International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 12, pp 105-108, December-2025

https://doi.org/10.47001/IRJIET/2025.912015

PeerLink: A Decentralized Peer-to-Peer Messenger

[1]Yashraj Pawar, [2]Satyajeet Chavan, [3]Ketan Gunjal, [4]Kalyani Chalke, [5]Prof. Dipika Pangudwale, [6]Prof. Nita Pawar

[1,2,3,4]Student, Department of Computer Engineering, Ajeenkya D.Y. Patil School of Engineering Polytechnic, Pune, Maharashtra, India

[5]Guide, Professor, Department of Computer Engineering, Ajeenkya D.Y. Patil School of Engineering Polytechnic, Pune, Maharashtra, India

[6]HOD, Professor, Department of Computer Engineering, Ajeenkya D.Y. Patil School of Engineering Polytechnic, Pune, Maharashtra, India

***Abstract* - PeerLink is an Android peer-to-peer, decentralized messaging service application which allows two-way text messaging without using intermediate servers. PeerLink permits mobile devices to communicate straight away by creating a peer-to-peer network unlike conventional messaging systems where authenticated routing and storage is undertaken by a central infrastructure to create privacy hazards and single points of failure. Every device act as a client and a message carrier enhancing fault tolerance and eliminating reliance on external services. The system is dedicated to the message delivery with low latency, better user privacy and high reliability of communication in a low or unstable connection environment. To assure safe message communication, end-to-end encryption is employed. It has been experimentally confirmed that PeerLink is capable of providing messages with reasonable latency to permit near real time communication. The findings indicate that the concept of decentralized peer-to-peer has been proven to be effective in developing lightweight and privacy conscious messaging applications that can be useful in a small-scale and infrastructure constrained system.**

Keywords: Peer-to-Peer Messaging, Android Application, Decentralized Communication, Real Time Chat, Mobile Networking.

I. INTRODUCTION

Mobile instant messaging is now considered a part of daily communication and billions of users of applications like WhatsApp, Telegram, and Signal use mobile apps to exchange texts in real-time. Nevertheless, the traditional systems require the use of centralized servers where the users are authenticated, message routing, and data are stored. The nature of this centralization brings on board a number of issues such as single points of failure, scalability, privacy complicates and reliance on constant internet connectivity.The solution to these limitations is therefore suggested that is PeerLink, which is a peer-to-peer based messaging application designed on Android platform. PeerLink also allows direct textual communication between nearby gadgets without involving a centralized infrastructure. A peer-to-peer network results in devices communicating at the same time; each node is a client and a relay in transmission of messages. PeerLink has a decentralized structure which means that it has high fault-tolerance, uses less user privacy, and can communicate even in locations with restricted or untrustworthy internet connectivity.

1.1 Peer Discovery

The first stage in the process of communication between the devices of the PeerLink system is peer discovery that allows communication. Under this process, the application establishes the presence of other devices that can be connected to PeerLink in the same network environment. The discovery mechanism enables the user to observed peers available in the vicinity willing to communicate. PeerLink is the peer-to-peer application that relies on local network discovery and does not use centralized servers.

1.2 Connectivity Establishment

PeerLink then connects the two communicating devices directly after peer discovery. The system handles connection requests, acknowledgement and session creation so that there is stable and reliable connection. One device is both a client and a server which provides flexible peer-to-peer connectivity. It establishes the connection using TCP socket programming which provides reliable and ordered data transmission. The adequate connection management methods are applied to keep active sessions and manage disconnections gracefully.

1.3 Message Sharing

Direct peer-to-peer communication is being used as a means of message exchange in PeerLink. Data transfer mechanisms are used to transmit messages in real time and they are reliable to promote ordered and loss-free delivery of messages. This is because the decentralized model of message sharing is more resilient to fault tolerance as well as privacy of users since it does not store or route messages centrally.

PeerLink provides message exchange in real time utilizing peer-to-peer communication without using centralized server.

1.4 TCP Connection Management

PeerLink is a TCP-based peer-to-peer system which uses socket messaging and channeling of reliable messages between interconnected peers. Connection setup, data transmission, error handling and graceful termination of connections are managed by the application. Smooth closure of TCP connections will make sure that there is proper use of resources and that there will be no communication failure in case of peer disconnection or unstable network connection.

II. LITERATURE SURVEY

The current literature in the field of the decentralized mobile communication gives special emphasis to infrastructure-independent messaging schemes particularly in situations when the traditional networks are inaccessible or unreliable like in the case of natural disasters or remote locations or infrastructure crashes. A variety of peer-to-peer (P2P) mobile applications and protocols have been suggested and modeled, with direct device communication, performance (velocity and latency) and resilience targeting emergency requirements.

2.1 P2P Mobile Messaging and Performance

Peer-to-peer mobile apps can create direct communication between mobile devices without the use of centralized servers. FireChat and Bridgefy were some of the earliest commonly discussed P2P messaging applications that relied on local wireless interfaces to communicate messages among protesters or attendees at a protest when the network was not especially available. Research on these systems demonstrates that the speed of message delivery and the end-to-end latency is very sensitive on the density of the network, the mobility of the devices within it and the effectiveness of the protocols used to route the message to a peer. No matter how much they managed to allow off-grid communication, the throughput and reliability of such implementations changed dramatically when the conditions were sparse or the movement was high. The discoveries make it clear that P2P mobile messaging requires strong peer discovery and effective routing.

2.2 Security and Privacy in Peer-to-Peer Communication

Security and privacy are core characteristics associated with any distributed peer-to-peer messaging application. PeerLink does not utilize any central server to process or archive any messages traversed. Hence, this negates the default risk exposure associated with large data sets and third-party surveillance. Messages are sent directly between the devices that are communicating, thus keeping the associated data within the control of the communicating users.

Also, PeerLink uses end to end encryption for secure peer-to-peer message transfer. Secure socket communication is used for protected data integrity and confidentiality as well as to prevent unauthorized access. By which we also avoid centralized storage and processing which in turn minimizes privacy issues and which also reduces the risk of surveillance or data misusing at the same time we do not observe a drop in performance or real time communication quality.

2.3 Decentralized Communication Architecture

Unlike what we observed in traditional centralized messaging which has a server at the center, in PeerLink we have devices talking to each other directly. Messages in this case go over a single, direct connection from point to point without the use of intermediate nodes or routing layers. We observed reduced latency and also, we do away with the complex issue of multi-hop or relay-based networks.

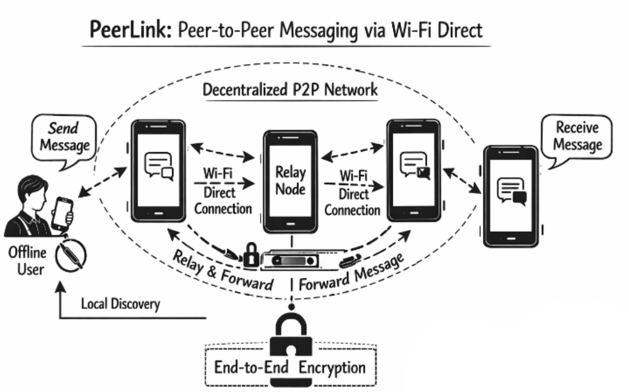


Figure 1: Architecture of Full-Duplex Peer-to-Peer Communication

Also, our peer-to-peer set up is very simple to manage and which in turn improves on the reliability of the network for small scale communications. By maintaining a dedicated TCP connection between peers we in turn guarantee that messages are delivered in order and without loss. That is what makes the system a great fit for when you value simplicity, privacy and reliability over large scale network growth.

III. METHODOLOGY

PeerLink is designed to facilitate secure and dependable and communications without the need for centralized servers. The approach taken is first to build a model for decentralized communications of which the building block is a single mobile device acting in the model as a node communicating as a peer.

ISSN (online): 2581-3048
Volume 9, Issue 12, pp 105-108, December-2025
https://doi.org/10.47001/IRJIET/2025.912015

3.1 System Architecture

PeerLink uses a decentralized and peer-to-peer architecture where mobile devices talk to each other directly and do not communicate through centralized servers. Every device function as a separate node that can both send and receive communication requests. Because of no centralized infrastructure, there are no single points of failure and overall reduced reliance on constant internet access.

3.2 Peer Discovery and Connection Establishment

Peer discovery is at the base of what enables device communication. PeerLink in our system we have observed to identify present peers in the same network which we do via local network detection methods. Once a peer is found the user is able to put out a connection request to set up direct communication. We use TCP socket programming for connection establishment which we do to guarantee reliable data transfer. We handle in this the connection requests, acks, and session which we put together to form a stable communication channel.

In terms of proper connection management we observed that we do what it takes for the communication sessions to run efficiently and also observed to it that they go out gracefully when the need arises. This we observed to also enable secure and constant message exchange which does not require external servers.

IV. SYSTEM IMPLEMENTATION

4.1 Application Development Environment

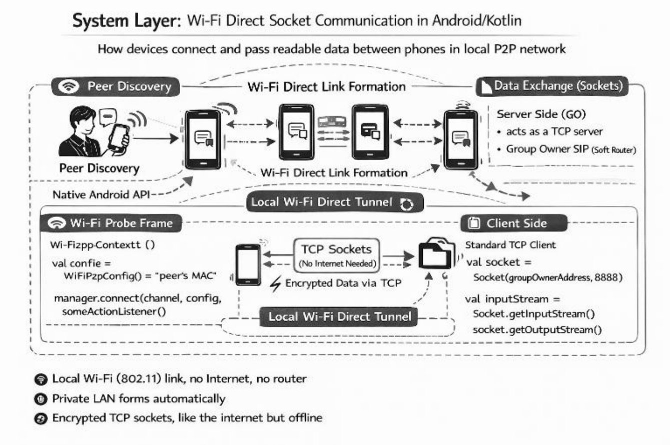
PeerLink is on Android platform with Android Studio as the main IDE. The application is implemented with the help of Kotlin which includes good support for programming sockets and multithreaded operations. Android Studio - Tools for interface design, debugging, and performance monitoring are provided to enable efficient development and testing. Background services are used to take care of network communication separately from the user interface. This makes sure message transmission/reception is done smoothly without having an effect on application responsiveness. The development environment includes support for testing on multiple Android devices as well, so that evaluation can be performed using different network conditions and device configurations.

4.2 Communication Module

The communication module is responsible for creation and maintaining of direct connection between the devices on a point-to-point basis. TCP socket programming is used to impose such reliable communication channels that provide support for ordered and loss-free data transfer. When a user sends an initial communication, the module establishes a socket connection and runs the data exchange session. The module is responsible for performing essential communication functionalities like message transmission, message reception and monitoring of connections. In addition, it incorporates error detection and exception handling mechanisms to handle network interruptions or unexpected disconnections. The proper connection termination routines are provided to release system resources efficiently and avoid communication failures.

4.3 Security Implementation

Security is a very basic part of the PeerLink system. Before transmission, all messages are encrypted with the help of end-to-end encryption techniques so that only the intended communicating peers can access the content of messages. Encryption is done on the application level and therefore confidentiality is ensured, even in transmission via the network.


System Layer: Wi-Fi Direct Socket Communication in Android/Kotlin
How devices connect and pass readable data between phones in local P2P network
Peer Discovery
Wi-Fi Direct Link Formation
Data Exchange (Sockets)
Peer Discovery
Server Side (GO)
• acts as a TCP server
• Group Owner SIP (Soft Router)
Wi-Fi Direct Link Formation
Native Android API
Local Wi-Fi Direct Tunnel
Wi-Fi Probe Frame
Client Side
TCP Sockets
(No Internet Needed)
Encrypted Data via TCP
Local Wi-Fi Direct Tunnel
Standard TCP Client
Local Wi-Fi (802.11) link, no Internet, no router
Private LAN forms automatically
Encrypted TCP sockets, like the internet but offline

```
Wi-Fizpp.Contextt ()
val confie =
  WiFiPzpConfig() = "peer's MAC"
manager.connect(channel, config,
  someActionListener()
```

```
val socket =
  Socket(groupOwnerAddress, 8888)
val inputStream =
  Socket.getInputStream()
  socket.getOutputStream()
```

Figure 2: System Layer Architecture of Full-Duplex Peer-to-Peer Messaging over Wi-Fi Direct

Securing the communication of sockets protects the data integrity further because it makes it impossible to intercept and modify the messages. On the receiving side, the encrypted messages are decrypted before the message is presented to the user. By a combination of encryption, combined with safe handling of sockets, PeerLink guarantees a high level of privacy and security against unauthorized access to peer-to-peer communication.

V. RESULTS AND DISCUSSIONS

PeerLink application was run in several Android devices with different network conditions so as to test its performance. It also tested both stable local networks and those environments with changing connectivity. During real-time communication, performance metrics like delivery of messages within a specified time, responsiveness and general system behavior were monitored. As an experimental result, PeerLink can deliver messages at almost real-time with low latency ranging between 120 ms and 300 ms. Direct peer-to-peer communication avoids the processing delays that are a result of centralized servers. Ordered and reliable communication transmission of messages is guaranteed by TCP socket communication, which contributes to a smooth chat. The application was found to be suitable in real time text messaging with no pronounced delay or loss of message through the constant flow of messages, identifying it as an app that can be used to address real time issues.

The reliability testing was performed based on observing the system behavior in case of connection interruption and peer disconnection. The application was able to handle disconnections and remain in constant communication without breaking down and restored communication within 2–4 seconds after network recovery. Network instability allowed the system to correctly release sessions as well as to reconnect and recover communication without data inconsistency. Security analysis proved the efficiency of the end-to-end encryption implemented. Any message sent was confidential in the process of communication and any attempt to access the message illegally failed. Secure socket handling also ensured a data integrity and intercepting/tampering of messages. The findings indicate that PeerLink is a reliable and secure peer-to-peer messaging without violating user privacy and system stability.

VI. CONCLUSION

The paper introduced PeerLink, that is, a peer-to-peer message application which was created to allow trusted and dependable communication without depending on central servers. The system attempts to overcome the most general limitations of conventional messaging systems, which include privacy concerns, reliance on the service, and single points of failure by ensuring direct connectivity between communicating devices. The achievable application of direct peer-to-peer communication with TCP sockets guarantees reliable, ordered, and low-latency messages delivery. End to end encryption of the message privacy ensures message confidentiality and curbs any unwarranted access to guarantee the privacy of the users. Experimental testing showed that in varying network conditions, PeerLink has been found to offer consistent run times as well as close real-time messaging. These findings validate that peer-to-peer communication that is central is indeed a feasible and effective method of mobile communication, and especially in those settings with limited or lack of connectivity. PeerLink is a privacy-oriented and simple alternative to a centralized messaging system. Future improvements could involve providing support to multimedia messaging, user authentication improvements and scaling improvements, without harming the decentralized architecture and security concepts.

REFERENCES

[1] J. F. Kurose and K. W. Ross, Computer Networking: A Top-Down Approach, *7th ed. Hoboken, NJ, USA: Pearson*, 2017.

[2] N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, and M. Smith, "SoK: Secure Messaging," *in Proc. 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA*, 2015, pp. 232–249.

[3] S. Trivedi and U. Shrawankar, "P2P communication for disaster management using Android devices," *in Proc. 2017 Int. Conf. Emerging Trends in Computing and Communication Technologies (ICETCCT), Dehradun, India*, 2017, pp. 1–6.

[4] R. Schollmeier, "A definition of peer-to-peer networking for the classification of P2P systems," *in Proc. First Int. Conf. Peer-to-Peer Computing, Linkoping, Sweden*, 2001, pp. 101–102.

Citation of this Article:

Yashraj Pawar, Satyajeet Chavan, Ketan Gunjal, Kalyani Chalke, Prof. Dipika Pangudwale, & Prof. Nita Pawar. (2025). PeerLink: A Decentralized Peer-to-Peer Messenger. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 9(12), 105-108. Article DOI https://doi.org/10.47001/IRJIET/2025.912015

****