Asian Journal of Information Technology 15 (15): 2602-2610, 2016
ISSN: 1682-3915
© Medwell Journals, 2016

Secure Rumor Riding Protocol Using Reputation and Packet Hiding for Unstructured Peer-To-Peer Network

[1]Mary Subaja Christo and [2]S. Meenakshi
[1]Department of Computer Science and Engineering, Sathyabama University, Chennai, Tamil Nadu, India
[2]Department of Information Technology, SRR Engineering College,
Padur, 603103 Chennai, Tamil Nadu, India

Abstract: In a Peer to Peer network, the involved nodes are considered as peers and these peers link with other neighboring peers directly to achieve the assigned task. It usually involves heterogeneous networks. Due to the network topology and features, this network is prone to several attacks and the security features available are relatively minimal. Thus, this network suffers from various attacks. In this study, we develop an attack prevention protocol based on the reputation aggregation and cryptographic message hiding technique. The reputation aggregation is performed based on the differential gossiping algorithm and the cryptographic message hiding technique is based on the cryptographic puzzle hiding scheme. This way, the network operation is secured and thus, it performs efficiently.

Key words: Attacks, security, aggregation, algorithm, cryptographic

INTRODUCTION

Unstructured Peer to Peer network: The P2P network has distributed topology and the tasks are divided among the peers. The peers in the P2P networks have equal privileges and provide potential performance during all network operations. In the P2P network, the peers link with various heterogeneous networks and also cooperate with it in any network configuration. In a Peer-to-Peer (P2P) network, the network functioning is dependent on the client's computation power instead of its computation power. So, clients which are considered as the peers perform operations to maintain its links instead of using a central server (Pretre, 2005). The P2P network has gained great importance and is subjected to research within the past few years. One major problem in the P2P network is the decentralized search technique. An efficient solution is to devise a searching technique which considers the local information necessary to maintain scalability and thus its success.

Security in Peer to Peer network: Peer to Peer network is subjected to various types of attacks (Pretre, 2005). Some of the serious attacks include: Denial of Service (DoS) attack, Man-in-the-middle attack, worm propagation, rational attack, file poisoning, sybil attack and eclipse attack. Peer to Peer network provides some potential security services (Balfe *et al*., 2005) like integrity, control of access, authentication, confidentiality and non repudiation.

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 (Arulkumar *et al*., 2012).

Corresponding Author: Mary Subaja Christo, Department of Computer Science and Engineering, Sathyabama University, Chennai, Tamil Nadu, India

Literature review: Zhou and Hwang (2007) proposed gossip-based reputation aggregation for unstructured Peer-to-Peer networks. In this scheme, the gossip trust is estimated for reputation aggregation without using any deployed infrastructure. Local trust can be aggregated quickly by the gossip trust technique and then it is converted into global reputation. The fast gossip-based aggregation algorithms, effective reputation storing with bloom filters as well as the secure communication with identity based cryptography are the three main enhancement made by the gossip trust calculation.

Li (2008) proposed a configurable online reputation aggregation system. In this protocol, the globality issue is addressed by collecting the rating related to the involved system node from several systems rather than collecting aggregated reputation information. The rating data collected from several systems are aggregated to develop a local reputation, then all the aggregated local reputation is converted into global reputation. This aggregation is performed on the basis of options as well as weights that are chosen by the querying agent based on the system requirements.

Sruthy (2014) proposed a Secure Cryptographic Puzzle based Approach Ensuring Total Security for transmitted Information with IP tracing. This approach is developed for the IP traceback by including the Digital Signature algorithm and a cryptographic puzzle hiding scheme. The Digital Signature algorithm protects the network from attacks and safeguards it. The cryptographic puzzle hiding scheme safeguards the system from attackers as well as hackers. This approach is carried out in an application which works on the basis of share market and hence share details are secured.

Jorvekar proposed puzzle based packet encoding technique to prevent jamming attacks. The issue of selective jamming attacks is addressed in this technique. Packet encoding, packet interleaving and puzzle based system are incorporated in this technique to ensure higher security to packets. AES algorithm is also included to enhance the security symmetric algorithm.

Ruchir proposed a reputation aggregation technique in Peer-to-Peer Network Using Differential Gossip algorithm. In the power law network, the trust values from various nodes are aggregated without identifying the power nodes and by using the aggregation mechanism. Since, the node identification is not required, this leads to the quick implementation of the approach as node identification which is a hard task is avoided. The reputation aggregation is performed in a differential method by taking into account the feedback from nodes that have increased weight. This makes the approach more robust towards collision and avoids the free riding issue.

Proano and Lazos (2012) have proposed packet-hiding methods for preventing selective jamming attacks. In this approach, jammers are used in the network being attacked and have knowledge of the shared network secrets and protocol specifications. These jammers are capable of differentiating the real time packets just by decoding the initial few symbols of the current transmission. This approach enhances performance with minimum efforts. This approach includes cryptographic techniques such as commitment mechanisms, cryptographic puzzles and all-or-nothing transformations with physical-layer features.

MATERIALS AND METHODS

Secure rumor riding protocol

Security issues of rumor riding (rr) protocol: Rumor Riding (RR) (Liu *et al*., 2011) 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 possess the file requested by the initiator is called as the responder node. The 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

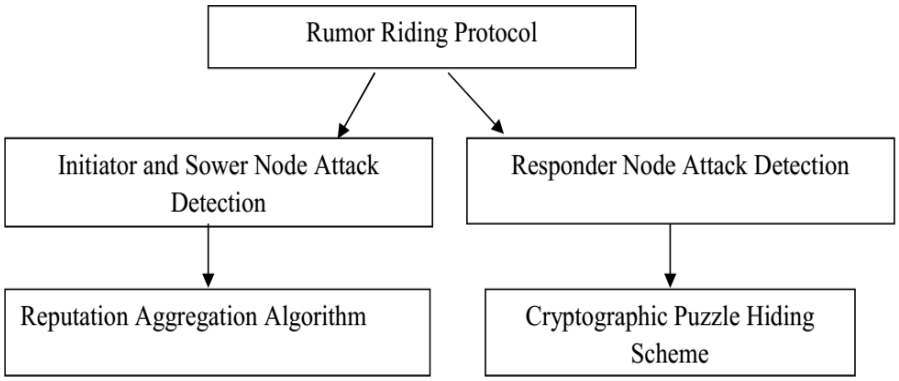

Fig. 1: Block diagram

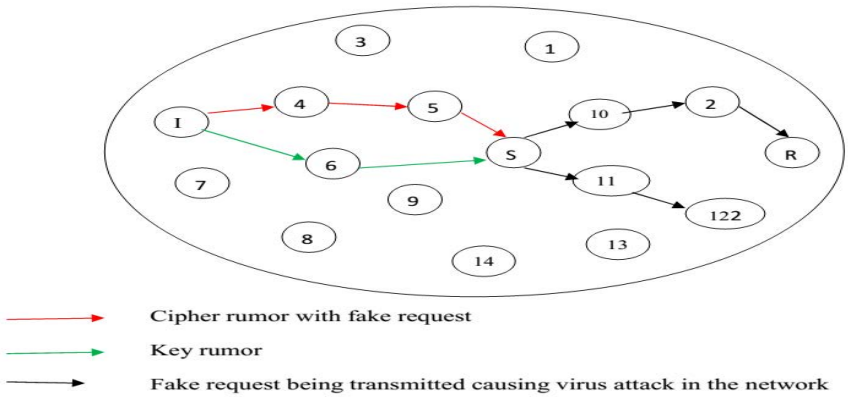

Fig. 2: Time vs delay diagram

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, cusing 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.

The various possible attacks in RR protocols are malicious initiator node attack, malicious respondent node attack and malicious intermediate node attack. 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.

In the previous study, to overcome these attacks, a trusted rumor-riding protocol for unstructured peer-to-peer network is proposed. In that protocol, a trust table and challenge response mechanism is used to prevent the initiator attack, sower attack and responder attacks.

In this extension work, instead of simple trust table, we use the reputation aggregation by applying the differential gossip algorithm (Gupta and Singh, 2014). Instead of challenge response mechanism, we use the Cryptographic Puzzle Hiding Scheme (CPHS) (Proano and Lazos, 2012) (Fig. 1).

Initiator and sower node attacks: 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

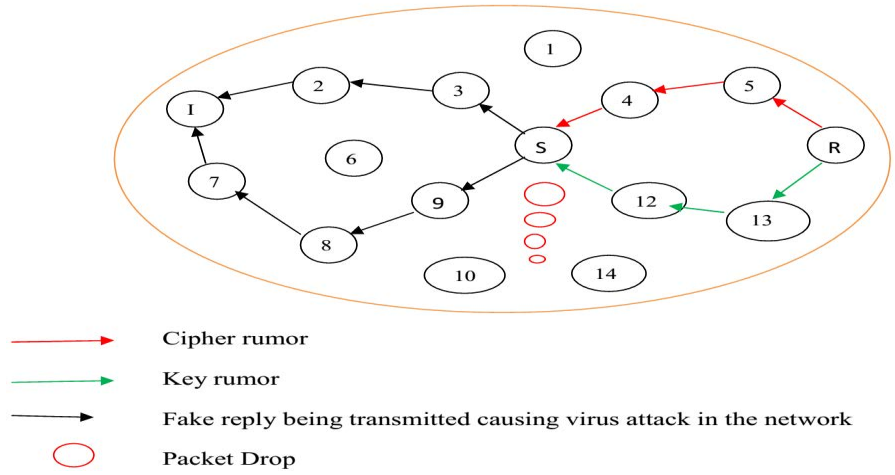

Fig. 3: Time vs delivery ratio diagram

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 these attacks, reputation aggregation algorithm (which is described in the next section) is used.

Reputation aggregation using differential gossip algorithm: Reputation aggregation is a process in which the trust value of any node is gathered from several neighbors by a node and its value is aggregated and recorded in a table. When the node receives new information related to the trust value of the surrounding nodes, the reputation value of that node is adjusted accordingly in the reputation table of the information receiving node.

When a node in the network requests its neighboring node for resource, then the node checks the reputation of the requesting node in its reputation table. Based on the trust value of the requesting node, the resource will be allocated to it. If a node receives request from a new node that is not its neighbor, then the requested node collects the reputation information of the requesting node through its neighbors and based on the aggregated reputation information, estimates the overall reputation of the requesting node.

In this study, the reputation aggregation is performed using the differential gossip algorithm (Gupta and Singh, 2014). In this technique, each node shares it information with a specific set of neighboring nodes. The nodes which receive the information share it with the remaining nodes. Thus, each node receives multiple trust values related to one specific node. The aggregated value is then tested for convergence. If the convergence condition is satisfied, then it indicates that the node is trust worthy and no more aggregation of the reputation is required. The reputation aggregation mechanism is described in algorithm 1.

Algorithm:

- During gossiping, each node randomly chooses a node from its neighborhood and shares some basic information with it
- The received information is stored by the receiving node
- Based on the information received from all the neighboring nodes, each node, i estimate the average neighbor degree
- Each node, i randomly choose q nodes from its neighborhood and then pushes some information into these neighbors
- All the nodes that have received some feedback from node, i stores it in the reputation table and then gossips its feedback with the remaining nodes
- The global reputation of every node is estimated based on the feedback received through gossiping from the surrounding nodes
- If i receives feedback from j, fb_{ij} then $gw_{ij} = 1$
- When i does not have any feedback about j, then $fb_{ij} = 0$ and $gw_{ij} = 0$

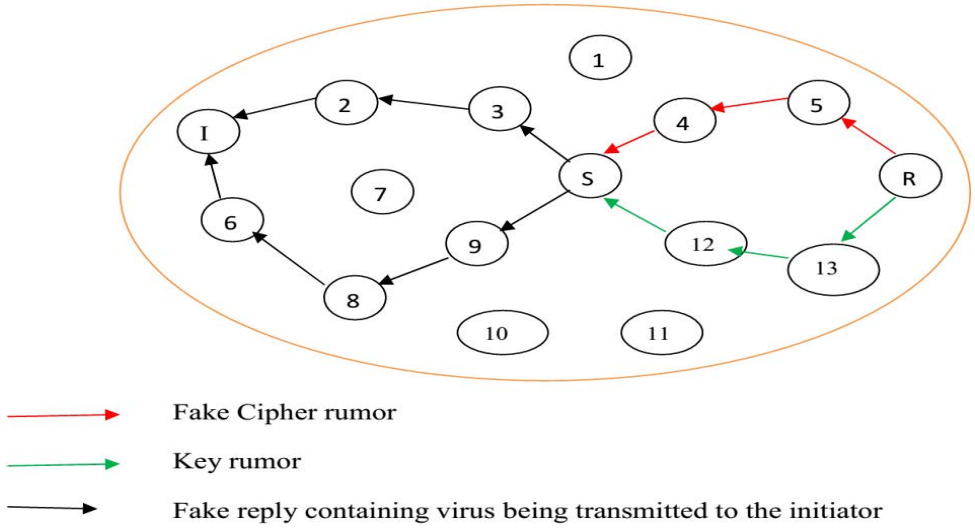

Fig. 4: Time vs drop ratio

- The value of fb_{ij} and gw_{ij} are recorded by every node in the reputation aggregation table and is considered as gossip pair
- During every gossiping step, the ratio of the gossip pair depicted by Eq. 1 is estimated to determine the convergence value and is recorded:

$$\text{Convergence}_{\text{value}} = \frac{\sum_i b_{ij}}{\sum_i gw_{ij}} \quad (1)$$

The value of q is rounded off to the nearest integer value and sends:

$$\left(\frac{1}{q+1} fb_{ij}, \frac{1}{q+1} gw_{ij}\right) \quad (2)$$

as the gossip pairs to all the q nodes. The total gossip pair received is determined. The convergence value as estimated in Eq. 1 is checked w.r.t a predefined error constant. If convergence condition is satisfied, then gossiping process is stopped. If convergence condition is not satisfied, then gossiping process is continued. When the node i stop gossiping, it announces among its neighbors that it has achieved convergence.

Thus, the valid nodes are detected and recorded as trust worthy based on the reputation aggregated through gossiping.

Attack detection algorithm: The initiator node sends its query message along with its id to the responder node according to the Rumor Generation and Recovery phase and Query Issuance phase of the RR protocol. When the sower node, receives the key and cipher rumours, it first verifies that the initiator id is in its reputation table. If it could not be find out its id, it then performs global reputation aggregation as described in algorithm 1. If the reputation of Initiator node is low, it does not decrypt the information and stops proceeding further.

Otherwise, it forwards the query along with its id, IP address and reputation value of the initiator. When the query reaches the responder, it verifies the id of sower is within its reputation table. If it could not find out, it then performs global reputation aggregation as described in algorithm 1. If the reputation of sower node is low, it stops proceeding further.

Otherwise, it retrieves the query and reputation value of initiator from the sower node. It checks the reputation value of initiator and verifies with its own table. If initiator has sufficient reputation, the responder generates the query response and the same steps are repeated until the response reaches the initiator.

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 4 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 attack, responder node should be tested 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 responder node validation process is described in using the cryptographic puzzle hiding scheme described in the next section.

Cryptographic Puzzle Hiding Scheme (CPHS): To ensure data security during its transmission from the source node to the destination node, packet hiding mechanism (Proano and Lazos, 2010) is used. In this study, the packet hiding mechanism is based on the cryptographic puzzle. When the cryptographic puzzles are used for packet hiding, a predefined set of computations is agreed between the source and the destination node. On receiving, the destination node is supposed to solve the puzzle using the computation set to obtain the key which is required to unhide the data packet. The puzzle, P generated by the sending/source node is given by:

$$P = \text{puzzle}\left(k, t_p\right) \quad (3)$$

Where:

puzzle ( ) = Puzzle generator function

tp = Time required to determine the solution for the puzzle

Algorithm 1:

When a node, S needs to transmit a data packet, pkt to a destination node D, it selects a random key, $k \in \{0,1\}^s$.

The S adds the Destination address in the pkt, but to be able to read it, every node needs to answer a challenge question.

Then, S generates a puzzle, P as depicted in Eq. 3.

After generating P, S transmits (C,P), to all of its neighboring nodes with good reputation that are detected using reputation aggregation technique.

The receiving nodes answer the challenge question of the source.

If the received answer is right, then the S considers it as a trustworthy node and lets it determine the D address.

Then it is forwarded through the intermediate nodes with good reputation since only nodes with good reputation can answer the challenge question, till it reaches D.

On receiving the puzzle p^1, the D sends a challenge question to S. Based on the aggregated reputation, the S replies to D.

If the reply is valid, then D considers S to have a valid reputation aggregation table and hence as a trustworthy node.

Next, D decrypts it and recovers the key k^1 and computes the message pkt^1 π^1 $(Ek^2(C^1))$ where $E_k^1(C^1) = pkt^1 \| r$.

The computed is transmitted to the S.

If the D has decrypted the P correctly, then the S considers D as a trust worthy.

If the computed packet pkt^1 has valid CRC and is within the destination node's communication context, then the destination accepts $pkt^1 = pkt$

Else the is discarded. Pkt^1

Attack detection algorithm: Along with the query message, the initiator generates a cryptographic puzzle and transmits towards the responder node. On receiving the query message, if the responder can solve the puzzle, it generates the query response along with the solution. It sends the response along with a new cryptographic puzzle towards the initiator, through the sower nodes. The sower nodes verifies the reputation value of the responder, if it is high, then forwards the response message along with the reputation value of the responder. On receiving the response from the sower nodes, the initiator first checks the reputation value of the responder and verifies it with its own reputation table. If the responder has sufficient reputation value, the initiator solves the puzzle and retrieves the response message. The remaining procedures of RR protocol will be continues in the same manner.

In this way, the packet is transmitted from the source to the destination through trust worthy intermediate nodes which are validated through reputation aggregation technique. The data packet is secured from all the attacks since the packet is hidden through the cryptographic puzzles. Thus, the data is secured by encrypting it and the path followed is also ensured to be safe based on the aggregated reputation. Therefore, this technique efficiently safeguards the data transmission in the network against every kind of attack.

Table 1: Simulation parameters

Parameters	Values
No. of nodes	24
Area	109×571
MAC	802.11
Simulation Time	50 sec
Traffic Source	CBR
Rate	100 Kb
Propagation	TwoRayGround
Antenna	OmniAntenna
Simulation Time	10, 20, 30, 40 and 50 sec

RESULTS AND DISCUSSION

Simulation results

Simulation parameters: We use NS-2 to simulate our proposed Secure Rumor Riding Protocol Using Reputation and Packet Hiding (SRRP) protocol. We use the IEEE 802.11 for unstructured network as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. In our simulation, the simulation time is varied as 10, 20, 30, 40 and 50. The area size is 109×571 m^2 region for 50 sec simulation time. The simulated traffic is Constant Bit Rate (CBR). We evaluate performance of the new protocol mainly according to the following parameters. We compare the RRP protocol with our proposed SRRP protocol. Simulation settings and parameters are summarized in Table 1.

For initiator attack: In the experiment we are varying the time as 10, 20, 30.40 and 50 for CBR traffic (Table 2-4). Figure 5-13 show the results of delay, delivery ratio and dropratio by varying the stop time from 10-50 for the CBR traffic in SRRP and RRP protocols. When comparing

Table 2: Delay for initiator attack

End-to-End delay		
Simulation time (sec)	SRRP	RRP
10	0.43	2.45
20	2.08	5.37
30	4.28	8.96
40	6.69	12.55
50	9.10	15.76

Table 3: Packet delivery ratio for initiator attack

Packet delivery ratio		
Simulation time (sec)	SRRP	RRP
10	0.8624	0.3552
20	0.5954	0.3174
30	0.5531	0.3149
40	0.5353	0.3169
50	0.5228	0.3118

Table 4: Fraction of affected communications for initiator attack

Fraction of affected communications		
Simulation time (sec)	SRRP	RRP
10	0.128	0.589
20	0.400	0.581
30	0.444	0.613
40	0.463	0.609
50	0.476	0.615

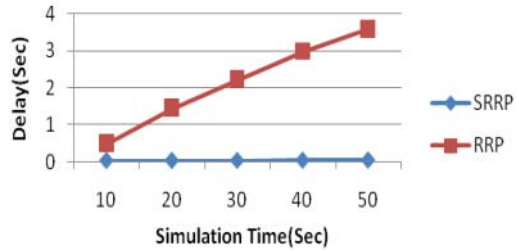

Fig. 5: Description of time vs delay

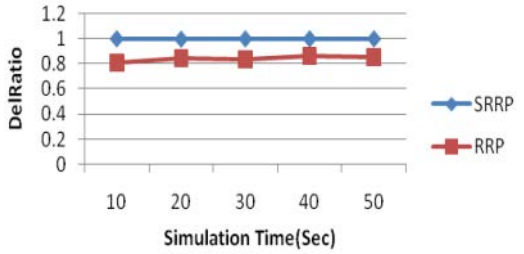

Fig. 6: Description of time vs delivery ratio

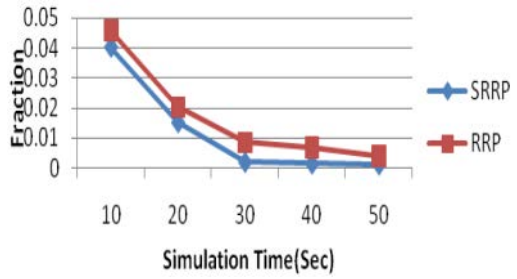

Fig. 7: Description of time vs drop ratio

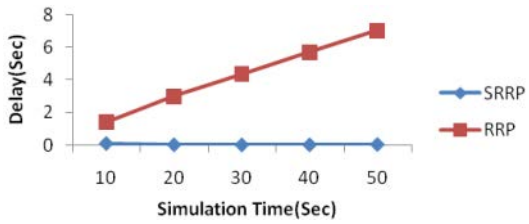

Fig. 8: Time vs delay

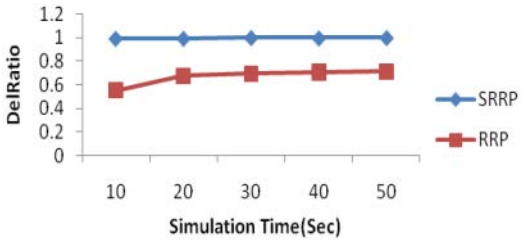

Fig. 9: Time vs delviery ratio

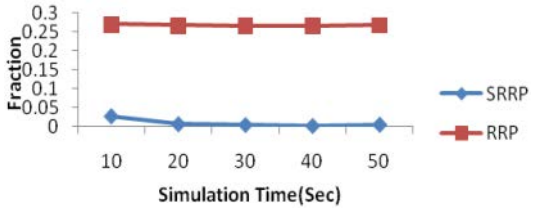

Fig. 10: Time vs drop ratio

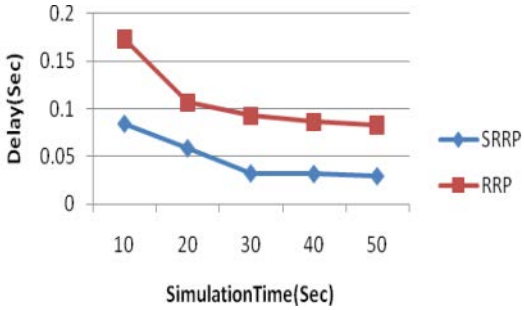

Fig. 11: Analysis between time vs delay

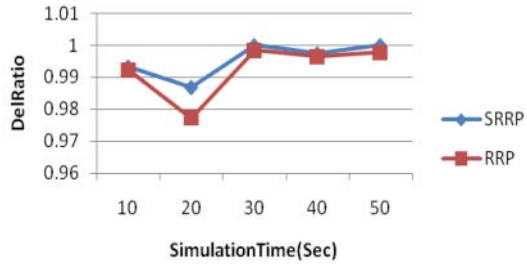

Fig. 12: Analysis time vs delievery ratio

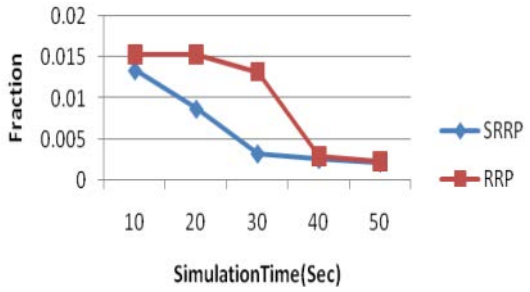

Fig. 13: Analysis between time vs drop ratio

Table 5: Delay for sower attack

End-to-End delay		
Simulation time (sec)	SRRP	RRP
10	0.43	1.36
20	2.09	5.41
30	4.59	9.42
40	6.52	13.4
50	9.19	17.5

Table 6: Packet delivery ratio for sower attack

Packet Delivery ratio		
Simulation time (sec)	SRRP	RRP
10	0.8624	0.2360
20	0.5384	0.2013
30	0.4909	0.1922
40	0.4178	0.1882
50	0.3832	0.1854

Table 7: Fraction of affected communications for sower attack

Fraction of affected communications		
Simulation time (sec)	SRRP	RRP
10	0.128	0.761
20	0.370	0.798
30	0.384	0.807
40	0.504	0.811
50	0.557	0.814

Table 8: Delay for responder attack

End-to-End delay		
Simulation time (sec)	SRRP	RRP
10	0.43	0.97
20	1.07	3.78
30	1.58	6.27
40	2.06	8.78
50	2.52	11.22

Table 9: Packet delivery ratio for responder attack

Packet Delivery ratio		
Simulation time (sec)	SRRP	RRP
10	0.862	0.524
20	0.885	0.509
30	0.893	0.509
40	0.897	0.513
50	0.896	0.514

Table 10: Fraction of affected communications for responder attack

Fraction of affected communications		
Simulation time (sec)	SRRP	RRP
10	0.128	0.416
20	0.096	0.488
30	0.095	0.488
40	0.093	0.486
50	0.096	0.484

For responder node attack: Figure 5-13 show the results of delay, delivery ratio and dropratio by varying the stop time from 10-50 for the CBR traffic in SRRP and RRP protocols. When comparing the performance of the two protocols, we infer that SRRP outperforms RRP by 57% in terms of delay, 1% in terms of delivery ratio and 29% in terms of dropratio (Table 8-10).

CONCLUSION

In this study, we have developed a secure data transmission technique which protects the data from all kinds of possible attacks. Initially, all the nodes in the network perform differential gossiping to aggregate reputation of its neighboring nodes. Based on the aggregated reputation, the overall reputation of the neighbors is determined by every node and recorded in the reputation table. Next, when a node needs to transmit data to a distant destination node, it encrypts the data and hides it using puzzles. Then the encrypted data is transmitted through intermediate nodes with good reputation which are determined using the reputation aggregation technique. When the destination node receives the puzzle, it decrypts it and recovers the original data. Thus, the security of data is ensured against all the attacks in this technique.

Notations:

i.	inode
j.	jnode
fb_{ij}.	feedback of node estimated by the node i
gw_{ij}.	gossip weight of node estimated by the node i
q.	: ratio of a node's degree to the average neighbor degree
$Convergence_{value}$:	converging value
S:	Source node
D:	Destination node
pkt	data packet transmitted by S
k:	random key generated by S
P:	Puzzle
E_k:	Commitment function denoted by symmetric encryption algorithm
π_1:	publicly known permutation
C:	variable, where $C = E_k(\pi_1(pkt))$
p^1:	Puzzle received by D
k^1:	key recovered by D
pkt^1:	Data packet decrypted by D and is estimated by
$E_k^1(C^1)$:	variable where $E_k^1(C^1) = pkt^1r$
r:	constant used to preserve the integrity of pkt^1
CRC:	Cyclic Redundancy Check

REFERENCES

Arulkumar, C.V., K. Jeyakumar, M. Malarmathi and T. Shanmugapriya, 2012. Secure communication in unstructured p2p networks based on reputation management and self certification. Intl. J. Comput. Appl., 44: 1-3.

Balfe, S., A.D. Lakhani and K.G. Paterson, 2005. Trusted computing: Providing security for peer-to-peer networks. Proceedings of the 5th IEEE International Conference on Peer-to-Peer Computing, August 31-September 2, 2005, IEEE, USA., ISBN: 0-7695-2376-5, pp: 117-124.

Gupta, R. and Y.N. Singh, 2015. Reputation aggregation in peer-to-peer network using differential gossip algorithm. IEEE. Trans. Knowl. Data Eng., 27: 2812-2823.

Li, H., 2008. A Configurable Online Reputation Aggregation System. University of Ottawa, Canada.

Liu, Y., J. Han and J. Wang, 2011. Rumor riding: Anonymizing unstructured peer-to-peer systems. IEEE. Trans. Parallel Distrib. Syst., 22: 464-475.

Pretre, B., 2005. Attacks on Peer-to-Peer Networks. Dept. of Computer Science Swiss Federal Institute of Technology, Zurich, Switzerland, Pages: 32.

Proano, A. and L. Lazos, 2012. Packet-hiding methods for preventing selective jamming attacks. IEEE. Trans. Depend. Secure Comput., 9: 101-114.

Sruthy, R.S., 2014. A secure cryptographic puzzle based approach ensuring total security for transmitted information with ip tracing. IOSR J. Comput. Eng., 16: 27-32.

Zhou, R. and K. Hwang, 2007. Gossip-based reputation aggregation for unstructured peer-to-peer networks. Proceedings of the IEEE. International Symposium Parallel and Distributed Processing, March 26-30, 2007, IEEE, Long Beach, California, ISBN: 1-4244-0909-8, pp: 1-10.