IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. VII (Nov – Dec. 2014), PP 32-36
www.iosrjournals.org

Algorithm for routing encrypted information in ad-hoc network with optimized gossip routing protocol using Bluetooth

Shaoni Paul, InderjitLal, Shreya Yadav, Vineet Pandey, Arnab Pal, AvranilTah
ESL, Dumdum Lab, Salt Lake City, Kolkata, India

Abstract: *The paper describes an optimized gossip routing protocol between nodes in an ad-hoc network. The backbone of the application is based on an algorithm which is used for routing information in an ad-hoc network from one node to another with the help of optimized gossip routing protocol using Bluetooth as the medium of transmission. Our system dynamically determines the path optimally given a source and destination node. The routing protocol is developed using python and file system is being used for storing purpose.*
Keywords: *Ad-Hoc Networks, Bluetooth, DES, Gossip Protocol, Python Programming*

I. Introduction

The technologies and the programming language used in developing the system are the gossip protocol, ad-hoc networks, Bluetooth technology and Python.

Gossip Protocol:

- A communication protocol among computer systems mimicking the form of gossip seen in social networks.
- The protocol serves an easy way of communication among large networks, large scale distributed systems and is also the most efficient ones in simplicity, scalability and high reliability even in constantly changing environments.
- Also, in the gossip based approach, each node forwards a message with some probability, to reduce the overhead of the routing protocols

Ad-hoc networks:

- The wireless ad-hoc network is used in our project. It's basically a decentralized, infrastructure-less network because it does not rely on a pre-existing infrastructure like the routers or access points.
- The nodes participating for data transmission in this network is dynamic, for instance, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity.

Bluetooth technology:

- A wireless technology standard for exchanging data over short distances,operates in the 2.4GHz frequency band without a license for wireless communication.
- This communication protocol is primarily designed for low-power consumption and also cost efficient.
- Bluetooth technology can be used for Real-time data transfer usually possible between 10-100 meters, which is reasonable within a small building. Moreover, the data-transfer rate of the Bluetooth technology is quite acceptable, i.e. 3-4Mbps
- Close proximity not required as with infrared data (IrDA) communication devices as Bluetooth doesn't suffer from interference from obstacles such as walls.
- Supports both point-to-point wireless connections between mobile phones and personal computers, as well as point-to-multipoint connections to enable ad hoc local wireless networks.

Python:

- A high level programming language extensively used now-a-days and is very similar to Perl, C and Java.
- It is used in both small and large scales but the syntax allows expressing concepts in fewer lines of code rather than C or Java.
- A wide variety of operating system allows installation of this interpreter and also this programming language supports object-oriented, imperative and procedural styles of programming making it a general purpose and convenient language for application.

DES:

- A symmetric-key algorithm for encryption
- It is used in various aspects in information security.

- In our application DES method of security measures are implemented using python programming while sending and receiving data through Bluetooth. It is used here for sending encrypted data from one hop to next hop, until the last or destination node where it is decrypted and the data is retrieved.

II. Motivation

As wireless technology has become more convenient and popular means of communication in every facet of work; be it in the industry, or hospital, or academic institutions. So data transmission in our application is based on Bluetooth. The preference of this technology over Wi-Fi is because of low power consumption, cost efficient, resistance to interference with medical devices and our need of short range transmission. Our application is needed to be confined within the boundary of the hospital, so Bluetooth works pretty well within this range. But, the major point is the implementation of the gossip protocol. As previously mentioned, this protocol works similar to public chit-chats or any social networking gossip; it suites best for spreading data or information within the system we have considered.

III. Methodology

A. Determining the path:

In our system we are proposing an algorithm to find out a shortest path for transmitting data from a given source node to a destination node. Geometrically the shortest path from a point to another is the straight line. We implemented this concept with distance vector minimization algorithm. Initially, we have described a virtual co-ordinate system in the environment where are going to implement the system. Then according to the co-ordinate system we have placed the Bluetooth modules at certain places where the distance between any two modules will not be more than 100 unit. Thus, each and every module has a co-ordinate on the co-ordinate system. As the Bluetooth modules have their own identification id called mac id, we have assigned a unique mac id to each Bluetooth module. Fig. 1 depicts the arrangements of the devices along with the coordinate system.

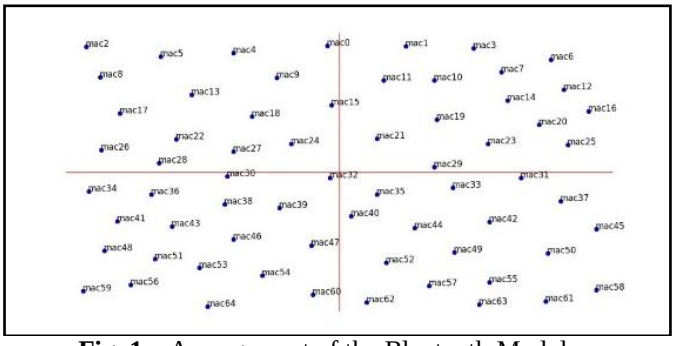

Fig. 1 – Arrangement of the Bluetooth Modules

It can be found that, a certain device has one or many nearby devices. Now to choose any one device among other nearby devices such that the data can take the shortest route to its destination is described below. The green dot implies the source address and the red dots imply the nearby devices around mac3.

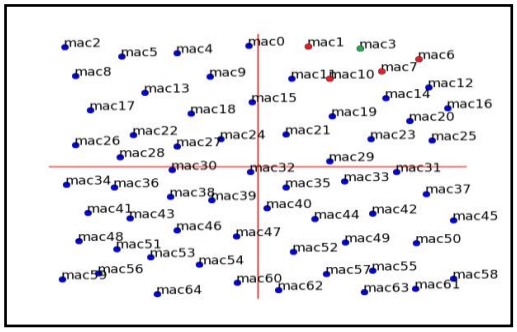

Fig. 2 – Nearby devices for the device having mac id mac3

In the next step we are given a source node with the mac id and a destination node. Then the transmission begins from the source node. In our system we are determining the address of the next hop dynamically. Now, according to the destination node, the source node determines the next hop. Suppose ***S***is the source node and ***D*** is the destination node. Now, $(S_x, S_y)$and (D_x, D_y) are the coordinates of the source and destination nodes respectively. We are calculating the slope ***M*** between the source and destination.

$$M = \frac{D_y - S_y}{D_x - S_x} \qquad (i)$$

Now, to find out the appropriate next destination, we are shifting the origin of the coordinate system to the source node and rotating the axes in the angle at which the source node and the destination node is inclined. To find out the angle of inclination θ,

$\theta = \tan^{-1} M$ (ii)

Now, we are changing all the coordinates of other nodes according the rotated and shifted co-ordinate system. To find out the coordinates according to that, we are using the equations below.

Suppose a node is ***C***. The original coordinate of the node is ***(C_x, C_y)***. In the shifted system, suppose it is (C_x', C_y').

$C_x' = x\cos\theta + y\sin\theta - C_x$ (iii)

$C_y' = -x\sin\theta + y\cos\theta - C_y$ (iv)

We are changing the coordinates of the nearby devices only. Now suppose there are four devices near the source node ***S*** i.e. ***D_1, D_2, D_3, D_4***. So we have four abscissa of the nearby devices. Now, as the destination node will be on the x-axis of the co-ordinate system, the node having minimum abscissa will be nearest to the x-axis, i.e. will have almost same inclination with the destination address. Now, suppose ***D_2*** has the minimum abscissa. Now we have to choose the node in the same direction with the destination. For that, we have determined the sign of the ordinate of the destination node. It will determine whether the destination is in the positive direction of the x-axis or in the negative direction. According to that, we will choose the next node which will be present in the same direction as the destination node. Finally, the data will be sent to the next node. In the next node, the received data will be decrypted and the destination node will be figured out. In the same way, the node will decide its next hop in the journey to the destination.

Packet Formation:

Each packet consist of two information. The destination address for that particular packet and the data that has to be sent. Fig. 3 shows the exemplary shape of a packet.

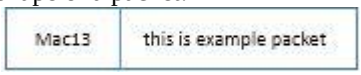

Fig. 3 – An exemplary shape of the packet

Now the entire packet is encrypted using DES algorithm and it is being sent to the node with the key that has been used to encrypt. As DES is a symmetric key encryption algorithm, the same key will be used to decrypt the encrypted content.

Flow Diagram:

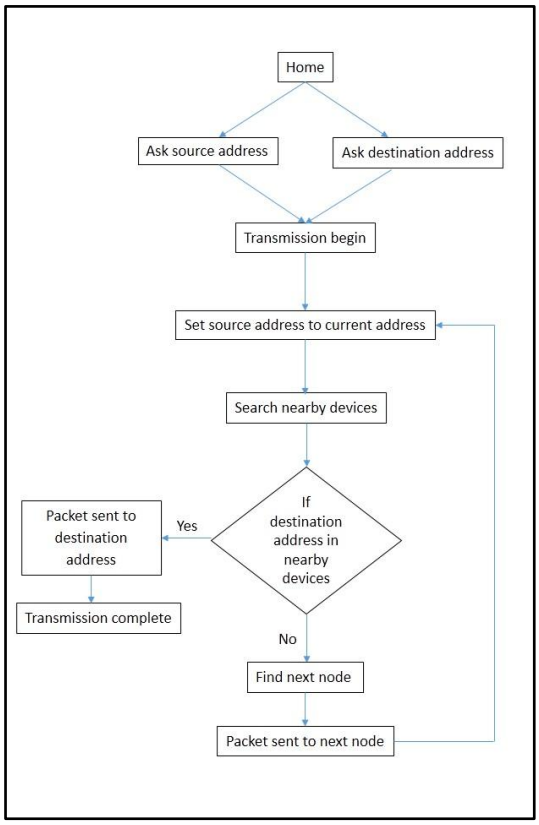

Fig. 4 – Flowchart of the algorithm of our project

A. Algorithm: As discussed earlier, we have formulated an algorithm for routing information in the ad-hoc networks using gossip protocol. The steps how it works are:

1. The Bluetooth devices participating in the process are plotted in a co-ordinate plane.
2. Through the co-ordinates we are now able to find the nearby devices of a particular Bluetooth device.
3. When a device knows its surrounding nearby devices it can send the data to any one of those devices.
4. Following the steps 2 and 3, a data can reach its destination from its source taking the shortest path, given the source and destination address.

B. **Data Structure:** The entire building block of the permanent data storage is data structure like dictionary, list, tuples etc. We have used the dictionary to store all Mac ids of the Bluetooth devices participating in the interactive system. The dictionary in turn is being kept in the list which is ultimately stored in the file. A dictionary is a special kind of data-structure of python, which support the following features. Keys must be immutable, and this key can be number, string, tuple or anything, but, it cannot be changed after creation, because of hashing. And moreover, the keys must be unique again because of hashing. There are no restrictions of values in a dictionary, and the keys will be listed in arbitrary order. For instance, we have used the Mac id of the devices as the key and the co-ordinates of the Mac id are stored in tuple with respect to the key.

```
[{'mac7': [190.0, 173.0], 'mac6': [248.0, 195.0], 'mac5': [-209.0, 200.0] ...}]
```

Fig. 5 – The data structure of the device map of our network

In this same manner, the nearby devices with respect to a particular Bluetooth device are stored in the dictionary as tuple and its key respectively.

```
[{'mac7': ['mac6', 'mac3', 'mac12', 'mac10', 'mac14'], 'mac6': ['mac7', 'mac3', 'mac12', 'mac14'],
'mac5': ['mac4', 'mac2', 'mac8', 'mac13'].....}]
```

Fig. 6 – The data structure for storing the nearby devices from a device

IV. Results

The following snapshot shows the path chosen by our algorithm given the source address **mac2** and the destination address **mac61**.

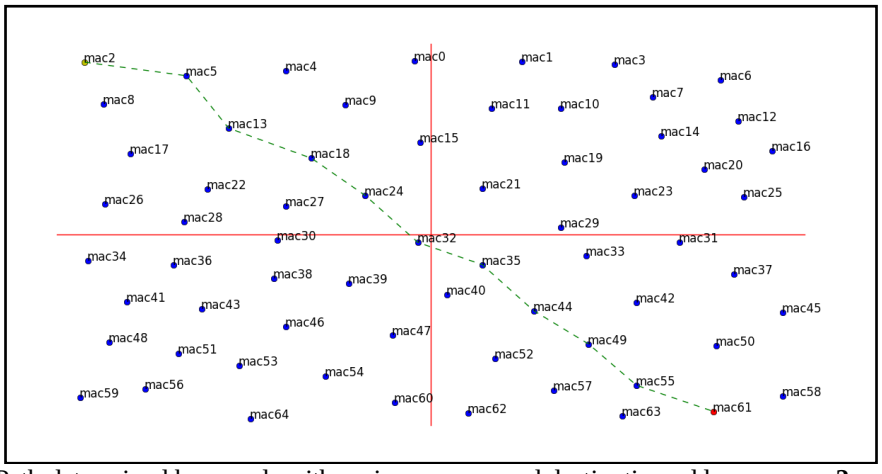

Fig. 7 – Path determined by our algorithm given source and destination address as **mac2** and **mac61** respectively

Another example of transmission is being shown in the next figure after choosing the source address as **mac3** and the destination address **mac34**.

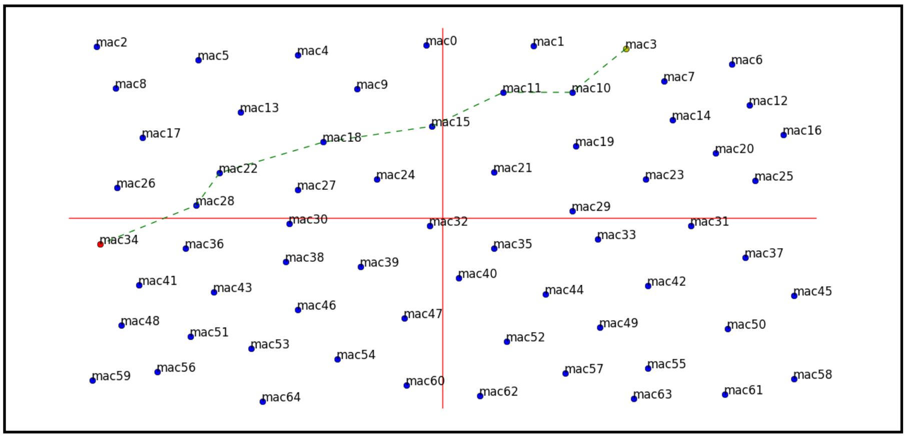

Fig. 8 – Path determined by our algorithm given source and destination address as **mac3** and **mac34** respectively

The following screenshot shows the encrypted packet that is being sent over the network.

```
>>>
original packet:  ('mac13', 'this is example packet')
encrypted packet:  ホ[ßÅγØú?Ó9/+1ヨÏ\IîØìårÆûQ ?Ûü

>>>
```

Fig. 9 – Result showing the encryption of the packets

V. Conclusion

The project is a combination of some of the very popular technologies and also it is implemented with less hassle using the python programming language. The ad hoc networks has some features like, limited power supply of individual nodes, limitation of wireless bandwidth, and the channel condition can alter greatly. In addition, since nodes are mobile, routes may constantly change. Thus, to enable efficient communication, robust routing protocols must be developed. So, the gossip based routing protocol is one of the very robust methods that we used to find out the smallest path to transmit a data. Several features are already discussed for selection of Bluetooth as a medium of transmission. We have experimented in different ways for developing the minimum path from the source to destination using this protocol and ultimately got the results discussed above. It seems likely that gossiping could be implemented in some other ways in finding out not only the minimum path but also in a little amount of time. In our future work we will emphasize on reducing the time and implementing further security measures and possibly a greater amount of data transfer.

Acknowledgements

We sincerely thank Mr. AvranilTah, (MSCS, University of Texas at El Paso) for guiding us in the entire journey of developing the project. We faced many difficulties during development of the project. We solved the problems with the guidance of our mentor Mr. AvranilTah. Moreover, we also than our friends and colleagues for helping us during this time.