IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 6, Dec-Jan, 2014
ISSN: 2320 - 8791
www.ijreat.org

Non Path Based Mutual Anonymity Protocol For Decentralized P2P Systems

JONISHA S[1], SUREKA V[2]
[1,2]Department of Computer Science and Engineering, Assistant Professors,
S.A ENGINEERING COLLEGE, Chennai, Tamil Nadu, INDIA

Abstract- Existing anonymity approaches are mainly path-based: peers have to pre-construct an anonymous path before transmission. The overhead of maintaining and updating such paths is significantly high. Although anonymizing Peer-to-Peer (P2P) systems often incurs extra traffic costs, many systems try to mask the identities of their users for privacy considerations. Thus the Rumor Riding (RR), a lightweight and non-path-based mutual anonymity protocol for decentralized P2P systems has proposed. Employing a random walk mechanism, RR takes advantage of lower overhead by mainly using the symmetric cryptographic algorithm. We conduct comprehensive trace-driven simulations to evaluate the effectiveness and efficiency of this design, and compare it with previous approaches.

Keywords - Mutual anonymity, Non-Path-Based, Random Walk, Peer-to-Peer.

1 INTRODUCTION

In distributed and decentralized 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 [1],[2],[3],[4], have been proposed to provide anonymity. Those approaches, also known as 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 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, for example RSA [5], when wrapping the layer-encrypted packets. Both the peer collection and content encryption introduce high costs. Practically, users often expect to establish a long anonymous path and update the path periodically to defend against the analysis from attackers [6]. In highly dynamic P2P systems, when a chosen peer leaves, the whole path fails. Unfortunately, such a failure is often difficult to be known by the initiator. Therefore, a "blindly-assigned" path is very unreliable, and users are frequently probe the path and retransmit messages.

To address the above issues, the non-path-based anonymous P2P protocol called Rumor Riding (RR) has proposed [9]. 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 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. We call the agent peer as a sower in this paper.The similar idea is also employed during the

query response, confirm, and file delivery processes. Thus, the rumors serve as the primitives of this protocol to achieve mutual anonymity and meet the design objectives. RR employs a symmetric cryptographic algorithm to achieve anonymity, which significantly reduces the cryptographic overhead for the initiator, the responder, and the middle nodes. In addition, as 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.

2 PROBLEM DEFINITIONS

A number of methods have been proposed to provide anonymity. Most, if not all, of them achieve anonymous message delivery via nontraceable paths comprised of multiple proxies or middle agent peers. Those approaches, also known as 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, which requires the initiator to collect a large number of IP addresses and public keys. In highly dynamic P2P systems, when a chosen peer leaves, the whole path fails. Unfortunately, such a failure is often difficult to be known by the initiator.

3 SYSTEM ARCHITECTURE

In this the initiator encrypts the query message with a symmetric key, and then send the key and the cipher text to different neighbors [5]. The key and the cipher text 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. 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.

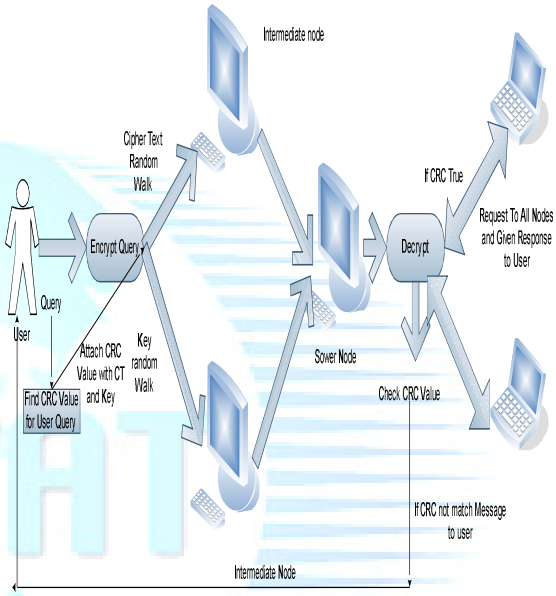

Fig. 1. System Architecture

Each packet is labeled with a Descriptor ID, a string that uniquely identifies the packet [3]. RR also uses the descriptors to identify rumors. For 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. The purpose of the CRC function is to avoid using a complex text understanding technique to distinguish a meaningful Message. 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.

4 MODULE DESCRIPTIONS

Rumor Riding includes four major components: *Topology Construction, Rumor Generation and Recovery, Query Issuance and Response, and Query Confirm and File Delivery.*

4.1 Topology Construction

In this the mesh topology is constructed by getting the names of the nodes and the connections among the nodes as input from the user [7], [10]. Each node has their associated port and IP address is obtained. While adding new nodes, comparison will be done so that there would be no node duplication. Then we identify the source and the destinations.

4.2 Rumor Generation and Recovery

In Rumor Generation and Recovery [2], the RR employs the AES algorithm to encrypt original messages. The key size is 128-bit.

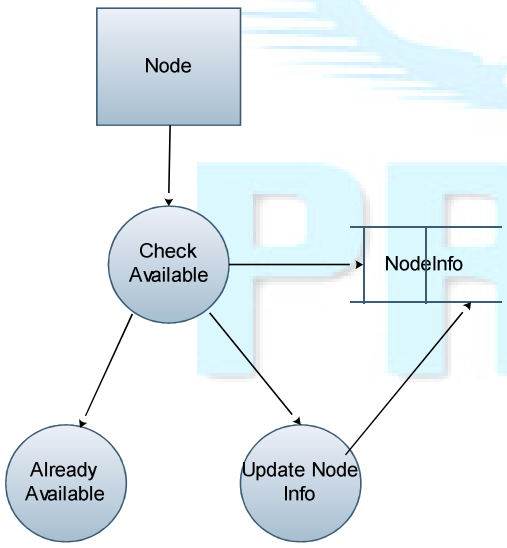

Fig. 2. Topology Construction

To determine whether a pair of cipher and key rumors hit, The Cyclic Redundancy Check (CRC) function is to attach a CRC value, CRC (M), to the message M. The purpose of the CRC function is to avoid using a complex text to distinguish a meaningful M.

4.2.1 Equation to calculate Sower Distribution, Collision Rate and Anonymity

First focus on how to ensure that each query has at the least one sower and that the sowers are evenly distributed over the system. On the key rumor path, the probability of a peer only being visited by this key rumor and not having the cipher rumor is

$$(1 - i \times L / n) \quad \text{---------- 1}$$

The probability of a key rumor terminating its walk without hitting a cipher rumor is given by

$$(1 - i \times L / n)^{L} \quad \text{---------- 2}$$

Thus, the probability of a successful collision in a (i, j)-RR is given by:

$$Ph = 1 - (1 - i \times L / n)^{j \times L} \quad \text{--------- 3}$$

The Degree of Anonymity can be calculated as:

$$(n - 2) / (n - 1) \quad \text{---------- 4}$$

(i.e.) the number of potential initiators/responders is n -1.

4.3 Query Issuance and Response

In Query Issuance and Response, the 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 with

CRC(M').Thus the message is successfully recovered.

4.4 Query Confirm and File Delivery

RR requires every node to temporarily keep a local cache to store the received rumors [3]. 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.

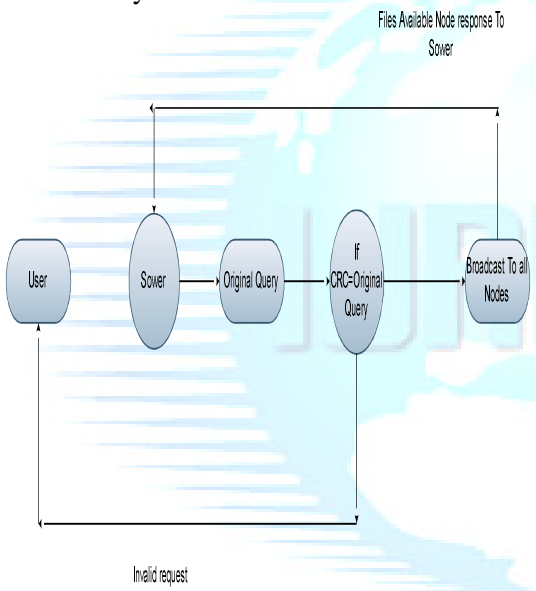

Fig. 3. Query Issuance and Response

5 IMPLEMENTATION RESULT

RR employs a random walk scheme which frees initiating peers from the heavy load of path construction. It eliminates the huge overhead of path construction and maintenance. Thus it provides more Efficient and avoids traffic avoidance. Thus the determination of the exact path where the query message has been walked randomly by design a lightweight mutual anonymous P2P protocol, RR, in which anonymous paths are automatically constructed via the rumors' random walks. So we can reduce the memory management cost for initiator.

6 CONCLUSION

Thus non-path-based mutual anonymity protocol for P2P systems, Rumor Riding (RR), employing a random walk concept, RR issues key rumors and cipher rumors separately, and expects that they meet in some random peers. The results of trace-driven simulations and simple implementations show that RR provides a high degree of anonymity and outperforms existing approaches in terms of reducing the traffic overhead and processing latency.

REFERENCES

[1] 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.
[2] L. Xiao, Z. Xu, and X. Zhang, "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.
[3] R. Sherwood, B. Bhattacharjee, and A. Srinivasan, "P5: A Protocol for 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] L. Xiao, Z. Xu, and X. Zhang, "Low-cost and reliable mutual anonymity Protocols in Peer-to-Peer networks", IEEE Transactions on Parallel and Distributed Systems, 2003.
[7] N. Bisnik and A. Abouzeid, "Modeling and analysis of random walk Search

Algorithms in P2P networks", In Proceedings of HOT-P2P, 2005.
[8] V. Scarlata, B. N. Levine, and C. Shields, "Responder anonymity and Anonymous Peer-to-Peer file sharing", In Proceedings of IEEE ICNP, 2001.
[9] Y. Liu, X. Liu, L. Xiao, L. M. Ni, and X. Zhang, "Location-aware topology Matching in P2P systems", In Proceedings of IEEE INFOCOM, 2004.
[10] C. Gkantsidis, M. Mihail, and A. Saberi,"Random Walks in Peer-to-Peer Networks," Pro. IEEE INFOCOM, 2004.