Providing Mutual Anonymity for Structured P2P Networks

R. Jennie Bharathi¹ A. T. Dharshini² J. Janani Sri³ P. Jayasudha⁴
¹,²,³ Student ⁴Assistant Professor
Department of Electronics & Communication Engineering
Sri Krishna College of Engineering and Technology India

Abstract— Peer to Peer (P2P) networks are known for their scalability and efficiency, widely implemented in transmission. P2P networks are used in sharing of files and hence preserving anonymity is very much important. There are a lot of methods to provide anonymity but these methods are only for unstructured Peer to Peer networks. Hence, we propose a method to provide mutual anonymity in structured P2P networks. With this method a more secure platform is developed for the transmission of packets between the nodes.

Key words: Tunneling, Mutual Anonymity, Security

I. INTRODUCTION

In Peer to Peer network, every machine plays the role of a client and a server at the same time. Peer to Peer network is an alternative model to that provided by traditional client server architecture. It differs from the traditional client server model where a client can only send request to a server and then wait for the server response. With a client server approach the performance of the server will deteriorate as the number of clients requesting services from the server increase. However, in P2P networks the overall network performance actually improves as an increasing number of peers are added to the networks.

P2P networks are classified into Structured and Unstructured Networks. Unstructured P2P networks do not impose a particular structure on the overlay network by design, but rather formed by nodes that directly form connections to each other. In Structured P2P networks the overlay is organized into specific topology, and the protocol ensures that any node can efficiently search the network for the file/source even if the source is extremely large. Although a P2P network has a number of advantages over the traditional client server model in terms of efficiency and fault tolerance, additional security threats can be introduced. These threats can occur due to the propagation of malicious code and vulnerabilities within P2P software.

Since the P2P networks are more vulnerable to attacks, in this paper a novel approach is provided for preserving mutual anonymity in structured P2P networks. In some of the existing methods like Agyaat, a special topology is required for preserving anonymity. But our proposed work needs no special modification and can be easily implemented. In this method, the concept of tunneling is employed to provide anonymity.

Tunneling is nothing but the process of creating a path between the nodes. A Tunneling protocol allows a network user to access or provide a network service that the underlying network does not support or provide directly. One important use of a tunneling protocol is to allow a foreign protocol to run over a network that does not support that particular protocol. Another important use is to provide services that are impractical or unsafe to be offered using only the underlying network services and a third use is to hide the nature of the traffic that is run through the tunnels.

In tunneling the data are broken into smaller pieces called packets has they move along the tunnel for transport. As the packets move through the tunnel, they are encrypted and another process called encapsulation occurs. At the final destination, decapsulation and decryption occur.

With the help of tunneling anonymity is achieved at the receiver side. By this process, the security in the network is increased. Hence this method becomes the most reliable method in transmission of packets between the nodes.

II. RELATED WORK

With the wide spread of internet applications in both the surface net and darknet, the necessity to safeguard privacy and anonymity has become more prominent than ever. There results many methods which provides secure transfer of data for P2P networks. Let us see the methods and its technical act of providing anonymity for structured P2P networks. The best way to provide security is based on defense system which actively prompts all the vulnerable acts.

Tunneling is one of the methods used for providing anonymity in P2P networks. It is also called as “Port forwarding” is the transmission of data intended for use only within a private, usually corporate network through a public network in such a way that the routing nodes in the public network are unaware that the transmission is part of a private network. Tunneling is generally done by encapsulating the private network data and protocol information within the public network transmission units so that the private network protocol information appears to the public network as data. Tunneling allows the use of the Internet, which is a public network, to convey data on behalf of a private network. One approach to tunneling is the Point-to-Point Tunneling Protocol (PPTP).

Mix-Net is a network which is used to preserve anonymity in a network. It is a routing protocol that creates hard-to-trace communications by using a chain of proxy servers known as mixes which take in messages from multiple senders, shuffle
them back out in random order to the next destination. This breaks the link between the source of the request and the destination, making it harder for eavesdroppers to trace end-to-end communications.

MorphMix and Tarzan are both fully distributed, P2P networks of anonymizing proxies, allowing people to tunnel out through the low latency mix network. Avoiding the use of secure address in onion routing, it will clump the group of nodes all together with identical identifications in order to improve fault act over churn. Crowds and Pastry are a proposed anonymity networks.

Broadcast encryption is the cryptographic problem of delivering encrypted content over a broadcast channel in such a way that only qualified users can decrypt the content. The concept of broadcast encryption scheme, the authority generates user’s private key using master secret key and each user identity, and user transmits an encrypted message through a broadcast channel. By the support of encryption and delivering messages constantly we can preserve anonymity. Then valid receiver can decrypt the message using private key.

Freenet and GNUnet are one of the popular networks used to preserve anonymity. It uses a decentralized distributed data store to keep and deliver information. The distributed data store of Freenet is used by many third-party programs and plugins to provide microblogging and media sharing, anonymous and decentralized version tracking.

Another method of providing anonymity is Friend-to-Friend network which is most promising method which serves it role at a simple manner. It uses passwords or digital signature can be used for authentication. Unlike other kinds of private P2P, users in a friend-to-friend network cannot find out who else is participating beyond their own circle of friends, so F2F networks can grow in size without compromising their user’s anonymity.

“Agyaat” –a decentralized P2P system, which promotes a generic non-cryptographic solution for mutual anonymity. Agyaat combines the best characteristics of both unstructured and structured P2P systems by providing mutually anonymous services, while maintaining the scalability and efficiency of DHT routing schemes. Compared with existing pure DHT based systems, the routing performance of Agyaat differs only by constants in both the numbers of hops and the aggregate messaging costs. Agyaat provides mutual anonymity by adding unstructured cloud topologies onto structured DHT overlays. It breaks the standard data-to-peer DHT mapping into two steps and utilizes an important feature of local query termination within cloud topologies to facilitate mutual anonymity.

However unstructured P2P systems have some lookup drawbacks. Since a query cannot be kept active in the network for an infinite period of time, it is typically prematurely terminated after a certain number of application level network hops. As a result there is no guaranteed lookup of data. Also due to the broadcast of to the broadcast of queries, the resource usage is high. This led to the emergence of a class of P2P system that include Chord, CAN, DHT based systems, the problem of mutual anonymity reduces to protecting the identities of the peer issuing the query and the peer responsible for that particular key.

III. PROPOSED WORK

In our method, we have used the concept of tunneling to achieve anonymity at the sender as well as in the receiver. Consider a network which consists of $2^m$ nodes where $m$ is a positive integer. Each node is assigned a particular identifier represented as IDi where i=0,1….(m-1). These are used in achieving anonymity in the network In case of preserving anonymity at the receiver side, the receiver sends a query to the sender from whom it needs to receive data X. The query that is sent to the receiver is usually sent in the form of a query package. The query package Qi=(X,PU(Ki),IDf) is sent to the owner of X. From the above PU(Ki) represents the Public key of the intended receiver. Here IDf represents the Identifier of the first node.

Public key cryptography is a communication where people exchange messages that can only be read by one another. In public key cryptography, each user has a pair of keys as public key and private key. The private key is kept secret while public key is widely distributed. Incoming messages are encrypted with the recipient’s public key and can only be decrypted with their corresponding private key.

Once the query is sent to the Owner of X, the sender encrypts the data X using the public key PU(Ki). After the encryption, the encrypted data X is sent to the first node as represented by the receiver in the query package.

For a network with $2^m$ nodes, the query sender usually decides the tunnel T. The tunnel T in the network is formed with the first node at a distance of $2^m-1+1$ from the query sender. So, it is clear that nf= ni+$2^m-1+1$ where nf is the first node and ni is the receiver node which requested the data X.

![Fig. 1: Achieving anonymity by construction of tunnel.](image)

From the first node the data X is traversed to the next node at a distance of $2^m-1$. This is done by reducing the exponent value by 1. The corresponding process continues till the data X is reached at the query sender. Here the receiver
assumes itself to be in the last position of the tunnel. Once the data is reached at the receiver side, the received data is decrypted with the help of a private key PR(Kj). This private key will be available only with the intended receiver.

During this process, the receiver nj need not have a direct communication with the owner of data X. So, the information about the first node will be sent to the sender in the query package Qi.

To further clarify this process, a detailed example is given. Consider a network with $2^4 = 16$ nodes. Consider n2 to be the query sender and n11 to be the data sender. Here n2 assumes itself to be in the last position of the tunnel. The query is sent as query package with the first node nf which is calculated as follows:

$2^4 = 16$

$2 + 2^{(4-1)} + 1 = 11 \mod 16 = 11$

$11 + 2^{(4-2)} = 15 \mod 16 = 15$

$15 + 2^{(4-3)} = 17 \mod 16 = 1$

$1 + 2^{(4-4)} = 2 \mod 16 = 2$

IV. TUNNELING

Tunneling is a protocol that allows for the secure movement of data from one network to another. Tunneling involves allowing private network communications to be sent across a public network, such as the Internet, through a process called encapsulation. The encapsulation process allows for data packets though they are of public nature to public network when they are actually private data packets to appear as though they are of a public nature to a public network when they are actually private data packets, allowing them to pass through unnoticed.

Tunneling is a way for communication to be conducted over a private network but tunneled through a public network. This is particularly useful in corporate setting and also offers security features such as encryption options.

In the above mentioned method, the receiver that is the query sender assumes itself to be in the last position in the tunnel. But this will increase the probability of monitoring over the network and hence in turn reduces the security in the network. Assumption of the receiver to be in the last position will increase the overhead.

To reduce the overhead, an alternative method is proposed. Consider a network with a maximum of $2^n$ nodes. According to this method, a counter is considered. Here the receiver assumes itself to be in the third position of the tunnel. At the initial step the value of counter C is initialized to be 0. The counter number increases by one unit in the following steps.

Consider position K which defines the position of the receiver. From the practical example, if K= 3, the receiver assumes itself to be in the third position of the tunnel. The corresponding calculations are made by the decision of the receiver.

$C = 1 (3 + 2^{(4-1)} + 2^{(4-3)}) \mod 2^4 = 13$

$C = 2 (13 + 2^{(4-2)}) \mod 2^4 = 1$

$C = 3 (1 + 2^{(4-3)}) \mod 2^4 = 3$

$C = 4 (3 + 2^{(4-4)}) \mod 2^4 = 4$

Thus by changing the position of the receiver, the number of overheads can be reduced. This will in turn create more complications on monitoring and hence increases the security in the network.

V. PERFORMANCE ANALYSIS

In this section we analyze the performance of our current work based on the existing infrastructure. Our proposed work in providing mutual anonymity has high security advancement, but it is not without its expense. Before implementing this work in circular networks, the cost should be analyzed carefully to handle extra overheads. In our design construction we have implemented Chord as a standard design for structured peer to peer networks. For proposed method using Peerism as a simulator tool, it provides us to manage the routing costs and overheads as well.

Firstly, extra cost of routing has been analyzed. In our proposed work we measure the probability of getting more hops. After finding an object in Chord network, connections are made directly between the nodes. As soon as the connections are made, extra nodes are searched in order to form tunnels. But as we mentioned before, tunnel size are not necessarily fixed. In order to reduce this effect the tunnel size has to be changed.

In this work experiment, the table illustrates how long the tunnel should be designed. The table contains three groups. Since we have created 1024 nodes, the tunnels can be created with the length of 9. In each group we have shown the probability of how long the tunnel can travel. In this table the probability of the first hop is taken as 100%. The reason behind this is that
the tunnel should contain at least one hop. In the table illustrated the first group has the lesser probability compared to the third group for extending its length.

![Fig. 3: Throughput Ratio](image1)

![Fig. 4: Energy Consumption](image2)

![Fig. 5: Packet Delivery Ratio](image3)

The result has been shown further. For each group, the experiment has been repeated for each stage of transactions. By doing so the extra hops are completely related to the tunnel length. In order to reduce the extra cost of the routing we need to manage the probability of the length of the tunnel for the created groups from 1 to 3.

The major concern in tunneling is that number of networks injected in the network. In such cases network shielded with tunneling has a better ability to reduce the cost of routing. In order to analyze these criteria we have developed 1024 nodes which consist of three groups. Table 1 provides the length of each tunnel. Each node consist a file size between 1 to 100 megabytes. The whole transaction and the overheads are in gigabyte. By this transaction we understand that the length of the tunnel should be chosen wisely in order to lessen the cost dramatically.

![Fig. 6: Transaction Overhead](image4)

VI. CONCLUSION

An anonymous P2P communication system is a peer to peer distributed application in which the nodes or participants that are anonymous or pseudonymous. Anonymity of participants is usually achieved by special routing overlay networks that hide the physical location of each node from other participant. Interest in another P2P system has increased in recent years for many reasons, ranging from the desire to share files without revealing one’s network identity and risking litigation to distrust in government, concerns over mass surveillances and data retention. There are two subdivisions in P2P networks they are structured and unstructured networks. There is less anonymous techniques laid on structured networks when compared to unstructured networks. This paper illustrates how to preserve receiver’s anonymity for structured P2P networks. We can implement this method by the use of Tunneling process on circular networks. Tunneling is one of the method which is laid mainly to provide anonymity for different types of networks. By the size of the tunnel overheads are decided. By choosing size of tunnel to be less cost can be reduce efficiently which is illustrated in proposed method.
REFERENCES


