ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Trusted rumor riding protocol in P2P network

Mary Subaja Christo[1*], Dr.S.Meenakshi[2]
[1]IT Department, Sathyabama University, Chennai, India
[2]IT Department, SRR Engineering College, Chennai, India
***Corresponding author: E-Mail: marysubaja@gmail.com**

ABSTRACT

Non Path P2P protocol is called Rumor Riding (RR). In RR protocol the initiator sends the key message and cipher text to different neighbors. The key and cipher text takes random walks separately in the system. Each walk is called rumor. Through the random walk rumor mechanically constructs the anonymous path. The initiator nor the responder need not be worried with the path structure and protection. The Rumor Riding protocol uses random walk based algorithms which can be easily exploited by uncooperative and malicious nodes. Rumor Riding protocol focuses only on anonymous searching and downloading on P2P systems. But anonymity opens the door to possible misuses and abuses, exploiting the P2P network, giving the chance to attacks like reply attack, Trojan Horse, IP Spoofing. In the Rumor Riding protocol, if the responder acts as a malicious node, then there are possibilities for replay attack to occur. In reply attack, IP Spoofing takes place where a malicious node can use the IP address of the responder node and acts as the responder's node. This eventually reduces the performance of the network. To address this problem Responder should be authenticated by the initiator. In this paper we propose a authentication scheme called pseudo Trust (PT) to implement in RR where each peer instead of using its real identity, generates an unforgettable Zero knowledge proof is based on the authentication so peers can authenticated without leaking any sensitive Information and also PT helps to evaluate the levels of security and anonymity in RR and also analyze the security issues of Rumor Riding protocol and the simulation results shows less packet delivery ratio, more delay time and less throughput and the poor performance of Rumor Riding with Responder attack and also shows better performance of Trust with RR protocol.

KEY WORDS: Rumor Riding, Reply Attack, Random Walk, Pseudo Trust, Annonymous Searching.

1. INTRODUCTION

P2P is an alternate network model it provided by the ancient client server architecture. A peer plays the role of a user and a server at the constant time. That is, the peer will initiate requests to alternative peers, and at constant time answer incoming requests from alternative peers on the network. It differs from the normal consumer-server model wherever a client will only send requests to a server so watch for the server's response. When a peer goes down or is disconnected from the network, the P2P application can continue by victimization alternative peers. As an example, in a very Bit Torrent system, any shoppers downloading a precise file are serving as servers. Once a consumer finds one among the peers isn't responding, it searches for alternative peers, picks up components of the file wherever the previous peer was, and continues the transfer method. Compared to a client-server model, where all communication can stop if the server is down, a P2P network is additional fault-tolerant. Rumor Riding protocol focuses only on anonymous searching and downloading on P2P systems. But anonymity opens the door to possible misuses and abuses, exploiting the P2P network, giving the chance to attacks like reply attack, Trojan Horse, IP Spoofing. In the Rumor Riding protocol, if the responder acts as a malicious node, then there are possibilities for replay attack to occur. In reply attack, IP Spoofing takes place where a malicious node can use the IP address of the responder node and acts as the responder's node. This eventually reduces the performance of the network. To address this problem Responder should be authenticated by the initiator so authentication is necessary to implement in peer to peer networks. In this paper, we propose a authentication scheme called pseudo Trust (PT) to implement in RR where each peer instead of using its real identity, generates an unforgettable Zero knowledge proof is based on the authentication, so peers can authenticate without leaking any sensitive Information and also PT helps to analyze the levels of security and anonymity in RR and also analyze the security issues of Rumor Riding protocol.

Related work: In this section we analyze the security problems in RR protocol and study the importance of Security in Peer to Peer networks and describe the different types of attackers in P2P network. The attacker is a node in the network and must discover the pseudo ID of its neighbors Sender is Probable Innocence to nodes and responder. Responder is Probable Innocence to nodes and sender. Its connections and the real addresses of the nodes each of these connections leads too. The pseudo IDs from the messages it has seen. For each pseudo ID, the ordered over which the attacker receives message the "to" and "from" pseudo address of all the messages past across it. The attacker may also send messages. It can form message out of its own random values, its own address or any address is has seen. In particular, it can send messages the wrong way. Attacker can make a message with another nodes pseudo ID as the from address. This lets it disrupt communication. We can generate a key pair and use the authentication key as the pseudo ID.

The sender signs the message ID. Hence the attacker cannot fake messages. Danezis (2006) studied attacks on peer discovery and route setup in anonymous peer-to-peer networks. They show that if the assailant learns the set

of nodes well-known to the instigator, its routes are often fingerprinted unless the instigator is aware of a few substantial fraction of the network. Danezis (2005) extend this work to look at that an assailant WHO learns that bound nodes ar unknown to the instigator will perform attacks still and separate traffic hunting a relay node. Each these attacks assume a world passive person, however are similar in spirit to the restricted topology attack. Another attack relevant to P2P systems is that the circuit preventative attack, as McLachlan (1998) ascertained that, in P2P systems, this attack will reveal verity instigator. They planned a random honest queuing mechanism to mitigate the attack. We tend to note that the circuit preventative attack is especially effective against a restricted route topology, since throughout trace back of the stochastic process, there square measure solely d potentialities at every step.

Our extension of exploitation solely the last 2 hops of AN l hop stochastic process for anonymous communication makes the trace back considerably tougher for the individual, since it's currently necessary to live d l2 hosts. Many necessary attacks think about the degradation of name endlessness with time. The precursor attack, originally planned by bacteriologist and Rubin (2002), has been analyzed thoroughly by Wright (2003; 2006). As applied to our work, the attack notes that eventually a low-anonymity circuit are made. Guard nodes [18] area unit a defense against precursor attacks that's employed in this version of Tor (2000). However, the utilization of guard nodes in P2P systems desires a lot of study; an easy implementation would permit attackers to quickly make an efficient obscurity set size of d. Intersection attacks work by noting that nodes area unit active at the time a message is received. These attacks square measure a specific concern for P2P systems thanks to the extremely dynamic participation of most nodes. The simplest approaches for combating these attacks square measure to scale back the attitude on the network that's given to the attackers. However, even with the simplest defenses, an oversized fraction of nodes are ready to bring home the bacon a near-global read. Our redundant topology exacerbates the matter by increasing the effective node degree. Whether or not a network that's resilient to intersection attacks can do similar levels of obscurity to our style remains Associate in nursing open question. A variant of intersection attack is applicable on our protocol, wherever rather than noting the set of active nodes, the antagonist will use the probabilistic data regarding the instigator victimization the restricted topology attack. This attack would work a lot of quicker as compared to the normal intersection attack. As a result of lack of house, we've omitted an entire analysis of this attack. Our results indicate that the Delaware Bruijn topology is ready to effectively resist this attack.

Kinds of attackers are: a) Global Attacker, b) System Membership, c) Time-to-Live Attacks (Mute, Mantis), d) Multiple Attackers (Mute), e) Statistical Attacks (Mixes), f) Forced Repeat (Crowds), g) Nodes Joining and Leaving, h) Denial of Service (Mute).

1.1. Security issue in RR: In this work RR protocol will be authenticated using Zero Knowledge Proof Speudo Trust Protocol. In this implementation Initiator send a query request to the Responder using non path method that is the query request has the content of Cipher Rumor and the Key Rumor and it takes a random walk to reach the Intermediate Agent node using the blind flooding method.

Agent node is one which gets these two Rumors (Cipher rumor and Key rumor) and it decrypts the Cipher text using the Key value it will get back the original message and the CRC (M). Now the CRC in Agent node will be calculated and this will be checked out with the existing CRC value of the original message to ensure that the original message has not been corrupted and now this Agent node will add the IP address to the message.

The Agent node will create a subset of peers which has not reached in the random walk method and now the agent node can broadcast the query message to the neighbors using the selective flooding method. More than one node in the subset has the desired copy of the original message and that node can act as a Responder.

1.2. Security Issues and Analyzes of RR Protocol: Rumor Riding protocol focusses exclusively on anonymous looking out and downloading in P2P systems. However obscurity opens the door to attainable misuses and abuses, exploiting the P2P network as the simplest way to unfold tampered with resources, as well as Trojan Horses, viruses, and spam. Below the study of RUMOR RIDING PROTOCOL we tend to known variety of security problems.

1.3. Responder Node as Malicious Node: In RR protocol forwarding message using anonymous non path based method here the responder node receive the request file from Initiator and send Query response message to Initiator using non path based method. In this transmission if the responder acts as a malicious node, then there are possibilities for reply attack to occur. In reply attack, IP Spoofing takes place where a malicious node can use the IP address of the responder node and acts as the responder node. This eventually reduces the performance of the network.

The list of issues are available in RR protocol if the Responder node as malicious:

- IP Spoofing takes place
- Sends Fake response message
- Reduce Network Performance
- Spreading virus to the network Making packet dropping

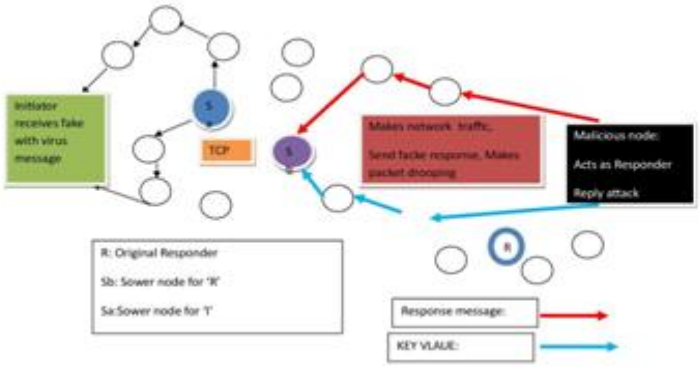

Fig.1. Responder as malicious node

2. PROPOSED WORK

In this work RR protocol will be authenticated using Zero Knowledge Proof Speudo Trust proto-col (ZKPT). In this implementation Initiator send a query re-quest to the Responder using non path method that is the query request has the content of Cipher Rumor, key Rumor and it takes a random walk to reach the Intermediate Agent node using the blind flooding method. Intermediate node is one which gets these two Rumors (Cipher rumor and Key rumor) and it decrypts the Cipher text using the Key value, it will get back the original message and the CRC (M). Now the CRC in Agent node will be calculated and this will be checked out with the existing CRC value of the original message to ensure that the original message has not been corrupted and now this Agent node will add the IP address to the message.

2.1. Query Issuance: The Intermediate node will create a subset of peers which has not reached in the random walk method and now the agent node can broadcast the query message to the neighbors using the selective flooding method. More than one node in the subset has the desired copy of the original message and that node can act as a Responder (R). In this proposed system the Responder will be Authenticated by Initiator before receiving the File here the Initiator ask the challenge question to responder and responder send the answer with proof ,then initiator ask proof verification responder send the proof verification now initiator check the verification if the responder is trusted node then the Initiator ready to Receive the File After this Authentication process Responder delivers the File to Initiator By making use of this authentication packet delivery ratio has been calculated and it results that authenticate with the Rumor Riding provides higher security and Most efficient one. In Fig. 2 shows Query issuance here In this implementation Initiator send a query request to the Responder using non path method that is the query request has the content of Cipher Rumor ENC (M, CRCM) and the key Rumor (Ki+-Public key of Initiator) and it takes a random walk to reach the Intermediate Agent node using the blind flooding method. Intermediate node is one which gets these two Rumors (Cipher rumor and Key rumor) and it decrypts the Cipher text using the Key value, it will get back the original message and the CRC (M). Now the CRC in Agent node will be calculated and this will be checked out with the existing CRC value of the original message to ensure that the original message has not been corrupted and now this Agent node will add the IP address to the message. The Intermediate node will create a subset of peers which has not reached in the random walk method and now the agent node can broadcast the query message to the neighbors using the selective flooding method. More than one node in the subset has the desired copy of the original message and that node can act as a Responder(R).

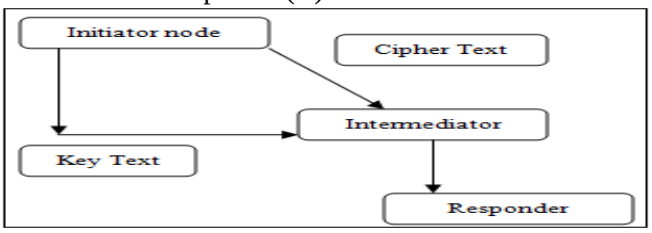

Fig.2.Query issuance

2.2. Query Response: In Fig 3 shows the responder sends the response message to the Initiator first responder encrypt the response message using Initiator public key and send the private key of responder also now these two keys takes random walk and meet new Agent B which is decrypt the message using key value and add IP address of Agent B then connect to Agent A using TCP connection now Agent A forward message to Initiator using length of Cipher text and Key text.

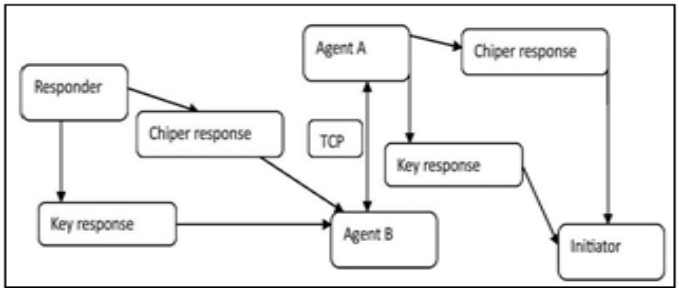

Fig.3.Query Response

2.3. Ask Challenge Question-Initiator: Due to lack of security problem in RR protocol the initiator should authenticate the responder because the responder's node may be act as a malicious node which can send fake message and spread virus Fig 4 shows initiator ask the challenge question to responder using non path methods and Fig 5 shows responder send the Answer to the initiator using non path method.

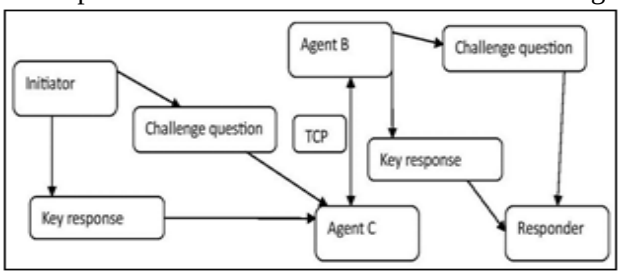

Fig. 4. Challenge question to the Responder

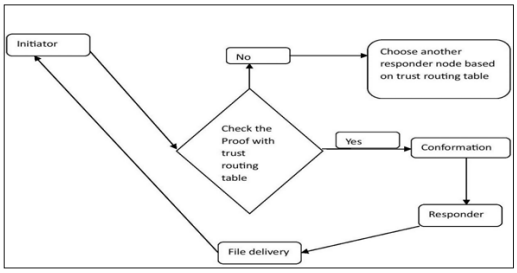

Fig.5. The responder sends the answer

2.4. Proof Verification: The Initiator receive the Challenge question answer from the responder and the initiator needs to verify the proof using the similar concept of (Ask challenge question) the initiator ask the proof and using the similar concept of (Responder Send the answer) the responder send the proof verification to Initiator. The challenge question is based on the secret information of responder now responder send the answer which is does not based on the real information but the answer should be matched with real information in Fig 6 shows Initiator receive both answer and proof from the responder now initiator need to verify that information with trust table value if it satisfied the responder transmit the file to initiator if it is not satisfied discard the responder and choose another responder using trust value method with help of trust based algorithm.

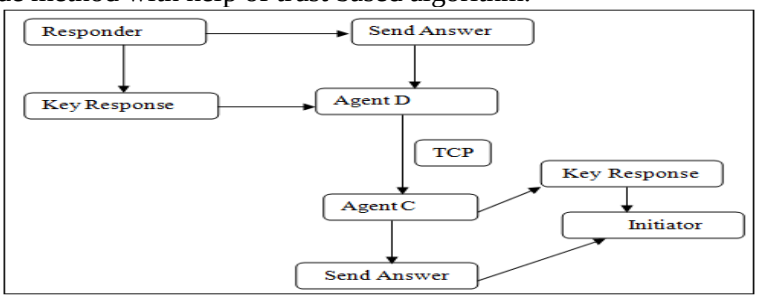

Fig. 6. File delivery

2.5. Implementation: We implemented a RR protocol on the NS2 simulator and we used the C++ library to implement all built in crypto-graphic algorithms. In Rumor Riding protocol following some components previous works show that In RR protocol using SOWER node (intermediate or agent) requires TCP links to forward queries between them. [2]In RR protocol using AES algorithm for ENCRYPT and DECRYPT the original query we are using the key size is 128 bit[3] In query generation we send query value and key value using random walk method We examined the throughput ,packet delivery ratio and end-end delay In this paper we implement RR protocol and add the malicious node in peer to peer network as Initiator, Responder and Sower nodes using NS2 simulator because in RR these three nodes are important nodes to forward the query from source node to Destination node finally show the simulation result and poor performance of RR protocol ,compare the results of RR without malicious and RR with malicious node. Our simulation results show that poor performance of RR when the malicious node occur in RR protocol.

3. RESULTS

When the malicious nodes occur in Rumor Riding Proto-col the network shows poor performance. In this result, we are calculating Packet delivery ratio, Throughput, End-End Delay.

Packet Delivery Ratio: The Packet delivery ratio used to find the average of successful received packets from the total number of sending packet. Packet Delivery Ratio=Number of successful Received pack-ets/total number of packets. Here we also find the ratio of the unsuccessful received packet we are using a graph to show the result in the graph X-shows simulation time (unit sec) and Y-shows successful received packets compare with RR results and RR with mali-cious node results. The network performance shows RR with malicious has very poor than the RR results.

Throughput: In this parameter we are calculating successful received packet at a particular time—(based on average). Throughput [kbps] = (recvdSize/(stopTime-startTime)) * (8/1000)). In the graph X-shows simulation time (Sec) and Y-shows packet successful received time (KBPS).

End-End delay: The delay time for communication between node to node End to End delay=End to End delay/count. Calculate how long time need for unsuccessful received packets so delay time will get more in RR with malicious node than the RR protocol In the graph X-shows simulation time(sec) and Y-shows delay time(MiliSec).

3.1. RR with Replay Attack RR-PDR: In Fig (7) shows the comparison between RR and RR with attacker In RR protocol shows good performance for delivering the packet, but when the replay attacker in RR protocol the simulation result shows poor performance of delivering the packet. In graph X-shows simulation time the unit is second Y-shows packet delivery ratio In the case of RR protocol the graph shows for 5 seconds 95 percentage, 10seconds 98 percentage, 15 seconds 98 percentage, 20 seconds 99 percent-age, 25 seconds 99 percentage, 30 seconds 99 percentage it is very good performance shows in RR protocol but In the case of Replay attacker with RR protocol the graph shows for 5 seconds 62 percentage, 10seconds 59 percentage, 15 seconds 58 percentage, 20 seconds 57 percentage, 25 seconds 56 percentage, 30 seconds 54 percentage it is show very poor performance than RR protocol.

3.2. RR with Replay Attack RR-Throughput: In Fig (8) shows the comparison between RR and RR with attacker In RR protocol shows high rate of successful received packet ratio but when the replay attacker in RR protocol the simulation result shows low rate of successful received packet ratio. In graph X-shows simulation time the unit is second Y-shows successful received packet ratio the unit is KBPS. In the case of RR protocol the graph shows for 5 seconds 471.95 KBPS, 10seconds 482.84 KBPS, 15 seconds 485.87 KBPS, 20 seconds 487.41 KBPS, 25 seconds 492.00 KBPS, 30 seconds 500.87 KBPS shows high rate of successful received packet ratio but In the case of Replay attacker with RR protocol the graph shows for 5 seconds 418.44 KBPS, 10seconds 449.04 KBPS, 15 seconds 465.06 KBPS, 20 seconds 472.37 KBPS, 25 seconds 467.03 KBPS, 30 seconds 465.91 KBPS the simulation result shows low rate of successful received packet ratio than RR with throughput.

3.3. Responder as Malicious Node-Delay: In Fig (9) shows the comparison between RR and RR with attacker In RR protocol shows very less delay ratio for received the data but when the replay attacker in RR protocol the simulation result shows very high delay rate of received packet ratio. In graph X-shows simulation time the unit is second Y-shows delay rate the unit is milliseconds. In the case of RR protocol the graph shows for 5 seconds 518.8011 MS, 10seconds 18.6059 MS, 15 seconds 19.5155 MS, 20 seconds 19.1753 MS, 25 seconds 23.9048 MS, 30 seconds 36.585 MS shows low delay rate of received packet but In the case of Replay attacker with RR protocol the graph shows for 5 seconds 421.071 MS, 10seconds 834.139 MS, 15 seconds 999.904 MS, 20 seconds 1067.84 MS, 25 seconds 1122.41 MS, 30 seconds 1197.92 MS, the simulation result shows high delay rate of received packet ratio than RR with throughput.

Fig. 7. Compare with RR and replay attack (PDR)

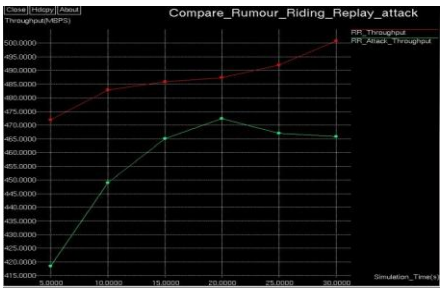

Fig. 8. Compare with RR and replay attack (Throughput)

Fig.9.Comparison replay RR with malicious RR –delay

3.4. RR with TRR-PDR: In Fig (10) shows the comparison between RR with TRR. In TRR protocol shows good performance for delivering the packet but in RR protocol the simulation result shows poor performance of delivering the packet. In graph X-shows simulation time the unit is second Y-shows packet delivery ratio.

In the case of RR protocol the graph shows for 5 seconds 96 percentage, 10seconds 98.3 percentage, 15

seconds 98.9 percentage, 20 seconds 99.5 percentage, 25 seconds 99.7 percentage, 30 seconds 99.7 percentage it is very good performance shows in TRR protocol but In the case of Replay attacker in RR protocol the graph shows for 5 seconds 95 percentage, 10seconds 98 percentage, 15 seconds 98 percent-age, 20 seconds 99 percentage, 25 seconds 99 percentage, 30 seconds 99 percentage it is show very poor performance than TRR protocol

3.5. RR with TRR-Throughput: In Fig (11) shows the comparison between RR with TRR. In TRR protocol shows high rate of successful received packet ratio but In RR protocol the simulation result shows low rate of successful received packet ratio. In graph X-shows simulation time the unit is second Y-shows successful received packet ratio the unit is KBPS. In the case of TRR protocol the graph shows for 5 seconds 502.95 KBPS, 10seconds 503.84 KBPS, 15 seconds 505.87 KBPS, 20 seconds 507.41 KBPS, 25 seconds 509.00 KBPS, 30 seconds 510.87 KBPS shows high rate of successful received packet ratio but In RR protocol the graph shows for 5 seconds 471.95 KBPS, 10seconds 482.84 KBPS, 15 seconds 485.87 KBPS, 20 seconds 487.41 KBPS, 25 seconds 492.00 KBPS, 30 seconds 500.87 KBPS the simulation result shows low rate of successful received packet ratio than RR with throughput.

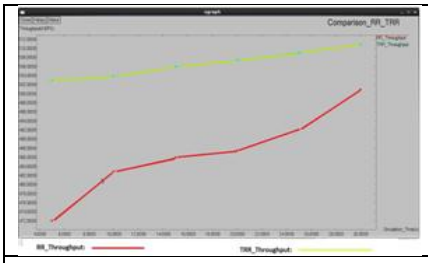

Fig.10. Comparison replay RR with TRR-PDR

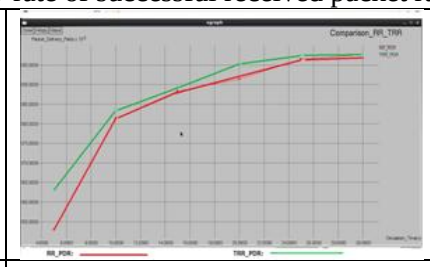

Fig.11.Comparison replay RR with TRR-Throughput

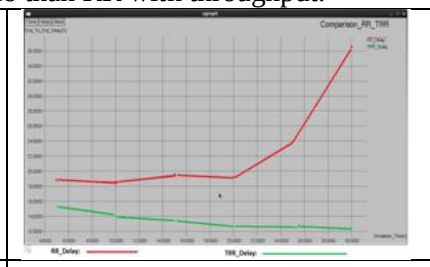

Fig.12.Comparison replay RR with TRR-Delay

3.6. RR with TRR-Delay: In Fig (12) shows the comparison between RR with TRR. In TRR protocol shows very less delay ratio for received the data but In RR protocol the simulation result shows very high delay rate of received packet ratio. In graph X-shows simulation time the unit is second Y-shows delay rate the unit is milliseconds. In the case of TRR protocol the graph shows for 5 seconds 15.1349 MS, 10seconds 14.1225 MS, 15 seconds 13.4563 MS, 20 seconds 12.6945 MS,25 seconds 12.575 MS ,30 seconds 12.523 MS shows low delay rate of received packet but In RR protocol the graph shows for 5 seconds 18.8011 MS, 10seconds 18.6059 MS, 15 seconds 19.1753 MS, 20 seconds 19.1753 MS, 25 seconds 23.9048 MS, 30 seconds 36.585 MS the simulation result shows high delay rate of received packet ratio than RR with throughput.

4. CONCLUSION

Overcome the number of security issues of the RR protocol this could be solved using authentication mechanism. So in this paper we analyze the security issues of Rumor Riding protocol and the simulation results shows less packet delivery ratio, more delay time and less throughput and the poor performance of Rumor Riding protocol when these attacks occur in RR protocol implemented.

Future enhancement: In RR the initiator is act as a malicious node which is may be send fake request message to the responder and the responder is a malicious node occur man in middle attack and may use another node IP address To address this problem Initiator should be authenticated by responder as well as responder should be authenticated by the inititor so authentication is necessary to implement in peer to peer networks. In our future work we propose a zero knowledge authentication scheme called pseudo Trust (PT) to implement in RR where each peer instead of using its real identity, generates an unforgettable Zero knowledge proof is based on the authentication so peers can authenticated without leaking any sensitive Information and also PT helps to analyze the levels of security and anonymity in RR and evaluate its performance using trace-driven simulations.

REFERENCES

Back A, Moller U, and Stiglic A, Traffic Analysis Attacks and Trade-Offs in Anonymity Providing Systems, In Proceedings of the IH, 2001.

Berthold O, Federrath H, and Kohntopp M, Project Anonymity and Un observability in the Internet, In Proceedings of CFP, 2000.

Bisnik N, and Abouzeid A, Modeling and Analysis of Random Walk-Search Algorithms in P2P Networks, Proceedings of Second International Workshop Hot Topics in Peer-to-Peer Systems, 2005.

Chuang, Ming-Chin, and Meng Chang Chen, An Anonymous Multi-Server Authenticated Key Agreement Scheme Based on Trust Computing Using Smart Cards and Biometrics, Expert Systems with Applications, 41 (4), 2014, 1411-1418.

Danezis G, and Clayton R, Route Fingerprinting in Anonymous Communications, Proceedings of the Sixth IEEE International Conference on Peer-to-Peer Computing, 2006.

Danezis G, and Syverson P, Bridging and fingerprinting: Epistemic Attacks on Route Selection, In Proceedings of PET, Leuven, Belgium, 2008.

Ernesto Damiani, and De Capitani di Vimercati, A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks, Proceedings of the 9th, 2002.

Goldschlag D, Reed M, and Syverson P, Onion Routing, Comm. ACM, 42 (2), 1999, 39.

Han J, Liu Y, Zero Knoweledge Proof Pesudo Trust Method in un structures Peer-to-Peer Systems, Technical Report, http://www.cse.ust.hk/ jasonhan/RR-TR.pdf, 2009.

Harlow R, Addison-Wesley, Sherwood R, Bhattacharjee B, and Srinivasan A, P5: A Protocol for Scalable Anonymous Com-Munication, Proceedings of IEEE Symp. Security and Privacy, 2002, 58-70.

Hazel, and Wiley B, Achord: A variant of the Chord Lookup Service for Use in Censorship Resistant Peer-to-Peer Publishing Systems, In Proceedings of IPTPS, Cambridge, MA, 2002.

Kopka H, and Daly P.W, A Guide to Latex, 3rd Ed. Harlow, England: Addison-Wesley, 1999.

McLachlan J, and Hopper N, Dont Clog the Queue: Circuit Clogging and Mitigation in P2P Anonymity Schemes, International Proceedings of FC, 2008.

Murdoch S.J, and Danezis G, Low-Cost Traffic Analysis of Tor, International Proceedings of S.P, 2005.

Raymond J.F, Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems, In H.Federrath, Editor, Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Un observability, Springer-Verlag, LNCS 2009, July 2000.

Reiter M, and Rubin A, Crowds: Anonymity for Web Transactions, ACM TISSEC, 1 (1), 1998.

Sherwood R, Bhattacharjee B, and Srinivasan A, P5: A Protocol for Scalable Anonymous Communication, Proceedings of IEEE Symp., Security and Privacy, 2002, 58-70.

Stefan Kraxberger, Ronald, Martin Pirker, Elisa Pintado Guijarro, and Guillermo Garcia Millan, Trusted Identity Management for Overlay Networks, Springer Publication, 7863, 2013, 16-30.

Verlier L, and Syverson P, Locating Hidden Servers, In Proceedings of S.P, IEEE CS, 2006.

Wright M, Adler M, Levine B.N, and Shields C, An Analysis of the Degradation of Anonymous Protocols, In Proceedings of NDSS, IEEE, 2002.

Wright M, Adler M, Levine B.N, and Shields C, Defending Anonymous Communication against Passive Logging Attacks, In Proceedings of S.P, 2003.

Wright M, Adler M, Levine B.N, and Shields C, Passive logging Attacks against Anonymous Communications, ACM TISSEC, 11 (2), 2008.

Yu H, Kaminsky M, Gibbons P.B, and Flaxman A, Sybil-Guard: Defending Against Sybil Attacks via Social Networks, IEEE/ACM Trans. Networking, 16 (3), 2008, 576-589.

Yunhao Liu, Jinsong Han, Jilong Wang, Rumor Riding, Anonymizing Unstructured Peer-to-Peer Systems, IEEE Transactions on Parallel and Distributed Systems, 22 (3), 2011.

Zhu Y, Fu X, Bettati R, and Zhao W, Analysis of Flow-Correlation Attacks in Anonymity Networks, International Journal of Security and Networks, 2 (1/2), 2007, 137-153.