RESEARCH ARTICLE OPEN ACCESS

Group Secret Key Generation in Wireless Networks: Algorithms and Rate Optimization

V.REKHA1 , A.KIRUTHIKA2 , R.KAVINILA3

[1] (Department of CS , Dhanalakshmi Srinivasan College of Arts & Science for Women, Perambalur-621 212.)

Abstract:

A group key generation algorithm investigates group secret key generation problems for different types of wireless networks, by exploiting physical layer characteristics of wireless channels. A new group key generation strategy with low complexity is proposed, which combines the well-established point-to-point pair wise key generation technique, the multisegment scheme, and the onetime pad. In particular, this group key generation process is studied for three types of communication networks: 1) A three-node network; 2) A multi node ring network; and 3) A multi node mesh network. Three group key generation algorithms are developed for these communication networks, respectively. The analysis8 shows that the first two algorithms yield optimal group key rates, whereas the third algorithm achieves the optimal multiplexing gain. Next, for the first two types of networks, we address the time allocation problem in the channel estimation step to maximize the group key rates. This non-convex max – min time allocation problem is first reformulated into a series of geometric programming, and then, a single-condensation method based iterative algorithm is proposed. Numerical results are also provided to validate the performance of the proposed key generation algorithms and the time allocation algorithm.

I. INTRODUCTION

In contrast to the channel model based techniques, recently the source model based PHY security approach has received a considerable attention, where correlative source observations between legitimate users are exploited to generate common randomness and information-theoretically secure symmetric keys. The works in aimed to find information theoretic secrecy key capacities in a variety of source models, however, they have not provided methods to obtain the source observations. Due to channel reciprocity in time-division duplex (TDD) systems, the correlative observations can be obtained via estimates of the wireless fading channels between the legitimate users, which demonstrate the advantages of the source model based key generation approach to support secure multimedia service. Along this direction, many works have investigated this channel reciprocity based key generation problem In addition, it is exploited the fact that the eavesdropper channels are independent from channels between the legitimate users as long as the eavesdroppers are half wave length away from the legitimate users, which is a general case in wireless networks The key generation problem between a group of terminals is more challenging due to the different random channels associated with these terminals. The information-theoretic secret key capacity for the group key generation in the multi-terminal source model was first provided in Since then, several tree-based algorithms have been developed to achieve the group secret key capacity for the multi-terminal pair wise independent network .

II.PROBLEM DESCRIPTION

2.1 EXISTING SYSTEM

Several pair wise key generation technique has been developed to achieve the group secret key capacity for the multi-terminal pair wise independent network. An algorithm was more practical for real systems at the expense of some scarification in the group key rate. Specifically a tree based group key algorithm divide each pair wise key into multiple one-bit segments. Then, in order to propagate these one-bit segments, the nodes adopt a transmission scheduler via repeatedly finding spanning trees in the corresponding multi graphs.An optimization problem dot not solve in pair-wise key based generation algorithm.

DISADVANTAGES

- Performance is not validating.
- Cannot prevent group key rate.
- Only generate pair-wise independent keys.

2.2 PROPOSED SYSTEM

A new group key generation algorithms for three types of wireless topologies, namely, the three-node network, the multi-node ring network, the multi-node mesh network.Firstly, A proposed scheme is demonstrated using a simple three-node wireless network, where three legitimate nodes wish to agree on a common group key without revealing this key to an external eavesdropper.The proposed key generation protocol is extended to the mesh wireless network, where a wireless link exists between every two nodes. To realize optimal or order-optimal group key rates, the propose key generation strategy is based on the careful combination of the well established point-to-point pair wise key generation technique, the Multi-segment and one-time pad.The propose algorithms not only design the segment-pairing scheme to perform the one-time pad, but also analyze the optimal rate allocated for each segment. A group key generation algorithm only divide each pair wise key into a small number of segments with optimal rate allocation, such that only a simple round-robin scheduler is adopted by the nods to transmit one-time pads of these segments in the group key agreement. To solve the key rate optimization problem with respect to optimal time allocation for these three type of networks, which is non-trivial due to the non-convex characteristic.

ADVANTAGE

- Low complexity.
- High authenticates transferring data.
- Highly Secured

III. MODULE DESCRIPTION

1. Authentication Server Module
2. Player Initialization Module
3. Group Formation Module
4. Key Generation Module
5. Cryptography Module

3.1 AUTHENTICATION SERVER MODULE:

An authentication server is an application that facilitates authentication of an entity that attempts to access a network. Such an entity may be a user or another server. An authentication server can reside in a dedicated computer, an Ethernet switch, an access point or a network access server.

3.2 PLAYER INITIALIZATION MODULE:

In the Player initialization process, the player is used to initialize there ID, Port number and there IP Address. By initialize there details they can form the group, without initialize they cannot form the group.

3.3 GROUP FORMATION MODULE:

In the Group formation, the no of player will be create an object and each player will share their object to the no of player in the in round1. In which we can view the alive players in round1.

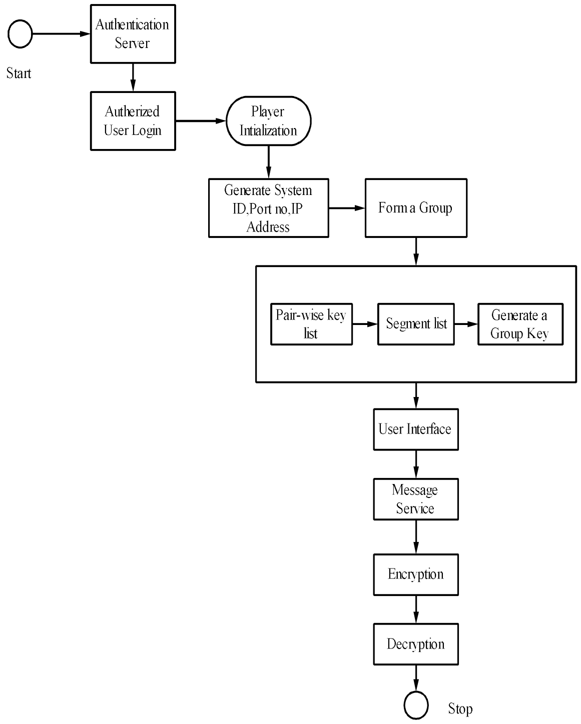
3.4 KEY GENERATION MODULE:

The common secret key for a group of users can be generated based on the channel of each pair of users. A two segment key generation algorithm is used to generate a common secret key for secured communication.

3.5 CRYPTOGRAPHY MODULE:

In message service process with the help of the session key, the group member can share the data. With the help of encryption engine will send in the encrypt format. At the receiver share the secret key help of decryption engine will receive in the decrypt format.

IV.SYSTEM ARCHITECTURE:



V.CONCLUSION

A new key generation strategy with low-complexity has been proposed for different types of wireless networks, which is based on the careful combination of well established point-to-point pair wise key generation technique, the multi-segment scheme, and the one-time pad.Each pair wise key is divided into two segments for the three-node network, whereas each pair wise key is divided into $M - 1$ segments for the M-node ring network.Both of these algorithms are optimal in terms of the achieved group key rates. Moreover, the proposed two-segment based algorithm for the three-node scenario has been extended to the M-node mesh wireless network and shown to achieve the optimal multiplexing gain $M/2$. Next, the optimal time allocation problems have been solved for some cases where the original non-convex max-min problem is reformulated into a series of geometric programming and an iterative algorithm has been developed by exploiting single condensation method.

FUTURE ENHANCEMENT

The proposed protocol provides authentication of the participants using segments with Public Key Infrastructure, which may be difficult in certain environments. It may be possible to provide authentication using different number of segment values is integrated signature scheme for group key agreement, with overall reduced computational and communicational loads. Also such security issues as, perfect forward secrecy, replay attack, forgery attack, key compromise impersonation, key control, etc. are yet to be studied for the proposed protocol

ACKNOWLEDGEMENT

The author deeply indebted to honorable First and foremost I bow my heads to almighty for blessing me to complete my project work successfully by overcoming all hurdles. I express my immense gratitude to correspondent SHRI A.SRINIVASAN. vice chairman SHRI A.SRINIVASAN(Founder chairman),SHRI P.NEELRAJ(Secreatry) Dhanalakshmi Srinivasan Group of institutions, perambalur for giving me opportunity to work and avail the facilities of the college campus. The author heartfelt and sincere thanks to principalDr. ARUNADINAKARAN, Vice Principal prof. S.H.AFROZE, HoD Mrs. V.VANEESWARI,(Dept.of CS& IT) Project Guide Ms.A.KIRUTHIKA,(Dept of CS &IT) of dhanalakshmi Srinivasan College of Arts & Science for women, Perambalur. The author also thanks to Parents, Family Members, Friends, Relatives for their support , freedom and motivation

REFERENCES

1. **Microsoft C#.NET Programmer's book** (Tata McGraw Hill Edition) 2002 -CHRIS GOODE, JOHN KAUFFMAN
2. C#.Net 2.0 for everyday Apps by Doug Lowe in Wiley Publishing Inc.,
3. **Programming C# : Building .NET Applications with C#** Jesse Liberty (O'Reilly)

4. "**Microsoft SQL Server 2000 Programming**" by Example Copyright © 2001 by Que Corporation, Fernando G. Guerrero and Carlos Eduardo Rojas.
5. **"SQL: The Complete Reference"** by James R. Groff and Paul N. Weinberg, Osborne/McGraw-Hill © 1999.
6. "**Professional ADO.NET Programming**" by BipinJoshi, Paul Dickinson,Fabio Claudo Ferracchiati, Wrox.Press.

BIOGRAPHICAL NOTES

Ms.REKHA.V*is presently pursuing ComputerScienceM.Sc.,Final year the Department of Science From Dhanalakshmi Srinivasan College of Arts and Science for Women, Perambalur, Tamil Nadu ,India*

A - *Received M.C.A., M.Phil Science. She is currently working asAssistant Professor in Department of Computer Science in DhanalakshmiSrinivasan College of Arts and Science for Women, Perambalur Tamil Nadu, India.She has Published papers in IJSTM & IJIRCCE journals and also Published two books Namely " Computer Basics and Internet " and "Introduction to Languages C,C++,Java" Her research areas are Networking,Web Technology and Cloud Computing. DhanalakshmiSrinivasan College of Arts and Science for Women,Perambalur, Tamil nadu, India.*

Ms.KAVINILA*is presently pursuing ComputerScienceM.Sc.,Final year the Department of Science From Dhanalakshmi Srinivasan College of Arts and Science for Women, Perambalur, Tamil Nadu ,India*