International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 01 | Jan -2017 www.irjet.net p-ISSN: 2395-0072

A SURVEY ON GROUP KEY AGREEMENT FOR SECURELY SHARING A SECRET KEY

Jaitee Bankar[1], Prof. Jyoti Raghatwan[2]

1 Jaitee Bankar, RMD Sinhgad School of Engineering, Pune

2 Prof. Jyoti Raghatwan , RMD Sinhgad School of Engineering, Pune

Abstract- *Key management, particularly in a group setting, is the corner stone for all other security services. As a result of the increased popularity of group-oriented applications and protocols, group communication occurs in lots of different settings: from network multicasting to application layer teleconferencing and video conferencing. Apart from of the application environment, security services are required for providing communication privacy and integrity. This fundamentally rules out the traditional key distribution paradigm because it calls for superior trust in the group member who generates and distributes keys. We focus on a group key agreement problem with local connectivity, where a user is only aware of his neighbors while the connectivity graph is arbitrary. There is no central authority to initialize the users. A group key agreement with these features is very suitable for social networks. We propose two efficient protocols with passive security: Diffie Hellman Key Agreement (DH-KA) protocol and a private coin tossing protocol protected by Diffie Hellman key (XO-KA). Finally, an actively secure protocol is constructed from a passively secure protocol by developing a two-stage protocol.*

***Key Words*: Group key agreement, Diffie Hellman Key Agreement, private coin tossing protocol, passively secure protocol, actively secure protocol**

1. INTRODUCTION

A key agreement is a method where two or more parties agree on a key such that both influence the result. This method allows two or more parties to share a secret key in a secure way. If this is properly done then it precludes undesired third parties form a forcing key selection on the agreeing parties. Several key exchange systems have one party generate the key and merely send that key to other party. The other party has no influence on that key. By using a key agreement protocol some of the key distribution problems can be avoided which are associated with such type of systems. Protocols in which both the parties manipulate the final derived key is the single way to implement perfect forward secrecy.

Nearly all the protocols assume a complete connectivity graph that is any two users can communicate directly. But, this is not the case, in the real world. For example, in social networks such as Facebook, Skype, Wechat and Google+, a user is simply connected with his friends. When a group of users desire to establish a session key, it is not necessary that any two of them must be friends. But they might still be connected indirectly through a friend network. Certainly, it can be still regarded as directly connected by regarding the intermediate users as routers. Although, this is somewhat different from the direct connection. Firstly, indirectly connected users may not have the public information of each other. Then, indirectly connected users may not know the existence of each other. Again, a message among two indirectly connected users needs a longer time than that between directly connected users.

Thus, a group key agreement with an arbitrary graph leads to a complex key agreement problem where each user is only aware of the neighbors and has no information about the other users as well as the user does not have any information regarding the network topology. In this paper, a group key agreement problem with local connectivity is studied, where a user is only knows his neighbors and the connectivity graph is arbitrary. There is no central authority for initializing the users. A group key agreement with these features is very appropriate for social networks. We propose two efficient protocols with passive security: Diffie Hellman Key Agreement (DH-KA) protocol and a private coin tossing protocol protected by Diffie Hellman key (XO-KA). Finally, an actively secure protocol is proposed.

In this paper we have surveyed on group key agreement having local connectivity. Section 2 of this

paper deals with Literature Survey and Section 3 presents Proposed System. Section 4 concludes this paper.

2. LITRATURE SURVEY

A comprehensive literature survey is performed in the support of the group key agreement problem. In literature, several techniques have been presented for allowing two or more parties to securely share a secret key called as session key. In network security field, the group key agreement problem is considered to be the challenging task that tries to address the issue of securely sharing a secret key between two or more parties. The group key agreement with an arbitrary graph is the main difficulty for securely sharing the secret key among multiple parties. Several methods have been proposed to solve the complexity observed in the group key agreement. Group key agreement still remains difficult task.

To send secret messages to any subset of the group members, the ConBE system is used. Group of members negotiate on a common public encryption key. ConBE system leads to a problem of establishing secure broadcast channels and secure numerous emerging distributed computation applications. [2] A fingerprinting system using the group property is used for generating the fingerprints in order to face the collusion attack made by group of users. In the collusion attack that includes several groups, the performance of system decreases. [3]

Broadcast encryption allows user to send a group key to only selected group of users. The security model proposed in [4] uses broadcast encryption for dynamic group key agreement protocols which is secure only against a limited number of users. The slot based multiple group key management scheme considers movement of single and multiple mobile receivers with backward secrecy and employs a rekeying scheme. This scheme updates the group key whenever there is a group membership change. It has the drawback of updating the group key upon member leave. [5]

A security model for a certificateless group key protocol has been presented in and a constant-round group key agreement protocol based on certificateless public key cryptography has been proposed. [6] This model employs a random oracle model and has dependency on long term secrets.

A generic construction idea based on the Chinese Remainder Theorem is used for asymmetric group key agreement. The group key is set up using central authority and there is a dependency between the keys of different users. [7] A conference key distribution scheme has been proposed in [8] which employ key pre-distribution system. This scheme has the drawback of group key updation upon membership leave and group key cannot be changed in case of key leakage. Two key pre-distribution schemes for sensor network with mobile sink are proposed in [9] that can be regarded as non-interactive group key agreement. The group key is fixed and key leakage is not easy to resolve. These schemes cannot handle group size greater than three members.

3. PROPOSED SYSTEM

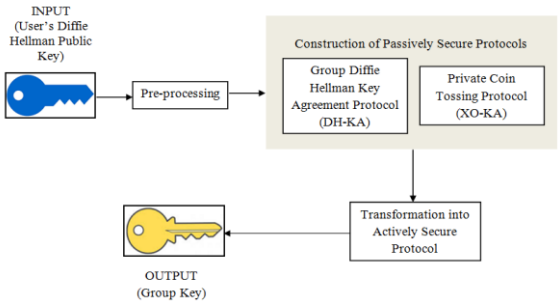

Figure 1: Proposed System Architecture

There is no universal methodology that can be used for group key agreement. Key establishment protocols have a long history of new protocols improving over past work in various aspects such as efficiency, features or security. However, this history is also paved with numerous flaws in many protocols which got only discovered later. Most of these flaws are due to an ad-hoc security analysis and due to overlooking various attacks. Building the protocol with systematic design and following prudent design and engineering principles can greatly reduce this risk. However, only a sound underlying formal model and rigorous security proofs can give real assurance of security. The majority of works employed in this domain fall under constructing actively secure protocols for group key agreement.

In the proposed system, basically two passively secure protocols have been proposed and then a real transformation of passively secure protocol into actively secure protocol has been done.

The proposed system follows the general three-step framework: preprocessing; construction of passively secure protocols and transformation into actively secure protocol as shown in figure 1. The first step is to notify each party of the key agreement event starting from an initiator. This is the starting assumption and it should be satisfied. The goal is to set up the session information and satisfy the starting assumption. The second step is construction of passively secure protocols. Two passively secure protocols: Diffie Hellman Key Agreement (DH-KA)

protocol and a private coin tossing protocol protected by Diffie Hellman key (XO-KA) have been constructed. The last step is real transformation from a passively secure protocol to an actively secure one. It is done to essentially authenticate each message in passively secure protocol using a signature and make the passively secure protocol actively secure.

4. CONCLUSION

In this paper, we surveyed the group key agreement techniques and studied the group key agreement problem where the user is only aware of the neighbors and the connectivity is graph is arbitrary. In addition, users are initialized completely independent of each other. A group key agreement in this setting is very suitable for applications such as social networks. Three protocols for solving a group key agreement problem have been presented. The proposed sytem is very suitable for applications such as social networks.

ACKNOWLEDGMENT

It is my privilege to acknowledge with deep sense of gratitude to my guide Prof. Jyoti Raghatwan for her kind cooperation, valuable suggestions and capable guidance and timely help given to me in completion of my paper. I express my gratitude to Prof. Vina M. Lomte, Head of Department, RMDSSOE (Computer Dept.) for her constant encouragement, suggestions, help and cooperation.

REFERENCES

[1] Shaoquan Jiang, “Group Key Agreement with Local Connectivity”, IEEE Transactions on Dependable and Secure Computing, Vol. 13, No. 3, 2016.

[2] Qianhong Wu, Bo Qin, Lei Zhang, Member, Josep Domingo-Ferrer, Oriol Farras, and Jesus A. Manjon, ”Contributory Broadcast Encryption with Efficient Encryption and Short Ciphertexts”, IEEE Transactions on Computers, Vol. 65, No. 2, pp. 466 -479, 2016.

[3] Faten Chaabane, Maha Charfeddine, Chokri Ben Amar, ”Clustering impact on group based traitor tracing schemes”, 15th International Conference on Intelligent Systems Design and Applications (ISDA), pp. 440 - 445, 2015.

[4] Lei Zhang, Qianhong Wu, Josep Domingo-Ferrer, Bo Qin, Zheming Dong, ”Round-Efficient and Sender-Unrestricted Dynamic Group Key Agreement Protocol for Secure Group Communications”, IEEE Transactions on Information Forensics and Security, Vol. 10, No. 11, pp. 2352 - 2364, 2015.

[5] Trust Tshepo Mapoka, Simon Shepherd, Raed Abd-Alhameed and Kelvin O. O. Anoh, ”Novel rekeying approach for secure multiple multicast groups over wireless mobile networks”, International Wireless Communications and Mobile Computing Conference (IWCMC), 2014.

[6] Jikai Teng and Chuankun Wu, ”Provable Authenticated Certificateless Group Key Agreement with Constant Rounds”, Journal Of Communications And Networks, Vol. 14, No. 1, 2012.

[7] X. Lv, H. Li and B.Wang, ”Group Key Agreement for Secure Group Communication in Dynamic Peer Systems”, J. Parallel Distributed Computing, vol. 72, no. 10, pp. 1195-1200, 2012.

[8] Reihaneh Safavi-Naini and Shaoquan Jiang, ”Unconditionally Secure Conference Key Distribution: Security Notions, Bounds and Constructions”, International Journal of Foundations of Computer Science, Vol. 22, No. 6, pp. 1369-1393, 2011.

[9] Amar Rasheed and Rabi N. Mahapatra, ”Key Predistribution Schemes for Establishing Pairwise Keys with a Mobile Sink in Sensor Networks”, IEEE Transactions On Parallel And Distributed Systems, Vol. 22, No. 1, 2011.