International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 5, Issue 01, January-2019

A Secure Protocol for Wireless ADHOC Network Creation

Roohi Jannat [1], Afroze Ansari[2]

[1]*M.Tech Student, Computer Science Department, KBN College of engineering Gulbarga 585104, Karnataka, India*
[2]*Assistant Professor, Computer Science Department, KBN College of engineering Gulbarga 585104, Karnataka, India*

Abstract— In this modern era when the number of users are increasing day by day there is more likelihood the data may be encrypted, stolen by third party user. Hence there is a need to develop a network which is secure enough to transfer personal information through it. In the present paper an attempt is being made to develop a Adhoc wireless network which is secure and trustable. Java language is used in the present paper to develop an ADHOC Ntework

Keywords: Secure protocol, Spontaneous Network, Adhoc network, Symmetric/asymmetric key, Encryption, Authentication.

I. INTRODUCTION

The present paper focuses on creation of ADHOC Network creation by using java language and UML language for coding and decoding. Although there are number of network creation available today ADHOC network is considered to be the safest and easiest network for transmission. The current framework has the combination of gadgets & administrations in a similar domain, enabling the client to avoid outer framework and to earn moment benefit. Moreover, security is provided and participation among the nodes is also ensured. All nodes will most likely be unable to give security conventions.

In the present system IDC Manager is used and three group leaders are assigned . Each group leader has two nodes to which different session keys are assigned. Apart from this source and remote user are also essential components of the present system. Netbeans software is used for analytic interpretation of results. The system focuses on creation of ADHOC network securely and the data of the user is saved by using secure unique IP address

II. LITERATURE REVIEW

Latvakoski et al. [15], present a defense for a correspondence structure idea for unconstrained frameworks, mix application-level unconstrained bunch correspondence, and specially appointed systems administration along. a gathering of approaches to adjust fitting and play, tending to and quality, associate to look availability, and furthermore the utilization of administrations additionally are given.

Liu et al. [16] appear anyway arranged hubs will self-rulingly bolster and get together with each other amid a distributed (P2P) way to rapidly find and self-design any administrations available on the zone and convey an ongoing capacity independent from anyone else sorting out themselves in unconstrained gatherings to supply higher adaptability and flexibility for catastrophe recognition and alleviation.

Gallo et al. [17] sought after 2 focuses in unconstrained systems: to boost responsiveness given a few imperatives on the vitality esteem and to constrict the vitality esteem given bound necessities on the responsiveness.

Nadjm-Tehrani [18] built up the essential genuine unconstrained system that gives benefits progressively utilizing the Jini innovation. They put forth a defense for the field of study plan of the contact administration and its usage. The model shows anyway significant standard, adaptability, reliability, productivity, and straightforwardness, influence the structure and administrations of a dynamic system of gadgets.

In [19], Untz et al. propose a light-weight and conservative interconnection convention fitting for unconstrained edge systems. They style and actualize Lilith, a picture of partner degree interconnection hub for unconstrained edge systems. It utilizes MPLS and allows very surprising correspondence routes on a for every stream premise, gives consistent change among operational and back-up ways, and makes available data on goal reachability

III.SYSTEM ARCHITECTURE

To accomplish the objective we will begin by creating an adhoc network spontaneously on request by a user. From that point we will take a gander at past research on the subject of securing networks deciding the best in class methods and strategies.

With the learning from past research and our own examinations we will think of an appropriate design for the framework taken after by executing a model able to secure the data transmissions though adhoc network and finally work towards making the system more efficient and secure.

We start by creating an IDC which holds all the users data securely and is responsible to authorizing the users to connect to an Adhoc network. .We simulate 3 different Adhoc networks each bearing two nodes in it. A Source node can join an Adhoc network amongst the before mentioned 3 network, send data to IDC for secure storage and the destination nodes can join the senders Adhoc network to search and download the file sent by the sender.

Each Adhoc network is secured by generating unique keys. Only the destination who are authorized and use these keys can join the network instantly and can access the data stored in IDC.We have also taken care of members from different Adhoc networks trying to access the file sent from sender of some other Adhoc network. Only members of a particular Adhoc network are allowed to search the files within that network and the IDC will let them know the user who transferred the file to it. The destination node can then download the file securely

IV. EXPERIMENTAL METHODOLOGY

The entire work can be depicted as shown in Fig 1

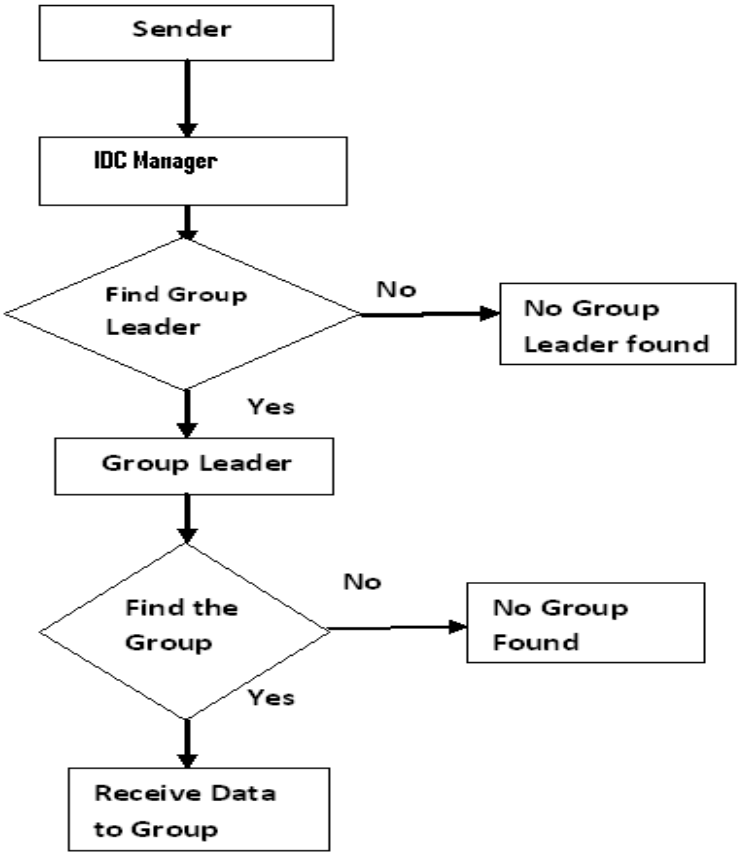


Fig 1 : Activity Diagram

V. EXPERIMENTAL RESULTS

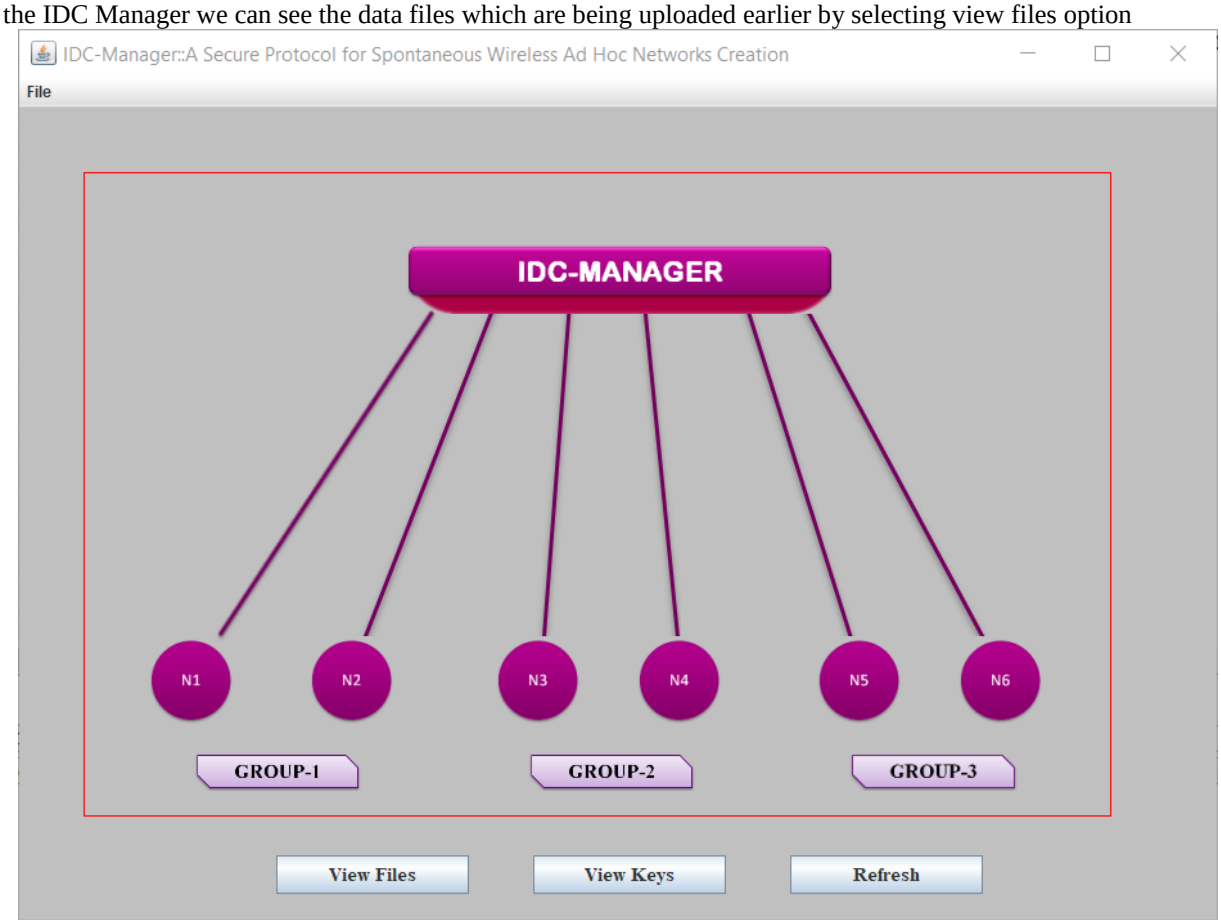
The data base which is stored in a secured folder consists of three groups namely key table, network nodes and storage which are being simulated in wifi network spontaneously. The key table consists of secret session keys which can be assigned to different nodes and can also be changed later on depending upon the security criteria.

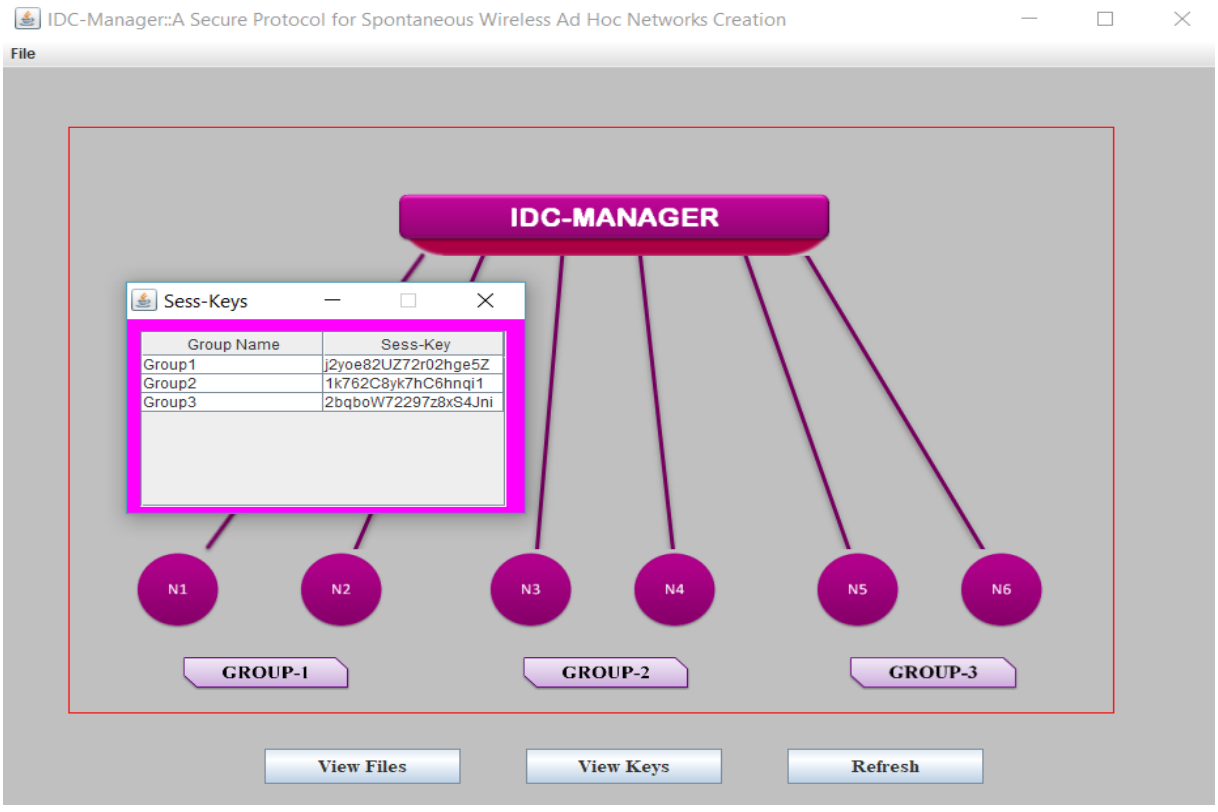
The network nodes gives the details of different nodes N1,N2,N3,N4,N5 and N6 assigned to different Group leader 1,2 and 3. The history of data saved or uploaded with date and time can also be tracked from the storage folder.

For running the application we need this services to be started namely XAMP Control Panel and NetBeans IDE. In NetBeans we need to select project than in source package select default package in which three files are needed to be run namely IDC Manager, Remote User and Source.

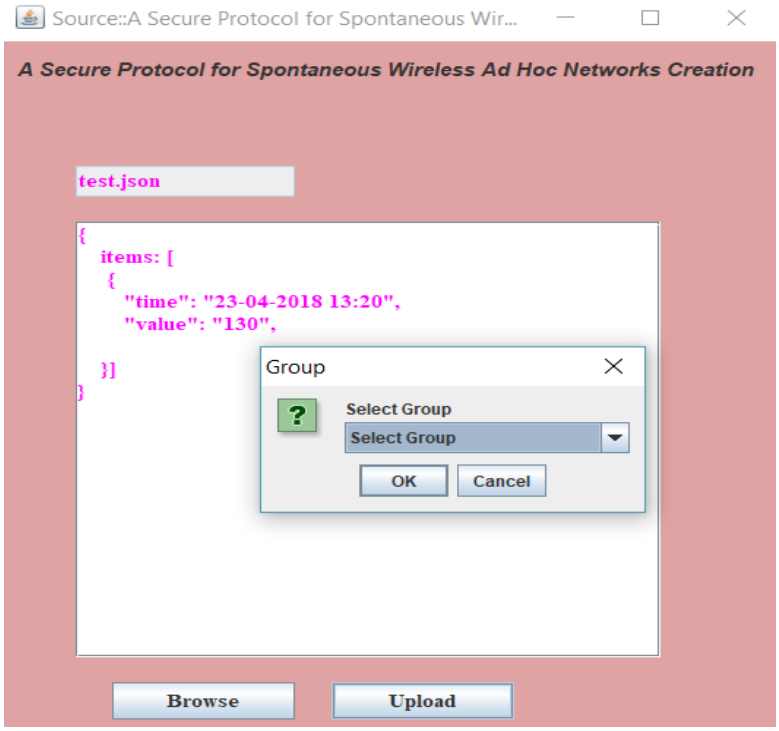
IDC MANAGER: is the central Internal Data Centre in which a single WiFi Network is spontaneously break in three groups namely Group 1,Group 2 and Group 3. In each group two nodes are present such as N1 and N2 in Group 1, N3 and N4 in Group 2 , N5 and N6 in Group 3. If for example data is uploaded in N1 node in group 1 than it cannot be access by Group 2 and Group 3 similarly if data is present in Group 3 than it cannot be access by the nodes present in Group 1and 2.

In the IDC Manager we can see the data files which are being uploaded earlier by selecting view files option

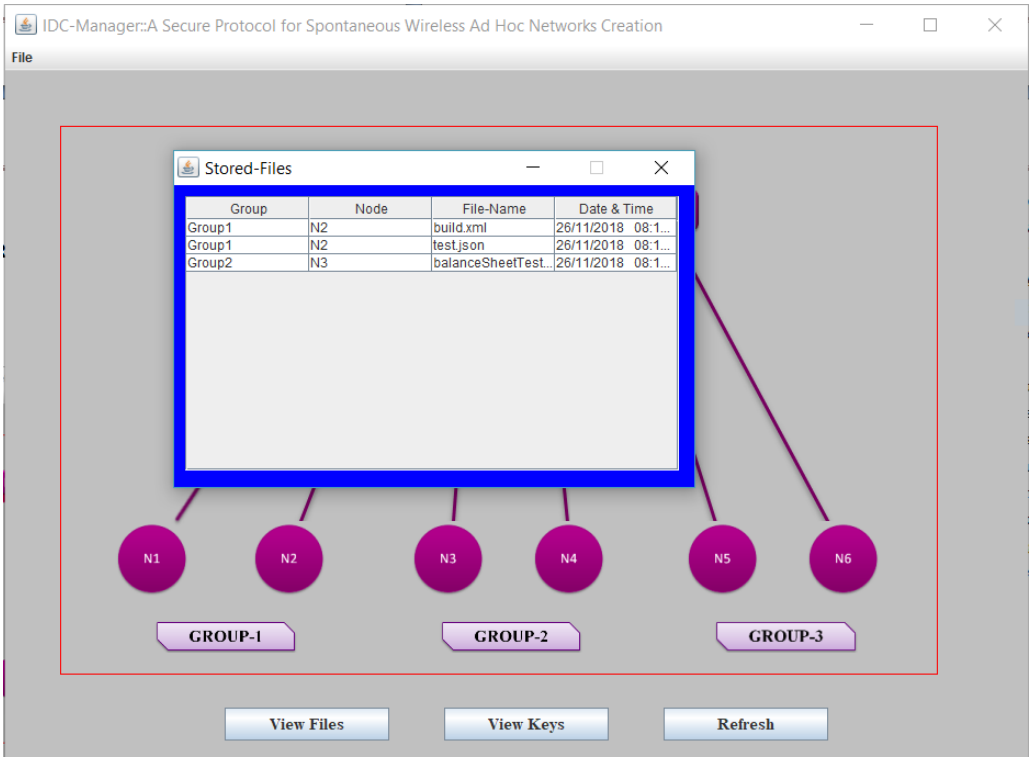




Further by selecting the View Keys option we can see the secrete keys allotted to individual nodes and can also update the keys and assign new keys depending upon the security needs in update keys option. We can also view the AdHoc network connections established between different nodes in View AdHoc network window.
Next step is to upload a file for which the following procedure is followed
Run Source : Browse and upload a file -> select a group and a node within that group to save the file to depending upon our choice



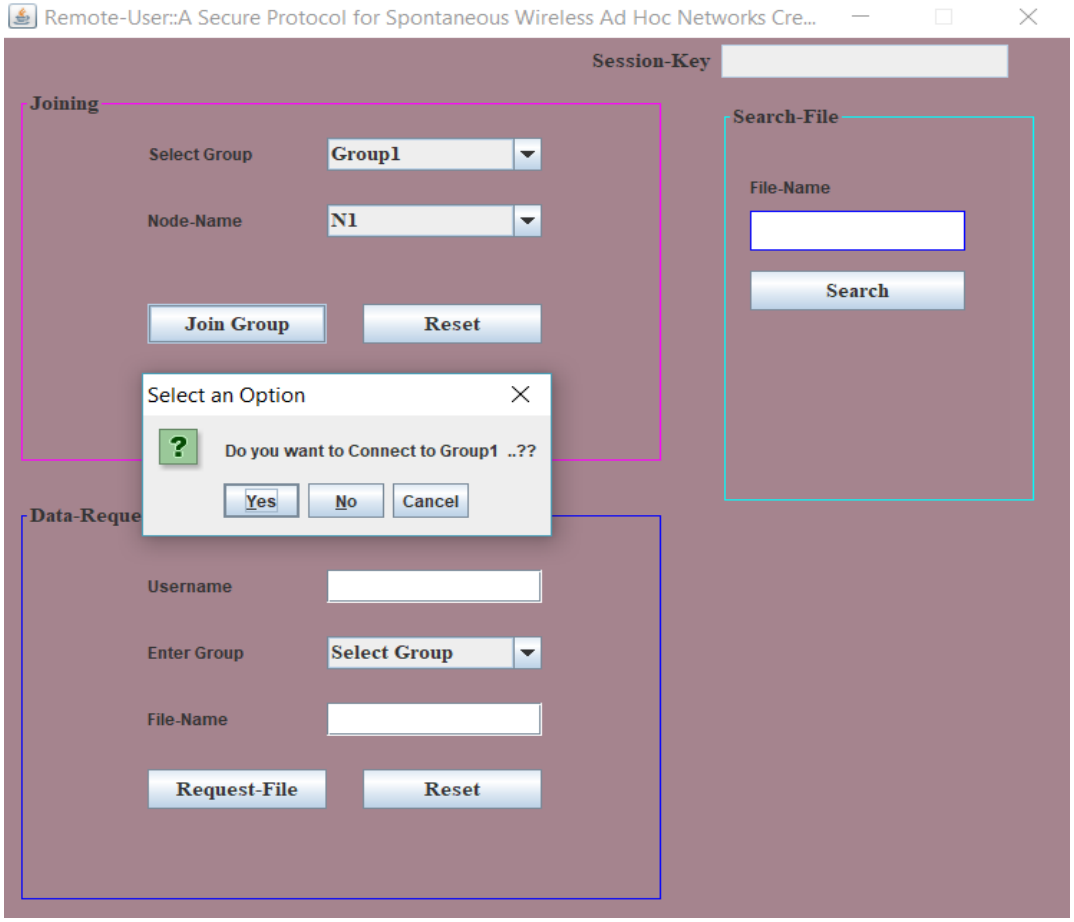
If a single user is using the entire connection on the same device than only that IP Addreess is needed. In this way the file is uploaded in IDC Manager a confirmation is also received. Further we can view the uploaded file in storage window of the IDC



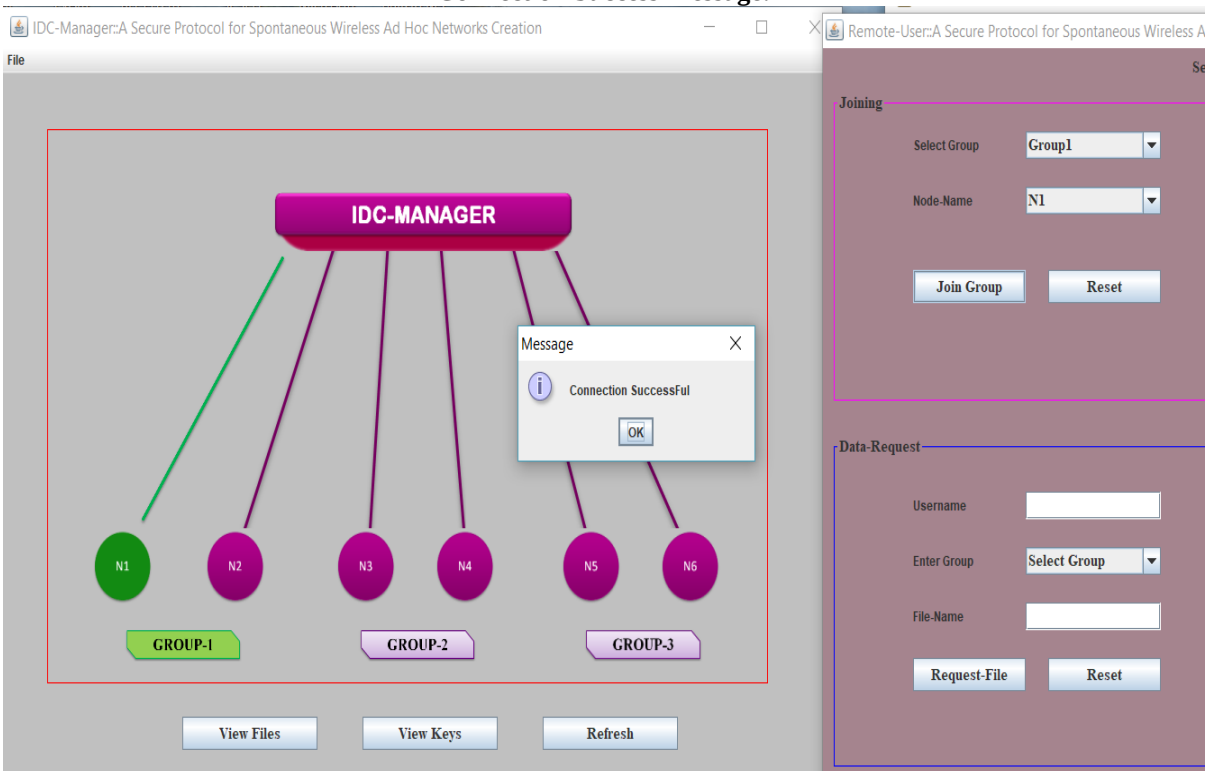
View Uploaded Files record in IDC Manager

Next step is to Run Remote User: Connect to Group within IDC

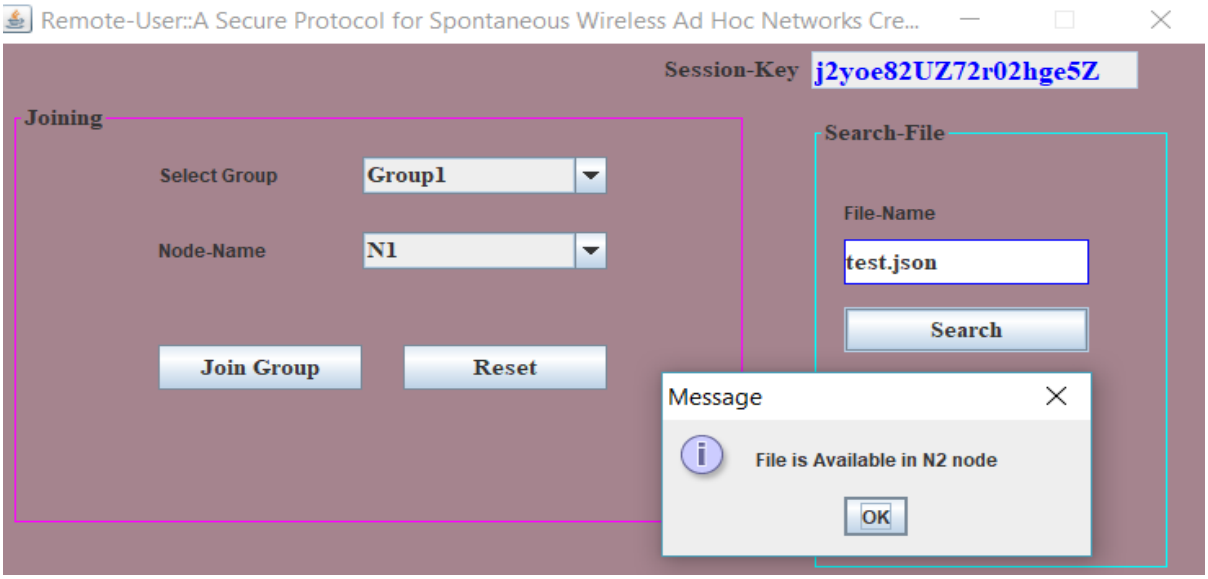
In this we can have multiple users for testing and demonstrating that we cannot access data from other group and nodes. In the present case we are establishing a connection with the help of Node 1 in Group 1 and a connection succesful meassage is received



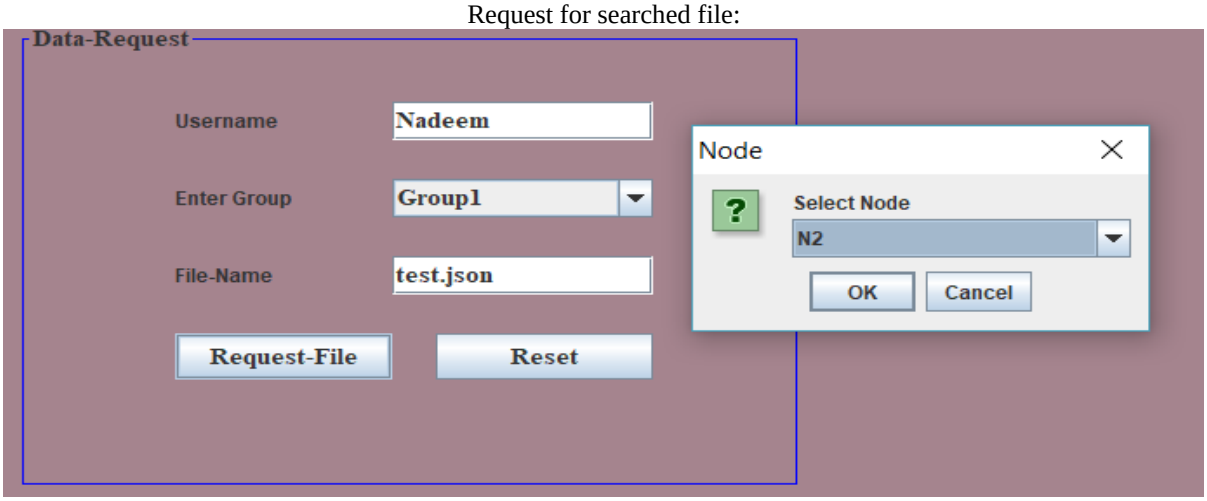
Connection Success Message:



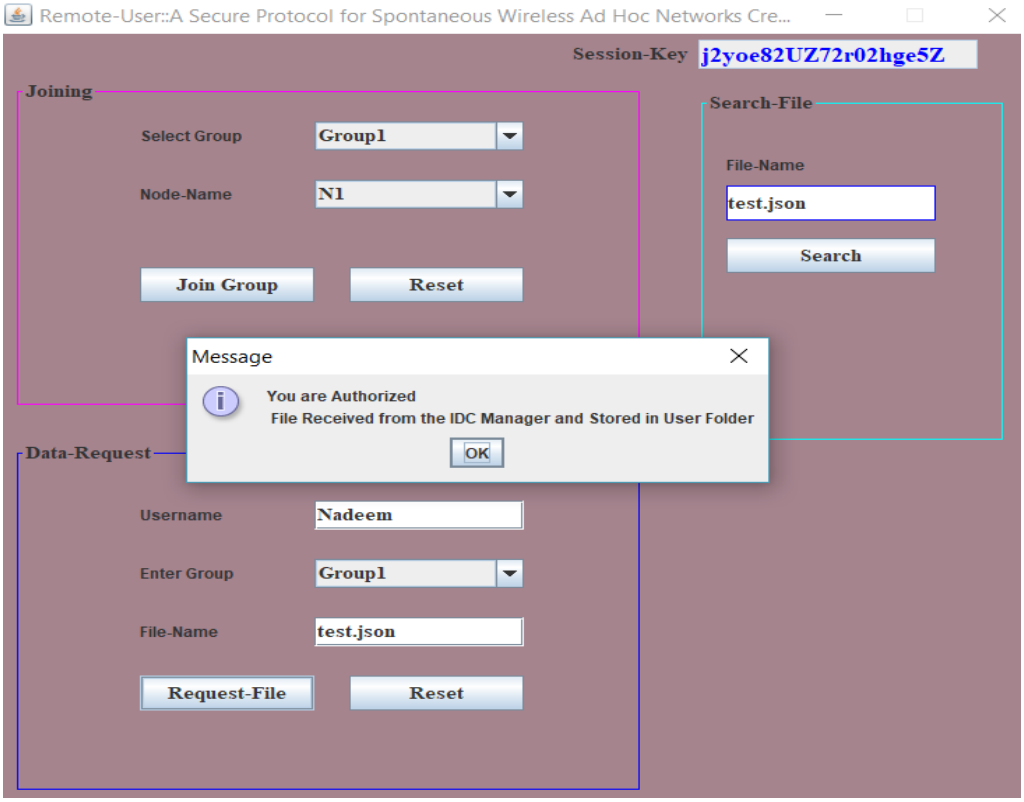
Next step is to search a File from remote user within same adhoc network group:



Request for searched file:

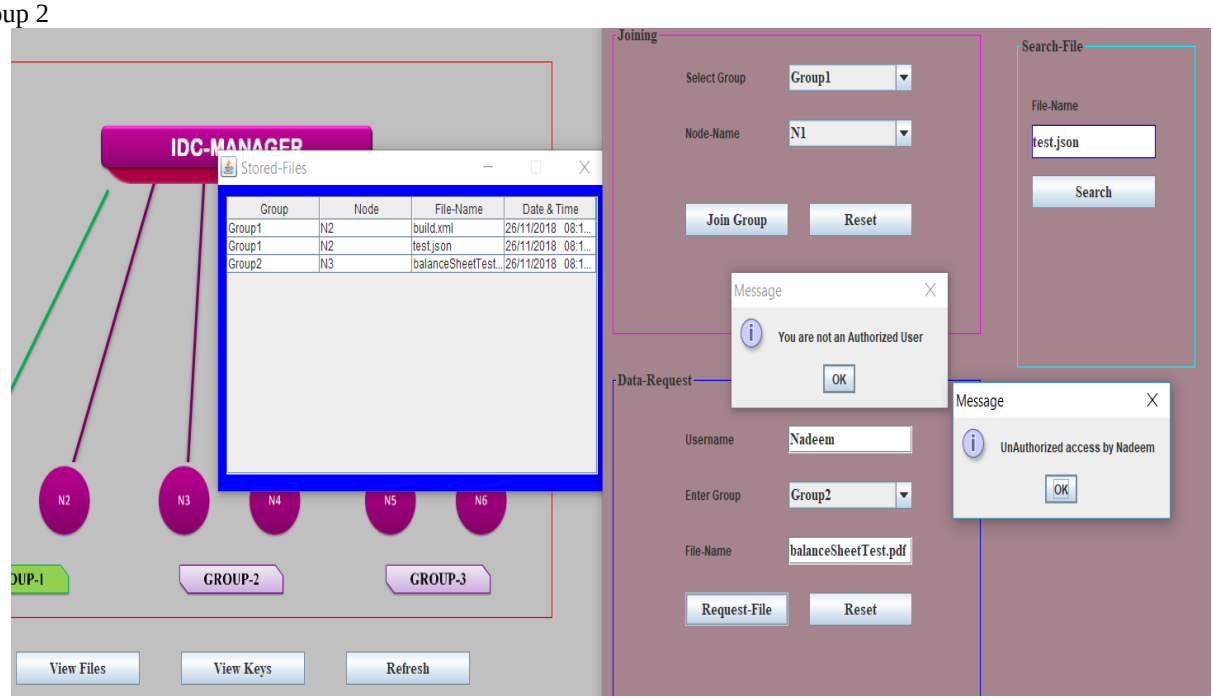


As We were part of same group and session keys were matching so we were authorized:



The file is received by group leader 1 and stored in User Folder

Next to check the security of the network Request Files from diff Ad-hoc group nodes such as request the file from Group 2



UnAuthorized Access was denied.

VI. CONCLUSION

In this paper we demonstrate the concept of a system which allows the making and controlling of an unconstrained distanced impromptu mechanism. It is based on a loose connection mirroring behavior of body system relations. Hence every user has to do work to be updated and increase the systems developed and send inputs to other user clients.

In order to deal with this techniques of self-arrangement is provided. Internet Protocol deliver is appointed for the electronic equipments however is ignored proficiently and detail information is obtained by simple basic steps

We have additionally made an easy to understand application that has negligible communication. Users without higher knowledge involving vital needs can take part in a hurdle less network. The necessary information included in the network allows the users perfect interconnection between different users.

In the final conclusion we tried to demonstrate some results to accept the usual activity .The system showed us the advantages of using self designing incorporated unconstrained network. The output units acquired of appropriate for need in genuine conditions without affecting the need of electronic equipments having limited resources.

REFERENCES

[1]H. Kopka and P.W. Daly, A Guide to LATEX, third ed. Harlow, U.K.: Addison-Wesley, 1999.
[2]L. Ji and M. S. Corson. Differential destination multicast: a MANET multicast routing protocol for small groups. In Proc. IEEE Infocom01, Anchorage, Alaska, April 2001.
[3]E. M. Royer and C. E. Perkins. Multicast operation of the ad hoc on-demand distance vector routing protocol. in Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM), August 1999, pp. 207218.
[4]C. Wu, Y. Tay, and C.-K. Toh. Ad hoc multicast routing protocol utilizing increasing id-numbers (AMRIS) functional specification. Internet draft, November 1998.
[5]X. Zhang and L. Jacob. Multicast zone routing protocol in mobile ad hoc wireless networks. in Proceedings of Local Computer Networks, 2003 (LCN 03), October 2003.
[6]C.-C. Chiang, M. Gerla, and L. Zhang. Forwarding group multicast protocol (FGMP) for multihop mobile wireless networks In AJ. Cluster Comp, Special Issue on Mobile Computing, vol. 1, no. 2, pp. 187196,1998.
[7]J. J. Garcia-Luna-Aceves and E. Madruga. The core-assisted mesh protocol. In IEEE JSAC, pp. 13801394, August 1999.
[8]M. Gerla, S. J. Lee, and W. Su. On-demand multicast routing protocol (ODMRP) for ad hoc networks. in Internet draft, draft-ietf-manet-odmrp-02.txt, 2000.
[9]S. Lee, W. Su, J. Hsu, M. Gerla, and R. Bagrodia. A performance comparison study of ad hoc wireless multicast protocols. In IEEE INFOCOM, 2000.
[10]E. Kaplan. Understanding GPS. Artech House, 1996.

[11] X. Xiang, Z. Zhou and X. Wang. Self-Adaptive On Demand Geographic Routing Protocols for Mobile Ad Hoc Networks. IEEE INFOCOM07 minisymposium, Anchorage, Alaska, May 2007.
[12] P. Bose, P. Morin, I. Stojmenovic and J. Urrutia. Routing with guaranteed delivery in ad hoc wireless networks. In Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications (DialM ´ 99), August 1999.
[13]B. Karp and H. T. Kung. Greedy perimeter stateless routing for wireless networks. In Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM), pages 243–254, August 2000.
[14]F. Kuhn, R. Wattenhofer, Y. Zhang and A. Zollinger. Geometric ad-hoc routing: Of theory and practice. In Int. Symposium on the Principles of Distributed Computing (PODC), 2003.
[15]J. Latvakoski, D. Pakkala, and P. Paakkonen, "A Communication Architecture for Spontaneous Systems," IEEE Wireless Comm., vol. 11, no. 3, pp. 36-42, June 2004.
[16]L. Liu, J. Xu, N. Antonopoulos, J. Li, and K. Wu, "Adaptive Service Discovery on Service-Oriented and Spontaneous Sensor Systems," Ad Hoc and Sensor Wireless Networks, vol. 14, nos. 1/2, pp. 107-132, 2012.
[17]S. Gallo, L. Galluccio, G. Morabito, and S. Palazzo, "Rapid and Energy Efficient Neighbor Discovery for Spontaneous Networks," Proc. Seventh ACM Int'l Symp. Modeling, Analysis and Simulation of Wireless and Mobile Systems, Oct. 2004.
[18]J. Ba¨ckstro¨m and S. Nadjm-Tehrani, "Design of a Contact Service in a Jini-Based Spontaneous Network," Proc. Int'l Conf. and Exhibits on the Convergence of IT and Comm., Aug. 2001.
[19]V. Untz, M. Heusse, F. Rousseau, and A. Duda, "Lilith: an Interconnection Architecture Based on Label Switching for Spontaneous Edge Networks," Proc. First Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (Mobiquitous '04), Aug. 2004.
[20]L.M. Feeney, B. Ahlgren, A. Westerlund, and A. Dunkels, "Spontnet: Experiences in Configuring and Securing Small Ad Hoc Networks," Proc. Fifth Int'l Workshop Network Appliances, Oct. 2002.