International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 6, August - 2012

Rumor Riding: A Random Walk Protocol For Providing Anonymity

Padmavathi Vanka, Manjula. T, SanthiLakshmi. A

***Abstract*— In peer-to-peer (P2P) computer network, each computer in the network can act as a client or server for the other computers in the network, allowing shared access to files and peripherals without the need for a central server.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 Bit Torrent are mainly path-based: peers have to pre-construct an anonymous path before transmission. It doesn't Provide Responder anonymity. Maintaining and updating such paths is difficult as the initiator have to collect the IP addresses of the neighboring peers. Rumor Riding (RR) is non-path-based mutual anonymity protocol for P2P systems. It provides high degree of initiator and responder anonymity. RR first encrypts the initiator query message. The key and the cipher text take random walks through different neighbors in the network, where each walk is a rumor. Employing a random walk mechanism, RR takes advantage of lower overhead by mainly using the cryptographic algorithm.**

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

I. INTRODUCTION

In Peer-to-Peer (P2P) networks, such as Bit Torrent, Crowds have become essential media for information broadcasting and sharing over the Internet. P2P environments, the individual users cannot rely on a trusted and centralized authority, for example a Certificate Authority (CA) center, 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. Even though the Path based protocols provide anonymity, an anonymous path has to be pre-constructed, which requires the initiator to collect a large number of IP addresses.

A Rumor riding is an non-path-based mutual anonymity protocol for P2P systems and it provides high degree of initiator and responder anonymity. 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. The rumors serve as the primitives of this protocol to achieve mutual anonymity and meet the design objectives. In RR, 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.

II. RELATED WORK

[1] The efficacy of random walks for erection 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 statistical analysis in which predetermined number of observations will be taken from a larger population.

[2] An Onion Routing(OR) is Path based protocol 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 can be used anywhere. An onion is a data structure which is treated as the destination address by onion routers thus it is used to establish an anonymous connection

[3] Tor is the second generation Onion Router, supporting the anonymous transport of TCP streams over the Internet. Its low latency makes it very suitable for common tasks, such as web browsing, but insecure against traffic analysis attacks by a global passive adversary. We present new traffic-analysis techniques that allow adversaries with only a partial view of the network to infer which nodes are being used to relay the anonymous streams and therefore greatly reduce the anonymity provided by Tor. Furthermore, we show that otherwise unrelated streams can be linked back to the same initiator. Our attack is feasible for the adversary anticipated by the Tor designers, Tor network. Our techniques should also be applicable to any low latency anonymous network.

[4] The popularity of peer-to-peer multimedia file sharing applications such as Gnutella and Napster has created a flurry

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 6, August - 2012

of recent research activity into peer-to-peer architectures. We believe that the proper evaluation of a peer to peer system must take into account the characteristics of the peers that choose to participate. In this paper, we remedy this situation by performing a detailed measurement study of the two popular peer-to-peer file sharing systems, namely Napster and Gnutella. In particular, our measurement study seeks to precisely characterize the population of end-user hosts that participate in these two systems. This characterization includes the bottleneck bandwidths between these hosts and the Internet at large, IP-level latencies to send packets to these hosts, how often hosts connect and disconnect from the system, how many files hosts share and download, the degree of cooperation between the hosts, and several correlations between these characteristics

[5] 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 very 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.

[6] In this process a protocol for anonymous communication over the internet.P5 (Peer-to-Peer Personal Privacy Protocol) is a protocol which provides sender, receiver, and sender-receiver anonymity. 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. We present a description of P5, an analysis of its anonymity and communication efficiency, and evaluate its performance and reconstruct the path.

[7] 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

III. EXISTING METHODOLOGY

In Existing anonymity approaches peers have to pre-construct an anonymous path before transmission. In crowds there is need to establish a anonymous path before transmission. Crowd is an path based protocol .Existing works, for example P5 employ the flooding pattern ,which is not suitable for P2p systems due to the huge traffic overhead. The end-to-end delivery, which is used by the path based approaches, however may compromise the anonymity of the initiator or responder but fails due to traffic and weak links. Initiator has to collect large numbers of IP addresses.

IV. PROPOSED METHODOLOGY

Rumor Riding (RR) is an non-path-based protocol for providing secure transmission of data with anonymity in P2P systems. RR uses a random walks mechanism. RR gives key rumors and cipher rumors and expect that they meet in some random peer. RR provides an efficient anonymity. It reduces the traffic overhead and processing. Efficient transactions, maintaining paths is significantly low, no need to collect large number of addresses and other details are advantages of this protocol.

In Anonymity Peer-to-Peer (P2P) networks, many systems try to mask the identities Rumor Riding consists of five major components: Rumor Generation and Recovery, Query Issuance, Query Response, Query Confirm, and File Delivery.

A. Rumor Generation and Recovery

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, CRC(M), to the message M. For received key rumors and cipher rumors, the sower S uses AES to recover a message M' and the checksum CRC (M'). It then performs the CRC function to the recovered M' and compares the result. If they match, the sower S is aware that it has successfully recovered a message M.

B. Query Issuance

When an initiator I wishes to issue an anonymous query, it first generates the query content q, and a public key K. Node I then uses an AES cryptographic algorithm to encrypt q into a cipher text C with a symmetric key K. It organizes the key K and the cipher text C into two query rumors, qK and qC. In Gnutella, each packet is labeled with a Descriptor ID. RR also uses the descriptors to identify rumors. Thus, two random number strings, IDqK and IDqC, are used to label the two rumors. After generation, I forward the rumor messages to two randomly chosen neighbors.

C. Query Response

When a receiving node the query has a copy of the desired file, it becomes a responder R. To respond to the query, R encrypts the plain text of the response message r, using the initiator's public key K. It encrypts key using AES, where KR is the public key generated by R, and encloses the cipher text and the key into two response rumors, rK and rC. They are then assigned with IDrK and IDrC, respectively

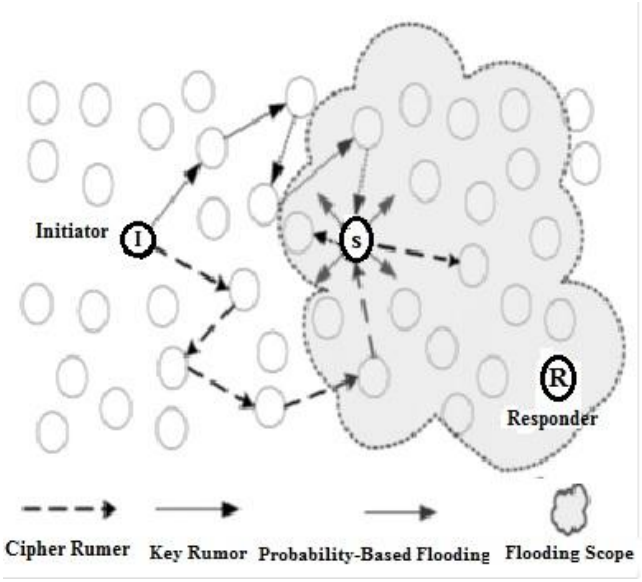

Fig. 1.Query Issuance

D. Query Confirm

In the query confirm phase, I uses the responder's public key to encrypt the confirm message c. It then encrypts <KþR ;IDrK; IDrC; IPSb> and obtains two confirm rumors, cK and cC, which take random walks in the system. Note that two confirm rumors are marked with new descriptors: IDcK and IDcC. We assume that cK and cC collide in a new sower S'a . We denote their paths from I to S'a by lcK and lcC . When S'a recovers the IP address of Sb from cK and cC, it directly contacts Sb to forward cK and cC attached with IDrK and IDrC via a TCP line.

E. File Delivery

It employs a digital envelope technique to encrypt the file into cipher CF. Instead of including CF into the rumor generation, R encrypts <IDcK; IDcC; IPS0a> to generate the data cipher rumor and the data key rumor, and attaches the digital envelop payload to the data cipher rumor. The large data cipher rumor and the small data key rumor first take random walks to meet each other at a sower.

F. Rumor TTL

The selection of rumor TTL, together with the number of cipher and key rumors, determines 1) how many sowers a query will have, and 2) how the sowers are distributed. The tradeoff is that for each query, RR requires a number of sowers randomly distributed in the entire system, but too many sowers will lead to unacceptable overhead. In order to guarantee the diversity of the sowers, a simple and lightweight method is needed for estimating O(log n), where n is the size of the P2P overlay. Also, to reduce the unnecessary overhead, peers need to observe the diversity of sampling sowers to adjust the TTL value of rumors. The adaptive TTL determination of RR comprises two phases: (a) setting initial TTL value, and (b) adaptively adjusting TTL.

V. CONCLUSION

Rumor Riding is a 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] 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.

[2] Morselli .R, Bhattacharjee .B, and. Marsh .M.A, "Anonymous Connections and Onion Routing," Proc. ACM SympIEEE Trans. Parallel and Distributed Systems, 2005

[3] Murdoch .S.J and Danezis .G, "Low-Cost Traffic Analysis of Tor," Proc. IEEE Symp. Security and Privacy, 2005.

[4] 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.

[5] Sen .S and Wang .J, "Analyzing Peer-to-Peer Traffic across Large Networks," IEEE/ACM Trans. Networking, vol. 12, no. 2, Apr. 2004.

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

[7] 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.

Padmavathi vanka is currently a student of, PBR Visvodhaya Institute of Science and Technology, Kavali at Department of Computer Science and Engineering from JNTU Ananthapur, Andhra Pradesh. She graduated in Computer Science & Engineering from JNTU University, Ananthapur during 2006. His areas of interests are Networking and Data Mining.

T. Manjula is currently a faculty with Department of Computer Science and Engineering, PBR Visvodhaya Institute of Science and Technology, Kavali from JNTU Ananthapur, Andhra Pradesh. She graduated in ME, M. Sc., MPhil. Her areas of interest are WebMining and Web Services.

Santhi Lakshmi is currently a student of, Audhi Sankara College of Engineering and Technology at Department of Computer Science and Engineering from JNTU Ananthapur, Andhra Pradesh. She graduated in Computer Science & Engineering from JNTU University, Ananthapur during 2009. His areas of interests are Networking and Data Mining.