Indian Journal of Science and Technology, Vol 9(21), DOI: 10.17485/ijst/2016/v9i21/95161, June 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Reliable and Authenticated Rumor Riding Protocol for Unstructured Peer-to-Peer Network

Mary Subaja Christo[1]* and S. Meenakshi[2]

[1]Sathyabama University, Chennai - 600119, Tamil Nadu, India; marysubaja@gmail.com
[2]IT Department, SRR Engineering College, Chennai - 603103, Tamil Nadu, India; meenakshimagesh72@gmail.com

Abstract

Objectives: Due to the distributed network topology of peer-to-peer network, there are high possibilities for the malicious node, thereby making security a very important criterion in managing the network performance. **Methods:** Security in the network is ensured by validation using Rumor Recovery (RR) protocol. Trust table verification method guarentees the validity of initiator node and sower node validity. In this method, the initiator node sends its query message to the responder node according to the rumor generation and recovery phase and query issuance phase of the RR protocol. Responder node validation process is used for saving responding nodes from attacks. **Findings:** In this paper, we mainly concentrate on the detection and elimination of initiator node attack, replay attack, and sower attack. The performance metrics considered for evalution are delay, delivery ratio and throughput. Simulation results show that the proposed Trusted Rumor Riding (TRR) protocol. 1. Out performs RR protocol by 34% in terms of delay, 1% in terms of delivery ratio and 17% in terms of throughput while detecting and eliminating the initiator attack; 2. Out performs RR by 98% in terms of delay, 41% in terms of delivery ratio and 19% in terms of throughput while detecting and eliminating the replay attack; and 3. Out performs RR by 95% in terms of delay, 9% in terms of delivery ratio and 36% in terms of throughput while detecting and eliminating the sower attack. Most of the existing works did not consider these three attacks; only few works considered it, but those were failed to meet the quality of service requirements. The detected attacks are avoided in a effective manner to provide the secure communication. **Applications/Improvement:** From the results, it is concluded that the proposed TRR protocol can detect several attack while satisfying the quality of service needs.

Keywords: Malicious Node, Peer-To-Peer Network, Rumor Riding, Security, Trust Node, Validation

1. Introduction

In a Peer-to-Peer (P2P) network, every member node link with one another wirelessly and does not require any aid from the servers. When compared with centralized networks, the P2P networks have several advantages such as ease in developing the network, communicating anonymously, and many more[1]. In P2P network, the nodes efficiently communicate with one another, share the resources, offer service, and interact with nodes of other networks. In P2P network, there is no central controlling node, and hence it is a decentralized system. So, the nodes in the P2P network are considered as peers or equals. Communication performed between the nodes is more secure when the P2P network is authenticated[2].

In the structure P2P network, routing algorithm is used in connecting the nodes with one another. A Distributed Hash Table (DHT) is used to index the nodes. In an unstructured P2P network, routing algorithm is not used for connecting the nodes, arranging, or optimizing the links. If the links between the nodes are formed randomly, then this form an unstructured P2P network. The available links of the nodes are copied to develop new peers. Once a new peer is formed, it develops its link with time[3].

*Author for correspondence

The P2P network is susceptible to attacks. The client server networks may include malicious code, Trojan, worms, virus, and so on. The conventional techniques used in the client server network for producing the trust and safeguarding the network cannot be applied in the P2P network. One of the main issues with the centralized network system is that the entire network will fail if the central controlling node becomes compromised. In P2P network, each peer is provided with a Certification Authority (CA) and so if a malicious peer wants to carry out a false transaction, it will have to produce several CA and then several identity groups.

In P2P networks, the peers are partitioned into groups on the basis of certain conditions like each peer can be a member of one group, so as to overcome the attack from the malicious peer. The corresponding authority provides a group certificate to every peer, which is attached to the CA. Every node within or outside the group can access the certificate provided by the group authority to every node. The group authority is provided with the peer's blinded signature (or) credentials. It is validated by the authority, and then the group certificate is signed. The authority does not record this information and hence cannot relate between a certificate and a peer. So, the group authority is a stateless authority[3].

In a P2P network, any node can access or exit the network randomly, and hence this network is considered as an unstable network. Since the P2P network is decentralized, the conventional security technique like VPN will not be able to work within the P2P network. Hence, in P2P network, the security related problems are demanding.

Every node has a routing table in the DHT-based P2P network. Based on the routing table entry values, the keys can be looked up and mapped. Some unusual activities will be observed in the P2P network when malicious node is actively present in the network. When an attacker sends the look up request to a different node, it is considered as an ordinary attack.

One of the regularly observed attacks is the Denial-of-Service (DoS). This attack is hard to avoid in conventional Internet as well as in P2P network. In this attack, several service requests are made by the attackers to overload the target node. This causes the targeted node to become unable to offer service to any of the legal nodes. Based on the DoS attack, the Distributed DoS (DDoS) attack is built. DDoS is similar to DoS in terms of purposes and features. But, the technique used in DDoS is different. In DDoS, several hosts are used to attack a target host, that is, it works in a greater scale.

In P2P network, poisoning attack is also a regularly observed attack. In this attack, the integrity of the network is failed by the attackers by utilizing some wrong information such as false file indexes, false IP addresses, false routing tables, etc.

The existing works related to the proposed mechanism are discussed below:

A Bruit Bait protocol, which is a lightweight mutual anonymity protocol designed for the distributed P2P network. This protocol uses the random walk technique, where the initiating nodes are involved in the construction of path towards destination. When the Bruit Bait protocol is considered in comparison with the conventional RSA based anonymity protocol, the Bruit Bait protocol is more advantageous due to its reduced cryptographic overhead which is a result of the usage of the symmetric cryptographic algorithm[4].

A Mutual anonymity Rumor Riding (RR) protocol for the distributed P2P network. The initiating peers are not involved in the hectic process of path construction. The RR protocol is estimated with respect to the conventional RSA protocol, anonymity protocol which works on the basis of AES. The RR protocol is determined to be more advantageous with reduced cryptographic overhead since the asymmetric cryptographic algorithm is used to maintain anonymity in the network system[5].

A Reputation aggregation algorithm which utilizes a particular type of gossip algorithm known as differential gossip. The reputation estimate of the differential gossip algorithm has two divisions. The first part is a common part, and it is present in all the nodes in the same way. The second part is the information that has been obtained from the surrounding direct neighbors through the interaction of the node with the immediate neighbors. This algorithm is very quick and uses lesser resources. This algorithm enables every node to perform the reputation value calculation for the remaining nodes in the network. When a power law network is built on the basis of the Preferential Attachment (PA) Model, a differential gossip trust is developed. When the differential gossip trust is used to estimate the reputation value, a high level of collusion immunity is depicted[6].

A Rumor Riding (RR), a lightweight and non-path-based mutual anonymity protocol for distributed P2P systems. When compared with other protocols, the RR protocol has the special benefit of reduced overhead because it uses the

symmetric cryptographic algorithm and also follows the random walk scheme in its execution[7].

A zero knowledge authentication technique known as the Pseudo Trust (PT). In this technique, peers never use its real identity, and so it produces a pseudonym based on the one-way hash function. This pseudonym cannot be forged but can be verified. To enable the authentication of the peers by assuring complete protection of the sensitive information, a new authentication technique is developed on the basis of the Zero-Knowledge Proof[8].

Linear Subsequence Algorithm (LSA) which increases data protection Today's large oblige of internet applications requires data to be transmitted in a protected manner. Data broadcast in the public communication system is not protected because of interception and inappropriate operation by an eavesdropper[9].

The Guillou-Quisquarter algorithm,Naughty algorithm and partition algorithms are used to improve the capability of the system to protect against intruders and hateful programs, the best way is to apply the trusted system technology. This in turn gives increase to different access rights which is being exercised by users in series and parallel[10].

"Message Digest","IDEA" and "GOST" algorithms are used to improve the security and authentication by sending data. Combination of digital signature algorithm and symmetric key cryptography algorithms are provide high security to transfer the data[11]. The current identity based trust management mechanisms can be applied in the mutual anonymous P2P networks with the aid of PT[12-15].

"Trusted Rumor Riding protocol" is used to authenticate the responder node by asking the challenge question from the initiator node[16].

2. Materials and Methods

2.1 Overview

The Rumor Riding (RR) protocol provides anonymity in P2P systems, but still there are chances of various attacks like misuse attack, reply attack, spoofing, and so on. The leader may act as a malicious node by sending fake request messages to the respondent node. Similarly, the respondent may act as a malicious node causing replay attacks. If the intermediate node acts as malicious, it will launch packet dropping attack. In all the 3 cases, the network performance is degraded with increased delay and packet drops.

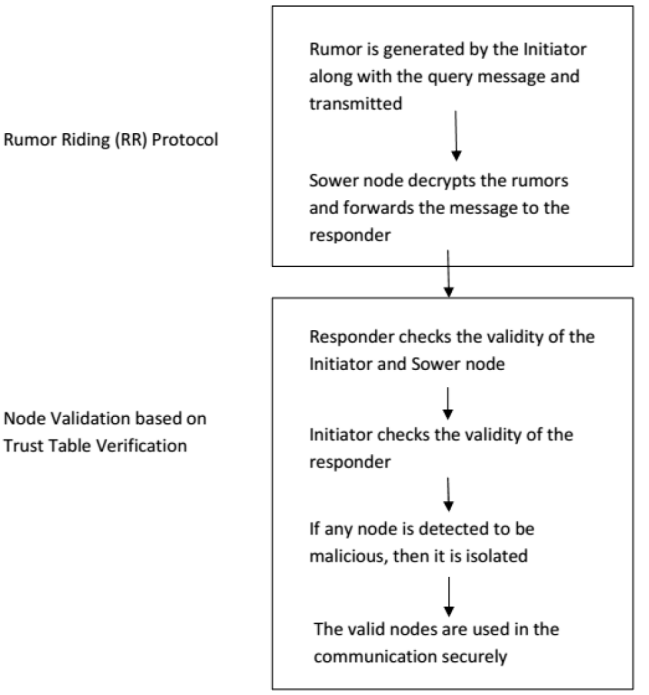

Figure 1. Validation in RR protocol.

This paper presents effective attack detection techniques for RR protocol by using trusting and secret message exchanges. Figure 1 illustrates the validation in RR protocol.

2.2 Rumor Riding (RR) Protocol

Rumor Riding (RR) is a non path based P2P protocol. In RR, the node which initiates a query is called as the initiator node. The nodes which forward the message till the destination is considered as an intermediate node and the node which provides the response message to the initiator because it possesses the file requested by the initiator is called as the responder node.

RR protocol consists of five phases.

- Rumor Generation and Recovery: The Initiator encrypts the query message, M with query content, q using a symmetric key, and the AES algorithm. This key and the cipher text are transmitted towards different nodes by the Initiator. The key and the cipher text move into different path randomly, and each of this movement is called as a rumor i.e., a key rumor and a cipher rumor. When these two rumors arrive at a peer, this peer is called as Sower node. Sower node recovers the query message, M .

- Query Issuance: Every node in the network maintains a temporary local cache to store all the received rumors. When a node receives a rumor either the key rumor or the cipher rumor, it performs RR procedure to check all the cached rumors. When the decrypted rumor contains a plain text matching the predefined value, then the query content is recovered. Even when the decrypted value matches or not, the intermediate reduces the Time To Live (TTL) by one value. This process continues until the TTL value reduces to 1.
- Query Response: When a node receives a query to which it has the desired file, then it becomes the responder, R. R sends the response message, r to the query by encrypting the plain text with Initiator's public key. R generates a public key which encloses the cipher test and also the key text into two response rumors, the response key rumor and the response cipher rumor. Then, the two rumors are transmitted towards the neighbors randomly. When any intermediate node receives both the rumors, the cipher text in cipher rumor is decrypted using the key rumor and recovers the ID of the sower node. The sower node then forwards the response to the Initiator, which recovers the response message, r.
- Query Confirmation: Initiator sends a confirmation message, c using confirmation cipher rumor and key rumor to the responder.
- File Recovery: When the responder receives the confirmation message, it delivers the file to the Initiator after encrypting it.

2.3 Initiator Node Attack

In wireless network, since any node can enter or exit the network randomly, there are possibilities for a malicious node to enter the network. If this malicious node initiates a query, then it becomes the initiator node. So, in this case, the initiator node is itself the malicious node and badly affects the network performance to a greater extent.

Figure 2 shows the scenario when the initiator node is a malicious node. This node sends fake request in the network and leads to virus being spread in the network. As a result, the network performance degrades gradually.

Similarly, there are possibilities for the intermediate node mainly the sower node to be a malicious node. On receiving the data packet, the malicious sower node drops it and transmits the fake response towards the initiator. Thus, spreading virus throughout the network and degrading the network performance.

Figure 3 shows the scenario when the sower node is a malicious node. When a valid response is sent from the responder to the initiator through a sower node which is malicious, the sower node acts as a selfish node and drops the data packet. It then sends fake response through out the network to spread virus in the network, inorder to degrade the network performance.

To overcome this issue, trust-based method is used. In this method, a trust table is maintained at every node. The trust table consists of several fields such as name and IP address of the node, username, password, and also a duplicate password.

Figure 4 shows the format of trust table. In this method, the RR protocol includes several new steps to

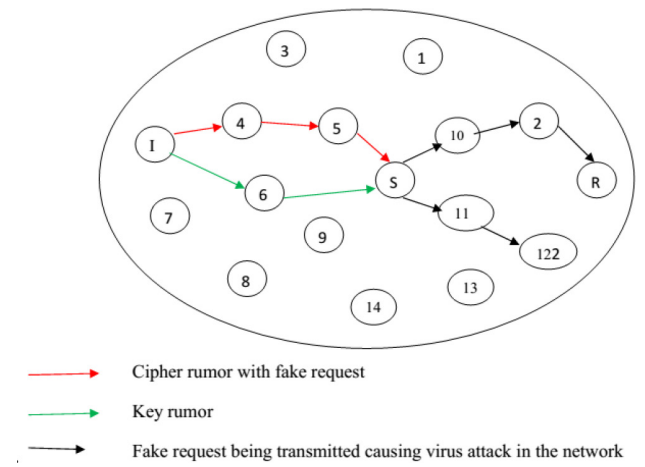

Figure 2. Initiator node as malicious.

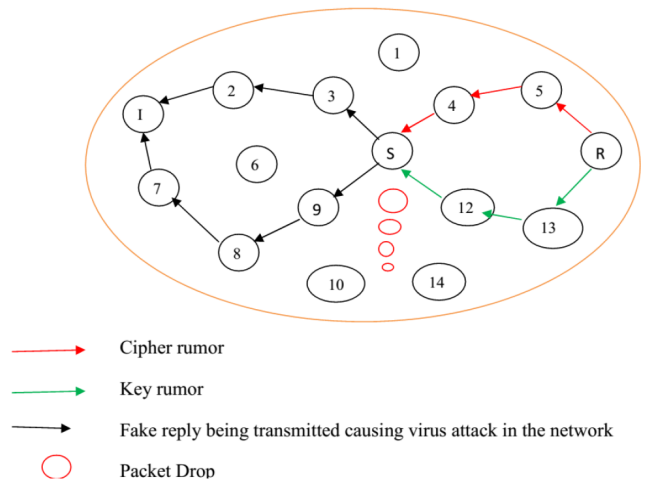

Figure 3. Sower node as malicious.

Node Name	IP Address	Username	Password	Duplicate Password
A				
B				
C				
D				
E				

Figure 4. Trust table format.

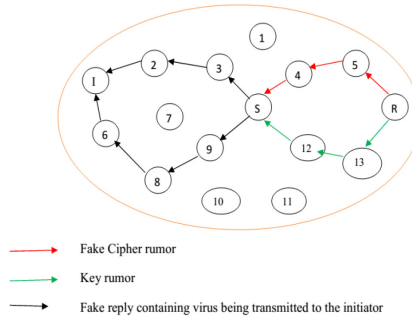

Figure 5. Responder node as malicious.

ensure validity of the initiator node along with the sower node validity.

The protocol is described in algorithm 1

Algorithm 1

- The initiator node sends its query message to the responder node according to the Rumor Generation and Recovery phase and Query Issuance phase of the RR protocol as described in Section 3.2.
- When the responder node receives the query message, it sends a challenge question to the Initiator node to check its validity.
- When replying to the responder node, the answer to the challenge question, the initiator uses two rumors, the key rumor and cipher rumor and also includes a challenge question to the node to check the validity of the sower node.
- When the two rumors meet at a sower node, it is asked a challenge question.
- If the sower node answers correctly, then the decryption is enabled and its IP address is trusted and included.
- Next, the second sower node is selected similarly and is connected to the responder by TCP connection.
- On receiving the reply from the initiator node, the responder node demands proof for the challenge question. This is to ensure that the initiator has a valid trust table and its replies are based on its own trust table values and not fake values.
- When the responder receives the proof, the proofs are verified against the data in the trust table.
- If the proof is determined to be correct and valid then, the responder considers it as a trustworthy node and hence a valid initiator.

2.4 Responder Node Attack

There are possibilities for the responder node to be a malicious node. This may lead to responder node attack in the network, which can also reduce the network performance.

Figure 5 shows the scenario when the responder node is a malicious node. When the responder is malicious, it provides fake response to the initiator's query, causing reply attack. When this fake reply is transmitted, it spreads virus throughout the network. It increases traffic, causes packet dropping, and thus degrades the network performance.

In order to overcome this issue, responder node is tested to be non malicious. So, after the determination of the responder node in the network, the initiator node needs to check the validity of the responder node. The verification of the responder node is also based on the trust table data. The responder node validation process is described in algorithm 2.

Algorithm 2

- responder node, along with the query message, a challenge question should also be enclosed.
- The responder node replies the answer to the challenge question using the two rumors.
- When the reply reaches the first sower node, it checks the answer to the challenge question and determines if it is valid or not based on the data in the trust table.
- If the answer is valid then the reply is forwarded to the second sower node, which includes its IP address and links the reply to its destination through the TCP connection.

- Once the valid reply reaches the initiator node, it considers the destination node to be trustworthy and is recorded as a valid responder.

Thus, the P2P communication can be performed securely.

2.5 Overall Process of Protocol

The overall working of this protocol which assures node safety against malicious attacks is described in algorithm 3.

Algorithm 3

- The initiator node which has a query generates two rumors: key rumor and cipher rumor.
- The two rumors are sent across the network through different paths.
- At the sower node the two rumors meet and decrypt the message and then forward the message to the responder node.
- On receiving the message, the responder checks the validity of the initiator node by asking the challenge question.
- When the initiator receives the challenge question from the responder, it responds to it and simultaneously tests the validity of the sower node and the responder by asking the challenge question.
- When the responder receives the answer from the initiator, it checks it. If the answer is right, it then asks the proof for the answer.
- When the responder receives the proof from initiator, it checks the value against the data present in the trust table.
- If the proofs are verified to be valid, then the responder considers the initiator as a valid node, else as a invalid node.
- When the sower node receives the challenge question from the initiator node, it sends its answer to the initiator.
- On receiving the reply from the sower node, the initiator compares the reply with the data present in the trust table.
- If the reply and the trust table value matches, then the sower node is considered as a valid node, else as an invalid node.
- When the responder receives the challenge question from the initiator, it sends its answer to the initiator.
- The initiator verifies it with the values in the trust table. If the reply is determined to be right, then the responder is considered to be a valid node, else a invalid node.
- All the nodes detected to be invalid are isolated and included in the data communication.
- Only the nodes detected to be valid are included in the communication. Thus, ensuring network security against every possible attack.
- Then the responder node sends the desired file to the initiator node through the sower node.

Hence, this protocol offers higher security to the nodes and thus effective network performance.

3. Results and Discussion

3.1 Simulation Parameters

We use NS2[17] to simulate our proposed Trusted Rumor Riding Protocol (TRR). We use the IEEE 802.11 for Peer-to-Peer Network. It has the functionality to notify the network layer about link breakage. In our simulation, the time is varied as 5,10,15,20,25 and 30sec. The area size is 109 meter x 471 meter square region for 50 seconds simulation time. The simulated traffic is Constant Bit Rate (CBR).

Our simulation settings and parameters are summarized in Table 1

3.2 Performance Metrics

We evaluate performance of the new protocol mainly according to the following parameters. We compare the RR protocol with our proposed TRR protocol.

Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.

Average end-to-end delay**:** The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Throughput**:** The throughput is the amount of data that can be sent from the sources to the destination.

3.3 Results and Analysis

The simulation results are presented in the next section.

3.3.1 Case-1(Initiator Attack)

- Based on Time

No. of Nodes	24
Area	109 X 471
MAC	802.11
Simulation Time	5,10,15,20,25 and 30 sec
Traffic Source	CBR
Rate	50Kb
Propagation	TwoRayGround
Antenna	OmniAntenna

Table 1. Simulation parameters.

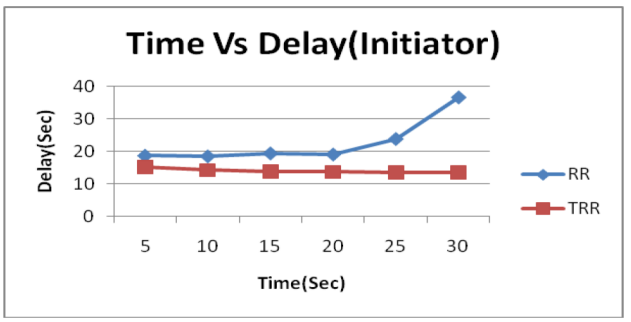

Figure 6. Time vs. delay.

In our experiment we are varying the time as 5, 10, 15, 20, 25 and 30 sec.

Figures 6 to 8 show the results of delay, delivery ratio and throughput by varying the time from 5 to 30 in TRR and RR protocols. When comparing the performance of the two protocols, we infer that TRR outperforms RR by 34% in terms of delay, 1% in terms of delivery ratio, and 17% in terms of throughput.

3.3.2 Case-2 (Replay Attack)

- Based on Time

In our experiment we are varying the time as 5, 10,15,20,25 and 30sec.

Figures 9 to 11 show the results of delay, delivery ratio and throughput by varying the time from 5 to 30 in TRR

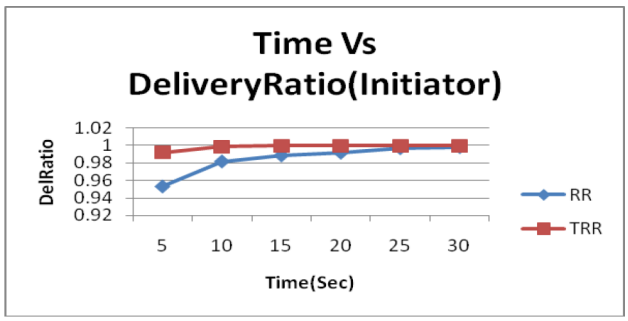

Figure 7. Time vs. delivery ratio.

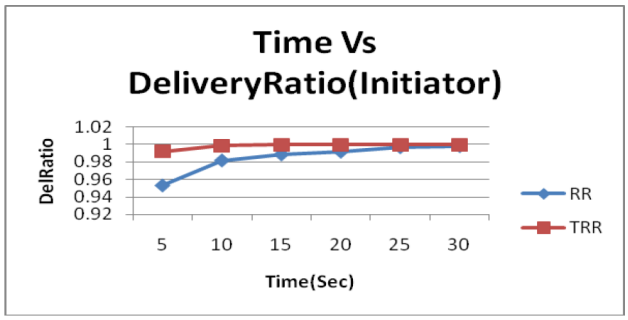

Figure 8. Time vs. throughput.

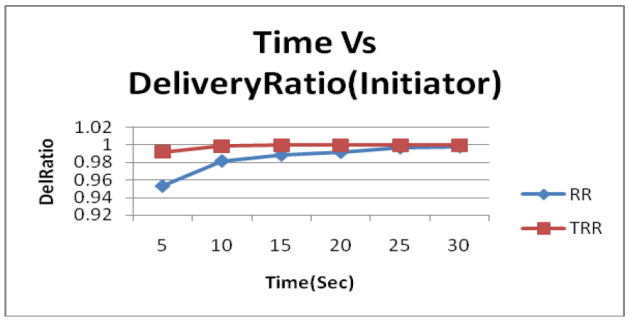

Figure 9. Time vs. delay.

and RR protocols. When comparing the performance of the two protocols, we infer that TRR outperforms RR by 98% in terms of delay, 41% in terms of delivery ratio, and 19% in terms of throughput.

3.3.3 Case-3 (Sower Attack)

- Based on Time

In our experiment we are varying the time as 5, 10,15,20,25 and 30sec.

Figures 12 to 14 show the results of delay, delivery ratio and throughput by varying the time from 5 to 30 in TRR and RR protocols. When comparing the performance of

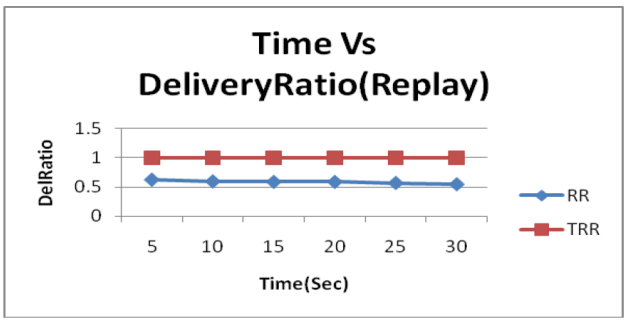

Figure 10. Time vs. delivery ratio.

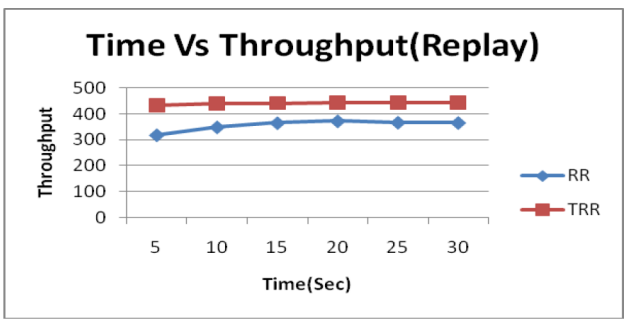

Figure 11. Time vs. throughput.

the two protocols, we infer that TRR outperforms RR by 95% in terms of delay, 9% in terms of delivery ratio, and 36% in terms of throughput.

4. Conclusion

In this paper, we have developed a technique to provide security in the unstructured Peer to Peer network. Basically, the Rumor Riding (RR) protocol is used to transfer the messages between the initiator and responder node through the intermediate node. But, since there are possibilities for the initiator, intermediate or the responder node to be malicious. So, special procedure is followed to validate the nodes. This validation is done based on security related questions, answers and its proof. The verification is done based on the trust table data. Once all the nodes are validated, then the node communication is carried out securely. Thus, this technique ensures security and therefore, efficient network performance.

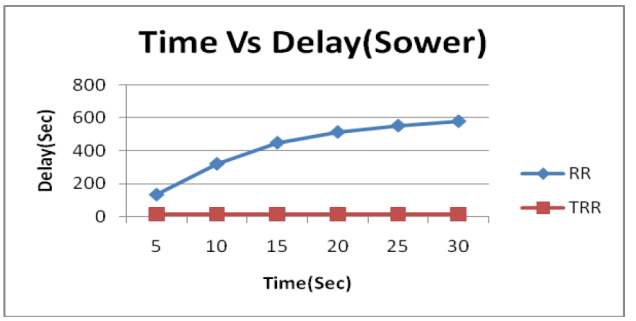

Figure 12. Time vs. delay.

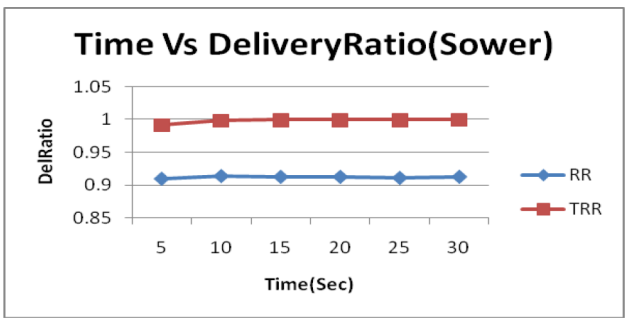

Figure 13. Time vs. delivery ratio.

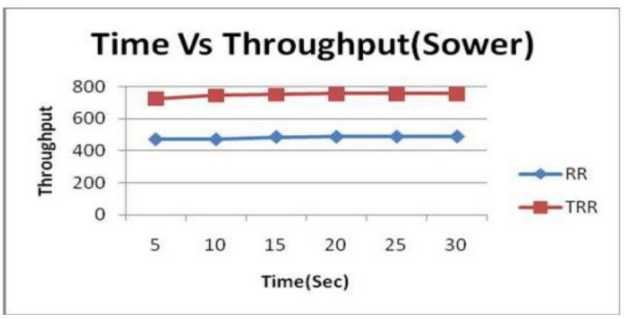

Figure 14. Time vs. throughput.

5. References

1. Takeda A, Chakraborty D, Kitagata G, Hashimoto K, Shiratori N. A new scalable distributed authentication for P2P network and its performance evaluation. WSEAS Transactions on Computers. 2008 Oct; 7(10):1628-37.
2. Cheng W, Tan Z. Correlation trust authentication model for peer-to-peer networks. Advanced Materials Research. 2013 Sep: 2237-42.

3. Arulkumar CV, Jeyakumar K, Malarmath M, Shanmugapriya T. Secure communication in unstructured P2P networks based on reputation management and self certification. International Journal of Computer Applications. 2012 Apr; 44(15):1-3.
4. Devika P, Ponmaga RS. Bruit bait: Peer To Peer systems. IJCER. 2012 Jul.
5. Mangi FA, Memon I, Jamro DA, Memon MH, Basit MA. The rumor riding anonymity approach for decentralized Peer To Peer systems. IJCSI. 2013 May; 10(3):180-7.
6. Gupta R, Singh YN. Reputation aggregation in Peer-to-Peer network using differential gossip algorithm. IEEE Transaction on Knowledge and Data Engineering. 2015 Oct; 27(10):2812-23.
7. Liu Y, Han J, Wang J. Rumor riding: Anonymizing unstructured Peer-to-Peer systems. IEEE Transactions on Parallel and Distributed Systems. 2011 Mar; 22(3):464-75.
8. Lu L, Han J, Hu L, Huai J, Liu Y, Ni LM. Pseudo trust: Zero-knowledge authentication in anonymous Peer-to-Peer. IEEE Transactions on Parallel and Distributed Systems. 2007 Mar:1325-37.
9. Valarmathi R, Kadhar Nawaz GM. Secure data transfer through audio signal with LSA. Indian Journal of Science and Technology. 2015 Jan; 8(1):17-22.
10. Thiyagarajan M, Raveendra C, Thiagarasu V. Web service authentication and multilevel security. Indian Journal of Science and Technology. 2015 Jul; 8(15):1-7.
11. Ganeshkumar K, Arivazhagan D. Generating a digital signature based on new cryptographic scheme for user authentication and security. Indian Journal of Science and Technology. 2014 Oct; 7(S6):1-5.
12. Wang L. Attacks against Peer-to-Peer networks and counter measures. Seminar on Network Security; 2006 Dec. p. 1-6.
13. Delafrooz N, Farzanfar E. Determining the Customer life-time value based on the benefit clustering in the insurance industry. Indian Journal of Science and Technology. 2016 Jan; 9(1):1-8.
14. Aarthi R, Anjana KP, Amudha J. Sketch based image retrieval using information content of orientation. Indian Journal of Science and Technology. 2016 Jan; 9(1):1-5.
15. Justin Samuel S, Jenitha SJ. Enhanced security and authentication mechanism in cloud transactions using HMAC. IEEE International Conference on Computational Intelligence and Computing Research; 2014 Dec. p. 1-4.
16. Christo MS, Meenakshi S. Trusted rumor riding protocol in P2P network. Journal of Chemical and Pharmaceutical Sciences. 2016 Mar; 9(1):440-6.
17. Network Simulator [Online]. 2012. Available from: http:///www.isi.edu/nsnam/ns