International Journal of MC Square Scientific Research Vol.9, No.1 April 2017

GROUP SECRET KEY GENERATION FOR WIRELESS NETWORK

Rahul Kumar [1], Aman Sharan [2], Vikash Kumar [3], Swapnil Shah [4]
[1, 2, 3, 4] *UG student,*
Department of Computer Science Engineering,
SRM University, Ramapuram, Chennai – 89.
[1]priteshkumar882@gmail.com, [2]ppiyush673@gmail.com,
[3]vipulkumar45@gmail.com, [4]swapnilshah06@gmail.com

Jaya Kumar [5]
[5] *Assistant Professor,*
Department of Computer Science Engineering,
SRM University, Ramapuram, Chennai – 89.

Abstract— This paper by exploiting physical layer characteristics of wireless channel investigates group secret key generation problem for different types of wireless network. A new group key generation strategy with low complexity is proposed, which combines point to point pair-wise key generation technique, the multi-segment scheme and the onetime pad. This group key generation technique works for three types of communication networks: the three node network, the multi node ring and multi node mesh network. For these communication networks three group key generation algorithms are developed, the first two algorithms yield optimal group key rates while the third algorithm gives the optimal multiplexing gain. We address the time allocation problem in the channel estimation step to maximize the group key rate. A series of geometric programming, and a single condensation method based iterative algorithm is proposed in order to solve the non-convex max min problem. To validate the performance of the proposed key generation algorithm and the time allocation problem the numerical results are also been provided.

Keywords— Physical layer, wireless channel, group key generation, multi segment scheme, Onetime pad.

1. Introduction

In 2010, a survey conducted by Microsoft company proved that there were lot of privacy concerns when it comes to data and query. Recently secret key generation technique came into attention to everyone when the matter of security came into the picture where it is being assumed that the size of the message cannot exceed the key and thus one time pad has been introduced in order to increase the security. In this it is being assumed that the eavesdropper won't be able to get through the secrecy of the message even if he has the unlimited computational power. Firstly the PHY based approach was introduced by Wyner to

realize the information theoretically secured communication in a wiretap channel, where the secrecy capacity was characterized as the difference between the mutual information of the main channel and the eavesdropper channel. In the literature such kind of model is known as the channel model. In recent years number of channel model studied was more as the main target was to have the secrecy and the integrity of the messages intact without the use of the secret keys.

The channel model based approach was not as efficient than the other approach has been implemented that is PHY security based approach in this correlative source observation between legitimate user is been exploited to generate common randomness and thus the information are being secured using the symmetric keys. Source model based key generation technique is a better approach and it can be said as due to channel reciprocity in time division duplex(TDD) system the correlative observation between the legitimate user can be obtained by the wireless fading channel. In wireless network it is assumed that the eavesdropper channel are independent from the legitimate user channel if the eavesdropper is half wavelength away from the legitimate user. In a System where there is group of terminals it is difficult to generate the key as due to the randomness between the channels. Since then there has been many tree based algorithm which has been developed to reduce the difficulty to generate the keys in the system where there is group of terminals with pair wise independent network (PIN). For the wireless networks several effective algorithms has been developed in order to reduce the complexity by examining the channel characteristics.

Difference between the proposed system and existing system:.

1. The existing system is less challenging than the proposed system as the existing system gives less preference in the key agreement process and it does not give consideration to the multi-segment scheme for each pair wise key, while the proposed system not only give preference in the key agreement process it also design the segment pairing scheme to perform the one time pad and also analyse the optimal rate allocated for each segment.
2. Existing system was basically based upon the tree based algorithm which has less efficiency and high complexity. But the proposed system has high efficiency and less complexity in the secret key generation process.
3. The tree based algorithm which was used in the existing system use to divide each pair-wise key into multiple one bit segments. Then in order to propagate that one bit segment, the nodes adopt a transmission scheduler by repeatedly finding spanning tree in the corresponding path in which the transmission was required to be done. Whereas in the proposed system the algorithms only divide each pair wise key into multiple one bit segments with optimal rate allocation, and thus it requires single round robin scheduler is required to transmit one time pad by the nodes in order to generate the secret key.

2. Literature Survey

For any secure communication system key management is an important part. The crypto system relies on some secure, robust and efficient key management system. The thesis in the particular document talks about some of the proposed algorithms and the document about the key generation technique in the ad-hoc wireless system. The usage of the ad-hoc system has increased drastically among the few years. So the ad-hoc system has an issue or one can say the security issue that is MANETs. Several researches have been done in order to find the security issues with the MANETs.

1. Maghmoumi et al Key Management Scheme generated his algorithm for the ad-hoc wireless system using the cluster based scalable key. A new clustering technique has been used in this algorithm. The affinity relationship among the nodes has been given the priority in order to partition the nodes into communities and the clusters. The protocol responded well to the hurdles such as nodes mobile battery power and the network switching, thus the protocol provided the secure system for the information transfer among the nodes in the ad-hoc system.

2. Nen-Chung Wang and Shian-Zang Fang Key Management Scheme, A key management protocol for the secure group management for the ad-hoc wireless communication channel has been proposed. For the secure group communication in MANETs hierarchical key management scheme was described, in this in order to make the security more efficient a packet was encrypted two times. The group maintenance was also been done in order to facilitate the change in the topology of the MANET. Finally the author compared the other scheme which has been proposed earlier with this new scheme and found that this scheme had a better result in the group communication in MANETs.

3. George et al. Key Management Scheme, he introduced a framework which provided key redundancy and robustness for SA establishment between pair of nodes in MANETs. A trust public key hierarchical model was introduced which was a framework which was used in which nodes could dynamically assume management roles. In this the author assumed that the users can leave and join at any time at their wish. In this every particular node has the power of generating own cryptography key and was powerful enough of securing own system. The system in this particular framework has been different from others as they used two concepts in it i.e., non-repudiation and behavior grading. This framework enjoyed additional feature of grading by combining the features of KMS with additional element node behavior. This scheme has the advantage of calculating the security efficiency of other nodes.

4. Rony Rahman and Lutfar Rahman Key Management Scheme, A new GKM protocol was put further by Rony Rahman and Lutfar Rahman for ad-hoc wireless network. They introduced a new protocol which was based on multi-party DH group key exchange and which was also password authenticated. The basic idea of the project or protocol was to securely create a key and a group session and to distribute the key for that particular session among the group in a secure manner. In this a spanning tree is being created by adding all the nodes in it. In this one thing is

kept in mind that each node was distinctly addressed and each and every node has the idea of their neighbor node. The password is being shared among all the valid member of the group. The password helped to provide the authorized user the access to the system and it also prevented attacks like man in the middle attack. There was the protocol which was different from other protocols as they did not need broadcast or multicast capabilities.

5. Jason et. al Key Management Scheme, They introduced a new scheme which was based on clustering nodes and scalable key management for secure group communication in the ad-hoc network. The scalability issue in the system is being corrected by dividing the group in subgroup and then each subgroup has a leader and also by dividing the subgroup in hierarchies. Each layer of the system was also known as the tier of the system. The system was highly efficient, scalable and ensures high security.

3. Existing Method

The existing system was mainly for the point to point modulated system, in which the system was mainly focused on the single user encryption key in which the user will have to connect with the group every time in order to get the key. The existing system has an algorithm in which the user will have to register every time he or she wish to connect with the group, thus the algorithm was not efficient, if the number of user was more than the desired number of user then the algorithm responded abruptly , i.e., the algorithm has the upper limit for the user. The time and space complexity of the algorithm was not the desired one,

Problems in the existing system:-

1. The algorithm was not the efficient algorithm.
2. The algorithm has an upper limit for the user.
3. The algorithm was not applicable for the real system.
4. The algorithm only supported the system for single node.
5. The algorithm which was used to generate the key had issues as it worked upon the terminals and they had different random channels.

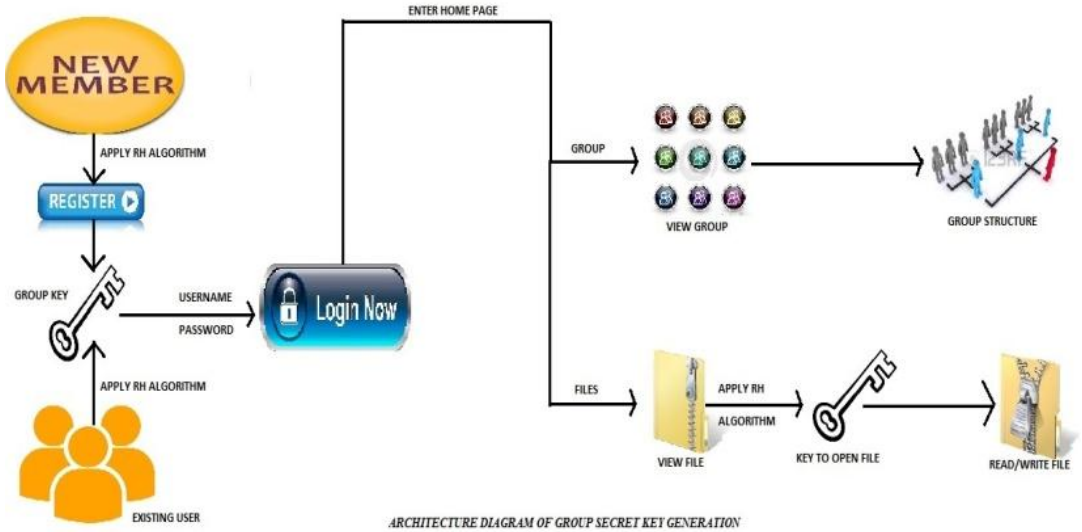
The problem arose mainly in the key generation scenario where the algorithm worked upon the terminals, these terminals were treated as nodes and in this every node is independent of the other nodes i.e., there is no connection between the neighbour nodes. Since the algorithm worked upon the terminals and every terminals has the random channel which changes so the algorithm failed in many instances. The group authority had an issue in managing the group members as the number of member in the group was based upon the terminals and the terminals was based upon the random channels which used to generate the keys based upon the random channel value so the key was different which was difficult to manage and was easy for the eavesdropper to get into so the random channel notion was important to be replaced. The algorithm failed to respond to the real system implementation, i.e., the algorithm was too complex to be implemented for the real system as it has to work through many channels and the complexity of the algorithm was not suited for it. The algorithm also had the upper limit for the number of users in the group, so if the

value of n where n is the number of user increased the substantial value then the algorithm use to behave in an absurd manner. Also the time and space complexity was more and was not suited for the real time system and thus the algorithm demanded more number of users and there was a limitation over the number of user. The key generation algorithm in the existing system is more challenging. The existing system which uses the tree based algorithm to increase its efficiency failed as the proposed system algorithm has greater advantages and it was also applicable for the real system and it was less complex also.

4. Proposed Method

The proposed system was designed mainly keeping the disadvantages in the existing system; the existing system used the tree based algorithm which was not efficient. The proposed system worked for multi node segment, multi ring segment and the one time pad. The new algorithm works on the three types of network topologies, three node networks, the multi node ring network and the multi node mesh network. Firstly the proposed system is demonstrated using a simple three node wireless network where all the three nodes accept to agree on a particular key without revealing the key to an external eavesdropper. Secondly, a more complicated ring network is being created where the wireless nodes i.e, m nodes are arranged in a ring where m>=3. In the wireless mesh network, where a wireless link exist between every two nodes. i) Three-Node Network: In this every pair wise key is divided into two segments, and then use them to generate the three-way group key. ii)Multi-Node Ring Network : A multi node ring network generation algorithm is proposed for a ring network where a key is divided into M-1 nodes. iii)Multi-Node Mesh Network : In this the two segment based algorithm for the three node mesh network is transformed into mesh network with m legitimate nodes, where each pair wise key is divided into two segment for generating group secret keys.

ARCHITECTURE DIAGRAM:



ARCHITECTURE DIAGRAM OF GROUP SECRET KEY GENERATION

The architecture diagrams initially works in two modules, in the first module, the new user objective is being shown, in the new user module the user will have to register, in order to register the user will have to fill some details then the user will hit on register button then a key is being generated, the key is being generated by using the R-H algorithm. In the second module the existing user exist in this module, in this module the user is already registered only the R-H algorithm works in order to generate the key. Then the algorithm works commonly for both the module as the user will have to provide their credentials in order to login into the system, if the username and the password provided by the user is correct then the user will allow to get into the home page of the system, where the user will get access to two modules:- 1.GROUP MODULE 2.FILES MODULE.

In the group module the can view group and the user can view the group only by getting the permission from the group authority to get into the member of the group. A user can only become the member of the group if the group user selects to get in is being accepted by the group authority and the valid key is being generated by the group authority. The user in this module can view the members in the group and has the authority of checking up the group structure. In the files module the user once getting into a group can view the files available in the group but won't be able to access the files. To access the files the user need to have the proper authority over the file and they need to get the permission from the group authority, the group authority provides with the permission by generating a key which is being generated by using the R-H algorithm. Once the key is generated for the user the user becomes the authorised user and can access the file and can also alter the content of the file.

Algorithm

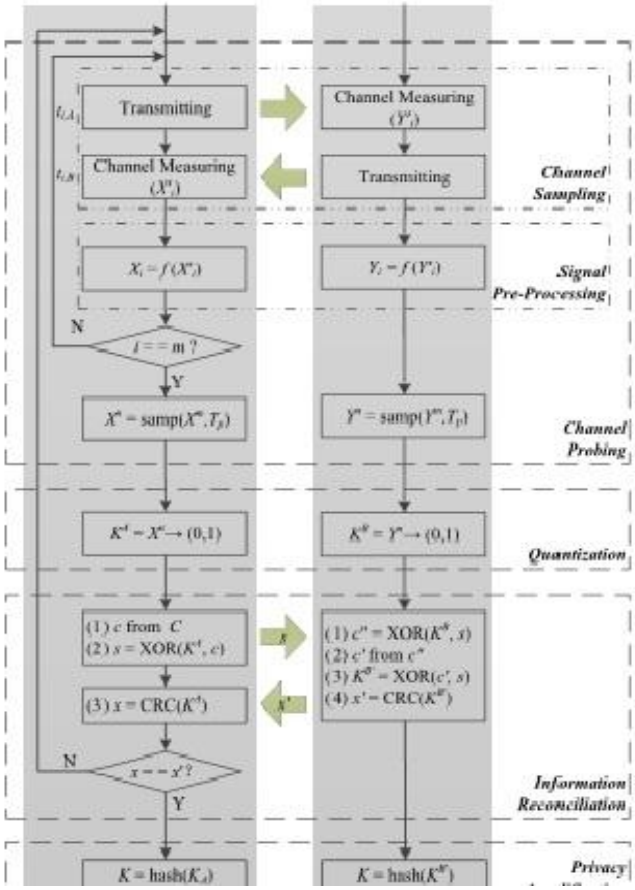
1. Key Generation: The key generation process can be divided into the four steps i.e. channel probing, quantization, information reconciliation and privacy amplification.

Channel probing - In this two user try to measure the randomness in the channel by checking the common channel in the received signals and thus the channel probing rate is calculated. In this threshold is being calculated using the formulae:

$$n+= u + a * sigma.$$

$$n-=u + a * sigma.$$

Quantization - The quantization method is being used to map the analog channel measurement into the binary value. There is always some disturbance in the received signals between the two user and it is being corrected by signal to noise ratio (SNR) of the channel. The key disagreement issue can also occur while the key is being shared among the two users to reduce that gray code is being used.



Algorithm 1 CDF-Based Quantization Algorithm

1: $F(x) = \Pr(X^n < x)$
2: $\eta_i = F^{-1}(\frac{i}{2^{QL}}), i = 1, 2, ..., 2^{QL} - 1$
3: $\eta_0 = -\infty$
4: $\eta_{2^{QL}} = \infty$
5: Construct Gray code b_i and assign them to different intervals $[\eta_{i-1}, \eta_i]$
6: $K(j, QL) = b_i$, if $\eta_{i-1} \leq X_j < \eta_i$

Information Reconciliation - The cross correlation while transferring the message between the two user can be corrected by using the algorithms, there still can be disagreement to accept the key between the two user. The disagreement in the acceptance of the key can be corrected by information reconciliation technique which can be done with the help of the protocols such as cascade or error correcting code. There is another protocol which is more efficient than the other two protocols i.e. ECC based reconciliation scheme, in this protocol selection of the ECC depends on the complexity and the correction capacity. The disadvantage of the ECC based system as they were more complex and also leak more information.

$$\text{CORRECTION RATE} = \frac{tmax}{n} = \frac{2^{m-2}-1}{2^{m}-1}$$

This approaches 0.25, when m becomes too large. Privacy Amplification: Privacy amplification and the information reconciliation always come together, which requires a cross design between these two stages. When the message is being transferred during the information reconciliation some message is being reveled to the eavesdropper to correct that Privacy Amplification is being done.

2. Key Exchange Algorithm: The algorithm used is the Diffie-Hellman algorithm which is being used for the key exchange purpose. Let us assume you have two user Alice and Bob. Steps in the given algorithm –

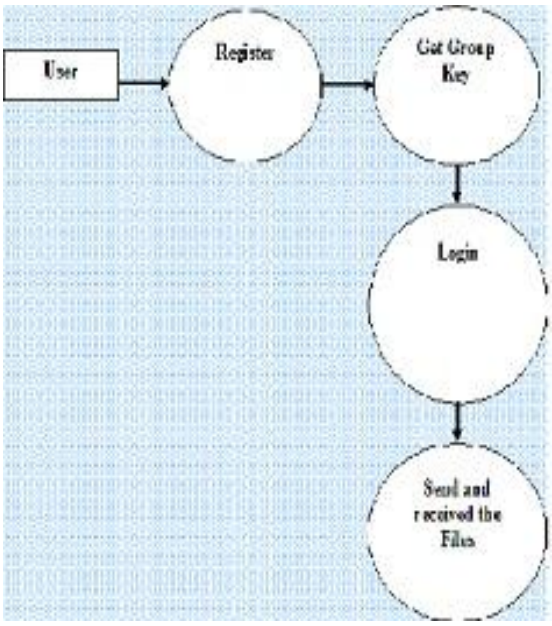
1.Select two prime numbers g and p, 2.Select a secret number for Alice (a) and compute (g^a mod p) and the result which is a public key is being returned to the group authority as (A). 3. Select another secret number for Bob (b) and compute (g^b mod p) and the result which is a public key is being returned to the group authority as (B). 4.Now calculate the private key for Alice to do that take the public key of Bob that is (B) and take the secret number of Alice which is a and calculate its private key. A'=(B^a mod p) where A' is the private key of Alice. 5. Now calculate the private key for Bob to do that take the public key of Alice that is (A) and take the secret number of Bob which is b and calculate its private key. B'=(A^b mod p) where B' is the private key of Bob.

Thus the algorithm works in such a manner that the value obtained at the step 4 is almost similar to the value obtained at the step 5. It is the module property of maths where, (B^a mod p) = = (A^b mod p). Thus the key generated is being obtained by both the user that is the sender and the receiver which is being obtained by the group authority member.

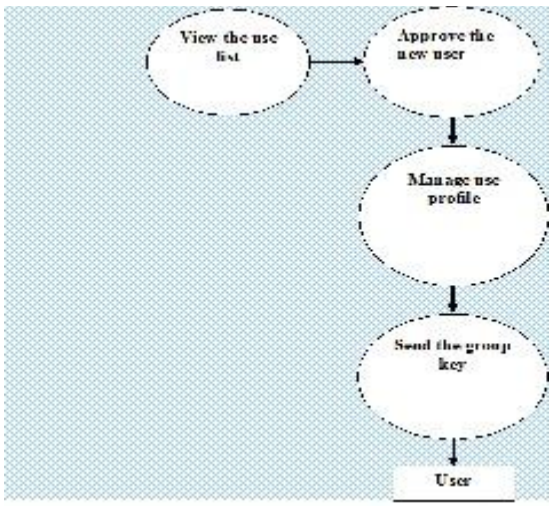
5. Experimental Results and Diagrams

Data Flow Diagram:

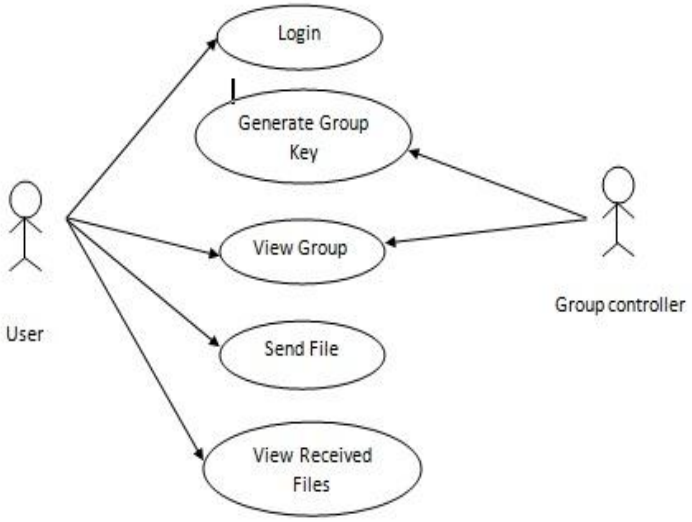
1. User



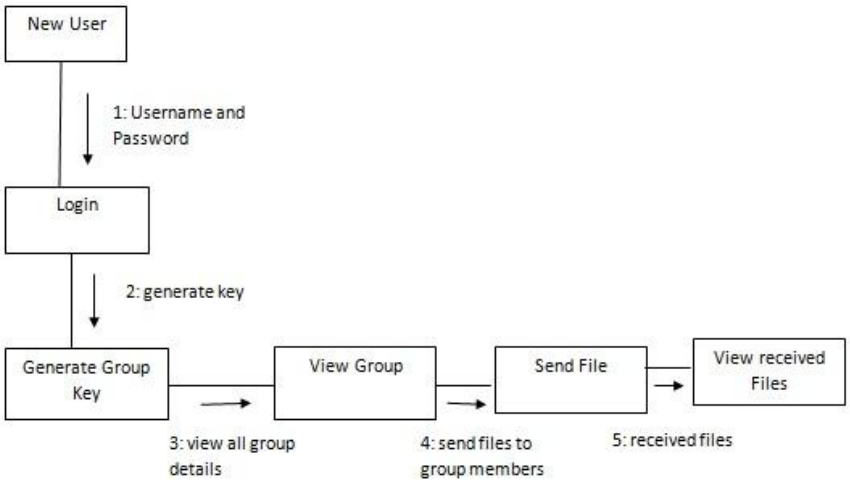
2. Group Controller



Use Case Diagram:

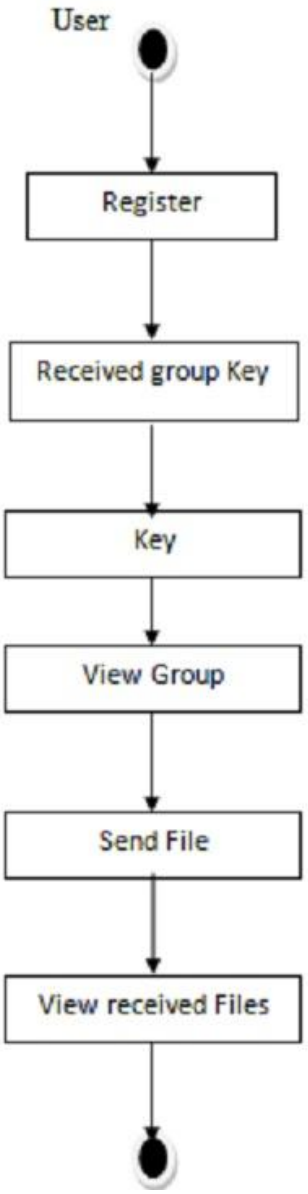


Collaboration Diagram

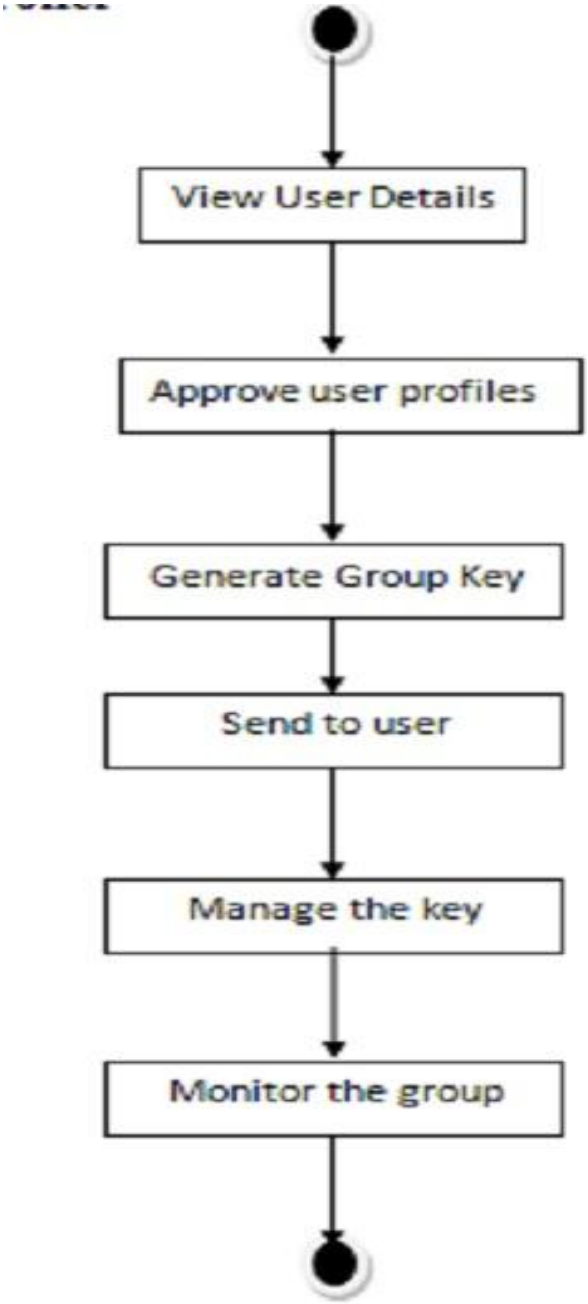


Flow Diagram:

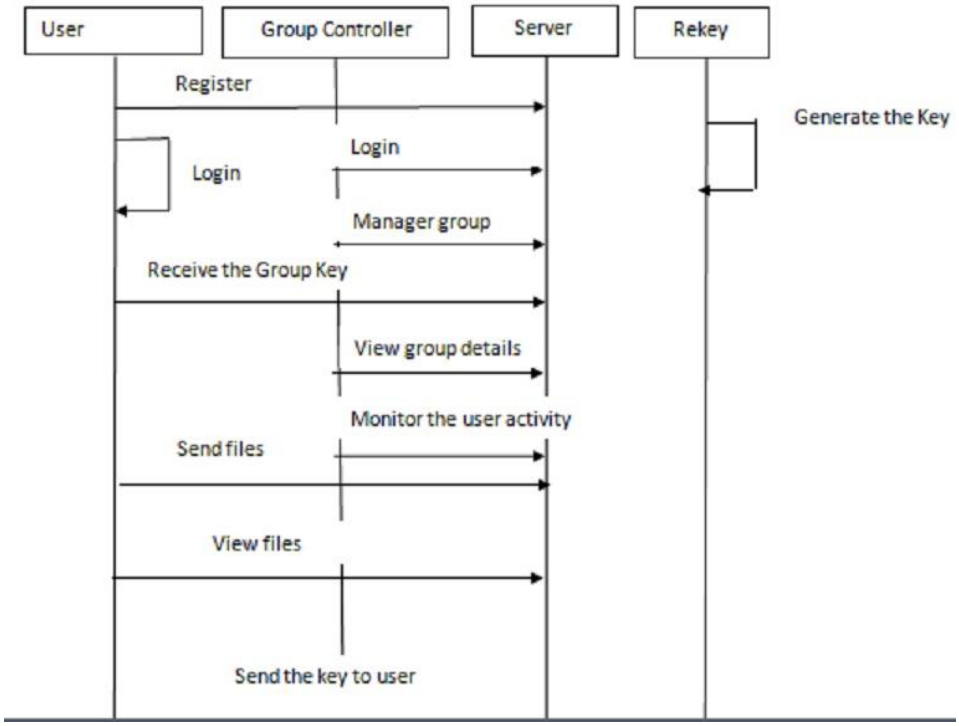
1. USER



2. GROUP CONTROLLER



Sequence Diagram:



6. Conclusion

For different types of wireless networks such as multi node network, multi node ring network and mesh network a new key generation strategy with low complexity and more security has been proposed and it is basically based upon the careful combination of well-established point to point pair wise key generation technique, the onetime pad and the multi segment scheme. In the algorithm every node is being divided into two segments for the three node network, whereas each pair wise key is divided into N-1 segments for the N node ring network. The group key rates are optimal for both the algorithms been proposed. The three node scenario proposed two node segment algorithm has been extended to the N- node mesh wireless network and the optimal multiplexing gain i.e., N/2 is being obtained. The original max min problem has been formulated into series of geometric programming and an iterative algorithm in the step by step sequence has been generated by obtaining the single condensation method to obtain the best result for the algorithm so that the algorithm can work for real system and also with the best results.

References

[1] C.Shannon, "Commuication theory of secrecy systems." Bell System Technical Journal, vol-28, no 4,pp 656-715,1949.

[2] A.Wyner, "The wire-tap channel," Bell System Technical Journal, vol,54, no.8 pp 1355-1387, Jan 1975.

[3] Y.Liang,H.V.Poor, and S.Shamai, "Secure communication over fading channel," IEEE Transactions on Information theory , vol 54,no.6, pp. 2470-2492,2008.

[4] P.K.Gopala,L.Lai, abd H. EL Gamal,"On the secrecy capacity of fading channels." IEEE Transactions on Information Theory, vol.54, no.10,pp 4687-4698,2008.

[5] P.Xu,Z.Ding,X. Dai, and K. Leung, " A general framework of wiretap channel with helping interference and state information "IEEE Transactions on Information Forensics and Security, vol,9,no.2, pp. 182-195, Feb 2014.

[6] D. Tse and P.Viswanath, Fundamentals of wireless communication Cambridge university press 2005.