Secure Peer-To-Peer Messenger and File Sharing Over IPV6

Ben Shaji[1]
Student,
Dept. Of Computer Science & Engineering, Mangalam College of Engineering, Kottayam, India,

Grace Abraham[2]
Student,
Dept. Of Computer Science & Engineering, Mangalam College of Engineering, Kottayam, India,

Vidya E S[3]
Student,
Dept. Of Computer Science & Engineering, Mangalam College of Engineering, Kottayam, India,

Vishnu S Sekhar[4]
Assistant Professor,
Dept. Of Computer Science & Engineering, Mangalam College of Engineering, Kottayam, India

***Abstract*-There is a need for a Privacy-Oriented messenger in a world where data security is becoming more important. In this paper we introduce a Fully End-to-Encrypted Peer-to-Peer Messenger and File sharing Application over IPV6. IPV6 is a domain where people have yet to do many projects. Our model will ensure more security and privacy when compared to other client-server models or even other Peer-to-Peer models since we use IPV6 's inbuilt security features. The application itself is portable since it was developed as a Progressive-Web-App (pwa). Thus making it portable and can be installed in any Operating System. This project is aimed to bring privacy at it's best to all users since there is no server to control or monitor. We have introduced a so-called "Tracker" which keeps track of IPV6 addresses of all users and passes it to someone when requested. Tacker act as the back-bone of the entire architecture.**

KeyTerms:- Security,IPV6,Messenger,Peer-to-peer architecture, Tracker, File sharing

I. INTRODUCTION

Messaging apps are those apps or platforms that make possible immediate messaging. Copious of such apps have developed into broad platforms which facilitate status updates, chatbots, payments and conversational commerce. They are normally centralised networks run by the servers of the platform's operators, unlike peer-to-peer protocols Bit-torrent. Some examples of popular messaging apps include WhatsApp, Facebook Messenger, Telegram etc. The feature which makes
our messenger secure is the fact that there is no-one to control/monitor the communication. With IPV6, we takeIPSec and other security features for granted which makes our model more secure to use.

II. LITERATURE SURVEY

IPV4 has certain disadvantages compared to IPV6.The scarcity of network address was especially extrusive for IPV4. Therefore IPV6 is generated.It is highly essential to research applications in IPv4/IPv6 coexistent network.Applications related to peer to peer network plays a major role in internet communication. Peer to peer related traffic is much more compared to other models. This model uses FSP2P as a P2P file sharing system in IPv4/IPv6 coexisting networks . It can be applied on IPV4/IPV6 coexist networks as well as pure IPV4 and IPV6 networks. Here P2P file sharing protocol is applied to IPV4/IPV6 coexist networks. When considering such a model, the model is very easy to install.Since there is no central dependency the model is more reliable.To build and maintain it needs only less cost is another advantage of this model. The model has some disadvantages too..Since it is decentralized it is very difficult to administer.Each computer keeps its own backup system.Therefore data recovery and backup of data is little bit difficult.There is no guarantee for security of the model is an important drawback of the models which should be avoided completely. When compared to IPV6, IPV4 has only less addresses to deliver. Even with IPV4, especially in mobile networks, NAT implementations such as CGNAT,NAT444 are used. This makes hosting a public web server impossible unless we port forward local port to a public server using SSH,VPN or other methods. Still, some ISPs have not yet implemented IPV6. For them, we could use IPV6 tunnel brokers which gives us an IPV6 address[1].

Efficient location of the node which keeps a desired data item is a problem of peer-to-peer protocol.The paper[3],introducing a model which gives solution for the particular problem. A distributed lookup protocol(chord) is used here to solve the problem. The distributed protocol gives support only for one operation. Here we have a key which maps the key onto a node. On top of the lookup protocol, location of data can be implemented, by combining a key with every data item , and by storing the key at the node to which the key maps. The chord is efficient to join nodes and leave the system, and can answer questions even if the system is changing simultaneously.The Chord is scalable:cost of communication and the state maintained by all nodes scale logarithmically with the number of nodes of Chord.Since IPV4 model is limited in IP-Addresses[3].

MMP2P which is an extended P2P protocol. MMP2P is based on IPv6.Several application for Windows using this are instant messenger, file sharing function and high-quality multimedia conference systems,are implemented.This model mainly focused on scalability to maintain peer to peer network and efficiency.This model has less response time compared to other models such as CAN and CHORD. Peer-to- peer algorithms ensure efficient management of resources.Resources and resource locators are scattered all

over the network.Therefore this protocol would help file sharing among friends. Information among peers used to reduce routing path.The model ensures better communication among users. Less response time provides support for more efficient communication.MMP2P provides better routing.The model is easy to implement[2].

Gnutella, is a virtual network which possesses its own routing mechanisms.The topology of the routing of Gnutella as well as network ensures performance, reliability,and scalability. Extracting the topology of the application level network of Gnutella by using a "crawler".Analyzing the graph of topology and evaluating generated network traffic . Gnutella has the merits as well as demerits of a power-law structure.Therefore some changes are required for Gnutella which will help to enhance performance as well as scalability.Connectivity of Gnutella nodes always keeps a multi-model distribution.This is made possible by combining a power law as well as a quasi-constant distribution. Therefore the network is reliable like a pure power-law network when considering random node failures,.This makes it not very easy to attack by a malicious adversary.The protocol takes some actions or precautions to prevent potential attacks. Consider an example, information of network topology that is obtained is very easy to obtain and that ensures efficient service attack prevention . Security mechanisms are capable of preventing an intruder from collecting information of topology that appears required for the long-term survival of the network.The application-level topology determines the volume of traffic generating, rate of successful searches, and reliability of application. An agent monitors the network constantly.The agent intervenes by asking servants to drop or add links as it is essential to keep the optimal network topology.Agents could embed some data of underlying physical network and builds the topology of virtual application.Only small modifications are required to implement these ideas is advantage of the model.Flooding can be replaced with a smarter as well as group communication mechanisms.Smarter mechanism is less expensive compared to other[9].

The paper [5], focuses on feasibility of personal inter network(PIN) and study how to attain the real coordination of multiple personal devices.It improves the usability of the hybrid as well as the pure P2P architecture in the personal scope. The particular paper proposing an Ipv6 based Node Discover Stack.It makes the usability of the personal P2P application possible. Nowadays the trend of adoption of the personal devices as well as official online devices that make small scale network users need .Using less costly broadcast internet connection many families can access high speed internet and which is make the peer -to- peer connection more important.Here to reduce the difficulty of configuration in application as well as IP layer.The IP layer configuration methods for the end users is required for the population of intelligent appliances. In the peer-to-peer network each of the nodes or workstations has equal responsibilities and capabilities.Sharing of the computer services and resources by the direct exchange between the system. The p2p node should work outside the DNS system and which have importance from central servers.Here the communication protocol that gives identification as well as location system for computers and routes traffic. The pure P2P is the fully distributed P2P architecture. But there are no popular pure P2P models currently due to resource allocation problems[5].

III. PROPOSED MODEL

The proposed model contains following modules:

- Socket-IO framework
- User id creation
- User id searching in DHT
- Key exchange
- Channel creation
- Data exchange

A. The Application

Application can be made using any framework/language since the idea is the same. Socket.IO provides the ability to implement real-time analytics, binary streaming, instant messaging, and document collaboration.

B. User id creation

Technically, User-Id is a way to map to a user's IPV6 address. Since we use DHT , there is a key (user-id) to map corresponding IPV6 addresses.

C. User id lookup

When Alice searches for Bob, Alice uses Bob's user-id as a key to find the address of Bob. This in terms makes a query to the tracker using the user-id.

D. Key exchange

Before the communication with Bob, Alice has to request a security-key exchange process. After both parties complete the process.

E. Channel creation

The 'channel' is an abstraction for the Alice-Bob peer-to-peer communication. For each new connection, there will be a new channel created with new key parameters.

F. Data exchange

After a secure channel is created, users can now start sharing files and messages. It is also possible to have real time video chats. At this time, the data exchange is expected to work.

IV. SYSTEM ARCHITECTURE

This project Aimed to Bring Privacy at it's best to all users. There is no server concept in this model. We have a so-called "Tracker" which keeps track of IPV6 addresses of all users And passes it to someone when requested. All communication between "Tracker" and client is encrypted. Once the client gets the Address, then we no longer need a tracker.

Alice <==> Tracker
Alice <==> Bob

Host-A and B checks for IPV6 GUA, Host-A gets User id of Host-B , Host-A asks for User-Id address of Host-B. If such

an address exists, the Distributed Hash Table will forward the address. More technically, we can simply think of a python dictionary having a key as user-id and value as address if someone is not comfortable with the idea of a DHT. At his point, Host-A and Host-B are initiating key exchange. A secure channel is created.Now both start P2P communication. Host-A or B can revoke when they exit. DHT key,values are cleared and the CHANNEL is revoked.

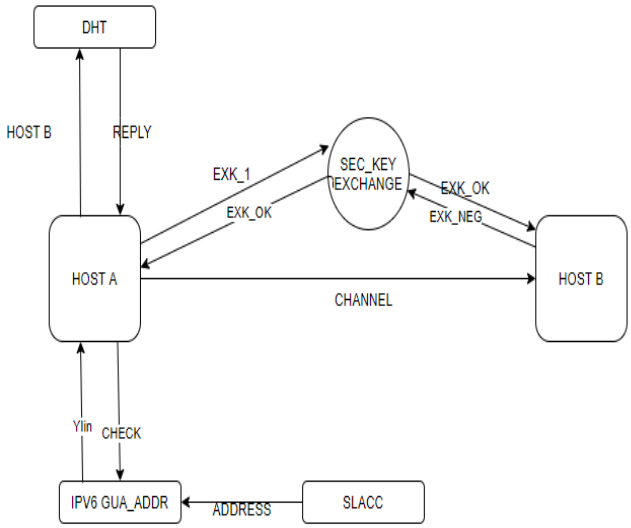

Fig1.Architecture of the model

A. *Concept of Tracker*

The Tracker uses Distributed Hash Table (DHT) for User-to-IP lookup. Technically, Tracker is built using Socket-IO and it is said to handle more requests than a synchronous model server. The communication from and to the tracker is encrypted and privacy is guaranteed.

B. *Global Unicast Address*

Global unicast addresses (GUAs), are addresses which are globally routable and accessible in the Internet version 6. GUAs start with **2000::/3** (hex 2 or 3) having 2 parts which are, the subnet ID and the interface ID.

C. *IPV6*

Internet Protocol version 6 (IPv6) is the most recent form of Internet Protocol (IP), which provides an identification and location system for computers on networks as well as routes traffic across the Internet.One of the greatest features is the usage of Internet Protocol Security (IPsec) which was developed for IPv6, but found widespread deployment first in IPv4, for which it was re-engineered. Internet protocol security(IPsec) is a mandatory part of all Internet protocol version 6 protocol implementations.

D. *Peer-to-Peer (P2P)*

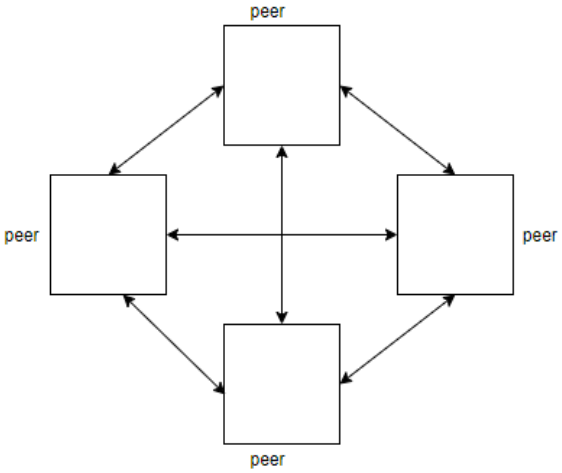

Fig 2. Peer-to-Peer architecture

Peer-to-peer(P2P) computing is a distributed architecture,in which tasks or works are assigned between each workstation(peer).All peers have equal privilege and the peers are equipotent participants in the application. In a peer to peer model, each individual node can perform as client as well as server. The username, addresses, chat history and everything is stored in a local database (client's own system).

Advantages of using peer to peer architecture

Peer to peer architecture is easy to build and maintain. It is very easy to install.Since the model is decentralized it is more reliable.For peer to peer architecture there is no need of a full time administrator.The user can control their resources,makes it expedient .So it is not necessary to have an administrator.

E. *SLAAC*

SLACC stands for Stateless Address Auto Configuration. It is a way to automatically assign an IPv6 address to the interface.It works by combining addresses from the gateway of the interface learned through router advertisements as well as the second layer of the interface. But, that is just an abstract idea.

V. RESULT

With a not-yet-complex model, we were able to develop a privacy oriented messenger. This can be made portable to work with any operating system. We ensured that ip-sec is really a protection suite in ipv6. The overall performance seems very impressive when a single socket-io connection. Since there is a need for multiple socket-io connections, WebRTC-like protocols would have been easier to deal with P2P connections. But, that would be an entirely different idea and something that is already implemented. The result of some experiments showed that firewalls are blocking and dropping socket-io connections. But, that is only happening in 3 out of

10 connections. Most of the time, there is no reason that a firewall would block inbound,outbound IPV6 packets without explicitly blocking it. Therefore our model should work fine. We have also noticed that there is a considerable decrease in bandwidth usage with this model since it is P2P.

VI. CONCLUSION

Common messengers like facebook, whatsapp, wechat etc are a real question to privacy and data security. Yet a complete safety from cyber attacks is not ensured. One of the problems we had in IPv4 was that not each individual had a public ip address when NAT was put in place. With IPV6, we have a rich number of IPV6 addresses that we no longer need to think about. Although IPV6 has all the above features, many experts argue that IPV6 is not a mature protocol since NDP (Neighbour Discovery Protocol) in IPV6 was vulnerable to many attacks. While some ISPs have not yet implemented IPV6, an IPV6 tunnel broker can be used to get one.

VII . ACKNOWLEDGEMENT

The authors wish to thank Principal Manoj George, Dr. Vinod P Vijayan, H.O.D, Computer Science Department, for the proper direction, significant help, and supportive remarks during the editing

VIII. REFERENCES

[1] Rui Zhao“ P2P File Sharing Software in IPv4/IPv6 Network” :2009 International conference on communication software and networks
[2] Minji I, Kunwoo Park, Hosik Cho, Taekyoung Kwon, Yanghee Choi, 'Taewan You and Seungyun Lee “Extended Peer-to-peer Protocol based on IPv6 ” :2005 7th International Conference on Advanced communication technology
[3] Stoica; R. Morris; D.Liben-Nowell; D.R. Karger; M.F. Kaashoek; F. Dabek; H. Balakrishnan “Chord: a scalable peer-to-peer lookup protocol for Internet applications” :2003 IEEE/ACM Transactions on Networking
[4] D. Liben-Nowell, H. Balakrishnan, and D. R. Karger, “Analysis of the evolution of peer-to-peer systems,” :2002 in Proc. 21st ACM Symp. On Principles of Distributed Computing (PODC), Monterey, CA
[5] Chen, Han-Chieh Chao and Wei-Ming Chen“Personal Internetworking Using P2P Architecture over IPv6” : 2005 9th International symposium on Consumer Electronics
[6] Wen Yen Lin,Kuang Po Hsueh and Pai-Shan Pa “ The Development of Emergency Communication APP Using Ad Hoc Network with IPv6” :2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing(IIH-MSP)
[7] Dongyu Qiu and R. Srikant“Modeling and Performance Analysis of BitTorrent- Like Peer-to-Peer Network” Proceedings of the ACM SIGCOMM 2004 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication
[8] Jiri Schafer and Kamil Malinka “Security I peer-to-peer Networks: Empiric model of file diffusion in Bit Torrent” :2009 4th International Conference on Internet Monitoring and Protection
[9] M.Ripeanu “Peer-to-peer architecture case study: Gnutella network” :2001 Proceedings 1st International Conference on Peer-to-Peer Computing