Full Name: Shujun Bian

Student ID: 903172758

Paper: 8.2 8

Title of the paper you choose to critique: Onion Routing for Anonymous and Private

Internet Connections

Because the simple application of cryptography within a packet-switched network can only hide the messages being sent, but can reveal who is talking to whom, and how often, which means any malicious user or hacker would know who is talking to whom and try to get the message through bunch of attacking method like man in the middle attack and so on. We need to find out a way to hide all the information in order to avoid the traffic analysis, so the Onion Routing, as a traffic analysis resistant infrastructure, comes out, which provides anonymous connections that are strongly resistant to both eavesdropping and traffic analysis.

The new idea and important points in this paper included as followings. 1. The connections are bidirectional, near real-time, and can be used for both connection-based and connectionless traffic. Through the distributed, fault tolerant, and under the control of multiple administrative domains onion-routers, the network becomes really strong and tracking one single onion-router cannot compromise user’s privacy. 2. Also through numbers of such onion-routers makes traffic analysis even more difficult. 3. Another important idea is that Onion Routing's anonymous connections are protocol independent in three parts: connection setup, data movement, and connection tear-down. So in this way, Onion Routing provides more protection. 4. Onion Routing's overhead is relatively small, which has no delay associated with normal web connection. 5. Onion Routing could mesh well with a wide variety of operational and policy environments because it has different component like Proxies, Onion Routers. In short, Onion Routing is a traffic analysis resistant infrastructure that is easily accessible, has low overhead, can protect variety of applications, and is flexible enough to adapt to various network environments and security needs.

For the extension, one natural extension could be the introduction of reply onions, which allows connections to be made back to an anonymous sender through the Onion Routing network. One way to use this extension is to reply previously received anonymous email anonymously.

Full Name: Shujun Bian

Student ID: 903172758

Paper: 8.4 2

Title of the paper you choose to critique: TrustMe: Anonymous Management of Trust Relationships in Decentralized P2P Systems

With the decentralized Peer-to-Peer (P2P) networks increasingly gaining acceptance on the Internet, both pros and cons comes out too. The malicious users could take use of its open and decentralized nature to do some malicious things like spreading harmful content like viruses, trojans or waste valuable resources of the network. There is rarely any method to prevent this threat or to punish such malicious users and no accountability of a peer for providing a particular resource. That’s why we need a trust measurement system or an anonymous management of trust relationships. And in the paper, there are some problem attempted to be answered like where should the trust value of a peer be stored and how to securely access other peers’ trust values?

The new idea and important points in this paper included as followings. 1. In order to construct such trust management, we could dynamically assign each peer a trust rating based on its performance in the network and store it at a suitable place. Then any peer wishing to interact with another peer can make an informed decision based on such a rating. 2. Then a secure and anonymous underlying protocol for the trust management, TrustMe, which provides mutual anonymity for both the trust host and the trust querying peer is presented in the paper. 3. The distribution and access of trust ratings should be distinguished from the routine functions such as file inquiry and downloading performed in a P2P system. 4. The most three important properties of TrustMe are security, reliability, and accountability. 5. Because of its greater robustness against malicious groups acting together, most of current work, including TrustMe use the user-based rating instead of Transaction-based rating, which causes some drawbacks and I have put those drawbacks in the third paragraph. 6. Some details in the protocol: Each peer is equipped with a couple of public-private key pairs and the trust values of a peer B are randomly assigned to another peer, which is unknown to all peers. And all the peers communicating with that peer would be knowledge the truest value of peer B. So if a peer A would like to know the trust value of peer B, then it would query and the peer that is assigned the peer B’s trust value would reply.

Because the TrustMe use user-based rating approach, which causes some drawbacks mainly are no persistence, no anonymity, and tedious decision-making. Also there are some future works including exploring various other cryptographic primitives which can be more efficient as compared to public key cryptography