. and S. Jajodia, 2003. Scalable Group rekeying for secure multicast: A survey. Lecture Notes Comput. Sci., 2918: 833-833. DOI: 10.1007/978-3-540-24604-6_1.

[10] Wong, C.K., M. Gouda and S.S. Lam, 2000. Secure group communications using key graphs. IEEE/ACM Trans. Netwo., 8: 16-30. DOI:10.1109/90.836475.

[11] Tu, F.K., C.S. Laih and H.H. Tung, 1999. On key distribution management for conditional access system on pay-TV system. IEEE Trans. Consumer Elect., 45: 151-158. DOI: 10.1109/30.754430.

Selcuk, A.A. and D. Sidhu, 2002. Probabilistic optimization techniques for multicast key management. Comput. Netw., 40: 219-234. DOI:10.1016/S1389-1286(02)00252-9.