A Survey on I2P Crypto Mechanism

[1] Miss. Dipal Vashi, [2] Mr. Girish Khilari
[1]IT Systems & Network Security,
[1]Gujarat Technological University, Ahmedabad, India

***Abstract* - The 'Darknet' is a part of the deep web as its contents are not accessible through search engines. But it is also anonymous cyber space. This anonymity is usually achieved using TOR-The Onion Router. Another darknet system (or 'privacy network') called I2P is growing in popularity. Although many users use TOR, there appears to be a precise shift towards I2P. I2P is original short for "Invisible Internet Project" which offers a range of improvements such as email, file sharing & storage plug-ins and other social applications like blogging and chatting. All information is wrapped with many layers of encryption (like AES). In this paper we will study TOR, I2P, and existing I2P Crypto. This study will help us to provide more security to identity of I2P hosts and users and also to find mechanism to avoid the attacks that can compromise the anonymity.**

***IndexTerms* - Darknet, Anonymous Network, TOR, I2P, I2P Crypto, Encryption Mechanism**

I. INTRODUCTION

A Darknet is a hidden network. It is a routed allocation of IP address space that cannot be discovered by any usual means. It is used to refer to both a non-public network and the collective portion of Internet address space that has been configured in that manner. Tor, Freenet and I2P are popular software used to access darknet. You can access darknet sites only if the traffic is routing through anonymizing networks (like TOR and I2P). Another purpose of darknet is to provide a venue for private communication when public communication is undesirable, dangerous or not permitted.

I2P is an anonymous network. It is a network within a network. It is supposed to protect communication from monitoring by third parties such as ISPs. I2P is used by people who care about their privacy: activists, oppressed people, journalists and whistleblowers, as well as the average person.[8]

This paper organized as follows: Section II briefly discuss about Invisible Internet Project. Section III describes The Onion Router (TOR). Section IV discusses existing Crypto Mechanism. Section V draws some conclusions.

II. INVISIBLE INTERNET PROJECT

There are several concepts for understanding working of I2P Protocol.[5]

The netDb : I2P uses the netDb as distributed database. It is only maintained by superpeers (floodfill peers) and it contains all needed information to make the network operate.

Two types of information are stored in netDb :

- ***routerInfo*** entities, which contain all the information needed to contact a particular router.
- ***leaseSets***, which give details of particular destination, which contains all information needed to contact the destination.

Tunnel : They are unidirectional path through several routers, which means that the sending path and the receiving path are different. (for example Bob and Alice want to communicate through I2P, they actually require 4 tunnels). After a definite quantity of your time, tunnels get expired. Tunnels are checked every time to get rid of failing tunnels. The default lifetime is set to 10 minutes. The length of a tunnel hop varies accordingly. Tunnels can be exploratory or client. There are two type of tunnels. One is inbound and the other is outbound tunnels see Figure 1 that is proposed by I2P.

Inbound and outbound tunnels are automatically built when I2P is started. It is also important to notice that connections to tunnels are only valid for nodes (systems) over which I2P has an installed paths.

Working of I2P Communication : Once the messages are sent, to anonymize them each client has their I2P router build a few inbound and outbound tunnels - a sequence of peers that pass messages in one direction to and from the client, respectively.

In other words, when someone wants to send a message to other one, the peer passes that message out one among their outbound tunnels targeting one of the other peer's inbound tunnels, finally reaching the destination. Every participant within the network chooses the length of those tunnels, and in doing so, makes a tradeoffs between anonymity, latency, and throughput in keeping with their own needs.

For The first time when a client wants to contact with another client, they send a request query to the fully distributed "network database" - a custom structured distributed hash table (DHT) which is based on the Kademlia algorithm. This is often done to find the other client's inbound tunnels efficiently, however subsequent messages between them usually includes that data so no further network database lookups are required.

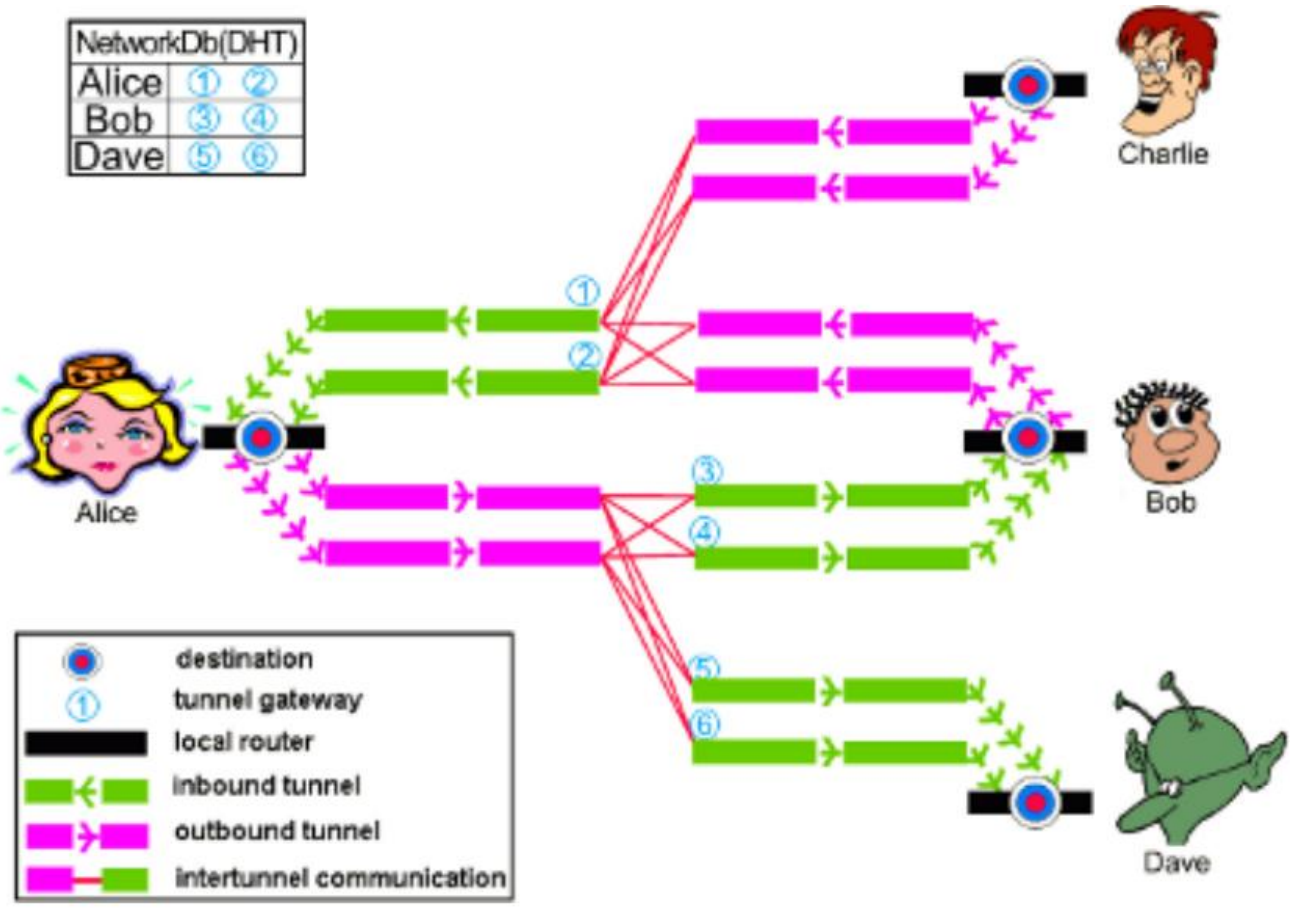

Figure 1 I2P Tunnel Overview[8]

III. THE ONION ROUTER

Originally, TOR was developed with the primary purpose of protecting government communications. Tor is stands for "The Onion Router". Today it is being used widely for different purposes by common people, the military people, law enforcement officers, journalists, activists and many others. It's use is intended to protect the privacy of users as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.

How does TOR work?

The term "onion routing" refers to application layers of encryption, nested like the layers of an onion, used to anonymize communication. Including the destination IP address, TOR encrypts the original data multiple times and sends it through a virtual circuit which contains successive, randomly selected TOR relays. To reveal only the next relay each relay decrypts a layer of encryption in circuit, in order to pass the remaining encrypted data on it. The last relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing or even knowing the source IP address.[9]

Major Weakness of TOR

- TOR cannot protect against traffic monitoring at the boundaries of TOR networks.
- **Exit node eavesdropping :** As Tor does not encrypt the traffic between an exit node and the target server, any exit node is in a position to capture any traffic passing through it that does not use end-to-end encryption such as SSL or TLS. So anyone can do MITM at the end of the TOR network
- **TOR exit node block :** Operators of Internet sites have the ability to offer reduced functionality to Tor users.

IV. EXISTING I2P CRYPTO

The cryptographic algorithms used within I2P are reduced to minimum to deal with the need of the system

- Symmetric Algorithm
- Asymmetric Algorithm
- Signing Algorithm
- Hashing Algorithm

For various types of communication I2P uses different cryptographic algorithms in a layered way. It uses following communication levels:[2]

1) Inter Router Communication
2) Tunnel Messages
3) Garlic Messages.

1) ***Inter Router Communication :*** The lowest level of communication between routers is inter router communication. Routers select an short-lived session key through Diffie-Hellman exchange. By using router's DSA key each router authenticates to the next router. A hash of each packet is used for local integrity checking.
2) ***Tunnel Messages :*** Exchange of messages are done at middle layer of the I2P stack. Tunnel messages use their own AES256/CBC encryption with an explicit IV and passed over the transporting routers. Verification of messages is done at the tunnel endpoint with an additional SHA256 hash.
3) ***Garlic Messages :*** It is top layer of encryption which combine the full path. It is uses another encryption sceme. Messages are passed in the form of garlic which are encrypted with ElGamanl/AES+SessionTags. Contents of a single message contains multiple cloves of garlic. Cloves contains messages with instructions for delivery. The client's router put message into a garlic, encrypt it to ElGamal public key published in receiver's leaseset and forward it through the appropriate tunnels. The delivery instructions are attached to each clove includes the ability to request that clove be forwarded locally to router or tunnel.

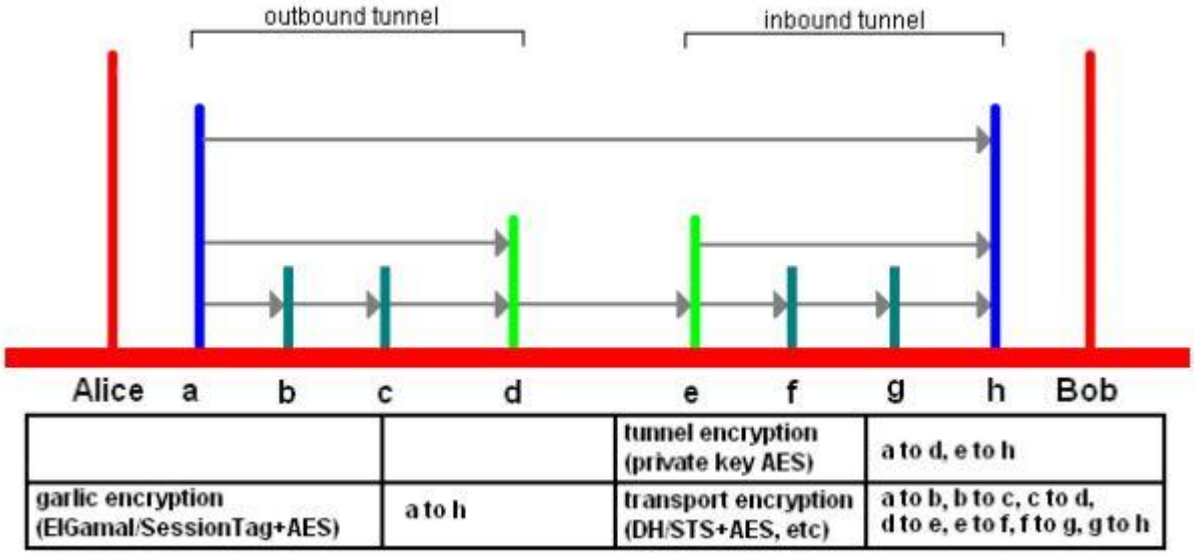

Figure 2 Encryption Layers in I2P

V. CONCLUSION

Based on the study it can be concluded that, traffic in I2P is encrypted in layered approach. Each & every router (peer) has to encrypt and decrypt incoming and outgoing traffic. It's tedious task for every router to encrypt & decrypt. It may be vulnerable for traffic analysis attack.

So from the analysis we can think to provide more security to I2P by integrating SSL in it so that from the beginning traffic can be flow in encrypted secure format. Currently I2P is not allowing secure traffic. It does not pass HTTPS traffic. If we use SSL in I2P, It will increase performance and improve security.

VI. ACKNOWLEDGMENT

I wish to express my heartfelt appreciation to all those who have contributed to this survey, both explicitly and implicitly, without the co-operation of whom, it would not have been possible to work on this.

REFERENCES

[1] Gildas Nya Tchabe and Yinhua Xu,"Anonymous Communications: A survey on I2P",CDC Publication Theoretische Informatik - Kryptographie und Computeralgebra (https://www.cdc.informatik.tu-darmstadt.de), 2014.

[2] Iwan Hoogendoorn, Tarik ElYassem and Joris Soeurt," Further reducing the anonymity set of web servers hidden within the I2P network", December 23, 2011.

[3] Sk. Subidh Ali and Debdeep Mukhopadhyay,"A Differential Fault Analysis on AES Key Schedule using Single Fault",pg. 35 – 42, Workshop on Fault Diagnosis and Tolerance in Cryptography,2011.

[4] Larry D. Bisel,"The Role of SSL in Cybersecurity", pg. 22 – 25, IT Professional (Volume:9 , Issue: 2)The IEEE Computer Society,March | April 2007.

[5] Peipeng Liu, Lihong Wang," Empirical Measurement and Analysis of I2P Routers", VOL. 9, NO. 9, JOURNAL OF NETWORKS,September 2014.
[6] Li,Bingdong,Erdin,Esra,Gunes,Mehmet Hadi,Bebis,George,Shipley,Todd,"An Analysis of Anonymity Usage",June 2011.
Websites:
[7] Darknet , http://searchnetworking.techtarget.com/definition/darknet.
[8] The Invisible Internet Project , https://geti2p.net/en/.
[9] TOR, https://www.torproject.org/