Rumor Riding: Peer to Peer Systems

Imran Memon[1], Farman Ali Mangi[2] , Deedar Ali Jamro[3] , MUHAMMAD ABDUL BASIT[4], MUHAMMAD HAMMAD MEMON[5]

Abstract

Peer to peer systems are frequently incurred more expense in terms of efficiency transfer and several systems make an effort to cover the uniqueness privacy considerations issues for their users. An anonymity approach mostly existing path base peer before transmits, it has pre-create an anonymous path. An information as well as maintenance transparency of path is a lot high. We proposed mutual anonymity Rumor riding (RR) protocol for decentralization environment peer to peer systems (P2P). The very heavy load path construction carries by RR system using random walk scheme for free initiate peers. We evaluate with before RSA based and also anonymity approach based on AES, RR get extra benefit of lower cryptographic overhead mostly to get anonymity using asymmetric cryptographic algorithm. We illustrate design and effectiveness during the simulations by trace driven. Rumor riding (RR) is very effect and efficient than previous protocols the experimental and analytical result shows us.

Keywords: Random walk, peer to peer (P2P), Mutual anonymity, Non-path-based

1.0 Introduction

Peer to peer (P2P) networks such as Bit Torrent and Gnutella etc could have essential media information spreading and sharing all over the internet. The privacy is growing with the gradually improving in the P2P system. The individual users cannot depend on the trusted and centralized authority in distributed and decentralized P2P environment. For example the defending their privacy is Certificate Authority. In the P2P network users secrete their behaviors and identities by themselves because they are without honest able entities. The both content requesters and providers' condition for anonymity will increase critical.

Some of method [1] proposed to provide the anonymity. Some of them achieve anonymous massage delivery paths are not defined various proxies and core peers agent. Approaches are called as path base approach. The user required to anonymous path setup before transmission. The most of cases data structure the path is a layer encrypted. The strong anonymity provides by path based protocol and an anonymous path to reconstruct the initiator needs to file its collect large number of IP address and private and public key. An initiator performs asymmetric key cryptographic encryption system. User expects to establish extend anonymous path and path update periodically to protect against from attackers [2]. Whole paths fails when leave a selected peer in the P2P system such failure is create difficulty by initiator. Therefore very unreliable path blindly assigned path and users retransmit massage frequently probe the path.

To address these issues, we are proposing anonymous P2P protocol is called Rumor Riding (RR) non path based. The initiator encrypt

[1]School of Computer Science and Engineering, University of Electronic Science & Technology
Chengdu, Sichuan 611731,China
smartimran86@yahoo.com

[2] School of Physical Electronics, University of Electronic Science & Technology
,Chengdu, Sichuan 611731 ,China
farmanali29@yahoo.com

[3] School of Physical Electronics, University of Electronic Science & Technology
Chengdu Sichuan ,611731 ,China
deedar.jamro@salu.edu.pk

[4]School of Communication & Information Engineering , University of Electronic Science and Technology, Chengdu Sichuan 610054
basit_266@hotmail.com

[5]School of Computer Science and Engineering, University of Electronic Science & Technology
Chengdu, Sichuan 611731,China

muhammadhammadmemon@yahoo.com

massage query with asymmetric key further send to cipher text and key to various nearest nodes. Each walk said to be rumor, the random walks individually take cipher text and as well as key in the system. The cipher and rumor key meet together some place only that peer has authority to able recover to the original query massage. In this paper we called agent peer as a sower. During response, file delivery process and confirmation query like similar idea about employed. Rumor gives out primitive to achieve mutual anonymity protocol and meet the design goal and their objectives.

The Rumor riding, random walks the rumor automatically constructed by the anonymous path. The initiator nor and responder neither needs to be concern the path construction and maintenance. Increase anonymity degree of system, RR significantly. Increase the importance of the anonymous servents from the small group nodes in P2P network.

RR employs the asymmetric cryptographic algorithm system to the achieve anonymity. For initiator, responder and middle nodes reduce the cryptographic overhead. Peer have no additional information so it can't build that paths or threat of peer information leakage and peer are request to IP addresses of anonymity but proxies eliminated that link.

2.0 Related Work

The concept of anonymity Chaum pioneered [3] several approaches propose to obtain anonymous communication. It falls in to two categories: anonymous multicasting and other is path based anonymous.Tor [4] is most well like path based protocol would provide initiator anonymity support encryption layer process and onion routing [5] as second generation protocol. They are essentially extra concentration on IP layer less than application layer level. According to response anonymity 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 [6]. Huge crowds present the initiate the random ahead process between two nodes. The peer receive packet there are two options: one it directly sends to the destination peer or it forwarding a packet to the randomly chosen peer.

P5 [1] protocol depend upon to multicast anonymous. Virtual tree P5 employs to make anonymous broadcasting groups, create broadcasting scalable. To sending 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 using symmetric key encryption cryptographic system and RSA algorithm techniques which is not highly sure and also previous work on unstructured P2P system [8] 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. We propose that algorithm it works well to power graphs. To reduce the network traffic, make search scalable. Random walk is statistical method it disclose factor to improving the system performance. The mathematical model [7] analyzed performance of the random walk. We present random based protocol in P2P systems [8]. To protect against sybilguard [9] attacks in the social network employs to random router. These all period study supports strongly and efficiently for random walk in P2P systems.

3.0 Rumour Routing Phases

3.1.1 Rumor Generation and Recovery

To encrypt original messages, RR utilizes ElGamal Cryptosystem. The decide cipher pair and key rumors hit, the Cyclic Redundancy Check (CRC) task used to put together a CRC value, CRC (M), to the message M. The receiving key and cipher rumors the Sower S_a uses ElGamal decryption to recover that message M' and the checksum CRC (M'). Further it performs the CRC task to be recovered M' and evaluate the result with CRC (M'). If they are match, the Sower S is aware that its successfully recovered a message M.

3.1.2 Query Issuance

First An Initiator *I* hope to concern an anonymous query than it creates query content q containing request for some service e.g. request of some file. Initiator then generates two pairs of asymmetric keys, Private Key - K_I^- and public

key - K_I^+ (using Cramer Soup Cryptosystem). The query content q will be made up of the requested service and the Initiator Public key K_I^+.

Before sending, the Initiator can tag this request with the required number of feedback expected. Node *I* then uses ElGamal Cryptosystem to encrypt q and it's Public key K_I^+ into a cipher texts pair **(c_1,c_2).** Initiator then prepares public value ***p*** and a private key ***x*** as the pairs of the keys to decrypt the two ciphers. It organizes the key pair ***(p, x)*** and the cipher texts pair **(c_1,c_2)** into two query rumors, $\mathbf{q_K}$ and $\mathbf{q_C}$. Then two random number strings, IDq_K and IDq_C , are used to two rumors labels and after generate to *I* rumor messages forward to two randomly select neighbors. They start their own random walk when cipher rumor query and query key rumor together.

RR needs each node to provisionally maintain their local cache and accumulate rumors received. The rumor query key of node receive, rumor recovery procedure will performed to check cipher rumor in all cached. If decrypt rumor holding plaintext match the CRC value, q will successfully recovered. Whatever there are match or not, the transitional node decrease the TTL value of the received rumor by one and kept temporary evidence consisting the ID of rumor in local cache and ahead it to a randomly selected neighbor. This is done to confuse the adversary not to suspect that the current node is a Sower. The process is going on up to when TTL value of rumor decrease become to zero. Process will be same when cipher rumor query received. No any specific sequence If rumors query pair reach to exacting node further node would be recover the unique q. The key issue of this procedure is that they select one rumor pair, they required rumors and their initial TTL values carefully as well as the key and cipher meets. Before send out first RR initialized non-zero positive number w (1<w<127) in the Hops rumors field. The undersized number between 8 and 11 would be sufficient confuse to attacker who could try to determine the location of the Initiator. For example, the probable length of rumors' walk is L and L + w is TTL value.

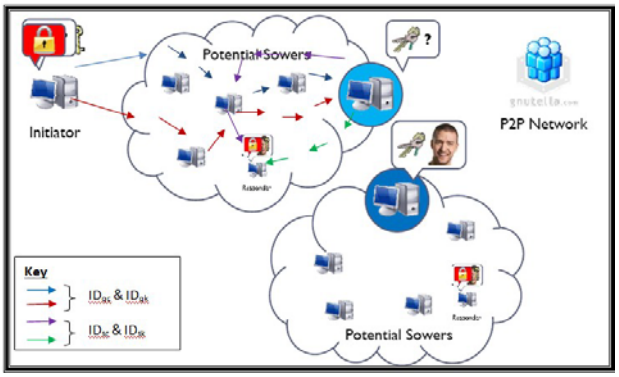

Figure: 1

3.1.3 Sower – Selection of trustworthy agents

The Sower, S_a select randomly a subset S_t of its trusted agents to send request to. The number of the subset agents targeted will be dictated by the request received from Initiator through tagging. Therefore again they are required to select one rumor pair ,initial TTL values and number of rumors as well as key and cipher meet. Sower agent will then change the TTL together with the initial Hop count value and prepare to send the query to get feedback from a subset of its trusted agents S_t. The Sower S_a will then attach the original query message qc (plus *I* Public key K_I^+) called ciphertext pair **(c_1,c_2)** and qk ***(p,x)*** and tag the request with a label ID_{sc} and ID_{sk} respectively plus its IP address in a plaintext. In this operation, sightless flood avoided. Instead, the Sower agent issues the query when agents choose trusted agents subset. Trusted agents are selected based on previous interactions and therefore trusted. Therefore, flooding is done through multicasting in a group of trusted agents. The selective flooding has a constrained flood scope compare to sightless flood, which can decrease the unnecessary traffic caused by multiple Sower flooding.

3.1.4 Query Response

A group of responders can conceal their identities by having all their messages sent to the same address by using multiple public keys generated using ElGamal Cryptosystem. These keys will be disposable, so that no information can be gained by their reuse. To do this, a group of recipients must all agree on one value of *p*. Then each entity chooses their various secret generators *g* and then calculates the values of *x* which correspond to their private key. Each individual then chooses a private key and publishes multiple public keys using it. So, both the Sower and the initiator are not in a position to associate a responder with a public key.

When the receiving node that is in the subset of the target nodes S_t has a copy of the file requested and is willing to respond, it becomes a responder. It will copy the query message and release the message to continue its random walk. Using secret generator *g*, the responder will calculate value of x corresponding to its private key. R then prepares its response as follows:- create two responses, r_k containing the public key pair ***(p,g,x)*** and r_c which contains encrypted response with initiator public key K_I^+ (the key generated using Cramer Soup cryptosystem). The responder then will send both r_k and r_c back to Sower Agent S_a through the normal TCP connection. The responder will do this without revealing its identity due to power of the generator *g*. To deter passive correlation attack the noise packets should be added such that a passive correlation attack becomes infeasible**.** When the Sower agent obtain the reply r_k and r_c, it would be deliver to the originate peers of qc and qk. The descendant nodes remain this process. Two rumors response create use of L_{qk} and L_{qc} to arrive at *I*.

Initiator will then copy received $\mathbf{r_k}$ and $\mathbf{r_c}$ and add few hop counts before sending them out randomly to two different recipients to confuse the adversary. Having two response rumors, *I* then using private key K_I^- (from Cramer Soup Cryptosystem), to get original response message ***r.***

3.1.5 Query Confirm

In the query confirm phase, *I* uses the responder's public key to encrypt the confirm message **c** forming two ciphertexts $\mathbf{(c_1,c_2)}$**.** To confuse the adversary, before send to them out, Initiator will initialize a positive number would be nonzero w (1<w<127) in rumor hops field. Typically, to confuse the adversaries the small number between 8 and 11 would be sufficient who could try to determine the location of the Initiator. The two confirm rumors marked $\mathbf{cr_1}$ and $\mathbf{cr_2}$ will then walk back L_{sk} and L_{sc} path to Sower S_a. The Sower will then flood the two ciphertexts in its group. The correct Responder will be able to decrypt the message since it's the only responder that possesses the corresponding private key.

3.1.6 File Delivery

The confirm message received after the responder using private key and R will encrypt the file with the Initiator Public key to get Data cipher rumor divided into two $\boldsymbol{(u_1,u_2)}$ and ***(e,v)*** and labelled DC_1 and DC_2. Note that the Initiator keys are generated using Cramer Soup Cryptosystem that has integrity check in its decryption step. R then will send the two ciphers to Sower S_a through a TCP connection. The reversed paths of L_{ck} and L_{cc} ,the ciphers would finally arrive *I.* recover I using private key its desired file after confirming the integrity of the file. For files size is high than responders split into multiple segments.

4.0 Security Analysis

First we discuss the anonymity model Rumor Riding protocol accomplishes and we examine its effectiveness under various scenario attack.

Anonymity Model:

Two main types of anonymity model for defining the anonymity degree. The first types of model we define as the anonymity model of the definite node as number of peers it have same chance of provider node, in this term is called anonymity set. Second type measure based information theory. For example mutual information [10], reflect between two same entities such as actual/suspected observer or input/output relations. The initial kind anonymity set almost used to adopt due to capabilities capturing of anonymity the common features. Another model employs focus to information leakage anonymity structure. The usages of this model to analyze the anonymity in so it's change mediums. The superior degree would enhanced the anonymity have been achieved.

4.1 Attacks:

Our assumption is that the number of adversaries' node P and peer chances P/n an adversary. Different situations the adversary would purely observe that the peer sends information lacking any awareness about data spreading. When initiator as well as responder interacts with each other if they cannot identified so initiator and responder we can claim that protocol accomplish unlink capability Our assumption is that report on the base, an adversary nodes look at particular node e communication traversing them and initiated those broadcasting. An adversaries' also have capability to do active attacks such as hijacking, dropping, Controlling flows, forging packets and connection of the networks etc .we analyze some

major attacks that threaten a P2P anonymity protocol this technical report [11].

4.1.1 Message coding attack:

The passive attackers try to trace the massage in the system. Adversary analyzes message coding format then modify massage coding format. An adversary mostly forced to do encryption in anonymous design. For example the anonymous structure previous to arrive. if the sender sends massage to receiver an adversary trace massages signal from sender and receiver [12], anonymity random walk forward protocol is vanished. RR give unlink capability to the fresh nodes if the observers get a rumor it cannot link the query to receiver because rumor riding uses asymmetric encryption and the massage splits in two parts. The single rumor could not disclose the information of the query.

4.1.2 Local collaborating attack:

Two collaborating adversaries might be neighbors of the initiator. Nearest attackers may be collaborator and could observe traffic transient through the possible neighboring initiators .Try to confuse the narrow adversaries and RR sower choice a subset its nearest nodes send to plaintext query and two collaborating nodes would not get by query (plaintext+ cipher/key). An initiator is monitoring node and a responder that attackers merely bet. The attackers do not compromise three e neatest nodes, Rumor riding does not focus of the local collaboration attack. The nonlocal collaboration attack, it's defending together with the trackback attack.

4.1.3 Timing attack:

The time attack [13], an adversary would deduces the association. The rumor riding is protected in because rumors are delivering information overlay in network and RTT measurement don't disclose distance to responder. An attacker trace to rumor due to limited time variation locate the responder and it required tracing . sower issue appeal after it gets pair of query rumors and time dependent on rumor random walks .

4.1.4 Predecessor attack:

Some anonymous system an initiator would frequently communicates to the specific responder in a lot of rounds. Predecessor attack [14] where the adversaries control to the subset of nodes. Rumor riding the random walks and communicates with random sowers. The sower gives initiator or responder is unpredictable and whole system is randomly distributed. Adversaries don't carry out such kind of an attack to verify responder or initiator. The rumor riding cannot subject to do these types of attacks.

4.1.5 Traffic analysis attack:

The adversary can take out information in the traffic flow management such as packet calculation, communication pattern, massage size [15].The same way traffic analysis attacks, If large fraction of the network controlled by attackers. Example, the traffic based shaping [16], an adversaries stop traffic in implicit nodes and the traffic variation examine when they are slightly moderate the blocking the traffic way. Show the real traffic. An attack performing consequentially the reverse path of traffic and adversaries can be determining initiator easily. This attack is much greater to RR vulnerable; the subsequent massage does not belong to similar traffic. There is no continuous path in rumor riding

5. Experiment and evaluation

We evaluate RR using three evaluation metrics in section A, in section B followed by experiment setup and evaluation results in section C.

A. Evaluation Metrics

We evaluate RR using following metrics.

Collision rate: we verify theoretical collision rate and we observed that the real tracing with distribution of collision rate. We also verify that use these result to show rumor parameters are selected.

Collision distance: The higher anonymity means longer collision distance also raising the query delay as well as traffic overhead.

Number of sower*:* we are suppose number of sowers in query cycle and every sower find to

an initiator also number of sower incur fake query message and few sower have fail to afford sufficient reliability and redundancy.

Traffic overhead: The lot of traffic overhead corresponds to broad latency in bandwidth and data delivery. We more concerned additional traffic overhead by anonymous components.

B. Experiment Setup

In our experiment setup, we use the BRITE [17] to generate the 40,000-150,000 node in the internet such as topologies. We simulated the physical internet layer p2p nodes overlay [18]. We using ultra peers for the snapshots it's performing the search hybrid Gnutella and also use Ion's tracing to simulated topologies. In our experiments we simulated ran different trace and range 15000 to 150,000 nodes.

To achieve to Elgamal algorithm use in RR protocol, we use cryptosystem which give normal cryptographic function. In our experiment for simulation and implementation both are contact using ThinkPad laptop with 2 GB memory and a Core (TM) 2 Duo 2.00 GHz Intel processor, 80 GB hard disk and network card. The dynamic properties we simulated of p2p overlay network query cycle each node and we choice 800 second [19, 20] for each node pass query cycle each second it become decreases disappear the following system after some second and new query peer select for physical internet layer connect and as previous one .

C. Evaluation Results

We first think about the single rumor spreading collision rate. We verify the theoretical collision rate. In RR scheme we trace rumor spreading process. The collision rates are normal results presented in figure 3. In figure 2 collision rate is typical upper than the theoretical result we observed. The Gnutella networks follow by the small world characteristic. In the random path P2P network higher node degree also collision rates higher than the homogenous network. We get the lower bound of rumors, TTL and k of each rumor L is same to k x L, to set the rumor in our protocol we obtain result.

We plotted figure. 4, the collision distance is important because it is corresponding tradeoff between query delay and user anonymity in RR design. This figure shows average distance tends no less than 80. The guarantees that most of collision distance is longer than 80. We are suggested that number of rumor should be 40. In figure. 5 show us the time, number of sowers sort to keep away from large number of fake query message. We choice only 20 sowers should be range [150-300] to meet scalability and reliability both requirements.

We think about the traffic overhead. We evaluated RR with other work. We put 15,000 queries our system and we plotted figure.6 cumulative distribution add RR schemes traffic overhead. In our experiment various traffic overhead further we observe that traffic overhead is lower than (7, 7)-RR scheme, traffic overhead is smaller than our protocol. In figure.7, we observed that cumulative distribution of a time response is different than RR scheme if we evaluated them increase the number of rumors and decrease the average response latency, larger number of rumor more traffic overhead and fake queries message we evaluate RR protocol has better time response compare and traffic overhead.

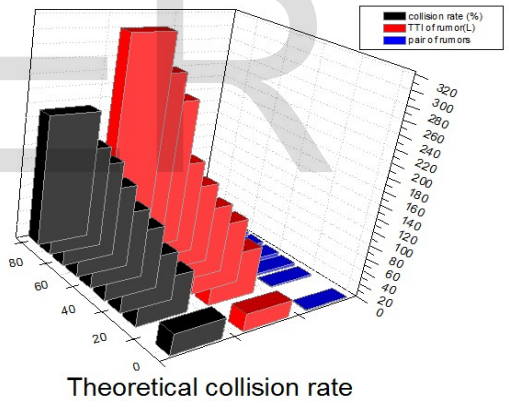

Figure 2

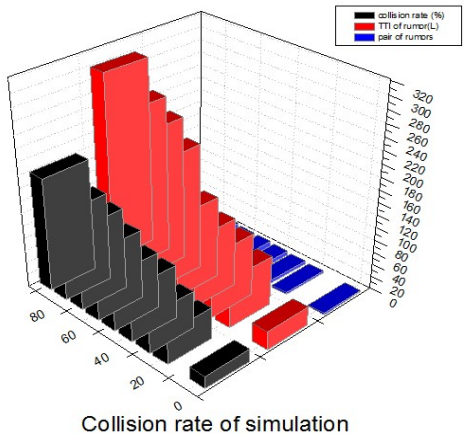

Figure 3

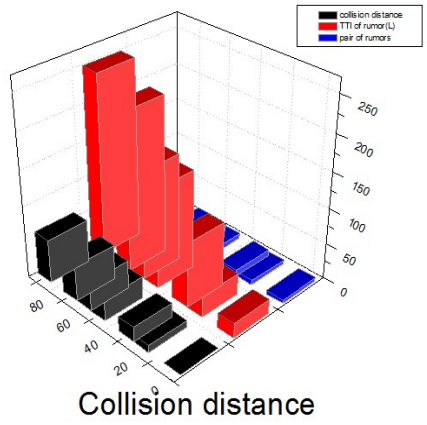

Figure 4

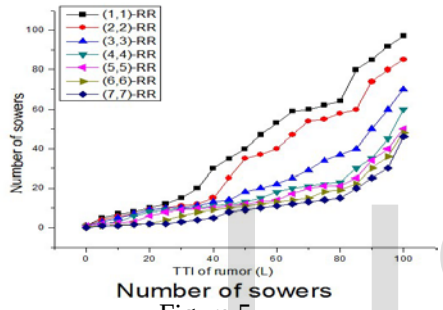

Figure 5

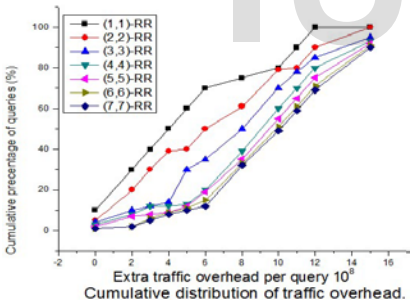

Figure 6

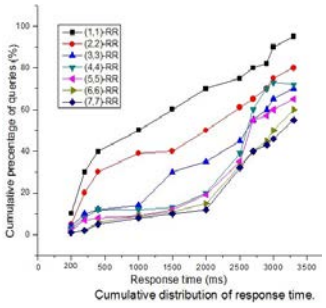

Figure 7

6.0 CONCLUSION

The mostly path base approaches are anonymity approaches. Before transmission peers select the core nodes and build paths. The updating and maintenance of paths are very high. This paper we focus on mutual anonymity non path base protocol use for the structure Peer to peer system. RR rumor key and cipher rumors, Rumor riding using random walk to disjointedly and guessing they would be meet in various random peers. RR give us higher level of anonymity and better performance in overhead traffic approach in result of trace driven simulation and RR can defend successfully against most popular attacks we already discuss in security analysis portion we practically implement our prototype. Our speed query ongoing work in traffic they confuse to attacker and also we reduce the overhead traffic. An information leakage, unlinkability and failure tolerance different attacks these properties we examine RR security.

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. Wright, M. Adler, B.N. Levine, and C. Shields, "Thev 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

[3] 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.

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

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

[6] 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.

[7] 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.

[8] Yunhao Liu, Senior Member, IEEE,Jinsong Han, Member, IEEE, and Jilong Wang, Member, IEEE "Rumor Riding: Anonymizing Unstructured Peer-to-Peer Systems", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 3, MARCH 2011.

[9] 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.

[10] Y. Zhu, X. Fu, R. Bettati, and W. Zhao, "Analysis of Flow-Correlation Attacks in Anonymity Networks," Int'l J. Security and Networks, vol. 2, nos. 1/2, pp. 137-153, Mar. 2007.

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

[12] R. Sherwood, B. Bhattacharjee, and A. Srinivasan, "P5: A protocol for scalable anonymous communication", In Proceedings of IEEE Symposium on Security and Privacy, 2002.

[13] B.N. Levine, M.K. Reiter, C. Wang, and M. Wright, "Timing Attacks in Low-Latency Mix Systems," Proc. Eighth Int'l Conf. Financial Cryptography, 2004.

[14] 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, 2004.

[15] Y. Zhu, X. Fu, B. Graham, R. Bettati, and W. Zhao, "Correlation-Based Traffic Analysis Attacks on Anonymity Networks," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 7, pp. 954-967,July 2009.

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

[17] A. Medina, A. Lakhina, I. Matta, and J. Byers, "BRITE: an approach to universal topology generation", In Proceedings of the International Workshop on Modeling, Analysis and Simulation of Computer and Telecommunications Systems (MASCOTS), 2001.

[18] X. Zhang, Q. Zhang, Z. Zhang, G. Song, and W. Zhu, "A construction of locality-aware overlay network: mOverlay and its performance", IEEE JSAC Special Issue on Recent Advances on Service Overlay Networks, 2004.

[19] S. Sen and J. Wang, "Analyzing Peer-to-Peer traffic across large networks", In Proceedings of ACM SIGCOMM Internet Measurement Workshop, 2002.

[20] 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.