Secure and Distributed Data Query In Intermittently Connected Passive Ad-Hoc Networks

Prof. Sridevi, Shruti

Abstract— **There was a problem that how to enable the data query efficiently in Mobile Ad hoc Social Networks. These MASON are nothing but a group of mobile users who are connected via Bluetooth or Wi-Fi and share the necessary files to each other. In MASON querying for the data faces several issues such as opportunistic link connectivity, Autonomous computing & storage and unknown or inaccurate data providers. With this problem in mind we are going to introduce a new system to determine a transmission strategy which supports the data query rate the user wish to give within the delay budget. And also the system minimizes the total communication cost for the data transmission. The development of this practical system involves the deep knowledge of distributed data query protocol. A test bed is prepared to carry out an experiment to explain the feasibility and efficiency of the newly designed system. Moreover the simulations were made use wherein some network settings are not practical to build in real-time labs. And these simulators are used to learn the performance of the system under different network settings.**

***Index Terms— Data Query, MASONs, Distributed Data Query Protocol, Test Bed, Simulators*.**

I. INTRODUCTION

Nowadays social networking technology is growing very fast as we see few of the networking sites Facebook, Twitter, LinkedIn and Google+. An Ad-hoc network is a wireless network constructed by the mobile users (users are having mobility and they are moving around the network). The chances of users getting disconnected from the network are more in ad-hoc networks. Since the nodes are mobile, frequent network disconnection may occur hence data accessibility will be affected.

Internet infrastructure is platform for web-based online social networks used for communication purpose. By using Bluetooth or Wi-Fi, mobile users are connected and the same data available in the network is shared by all the users.

A MASON is established for those who are in a local community where users interact with each other regularly. Ex: People living in an urban area, students studying in a college etc. The size of the community varies from higher to smaller. Long span of years is an example for large size and few hours is an example for lower span.

Unique challenges:

1. Opportunistic link connectivity**:**

In MASON mobile nodes are moving randomly in the network. There will not be any pre-specified path for data transmission. While transmitting data from one node to another node they choose the path randomly. So probability of link failure in ad hoc network is more, it leads to a more delay in the network at the same time cost will be more.

2. Autonomous computing and storage**:**

To store and process user data there will be central servers in online social networks. In MASON these kinds of servers are not there, a single portable device has to perform distributed data storage and computation. These devices have specified limited computing, storage and energy capacity. These are disadvantageous to MASONs. Before sending the data to another node each node must perform data distribution and store them locally. This local data will act as back-up data if the data transmission fails because of any network issue.

3. Unknown or inaccurate expertise:

When a node wants to query to any other node it will not check whether that node is expertise to answer to that query. Prohibitively it takes high cost to build the index data of structure like P2P network. A node hardly knows their ability to answer a query which is requested by some other node in the network this is considered as a worst case scenario.

II. RELATED WORK

Nowadays ad hoc network is more commonly used. It came to light, when investigation is done on wireless communication technologies. Ad hoc network is formed by mobile hosts those are used temporarily on the network

1. In Ad-Hoc networks, mobile hosts move randomly so chances of disconnections are more. This leads to poor data accessibility compared to the conventional fixed network. Using "Three Replica Allocation" [1] approach by T. Hara et.al, data accessibility is increased by frequently adding data items on the Mobile Hosts. Now mobile hosts can change their relative positions while retaining network connections.

2. Most existing information search techniques only focus on Publish-subscribe paradigm. J. Fan et.al[2] proposed DELQUE [2], an information searching technique on Delay tolerant networks. To forward query to other users DELQUE does not require any selected relays, thus overhead is reduced. The ultimate goal of Delay Tolerant Networks (DTNs) is to permit accessing the information quickly and efficiently for mobile users.

3. An application by W.Gao et.al [3] Disruption Tolerant Networks (DTNs) have taken the benefits from data dissemination. It is a concept in which it considers all the user interest and their requirements. Main goal of this approach is satisfying the interest of the users and increasing cost-effectiveness of data dissemination. In this approach the data is randomly transmitted to all the nodes in the network though they are not interested about the data, so lot of bandwidth and resources are wasted. To avoid these problem data receivers should be appropriately identified based on how much interest they have about a particular data.

4. Bikenet is an application developed by S. B. Eisenman et.al[4] involves sensor networking principles and techniques is a multifaceted and senses personal, bicycle and environmental necessities through mobile phones. It also helps socialize with other members of the cyclist community with the help of real-time data sharing through web. It helps to evaluate the performance of cyclist and their environmental conditions.

5. This application is developed by E.Miluzzo et.al[5]. Interference of the individuals is combined by the CenceMe system with the help of off-the shelf, sensor-enabled mobile phones and sharing of this information through the social networking applications such as Facebook/MySpace. This paper includes the design, implementation, evolution and user experience of the application named CenceMe. Exploiting of the off-the-shelf is done by the people centric application. Sensing the presence of the people is automatically detected by the mobile phones which are sensor enabled (Ex. Dancing with friends at the party hall) and then shares this information through the social network portals such as Facebook. The main functionality of this CenceMe application is retrieving the user information automatically and publishing the same information on the social networks using the mobile phones.

III. PROPOSED SYSTEM

To overcome the disadvantages of existing system we are going to introduce a centralized distributed model that offers useful theoretic insights. Its main goal is to develop a model which issues a query and responds to query in a very efficient manner. We are introducing a protocol in MASON that is distributed protocol which is based on two methods. In first method it employs “reachable expertise” it means pre-determining whether the nodes are reachable from each other. If nodes are not reachable because there is no path exists from one node to another hence transmitting the data from source to the destination is highly impossible. So before sending a data to other node it is mandatory to check whether the current node is reachable to destination or not. If path exists then only send data to otherwise start searching another path to other node.

If there is no direct path from Source to Destination, Source will query the data to immediate neighbour node which is reachable to the destination. Finally make sure that the data has reached to the destination without any network failure. In query transmission redundancy is exploited. Redundancy is not considered as important but it increases the data delivery rate and it responds to a query in efficient manner.

Advantages of Proposing System:

1. The efficiency and feasibility of the data query protocol is increased:

All the groups are distributed and router is at the centre. Each group contains set of members and all the groups are connected so chances of link failures in the network are less. A node can issue and respond to query in a more efficient manner. As members of a group are connected delay is less because data transmission is done very fast.

2. Total communication cost is minimized:

As delay is very low in this centralised distributed model because the members of a group are connected to centralized router and time taken to respond a query is less consequently cost of communication will be less.

3. Facilities to gain useful empirical insights is given by proposed system.

3.1 Algorithms Used:

1) Encrypting Using AES Algorithm Begin:

```
Encrypting(string data, string keydata)

 Take  string outputstring="";  int j=0;

 char[] outchar = data.ToCharArray();
 char[] keychar = keydata.ToCharArray();
for(int i=0;i<keychar.Length;i++)

key[i] =Convert.ToByte(keychar[i]);

byte[] outbyte = new byte[outchar.Length];

int loop = outchar.Length/16;

for(int kk=0;kk<loop;kk++)

for(int i=0;i<16;i++)

outbyte[i] =Convert.ToByte(outchar[j]);j++;

IBlockCipher  = AesFactory.GetAes();

InitCipher(key);

Cipher(outbyte,output);

for(int i=0;i<16;i++)
```



```
outputstring = outputstring +
Convert.ToChar(output[i]);

return outputstring;
```

2) Decrypting Using AES Algorithm:

```
Decrypting(data,  keydata)

Begin string outputstring=""; int j=0;

char[] outchar = data.ToCharArray();    char[] keychar =

keydata.ToCharArray();

for(int i=0;i<keychar.Length;i++)

key[i]=Convert.ToByte(keychar[i]);

byte[] outbyte = new byte[outchar.Length];

int loop = outchar.Length/16;

for(int kk=0;kk<loop;kk++)

for(int i=0;i<16;i++)

outbyte[i] =Convert.ToByte(outchar[j]); j++;

IBlockCipher = AesFactory.GetAes();

InitCipher(key); InvCipher(outbyte,output);

for(int i=0;i<16;i++)
      outputstring = outputstring +
      Convert.ToChar(output[i]);

return outputstring;
```

3.2 Modules:

1) Data Owner:
In this module, Data Owner Registers to a particular group in Router and Login by using his Username, Password and Group Name (Group1, Group2 and Group3). Then he uploads a file to associated node in the Router, Based on its minimal cost and lesser bandwidth of node in the group.

2) Router**:**
The Router is responsible to issue the query to the group as depicted by an arrow to the associated nodes, when the query request is transmitted from one node to another node in the group. The Router can view the files, can also view the Registered Users in Router, Router assigns the cost for the users in groups and also can view the distance details of all the users.

3) Social Network Manager:
The Social Network Manager is responsible to view the Query Transaction with their tags Requested user, File Name, Secret key, Group Name, Responsible user for that file details and he can also provide the access permission to users for searching the file in different groups.

3) End User:
In this module Data Consumer is only responsible to download the file, it will search the availability of mentioned file within the same group. If file is not available within the same group then it should predict access permission with Social Network Manager to search for the file in other groups. If file or secret key hadn't been matched in any group then the user will be considered as an Attacker.

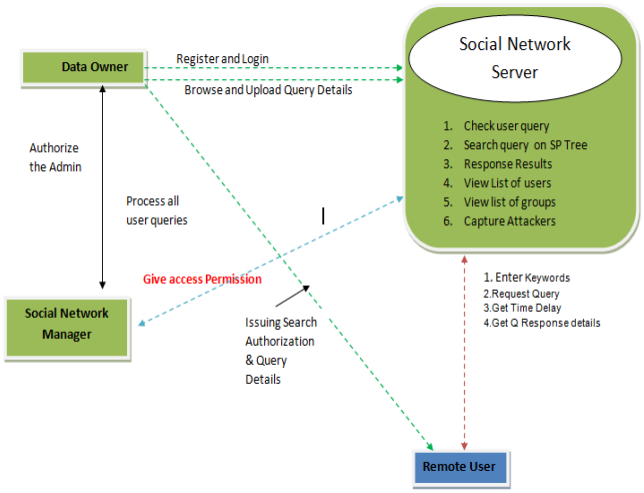

Figure 1: Architecture Design of Proposed System

The architecture contains four modules namely Data Owner, Social Network Server, Social Network Manager and Remote User.

The functions of data owner are to allow the user to register and login to the system. This needs some data members to store and retrieve the data. Those data members are user name, password and name of the group to which a particular user belongs. And the other functionalities are browsing and uploading a query. This architecture has given access to the users to upload a file of their wish so that other members of the same group can download it without any hassles. In case if a user in some other group wants to access the file, they have to get access permission from Social Network Manager.

Social Network Server has got its own functionalities like checking user query, searching a query on the shortest path tree, Response results, viewing list of users and viewing list of users finally capturing attackers.
Social Network Manager authorizes the admin and also makes sure all the user queries are processed. The crucial task of Social Network Manager is giving the users access permission to the social network server.

IV. RESULTS AND DISCUSSIONS

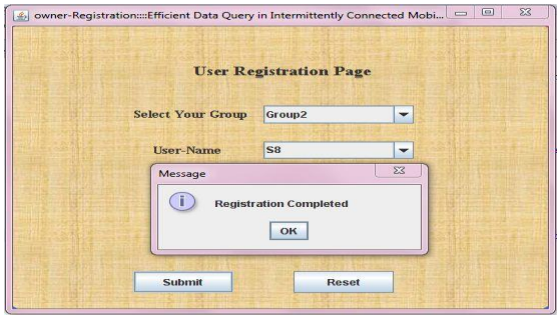

Figure 1: User Registration Successful

This snapshot shows the successful registration. The user is registered to the mentioned group successfully

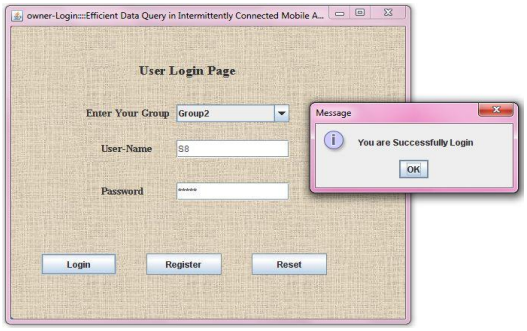

Figure 2: Login Successful

The user has provided the correct credentials and logged in to the network

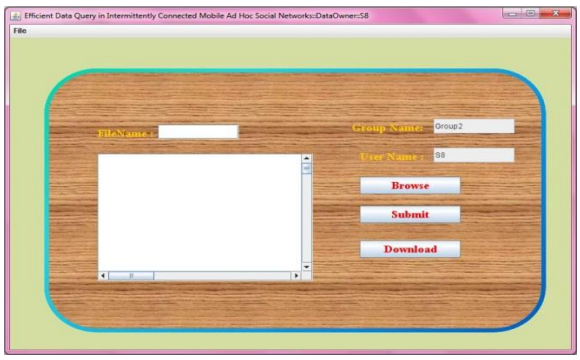

Figure 3: User Home Page

Once the user logs in with the correct credentials, user is taken to the home page where he can see the buttons/options for the operations that the user could perform

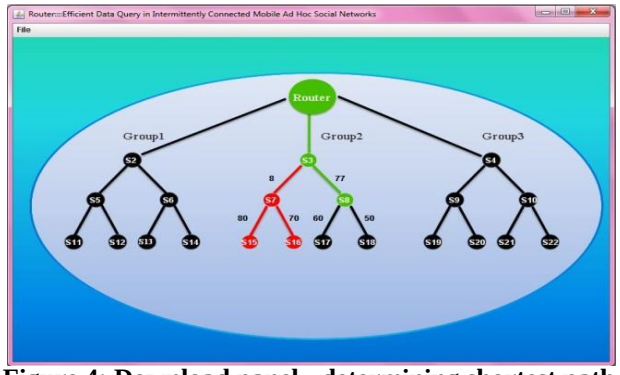

Figure 4: Download panel - determining shortest path

As the tree traversed while uploading a file to the node, same way it traverses while downloading too. If the node having the requested file comes along the path, the file gets downloaded to the local tray of that user.

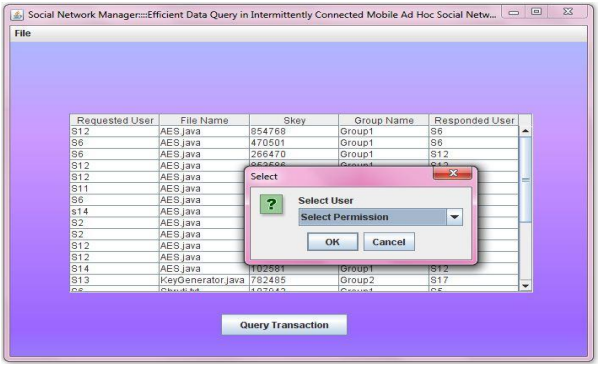

Figure 5: Social Network Manager –Assign access permission – (Provide / take back)

Social Network Manager selects the user and the permission it wish to give to a user. It can also take back the permission n he same way as t assigns the permission. For taking back the Access Permission Social Network Manager selects "Don't Allow" permission for that user.

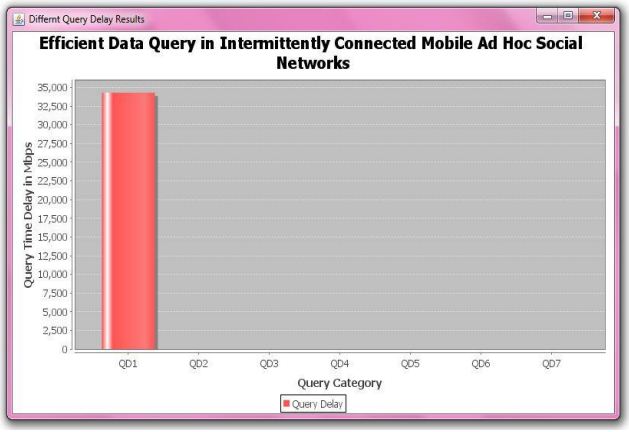

Figure 6: performance analysis graph – file download from native group

This bar shows the time delay to download the file mentioned by the user in the Ad Hoc network. If the file is found in the same group, only one bar will be shown. If the user has searched multiple groups for that file then that number of bars will be displayed in the graph.

V. APPLICATIONS

1. Applications will be in Storage area networks where the system throughput will be maximized to store the social network user data.

2. The query processing speed will be high since the searching is based on the cost or distance of the nodes in the social networks.

3. This system security will be more since the query retrieval is based on the group in the social networks.

4. There is no link failure between the nodes since MASON technique is used in the social networks.

Note: Here the users are considering as nodes.

VI. CONCLUSION

We have studied how to overcome from the problem in mobile ad hoc social networks (MASONs), as there will not be any path from source to destination, link failure occurs frequently as a result data accessibility in ad hoc network is also low. To avoid from these problems we have introduced a centralized distributed model in which router is at the center and some groups are created each group contains specific members. Each member can act like query issuer or query responder. All the groups are connected with each other. Consequently delay required to response a query is low finally we can conclude that this method is cost effective and it performance the operation within the delay budget hence we can say this method is effective.

REFERENCES

[1] T.Hara, "Effective Replica Allocation in Ad Hoc Networks for Improving Data Accessibility," in Proc. of INFOCOM, pp. 1568–1576, 2001.

[2] J. Fan, J. Chen, Y. Du, P. Wang, and Y. Sun, "DelQue: A Socially Aware Delegation Query Scheme in Delay-Tolerant Networks," IEEE Transactions on Vehicular Technology, vol. 60, no. 5, pp. 2181–2193, 2011.

[3] W. Gao and G. Cao, "User-Centric Data Dissemination in Disruption Tolerant Networks," in Proc. of INFOCOM, pp. 3119–3127, 2011.

[4] S. B. Eisenman, E. Miluzzo, N. D. Lane, R. A. Peterson, G.-S. Ahn, and A. T. Campbell, "The BikeNet Mobile Sensing System for Cyclist Experience Mapping," in Proc. of SenSys, pp. 87–101, 2007.

[5] E. Miluzzo, N. D. Lane, K. Fodor, R. A. Peterson, H. Lu, M. Musolesi, S. B. Eisenman, X. Zheng, and A. T. Campbell, "Sensing Meets Mobile Social Networks: The Design, Implementation and Evaluation of the CenceMe Application," in Proc. of SenSys, pp. 337–350, 2008.

[6] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Efficient Routing in Intermittently Connected Mobile Networks: The Single-Copy Case," IEEE/ACM Transactions on Networking, vol. 16, no. 1, pp. 77–90, 2008.

[7] A. Mei, G. Morabito, P. Santi, and J. Stefa, "Social-Aware Stateless Forwarding in Pocket Switched Networks," in Proc. of INFOCOM, pp. 251–255, 2011.

SHRUTI Received the B.E Degree in Computer Science and Engineering From Visvesvaraya Technological University Belgaum, Karnataka, India in 2013, now doing M.Tech (4th sem) degree in Computer Science from Visvesvaraya Technological University, Godutai Engineering College for Women Gulbarga, Karnataka, India in 2015 (pursuing).

