International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 2, Issue 9 (May 2013) PP: 50-54

Non Path-Based Mutual Anonymity Protocol for Decentralized P2P System

J. Chozhamadevi, S. Mohanarangan M.Tech (P.hd.), Dr. D. Sivakumar
PG Scholar, Asst. Professor, Professor & Dean
Dept of Computer Science Arunai College of Engineering
Dept of ECE Arunai College of Engineering

Abstract: *Each and every end-to-end systems try to mask the information and details of their users for privacy considerations. Existing quality of being anonymous approaches are mainly path-based: peers have to pre-construct an anonymous path before transmissio of any files and queries.The overhead of maintaining and updating such paths is significantly high also introduce high cost. Its called as blindly assigned path. We propose Rumor Riding (RR), 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. Accelerating the query speed. Introducing mimic traffic to confuse attackers. Mimic traffic generates duplicate cipher and key rumor to confuse the attackers. This mimic traffic generates traffic in a purposefully irregular manner. Mimic is undetectable by any known detection technique at without loss of throughput.*

Index Terms: *Mutual anonymity, non-path-based, random walk, peer-to-peer.*

I. Introduction:

PEER-TO-PEER (P2P) networks, such as Napster, Gnutella, and Bit Torrent, have become essential media for information dissemination and sharing over the Internet. Indistributed and decentralized P2P environments, the individual users cannot rely on a trusted and centralized authority, 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 have been proposedto provide anonymity. Those approaches are purely path-based approaches, require users to setup anonymous paths before transmission. Although path-based protocols provide strong anonymity, an anonymous path has to be preconstructed, which requires the initiator to collect a large number of IP addresses and public keys.Also, an initiator has to perform asymmetric key based cryptographic encryptions, Both the peer collection and content encryption introduce high costs In highly dynamic p2p system, when a chosen peer leaves, the whole path fails, Unfortunatly such a failure is often difficult to be known by the initiator. Therefore, a “blindly-assigned” path is very unreliable, and users have to frequently probe the path and retransmit messages.

To address the above issues, we propose a non-path-based anonymous P2P protocol called Rumor Riding (RR). 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 neighbor. The key and cipher texts take random walks separately in the system. 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.We call the agent peer as a sower. The similar idea is also employed during the query response, confirm, and file delivery processes.

In RR, paths are automatically constructed via the rumors’ random walks. RR employs asymmetric cryptographic algorithm to achieve anonymity, which significantly reduces the crypto-graphic overhead for the initiator, the responder, and the middle nodes. Also as initiating peers have no requirement on extra information for constructing paths, risk of information leakage.

We introduce mimic traffic in the constructed topology. Mimic traffic consist of duplicate cipher text and duplicate keys. These duplicate keys are identified by the server and nodes in the topology. They can differentiate the original rumors and duplicate rumors. These duplicate cipher rumor and key rumor take random walk in the constructed topology. It does not interrupt the original rumors random walk. The main goal of the mimic traffic ics to introduce the duplicate traffic and to confuse the attackers.

II. Literature Survey:

2.1 Search and Replication in Unstructured Peer-to-Peer Networks:

Decentralized and unstructured p2p networks are attractive for certain applications because they require no centralized directories and no precise control over network topology or data placement. However, the flooding based query algorithm used in Gnutella does not scale; each query generates a large amount of traffic and large systems quickly become overwhelmed by the query-induced load. This paper explores, through simulation, various alternatives to Gnutella's query algorithm. They propose a query algorithm based on multiple random walks that resolves queries while reducing the network traffic by two orders of magnitude in many cases. Finally, they find that among the various network topologies we consider, uniform random graphs yield the best performance. This study is our first step towards understanding the properties of scalable search algorithms, replication strategies, and network topologies for decentralized, unstructured p2p networks. There are still many open issues to study. It would be useful to model various search algorithms with certain network topologies and study them analytically.

2.2 Onion Routing:

Onion routing provides anonymous connections that are strongly resistant to both eavesdropping and traffic analysis. Unmodified internet application can use this anonymous connection by means of proxies. Proxies can also make communication anonymous by removing identifying information from the data stream. Onion routing is implemented on Sun Solaris 2.X with proxies for Web Browsing, remote login and email. This paper contribution is 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 that accepts onion from its subscribers. Subscribers would generates these 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.

2.3 Random Walks in Peer-to-Peer Networks:

This paper quantify the effectiveness of random walks for searching and construction of unstructured peer-to-peer (P2P) networks. For searching, they argue that random walks achieve improvement over flooding.. For construction, they argue that an expander can be maintained dynamically with constant operations per addition. The key technical ingredient of their approach is a deep result of stochastic processes indicating that samples taken from consecutive steps of a random walk can achieve statistical properties similar to independent sampling This property has been previously used in complexity theory for construction of pseudorandom number generators. We reveal another facet of this theory and translate savings in random bits to savings in processing overhead. Open problems in this paper are the construction algorithm is weakly decentralized; we wish to make it strongly decentralized. They have reduced deletions too. And can handle them more effectively. They have suppressed many implementational details. In practice, we expect adaptations of the random walk methods and in general a hybrid between random walks and other methods.

2.4: Modeling and Analysis of Random Walk Search Algorithms in P2P Networks.

Developing a model for random walk search mechanism in unstructured P2P networks. Using the model they obtain analytical expressions for the performance metrics of random walk search in terms of the popularity of the resource being searched for and the parameters of random walk. They propose an equation based adaptive search mechanism that uses estimate of popularity of a resource in order to choose the parameters of random walk such that a targeted performance level is achieved by the search. We also propose a low-overhead method for maintaining an estimate of popularity that utilizes feedback obtained from previous searches. Simulation results show that the performance of equation based adaptive search is significantly better than the non-adaptive random walk. Overhead incurred in order to maintain popularity estimates is confined to transfer of popularity estimates to a new node that joins the network. Thus the overhead for arrival of each node is of the order of n. Total overhead caused would depend upon the node arrival rate of the network. This overhead will not effect the scalability of the network if the node arrival rate of the network is not very large. More importantly, the overhead affects only the one-hop neighbor.

2.5: Tor: The Second-Generation Onion Router

In this paper they present Tor, a circuit-based low-latency anonymous communication service. This second-generation Onion Routing System 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 via rendezvous points.Tor works on the real world Internet, requires no

special privileges or kernel modifications, requires little synchronization or coordination between nodes, and provides a reasonabletradeoff between anonymity, usability, and efficiency. We briefly describe our experiences with an international network of more than 30 nodes. We close with a list of open problems in anonymous communication. Tor's emphasis on deploy ability and design simplicity has led us to adopt a clique topology, semi centralized directories, and a full-network-visibility model
for client knowledge. This paper assumes that all ORs have good bandwidth and latency. Volunteers who run nodes are rewarded with publicity and possibly better anonymity.More nodes means increased scalability, and more users can mean more anonymity. Perhaps each exit node should run a caching web proxy to improve anonymity for cached pages to improve speed, and to reduce bandwidth cost.

III. Existing System:

Peer-to-peer (P2P) networks, such as Napster, Gnutella, and Bit Torrent, have become essential media for information dissemination and sharing over the Internet. Recently, a number of P2P users have encountered problems caused by being traced on non-anonymous P2P systems due to their plain-text query messages and direct-downloading behaviors. Hence, the requirement for *anonymity* has become increasingly essential in current P2P applications for both content requesters and providers. Most, if not all of them, deliver messages via non-traceable paths comprised of several anonymous proxies or middle agent peers. In these approaches, known as path-based approaches, users usually need to construct anonymous paths before transmissions. Path-based approaches require users to setup anonymous paths before transmission. In most cases, the path is a layer-encrypted data structure. Although path-based protocols provide strong anonymity, an anonymous path has to be pre-constructed All nodes in the path cooperate to forward data to a receiver. Data is pre-wrapped by the initiator in a layered-encryption packet (usually using asymmetric cryptographic algorithms, such as RSA), which will be peeled off along the path to the receiver. Although path-based protocols provide strong anonymity, they have the following problems.

3.1DRAWBACK:

- Pre-construction of paths requires users to obtain a large number of IP addresses and public keys from other peers in advance. Both the collection of information and the preparation of packets incur high costs.
- Initiators have to periodically update middle nodes along the anonymous paths. An invariable path might otherwise become increasingly vulnerable under the analysis of attackers. In addition, users often expect to extend the length of anonymous paths, as a longer path entails a higher degree of anonymity. Both of these requirements increase the maintenance and update overhead.
- In highly dynamic P2P systems, peers randomly join and leave. If a chosen node goes offline, the whole path fails, and such a failure is often undetected by the initiator.

IV. Proposed System:

In RR, anonymous paths are automatically constructed via the rumors' random walks. Neither the initiator nor the responder needs to be concerned with path construction and maintenance. key rumors and cipher rumors serve as the primitives of this protocol to achieve mutual anonymity and meet the design objectives. Demonstrating the effectiveness of this design through trace-driven simulations. The analytical and experimental results show that RR is more efficient than existing protocols. Mimic traffic which introduse duplicate traffc between the topology to confuse the attacker.

4.1ADVANTAGES:

- Generating lightweight and non-path-based mutual anonymity protocol for P2P systems.
- Anonymous paths are automatically constructed via the rumors' random walks. Eliminates the huge overhead of path construction and maintenance.
- Uses a symmetric cryptographic algorithm to replace the asymmetric to reduce the cryptographic overhead and make the protocol more practical.
- Each initiating peer has no requirement of extra information to construct paths, thus eliminates the risk of information leakage caused by links that are used for peers to request the IP addresses of anonymous proxies.
- Introducing new approach called Mimic traffic.
- Mimic traffic generates duplicate cipher and key rumor to confuse the attackers.
- These duplicate cipher rumor and key rumor take random walk in the constructed topology. It does not interrupt the original rumors random walk.
- The main goal of the mimic traffic ics to introduce the duplicate traffic and to confuse the attackers.

4.2 SYSTEM ARCHITECTURE:

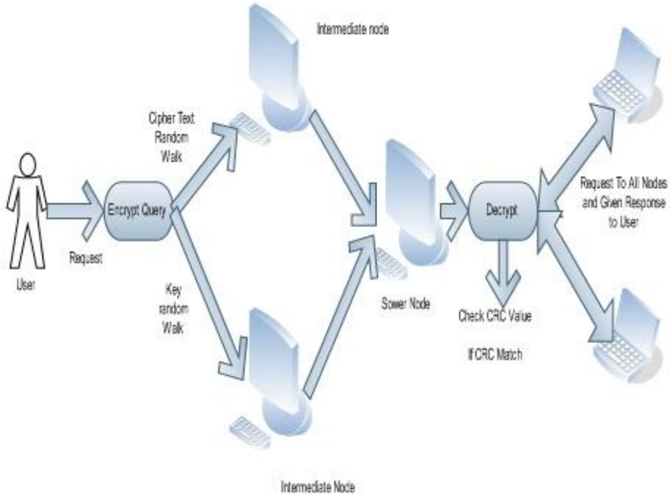

Fig: 4.1.Proposed Architecture

4.3 PROPOSED MODULES:

4.3.1TOPOLOGY CONSTRUCTION:

In this module, we 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. While adding nodes, comparison will be done so that there would be no node duplication. Then we identify the source and the destinations.

4.3.2 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. 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.

4.3.3QUERY ISSUANCE AND RESPONSE:

In this module received key rumors and cipher rumors, the sower uses AES to recover a message and the checksum CRC. It then performs the CRC function to the recovered message and compares the result with CRC. If they match, the sower S is aware that it has successfully recovered a message.If a decrypted rumor holds a plaintext matching the CRC value, q will be successfully recovered.

4.3.4 QUERY CONFIRM AND FILE DELIVERY:

RR 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 eventually reach I along the reversed paths of initiator. Upon receiving the digital envelop, recovers the desired file using its private key.

4.3.5 MIMIC TRAFFIC

To resist both traffic analysis and defense detection attacks,we propose using realistic cover traffic tunnels to mask the observable behavior of the real traffic to be transmitted.The user tunnels his or her real traffic via a proxy service, which embeds the traffic inside fake cover traffic.This tunneling approach incurs overhead in time and in the number of excess bytes transmitted. To trade off over-head and privacy, the user may vary his or her choice of cover traffic model. In this paper, we introduce the basic design and evaluation of a cover traffic tunneling system called TrafficMimic.We utilize methods for generating realistic cover traffic, borrowing from prior work on traffic generation from the simulation and modeling research community Using several protocol classification and anomaly detection attacks, we show that TrafficMimic is able to reproduce cover traffic reliably and securely.

TrafficMimic uses two phases: i)learning traffic models, and ii) secure playback. TrafficMimic itself performs secure playback of cover traffic and incorporates a tunnel of real data inside the cover traffic. TrafficMimic accepts connections from other applications and forwards all data sent and received over the input port across an encrypted tunnel using cover traffic. To use TrafficMimic, the user must have TrafficMimic nodes at both end points of the communication. The remote TrafficMimic node removes the added control and padding information and delivers the decrypted data to the destination; likewise, data from the destination is encrypted and padded at the remote node and decrypted by the local TrafficMimic node.

V. Conclusion

RR provides a high degree of anonymity and outperforms in terms of reducing the traffic overhead and processing latency. RR can effectively defend against various attacks accelerating the query speed.We demonstrate the effectiveness of this design through trace-driven simulations.The analytical and experimental results show that RR is more efficient than existing protocols.Future and ongoing work includes accelerating the query speed. We will also investigate other security properties of RR, such as the unlinkability, information leakage, and failure tolerance when facing different attacks.It would also be interesting to explore the possibility of implementing this lightweight protocol in other distributed systems, such as grid systems and ad-hoc networks.

References

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

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

[3] R. Sherwood, B. Bhattacharjee, and A.Srinivasan, “P^5: A Protocolfor Scalable Anonymous Communication,” Proc. IEEE Symp. Security and Privacy, pp. 58-70, 2002.

[4] D. Chaum, “Untraceable Electronic Mail Return Addresses, and Digital Pseudonyms,” Comm. ACM, vol. 24, no. 2, pp. 84-90, Feb. 1981.

[5] R. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[6] 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, Nov. 2004.

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

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

[9] V. Scarlata, B.N. , B.N. Levine, and C. Shields, “Responder Anonymity and Anonymous Peer-to-Peer File Sharing,” Proc. IEEE Int’l Conf. Network Protocols (ICNP), pp. 272-280, Nov. 2001.

[10] Q.Lv, P.Cao, E.Cohen, K.Li, and S. Shenker, “Search and Replication in Unstructured Peer-to-Peer Networks,” Proc. 16thACM Int’l Conf. Supercomputing, pp. 84-95, 2002.

[11] L.A.Adamic, R.M.Lukose, A.R.Puniyani, and B.A. Huberman, “Search in Power-Law Networks,” Physical Rev. E., vol. 64,p. 046135, 2001.

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

[13] N. Bisnik and A. Abouzeid, “Modeling and Analysis of Random Walk Search Algorithms in P2P Networks,” Proc. Second in p2p Systems, 2005.

[14] R.Morselli, B.Bhattacharjee, A. Srinivasan, and M.A.Marsh,“Efficient Lookup on Unstructured Topologies,” Proc. ACM Symp. Principles of Distributed Computing, 2005.

[15] 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.

[17] K. Sripanidkulchai, “The Popularity of Gnutella Queries and Its Implications on Scalability,” http://www-2.cs.cmu.edu/ ~kunwadee/research/p2p/gnutella.html, 2009.

[18] J. Han, Y. Liu, and J. Wang, “Rumor Riding: Anonymizing Unstructured Peer-to-Peer Systems,” technical report, http://www.cse.ust.hk/~jasonhan/RR-TR.pdf, 2009.

[19] S. Jiang, L. Guo, X. Zhang, and H. Wang, “LightFlood: MinimizingRedundant Messages and Maximizing Scope of Peer-to-Peer Search,” IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 5, pp. 601-614, May 2008.

[20] Abraham and D. Malkhi, “Probabilistic Quorums for Dynamic Systems,”Proc. Int’l Symp. Distributed Computing, 2003.

[21] D. Stutzbach, R. Rejaie, and S. Sen, “Characterizing Unstructured Overlay Topologies in Modern P2P File-Sharing Systems,” IEEE/ ACM Trans. Networking, vol. 16, no. 2, pp. 267-280, Apr. 2008.

[22] A. Medina, A. Lakhina, I. Matta, andJ. Byers, “BRITE: An Approach to Universal Topology Generation,” Proc. Int’l Workshop Modeling, Analysis and Simulation of Computer and Telecomm. Systems (MASCOTS), 2001.

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

[24] S. Sen and J. Wang, “Analyzing Peer-to Peer Traffic across Large Networks,” IEEE/ACM Trans. Networking, vol. 12, no. 2, pp. 219-232, Apr. 2004.