International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

A Novel and Secure Approach to Group Key Agreement

Naila N N[1], Prof. L M Bernaldu[2]

[1]*PG Scholar, Dept of CSE, Rajadhani Institute of Engineering and Technology, TVM, Kerala*
[2]*Professor, Dept of CSE, Rajadhani Institute of Engineering and Technology, TVM, Kerala*

Abstract - *The objective of this paper is to study a group key agreement problem of assigning a unique key for communication. Group key agreement provides the mechanism where any two unknown person can communicate directly. To make this possible we are using the theory of Diffie-Hellman algorithm. Group key agreement is more effective for the social networks. In our system we are using passively secure protocol to construct an actively secure protocol which is round efficient. Also we are using Identity-based (ID-based) ring signature with forward security in Group key Agreement to enhance security for data sharing between users.*

Key Words: **Group Key Agreement, Diffie Hellman Key Agreement, ID-based Ring Signature, Forward Security.**

1. INTRODUCTION

Group Key agreement is a process of assigning a unique key for communication. On social networks mostly it is not possible to communicate with unknown person directly. Group key agreement is a mechanism that allows two or more parties to securely share a secret key called a session key. Group key agreement provides the mechanism where any two unknown person can communicate directly. For example on social sites there are groups of people communicate together. But it is not necessary that each and every person in a group well knows each other. Assume there are persons A, B and C. Person A and B is good friends. Person C is a friend of A but B wants to communicate C. So to get the authority to communicate with C, B must have to go through A. Then the communication between them can possible. But in Group Key Agreement mechanism direct communication between B and C can possible. To make this possible we are using the theory of Diffie-Hellman algorithm. Diffie-Hellman algorithm provides the key exchange mechanism for communication.

In the Group key agreement, each user is only know his neighbors and has no information about the existence of other users. Further, he has no data about the system topology. In this system, a user does not need to trust a user who is not his neighbor. Thus, if one is initialized using PKI, then he need not trust or remember public-keys of users beyond his neighbors. Group key agreement is more effective for the social networks. In our system we are using passively secure protocol to construct an actively secure protocol which is round efficient. Many group communication applications needs security services which are built on the top of secure group key management. Data sharing with a large number of participants in group must take into account several problems, including data integrity, confidentiality and efficiency of sender. Ring signature is an approach to construct an authentic and data sharing system. It allows a data sender to authenticate his data anonymously. Since the costly certificate verification in the public key infrastructure (PKI) setting becomes a problem for this solution to be scalable. Instead Identity-based ring signature, which removes the process of certificate verification, can be used.

2. LITERATURE SURVEY

2.1 Group key agreement with local connectivity

In this paper [1], deals with group key agreement problem, where a user is only aware of his neighbors while the connectivity graph is arbitrary. In addition, users are initialized completely independent of each other. A group key agreement in this system is very suitable for applications such as social networks. They constructed two passively secure protocols with contributiveness and proved lower bounds on a round complexity, demonstrating that protocols are round efficient. Finally, they constructed an actively secure protocol from a passively secure one. They did not consider how to update the group key more efficiently than just running the protocol again, when user memberships are changing.

2.2 Cost Effective Authentic and Anonymous Data Sharing with Forward Security

In this paper [2], deals with ring signature in ID-predicated settings. The scheme provides of unconditional anonymity and can be proven forward-secure in the desultory oracle model. The scheme is very efficient and does not require any pairing operations. The size of utilizer secret key is just one integer, while a key update process only requires an exponentiation. This will be very utilizable in many other practical applications, especially to those require authentication and utilizer privacy, such as ad-hoc network, e-commerce of activities and perspicacious grid. The system withal implemented in multi-cloud system is used to increase the efficiency of the sizably voluminous storage and data sharing system. Thus it reduces the computation. Reduction of space and time requisites makes better the cost efficient mechanism. The current scheme relies on the arbitrary oracle postulation in order to prove its security. The provably secure scheme with the same features in the standard model as an open for future research work.

2.3 Cost Effective Region-Based Group Key Agreement Protocol for Secure Group Communication

This paper deals with a fascinating security issue in remote spontaneous systems: the Dynamic Group Key Agreement

key foundation. In an Ad hoc system for secure gathering correspondence, a gathering key that is shared by all gathering individuals is needed. This gathering key must to be updated when the new party joins or current party leaves in the gathering. In this paper, author proposed a novel, secure and effective Region-Based Group Key Agreement convention (RBGKA) for specially appointed systems. This was executed by a two-level structure and had another plan of gathering key update[3].

2.4 Security in User Data Using Multicast Key Agreement

In this work they are intended to give a grouping of clients with a common secret key such that the clients can safely communicate with one another over an open system. Gathering makes a typical mystery key to be utilized to trade data safely. They consider the gathering key concurrence with a self-assertive network diagram, where each client has lots of neighbours and has no knowledge about the presence of different clients. Also he has no knowledge about the system topology. In this system, there is no focal power to in state clients and can be instated autonomously utilizing PKI. [4]

2.5 Performance of Group Key Agreement Protocols

This paper deals with a five outstanding key administration methods incorporated with a solid gathering correspondence framework. The five procedures is presented in light of trial results got in genuine nearby and wide-zone systems. The estimation analyses led for all routines offer experiences into their adaptability and reasonableness. Also their examination of the trial results highlights a only few perceptions which are vague compared to the hypothetical analysis [5].

3. PROBLEM DEFINITION

A key-agreement protocol is a protocol where one user is only knowledge of his neighbors. Two or more parties can agree on a key in manner that they both influence the outcome. If properly done, this eliminates undesired third parties from forcing a key choice on the agreeing parties. Sender generates key and sends it to receiver. The connection made between is actively secure protocol using passively secure one. Protocols that are useful in practice also do not reveal to any attacker what key has been agreed upon. Public-key agreement protocol that satisfies the above condition was the Diffie–Hellman key exchange. In this key exchange two parties jointly exponentiation a generator using random numbers, in such a manner that an attacker cannot determine what the resultant value used to produce a shared key. Exponential key exchange in and of itself did not specify any prior agreement or subsequent authentication between the group participants. So it was described as an anonymous key agreement protocol.

The Existing system has the drawbacks such as it did not consider how to update the group key more efficiently than just running the protocol again, when user memberships are changing. So lot of bottleneck's to the group controller in the sub group. Efficiently managing the group key is a difficult problem for large dynamic groups. Each time a member is added to or evicted from the communication group, the group key must be refreshed. The members in the group must be able to compute the new group key efficiently, at the same time forward and backward secrecy must be guaranteed. Because the group re-keying is very consumptive and frequently performed due to multi-secure computing communication, the way to update it in a scalable and secure fashion is required.

3.1 Broadcast encryption

This mechanism allows a sender to send a group key to a selected number of users. This can be considered as a group key agreement of one message by the sender. . The sender is a fixed authority in a symmetric key based broadcast encryption system. In this case, the user key size is combinatorial lower bounded.

The disadvantages consist of:

1. It is secure only against a limited number of users.
2. In a public key broadcast encryption, the key size problem can be waived. But one still has to set the threshold for the number of bad users.
3. Cipher text size depends on the number of users and hence could be large.
4. Users are initialized by a central authority which is not desired in our setting.

In proposed system we implement the existing system with more time efficient manner and provide a the upgraded concept of the secure ID-based signature provides with forward security: If a secret key of any user has been bargained, all past created signatures that incorporate these users still remain legitimate. This property is particularly critical to data sharing system which provide multilevel security, as it is difficult to ask all data owner to re-authenticate their data regardless of the possibility that a secret key of one single user has been traded off. A strong and effective instantiation of the plan, exhibit its security and give an execution to show its sound judgment. The basic plan eliminates the correlation among data and thus provides the perfect resilience to data security, and it is also proficient in terms of, computation, latency and communication overhead which support the validation of any number of data simultaneously

1. In this paper, propose an approach called ID-based ring signature, which is an essential tool for building authentic and anonymous data sharing along with group key agreement.
2. Also using forward security to enhance the ID-based ring signature.

3. Prove the security of the proposed scheme in the random oracle model, under the standard RSA assumption.

4. METHADOLOGY

The Identity-based (ID-based) ring signature with forward security in Group key Agreement for Multi secure computing communication provides an efficient way of Multi secure computing communication key Agreement in terms of Scalability and Authenticity between the Sub multi secure computing communication members and to other multi secure computing communication members in the network.

4.1 Group Key Agreement

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

4.2 Key pre-distribution System

Key pre-distribution system (KPS) can be considered as a non-interactive group key agreement. There is a shared key for each group that is fixed in this system. When a group is updated, then the group key changes to the shared key of the new group. The disadvantages of KPS is that the user key size is combinatorial large in the total number of users even if the system secure. Another disadvantage is that the key of a given group(e.g., cryptanalysis of cipher texts bearing this key) cannot be changed even if it is leaked. The problem in the key size may be overcome when a computationally secure system is used.

4.3 Lower Bound

Broadcast encryption mechanism allows a sender to send a group key to a selected number of users. This can be regarded as a group key agreement of one message by the sender. The sender is a fixed authority in a symmetric key broadcast encryption system. The user key size is combinatorically lower bounded. Also it is secure only for a limited number of users. The key size problem couldn't be considered in public key broadcast encryption. The threshold for the number of bad users is to be set. Also the cipher text size depends on the number of users. Also, users are initialized by a fixed authority which is not desired. In this system, construct two efficient passively secure protocols and also prove lower bounds on the round complexity which demonstrates that protocols are round efficient. Finally, develop an actively secure protocol from a passively secure one.

4.5 Diffie -Hellman Algorithm

Diffie Hellman algorithm provides the computationally secure group key exchange mechanism for communication in a passive model. In Diffie-Hellman protocol we use the tuple (a; b; c) to represent a protocol that has a rounds, b elements of messages per user (the unit is a field element in Z_ p for a large prime p) and computation cost c. it is used to design a group key agreement for n users in a ring with an efficiency tuple.

4.6 Identity-based Ring Signature

The private or hybrid Identity-based (ID-based) crypto-system, reduce the need for verifying the validity of public key certificates whose management is both time and cost consuming. In an ID based cryptosystem, the public key of each user was easily computed from a string corresponding to this user's publicly known identity (e.g., an email address, residential address, etc.). A private key generator (PKG) then calculate the private keys from its master secret for users. This property avoids the requirement of certificates (which are necessary in traditional public-key infrastructure) and associates an implicit public key (user identity) to each user within the system. In order to prove an ID-based signature, different from the traditional public key based signature, one need not to verify the certificate first. The elimination of the certificate verification makes the whole verification process more efficient, which will lead to a significant save in communication and computation when a large number of users are involved.

4.7 Forward security

In cryptography, the property of key-agreement protocols called forward secrecy or perfect forward secrecy which ensures that a session key derived from a set of keys couldn't be discovered if one of the long-term keys was discovered in the future. The attacker only needs to include the compromised user in the group of his choice. As a result, the disclosure of one of the user's secret key causes all previously obtained ring signatures becomes invalid (if that user is one of the ring members), since one cannot distinguish whether a ring signature is generated prior to the key exposure or by which user. Therefore, forward security is a necessary requirement for a data sharing system. Otherwise, it will lead to a huge waste of time and resource.

5. CONCLUSION

Here studied a group key agreement problem where a user is only knowledge of his neighbors while the connectivity graph is arbitrary. Also there is no centralized initialization for users In this system construct two protocols with passive security. Then obtain lower bounds on the round complexity for this type of protocol, which demonstrates that constructions are round efficient. Finally, constructs actively secure protocol from a passively secure protocol. In addition to this for secure data sharing through group also proposed a notion called Forward Secure ID-Based Ring Signature which allows an Identity-based ring signature scheme with forward security to enhance it. . A group key agreement with these features is very suitable for social networks and also this property is useful in large scale data sharing system through group.

REFERENCES

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

[2] Xinyi Huang, Joseph K. Liu+, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, Jianying Zhou," Cost-Effective Authentic and Anonymous Data Sharing with Forward Security", IEEE Transactions on computers (Vol: 64, No: 6), 2015.

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

[4] Shahela A Khan, Prof. Dhananjay M. Sable,"Survey on Security User Data in Local Connectivity Using Multicast Key Agreement", in International Journal on Recent and Innovation Trends in Computing and Communication ,Volume: 3 Issue: 10.

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

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

[7] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen. Forward secure identity-based signature: Security notions and construction. Inf. Sci., 181(3):648–660, 2011.