Computer Networks : Group 1

TORSA

CH. Sree Ram Sreekar
Akshita Mittel

Internet Anonymity

- Internet anonymity applies to any interaction a user has on the Internet that protects his or her identity from being shared with another user or with a third party.
- This also means to ensure that your activities cannot be traced back to your IP address.

Applications of Internet Anonymity

There are several applications of Internet Anonymity, some trivial yet others excessively crucial. The vast range of applications that incorporate internet anonymity include:

- Anonymous blogging and posting (Twitter).
- Forums that allow anonymous exchange of questions and answers.
- Secure Billing; allowing users to purchase items online, without having to reveal any personal information (PayPal).
- Anonymous peer-to-peer file sharing. This is one of the main examples that has been projected in this document.
- It plays a vital role in many military applications to ensure that intercept-able data is passed along in a secure manner. In fact this is the very purpose for generation of TOR.

Computer Networks

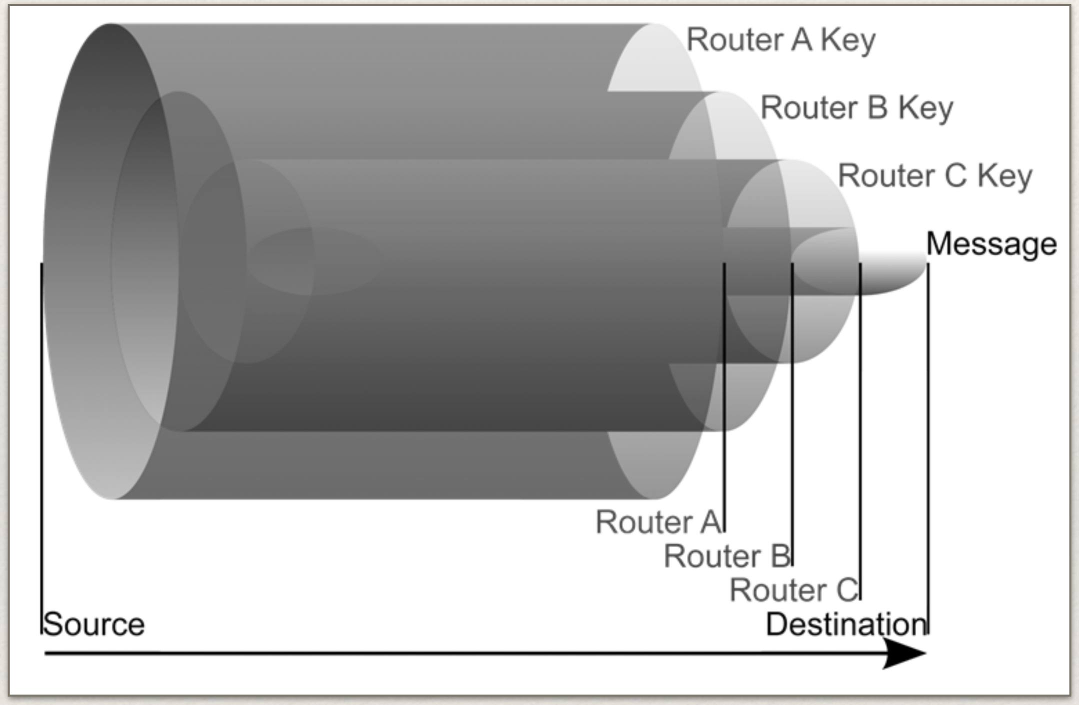
Objective

The main objective of this project is to design and implement the second generation Onion Routing protocol between two users, through a TOR network.

This network assists in masking the message of the sender, so that neither the message nor information regarding both the final participants of the transaction can be intercepted by any third party.

In order to establish legitimacy and uniformity, the distribution of keys and routing algorithms are centralised through an authoritative proxy.

Onion Routing



To initiate a communication, a simple plaintext message is encrypted (wrapped) with successive layers of encryption (onion) such that each layer can be decrypted (un-wrapped) by one intermediary (node or router) in a succession of intermediaries in the path taken by the onion routers (circuit). The message transmission is accomplished as follows:

- The sender picks nodes from a list which provide a path for transmitting the message.
- Using asymmetric cryptography, the sender encrypts the message with the public keys of the chosen nodes which are obtained from an advertised list.
- As the message passes through each node, a layer of encryption is removed by the receiving nodes (by using their private keys) until it reaches its destination.

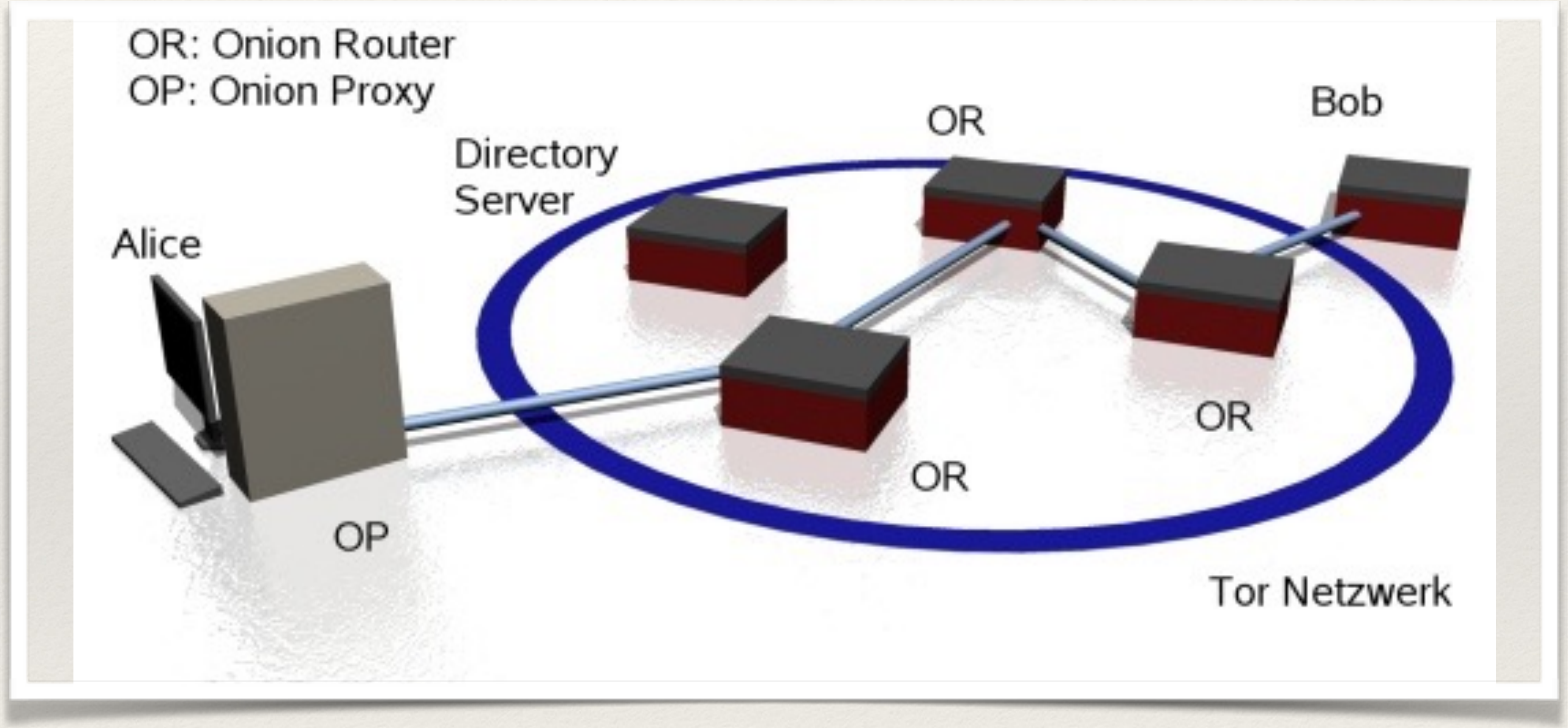
The TOR Network

An Example:

Suppose Alice wants to send Bob a message anonymously….

The Components

1. APP-PROXY
2. CLIENT
3. ROUTER
4. SERVER
5. ROUTING TABLE



Key Transfer and encryption

Index	0	1	2	3	Bob
Router	1	2	3	4	Server
Key	A	B	C	D	E
Message	A,2				
	A[B, 3]	B, 3			
	AB[C, 4]	B[C, 4]	C, 4		
	ABC[D, des]	BC[D, des]	C[D, des]	D, des	
	ABCD[S, des]	BCD[S, des]	CD[S, des]	D[S, des]	S, des

The Pros of the implementation

There are three main aspects that the TOR networks aims to tackle, these include:

- **Mask-ability:** Ensuring that Alice and Bob can communicate with one another secretly. This includes both their identities and the messages that are transferred between them.\

- **Accountability:** In order to vouch for the integrity of the system, the distribution of keys, the main encryption/decryption are done in the Authorised server itself. It is here that the routing algorithm is decided.

- **Conceal-ability:** In a conventional routing algorithms, packets can be transmitted over a arbitrary number of nodes and are prone to interception of the messages. This can be avoided completely. One of the prerequisites for the Onion routing algorithm is that it predefines the path taken by the packet, and encrypts it accordingly, thereby eliminating the opportunity for a third party to interfere with the transaction in any way.

The Results

- Based on our implementation strategies, we decided to use both performance based and security based metrics to analyse and test the feasibility of our system.

- We made extensive use of Wireshark in order to monitor and capture the flow of packets being transmitted and to analyze the structure of each packet to determine if any useful information could be obtained.

Conclusion

- From our simulations and demonstrations, our routing protocol was able to mask the contents of a transmitted packet, conceal the identity of the users (senders and users) while ensuring that the messages were only sent via authorized nodes.

- However, the application was plagued by a number of issues during the implementation phase. The complexity of implementing such a protocol is extremely high due to the multiple layers of encryption involved. This proved to be an additional challenge to our routing strategy as RSA algorithms are time consuming and hence, having an impact on the reliability of the network while trying to pick a route.

THANK YOU