RESEARCH ARTICLE OPEN ACCESS

Bluetooth Message Hopping Chat Application

Prof. Govind Wakure[1], Tanzeel Shaikh[2], Kirti Karande[3], Ibrahim Shaikh[4], Hardik Vaghela[5]
[1,2,3,4,5](Information Technology, Rajiv Gandhi Institute of Technology, Versova,Mumbai.)

----------**********----------

Abstract:

Places where internet and cellular connectivity is weak and mobile devices are used, Bluetooth can prove to be a beneficial communication medium. Also, Android operating systems are quite often used in the organizations by the employees and the staff. Hence, we propose a Bluetooth based Android Chat Application that can communicate with a BT device outside the Bluetooth range of the Source device. For this, an adhoc network is created that acts as a mediator between the source and the destination BT device. The path within this network is found using the MPR flooding technique. As privacy of messages is crucial, RSA encryption is used for securing the messages.

Keywords **—Bluetooth, Android Chat Application, Adhoc Network, MPR flooding, RSA.**

----------**********----------

I. INTRODUCTION

In organizations or companies where communication is essential butdue to prohibitions on the use of internet or due to unreachable cellular network; if one has to send a message to one of the colleagues or broadcast it to a group of them, then this can be done using a Bluetooth chat app. The objective of this app would be to send messages beyond the Bluetooth's normal range of 10m via the intermediary devices.The intermediary devices must also have the app running in the background. These devices can act as nodes buffering the message for certain time and then sending the message to their nearest neighbours till the message is reached to the destination. So as to achieve this, flooding algorithm is used.But using usual flooding have many limitations like a broadcast storm is created and then the complexity of the app increases for handlingthe duplicate messages. To avoidblind sending of messages, packets are sent to those nodes only which are most likely to fall in the destination route. This is achieved by Multi Point Relay (MPR) that is based on 2 hop neighbour knowledge of the node.

The main purpose of the app is to achieve network transparency and to allow secure communication between devices. For this type of communication, the message content would be encrypted with the public key that is exchanged when the devices are paired and will be decrypted at the destination with the private key that was generated along with public key. The public key and the private key are generated when the user logs in the app for the first time on a device.

The only limitation of this app arrives when the Bluetooth of the intermediary devices should be on, even though they are not sending messages and hence, the battery is getting consumed.However, as compared to other technologies like Wi-Fi,Bluetooth consumes lesser battery power and therefore, proves to be a better alternative for chat messenger.

II. LITERATURE SURVEY

A. Adhoc Network

A network that consists of independent nodes connected wirelessly such that those nodes have the ability form connections dynamically, such a network is called an Adhoc Network. A wireless ad hoc network (WANET) is a decentralized type of wireless network. In a Bluetooth network,

there are two types of nodes: a slave and a master. Each node has the ability to be either or both at the same time. Hence, we can say that, Wireless Ad-hoc Network is a set of wireless independent multi-hop nodes which does not require any pre-existing infrastructure. All wireless devices in the network, including the ones that are present outside the range of a particular node are discovered and peer-to-peer communication takes place between them using multi-hop technique. So, some of the nodes in ad-hoc network may not be able to communicate directly with each other and are dependent on some other nodes to pass their message. Such networks are often known as multi-hop or store and forward networks. The intermediate node(s) act as routers, which discover and maintain a table to forward the message to other nodes in the networks. Many significant applications of Ad-hoc networks include sharing internet without having an access point, exchanging files and data in a group, underwater sensor networks and disaster recovery.

As topology of a Wireless Adhoc network is not static, selection of routing process becomes difficult. Thus, routing algorithms like link state routing and distance vector routing are not efficient for Adhoc networking due to the reasons mentioned before. So, to overcome this problem, several ad-hoc routing protocols have been proposed[1][2][3][4][5]. These routing protocols can be classified as firstly, proactive algorithm that maintains routing tables that contains the lists of destinations and their corresponding routes where the tables are updated periodically by sharing of tables with the adjacent node. Secondly, Reactive Algorithm, also known as on-Demand routing where the sender will try to find the route to destination (using shortest path algorithm) only if it has to send some data. Lastly, Hybrid Routing Algorithm which is a combination of both reactive and proactive protocol where each node first maintains the routing tables (as in case of proactive protocol) and will also participate in on-demand routing by exchanging routing tables on request by sender node (reactive protocol).

B. Flooding

This is the most common algorithm used for adhoc networks, as in Adhoc network every node acts like a server and a client, there is no dedicated server. Similarly, the flooding algorithm treats every node as a receiver and transmitter. It tries to forward the message to its neighbouring nodes except for the node it has received the message from. However the uncontrolled flooding will keep on routing packets indefinitely and therefore various techniques are used to control this flooding .One such technique is to broadcast the messages to only those nodes that are likely to be on the destination route called MPR flooding(Multi point Relay) discussed in the next section.

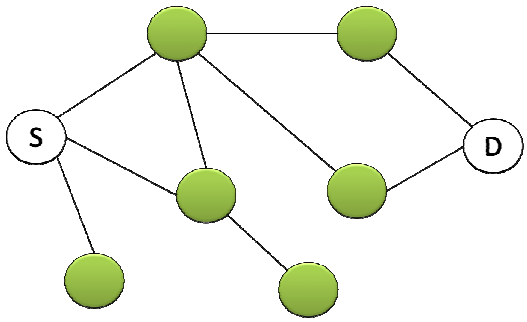

Fig. 1 nodes receiving packets from Blind Flooding.

C. Multipoint Relay flooding

This algorithm [6] is based on 2 hop neighbour knowledge of the node implemented in the OLSR routing protocol[7]. Here the number of nodes retransmitting the messages are limited as compared to blind flooding .The nodes that are retransmitting these messages are called multipoint relay and then they decide their own MPR set to relay the messages. This keep on continuing till the destination is found.

Thealgorithm is as follows:

(i) The sender will first make two sets of nodes,one being h1 (1 hop neighbours)and the second one being h2 (2 hop neighbours).

(ii) Then its checks which h1 nodes have the h2 nodes as only their neighbours from the h1 node set and then adds that h1 node to MPR set.

(iii) From the remaining h1 nodes it is then checked which one of them covers the

maximum of uncovered nodes of h2 and then adds that h1 node in MPRset. In case of, if two or more nodes from h1 set have same number of uncovered nodes of h2 then both covered and uncovered nodes are compared.

(iv) This keep on continuing for every node in the MPR set.

(v) The loop stops once the destination is reached.

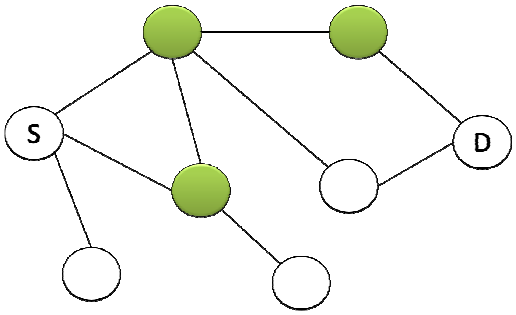

Fig. 2 nodes receiving packets from MPR Flooding.

D. Public Key Encryption

Encryption is the process of transforming a plain text data into encrypted form such that only the intended destination can decrypt or get the original data back from the encrypted data. Now, this process uses key (a piece of information or sequence of random elements that acts as a parameter being used in the algorithm). Keys are of 2 types, namely, public key and private (or secret) key. Public keys are the ones that are known to anybody who tries to communicate with the key-holder whereas the private keys are the ones that are only known to the key-holder. The public key and private key are mathematically related.

The main idea of encryption lies in the algorithm used to generate and use these keys and these algorithms are categorized into 2 categories: Asymmetric Key techniques and Symmetric key techniques. In symmetric, same key is used for encryption as well as decryption. As public key is available to both, the sender and the receiver, the public key is used for encryption and decryption. These types are comparatively less secure. However, in asymmetric, keys used for encryption and decryption are not the same i.e. only the private key corresponding to a respective public key can decrypt the message encrypted by that public key. Asymmetric encryption is often referred to as Public key encryption.

Various public key encryption algorithms have been proposed. Some of the commonly used are Diffie–Hellman key exchange (used for secure key distribution), DSA (Digital signature algorithm) and RSA (for key generation, encryption and decryption). The algorithm that will be implemented here is RSA.

E. RSA

RSA is an algorithm that achieves both key generation as well as encryption and decryption. This algorithm is widely used for transmitting data securely.

The pseudo-code for the same can be given as follows:

(i) Choose 2 prime numbers p & q.
(ii) Compute n such that n = p * q.
(iii) Compute φ(n) as φ(n) = (p - 1) * (q - 1).
(iv) Choose encryption factor ‘e’ such that $1 < e < \varphi(n)$ and e and n are co-prime.
(v) Compute a value for decryption factor ‘d’ such that $(d * e) \% \varphi(n) = 1$.
(vi) Public Key is (e, n).
(vii) Private Key is (d, n).
(viii) The encryption of message ‘m’ is done usingthe public key which results in cipher text ‘c’.
(ix) The decryption of cipher text ‘c’ is doneusing the private key which results in message ‘m’.

III. PROPOSED SYSTEM

A. The Chat Application

1. At the installation of the app on the device, a public and a private key is generated using RSA algorithm.
2. Now, the device that wants to send the message to the destination device should be paired with the destination through the app

at least once so as to retrieve the MAC address and the public key of the destination.

3. Before sending the message, the message is encrypted with the public key of the destination and the packet is structured. The Message format is described in the next section.
4. The message is then transmitted to the destination using MPR flooding algorithm, such that.
   (i) If message reaches destination, an ACK is transmitted back to the sender.
   (ii) If the destination was not found, an error report is generated.

B. Message Format

All the messages transmitted contain the sender Mac address and the receiver MAC address and the message content. The message has a time to live count attached to it i.e. the hop count, maximum hop counts it can travel before getting self-destructed. If the sender does not receive the ACK message from the destination for a certain period of time delivery error is reported. However this is possible when the destination phone could not be found or some hoe after receiving the message the destination device was turned off before it could send the ack.

Now, the messages exchanged need to be secured. For that, encryption techniques need to be used. The message format for the message that will be exchanged through the chat application is shown in figure 3.

Sender MAC Address	Receiver MAC Address	Message Content	Hop Count	ACK (YES / NO)

Fig. 3 Message Format.

C. Encryption used for Chat Application

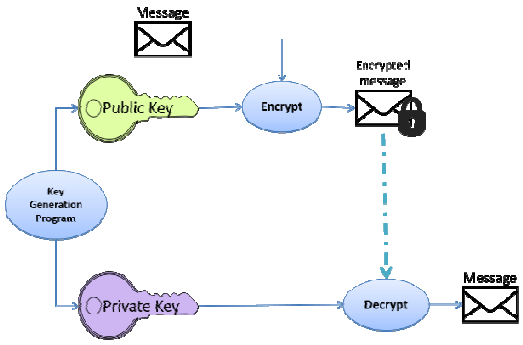

Fig. 3 Encryption used for Chat application.

Here, as soon as the app is installed (or user logs in) the app generates the public key and the private key for the user. For two devices to communicate, they must be paired. So, just after the pairing is done, the public key is shared. Now, looking from the destination's point of view, the public key will be used by the sender devices to encrypt the message that are to be sent to the destination device. When the destination device receives that message, the private key which was generated along with the public key will be used to decrypt it and obtain back the actual message at the destination end.

D. Limitations

Every device should have the app running. This app requires the Bluetooth to be enabled for infinite amount of time.

IV. CONCLUSIONS

So, now with this chat application, people can communicate with each other via Bluetooth at places where internet and Wi-Fi chat applications cannot be afforded due to low internet connectivity or battery consumption problems.Being a chat application, security of messages is a critical issue here and hence the security provided needs to be enhanced.

ACKNOWLEDGEMENTS

We wish to express our sincere gratitude to Dr. U. V. Bhosle, Principal and Prof. D. M. Dalgade, H.O.D of Information Technology Department of

RGIT for providing us an opportunity to do our project work on “Bluetooth Message Hopping". This project bears on imprint of many people. We sincerely thank our project guide Prof. Govind Wakure for his guidance and encouragement in successful completion of our project synopsis. We would also like to thank our staff members for their help in carrying out this project work. Finally, we would like to thank our colleagues and friends who helped us in completing the project synopsis successfully.

REFERENCES

[1] S. Basagni, I. Chlamtac, V.R. Syrotiuk and B.A. Woodward. A Distance Routing Effect Algorithm for Mobility (DREAM), Proceedings of the fourth annual mobile computing and networking, October 1998.

[2] P. Krishna, M. Chatterjee, N.H. Vaidya and D.K. Pradhan. A Cluster-based Approach for Routing in Ad hoc Networks. In proceedings of Second USENIX Symposium on mobile and Location Independent Computing, pp. 1–10, January 1996.

[3] S. Murthy and J.J. Garcia–Luna–Aceves. An Efficient Routing Protocol for Wire-Less Networks. ACM Mobile Networks and Applications, Special Issue on Routing in Mobile Communication Networks, 1(1):183–197, October 1996.

[4] C.E. Perkins. Ad hoc on-demand distance vector routing, Internet Draft, Internet Engineering Task Force, work in progress, December 1997.

[5] C.-H. Toh. A novel distributed routing protocol to support ad-hoc mobile computing, Proceeding of 15th IEEE Annual International Phoenix Conference on Computer Communications, pp. 480–486, 1996.

[6] A. Qayyum, L. Viennot, and A. Laouiti. Multipoint relaying: An efficient technique for flooding in mobile wireless networks. 35th Annual Hawaii International Conference on System Sciences, 2001.

[7] P. Jacquet, P. Muhlethaler, A. Qayyum, A. Laouitim, and L.Viennot. Optimized link state routing. draft-ietf-manet-olsr-06.txt, 2000.