A Two Walk Protocol: Anonymizing Unstructured Peer-to-Peer Systems

Anuradha Ganivada $^{\#1}$**, Dr.K.Venkata Rao**^{*2}

Department of Computer Science & Engineering,
Vignan Institute of Information Technology,
Visakhapatnam, AP, India.

Abstract

Now a day's peer-to-peer (P2P) systems are major form of communication model in which each node acts as both a server and client. These systems are mainly used to share large files, telephony communications, private discussion forms, and also for media streaming. In anonymity Peer-to-Peer (P2P) networks, many systems try to mask the identities of their users for privacy considerations. In the past there was some anonymity approaches like Crowd based approach which is mainly path-based: In this path based approach, the peers have to pre-construct an anonymous path before transmission the data. So it is not able to provide responder anonymity, due to this limitation maintaining and updating of such a paths is very difficult. In this paper we mainly proposed a new protocol called Rumor Riding (RR) which is non-path-based mutual anonymity protocol for P2P systems and it clearly provides a high degree of initiator and responder anonymity. In this protocol, the initiator query message is first encrypted and after that the key and the cipher texts take random walks separately in the system, where each walk is called as a rumor. By using a random walk mechanism, our proposed protocol takes advantage of lower overhead by mainly using the cryptographic algorithm.

Keywords

Mutual anonymity, non-path-based, random walk, responder, peer-to-peer.

1. Introduction

In P2P(Peer-to-Peer) environments, we can observe that no individual users cannot rely on a trusted authority and centralized authority person, for example a Certificate Authority (CA) center, an entity that issues digital certificate, for protecting their privacy. If this type of trusted authorities is not present, the users face a lot of problems in order to expose their personal data. Without such trustworthy entities or methods, the P2P users have to hide their personal identities and behaviors by themselves. Hence, the requirement for anonymity has become increasingly critical for both content requesters and content providers. Till then there were a number of methods like crowds based method as shown in figure 1, P5 based method have been proposed to provide anonymity for the user data. Those existing approaches, also known as predefined path-based approaches, which require users to setup a predefined anonymous paths before transmission of data. For constructing path based approaches the initiator requires to collect a large number of IP addresses and public keys. After creating a predefined path if there is any node leaves the peer, they have to again reconstruct the new path with the available nodes.

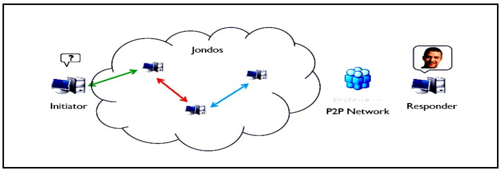


Fig.1. Represents the Existing Crowds Network

By using a new type of mechanism in this paper, we proposed a new protocol called RR (Rumor Riding) in which an initiator encrypt the query message firstly with a symmetric key, and then send the encrypted key and the cipher text to different neighbors who are present in that network. The key and the cipher texts don't travel all in a single path, but they take random walks separately in the system, where each walk is called as a rumor. The key rumor and a cipher rumor meet at some peer after passing from various neighbors, the peer is then able to recover the original query message and act as an agent node to issue the original search query for the initiator.

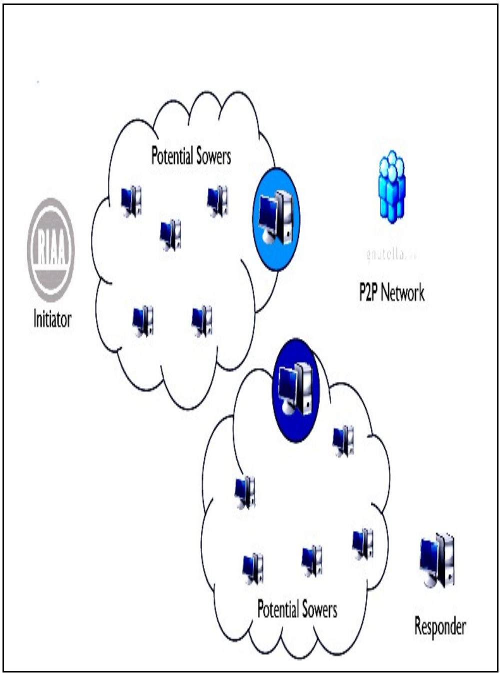


Fig.2. Represents Rumor Riding Framework

We also call the agent peer as a Sower Node. The same idea is also employed reversely during the query response, confirm, and file delivery process. The two rumors serve as the main primitives of this protocol to achieve mutual anonymity and meet the design objectives. In our proposed protocol, anonymous paths are automatically constructed via the rumors random walks. Extending the scope of anonymous servants from a small clique of nodes to the entire P2P network, RR significantly increases the anonymity degree of a system. RR employs a symmetric cryptographic algorithm to cryptographic overhead for the initiator, the responder, and the middle nodes. In addition, as initiating peers have no requirement on extra information for construction paths, the risk of information leakage, caused by links that are used for peers to IP addresses of anonymous proxies, is eliminated.

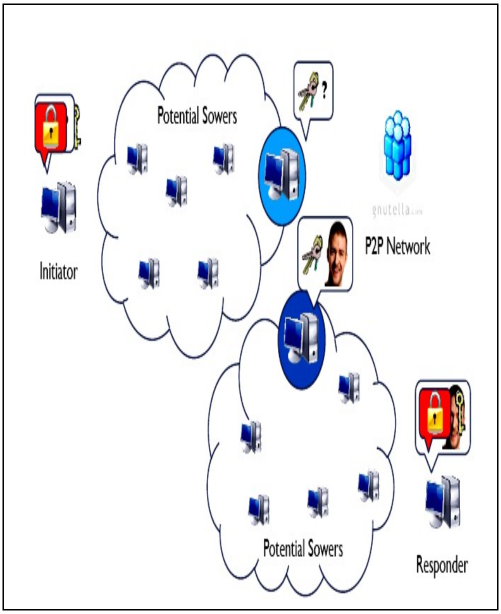


Fig.3. Example of Rumor Riding Protocol

2. Related Work

In this section, we will find the information which was very near to our current RR approach in detail.

The concept of anonymity is elaborated by an author called Chaum made [2] several approaches to obtain anonymous communication, which is obviously falls in to two categories:

1) Anonymous multicasting and other
2) Path Based Anonymous.

According to Tor [3] which is most well like path based protocol would provide initiator anonymity support encryption layer process and onion routing [4] as second generation protocol. According to response anonymity technique an initiator anonymity protocol is mostly similar to Onion Routing protocol in P2P system. The mutual anonymity P2P system with the reduce response delay provides by shortcut protocol [5].As we know that Huge crowds present the initiate the random ahead process between two different nodes. The peer receive packet there are two options:

1) One it directly sends to the destination peer or
2) It forwards a packet to the randomly chosen peer.

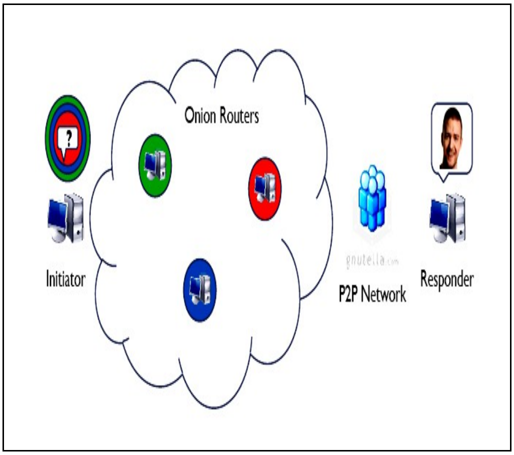


Fig.4. Example of P5 Anonymous Network

P5 (Peer-to-Peer Personal Privacy Protocol) [1] protocol mainly depend upon to anonymous multicasting. Many employs to make anonymous broadcasting groups, create broadcasting scalable by using Virtual tree P5. To send the packets for secure hide initiator ID, first the make the peer with the group when P5 protocol is enable peers. In peer to peer system an anonymous can't appropriate for initiator identified receiver nodes ID, it is multicast base approaches.

The rumor riding protocol using symmetric key encryption cryptographic system and RSA algorithm techniques which is not highly sure and also previous work on unstructured P2P system [7] but we propose asymmetric encryption algorithm system. Our protocol design the main idea is random walk. We discuss about random walk and propose the multiple random walk to reduce the network traffic, the query based algorithm to eliminate the flood process. The mathematical model [6] analyzed performance of the random walk. We present random based protocol in P2P systems [7]. To protect against sybilguard [8] attacks in the social network employs to random router. These all period study supports strongly and efficiently for random walk in P2P systems.

2.1 Onion Routing Protocol

Onion routing protocol is also one type of security oriented protocol which provides anonymous connections that are strongly resistant to both eavesdropping and traffic analysis. Unmodified internet application can use this anonymous connection in the form of proxies. Proxies are those which can also make communication anonymous by removing identifying information from the data stream. Onion routing protocol is mainly implemented on Sun Solaris 2.X with proxies for Web Browsing, remote login and email. This paper mainly contributes a detailed specification of the implemented onion routing system, vulnerability analysis based on this specification and performance result. In this paper alternatives to the basic configuration exist which move trust closer to the user. For example, an Internet Service Provider (IPS) could run an onion router protocol that accepts onion from its subscribers. Subscribers would generate this onion on their trusted local machines. The ISP would not know with whom the customer is communicating. And the subscriber need not fully trust the IPS to maintain his privacy. Anonymous connection may be used as a new primitive that enable novel application in addition to facilitating secure version of existing service.

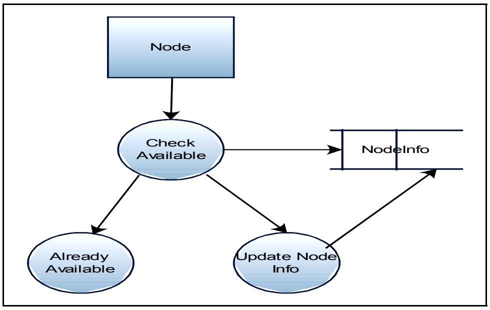
3. Rumor Riding Anonymous Protocol

In this section, we present our work, the Rumor Riding (RR) protocol, which includes 4 major components or modules. Although RR is designed for unstructured P2P systems, it can be easily extended into other distributed systems.

1. Topology Construction Module
2. Rumor Generation and Recovery
3. Query Issuance and Response
4. Query Confirm and File Delivery

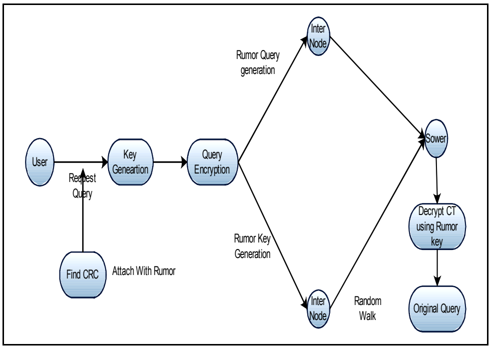
1. Topology Construction Module

In this module, initially we need to construct a topology structure. Here we use mesh topology because of its unstructured nature. Topology is constructed by getting the names of the nodes and the connections among the nodes as input from the user. While getting each of the nodes, their associated port and ip address is also obtained. For successive nodes, the node to which it should be connected is also accepted from the user. While adding nodes, comparison will be done so that there would be no node duplication. Then we identify the source and the destinations.



2. Rumor Generation and Recovery

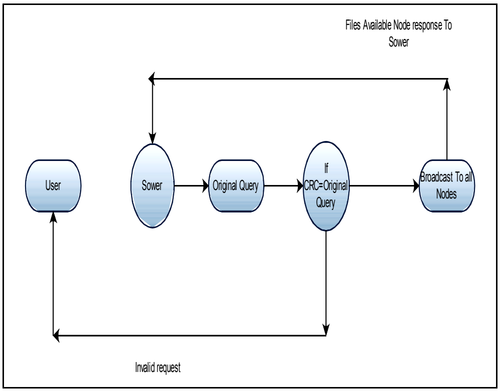
This is the second module in which we let an initiator encrypt the query message with a symmetric key, and then send the key and the cipher text to different neighbors. The key and the cipher text take random walks separately in the system, where each walk is called a rumor; it is a two way walk mechanism.



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.RR employs the AES algorithm to encrypt original messages. The key size is 128-bit. To determine whether a pair of cipher and key rumors hit, we employ a Cyclic Redundancy Check (CRC) function to attach a CRC value. It organizes the key and the cipher text into two query rumors. Each packet is labeled with a Descriptor ID, a string that uniquely identifies the packet. RR also uses the descriptors to identify rumors.

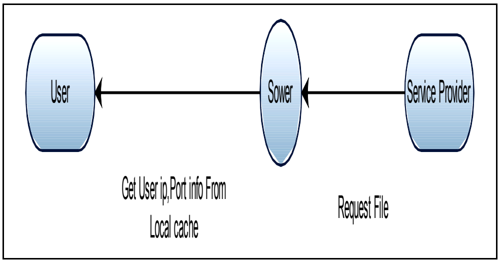
3. Query Issuance and Response

In this module, query issuance is done for received key rumors and cipher rumors; the sower node uses AES to recover a message and the checksum CRC. It then performs the Cyclic Redundancy Check function to the recovered message and compares the result with CRC. If they match, the sower node S is aware that it has successfully recovered a message. The purpose of the CRC function is to avoid using a complex text understanding technique to distinguish a meaningful Message. If a decrypted rumor holds a plaintext matching the CRC value, q will be successfully recovered. Whatever there is a match or not, this intermediate node reduces the TTL value of the received rumor by one, keeps a temporary record containing the ID of the rumor in the local cache, and forwards it to a randomly chosen neighbor. The procedure continues until the TTL value of this rumor is reduced to zero.



4. Query Confirm and File Delivery

This is the final module in our implementation of our RR Protocol in this Rumor Riding protocol it requires every node to temporarily keep a local cache to store the received rumors. When a node receives a query key rumor, it performs the rumor recovery procedure to check all cached cipher rumors. If a decrypted rumor holds a plaintext matching the CRC value, q will be successfully recovered. The large data cipher rumor and the small data key rumor first take random walks to meet each other at a sower, and eventually reach I along the reversed paths of initiator. Upon receiving the digital envelop, recovers the desired file using its private key.



4. Conclusion

In this paper, we successfully proposed a new lightweight and non path-based mutual anonymity protocol for unstructured P2P systems, called as Rumor Riding (RR) protocol. Employing a random walk concept, RR issues key rumors and cipher rumors separately, and expects that they meet in several random peers. The results of extensive trace-driven simulations in java technology conducted by me clearly show that RR provides a high degree of anonymity and outperforms existing approaches in traffic overhead and processing latency. We also discuss how RR can effectively defend against popular attacks. The early experience of our prototype implementation shows its practicality.

5. References

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

[2] 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.

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

[4] D. Goldschlag, M. Reed, and P. Syverson, “Onion Routing,” Comm. ACM, vol. 42, no. 2, p. 39, 1999.

[5] L. Xiao, Z. Xu, and X. Zhang, “Low-Cost and Reliable Mutual Anonymity Protocols in Peer-to- Peer Networks,” .

[6] N. Bisnik and A. Abouzeid, “Modeling and Analysis of Random Walk Search Algorithms

in P2P Networks,” Proc. Second Int’l Workshop Hot Topics in Peer-to-Peer Systems, 2005.

[7] Yunhao Liu, Senior Member, IEEE,Jinsong Han, Member, IEEE, and Jilong Wang, Member, IEEE “Rumor Riding: Anonymizing Unstructured Peer-to-Peer Systems”.

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

6. About the Authors

Anuradha Ganivada is currently pursuing her 2 Years M.Tech (CSE) in Computer Science and Engineering at Vignan Institute of Information Technology, Duvvada, Visakhapatnam. She completed her B.Tech in CSE department from Maharaj Vijayram Gajapathi Raj college of Engineering. Her area of interests includes Networks, Data Mining.

Dr. K. Venkata Rao Ph.D (CSE) is currently working as Prof & Head of Department of CSE Branch in Computer Science and Engineering department, at Vignan Institute of Information Technology, Duvvada, Visakhapatnam. His research interests include Networks, Security, and Data Mining and Warehousing.