Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 6, June 2013, pg.322 – 324

RESEARCH ARTICLE

An Improved Method in Peer-To-Peer System

Neetha Thomas
CSE & Calicut University, India

ntnithoos@gmail.com

Abstract— Rumor Riding (RR) is a lightweight and non-path-based mutual anonymity protocol for P2P systems In RR, an initiator encrypts the query message with a symmetric key, and then sends 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. Employing a random walk concept, RR issues key rumors and cipher rumors separately, and expects that they meet in some random peers. 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 a sower. RR provides a high degree of anonymity and outperforms existing approaches in terms of reducing the traffic overhead and processing latency. The disadvantage is the time taken to send and receive the data. It is overcome by increasing the speed of the existing system. A message digest algorithm is used for sending the request to the responder. It improves the speed of the system.

Key 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. But in RR the

processing time is more hence we need to minimize the processing time. Thus in this paper a message digest algorithm is used to minimize processing time.

II. RELATED WORK

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.

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.

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. But the processing time of RR is more. In this paper a method is proposed to reduce the processing time compared to the existing system.

III. RUMOR RIDING

Rumor Riding (RR) includes five major components: Rumor Generation and Recovery, Query Issuance, Query Response, Query Confirm, and File Delivery. In rumor generation and recovery the rumor is generated. In query issuance query is issued. In query response the responder responds to the request. In query confirm the query is confirmed. In file delivery the file is delivered to the requester. In rumor riding the processing time is more hence a method is used to reduce the current processing time.

IV. PROPOSED SYSTEM

There are many systems like tor, onion routing, p5 which are path based in which the path has to be specified before sending query request. They used asymmetric cryptographic algorithm. It has high cost and high traffic overhead. They have high probability of information leakage. They provide only low anonymity. Rumor riding (RR) is non-path based and light weight mutual anonymity protocol for decentralized system. RR uses symmetric algorithm and have low cost compared to the previous system. It provides high anonymity. The total processing time of rumor riding is more hence a message digest algorithm is used. A message digest algorithm is used in sending the query to the responder and AES algorithm is used for the file delivery.

V. CONCLUSIONS

Rumor riding is a light weight and non-path based mutual anonymity for decentralized system. RR provides a high degree of anonymity and outperforms existing approaches in terms of reducing the traffic overhead. RR uses symmetric cryptographic algorithm for encryption. But RR takes more processing time hence a message digest algorithm is used for sending the request to the responder which reduces the total processing time.

ACKNOWLEDGEMENT

I acknowledge my professors for supporting me to complete my research.

REFERENCES

[1] R 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] Sherwood. R, Bhattacharjee. R, and Srinivasan .A, "P5: A Protocol for Scalable Anonymous Communication," Proc. IEEE Symposium Security and Privacy, pp. 58-70, 2002.
[4] Yunhao Liu, Jinsong Han and Jilong Wang, "Rumor Riding: Anonymizing Unstructured Peer-to-Peer Systems," IEEE Transaction on parallel and distributed systems, vol.22, no.3, 464-475, March 2011

