International Journal of Engineering Research and Development
e-ISSN : 2278-067X, p-ISSN : 2278-800X, www.ijerd.com
Volume 2, Issue 6 (August 2012), PP. 64-70

An Efficient Group Key Management for Wireless Multicast Networks

Anusha Bandari[1], Santoshkumari P.[2], Yatelli Prashanti[3], Dr. G.Manjunath[4]
[1,2,3] *Student, Dept. Of IT, JNIT, Hyderabad.*
[4]*Head, Dept of CSE & IT, JNIT, Hyderabad.*

Abstract—In a wireless multicast group, efficient key management is a big challenge due to constant changes in the network, limited processing capabilities and network constraints. Therefore continuously exchanging keys for peer authentication consumes tremendous bandwidth. Hence in this work we propose an efficient group key management technique which authenticates all the nodes in a multicast group by group authentication which eliminates the need for individual authentication of the nodes. The main challenges for secure multicast are scalability, efficiency and authenticity. In this project, we propose a scalable, efficient, authenticated group key agreement scheme for fixed multicast systems. The proposed key agreement scheme is identity-based which uses the combination of AES with Rinjdal, BLS, RSA. Compared with the existing system, the proposed system provides group member authenticity without imposing extra mechanism. Furthermore, we give a scalability solution based on the subgroups, which has advantages over the existing schemes. Security analysis shows that our scheme satisfies both forward secrecy and backward secrecy. Results shows that the scheme not only provides 100% accuracy in authentication but at the same time maintains optimum network performance.

Keywords— AES, Wireless Multicast Group, Key management, Security, Authenticity

I. INTRODUCTION

The Efficient Key Agreement for Large and Dynamic Multicast Groups provides an efficient way of Group key Agreement in terms of Scalability and Authenticity between the Sub group members and to other group members in the network. The Existing system have the drawbacks such as the Group Controller takes all responsibilities of key generation, re keys generation, message transmission to its sub group members and also to any other group controllers. So lot of bottleneck's to the group controller in the sub group. The sub group's members are not able to send information's to any other subgroup at the time of re keying process. So performance of the sub group degrades at that time. The re keying process is done every time once a communication is completed between the users in the same group or to any other group members. One of the main challenges for secure multicast is access control for making sure that only legitimate members of multicast group have access to the group communication. In the passed two or three decades, cryptography has become the well established means to solve the security problems in networking. However, there are still a lot of difficulties for directly deploying cryptography algorithms into multicasting environment as what has been done for unicasting environment. The commonly used Technique to secure multicast communication is to maintain a group key that is known to all users in the multicast group, but is unknown to anyone outside the 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 the nature of multicast communication, the way to update it in a scalable and secure fashion is required.

A. Benefits of Efficient Key Agreement for Large and Dynamic Multicast Groups

- Use identity tree based structure
- Less over head on key generation process
- The Group controller responsibilities can be shared by other members in the group (Group control Intermediate)
- Centralized server for the key generation process
- The group members in the same group directly communicate with each other without having the permission of authority persons.
- The Group controller key is act as a group key for group to group communication and scalability of the group
- The group members are not affected by the key generation process when they communicate with any other groups.

II. MOTIVATION

A. Existing System

In the Existing system we use Iolus approach proposed the notion of hierarchy subgroup for scalable and secure multicast. In this method, a large communication group is divided into smaller subgroups. Each subgroup is treated almost like a separate multicast group and is managed by a trusted group security intermediary (GSI). GSI connect between the subgroups and share the subgroup key with each of their subgroup members. GSIs act as message relays and key translators

between the subgroups by receiving the multicast messages from one subgroup, decrypting them and then re multicasting to the next subgroup after encrypting them by the subgroup key of the next subgroup. The GSIs are also grouped in a top-level group that is managed by a group security controller (GSC).
When a group member joins or leaves only affect subgroup only while the other subgroup will not be affected. It has the drawback of affecting data path. This occurs in the sense that there is a need for translating the data that goes from one subgroup, and thereby one key, to another. This becomes even more problematic when it takes into account that the GSI has to manage the subgroup and perform the translation needed. The GSI may thus become the bottleneck.

B. Limitations of the Existing System

- The Group controller takes all responsibilities for the group such as key generation, re keying process and message transfer to any other groups
- The group members are not able to communicate with any other groups during the re keying process.
- The Group controller maintains logical key tree where each nodes represents a key encryption key. The root of the key tree is the group key used for encrypting data in group communications and it is shared by all Users.

C. Proposed System

The advantages over the existing system are, we use an identity tree instead of key tree in our scheme. Each node in the identity tree is associated with an identity. The leaf node's identity is corresponding to the user's identity and the intermediate node's identity is generated by its children's identity. Hence, in an identity tree, an intermediate node represents a set user in the sub tree rooted at this node.

The keys used in each subgroup can be generated by a group of key generation centers (KGCs) in parallel. All the members in the same subgroup can compute the same subgroup key though the keys for them are generated by different KGCs. This is a desirable feature especially for the large-scale network systems, because it minimizes the problem of concentrating the workload on a single entity.

D. Advantages of Proposed System

- The Group controller responsibilities are shared by the Group control intermediater such as Re keying process and scalability of the group process.
- Use the Identity tree based structure.
- The group members are not affected by the key generation process when they are willing to communicate with any other group members.
- The Centralized key server used for key generation process and the KGC is also act as a Router for group to group communication.
- The Re keying process is done only to the particular group members not to the entire group members.

III. PROBLEM FORMULATION

A. Objectives

The objectives of the project are as follows:

- Design the single multicast group.
- Generation of private keys for users.
- Encoding and decoding of text message
- Secure transmission of session key by using the algorithm Advanced Encryption Standard (AES).
- Secured transmission of data using BLS
- Secured route discovery in inter group messaging using RSA
- Design the multi group with multiple data stream in such a way that reduced overhead of key server.
- Use Identity tree based structure. Each node in the identity tree is associated with an identity. The leaf node's identity is corresponding to the user's identity and the intermediate node's identity is generated by its children's identity. Hence, in an identity tree, an intermediate node represents a set of users in the sub tree rooted at this node.

IV. METHODOLOGY

The system overview is as follows. Each node can be part of one or more multicast groups. The group dynamic is presented in the figure below.

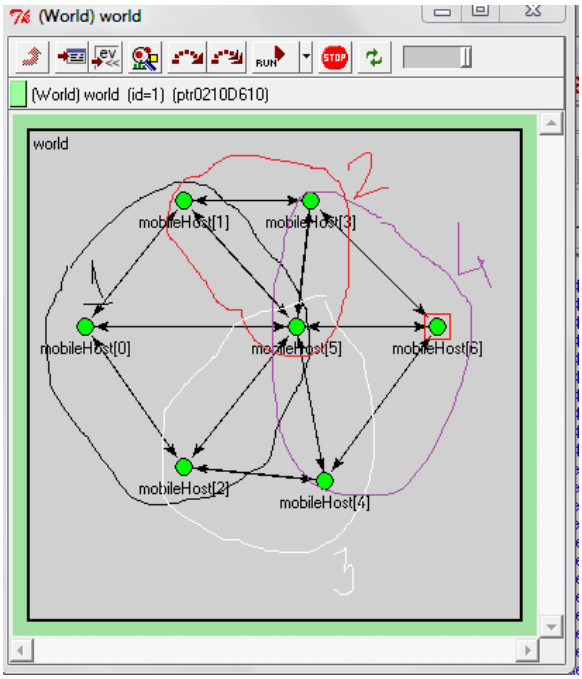

Fig. 1 Overview of the System

At the time of mitigating the network information, each node exchanges hello packets with it's neighbors. The HEllo message is broadcasted instead of multicasted. A node selects the group it belongs to and sign the packet with it's private key. The message is recived by the other nodes which decrypts the message using their public key, those nodes that successfully decrypts the message puts the sender's address in it's neighbors table, thus authenticating the node. This mechanism successfully authenticates the In-group nodes who do not need separate authentication for message exchange. The technique is further improved by demonstrating inter group authentication. Whenever a route request is generated from one group to another, the message is signed by a challenge digest. The groups aware of the inter group communication decrypts the message with AES. Once a route is formed, data is transferred as encrypted message with BLS technique. Hence here also for data communication, no separate authentication is needed.

A. Key Generation

Private Key:

The Private Key is generated using AES. There is no (Group Controller). All the nodes in a group are assumed to know it's private key as well as the public key of the group.

Session Key:

In session key generation, initially 128 decimal digits are generated by using random number generation method .Then each decimal digit is splited and compared with pre determined binary format. In AES algorithm the 128 bits session key is considered as a message file and generated user's private key is considered as a key file. AES algorithm encrypts the session key by using user's private key and transmitted to the appropriate users.

B. Joint Operation

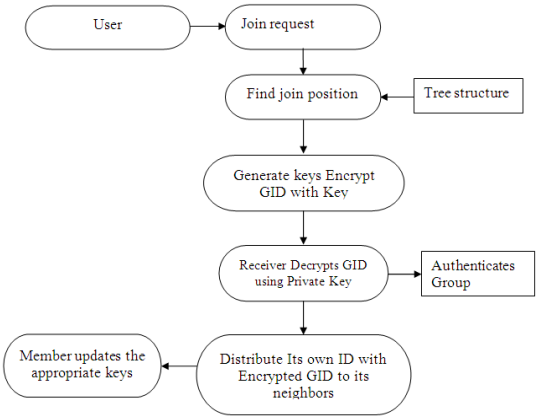

Fig. 2 Join Operation

C. Message Transmission

Multicasting is a process of sending a message to a selected group. Internet applications, such as online games, newscast, stock quotes, multiparty conferences, and military communications can benefit from secure multicast communications. In most of these applications, users typically receive identical information from a single or multiple senders. Hence, grouping these users into a single multicast group and providing a common session encryption key to all of them will reduce the number of message units to be encrypted by the senders. Various types of data communication are broadcast, Multicast, group communication.

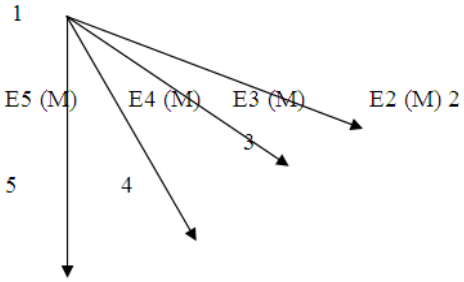

Fig. 3 Transmission of the message M through 4 point-to-point connections

Figure 3 shows the transmission of message m to four point to point connections. Here node number 1 is the service provider. Nodes 2,3,4,5 are the receiving nodes. Nodes 2,3,4,5 are receiving the same message.

D. Group communication

For group communications, the server distributes to each member a group key to be shared by all members of the group, distributing the group key securely to all members requires messages encrypted with individual keys (a computation cost proportional to group size). Each such message may be sent separately via unicast. Alternatively, the messages may be sent as a combined message to all group members via multicast. Either way, there is a communication cost proportional to group size (measured in terms of the number of messages or the size of the combined message). Observe that for a point-to-point session, the costs of session establishment and key distribution are incurred just once, at the beginning of the session. A group session, on the other hand, may persist for a relatively long time with members joining and leaving the session. Consequently, the group key should be changed frequently. To achieve a high level of security, the group key should be changed after every join and leave so that a former group member has no access to current communications and a new member has no access to previous communications.

E. Authentication

Authenticity means that when a user receives a message, it is assured about the identity of the sender. The authenticity requirement can be translated in the context of secure multicast into two requirements on key and data distribution.

Key authenticity: only the center can generate a session key.

Data authenticity: the users can distinguish among the data sent by the center and the malicious data sent by an attacker.

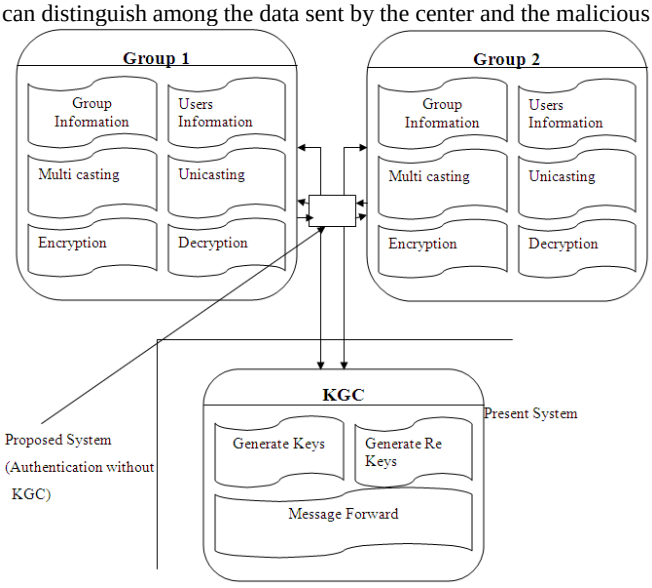

Fig. 4 Context Diagram

F. Message Transmission and Cryptography

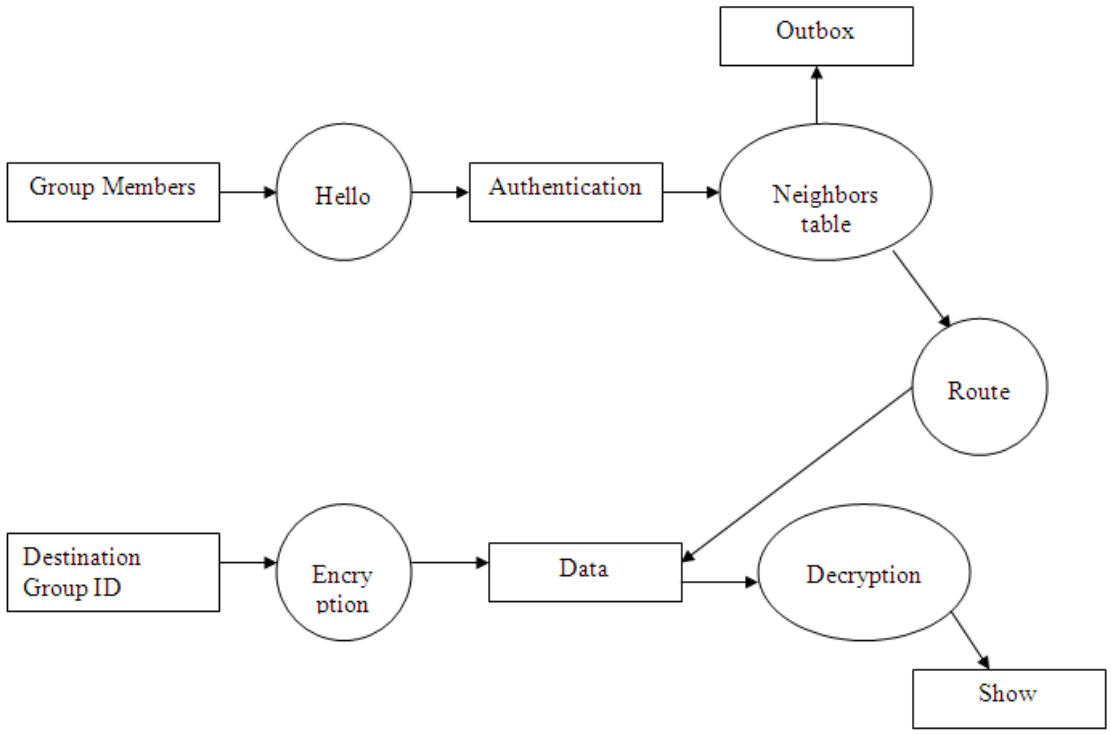

Fig. 5 Group to Group Communication

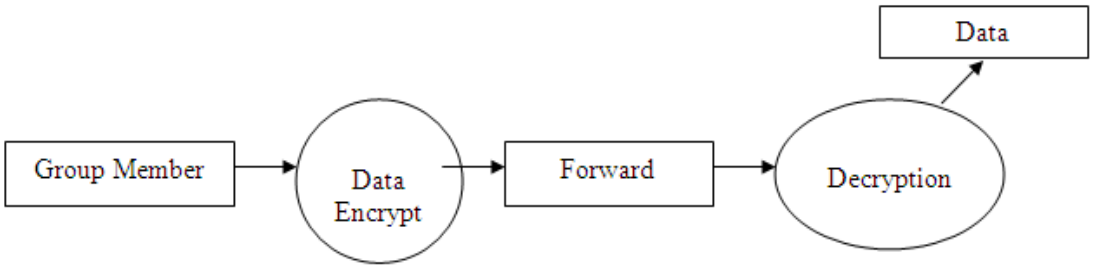

Fig. 6 Same Group Communication

G. Architectural Design

The Architectural Design is a process of dividing the project components into the processing modules and conceptual data structures.

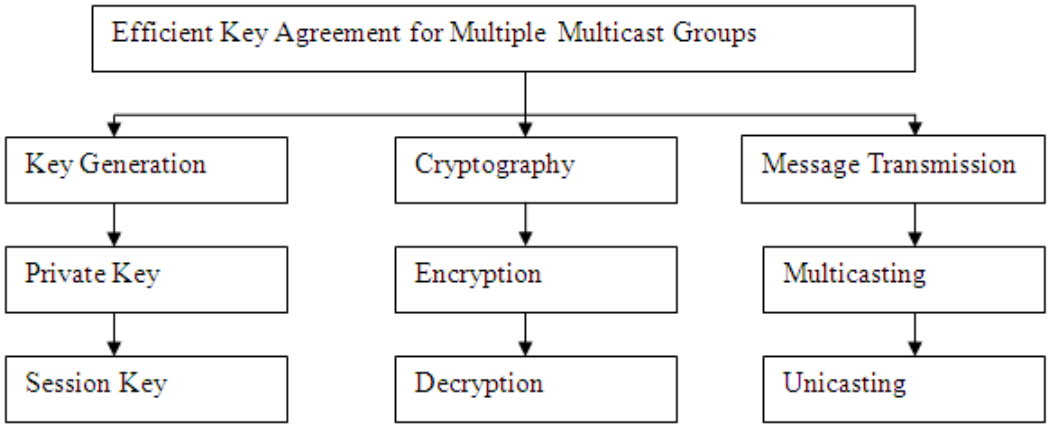

Fig. 6 Architectural Design

H. Sequence Design

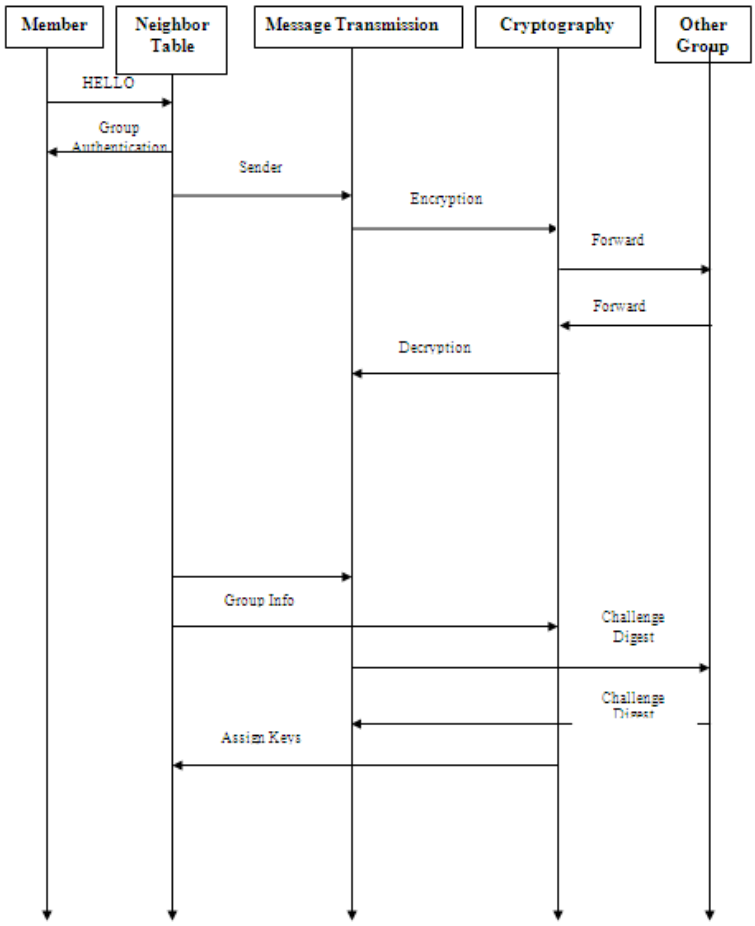

Fig. 7 Sequence Design

V. RESULTS

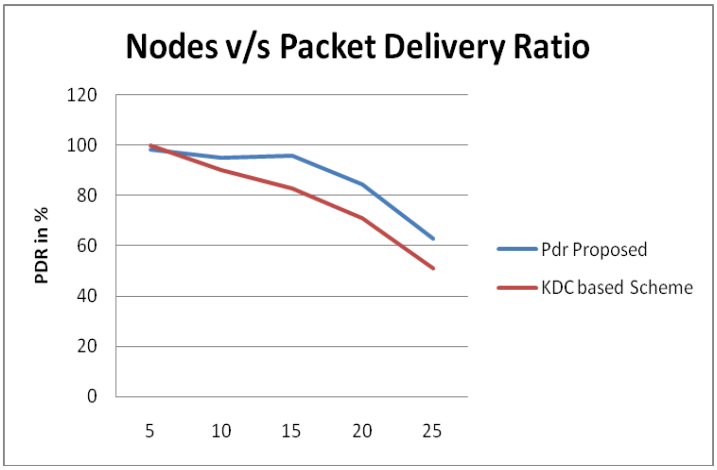

Fig. 7 Comparison of Packet Delivery Ratio with different number of nodes.

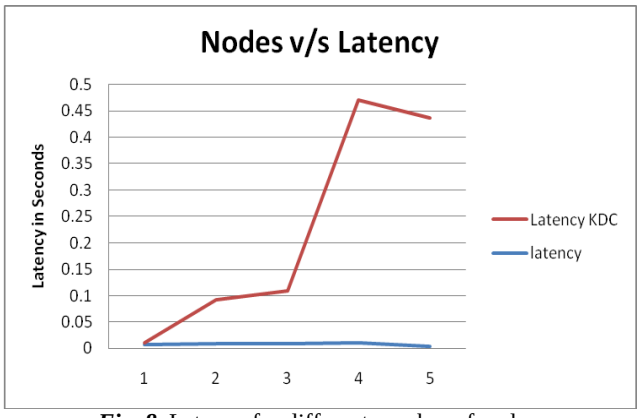

Fig. 8 Latency for different number of nodes.

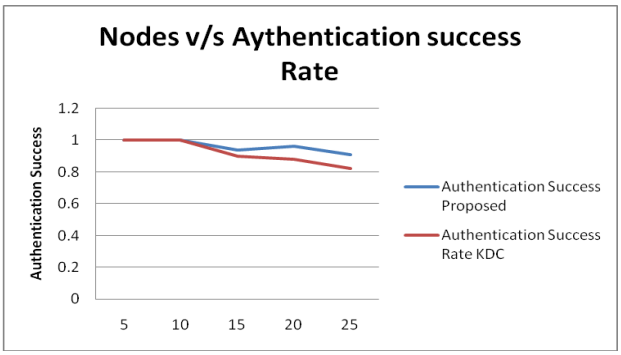

Fig. 9 Authentication Success rate for different number of nodes.

Results show that the authentication success rate of the proposed system is better for larger networks and for more groups. The system, along with providing best authentication solution provides a good performance as par as the packet delivery is concerned. Due to authenticating the group through control message exchange the system minimizes the latency. An easy way to comply with the paper formatting requirements is to use this document as a template and simply type your text into it.

VI. CONCLUSIONS

The Proposed system is an efficient, authenticated, scalable key agreement for communication amongst multicast systems without the requirement of separate key distribution server. Compared with the Existing system the proposed system is faster, more scalable and demands less data exchange as HELLO,RREQ and data message carries the authentication information as encrypted entity. Simulation shows that the rate of misclassification is low and invariable in comparision to data exchange rate or simulation time. The system can be further improved by incorporating session authentication using inter group session management.

REFERENCES

[1]. Y. Amir, Y.Kim, C. Nita-Rotaru, J. L. Schultz, J. Stanton, and G.Tsudik, ”Secure group communication using robust contributory key agreement,” IEEE Trans, Parallel Distrib. Syst., vol:15, no.5,pp,468-480, May 2004.

[2]. G. Ateniese, M. Steiner, and G. Tsudik , “Authenticated group key agreement protocols, ”in Proc.5th Annu. Workshop on selected Areas in Cryptography Security(SAC’98),1998,pp. 17-26.

[3]. S.Blake-Wilson and A.Menezes, “Authenticated Diffie-Hellman Key agreement protocols,” in Proc. 5th Annu. Workshop on selected Areas in Cyrptography (SAC’98),1998, vol. LNCS 950, pp. 275-286.

[4]. W. Diffie and M. Hellman, “New directions in cryptography,” IEEE Trans. Inf. Theory, vol. 22, no. 6, pp. 644–654, 1976.