iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.43968

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Secure Message Transmission Using Centralized Group Key Distribution Protocol

P. Vetrivel[1], M. Gopiya[2], S. Sangareswari[3], B. Karpagajothi[4]
[1, 2, 3, 4]*Sree Sowdambika College of Engg*

Abstract: ***In the secure message transmission, transmitted information can only receive by the authorized group members. To achieve a secure communication, symmetric key (group key) is used to both encrypt and decrypt the information, that shared among the group members. This paper, proposes an efficient centralized group key management scheme (GKDP) for achieving a secure multicast communication between the group members that reduces the cost of computation of SERVER(S) and rekeying cost of group members. The group key (GK) generated in the multicast network is securely distributed with the help of the RSA cryptosystem. Whenever the new member joins the group, computation cost of S reduced by performing single addition, multiplication and encryption, for updating the group key (GK). Whenever the member leaves the group, S performs single subtraction, division and encryption, for updating the group key (GK). By comparing with existing group key management protocol, the proposed protocol has significantly reduced computation complexity and rekeying cost. The proposed protocol is tested on star topology, the test results compared with existing group key management protocol. The comparison results show that the proposed protocol is efficient in terms of reducing the computational complexity of S and rekeying cost of group members.***

Index Terms: ***Secure multicast, rekeying cost, computational complexity, centralized group key management.***

I. INTRODUCTION

In the present information era, the multicast communication is very prevalent for sending secret information from a single sender to various receivers in the group. The advancement of multicast communication and the quick improvement of the web, many multicast services, for example, a video server sending out Television stations, network games, pay-per-see, distance learning, stock statements are playing noteworthy jobs. In centralized key management schemes, a single trusted substance called a S is utilized to deal with the Group Key (GK) and other supporting keys for the whole group. In dynamic multicast communication, the group members may join/leave the group at any time of the communication. Because of dynamic nature of the group, the group enrollment may change frequently and again, which drives the security issues with respect to forward and backward secrecy. Different key management approaches have been proposed in the literature for secure multicast communication.

The existing group key management approaches are isolated into three general classifications in particular centralized, de-centralized and distributed key management schemes. In the centralized key management schemes, a single centralized server is responsible for the key creation and key circulation among the group members.

In the de-centralized key management schemes, the bigger groups are divided into subgroups to minimize the computation load on single centralized sever and wipe out the single point of failure issue. Conversely, the distributed key management schemes don't utilize a single centralized server for generation and also, the distribution of the keys. In the distributed key management schemes, each group member contributes to create and circulate the keys. These three classifications have its own merits and demerits and are utilized by the necessity of application in various areas. The group key management schemes must, satisfy some security requirements in all conditions. The fundamental security requirements are forward and backward secrecy in the group. To provide the backward secrecy in the group, the S has been responsible to prevent recently joining group members from having access to recently shared information. Likewise, to provide the forward secrecy, the S is responsible to prevent the leaving group members from further access of future communication. For secure multicast communication a same group key GK is needed for sender and different receivers to encrypt and decrypt the information among the group. To provide the dynamic enrollment in the group, the GK should be refreshed also, distributed to the group members at whatever point the group enrollment is changed. The GK is refreshed frequently and hence the rekeying cost increased massively. In some of the centralized group key management schemes, the S allots a private key to each group members and encrypt the GK independently with every member's private key when rekeying occurs. The rekeying cost is directly relative to the group size, which makes inefficient communication. In multicast communications, the star topology has been commonly used to reduce the rekeying cost.

©IJRASET: All Rights are Reserved

This paper proposes an RSA public key cryptosystem based centralized key circulation scheme that reduce the computation complexity of S, group members and at the same time, it reduces the storage overhead of S while keeping up balanced storage overhead of each group members. The S needs to perform just a single multiplication operation to refresh the GK at whatever point a member joins the group. So also, the S needs to perform just a single division operation at whatever point a member leaves the group. What's more, the group members need to perform mathematical operations to recover the GK. The advantage of the proposed centralized key management scheme is that it is reducing the computational complexity and suitable for many dynamic multicast applications like TV-pay frameworks to perform secure multicast communication.

The rest of the paper is organized as follows: Section 2 gives the survey of many significant centralized key management schemes for multicast communication. The system model, multicast communication and RSA public key cryptosystem used in this paper are described in Section 3. The proposed GKDP protocol with detailed clarification is presented in Section 4. The security analysis of the proposed scheme is described in Section 5. The experimental results and analysis are provided in section 6. At last, the paper winds up with conclusion in Section 7.

II. LITERATURE SURVEY

In the centralized group key management scheme, a single server is responsible for key creation, key distribution, rekeying and to maintaining the group communication. The real difficulties of centralized key distribution schemes are adaptability complexity, communication complexity, computational complexity, storage complexity, and keeping up of forward and in backward secrecy. In order to manage these issues, we need to analyze the various key distribution schemes.

(Payal Sharma, et al., 2020) proposed for secure single group communication .The main advantage of this scheme is good in their performance metrics then the complexity get reduced.

(P. Vijayakumar, et al., 2011) Proposed binary tree-based group key computation protocol used to provide effective security in group communications. The main advantage of this scheme is, the computation complexity of S and group members get reduced. Group initialization step requires more time to setup the binary tree-based group.

(Khan, et al., 2014) Proposed a rekeying algorithm dependent on broadcasting a new message on joining and leaving of a member for refreshing the group. The proposed scheme is very adaptable and gives forward and backward secrecy in a productive way.

(R Keerthana1, et al., 2014) Proposed Cost Effective Multicast Key Management Scheme used to achieve the secure group communication. The star-based architecture reduces the rekeying complexity. The proposed scheme is, scalable and simple to execute when the number of members is very high and dynamic in nature.

(Vijayakumar et al., 2014) Computational complexity of S reduced by proposed CRT-based GKM scheme. Furthermore, the computational complexity of group participants is also reduced. In any case, the S storage complexity and S initialization cost is excessively high.

(Elhoseny et al., 2016) Proposed an Elliptic Curve Cryptography (ECC) and Homomorphic Encryption (HE) based novel encryption scheme for secure information transmission in WSN. The proposed scheme improves the performance of network by improving the computational complexity and communication complexity.

(Lin et al., 2017) Proposed a Cluster-based Elliptic Curve Key Management (CECKM) protocol for secure group communications in WSNs. The CECKM protocol gives same security level as RSA and Diffe-Hellman with keys. It takes a minimum amount of key resynchronization time as contrast with Diffe-Hellman and Group Diffe-Hellman protocols.

(Islam et al., 2017) Proposed a pairing -free Identity-based Two-party Authenticated Key Agreement (ID-2PAKA) protocol.

The proposed scheme provides an efficient method to create a common session key between two members through an open network and is appropriate for secure peer to peer communications.

In this article, we proposed new centralized group key management scheme dependent on RSA public key cryptosystem which is efficient in multiple points of view. It radically reduced the computation complexity of S by minimizing the required number of arithmetic activities needs to perform during key refreshing. It also reduced the storage complexity of S by minimizing the number of keys occupied in S memory. Besides, the proposed GKDP scheme gives high security against different assaults. So as to increase the level of the security, the proposed protocol uses an extra key called group key encryption key.

III. PRELIMINARIES

This segment describes our system model, multicast communication and RSA public key cryptosystem, which have been used in the proposed GKDP protocol.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

A. System model

We demonstrate the multicast group communication as star topology, where a lot of authorized members directly connected with centralized server called S. The S is a highly trusted authority, which is responsible to circulating the key to group members. The system model consists of highly trusted authority S, sender and group members. The multicast group represents a specific set of members, who are entitled for accepting the basic secret data or messages. The number of members considered in the multicast communication is n. In our model of multicast communication, the group members are named as 'gm_i'. A public key 'e' which is publicly available to all group members, private key 'd_i' and secret parameter 'k_i', which are known only to members and the modulus 'w_i', which is known to S and group members are used inside a multicast group for secure communication. To compute the group key encryption key 'd_q', the Chinese reminder theorem with secret parameters 'k_i' and 'w_i' of group members is used. The public key 'e' is generated by S, using the secret parameter ' $\Phi(w_i)$' which was transmitted to the group members. The private keys are calculated by the members itself at its own side with the help of public key 'e' and the secret parameter ' $\Phi(w_i)$'. In our system, the communication among the group members done by using AES symmetric key cryptosystem. Where the group key GK used for both encryption and decryption. The number of group members might be dynamic, for example, whenever a group member may leave or new member may join the group G.

B. Multicast communication

In multicast group communication, the sender transmits the secret information to a large number of receivers simultaneously. A secret information should be encrypted and only the authorized group members can decrypt the secret information. To achieve a secure multicast communication a common group key is needed for the group members to encrypt and decrypt the message.

Multicasting has many applications such as access to distributed database, information dissemination, distance learning and multimedia communications. The main issue that must be addressed in secure multicast communication is key distribution, Confidentiality, Integrity and Authenticity (CIA) of the data.

Confidentiality services are basic in making a private multicast session. The encryption operation is normally used to give this service, a more fragile type of confidentiality might be accomplished by restricting data circulation through time-to-live (ttl) settings. We can provide confidentiality services through encryption. Confidentiality services ought to likewise be applied to key management schemes during the circulation of key material.

Integrity services provide confirmation that multicast traffic is not adjusted during communication or transmission. Solid integrity schemes can be applied indirectly at the network layer with security protocol, for example, the Encapsulating Security Payload (ESP).

Authentication services might be applied by the traffic source. To define the group participation by identifying the group members along with their information being sourced to the group.

To securely circulate the keys to each group member. Security requirements are, to achieve the secure multicast communication. 1. Backward secrecy, 2. Forward secrecy.

1) Backward secrecy

This gives past secrecy implies, provides the security from the new group members who join the group.

2) Forward secrecy

This gives future secrecy implies, provides the security from the group members who left the group.

The fundamental structure of secure communication protocol is to utilize asymmetric cryptography for member's validation and keys confidentiality, and then utilize symmetric cryptography for information encryption and information realness. Multicasting classified into two main categories, such as 1. IP multicast and 2. Overlay multicast. IP multicast and overlay multicast provides some mechanism for distributing the same message to multiple recipients in a more efficient manner.

1. IP multicast

IP multicast uses UDP protocol for establishing the communication, so this type of communication is unreliable. To join the multicast group, each member sends a join message using Internet Group Management Protocol (IGMP). Group members are identified by IP address. For IP multicast the specific IP address range is available, the IP address range is (224.0.0.0 to 239.255.255.255).

In IP multicast, each group members organize into a tree structure. A tree is formed by the sender.

©IJRASET: All Rights are Reserved

2. Overlay multicast

In an overlay multicast, each group members organize into a delivery tree. Each group member gets the content from their parent and forward to its child.

Multicast key circulation

multicast key circulation should be combined with group access control. Without group access control, there is no reason for utilizing multicast key circulation, since, if there are no group limitations, at that point it ought not make any difference to whom multicast data is unveiled. The fundamental issue of circulating a group key to a group of multicast members lies in the way that some centralized key management entity, such as SERVER(S).

It is a third-party entity, which is responsible to generate and circulate a group key to peers, or group receiver on multicast, wishing to participate in a secure communication. It should in this way have the ability to identify and reliably authenticate the requests of group key, must authenticate every one of a group's receivers, as well as securely circulate a group key to every one of them.

Multicast applications video and audio conferencing, distance learning from the centralized location, multi-media streaming, Web-cache updates and distributed interactive gaming or simulations.

C. RSA public key cryptosystem

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys such as, Public Key and Private Key. Public Key is known to everyone and Private key is kept private.

An example of asymmetric cryptography:

1) A client sends its public key to the server and requests for some data.
2) The server encrypts the data using client's public key and sends the encrypted data.
3) Client receives this data and decrypts it.

RSA public key cryptosystem was introduced by Rivest, Shamir and Adleman, which is broadly used for secure information transmission. The security of RSA depends on the trouble of factoring the product of two large primes. The detail clarification of RSA cryptosystem is as per the following.

Key initialization

1. Choose two different large random prime numbers P and Q.
2. Calculate $w_i = P*Q$.
   - w_i is the modulus for the public key and private keys.
3. Calculate $\Phi(w_i) = (P-1) * (Q-1)$.
4. Choose e such that $1< e < \Phi(w_i)$, and e is co-prime to $\Phi(w_i)$, $\gcd(e, \Phi(w_i)) = 1$
   - e is released as public key exponent.

5. Compute d to satisfy the congruence relation $(d*e) -1 = 0 \bmod (\Phi(w_i))$.
   - d is kept as private key exponent.

Encryption

Public key parameters (e & n) are publicly available, sender wants to send the message M to the receiver. He computes chipper text by, $C = M^e \bmod n$.

Decryption

The receiver can recover the message M from C by using his private key d in following procedure. $M = C^d \bmod n$.

RSA digital signature

$$s \equiv M^d \pmod n$$

where (n, d) is a private key. The signature is verified by recovering the message M using public key (n, e).

IV. PROPOSED GKDP PROTOCOL

In this segment, we describe our centralized group key management protocol (GKDP) which depends on an RSA public key cryptosystem and implemented on star topology. The proposed GKDP contains five stages. Initialization stage, where the S randomly generates two distinct large prime numbers and compute w_i and $\Phi(w_i)$. The S also generates the secret parameter k_i for n number of members and compute the R_i. Member join stage, where the group members calculate l_i and their private key d_i.

Key update stage, in this stage the S circulates the group key GK among the members who initially join the group and refresh the new GK when any new member joins or existing member leaves the group. Key recovery stage, in which the group members can recover the GK at the member area, that circulated by the S. Member leave stage, where the S need to recirculate the updated GK among the remaining members in the group. The proposed GKDP protocol implemented on star topology is shown in fig. 1. The detailed description of five stages is given as follows.

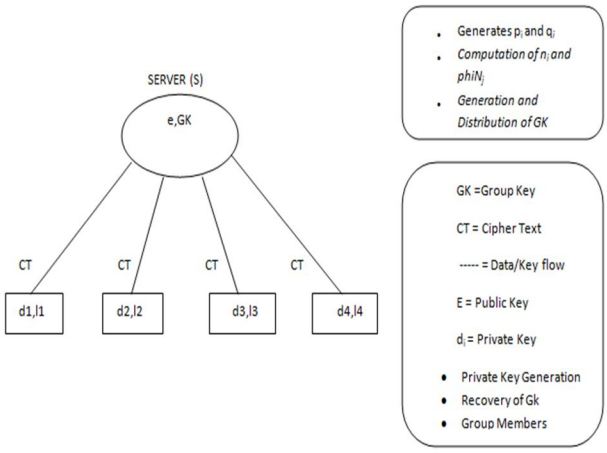


Fig. 1. Centralized group key management

A. Initialization Stage

Initially, the S randomly generates two distinct large prime numbers P_i and Q_i and compute w_i and $\Phi(w_i)$, such that $w_i = P_i * Q_i$ and $\Phi(w_i) = (P_i - 1) * (Q_i - 1)$; for $1 \leq i \leq n$, where n is a size the group G. The S also generates large distinct secret prime numbers k_i for n members and execute the following steps.

1.TheS computes $m = \prod_{i=1}^{n}(w_i)$ and r_i such that $r_i = \frac{m}{w_i}$ where i = 1, 2, …, n.

2.Then the S computes s_i, such that $r_i * s_i \equiv 1 \bmod (w_i)$, where s_i is the multiplicative inverse of r_i modulus w_i.

The S computes R_i for each group member using following equation.

$$R_i = k_i * r_i * s_i \quad (1)$$

Next, the S verify the member who needs to join the group. The S additionally select a large positive integer 'e' as a public key, such that $n < e < \min(\Phi(w_1), \Phi(w_2), \ldots, \Phi(w_n))$ and public key e circulated to group members. After that, the S initialize the parameter W as W =1, which is utilized in the key update stage to encrypt the group key.

2. Member join stage

Any new member gm_i is verified by S to join the group G for the first time, the S needs to send the secret parameters k_i, W_i, $\Phi(w_i)$ to the new member, that are generated in the initialization stage by the S. After that, the S computes the new value of the parameter W, such that $W = W^* \prod_{i=1}^{n} w_i$, and the S computes group key encryption key d_q by following equation.

$$d_q = \sum_{i=1}^{n} R_i \quad (2)$$

The newly joined members execute the following steps:

Initially the members generate his/her own private key d_i by using the following modular equation.

$$e*d \equiv 1 \bmod (\Phi(w_i)) \quad (3)$$

1. Next, the members generate l_i, such that l_i is multiplicative inverse of the secret parameter k_i by using the following equation.

$$k_i * l_i \equiv 1 \bmod (w_i) \quad (4)$$

The private key d_i and the value of l_i are kept secret in the member's database. Next the S computes the group key, GK for the multicast communication by the following equation.

$$GK \epsilon \min (w_1, w_2, w_3, \ldots, w_n)$$

The minimum value of w_i selected as a group key of the group G. After that, the S encrypt the group key GK by the steps explained in key update stage and circulate the GK among the group. Upon receiving the encrypted GK, the member the recover the GK by the steps explained in key recovery stage.

3.Key update stage

Whenever, the new members need to join the group or existing members need to leave the group G, the S needs to compute and circulate the new GK to all the participants of the group G in secure manner with minimum computation cast.

The S encrypt the group key GK and computes the cipher text CT using the following equation.

$$CT = (d_q * (GK)^e) \bmod W \quad (5)$$

4. Key recovery stage

After receiving the cipher text CT, the group member gm_i recover the group key GK by decrypting CT, by his/her own private key d_i, parameter l_i and x_i as

$$GK = ((CT \ mod(w_i) * l_i) \ mod(w))^{d_i} \ mod \ (w_i) \quad (6)$$

5.Member leave stage

Due to dynamic nature the group, the group members gm_i can leave the group at any time. When group member wants to leave the group, the S delete his/her w_i value from the database and refresh the parameter W as W' = $\frac{w}{w_i}$. After that the S refresh the group key encryption key d_q as $d_q' = d_q - R_i$. After compute the d_q' and W' value, the S regenerate the group key GK and encrypts using dQ' and W' as

$$CT' = (d_q' * (GK')^e) \bmod W \quad (7)$$

The computation complexity of S during key refreshing is reduced by minimizing the number of activities performed by S. These activities are decreased by wiping out the computation of w_i, $\Phi(w_i)$ and R_i during key refreshing. In the proposed GKDP protocol the computation of w_i, $\Phi(w_i)$ and R_i is done in S initialization stage.

When a new group member needs to join the group, the S needs to perform a single addition, multiplication and one encryption. Similarly, when an existing member needs to leave the group, the S needs to perform a single subtraction, division and one encryption. To provide high security, we introduce an additional key called group key encryption key for encrypting the group key. If any changes occur in group, the S broadcast the message to provide the information about the refreshed GK to the group members.

V. SECURITY ANALYSIS

In this section we analyze the security strength of the proposed GKDP protocol and prove that the protocol is secure against factorization attack, collision attack and satisfy the backward and forward secrecy. In proposed GKDP the value of W_i, Φ (W_i) and Ri are kept secret by SERVER. The value of l_i and d_i are kept secret by group members.

A. Factorization Attack

Using the factorization attack, the adversary A can factors the modulus xi and computes Φ (w_i). To compute the private key d_i of a member, an adversary A needs publicly available parameter e and Φ (w_i). In GKDP protocol the value of w_i, Φ (w_i) and Ri are kept secret by SERVER. Therefore, the value of w_i and Φ (w_i) are not publically available. Without know the value of w_i and Φ (w_i), the adversary A cannot compute private key d_i. So that, the proposed GKDP protocol secure against the factorization attack.

B. Collision Attack

In collision attack, at least two adversaries who are participating the group communication may collaboratively compute the refreshed GK after leaving the group. In proposed GKDP protocol, each group members gm_i have their own private key d_i, secret parameter l_i, public key and modulus w_i. Modulus w_i value is removed from W after the existing group member leave the group. Without knowing the modulus w_i, the group member who have leave the group is cannot compute the private key d_i. To get the refreshed GK, the value of w_i, l_i and private key d_i are used. The members who have leave the group are cannot able to compute the refreshed GK.

C. Backward Secrecy

To provide the forward secrecy in the group, the S is responsible to prevent the newly joining members form having the access to previously communicated data. The newly joined group members are cannot get the previous communication details, because in the encryption of old GK, the parameter w_i of recently joined members have not been utilized. If an adversary A is a member of group G and try to access the previous communication details, adversary A needs to recover the old GK. Which is impossible.

D. Forward Secrecy

To provide the backward secrecy in the group, the S responsible to prevent the leaving members from the furtherof communication. The members who leave from the group G, the S removed their w_i value from the member list and then the S refreshes the parameter W. This refreshed W value such as W' used to encrypt the new GK. The members who leave the group are unable to compute the new GK.

VI. EXPERIMENTAL RESULTS AND ANALYSIS

The proposed GKDP scheme is implemented in JAVA and executed on the computer with configuration Intel Core i5 processor, 4 GB RAM, 350 GB HDD, windows-10 OS. To perform the key update and key recovery operations with different key sizes varying from 64 bits to 512 bits and group sizes varying from 10 to 100 members. The computation time for GK update and GK recovery are measured in various group sizes as well as various key sizes are shown in table 1 and table 2.

Table 1
Key update operation's computation cost shown in Sec

$no.\ of\ members / key\ sizes$	64 bits key	128 bits key	256 bits key	512 bits key
10 members	1.9	3.8	4.8	5.3
20 members	2.3	4.4	6.4	8.8
30 members	2.9	6.7	9.5	10.8

Table 2
Key recovery operation's computation cost shown in Sec

$no.\ of\ members / key\ sizes$	64 bits key	128 bits key	256 bits key	512 bits key
10 members	1	1.5	1.6	2.2
20 members	1.5	1.6	1.8	2.5
30 members	1.7	1.9	2.1	2.9

The experimental results shown in Fig.2. and Fig.3. compared the computation cost (time) in seconds for key size of 64 bits and various group members varying from 10 to 30. In Fig.2. and Fig.3. The computation cost shown in y-axis and a number of members shown in x-axis.

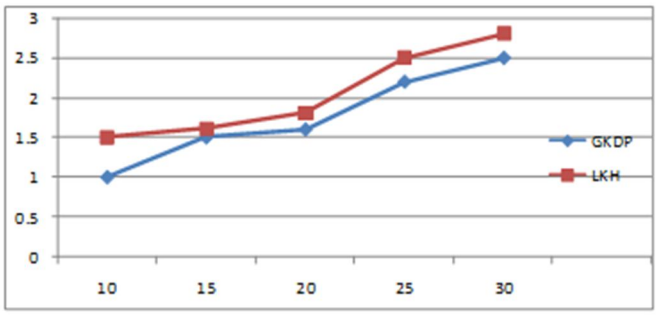


Fig. 2. Computation cost of GK update.

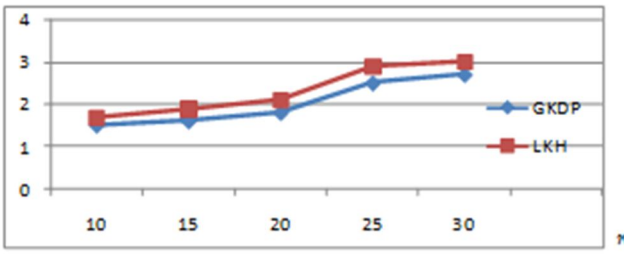


Fig. 3. Computation cost of GK recovery

VII. CONCLUSION

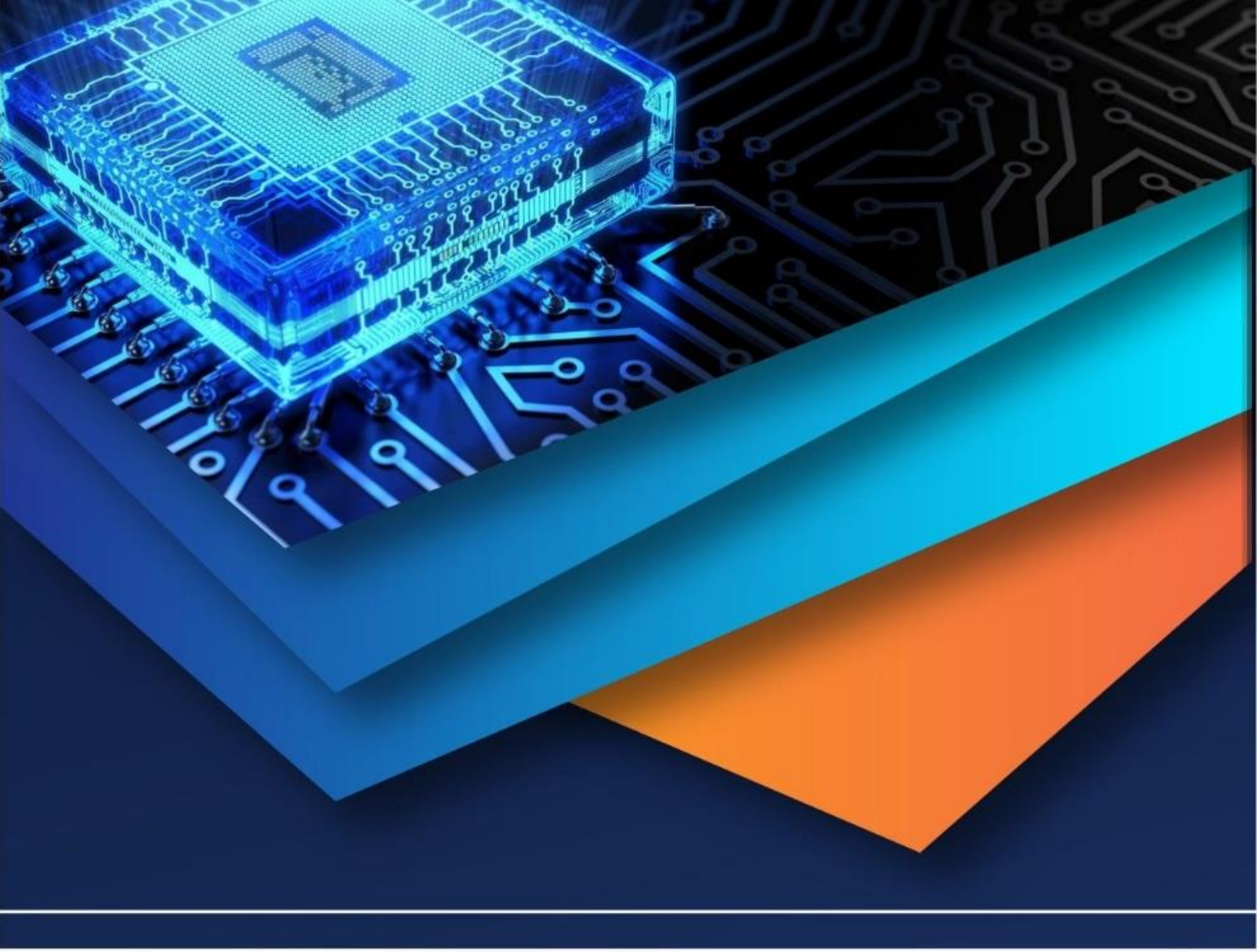
This paper proposes an efficient group key management protocol for secure multicast communication on star topology that reduces the computational complexity of S. The computational complexity of group members is also reduced. In the proposed scheme, just single message is required to refresh the GK. The proposed GKDP protocol provides both forward and backward secrecy. This scheme, secure against factorization and collision attacks. GKDP protocol is efficient and adaptable for small group working in the centralized environment.

REFERENCES

[1] Payal Sharma and Purushothama B. R, Analysis of Traditional Secure Group Key Management Schemes in Secure Multi-group Communication, International Conference on Communication and Signal Processing, July 28 - 30, 2020.
[2] P. Vijayakumar, S.Bose, A.Kannan, Error Detection and Correction for Distributed Group Key Agreement Protocol, international Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.
[3] Khan, Adnan Shahid, Secure and efficient distributed relay-based rekeying algorithm for group communication in mobile multihop relay network. Int. J.Commun. Netw. Inf. Secur. 6 (3), 189.2014.
[4] R Keerthana, Dr.N.M Saravana Kumar, A Cost-Effective Multicast Key Management Scheme for Secure Group Communication, International Journal of Innovative Research in Computer and Communication Engineering, An ISO 3297: 2007 Certified Organization Vol.2, Special Issue 1, March 2014.
[5] VijayaKumar, P., Bose, S., Kannan, A., Chinese remainder theorem based centralized group key management for secure multicast communication. IET Inf. Secur. 8 (3), 179–187, 2014.
[6] Elhoseny, Mohamed, A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic Lin, encryption. J. King Saud Univ.-Comput. Inf. Sci. 28 (3), 262–275, 2016.
[7] Hua-yi, Hsieh, Meng-yen, Li, Kuan-ching, The cluster-based key management mechanism with secure data transmissions scheme in wireless sensor networks. DEStech Trans. Eng. Technol. Res. Amma 2017.
[8] Islam, S.K. Hafizul, Biswas, G.P., A pairing-free identity-based two-party authenticated key agreement protocol for secure and efficient communication. J. King Saud Univ.-Comput. Inf. Sci. 29 (1), 63–73, 2017.
[9] Liu, Z., Lai, Y., Ren, X., Bu, S., 2012. An efficient LKH tree balancing algorithm for group key management. In: 2012 International Conference on Control Engineering and Communication Technology, Liaoning. pp.1003–1005.
[10] Wallner, D.M., Harder, E.J., Agee, R.C., 1998. Key management for multicast: issues and architectures. Internet Draft Report. Filename: draft-wallner-key-arch-01. txt.
[11] Xu, L., Huang, C., 2008. Computation-efficient multicast key distribution. IEEE Trans. Parallel Distrib. Syst. 19 (5), 577–587.
[12] Tegshbayar Gerelbayar, Jong Sou Park A New Centralized Group Key Distribution and Revocation in Sensor Network, 2007 International Conference on Computational Intelligence and Security.
[13] E.Munivel, ILokesh Design of Secure Group Key Management Scheme for Multicast Networks using Number Theory.
[14] Safdar Hussain Shaheen, Muhammad Yousaf Source Specific Centralized Secure Multicast Scheme based on IPSec, 2015 Conference on Information Assurance and Cyber Security (CIACS).
[15] Francisco Jordan and Manuel Medina Secure Multicast Communications using a key Distribution Center DAC/UPC Report No. RR-93/21 November 1993.

[16] Yuhong Luo, Jianxin Wang, Weihua Gui A Distributed Algorithm for Building Energyefficient Group-Shared Multicast Tree in Ad Hoc Networks, 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing.
[17] Chenglian Liu, Yongning Guo, and Juan Lin Security Analysis of RSA Cryptosystem Algorithm and it's Properties, International Conference of Computational Methods in Sciences and Engineering 2014 (ICCMSE 2014) AIP Conf. Proc. 1618, 468-470 (2014).
[18] Wong, C.K., Gouda, M., Lam, S.S., 2000. Secure Group Communications Using Key Graphs. IEEE/ACM Trans. Networking 8 (1), 16–30.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)