Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/13S126

Onion Routing in Anonymous Network

*K. Balasubramanian** *and S. Kannan*

Department of Computer Science and Engineering, E.G.S Pillay Engineering College, Nagapattinam,Tamilnadu, India

Received: 2 Dec. 2018, Revised: 2 Jan. 2019, Accepted: 3 Mar. 2019
Published online: 1 Aug. 2019

Abstract: Communication on the anonymous network is to interact with unknown parties that give privacy and secure communication through the network. As the existing framework depends on tunnel port forwarding method that directly gives their user identity information such as ip address, an attacker can easily access user privacy data and also it uses a single server for the establishment of WebRTC connection. The single server is used by all the clients in the network it may occurs single point failure which results traffic and work burden increased. The proposed system uses peer-to-peer communication in the network as a distributed way to avoid network traffic and single point failure, for the secure communication using multiple directory servers instead of only one server. Using multiple directory servers, attacker activities can be controlled. This paper provides onion routing techniques that give secure communication and also protecting user privacy data. This routing method hides user identity information by using onion routing chain. This chain give an easy way to find and communicate unknown node in the peer-to-peer network. This work will give a secure way to communicate their unknown parties and protecting user privacy data on the anonymous network.

Keywords: WebRTC,onionchain,Tor Software,AES,Web crpto API,RSA.

1 Introduction

Nowadays, network usage is increased day by day and increased human interaction. These human activities are translated into the electronic equivalent for example voting machine, payment, email etc. To communicating the internet to enable user privacy for the secure communication using an anonymous network [1]. The communication and data security is a very essential feature in this area. This paper discussed anonymous communication and onion routing methods. These two methods are used to support user privacy, secure communication through the network.

1.1 Anonymous Network

An Anonymous is a property of network security. It gives a peer-to-peer communication, to connect unknown nodes [7]. It achieved by overlay network. For the secure communication to give hide physical location each node from other so an attacker could not easily find sender and receiver IP address the main goal is to provide low latency connection and enable the user to reach while blocking or network traffic. Till now an anonymous network on application level is supported by external application applications by instance tunnelling. Tunnelling is a port forwarding or port mapping method. This method is used to translate communication request with port number and translate the packet to the node, this packet are traversing a network gateway so increasing packet delay and burden to the network to avoid this problem to apply web technology and web standard[1] methods to an integrated class platform of the network.

In this paper we provide peer-to-peer communication on anonymity layer [6]. Our main goal is secure way of communicating their unknown node and maintains user privacy Information. In peer-to-peer (P2P) is based on mix anonymity network [6,7]. There is a mix act between sender and receiver. It enables an anonymous communication by cryptography unifying methods (padding bit, message size). The main usage it controlling traffic and it based on using the browser in WebRTC and it allows direct web-to-web interaction between their data with the web application API node by using network address translation (NAT) gateway[1]. An anonymous protocol is a lightweight method to executed node .This network interacts aware and unaware node in anonymously. For the efficient and secure way to

* Corresponding author e-mail: balasubramanian.kcse22@gmail.com

communicate their an anonymous network using onion routing method.

1.2 Onion Routing Method

Onion routing is a real-time bidirectional application independent mixed based infrastructure for private communication over a public network [3] it actively resists traffic analysis eaves dropping and hiding the identities of communication parties (sender and receiver IP address) so protecting service are increased so easily give secure communication. During the anonymous communication sender before sending the data to the receiver, data should be sending to an onion routing overlay layer .onion router act intermediate between sender and receiver[8]. It builds a sequence of a chain in this chain creates N number of nodes it is depending upon the receiver destination[3]. Initial node is connected to their sender and last node to connect the receiver. This onion routing chain does not share IP address it's creates sequence bit to communicate nearest neighbour and chain can only find immediate neighbour router node so an attacker could not easily find user privacy information.

To send the data the first onion router it creates an encryption layer for all onion routers. For an example, onion router size is n and the key for the last router k_n, for the last node encryption using a key for previous router k_{n-1} after adding encryption layer to data is sent to onion routing. This onion routing intermediate node performing encryption and last node perform decryption so the data securely arrives in the receiver as a consequence of the layering, data appeared different at each onion router so it cannot be tracked and cannot be maliciously collaborated[9]. It has two important feature one is communicating untraceable node another one is protecting user privacy information.

Onion router working:

Figure1 illustrates Onion router performing given follow description first defining a route and construct onion overlay network next connecting path to the intermediate node. The sender sends the data through onion routing with encryption techniques and after encryption, this data send to the receiver[3]. The Receiver applies decryption techniques to retrieved data in a secure way.

2 Background and Related Work

To implementing onion routing method by using Tor software [3].Tor is a distributed anonymous network, this application is used to communicate anonymous network. Tor software using a directory server it contains list of node address and entry-exit node so client easily choose

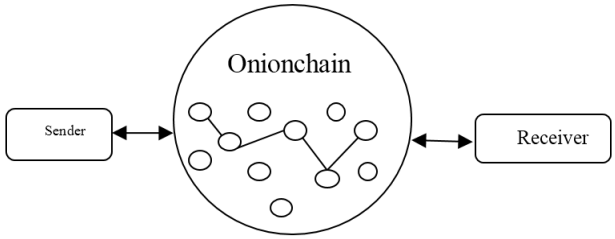

Fig. 1: Onion routing techniques.

path in network to reach destination the client connect the first node and the first node connect next nearest neighbour node to connect the last node by using node identity key so easily route the destination node .this node based on bidirectional channel to end-to-end communication so easily interact unknown node with secure communication.

David chaum [2] it implements onion routing method is composed onion routing chain it compares to [3] the client locally installed onion proxy node is easily accessed directory server. Each node must be registered after the build chain with sequence number after forming routing chain to an established connection to the network.

Jain[1] sender want to communicate anonymously with particular receiver node to interact their node using public key encryption standards. This connection is enabled anonymous connection identifier. It enables onion routing chain. This chain sent data from the client to receiver before sending data must be encrypted using the public symmetric key.

[4,5] provide bidirectional communication through an anonymous network so easily connect End-to-End communication. It enables request-response interaction with enabling WebRTC connection to communicate the web data and transfer audio, video data. And also support mobile web browser to exchange their data. This API channel is to set up peer-peer overlay network and directly communicate to their node so no need to install any software installation.

MorphicMix [6] is peer-peer connection based on mix anonymous communication this application rely on TCP stream it focused on peer-peer communication. Once the connection is established Web RTC. It directly connects to address translate using Network Address Translation gateway to enable directory connection. Traditional mix based system is a small set of static, reliable and difficult to handle network traffic. It suffers scalability problem, so using MorphicMix,a system for peer-to-peer communication. It easily joins to the network so overcome network delay. But it introduced new challenge. An attacker can easily find an anonymous path and try to break the network path. to counter this attack we have used collision detection mechanism.

WebRTC[10] for peer-to-peer distribution in a web browser it enables the web application to direct

communication channel between two peers without relaying through a web server. It contains API defined by W3C and set of the protocol defined by IETF RTCWEB.it used to establish peer-to-peer communication.

3 Architectuure

The goal of the work is to make an anonymity network of communicating unknown node. The secure way of communication unknown parties in anonymity network mainly focused on web-to-web communication this done by onion network it performs hide the user identity information (IP address) by using onion routing chain method [8]. For the security purpose, this chain creates three nodes each node shared public key by using cryptography techniques. Each node shares the information in a bidirectional way so each node has information only predecessor and successor so an attacker cannot easily hack user information data. Performing an anonymous communication client sends the data to onion network. Onion router to create onion overlay node this contains three nodes. Initially, onion chain is established chain group. In the first set of the chain choose nodes to connect destination after choose the node client sends the data to first node this node called entry node this client and entry node interaction secure way using public shared key. So this node shares their data by using the public key encryption. This will subsequently be used for communication within the onion chain. The first node to send the data to the next node this two node shared data again using the public shared key. This node called intermediate node. This process is continued until find destination node after finding the last node the intermediate nodes send data to the last node is called exist node. This node shared information to the destination using a public key. After data reach their destination receiver send the data to the client using decryption techniques using the bidirectional request response method [7].

Figure2 illustrate how onion routing message sends through the anonymous network in order onion chain protocol stacks split into three stacks, this protocol stack consists of three-layer, namely communication layer, onion layer, end-to-end communication layer.

The communication layer is used to communicate an unknown node. This is based on peer-to-peer communication to transfer data between two nodes. Before the communication, each node must register the directory server is also called register point [9,10]. This server maintains the address of each node. Client request to their directory server and the server gives connection to

an onion overlay network that creates onion chain. This chain contains onion router node. Each node to connect nearest neighbouring node by using sequence identifier number these numbers is stored in the directory server. These interactions enable by onion router each node contain only nearest node information and does not

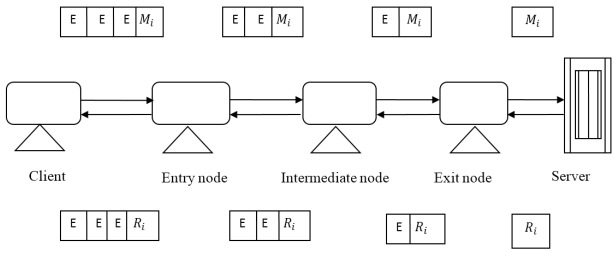

Fig. 2: Flow of onion message.

directly shared user personal information so attacker not easily accesses their data. Handling disconnection of an individual node is critical. To this end, whenever a node disconnects from the network it is necessary to rebuild the chain. This is done by fully automatically to perform by using Tor software, to avoid delay performance every node to perform encryption and decryption should be done in parallel.

Figure2 describes a flow of onion routing information. Message M_i sends from client to destination every node encapsulated in the layer of encryption. And the response R_i message from destination to client each node adds decryption the layer through an onion routing chain [3,8].

Figure3 indicates End-To-End communications enables to connecting two onion chain routing layer. It allows anonymous connection to the two exit onion node. it provides sender and receiver exchange the data through anonymously. It easily communicates two exit nodes. Therefore it is necessary to apply an additional an encryption layer in the end -to-end communication[4]. Otherwise, the data may be hacked by third parties so enable security properties during anonymous communication to implement that high level abstraction.

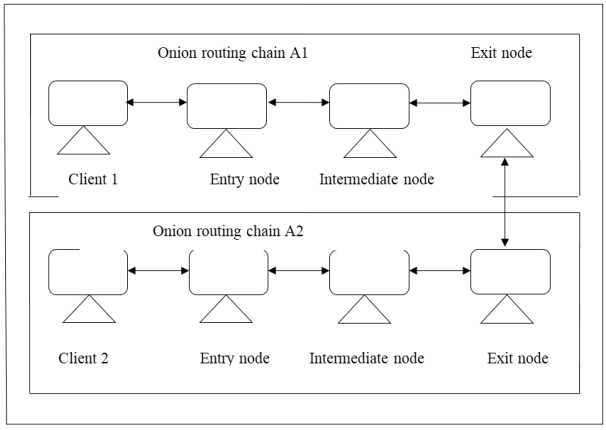

Fig. 3: End-To-End Communication.

4 Implementation

As this paper will be provide proof of this concept of implementing an anonymous network by using AJAX language. This library enables data exchange of two nodes via end-to-end communication. During the anonymous communication, the client can directly communicate the receiver node without any software installation process. This process implemented by Web standard and technology[5].

For the applying cryptographic techniques, the web browser first builds cryptography API (Web Crypto API) and this API provide indirect an interface to apply cryptography in the web application without requiring the additional library. This Web crypto API [4] enables all browser including a recent version of mobile web browser, this crypto techniques added security properties it's done by cryptography encryption and decryption. It allows asynchronous performance without blocking and tracing.

4.1 Communication Layer

The communication layer is an efficient way to exchange their data in the web browser this layer an enabled peer-to-peer communication to transfer data and keep up connection state is alive. To transfer data from one node to another node using WEBRTC API [4]. To make sure the encryption communication through anonymous communication enables Transport Layer Security (TLS). It's based on Stream Control Transmission Protocol (SCTM) and Datagram Transport Layer Security (DTLS) to exchange their data in two peers and maintain proper connection this layer enables two technologies.

Signalling:

This signalling helps to suggest how a new peer connects to their directory and how to established connection to their node [7]. Every node is using bidirectional connection to connect to their entry-exit node .their signalling server using Web Socket. Each node registers signalling server and saves the information to the server. The server responds the request based on their IP address. if the peer want to connect to another peer it should be registered signalling server this server established the connection to a particular node using WebRTC API [4, 5].it enable to communicate with a web browser and transfer data in audio, video media format and also connect mobile browser application easily.

Data channel communication:

After peer register signalling server WebRTC is established the Data channel communication. This channel manages to send and retrieve data function. WebRTC is used to send their data to the browser. This data send to the different browser so the limitation of data size is significant because this data size is varying different browser so before sending the data must be split the data. it must be smaller than the maximum capacity of the channel. The data should be concatenated before sending the destination node to the data channel must be maintained below the threshold value of buffer so avoid overloading data and traffic problem. If above the threshold value this buffer can be an overload so data error has occurred so peer could not communicate another node so data channel will be closed .so before sending their data should be split the data to send data channel communication.

4.2 Onion Layer

If the node wants to join onion routing layer this node should be resister directory server this server maintains the list of node all client can retrieve this node so the client can use all node list so easily build the overlay onion chain. In single directory server is handling more difficult because occurred single point failure and cannot handle attacker activities. Instead of one directory server using multiple directories this paper provides to build multiple directories .this help of handle attacker so an attacker cannot route all traffic node .as the node list would contain node information in a different directory server. Before sending the data to destination all nodes must be registered directory server by using the public key [8]. Each node contain socket information and public key in additionally add section identifier because onion router cannot directly share IP address for the security purpose it hides the user information to each node share sequence identifier number so the third party cannot find user information.

Chain builds up:

Initially each node generates session RSA key this pair of key based on cryptography security for the node within onion network. First each node register directory server using the public key, next client connects to the onion router. This onion router builds routing chain. These chains randomly select three nodes, first node is entry node and next neighbour node is intermediate node and the last node is an exit node. This exit node connects to the receiver.

These node bidirectional ways communicate all request and response node. For selection, each node with in chain keeps up 128-bit AES key generation. It wrapped with the public key RS-key pair of the node. AES-key maintains socket of information of the next node and enables node encryption and decryption [7]. Each node

maps its own sequence identifier number to communicate to the next nearest neighbouring node. This sequence number is initially zero. Using a race condition duplicate sequence number is avoided.

$$Secure\ ID = H\,(Identifier||sequence\ number)$$

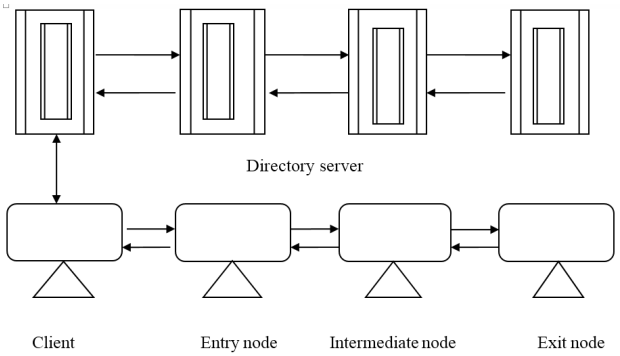

Fig. 4: Multiple Directory Servers with Sequence of Onion Chain.

Each node sending the data to chain this chain has identifier node number and mapping its sequence number. Here H is a hash function it has the list of a node and its sequence number so easily handle mapping function. If the node cannot connect next sequence address that the node should be pre-computes the hash function.

Node communication:

In the client side, each node must encrypt the data and sharing the data in the chain using the shared public key, each encryption layer is subsequently removed from the message on each node by decryption payload. Once the message is received the destination to do decryption techniques to the retrieved node. Here IVN (initialization vector number) is contain node address, each node shared public key $e_k, k = 1,2,3$ (three node). These key permutation next sequence number so used synchronization point for received message, it handle synchronization queue to stored receiving information so easily verified identifier number[3]. Example layered encryption and decryption for chain using three nodes.

$$Encryption\,(ENC) = (IVN_1, e_{k1}\,(IVN_2, e_{k2}, (IVN_3, e_{k3}(M))).$$

$$Decryption(DNC) = (IVN_3, d_{k3}\,(IVN_2, d_{k2}, (IVN_3, d_{k1}\,(M)))).$$

To avoid attacker to link cryptography encrypted payload with sequence number this encryption and decryption done by parallel, for the more secure communication and add extra data using MAC address (message authentication node) is concatenation of sequence number, chain id, encryption key payload) for decryption contain (sequence number, chain id, decryption key) its handle message and verification node address by the receiver.

Encryption function:

$$MAC = H\,(sequencenumber\,||chainid||\,encryptionkey)\,.$$

Decryption function:

$$MAC = H\,(sequence\ number\,||chainid||\,decryptionkey)\,.$$

Failure Recovery:

Operating the onion chain during the browser implementation to occurred failure mode due to disconnected to their node. So onion chain used message type of error. This message error produced build error, chain error, message error, node error. So easily find disconnection node. So easily rebuild the new connection to invoke the new build up chain.

Tear Down:

After finished sender and receiver communication client close onion chain to sending the close message through onion chain each node receiving the close message so each node clear the information it's done automatically.

4.3 End-End Communication

Figure 4 illustrates the structure of how the two onion chain connection through onion routing network. This end-to-end communication will give (intra–chain) communication and (inter-chain) communication. Intra-chain describes how the two onion chain group connection in the network and inter-chain describe how the individual chain connection[7]. When the client wants to send the data to receiver client must be connected to onion routing layer this connection is called end-end communication. To communicating their data in outside channel to interact in secure way client encrypt the data with RSA keys, in inside channel communication using AES encryption.

Connection Establishment:

The build-up of the connection between each node using the public key, each node contains identifier number so easily map client and node, and receiver. Here using Ek_n denotes the symmetric key generation and Dk_n is d is denotes decryption symmetric key which is wrapped to connect remote client using the asymmetric public key. CK_{pubA}, is denote local client key information, the connection identifier id is ID, the socket information is SI_A and public chain information is $PCID_A$ and the remote client key information is CK_{pubB}, public chain information. $PCID_B$ and socket is SI_B. when the exit node of the local chain it message to remote client so apply end-end communication to their onion routing network to passing data to next node by using node identifier [7,8].

Once the message is sent to the remote chain and it received by the remote client to apply symmetric key using corresponding node private key .after encryption payload performing each node is decrypted the data in the same way. Remote node sends the information to local the client using the public key .if receiver response to local exit node, it used the public identifier number, in order to forward the message back to the remote client through onion layer[9].

$$ENY = \left\{E_{kn}\left(CK_{pubA}, SI_A, PCIA_A, ID\right), E_{kn}\left(CK_{pubB}, SI_B, PCIA_B, ID\right)\right\}$$

$$ENY = \left\{D_{kn}\left(CK_{pubB}, SI_B, PCID_B, ID\right), E_{kn}\left(CK_{pubA}, SI_A, PCID_A, ID\right)\right\}$$

Communication:

Sender sends data to the end-to-end connection using symmetric key encryption .after receiver receiving the data end-to-end connection using decryption symmetric key. The connection specific data consist of sequence number and identifier and the message. So it is easy for the end-to-end communication through the network. This system provides reliable connection it handles acknowledge message.

Failure Recover:

During the end-to-end communication if the any one the node is a failure the chain must rebuild the chain. for the example in remote chain node occurred failure the node inform all other nodes with help of public node. once the chain received the rebuild information to the local chain so rebuild new onion overlay chain.

5 Evaluation

Performance evaluation

To evaluate the anonymous network performance are based on below criteria.

1.File download: AJAX file downloading function used to retrieve file of various size through onion routing method. Figure5 is illustrates retrieving file using onion routing peer-to-peer communication. Direct file downloading is average time of 63 ms$<$1 msits varying from different sites. Its send large amount data required WebRTC connection to send the data.

2.End-To-End Latency:

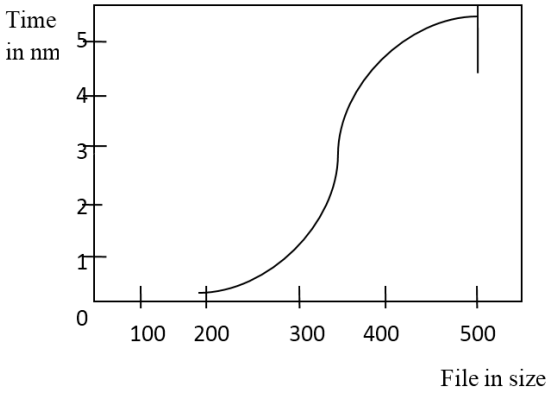

Fig. 5: Performance evaluation curve.

To test performance using of four browser tabs, for the example two tables were used clients, each client node build up chain using to connect another remaining node this node is intermediary node. The client A send message to B, who again replied process with text message this process is repeated until the node reached the destination.

3.CPU load: To measurements of CPU performed in section $v-A2$ the CPU it measurement are done by "pidstat" tool. This measurement handles two state there is idle and execution. CPU load are shown in given below table (1).

6 Conclusion

In this paper we followed peer-to-peer communication with the focus on interoperability and usability of Web technology and standards through the anonymous network, to enable communication between unknown parties in anonymous network using onion routing method. Our proof of concept is implementing onion routing method with cryptography techniques, as it provides secure way of communication and it hides user identity information. Hence it is easy to maintain user privacy data. Maintaining multiple directory servers instead of one is controlling the attacker activities. Our work approach is for an efficient and secure way to communication unknown node through the anonymous network.

Table 1: Average CPU Load browser processes in various states.

BROWSER	IDLE	EXCECUTION
Tab 1	2.45(%)	12.84(%)
Tab 2	0.65(%)	24.79(%)
Tab 3	0.77(%)	18.65(%)
Tab 4	0.72(%)	28.05(%)

References

[1] Jian Ren, Tongtong LI, Yun LI Anonymous communications in overlay networks, IEEE Secure Communications Conference 2008.

[2] David Chaum,Untraceble Electronic Mail Return Address and Aigital Pseudonyms COMMUNICATION OF THE ACM, 24, 84-88,1981.

[3] The Second-Generation Onion Router Using TOR , Roger Dingledine, Nick Mathewson, PaulSyverson, IEEEInternational Conference on 2014.

[4] Pooja Birajdar, Sagar Soni, Nandkishor Surashe, Vishal Telsan, Restriction System For Communication of Browsers in Web-RTC IJCAT - International Journal of a Computing and Technology, Volume 3, 3, March 2016 .

[5] WillemDeGhroef, Deepak Subramabnian, Martin Johns, Ensuring endpoint authenticity in WebRTC peer-to-peer communication, IEEE International Conference 2016.

[6] Marc Reinhardt and Bernhard Platter, Introducing Morphix:Peer-to-Peer Based Ano-nymous Internet Usage With Collusion DetectionNewYork,NY, USA, 2002.AMC.

[7] FlorianBurgstaller, Andreasderler, Stefan Kern, Anonymous Communication in the Browser Via Onion Routing, IEEE International Conference on P2P Network on 2015.

[8] R.David,AniketandIanGoldberg,Using Sphinx to Improve Onion Routing circuit Construction, IEEE International Conference on 2014.

[9] Paul, F.Syversonand David, M.Goldschlag, G.MichaelReed, Anonymous connection and Onion Routing, Saarland University Germany on 2002.

[10] Michael Backes, Jeremy Clark, Peter Druschel, AniketKateandmilivojsimeonovki Introducing Accountability to Anonymity Networks, IEEE International Conference On 2013.

[11] Bogdan Davidoaia, Leordeanu,Valentin Cristea, Anonymity of Web Service Inovation, IEEE 10th International Conference (ICCP) 2014.

K. Balasubramanian received the B.Tech Information degree (2005) and M.E Computer Science and Engineering (2010) degree from Anna University Chennai. Pursuing Ph.D in networking domain in part time mode in Anna University, Chennai. Life Member in ISTE Membership No:LM78595. Member in International Association of Engineers Membership No: 167642.

S. Kannan is a Professor of Information Technology at EGS Pillay Engineering College at Nagapattinam. He holds MS in Information Technology from Bharathidhasan University at Tiruchirappalli, ME in Software Engineering at Periyar Maniammai College of Technology for women, Anna University Chennai and PhD in Computer Science and Engineering from Manonmaniam Sundaranar University at Tirunelveli. He special interests include Business Intelligence Systems, Data Mining, Wireless Sensor Network and soft computing