A Protocol for Peer-Peer System to Provide Anonymity

Neetha Thomas*

[*] CSE Department, Calicut University, India

Abstract- Peer-to-peer (P2P) systems can be used to share files, telephony, discussion forms, and streaming media. In Anonymity Peer-to-Peer (P2P) networks, many systems try to mask the identities of their users for privacy considerations. Existing anonymity approaches like Onion routing, Tor, Crowd are mainly path-based: peers have to pre-construct an anonymous path before transmission. If any peer leaves then whole path fails. Maintaining and updating such paths is difficult. Rumor Riding (RR) is a lightweight and non-path-based mutual anonymity protocol for decentralized P2P systems. Employing a random walk mechanism, RR takes advantage of lower overhead by mainly using the symmetric cryptographic algorithm. This paper is literature survey of rumor riding with existing systems.

Index Terms- anonymity, mutual anonymity, non-path-based, peer-to-peer, random walk

I. Introduction

In P2P(Peer-to-Peer) environments, the individual users cannot rely on a trusted and centralized authority, for example a Certificate Authority (CA) center, an entity that issues digital certificate, for protecting their privacy. Without such trustworthy entities, the P2P users have to hide their identities and behaviors by themselves. Hence, the requirement for anonymity has become increasingly critical for both content requesters and providers. A number of methods like crowds, P5 have been proposed to provide anonymity. Most, if not all, of them achieve anonymous message delivery. Those approaches, also known as path-based approaches, require users to setup anonymous paths before transmission. Path based protocols provide an anonymous path that has to be preconstructed, which requires the initiator to collect a large number of IP addresses and public keys. When a chosen peer leaves, they have to again reconstruct the path.

Rumor Riding (RR) is a non-path-based protocol for providing secure transmission of data with anonymity in P2P systems. In RR, anonymous paths are automatically constructed .RR uses symmetric key encryption instead of asymmetric which causes high cost. RR uses a random walks mechanism. RR gives key rumors and cipher rumors and expects that they meet in some random peer. RR provides an efficient anonymity. It reduces the traffic overhead and processing. RR uses probability flooding instead of blind flooding. Efficient transactions, maintaining paths are significantly low, no need to collect large number of addresses and public keys.

In RR, we first let an initiator encrypt the query message with a symmetric key, and then send the key and the cipher text to different neighbors. The key and the cipher texts take random walks separately in the system, where each walk is a rumor. The key rumor and a cipher rumor meet at some peer, the peer is able to recover the original query message and act as an agent to issue the query for the initiator. We call the agent peer as a sower. The same idea is also employed during the query response, confirm, and file delivery process**.**.

II. IDENTIFY, RESEARCH AND COLLECT IDEA

Onion Routing is an infrastructure for private communication over a public network. It provides anonymous connections that are strongly resistant to hackers. Onion Routing's anonymous connections are bidirectional and near real-time, and can be used for both connection-based and connectionless traffic. It is a path based approach i.e. it specifies properties of the connection at each point along the route, which requires the initiator to collect a large number of IP addresses and public keys. It uses layered public key cryptography, which have cryptographic overhead for the initiator, the responder, and the middle nodes.

Tor is the second generation Onion Router, supporting the anonymous transport of TCP streams over the Internet. Tor addresses limitations in the original design by adding perfect forward secrecy, congestion control, directory servers, integrity checking, configurable exit policies, and a practical design for location-hidden services. In the original Onion Routing design, a single hostile node could record traffic and later compromise successive nodes in the circuit and force them to decrypt it while Tor uses an incremental path-building design, where the initiator negotiates session keys with each successive hop in the circuit. Tor supports most TCP based programs without modification. Decentralized congestion control of Tor uses end-to-end acknowledgements to maintain anonymity while allowing nodes at the edges of the network to detect congestion or flooding and send less data until the congestion subsides. But Tor is not secure against end-to-end attacks. Tor is path-based approach which requires large number of IP addresses and public keys and it is based on asymmetric cryptography.

Gnutella builds, at the application level, a virtual network with its own routing mechanisms. The topologies of this virtual network and the routing mechanisms used have a significant influence on application properties such as performance, reliability and scalability.

To know the effectiveness of random walks for construction of unstructured peer-to-peer (P2P) networks we have identified two cases where the use of random walks for searching achieves better results than flooding: a) when the overlay topology is clustered, and b) when a client re-issues the same query while its horizon does not change much Stochastic processes indicating that samples taken from consecutive steps of a random walk can achieve statistical properties similar to independent sampling. In this power of sampling can be shown by using random walks in peer to peer to systems. Sampling is a process used in stastical analysis in which predetermined number of observations will be taken from a larger population.

In crowds, web servers are unable to know the orginator of the request from member who is forwarding the reauest on behalf of the another. Crowds makes no effort to defend against denial-of-attacks by rogue crowd members. Crowds have no responder anonymity by default. Symmetric decryption at every hop provides weaker anonymity. Pathing must be persistent for duration of file transfer. Lack of source-routing provides weaker anonymity.

Peer-To-Peer networks, such as Napster and Gnutella have become essential media for information dissemination and sharing over the Internet. The popularity of peer-to-peer multimedia file sharing applications such as Gnutella and Napster has created a flurry of recent research activity into peer-to-peer architectures. Napster and Gnutella facilitate the location and exchange of files among a large group of independent users connected through the Internet. In Napster and Gnutella files are stored on the computers of the individual peers, and exchanged through a direct connection between the downloading and uploading peers, over an HTTP-style protocol. All peers in this system are symmetric: they all have the ability to function both as a client and a server. In Napster and Gnutella there is a significant amount of heterogeneity in both Gnutella and Napster; bandwidth, latency, availability, and the degree of sharing vary between three and five orders of magnitude across the peers in the system. This implies that any similar peer-to-peer system must be very careful about delegating responsibilities across peers. Second, peers tend to deliberately misreport information if there is an incentive to do so.

The use of peer-to-peer (P2P) applications is growing dramatically, particularly for sharing large video/audio files and software. In this paper, we analyze P2P traffic by measuring flow level information collected at multiple border routers across a large ISP network, and report our investigation of three popular P2P systems—Fast Track, Gnutella, and Direct-Connect. We characterize the P2P traffic observed at a single ISP and its impact on the underlying network. We observe much skewed distribution in the traffic across the network at different levels of spatial aggregation (IP, prefix, AS). All three P2P systems exhibit significant dynamics at short time scale and particularly at the IP address level.

P5 (Peer-to-Peer Personal Privacy Protocol) is a protocol for anonymous communication over the Internet.P5 allows secure anonymous connections between a hierarchy of progressively smaller broadcast groups, and allows individual users to trade off anonymity for communication efficiency. P5 is designed to be implemented over the current Internet protocols, and does not require any special infrastructure support. A novel feature of P5 is that it allows individual participants to trade-off degree of anonymity for communication efficiency, and hence can be used to scalable implement large anonymous groups. Only one sender-receiver pair may simultaneously communicate in this system. P5 is based upon public-key cryptography.

There are several protocols to achieve mutual communication anonymity between an information requester and a provider in a P2P information-sharing environment, such that neither the requester nor the provider can identify each other, and no other peers can identify the two communicating parties with certainty. First, utilizing trusted third parties and aiming at both reliability and low-cost, there are group of mutual anonymity protocols.

Peer-to-peer and other decentralized, distributed systems are known to be particularly vulnerable to sybil attacks. In a sybil attack, a malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system. Sybil Guard is a protocol for limiting the corruptive influences of sybil attacks. Malicious users can create many identities but few trust relationships. Sybil Guard exploits this property to bound the number of identities a malicious user can create.

There have been a number of protocols proposed for anonymous network communication. We prove that when a particular initiator continues communication with a particular responder across path reformations, existing protocols are subject to the attack. The results show that fully connected DC-Net is the most resilient to these attacks, but it suffers from scalability issues that keep anonymity group sizes small. We also show through simulation that the underlying topography of the DC-Net has affects the resilience of the protocol: as the number of neighbors a node has increases both the communications overhead and the strength of the protocol increase.

III. WRITE DOWN YOUR STUDIES AND FINDINGS

We have done the literature survey of rumor riding with other existing systems. Most of the existing system like Tor, Onion Routing is path-based in which the path must be pre-constructed which requires the initiator to collect a large number of IP addresses and public keys. And when a chosen peer leaves whole path fails. Such a failure is difficult to known by user. In the existing system the initiator have to perform asymmetric key based cryptographic encryptions. Rumor riding is a non-path-based anonymous protocol. In RR anonymous path are automatically constructed In RR, an initiator encrypt the query message with a symmetric key, and then send the key and the cipher text to different neighbors. The key and the cipher texts take random walks separately in the system, where each walk is called a rumor. Once a key rumor and a cipher rumor meet at some peer, the peer is able to recover the original query message and act as an agent to issue the query for the initiator. The agent peer is known as sower . The similar idea is also employed during the query response, query confirm, and file delivery processes. RR employs a symmetric cryptographic algorithm to achieve anonymity, which significantly reduces the cryptographic overhead for the initiator, the responder, and the middle nodes. The initiating peers have no requirement on extra information for constructing paths, the risk of information leakage, caused by links that are used for peers to request the IP addresses of anonymous proxies, is eliminated. The comparison table is given below.

Rumor Riding	Non-path based	It uses symmetric cryptographic method	Low costs	Low traffic overhead compared to existing systems
Onion Routing	Path based	It uses asymmetric cryptographic method	High costs	High traffic overhead
Tor	Path based	It uses asymmetric cryptographic method	High costs	High traffic overhead
Crowds	Path based	It uses asymmetric cryptographic method	Lower than Onion routing	High traffic overhead
P5	Path based	It uses asymmetric cryptographic method	High cost	High traffic overhead
Sybil Guard	Path based	It uses symmetric cryptographic method	--------------	High traffic overhead

Table1. Comparison Table

Rumor Riding	Efficient transaction	No risk of information leakage	High degree of anonymity
Onion Routing	Delay transaction	Risk of information leakage	Low degree of anonymity
Tor	Delay transaction	Risk of information leakage	Low degree of anonymity
Crowds	Delay transaction	Risk of information	Low degree of anonymity

		leakage	
P5	Delay transaction	Risk of information leakage	High degree of anonymity
Sybil Guard	Efficient transaction	Less risk of information leakage	High degree of anonymity

Table1. Comparison Table

IV. CONCLUSION

Rumor Riding is an lightweight and non-path-based mutual anonymity protocol for P2P systems, Rumor Riding (RR). Using a random walk concept, RR gives key rumors and cipher rumors separately, and expects that they meet in some random peers. Sower is a peer where key rumor and cipher rumor meet and decryption can be done and send to responder. Rumor Riding (RR) provides a high degree of anonymity and outperforms existing approaches in terms of reducing the traffic overhead and processing latency. It eliminates to collect large number of IP addresses when sending a data.

REFERENCES

[1] D.Goldschlag, M. Reed, and P. Syverson, “Onion Routing,” Comm. ACM,p.39, 1999.

[2] R. Dingledine, N. Mathewson, and P. Syverson, “Tor: The Second Generation Onion Router,” Proc. 13th USENIX Security Symp., p. 303-320, 2004.

[3] Sripanidkulchai, “The Popularity of Gnutella Queries and Its implications on Scalability,”

[4] Gkantsidis .C, Mihail.M, and Saberi .A, “Random Walks in Peer to- Peer Networks,” Proc. IEEE INFOCOM, 2004.

[5] M.K. Reiter and A.D. Rubin, “Crowds: Anonymity for Web Transactions,” ACM Trans. Information and System Security, vol. 1, no. 1, pp. 66-92, Nov. 1998.

[6] Saroiu.S, Gummadi. P, and Gribble.S, “A Measurement Study of Peer-to-Peer File Sharing Systems,” Proc. Multimedia Computing and Networking (MMCN) Conf., 2002.

[7] Saroiu.S, Gummadi. P, and Gribble.S, “A Measurement Study of Peer-to-Peer File Sharing Systems,” Proc. Multimedia Computing and Networking (MMCN) Conf., 2002.

[8]] Sherwood. R, Bhattacharjee. R, and Srinivasan .A, “P5: A Protocol for Scalable Anonymous Communication,” Proc. IEEE Symposium Security and Privacy, pp. 58-70, 2002.

[9]]Xiao .L , Xu v, and Zhang .X, “Low-Cost and Reliable Mutual Anonymity Protocols in Peer-to-Peer Networks,” IEEE Trans. Parallel and Distributed Systems, vol. 14, no. 9, pp. 829-840, Sept. 2003.

[10]] H. Yu, M. Kaminsky, P.B. Gibbons, and A. Flaxman, “Sybil Guard: Defending against Sybil Attacks via Social Networks,” IEEE/ACM Trans. Networking, vol. 16, no. 3, pp. 576-589, June 2008.

[11]] M.K. Wright, M. Adler, B.N. Levine, and C. Shields, “The Predecessor Attack: An Analysis of a Threat to Anonymous Communications Systems,” ACM Trans. Information and System Security, vol. 7, no. 4, pp. 489-522, 2004.

AUTHORS

First Author – Neetha Thomas, M.Tech and ntnithoos@gmail.com.